Swansea University
Prifysgol Abertawe

Cronfa
Setting Research Free

Swansea University E-Theses

Investigation of quality of services (QoS) support for real-time or mission critical services over IEEE 802.11e wireless networks.

Nwizege, Kenneth Sorle

How to cite:

Nwizege, Kenneth Sorle (2010) *Investigation of quality of services (QoS) support for real-time or mission critical services over IEEE 802.11e wireless networks..* thesis, Swansea University.
http://cronfa.swan.ac.uk/Record/cronfa42850

Use policy:

This item is brought to you by Swansea University. Any person downloading material is agreeing to abide by the terms of the repository licence: copies of full text items may be used or reproduced in any format or medium, without prior permission for personal research or study, educational or non-commercial purposes only. The copyright for any work remains with the original author unless otherwise specified. The full-text must not be sold in any format or medium without the formal permission of the copyright holder. Permission for multiple reproductions should be obtained from the original author.

Authors are personally responsible for adhering to copyright and publisher restrictions when uploading content to the repository.

Please link to the metadata record in the Swansea University repository, Cronfa (link given in the citation reference above.)

http://www.swansea.ac.uk/library/researchsupport/ris-support/

Institute of Advanced Telecommunications

Swansea University

Prifysgol Abertawe

United Kingdom

Swansea University
Prifysgol Abertawe

MPhil: Wireless Communications

Investigation of Quality of Services (QoS) Support for Real-Time or Mission Critical Services over IEEE 802.11e Wireless Networks.

Kenneth Sorle Nwizege

January 2010.

Supervisors:

Dr. Jianhua He and Prof. Tom Chen

ProQuest Number: 10821240

All rights reserved

INFORMATION TO ALL USERS
The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript
and there are missing pages, these will be noted. Also, if material had to be removed,
a note will indicate the deletion.

ProQuest 10821240

Published by ProQuest LLC (2018). Copyright of the Dissertation is held by the Author.

All rights reserved.
This work is protected against unauthorized copying under Title 17, United States Code
Microform Edition © ProQuest LLC.

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 – 1346

UNIVERSITY OF
LIBRARY
WALES SWANSEA

I certified that this project was carried out to the best of my knowledge through the supervision of my supervisors and other people's contributions. All the materials that are not original to this project are acknowledged in my references, and that the laws and principles used are according to scientific rules and valid, and also comply with IEEE and ITU-T standards.

Abstract.

Multimedia application is currently making much impact in this technological era. It has been the key driving force behind the convergence of fixed, mobile and IP networks. Furthermore, real-time applications are making head way in vehicular networks, mission critical applications which use dedicated short range communications (DSRC). 802.11e standards support quality of services (QoS) guarantees in these applications. This is opposed to the problem with 802.11 legacy which is based on distributed coordination function (DCF) , and its inability to prioritized applications for service differentiation. Simulation was done on various 802.11e networks which use enhanced DCF (EDCF). In these simulations, it was observed that controlling low priority applications enhances the effectiveness of high priority applications. Different MAC and traffic generation parameters were used in various scenarios. It was actually observed that high priority applications have greater impacts on the performance of the network and hence performs better when it comes to delay and throughput requirements. Even when the number of high priority applications were reduced, the results obtained was still able to satisfy QoS requirements for each traffic type. Results for different scenarios were taken and discussed. Also, differentiated values of delay, throughput and packet loss were recorded when same and different values of MAC and traffic generation parameters were used. In all results the International Telecommunications Union (ITU-T) values of these metrics parameters were kept low. These make the network design suitable for road safety application where very low delay is required for emergency messages and tolerable delay in routine messages. The results obtained show that , this network can be applicable in road safety, simply because of the low delay, and low loss which implies , messages to cars can be successfully delivered and also good throughput. 802.11 legacy standard lacks service differentiation that limits QoS support for real-time applications. These simulations were able to handle the drawback associated with this standard and prefer a better standard which is 802.11e that provides differentiated access to the metrics that was used in analyzing QoS in this research.

Acknowledgements

I am very grateful to the Almighty God for the wisdom and strength given to me to embark in this research. My sincere thanks to all my friends, and especially my family members. I appreciate the patience of my wife Mrs. Dorathy Nwizege and also for standing by me.

I am finally grateful to my supervisors, Dr. Jianhua He and Prof. Tom Chen For their great support and contributions during this research.

Table of Contents

List of Figures

List of Tables

1 Introduction

Wireless networks have emerged so well and become popular as they are deployed in almost every sector of life such as Schools, hospitals, coffee shops, airports, restaurants etc. Modern mobile devices such as laptops, PDAs are capable of deploying these services. The interesting thing is that, multimedia services such as voice over internet protocol (VoIP), video can be deployed using wireless technology known as WLAN. 802.11e is medium access control (MAC) is an emerging supplement to the IEEE 802.11.

Quality of service (QoS) in wireless networks is the primary focus of this thesis. It also helps to investigate the performance of IEEE 802.11 and IEEE 802.11e. The investigations made in Wireless networks has helped in learning more on the performance metrics and the advantages that 802.11e have compared to the other flavors like a, b, g etc, when it comes to QoS guarantee. This thesis is able to investigate the effect of the following metrics on network applications:

- delay
- throughput
- packet loss
- load analyses etc

1.1 Motivation

The rate at which WLAN and multimedia applications are so popular and challenging, is of great interest to us to work in this area, because almost every sector now makes use of WLAN, and wants to communicate via it using any of the multimedia applications. It is applicable in road safety, DSRC etc. And finally, because there is limitation of IEEE 802.11 when it comes to QoS guarantee, this motivated us to work on 802.11e that has Enhanced QoS features that offers differentiated services, although WIMAX has more than it, and this will be future area of research.

1.2 Problem Statement

The two access methods used in 802.11 Wireless LAN are distributed coordination function (DCF) and point coordination function (PCF). The 802.11 legacy DCF access mechanism does not support the concept of differentiating frames with different priorities. Basically, DCF is supposed to provide a channel access with equal probabilities to all stations contending for the channel access in a distributed manner. However, equal access probabilities are not desirable among stations with different priority frames. The emerging enhanced DCF (EDCF) is designed to provide differentiated, distributed channel accesses for frames with different priorities. EDCF is supposed to provide better performance enhancement for real time traffic as compared to DCF.

1.3 Objectives

The objectives for carrying out this project are as follows:

- to investigate the QoS metrics over multimedia applications
- to compare the performance of 802.11 and 801.11e in IEEE wireless standards
- analyze some of the applications of IEEE 802.11e in areas like mission critical collision, vehicle network, and road traffic safety applications etc.

1.4 Organization of thesis

Chapter 1 gives the summary of all that is involved in this thesis. It touches all the concepts that were used in this research. Chapter 2 reviews the work done and explanations of some of the concepts used. Chapter 3 expatiates on QoS architecture, in this chapter; all the metrics and enhancements in 802.11e are explained. Different mechanisms of the MAC layers are also explained in this chapter. Chapter4 talks about the Simulator that is used in this thesis, the Network simulator is called NS-2. Chapter 5 talks about the network design, topology, graphs, parameters used in our simulations, discussion of results and analysis. Chapter 6 concludes this research, contributions made were also mentioned and problem encountered. Recommendations and future work are also part of this chapter.

1.5 Background

Recent emergence of 3G and 4G of universal mobile telecommunications systems (UMTS) or wireless technologies has stirred up the interest of most researchers that are interested in the wireless transmission of video streams. The 3G replaces the GSM network in the early 1990s and work was done in this area in order to secure major global role after the comparative failures with previous generations of this technology. UMTS has the capability to handle data rate as high as 14.0 Mbps [1] using W-CDMA in theory with what HSDPA can offer. UMTS has been in deployable state in many countries since 2006 [1] and been in the state to be upgraded to HSDPA which is sometimes called 3.5G.

However, the explosion of (3G) and fourth generation (4G) wireless are now deploying and making [1] high-fidelity video over wireless channels to be a reality. In addition, Internet Protocol (IP) based architecture for 3G wireless systems promises to provide next generation wireless services such as voice, high-speed data, Internet access, audio and video streaming on all IP network [3] . On the contrary wireless video [5] has bandwidth, delay, and loss requirements, of which it is difficult for many existing mobile networks to provide a guaranteed quality of service since temporally high bit error rates are unavoidable during fading periods.

Road traffic safety has been a subject of worldwide concern of which road accidents have resulted in tremendous economic and productivity lost. During the last decade extensive studies have been conducted on road safety systems to actively prevent accidents or passively minimize the consequences of accidents. With the advances in wireless communications and mobile networking, collaborative safety applications (CSA) enabled by vehicular communications is widely regarded as a key to future road safety. Through vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications, complex traffic situation information may be acquired to support collaborative safe driving. For example, V2V communications can be used to determine and warn the driver of hazardous conditions such as other vehicles braking.

In addition, dedicated short range communications (DSRC) has been regarded as one of the most promising technology to provide a robust medium and affordable enough to be built into every vehicle. It is designed to provide both road safety (e.g. collaborative collision warning and collaborative collision avoidance) and commercial services (e.g. navigation, map and Internet access). Road safety applications will require reliable and timely wireless communications [71].

Furthermore, media access control (MAC) layer of DSRC is based on the IEEE 802.11 distributed coordination function (DCF), it is of the fact that due to random channel access based, MAC cannot provide guaranteed QoS. It is very important to understand quantitatively the performance of DSRC, in order to make better decisions on the adoption, control, adaptation and improvement of it. In this research work, we have investigated the impacts of the channel access parameters associated with the different services including AIFS and contention window. Based on the proposed model, we analyze the successful message delivery ratio and channel service delay for broadcast messages. The proposed analytical model can provide a convenient tool to evaluate the inter-vehicle safety applications and analyze the suitability of 802.11a based DSRC for road safety applications [71] .

1.6 OSI Reference Model

This was introduced by the international standard organization (ISO) to segment different stages in which packets or data are transmitted over the network. It gives an overview for distributed applications to be connected. The accepted structuring technique accepted by OSI is called Layering. The different layers perform a task of communicating with each system in a related subset. That is, the layers depend on the next lower layer to perform its functions and to withhold the information available in other layers. Communication in the OSI reference model is made possible by having corresponding peer layers in two systems to communicate .They communicate by a set of rules known as Protocols.

Layers are essential in this model since it helps to perform a well define function. When choosing each layer, it should be aimed at defining internationality standard protocols, layers boundaries as well should be chosen in order to reduced the information flow across the interfaces and number of layers should be large enough so that distinct functions needs to be thrown together in the same layer out of necessity and small enough that the architecture does not become un widely.

1.7 Layers

Physical: Deals with transmitting raw bits via a communication channel. The design criteria deal with ensuring that when one side sends a bit, the other side also receives a 1 bit and not a 0 bit. Design modalities in this layer greatly deals with mechanical, electrical and timing interfaces and the physical transmission medium that lies below the physical layer.

Data link: Responsible for transforming raw transmission facility into a line that appears free of undetected transmission errors to the network layer, to achieve this, the sender will break up the input data into data frames and transmit the frame sequentially. In the event of a reliable service, the receiver confirms correct receipt of each frame by sending back an acknowledgment frame. The major concern about this layer and other higher layers is to keep a fast transmitter from drowning a slow receiver in data. The mechanism is also incorporated with flow regulations and error handler to monitor the buffer capacity.

Network: This controls the operation of the subnet .The design criteria is aimed at determining how packets are routed from source to destinations. The design mechanism can also be highly dynamic, being determined a new for each packet to reflect the current network head.

Transport :The role of this layer is the breaking down of data that is accepted from the upper layers into small units if there is need and then send it to the network layer, and ensuring that the pieces arrives correctly at the other end. In addition, it determines what type of service that is to be provided by the session layer .It is a true end-to-end layer, from source to destination.

Session: This layer allows users in varying machines to establish sessions between them. It offers various services such as dialog control, token management and synchronization.

Presentation: This is concerned with the syntax and semantics of the information transmitted. It manages abstract data structures and allows higher-level data structures (e.g. banking records) to be defined and exchanged.

Application: This contains protocols that are frequently needed by users. Example is the HTTP which is the basis of the World Wide Web. Other application protocols are used for file transfer, email and network news.

1.7.1 Layers and unit of exchanged

Physical: Bit

Data link: frame

Network: Packet

Transport: TPDU

Session: SPDU

Presentation: PPDU

Application: APDU

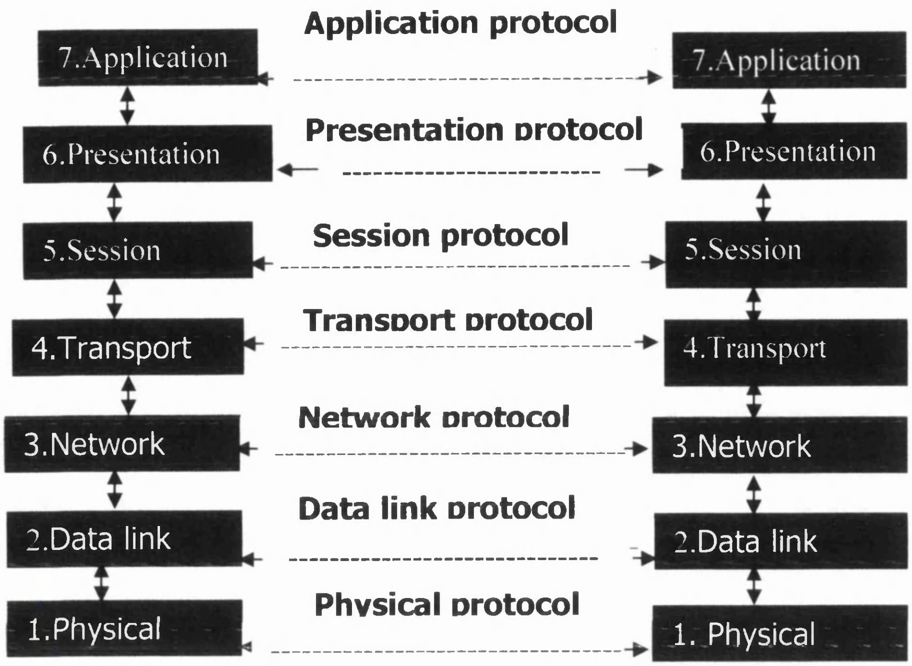

Fig 1.0 OSI Reference Model

The IEEE Std 802.11, 1999 Edition is a revision of IEEE Std 802.11-1997. This standard defines the protocol and compatible interconnection of data communication equipment via the "air", radio or infrared, in a local area network (LAN) using the carrier sense multiple access protocol with collision avoidance (CSMA/CA) medium sharing mechanism. The MAC supports operation under control of an access point (AP) as well as between independent stations. The protocol includes authentication, association, and reassociation services, an optional encryption or decryption procedure, power management to reduce power consumption in mobile stations, and a point coordination function for time bounded transfer of data. The standard includes the definition of the management information base (MIB) using Abstract Syntax Notation 1 (ASN.1) and specifies the MAC protocol in a formal way, using the Specification and Description Language (SDL). The infrared implementation of the PHY supports 1 Mbps data rate with an optional 2 Mbps extension.

The radio implementations of the PHY specify either a frequency-hopping spread spectrum (FHSS) supporting 1 Mbps and an optional 2 Mbps data rate or a direct sequence spread spectrum (DSSS) supporting both 1 and 2 Mbps data rates.

The scope of this standard is to develop a medium access control (MAC) and physical layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within a local area. The purpose of this standard is to provide wireless connectivity to automatic machinery, equipment, or stations that require rapid deployment, which may be portable or hand-held, or which may be mounted on moving vehicles within a local area. This standard also offers regulatory bodies a means of standardizing access to one or more frequency bands for the purpose of local area communication. Specifically, this standard

- describes the functions and services required by an IEEE 802.11 compliant device to operate within ad hoc and infrastructure networks as well as the aspects of station mobility (transition) within those networks.
- defines the MAC procedures to support the asynchronous MAC service data unit (MSDU) delivery services.
- defines several PHY signalling techniques and interface functions that are controlled by the IEEE 802.11 MAC.
- permits the operation of an IEEE 802.11 conformant device within a wireless local area network (LAN) that may coexist with multiple overlapping IEEE 802.11 wireless LANs.
- describes the requirements and procedures to provide privacy of user information being transferred over the wireless medium (WM) and authentication of IEEE 802.11 conformant devices [94] .

As many 802.x protocol, the 802.11 protocol covers the MAC and Physical Layer, the Standards currently defines a single MAC which interacts with three PHYs (all of them running at 1 and 2 Mbps):

- frequency hopping spread spectrum in the 2.4 GHz Band
- direct sequence spread spectrum in the 2.4 GHz Band
- InfraRed

<table>
<tr><td colspan="3">802.2</td><td rowspan="2">Data link layer</td></tr>
<tr><td colspan="3">802.11 MAC</td></tr>
<tr><td>FH</td><td>DS</td><td>IR</td><td>PHY</td></tr>
</table>

Fig 1.1 MAC and PHY Layer

eyond the standard functionality usually performed by MAC Layers, the 802.11 MAC performs other nctions that are typically related to upper layer protocols, such as Fragmentation, Packet transmissions and Acknowledgments. The MAC Layer defines two different access methods, the stributed coordination function (DCF) and the point coordination function (PCF) [94] . While the DCF responsible for asynchronous data services, the PCF was developed for time-bounded services. The CF is used in the contention-free period (CFP), while the DCF handles the contention period (CP).

ne CFP and one CP are combined to a superframe. Superframes are separated by periodic anagement frames, the so-called Beacon frames. 802.11 uses three different inter-packet gaps, enoted as interframe spaces, to control the medium access, i.e. to give stations in specific cases a gher or lower priority:

- Short interframe space (SIFS)
- PCF interframe space (PIFS)
- DCF interframe space (DIFS)

SIFS is the shortest interframe space and is used for acknowledgments (ACKs), CTS (clear-to-send) frames and several following MAC protocol data unit (MPDUs) of a fragment burst as well as for the response of a polled station in the PCF. SIFS personates the highest priority and assures that a station is able to finish a frame-exchange sequence before other stations are in the position to gain access to the medium. In the CFP the point coordinator (PC) polls stations and must have therefore a prioritized access to the medium. This is realized by PIFS which is longer than SIFS but smaller than DIFS.

The DIFS is used in the CP and describes the duration of time in which the medium has to be idle before a station is allowed to send or decrement its backoff. DIFS is the longest interframe space and consequently has the lowest priority. Under legacy DCF access method; there are three access mechanisms with the priority based such as Blackburst, enhanced DCF (EDCF) and Deng's scheme. Meanwhile, there are also three access mechanisms with using fair scheduling such as distributed weighted fair queuing (DWFQ), distributed fair scheduling (DFS) and distributed deficit round robin (DDRR) .Under legacy PCF access method, the access mechanism that is used is hybrid coordination function (HCF). Although, in this project, the task only focus on DCF access method and evaluation only be done for the legacy DCF mode and EDCF mode.

1.7.2 Distributed Coordination Function (DCF)

This is one of the basic access mechanics used by IEEE 802.11 MAC to provide contention based channel access and MAC layer protocol in 802.11 standard [6, 7] . It uses carrier sense multiple access/collision avoidance (CSMA/CA) scheme with binary exponential back off [8]. DCF is also regarded as a mandatory based access mechanism.

The problem of 802.11 legacy is that is does not support the concept of differentiating frames with different priorities. Also due to the random nature of channel based, the MAC it not able to provide guaranteed QoS .DCF provides channel access with equal probabilities to all stations contending for the channel access in a distributed manner. On the other hand, equal access probabilities are not desirable among stations with different priority frames.DCF does not guarantee QoS; it can only support best effort services.

In DCF, all the stations compete for the available resources and channel having same priority.DCF has many limitations: It does not provide QoS guarantee, neither does it support real time application. It was primarily designed for equal priorities, but it does not support the concept of differentiation of frames with different user priorities. Increasing time during contention at the channel leads to throughout degradation and high delay. However it is simple and robust and can provide priority service with little modifications.

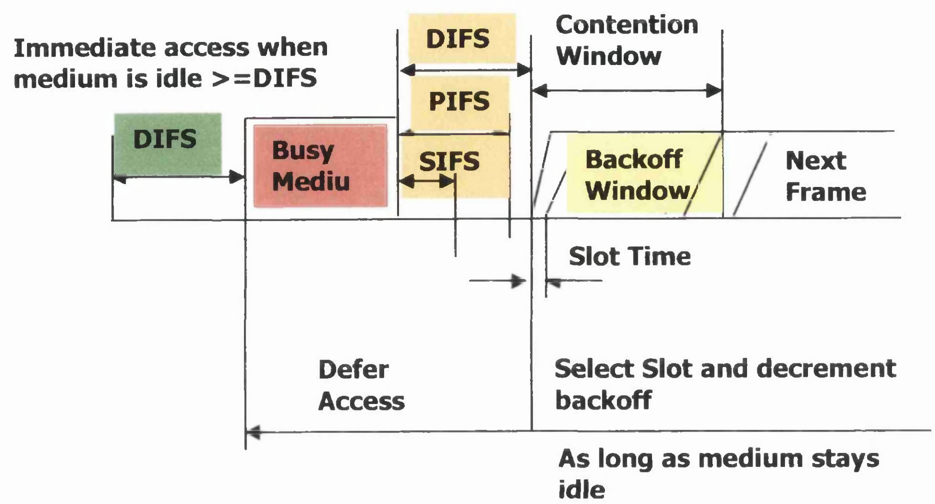

Fig 1.2 IEEE 802.11 DCF Channel Access

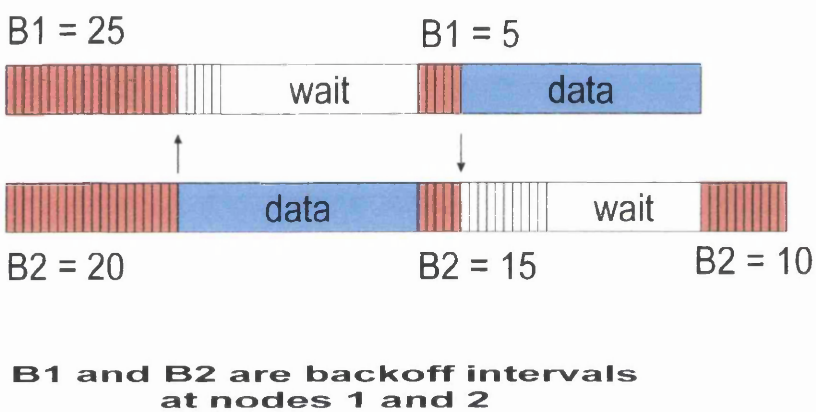

Fig.1.3 Example of DCF [79]

1.7.3 Point Coordination Function (PCF)

This uses the centralized or polling based to provide free channel access in 802.11 MAC layer and also known as an optional access mechanism. This mechanism can provide a level of service guarantee by using a central scheduling scheme unlike DCF but introduces extra complexity and protocol overhead .However, it provides good real time operation and also enhances data transmission rate [79] . PCF defines a coordinator station that is known as point coordinator (PC), which might start transmission after it senses the channels is idle for a PCF interframe space (PIFS).To avoid collision with current transmissions, PIFS must be higher than the short interframe space (SIFS) which is used for fragmentation and control frames [9].

PCF mechanism has some problems that may lead to poor QoS performance , and hence is not widely used among existing WLAN, and in all is not ideal for handling QoS requirements [9] ,it can only be used in infrastructure –based network [10].

1.7.4 Enhanced Distributed Coordination Function (EDCF)

This mechanism is what really made the difference between 802.11 and 802.1e. It is able to provide a differentiated channel access to frames with different priorities [11]. It exhibits an optional feature called the contention-free burst (CFB) that enables multiple MAC frame transmissions during a single transmission opportunity (TXOP). With this new scheme, multiple queues can work independently with a single MAC which is not available in DCF mechanism.

Furthermore, in this scheme, a station cannot transmit a frame that goes beyond a time interval called EDCF transmission opportunity (TXOP) limit [11]. EDCF is not a separate coordination function but part of a single coordination function known as hybrid coordination function (HCF) which combines both attributes of DCF and PCF [11].

The improvement of DCF mechanism also bring to what is known as the Enhanced distributed channel access (EDCA) so that traffic prioritization can be deployed as oppose to what is obtained in DCF. This provides quantitative bandwidth guarantees for WLANs, rather a prioritized service .It is an extension of DCF mechanism that enables distributed differentiated access to the wireless channel with the support of multiple access categories (ACs) [12]. Furthermore, in this mechanism, higher priority access category has smaller minimum contention window CW_{min} , but have higher probability in accessing channel [12].

In EDCA, each traffic flow has one of the four ACs, with each one having a different medium access priority, them attribute works well when the network is moderately loaded [13]. This mechanism provides service differentiation and also classifies the traffic in to 8 different classed, and is able to provide contention-based channel access.

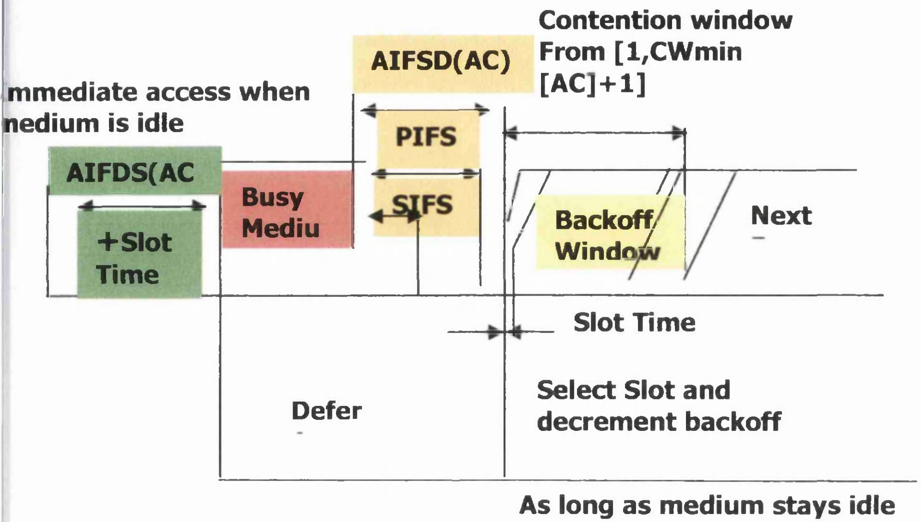

Fig 1.4 IEEE 802.11e Access

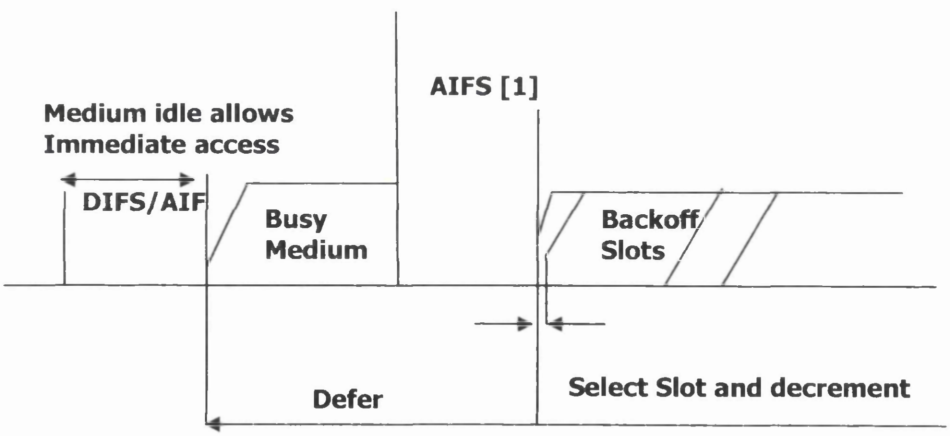

Fig 1.5 EDCA Prioritized Channel Access

Table 1.0: IEEE 802.11e Priority to Access Category Mappings [52]

Priority	Access Category (AC)	Designation (Informative)
0	0	Best Effort
1	0	Best Effort
2	0	Best Effort
3	1	Video Probe
4	2	Video
5	2	Video
6	3	Voice
7	3	Voice

Table 1.1 IEEE 802.11e Typical QoS Parameters [52]

Access Category	CW_{min}	CW_{max}	AIFS
0	CW_{min}	CW_{max}	2* DIFS
1	CW_{min}	CW_{max}	DIFS
2	$(CW_{min}+1)/2-1$	CW_{min}	DIFS
3	$(CW_{min}+1)/4-1$	$(CW_{min}+1)/2-1$	DIFS

1.7.5 Hybrid Coordination Function (HCF)

This mechanism utilizes a contention-based channel access scheme known as the EDCA, together with a polling-based method, called HCF Controlled Channel Access (HCCA). This is the basis for EDCF and it controls both CFP and CP, hence it is required that one station should be responsible for the management of the medium access [10].

HCF controlled channel access (HCCA) is a substitute of PCF. It uses a hybrid coordinators(HC) which is located at QoS access point (QAP), so as to schedule and distribute time intervals known as transmission opportunities (TXOPs) to QoS stations (QSTAs) in accordance to a particular flow requirement known as traffic specifications (TSPECs) [9]. It reserves bandwidth by accessing the control which holds the bandwidth for a certain time (parameterized QoS) which is mostly used by CFP. Features of this mechanism include:

- operates in CFP and CP.
- provides Guaranteed Services with a much higher probability than EDCA.
- combines the advantages of PCF and DCF.
- coordinates the traffic in any fashion (not just round- robin).

1.7.6 Basic EDCF Parameters

The basic features that really differentiate DCF from EDCF are:

- arbitrary interframe space access category (AIFS[AC]): This is an integer greater than zero and it has this mathematical relationship

AIFSD [AC] = SIFS +AIFS [AC] .SlotTime

- minimum contention window access category (CW_{min} [AC]): This is used to select the backoff timer of which its value is set from CW to CW_{min} after each successful transmission, this depends on BI
- maximum contention window access category (CW_{max} [AC]: Maximal CW value for a given AC similar to CW_{min}. It is also on a per AC basis [14].

ACs with smaller values of these 3 parameters have higher priority to access the medium [14], also depends on BI.

1.8 Wireless Local Area Networks (WLANs)

The emergence of Wireless local areas networks (WLANs) has made the deployment of multimedia applications more popular and has become the key behind mobile and IP networks. The rapid growth and deployment of WLANs cannot be overemphasised. Mobile communication devices like Laptops and PDAs have become more and more popular. For easy communication between these devices as well as the connection to the Internet, Wireless LAN (IEEE 802.11) is used in a lot of scenarios today. Especially the number of WLANs in public facilities likes railway stations, official buildings and airports increases rapidly, not taking into account the entire small private "home" WLANs. The increase in popularity of Wireless LANs led to more close considerations with respect to multimedia traffic over WLANs in the past. The most sensitive area of multimedia traffic is Internet telephony (Voice-over-IP).

In particular the delay is most critical in voice-over-IP (VoIP) applications. With the emergence of this technology, most campuses, hospitals, airports, Offices, homes etc are now enjoying the existence of this technology. The fascinating thing about it is its flexibility in usage; multiple people can roam about the house or office while accessing the internet. It stands out to be one of the cheapest means of surfing the internet. It also allows files transfer for immediate use. In this technology, computers communicate with one another via wireless media using short range frequencies [15].

However, the flexibility WLANs has also encourage many users today, this is because it is easy to set up since no cables are needed for connection and our mobile phones can also be used to surf the internet any where you are. It makes job easier and faster and moreover saves much time. WLAN technology uses infrared, spread spectrum, laser, microwave and satellite to support multimedia services like VoIP, data transfer and video in both local and metropolitan area networks (MAN). Wireless network is not really vendor specific, as it can connect to any other wired network without problems, it works perfectly with wired network, and this can be seen in cases where the network is so large like that of MAN.

IEEE 802.11 WLAN is a fast growing technology all over the world and sets to be the most deployable in the next generation, wireless networks. The ubiquitous characteristics of WLAN such as convenience, expandability, low cost make it an attractive service to go by. It provides ease of access and usability in homes, offices, schools, business environments etc. The flexibility and ease of this technology has made it so popular and everyone wanting to use it. There is no much about setting up, since cables are not required.

The IEEE 802.11-based wireless LANs have been widely deployed for local area high-speed data access [8, 14] .It include a set of specifications developed by the IEEE for the WLAN technology.

It consists of groups of wireless stations called basic service sets (BSS) which executes a distribution function (DF) to regulate the exclusive access to the shared wireless medium. Ideally, all BSS can communicate with each other. To transmit to a BSS, an AP is required, which has similar functions as that of base stations.

In 802.11 WLANS, MAC layer defines the procedure for 802.11 stations to share a common radio channel. The mechanisms are: the mandatory DCF and the optional PCF. More details on these mechanisms will be explained deeply in a later chapter. There are different flavors of 802.11 standards, these include, a, b, g. n. and the enhanced e. Full details about these standards are listed in the table below.

Table 1.2 WLAN Standards [81]

Standard	Release	Data Rate	Range(Maximum)
802.11	1997	2Mbits/s	20metres
802.11a	1999	54Mbits/s	35metres
802.11b	1999	11Mbits/s	38metres
802.11g	2003	54Mbits/s	38metres
802.11n	Draft version	>200Mbits/s	70metres
802.16e-2005	2005	70Mbits/s(Short range) 10Mbits/s(10Km)	70Km

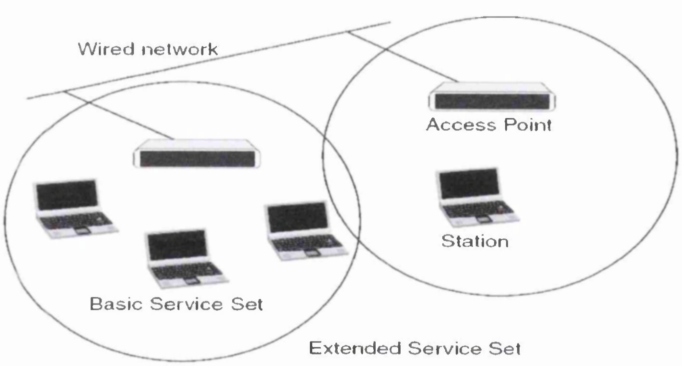

Fig 1.6 IEEE 802.11 Service Set

1.9 IEEE 802.11e

Since 802.11 lack the features for QoS support , there was the need to move ahead for another standard of WLAN so that multimedia applications can be deployed with QoS guarantee. This is what led to 802.11e standard which has QoS improvements of the 802.11 MAC layer. It was approved by IEEE in July 2005 [16]. It basically adds priorities to the MAC layer and also provides improvements of the MAC access mechanisms known from the legacy 802.11 WLAN.It implements two access mechanisms, the enhanced distributed channel access (EDCA) and the HCF controlled channel access (HCCA). Details of these mechanisms will be explained in a later chapter.

The benefits of wireless LANs include:

- **Convenience**: The wireless nature of such networks allows users to access network resources from nearly any convenient location within their primary network environment (home or office). With the increasing saturation of laptop-style computers, this is particularly relevant.
- **Mobility:** With the emergence of public wireless networks, users can access the internet even outside their normal work environment. Most chain coffee shops, for example, offer their customers a wireless connection to the internet at little or no cost.
- **Productivity**: Users connected to a wireless network can maintain a nearly constant affiliation with their desired network as they roam from place to place. For a business, this implies that an employment can potentially be more productive as his or her work can be accomplished from any convenient location.
- **Deployment**: Initial setup of an infrastructure-based wireless network requires little more than a single AP. Wired networks, on the other hand, have the additional cost and complexity of actual physical cables being run to numerous locations (which can even be impossible for hard-to-reach locations within a building).
- **Expandability**: Wireless networks can serve a suddenly-increased number of clients with the existing equipment. In a wired network, additional clients would require additional wiring.

- **Cost**: Wireless networking hardware is at worst modest increase from wired counterparts. This potentially reduces cost more than the wired counterpart and labor associated to running physical cables.

2.1 Introduction

This chapter discusses about wireless networks, the different flavors and their features, access mechanisms available in wireless networks, etc.

IEEE 802.11 WLAN is a fast growing technology all over the world and sets to be the most deployabe in the next generation, wireless networks. The ubiquitous characteristics of WLAN such as convenience, expandability, low cost make it an attractive service to go by. It provides ease of access and usability in homes, offices, schools, business environments etc. The flexibility and ease of this technology has made it so popular and everyone wanting to use it. There is no much about setting up, since cables are not required.

With current research and analysis on WLAN parameters, it is slower than wired LAN having a data rate between 11 and 54 Mbps compared to wired network operating between 100Mbps and 1000Mbps [21]. Wireless networks involve various kinds of radio access networks such as WLAN and mobile cellular networks. Although can be independent, they are more of a typical extension to a wired network [22] WLAN is typically used with wireless enabled mobile devices such as computers, notebooks, PDAs and Tablets PCs. This gives users the opportunity to exploit the features of wireless network such as convenience, portability, mobility etc.

With the explosion of IEEE.802.11 technology, multimedia applications such as video conferencing, VoIP, etc finds more usefulness with the existence of WLAN. People now can surf the internet, make file transfers, share documents while at the airports, coffee shops, offices and on campuses. There is no need to wait until cables are connected from one computer to the other to establish a network and centrally getting access from a server. However, QoS is required to deploy these services mentioned.

2.2 How does it work?

Ad-hoc networks remains the simplest [22], form of wireless network for now, that can be created by two or more wireless enabled computers with the aim of mutual Communications.

There are two main types of wireless networks, ad-doc mode and infrastructure mode. The former does not need an access point (AP) because there is direct communication while the later needs an AP.

Wireless network interface cards (NIC) must be built or be available on any device that is expected to be used in WLAN operations. Different interfaces are available to be used along with the different WLAN devices, some of them are: PCMCIA and PCI cards CF (Compact Flash), SD (Secure Digital) cards, and USB wireless network adaptors [22]. In many scenarios, it is needed to be installed before the device can function. Once the proper configurations and installation has been done, the wireless device is set to be in used.

2.2.1 Challenges in Wireless Networks.

Despite wireless networks owe a lot of advantages over wired, it is a recommendable and deployable technology welcomes by 3GPP, there is still much challenges to be faced and also to find a lasting solution to it. But the weakest area of wireless network is **SECURITY**. Some of the challenges for researchers and those deploying wireless technology include:

Data encryption: Wireless equivalent privacy (WEP) being the standard for wireless encryption has been broken. Although wireless application protocol (WAP) is more robust than WEP, but it can still be intruded.

Bandwidth hijacking, as one of the insecurity issues can be penetrated with a wireless laptop which can maliciously tap into your bandwidth without thanking you. Many more of these hijackers can even penetrate into your internal network resources through an unsecured WAP.

Malicious codes have been written to force wireless device to make phone calls, because many of them also have telephony capabilities.

Data theft which is more alarming in businesses is the reason why encryption has to be properly done, so that before data is transmitted, it is properly encrypted.

Low power networking: the size and battery power limitation of wireless mobile devices place a limitation on the range and throughput that can be supported by a WLAN.

Data rate enhancement: there is the need to improve on the current data rate to support high data rate applications like video transmission. Data compression plays a major role when a multimedia application such as video conferencing is to be in a wireless network. MPEG-4 standard of video transmission produces compression ratios of the order of 75 to 100. The challenge now is on how to improve these data compression to produce high quality audio.

2.2.2 How to handle the problems of WLAN

❖ **Security issues**

Wireless LAN equipment come with default WEP and this security standard is not strong and reliable as compared to others. Some of the weaknesses associated with it are: weak key management, weak endpoint authentication, and is advisable to be used if there is no other solution.

However, there are some better security standards such as Wi-Fi protected access (WPA).This was first deployed in 2003, it is identified as a subset of 802.11i security standard for wireless LAN [22], which was ratified in June 2004. To maintain its security standard, 802.11b and 802.11g products were in August 2003 required to be in conformity with WPA standard. Equipment having the later standard can be upgraded to this current WPA standard using a software upgrade. The unique elements of WPA are:

- ❖ authentication using 802.1x protocol (enterprise mode only) [22].
- ❖ data encryption through temporal key integrity protocol (TKIP) [22].
- ❖ data validation with message integrity check (MIC) [22].

WPA is compatible with the usage of several extensible authentication protocols (EAPs). It has features of 1EEE 802.11i standard and runs either on enterprise or Pre-shared key (PSK) mode. For authentication, the former requires an authentication server and dynamic key distribution while the later does not [22].

Wireless LAN transceivers are designed [21] to serve computers throughout a structure with uninterrupted service using radio frequencies. Because of space and cost, the antennas typically present on wireless networking cards in the end computers and are generally relatively poor [21].

To get a perfect reception of signals by using such limited antennas throughout even a modest area, the wireless LAN transceiver has to make do with a fairly considerable amount of power. What this means is that not only can the wireless packets be intercepted by a nearby adversary's poorly-equipped computer, but more importantly, a user willing to spend a small amount of money on a good quality antenna can pick up packets at a remarkable distance; perhaps hundreds of times the radius as the typical user.

Computer users who are dedicated to cracking wireless networks are called wardrivers. On a wired network, any adversary would first have to overcome the physical limitation of tapping into the actual wires, but this is not an issue with wireless packets.

To overcome this, wireless network users usually choose to utilize various encryption technologies available such as Wi-Fi protected access (WPA). Some of the older encryption methods, such as WEP are known to have weaknesses that a dedicated adversary can compromise. The typical range of a common 802.11g [23,24], network with standard equipment is on the order of tens of meters. While sufficient for a typical home, it will be insufficient in a larger structure.

To obtain additional range, repeaters or additional access points will have to be purchased. Costs for these items can add up quickly. Other technologies are in the development phase, however, which feature increased range, hoping to render this disadvantage irrelevant .There is the solution to this issue, which is simply just to install a specialized antenna to handle this issue.

❖ Speed

This is one of the problems faced by this technology. The transmission speed of all wireless LANs vary with file size, number of users, distance from the AP and any interference present in the environment. At the distance from the AP [22] the data rate for 802.11a,802.11g standard equipment reduces from 54Mbps to 48, 36, 24, 18, 12, 9 or 6 Mbps, while that of 802.11b reduced from 11Mbps to 5.5Mbps, 2Mbps or 1Mbps [22].

The speed on most wireless networks (typically 1-108 Mbps) [25,26] is reasonably slow compared to the slowest common wired networks (100 Mbps up to several Gbps). There are also performance issues caused by TCP and its built-in congestion avoidance. For most users, however, this observation is irrelevant since the speed bottleneck is not in the wireless routing but rather in the outside network connectivity itself. For example, the maximum ADSL throughput (usually 8 Mbps or less) offered by telecommunication companies to general-purpose customers is already far slower than the slowest wireless network to which it is typically connected. That is to say, in most environments, a wireless network running at its slowest speed is still faster than the internet connection serving it in the first place. However, in specialized environments, the throughput of a wired network might be necessary. Newer standards such as 802.11n [26] are addressing this limitation and will support peak throughputs in the range of 100-200 Mbps.

❖ Reliability

Like any radio frequency transmission, wireless networking signals are subject to a wide variety of interference, as well as complex propagation effects (such as multipath, or especially in this case Racian fading [26] that are beyond the control of the network administrator. In the case of typical networks, modulation is achieved by complicated forms of phase-shift keying (PSK) or quadrature amplitude modulation (QAM), making interference and propagation effects all the more disturbing.

As a result, important network resources such as servers are rarely connected wirelessly. In wireless network implementation, users have the mobility to move around within a broad coverage area and still be in connection to the network, as per home users, the ease in its installation makes me more usable by many. For business on the other hand, public places like airports, coffee shops has began to offer wireless services for the ease and comfort of the waiting customers, so that they can conveniently surf the web, and share file while waiting. Wireless hardware gives us the necessary horsepower.

2.3 Classification of Wireless Networks

To understand the operation of wireless network, categorizing it has helped for better implementation of its different technologies because of its varying standards. Some of these classes include:

- ❖ personal area network (PAN, few 10s of meters)
- ❖ local area network (LAN, few 100 meters)
- ❖ metropolitan area network (MAN, several KMs)
- ❖ wide area network (WAN, national/global coverage)
- ❖ wireless personal area network (WPAN) WPAN operates within 10s of meters, and network between devices is carried or won by a near person. The followings are examples of WPAN
- ❖ interconnection between a laptop and projector equipment
- ❖ interconnection between a mobile phone and a headset.

WPAN uses the following technologies, InfraRed (IrDA) and IEEE 802.15 radio standards.

Wireless local area networks (WLAN) are peculiar in home and office environment, which typically gives access to a fixed infrastructure. Some of these examples include: Internet access at public places like coffee shops, campus communities, pubs, restaurants, airports, interconnection of stationary and mobile devices such as desktops, laptops, telephones, and television etc. WLAN uses the following technologies, IEEE 802.11 radio standards (Wi-Fi), digital enhanced cordless telephony (DECT).

Wireless metropolitan area network (WMAN). This type of network covers a city or metropolitan area, which is implemented alternatively for lying of cables and optic fibres. Examples include: Broadband wireless solution for access to homes interconnecting operator network to WLANS or end user WMAN uses IEEE 802.16 radio standards):Wireless wide area networks (WWAN) .This type of network coverage covers a country or entire globe, by interconnecting several WMANs, access can be provided at anytime and anywhere. Examples of these include: Cellular network, Satellite systems. WWAN use the following technologies, GSM, MTS, and HSDPA.

❖ 802.11 Family

The most basic security features of 802.11 are: Authentication, Confidentiality and Integrity. The 802.11 family currently include six over-the –air modulation techniques that all uses same protocol. 802.11a, b, g are the most popular techniques. 802.11b was the first widely accepted wireless networking standard, followed by 802.11a and 802.11g .802.11b and 802.11g standards use the 2.40 GHz band while 802.11a standard uses the 5GHz band.

2.3.1 Description of 802.11 Wireless standards

❖ 802.11a

This was released after 802.11b, it is more expensive than 802.11b and so not so much adopted. Manufactures of equipment for this standard responded to lack of market success by improving the implementations and by making technology that can use more than one 802.11 standard.

It has advantage of less interference because of its 5GHz band occupancy .The disadvantage about this standard is that there is restriction in its line of site, because of high frequency band requirements, this makes this standard to use more APs. 802.11a cannot penetrate as far as 802.11b, since it is absorbed more readily.

❖ 802.11b

Its cards can operate at 11Mbit/s, but will scale back to 5.5, then 2 and then 1Mbit/s respectively. It is less susceptible to corruption due to interference and signal attenuation. It's typical range is 30m at 11Mbps and 90m at 1Mbps.

❖ 802.11e

This is an enhancement version of 802.11 standards; it offers more QoS features because of the access mechanisms used. Much detail about the flavor is discussed later in this chapter. It defines how the minimum contention windows for the different classes are communicated to the wireless stations, but not how to depend on the network load and traffic characteristics in order to achieve efficient channel utilization [12]. Resource control is efficient in this type of wireless network when properly planned and implemented. This is what led of QoS support that is not obtainable in the order standards.

Table 2.0 IEEE 802.11e Parameters [81]

Basic Rate	1 Mbps
Data Rate	11Mbps
PLCP Preamble and Header	192 bits
MAC Header +FCS (Frame Check Sequence)	224 bits
ACK Frame Size (Not including PLCP)	112 bits
SIFS	20 μs
Time slot	10 μs

It defines a frame-work for the management of resources and traffic, but the actual algorithms and techniques used within the framework are open to competing implementations, and which can easily affect the performance obtained by a QoS enabled access point (QAP) [27].

This standard supplements and addresses the issue of QoS support in wireless LANs. The MAC protocol of 802.11e is the hybrid coordination function (HCF), which supports both contention – based and controls channel access [27].

❖ 802.11g

This has net throughput like that of 802.11a, and works in the 2.4GHz band like 802.11b but operates at a maximum raw data rate of 54Mbps. It suffers from same interference problem as 802.11b which is already crowded in the 2.4GHz range. The devices that operate in this range include: Bluetooth devices, cordless telephones, microwave ovens .The presence of 802.11b reduces the speed of 802.11g network in older networks.

❖ 802.11i

This is a supplemental draft standard with its intention to improve WLAN Security

This standard describes the encrypted transmission of data between systems of 802.11a and 802.11b WLANs. Is also defines new encryption key protocols including the temporal key integrity protocol (TKIP) and the advanced encryption standard (AES) .AES requires hardware upgrades. This is the ratified security standard.

❖ 802.11n

This is about 50 times faster than 802.11b, and up to 10 times faster than 802.11a or 802.11g.The real data throughput is estimated to reach a theoretical 540Mbps; this requires a higher raw data rate at the physical layer.

802.11n is another standard that has recently been developed; the standard is still under development, although products designed based on draft versions of the standard are being sold. Other standards in the family (c-f, h, j) are service enhancements and extensions or corrections to previous specifications.

❖ 802.11r

This is a standard in development for fast roaming between APs .Due to reauthentication with each AP resulting to the mobility of users, it leads to delay and then disrupt low latency applications such as voice and video .But this new standard will allow for pre-authentication with other APs before handover takes place.

❖ 802.11s

As of march 2006, the IEEE ESS mesh networking task group (TGs) was developing a standard for wireless mesh networks (IEEE 802.11 s), although there is existing Wi-Fi mesh network that plays same role with this, but there is no 802.11s, this standard has expected a ratification in 2007 [22].Mesh networks have some peculiar characteristics such as expandability, resilience, large coverage, flexibility etc.

❖ 802.16/WIMAX

WIMAX is based on IEEE802.16 standards, and a very high speed deplorable wireless technology currently exhibited by wireless users. Worldwide interoperability for microwave access (WIMAX) forum [22] is a group that is responsible for this technology and ensure that the standard be kept and maintained according to the rules. It is intended to provide a wireless broadband coverage over a large area and has an in-built QoS. There are two main standards for this:

- **IEEE 802.16-2004**:This was ratified in June 2004 [22] and is expected to provide fixed/nomadic wireless broadband access at a theoretical shared peak rate of 72Mbps and a maximum range of 50km. The first WIMAX implementations are expected to provide a wireless alternative to DSL/cable broadband internet access. The first WIMAX certified equipment appeared in January 2006 [22].

- **IEEE 802.16e-2005**: This standard is for mobile wireless broadband and was ratified in December 2005, and the first product was expected to go through WIMAX certification as of 2006. The expectation of WIMAX operability is to be able to achieve 3 Km coverage and a speed of 15Mbps that can be shared by all users on the network.

❖ 802.11 Operational mode

An 802.11 AP may operate in one of the three modes: Legacy (only 802.11a, b, and g), mixed (802.11a, b, g, and n), greenfield (only 802.11n) –maximum performance.

2.4 Types of WLANS

WIMAX is a telecommunications technology aimed at providing wireless data over long distances in a variety of ways, from point-to-point links to full mobile cellular type access. It is based on the IEEE 802.16 standard, which is also called wireless MAN. WIMAX allows a user, for example, to browse the Internet on a laptop computer without physically connecting the laptop to a router, hub or switch via an Ethernet cable.

WIMAX is an open, worldwide standard that covers both fixed and mobile deployments. The only broadband wireless standard built specifically to deliver data, Mobile WIMAX's multi-megabit data rates can lay the foundation for innovative multimedia services and support multimedia content.
The word "Multimedia" simply means being able to communicate in more than one way. This means that, whether you are aware of it or not, you already give multimedia presentations. It is all about communicating in several ways. For example the computer you are using to view this material is capable of flashing text and beeping when there is a problem. It is already a multimedia computer- anything else is a matter of degree. In other words the more capable your computer is at handling sound, video and graphics the better your multimedia packages will look.
Ultra-Wideband (UWB): This is a technology for transmitting information spread over a large bandwidth (>500 MHz) that should, in theory and under the right circumstances, be able to share spectrum with other users.

Ultra Wideband was traditionally accepted as pulse radio, but FCC and ITU-R now define UWB in terms of a transmission from an antenna for which the emitted signal bandwidth exceeds the lesser of 500 MHz or 20% of the center frequency. A significant difference between traditional radio transmissions and UWB radio transmissions is that traditional transmissions transmit information by varying the power/frequency/and or phase of a sinusoidal wave. UWB transmissions can transmit information by generating radio energy at specific time instants and occupying large bandwidth thus enabling a pulse-position or time-modulation. UWB is used as a part of location systems and real time location systems, is also used in "see-through-the- all" precision radar imaging technology, it is a possible technology for use in personal area networks.

2.4.1 ZigBee/802.15.4

This is a wireless technology specification that is based on the IEEE 802.15.4 standard [22].It is intended to be a low power , data and cost wireless networking standard for sensor and control networks. It has the ability to create mesh networks, routing traffic and works in the 2.4GHz band with a data rate of 250Kbps [22].

2.4.2 Wi-Fi

Wireless Fidelity is an emerging technology that showed substantial signs of growth, in particular, in 2003. The prospects in deploying this technology were in the increase in 2004. It is far more recognized now and of the increase in use by all those that deals with networks and internet technology. It is a technology surrounding the radio transmission of internet protocol data from an internet connection wirelessly to a host computer. It is basically a wireless connection between your computer and the internet connection in your house.

One of the earliest companies to deploy and sell **Wi-Fi** technologies to the home consumer is Apple Computer using the **Wi-Fi** transmitter called "Airport". Apple made connecting wirelessly to the internet from most anywhere in your house a simple task. Is it now popularly deployable, that majority of laptop computers are now Wi-Fi enable. Wi-Fi technology uses radio technologies called IEEE802.11 to transmit data from the internet connection to the host computer. A Wi-Fi network can be used to connect computers to each other, to the internet, and to wired networks.
Wi-Fi comes in two speeds: 802.11b (data transfer rates up to 11 Megabits per second) or the newer to 54 Mbps, 802.11g (data transfer rates up to 54Mbps). This compares with Bluetooth's much slower speed of 0.57 Megabits per second. There's a newer standard, 802.11n due in 2007 that offers even faster connectivity.

Wi-Fi 802.11b/g operates in the 2.4GHz frequency band (also used by Bluetooth and microwave ovens), and has a typical range of around 500 feet (with clear line of site). Indoors, you can expect around 150 feet with 802.11 - this will increase with the 802.11n protocol. It can provide real-world performance similar to the basic 10Base T wired Ethernet networks used in many offices.

Wi-Fi was originally a brand licensed by the Wi-Fi Alliance to describe the embedded technology of wireless local area networks (WLANs) based on the IEEE802.11 standard.

Other types of WLANs are been implemented based on the appropriate application and maybe the required demand by the user on any of the multimedia applications.

Wireless data is advancing at a particular swift clip, as more companies introduce more features for consumers and business users alike. There is tremendous growth and awareness in this technology. Almost every one that can tell what wireless network is about, and in all, the technology is broadly now in use by many that surf the internet.

2.4.3 What has been done with WLAN

In 1970 University of Hawali, under the leadership of Norman Abramson, developed the world's first computer communication network using low-cost ham-like radios, ALOHAnet [28] .The bi-directional star topology of the system included seven computers deployed over four islands to communicate with the central computer on the Oahu Island without using phone lines . Not too long from then in 1980, P. Ferrert made a report on an application using SCSS (Single Code Spread Spectrum) radio for wireless terminal communications [22] in the IEEE National Telecommunications Conference. In 1984, there was a comparison between Infrared and CDMA spread spectrum communications for wireless office information networks was published by Kaveh Pahlavan in IEEE Computer Networking Symposium which later was published in the IEEE

Communication Society Magazine [29]. Marcus made another effort in May 1985, which led the FCC to announce experimental ISM bands for commercial application of spread spectrum technology. Thereafter, M. Kavehrad investigated on an experimental wireless PBX system using CDMA (Code Division Multiple Access) [30]. These efforts prompted significant industrial activities in the development of a new generation of wireless local area networks and it updated several old discussions in the portable and mobile radio industry.

The first generation of wireless data modems was developed in the early 1980's by amateur radio operators .This technology was exploited by adding a voice band data communication modem, with data rates below 9600 bit/s, to an existing short distance radio system, typically in the two meter amateur band. The second generation of wireless modems was developed immediately after the FCC announcement in the experimental bands for non-military use of the spread spectrum technology. These modems provided data rates in the order of hundreds of Kbit/s. The third generation of wireless modem aimed at compatibility with the existing LANs with data rates in the order of Mbps. Several companies developed the third generation products with data rates above 1 Mbps and several products had already been declared by the time of the first IEEE Workshop on Wireless LANs.

The first of the IEEE workshops on Wireless LAN was held in 1991 [31]. At that time early wireless LAN products had just been released in the market and the IEEE 802.11 committee had just started its activities to develop a standard for wireless LANs. The aim of that first workshop was to evaluate alternative technologies. By 1996, the technology [31] was relatively mature, tangible applications had been identified and addressed and technologies that enable these applications were well understood. Chip sets aimed at wireless LAN implementations and applications, a key enabling technology for rapid market growth, were emerging in the market. Wireless LANs were being deployed in schools by using access, point-to-point LAN bridges, ad-hoc networking, and even larger applications through internetworking, hospitals, airports, business environments etc [29].

The IEEE 802.11 standard and variants are alternatives, such as the wireless LAN interoperability forum and the European HIPERLAN specification had made rapid progress, and the unlicensed PCs, Unlicensed Personal Communications Services and the proposed SUPERNet, later on renamed as U-NII, bands also presented new opportunities.

On July 21, 1999, Airport debuted at the Macworld Expo in New York City with Steve Jobs picking up an iBook supposedly to give the cameraman a better shot as he surfed the Web [31] [28]. Applause quickly built as people realized there were no wires. This was the first time Wireless LAN became publicly available at consumer pricing and easily available for home use. Before the release of the Airport, Wireless LAN was too expensive for consumer use and used exclusively in large corporate settings [31].

Originally WLAN hardware was so expensive that it was only used as an alternative to cabled LAN [23] in places where cabling was difficult or impossible. Early development included industry-specific solutions and proprietary protocols, but at the end of the 1990s these were replaced by standards, primarily the various versions of IEEE 802.11 (Wi-Fi)). An alternative ATM-like 5 GHz standardized technology, HIPERLAN, has so far not succeeded in the market, and with the release of the faster 54 Mbps 802.11a (5 GHz) and 802.11g (2.4 GHz) standards, almost certainly never will [26].

In November 2006, the Australian Commonwealth Scientific and Industrial Research Organization [26], won a legal battle in the US federal court of Texas against Buffalo Technology which found the US manufacturer had failed to pay royalties on a US WLAN patent CSIRO had filed in 1996. CSIRO are currently engaged in legal cases with computer companies including Microsoft, Intel, Dell, Hewlett-Packard and Net gear which argue that the patent is invalid and should negate any royalties paid to CSIRO for WLAN-based products.

2.5 Multimedia

Multimedia entails the ability to communicate in more than one way. Multimedia services involves video transmission, VoIP, video conferring etc. it has being implemented in wired network, but it has its space also for implementing it in wireless networks.

Recent advances in computing technology, data compression, high-bandwidth, storage devices, high-speed networks, and the third generation (3G) wireless technology have made it feasible to provide the delivery video over wireless channels .Future wireless communication systems promise to offer a variety of multimedia services which require reliable transmission at high data rates. In order to achieve such high data rates, transmission over OFDM channels is of great concern and will be very necessary to achieve this goal.

Multimedia delivery over wireless networks [28] is an important topic which requires high transmission reliability and stringent end-to-end delay. Since wireless links are usually error-prone, band limited and time-varying, error control schemes are vital tools that will help in obtaining high transmission reliability. In general, researchers of interest have used forward error correction

(FEC) codes for delivery transmission because they maintain a constant throughput and a bounded delay.

The major challenges of video transmission over WLAN that are to be dealt with are low bandwidth and high transmission error rate. By providing error resilient architecture for video transmission over WLANs, this problem can be minimized. This can be achieved by modifying radio links layer error control, modifying UDP, and also a general frame for error control in application layer. The objective of implementing this scheme is to conquer the error-prone nature of wireless links. Since this is a common problem in wireless networks, error correcting techniques like FEC, and ARQ. An alternative to FEC, ARQ can also be deployed.

2.5.1 Challenges in Multimedia systems.

The challenges faced by Multimedia applications [32] are guaranteed bandwidth, delay, and jitter and error rate. This is a big challenge according to [32] to guarantee these QoS requirements in IEEE 802.11 in WLAN.

This challenging fact has been found out to be as a result of the unaware functions of Medium Access Control (MAC) layer, physical (PHY) layer characterized by noisy behavior. Additional hurdles that befall multimedia applications include:

- host computer power requirement
- human interface usability requirements
- network latency and throughput requirements
- how to represent and store temporal information
- how to strictly maintain the temporal relationships on play back/retrieval

2.5.2 Multimedia Applications

We can find application of multimedia in the following areas:

- world wide web
- hypermedia courseware
- video conferencing

- video-on-demand
- interactive TV
- groupware
- home shopping
- games
- virtual reality
- digital video editing and production systems
- multimedia database systems

2.6 VoIP

VoIP is one of the most important applications for the IEEE 802.11 WLANs, although there is limitation for QoS support for Multimedia in WLANs [8, 14] [12]. VoIP is a solid technology available since 1974, which was successfully demonstrated by the ARPANET and how the IP started [17] [18]. It is a telephony technology that commonly use the real time transport protocol (RTP) to transport voice packets over a packet switched network. RTP runs on top of user datagram protocol (UDP). This technology allows people to communicate via voice using the IP protocol instead of telephone lines. The traffic types are UDP and TCP, while the traffic applications are CBR and FTP.

VoIP is one of the fastest growing Internet applications today and is currently considered as one of the most important technologies for telecommunications. It is expected to accommodate many of multimedia services despite its low cost of deployment.

VoIP is a growing technology that enables the transport of voice over data networks such as the public internet. It uses a number of protocols which ensures that voice communications is appropriately established between parties, and that voice is transmitted with quality close to that we are accustomed to in the public switched telephone network (PSTN).

VoIP is Cost savings by reducing or eliminating the toll charges associated with PSTN. Network management can be centralized and consolidated. It makes more sense to transfer voice over data networks rather than data over voice network as internet traffic exceeds voice traffic in terms of volume. By making voice "just another IP application" companies can build truly integrated networks for voice and data, which provides companies to quickly and flexibly take advantage of new opportunities within the changing world of communications.

In all, VoIP solutions are often used at corporate level as a cost effective solution to telephone communications, whereas proprietary VoIP applications are used for letting people talk about either computer-to computer or computer –to –telephone using a PC equipped with a special application and a headset.

2.6.1 Evolutional concepts behind VoIP

Shuzo Saito of NTT in December 1966, published a report on the statistical approach to speech coding, where short segments of speech were modeled using Gaussian autoregressive processes [2, 25]. The basic idea behind this report was to form a maximum likelihood selection of the underlying probabilistic model based on observed speech data, where the model was described by regression or linear prediction.

Glen Culler in 1966 also introduced his online system. This system was a computer which allowed real time signal processing at different terminals. In 1968, Culler joined the ARPANET pioneers [34], to complete the specification of the interface message processor (IMP).
The first efforts towards developing packet speech transmission on the ARPANET were initiated in 1972 by Bob Kahn [28]. He worked on real time visual flight simulation to bring real time video and speech to the ARPANET.

Cohen in 1973 [2] moved to ISI, where he worked with Steve Casner, Randy Cole and others to work on real- time operating systems and eventually real-time signal processing of both speech and video. In order to exploit the possibilities of packet speech on the ARPANET, Kahn formed the network secure communications (NSC) group and became its "eminence". The network voice protocol (NVP) was also implemented that year specifically in December, and since then has being in use for local and real-time voice communication over the ARPANET.

In 1974, two major developments in internet [2], technology occurred. The first was the specification of the transmission control protocol (TCP) by Bob Kahn and Vint Cerf [2]. The second was the development and description of the network voice protocol (NVP) by Danny Cohen and his colleagues, who explained how real-time speech can be communicated on the ARPANET. He also argued with Vint Cerf in 1974, that the extraction from the original TCP of a simple protocol more amendable to real-time processing was required. In order to distinguish real-time traffic from reliable data transmission, Cohen characterized them by making analogy between milk and wine. "You have to deliver the milk quickly before it spoiled even if you spilled some on the way, but you could deliver wine a lot more slowly" [2].

Furthermore, in August 1977, Cohen, Cerf, and internet legend on Postel agreed to separate IP from TCP so that real-time applications can be implemented. In order to actualize this, they firstly created UDP, and the separation of IP and TCP was then made official in January 1978 in TCP version 3 [35]. And it is with this trend that the technology of VoIP has being developed till date. This was built up as a result of getting the basics of what is expected in it, how it can be done and how to achieve it. And today, VoIP is now a deployable service because of the internet evolution and is now something interesting to talk about.

While VoIP on wired network is maturing, VoIP on wireless mobile network is still in its infancy. This disparity is due to the fact that the Wireline bandwidth is abundant and can be traded off for delay performance and overhead, whereas bandwidth in wireless mobile network is still a scarce resource.

2.6.2 Why VoIP?

It is important to know why there should be adoption of VoIP despite the existence of the popularly used PSTN. VoIP technology is widely deployed because of its low cost, it also enable the creation of novel application which integrates both voice and data.

ata network is packet switched, in which over data links shared with other traffic. In each network ode, packets are queued or buffered, resulting in variable delay. Data can be more tolerable to elay and jitter unlike the former, but cannot tolerate loss. This philosophy is centered on providing liable data transmission over unreliable media, almost regardless of delay [19]. It is generally not fected by delay [20]. But voice transmissions are degraded by a small amount of delay and cannot e retransmitted. On the other hand, a small amount of packet loss does not affect voice quality at e receiver's ear, but even a small loss of data can corrupt an entire file or application. So, giving ority to voice during queuing will not really affect data transmission.

7 VoIP Protocols

[P enables the transport of voice over data networks such as the public internet. It uses a number protocols which ensure that voice communications are appropriately established between parties, d that voice is transmitted with quality close to that we are accustomed to in the PSTN. Some of e protocols that are used in VoIP as listed below.

Table 2.1 Protocols use in VoIP [58]

Megaco H. 248	Gateway Control Protocol
MGCP MIME	Media Gateway Control Protocol
RVP over IP	Remote Voice Protocol Over IP Specification
SAPv2	Session Announcement Protocol
SDP	Session Description Protocol
SGCP	Simple Gateway Control Protocol
SIP	Session Initiation Protocol
Skinny	Skinny Client Control Protocol (SCCP)

VoIP handles both voice and data applications. Calls can be made as well as sending messages with its supported means. Nevertheless, standard VoIP protocol such as SIP and H.323 are very popular in the carrier environment and in many other fields not limited to VoIP, such as messenger and chat. In addition to these standards-based applications, there are other applications such as Skype or VoIPstunt and other hybrid applications partially based on open standards such as Google talk.

The result is that VoIP is becoming in some ways similar to P2P (peer to peer) as new applications appear, grow and disappear very often. Some VoIP applications (e.g. Skype) are using P2P as communication transport for building the communication infrastructure and crossing firewalls, a typical scenario where many standards-based VoIP applications fail to operate.

Transmission control protocol (TCP) is a connection oriented protocol; that is, it establishes a connection prior to transmitting data. It handles sequencing and error detection, ensuring that a reliable stream of data is received by the destination application. TCP divides the HTTP messages into smaller bits (segments) and is then sent to its destination. A TCP segment consists of two sections header and data. The TCP header includes an error checking field, a sequence number and an acknowledgement number. TCP controls the size and rate of sending messages and also defines routines to fix anything that may go wrong.

Two protocols and very vital in VoIP application as real time application: User datagram protocol (UDP) and real time protocol (RTP) [33].RTP allows users to communicate via voice using Internet Protocol instead of telephone lines. On the other hand, UDP is used for real time application where transmission may be more problematic than packet losses to provide a best –effort service with no attempt to recover lost or errored packets.

Voice is a real-time application, and mechanisms must be in place to ensure that information is received in the correct sequence, reliably and with predictable delay characteristics. Although TCP would address these requirements to a certain extent, there are some functions which are reserved for the layer above TCP. Therefore, for the transport layer, TCP is not used, and the alternative protocol, UDP, is commonly used.

VoIP is a solid technology available since 1974, which was successfully demonstrated by the ARPANET and how the IP started [28] .It is a telephony technology that commonly use the real time transport protocol (RTP) to transport voice packets over a packet switched network. VoIP is one of the fastest growing Internet applications today and is currently considered as one of the most important technologies for telecommunications. It is expected to accommodate many of multimedia services despite its low cost of deployment; one of the most popular uses of this application is **Skype**.

2.8 Performance Metrics

When implementing VoIP, the following factors are required [2, 36].Delay, Jitter, packet loss, packet mis-order, available bandwidth, packet prioritization, network design, transcoding, echo, silence suppression, duplex Codec selection, router and data-switch configuration, QoS policy, encryption /decryption.

❖ Delay

Switches, routers travel through the network as an element of the network, so the time it takes a packet to travel through the network is called the **packet delay.** It is caused by processing in the endpoint equipment (and in the network), the collection of voice samples to implement voice compression, and the collection of voice (compresses or uncompressed) into network packets [25]. Distance travel through the network, firewalls and jitter buffers adds to packet delay. Of course then, even if delay occurs, there should be some tolerable level which will not cause so much effect to especially voice, hence it requires there should be some guidelines to these, some of them are as follows. Under 150-200ms delay can give very good voice quality [35].

Delay exceeding 200ms may still be quite unacceptable depending on customer expectations, analog trunks used, codec type etc [14] .The H.323 protocol defines a maximum end-to-end delay of 400ms; anything beyond this may cause the network to be unstable [35].The recommendation for delay by ITU-T is 150ms for one-way (including endpoints) as the limit for excellent" voice quality [35, 36].

Delay can be mitigated with efficient VoIP gateway and network design [28].The minimum path latency local parameter is a representation of the latency in forwarding process associated with the nodes, where the latency is defined to the smallest possible packet delay added by the node itself. This delay results from speed-of –light propagation delay, packet-processing limitations, or both. It does not include any variable queuing delay that may be introduced.

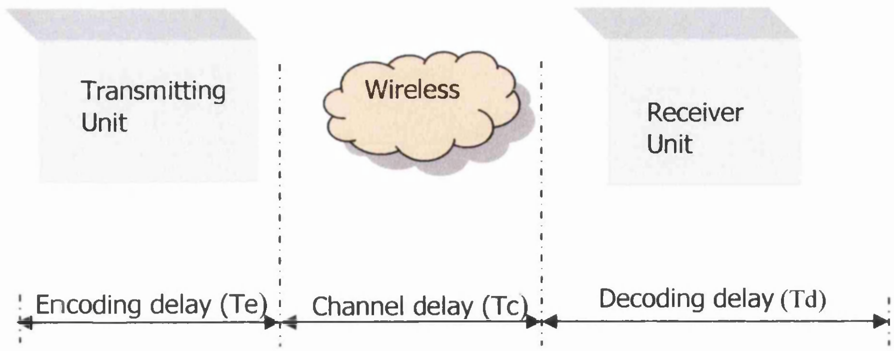

Fig 2.0 Wireless Channel Delay Analysis

❖ Jitter

The variation between when a packet is expected to arrive and when it was actually received is called Jitter. This occurs as a result of network congestion which is experienced during instantaneous buffer utilization, which in turn results to difference in delay times between packets in the same voice stream. It is caused by variation in delay characteristics of packet transport network .It is able to generate audible voice problem [2], if it exceeds 20ms. High delay results to high jitter because in both cases packets are discarded if the packet delay exceeds half the jitter buffer size.

This effect is usually compensated by some vendors by implementing a jitter buffer in their H.323 voice applications, so that jitter buffer (designed to smooth packet flow) can hold incoming packets for a specified period of time before forwarding them to the decompression process.
It can be best mitigated by adaptive jitter buffer management in the packet receive path, to effectively remove the jitter before the voice samples are played out to the listener [28].

❖ Packet loss

This occurs when packets are sent and are not received at the final destination as a result of some network problem. It is caused by packet buffer or processor overload in the network or receive VoIP endpoint, or by packet bit errors [25]. This varies depending on the type of codec that is in use. Voice quality is better when a compression codec (G.729A) is used than using a bandwidth G.711 codec [25] [2]. Acceptable rate of packet loss vary with the needs of the end users.

It can be best mitigated by using packet loss concealment techniques as part of the voice compression algorithm to replay previously received voice and/or comfort noise samples until new information can be received.

❖ Echo

Echo will result when a VoIP call leaves the LAN through a poorly administered analog trunk into a PSTN. Echo that is sufficiently attenuated and /or that is delayed by less than 15ms [37], will not be noticed. Echo between 15ms to 35ms will give the speech a "hollow" sound, while that which is more than 50ms will be distinctly heard and should be cancelled (ITU-T Recommendation G.131) [37] . Echo can be mitigated by robust echo cancellation solutions in the gateways between VoIP and the PSTN.

The main types of echo are acoustic and impedance, although the sources of echo can be many. Another major cause is from an impedance mismatch between four wired and two-wired systems. Echo also results when impedance mismatch exits in the conversion between TDM time division multiplexing (TDM) networks and the LAN, or the impedance mismatch between the handset and its adapter.

Impedance mismatch causes inefficient energy transfer. The energy imbalance must go somewhere and so it is reflected back in the form of echo. Usually the speaker hears an echo but the receiver does not. Echo cancellers which have varying amounts or memory, compare the received voice with the current voice patterns. If the patterns match, the canceller cancels the echo. Echo cancellers are not perfect, however. Under some circumstances, the echo gets past the canceller. The problem is exacerbated in VoIP systems. If the one-way trip delay between endpoints is larger than the echo canceller memory, the echo canceller will not ever find a pattern to cancel [25].

❖ Packet Prioritization

Prioritization of network traffic is a simple concept which gives important network traffic precedence over important network traffic. One Prioritization scheme assigns the priority based on the UDP port numbers that the voice packets use. This scheme allows you to use network equipment that can mark the packets on these ports with a priority. UDP is used to transport voice through LAN because, unlike TCP, it is not connection-based. Because of human ear's sensitivity to delay, it is better to drop packets rather than retransmit voice in real-time environment. Prioritization is also called class of service (COS) because traffic is classed into categories such as high, medium, and low, and the lower the priority, the more "drop eligible" is a packet [25].

❖ Throughput

This is the total number of bits sent to the higher layer from MAC layer. It can also be defined as the minimum end –to end transmission rate measured in bytes/sec or bits/sec. It can also be defined as the number of packets that are successfully received at the destination. This is because during transmission, not all the packets that were transmitted are received, some will be dropped while some is been retransmitted. A network is rated based on the successful transmission.

❖ Media Access Delay

This is the total in seconds that the packets in the higher layer queue, from arrival to the point when it is removed from the queue for transmission.

3 Quality of Service

3.1 Introduction

Quality of service (QoS) is an act of delivering data or packet across a network with an assurance of consistent and safe delivery of its services to the required destination at the receiver. It is the capability to provide resource assurance on network. In order to render QoS to multimedia services [38], the challenges of latency, availability, jitter, throughput etc, has to be addressed. This is done by studying a wide range of networking technologies and techniques and network characteristics has to be maintained. For example like in video transmission, the quality has to be maintained despite the compression it will undergo before transmission. So at the receiver, it is expected that the quality is same as that before transmission. QoS parameters include: bandwidth, jitter and packet loss rate.

Furthermore, QoS is not guaranteed in IP network and also have limitations. For instance in DCF where it can only support best- effort services, and in PCF where the centralized polling scheme is questionable because PCF operates on a central polling scheme which depend on AP as a point coordinator.

QoS is simply a set of techniques which is needed to manage network bandwidth, latency, jitter, packet loss etc. However, QoS works in hand with Reservation Resource protocol so that network expectations can be achieved.

3.2 Steps taken to implement QoS

In order to achieve QoS in a network, we must identify traffic type, determine QoS parameter and finally apply QoS technique.

The following routine leads to what is known as the QoS triangle, which is shown below

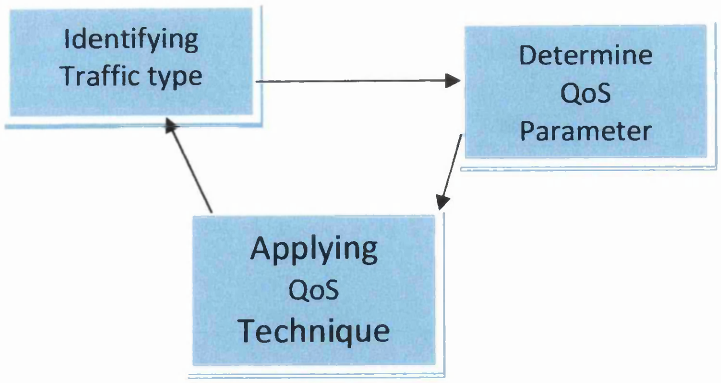

Fig 3.0 Block Diagram of QoS [57].

From the above figure, traffic to be transmitted on the network must be first identified, so that it can be compared with the resources available in the network, and then, the QoS metrics that is to be used in analyzing the network must also be known, and finally applying the appropriate QoS technique.

3.2.1 Providing QoS on Network

Inability to meet up with network requirement causes impairments to voice and reduces its quality. This gives designers of network more challenges and also incurs commitment to proper management of network and its resources. QoS can be achieved by employing different techniques.

In Capacity Management, Larger networks like WAN pose bandwidth management problems in network .But network inside enterprise sparingly causes bandwidth management problem. In essence, the more the network availability, the more difficult it is to manage its network bandwidth.

Also in prioritization techniques involves applying priority scheme in the scheduler is another way of rendering QoS to the network. Among multimedia services, voice is given much priority over less time-critical data during scheduling either in switches or router. Latency and delay variation can be drastically minimized without significant effect on data traffic.

Consequently, in network monitoring, network requirements changes with respect to time and demands. However, as these changes occur, it is imperative to execute continuous monitoring.

And finally in management of Network, network QoS offers a reliable way of achieving high network performance that result to high voice quality.

3.2.2 Techniques for providing QoS

There are basically two signaling techniques for deploying QoS, they are: reservation-based and prioritization-based schemes for the internet. Reservation-based signaling system negotiates and books its QoS requirements with the network while prioritization-based simply marks its traffic to indicate the QoS requirements and sends the packets to the network. Furthermore, reservation-based has the ability to provide efficient use of scarce resources to be used by the network and well providing strong service guarantee. Examples of these include integrated service (IntServ) and differentiated service (DiffServ).

3.3 Integrated service (IntServ) Model

Internet only offers a best effort service, which can meet the traditional non-real-time Internet traffics. For real-time traffic, it needs a new scheme to make reservation for the traffic. Integrated services (IntServ) can provide resource allocation to meet the requirement of real-time application. IntServ is per-flow service.

This service is offered on request from end user, a user makes request before transmission is done. Traffics travels hop-by hop. Request can be refused if there is insufficient capacity available, which makes billing difficult. This is known as Hard QoS. IntServ reserves resources by using RSVP, it also controls load service and has firm bound of throughout and delay.
However, it is complex, also needs administer allocations and scalability.

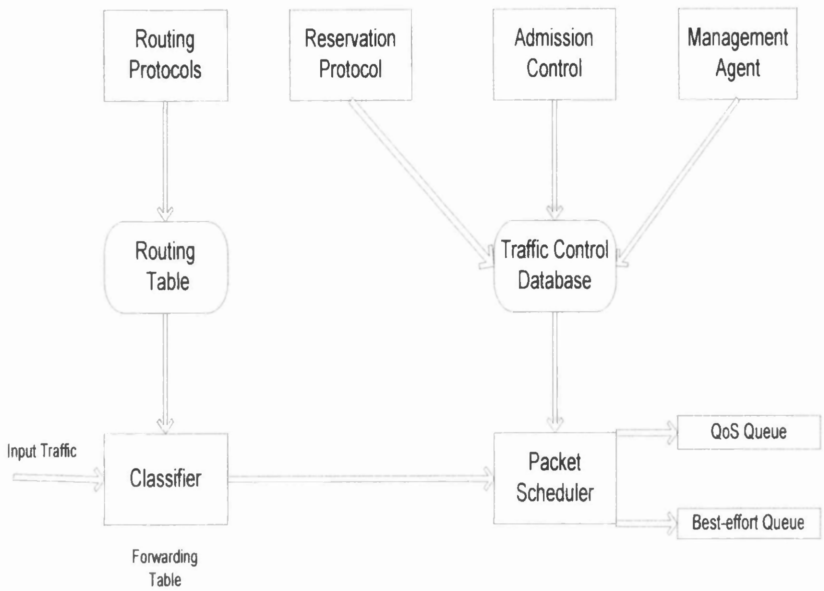

Fig 3.1 IntServ Implementation Framework

3.4 Differentiated Service (Diffserv)

Is a set of End-to-end QoS capabilities: End –to end QoS is the ability of network to deliver service required by specific network traffic from one end of the network to another. It is a multiple service model that can satisfy different QoS requirements. With this method, network tries to deliver a particular type of service based on the QoS specified by each packet. In this type of QoS, network agrees to limit amount of traffic and render better services. It deals with service level agreement (SLA) .Also referred to as Soft QoS.

In this technique, it offers aggregate connection flows to different classes and each flow gets required services statistically. Furthermore, it reduces the burden on network devices and easily scales as the network grows, allows customers to keep any existing layer 3 type of service (TOP) prioritization scheme that may be in use, allow customers to maximize DiffServ –complaint devices with any existing TOS –enabled equipment in use and it relives bottlenecks through thorough management of current corporate network resources.

3.5 Network Architecture

The 802.22 standard specifies a common medium access control (MAC) Layer, which provides some functions that aids the deploying the 802.11 –based WLANs. The function of the MAC Layer is to manage and maintain communication between 802.11 stations (radio network cards and access points) by coordinating access to a shared radio channel and using the protocols that enables the communications over wireless medium. Furthermore, 802.11 MAC Layer uses an 802.11 Physical (PHY) Layer like 802.11b or 802.11a, to perform carrier sensing, transmission and receiving of 802.11 frames.

3.6 Medium Access Basics

Prior to transmission of frames, a station must have to gain access to the medium first which is a radio channel that shares stations. Since 802.11 standards defines two forms of medium access, DCF and PCF, with DCF the 802.11 stations contends for access and attempts to send frames when there is no other station transmitting. If another station is sending, other stations will wait until the channel is free.

The MAC Layer checks the value of its network allocation vector (NAV) which is a counter resident at each station that represents the amount of time that the previous frame needs to send its frame. NAV must be zero before a station can attempt to send a frame. Before transmitting a frame, a station calculates the amount of time required to send a frame based on the frame's length and data rate. So when stations now receive frames, they will now examine this duration field value and use it as a guide for setting their corresponding NAVs. This process is what reserves the medium for the sending station.

3.6.1 802.11 MAC layer Functions

The following features summarize the 802.11 MAC functions in relationship to infrastructural WLANs.

- **Scanning:** Passive and active scanning are defined by 802.11 standard, the later is where the NIC searches for APs and the former where the NIC scans individual channels to find the best AP signal. Active scanning enables a radio NIC to receive immediate response from APs, without waiting for a beacon transmission.

- **Authentication**: This is the process of proving identity of which 802.11 standards specifies two forms: Open system and shared key. The later is optional while the former is mandatory.

- **Association**: This is necessary to synchronize the radio NIC and AP with information like data rates. One authentication has been done, the radio NIC must associate with the AP before sending data frames.

- **WEP**: With optional WEP enabled, wireless NIC will encrypt the body (not header) of each frame before transmission using a common key, and the receiving station will decrypt the frame upon receipt using the common key.

- **Power safe mode**: The optional power safe mode which a user can turn on or off enables the radio NIC to conserve battery power when there is no need to send data. With power save mode on, the radio NIC indicates its desire to enter "sleep" state.

- **RTS/CTS**: The optional request-to send and clear-to-send (RTS/CTS) function allows the AP to control use of the medium for stations activating RTS/CTS.

- **Fragmentation:** The optional fragmentation function enables an 802.11 station to divide data packets into smaller frames.

3.6.2 MAC layer Limitations

There are two basic limitations of the MAC layer protocol, they are asymmetric interactions and Sub-optional default allocation .The former is the interference between two flows either at the sender or at the receiver which results to one flow to be shut-off while the later is shows that the default allocation of the transmission medium by the MAC layer fails to meet the requirements of some applications.

More sophisticated back-off protocols or slot algorithms can be used to implement ,more flexible allocation policies like Weighted Fair Queuing, other solutions to this can also be achieved by using a combination of both back-off and slot allocation algorithm.

Furthermore, since the MAC layer of 802.11 lack QoS support, 802.11e which has EDCA features which was lacking in DCF used by 802.11 can improve the performance metrics of wireless networks in MAC protocol. In this research, I have used this method to improve some metrics like Throughput, delay, jitter, packet loss etc.

3.7 RTS and CTS Overhead

RTS/CTS help to solve hidden terminal problem faced by 802.11 standards. This hidden terminal problem is well known in WLAN networks where a node **A** and **B** can hear frames sent from an AP but are not able to hear each other [36]. Collision errors that have resulted to this effect can be prevented by allowing stations to send request to send (RTS) and clear to send (CTS) control frames prior to the transmission of any data. The CTS response frame sent by the AP is heard by the hidden nodes and imposes a silence period until the data and acknowledge (ACK) packets are exchanged.

An ACK is transmitted after a short-inter –frame space (SIFS) at the end of the received packet. See diagram below.

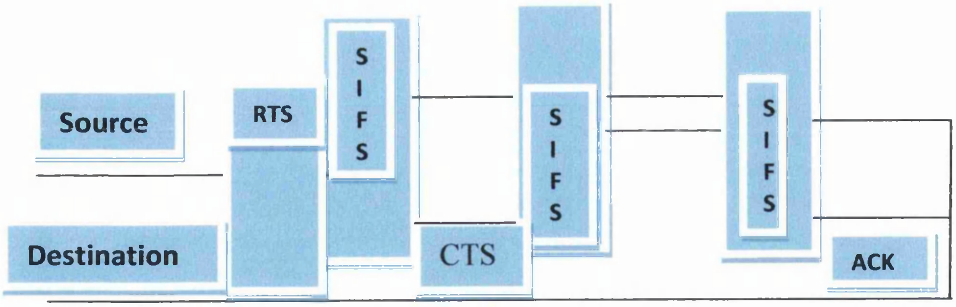

Fig 3.2 RTS/CTS Mechanism

RTS causes more packets to be sent often thereby consuming more bandwidth and reducing throughput of the other network packets. Furthermore, RTS/CTS procedure consumes fair amount of capacity in addition to the latency incurred prior to data transmission can take place [36].

3.8 Vehicular Network

DSRC (a robust technology) [39], can be deployed in road safety applications. Vehicle communication is possible so that vehicle to vehicle can communicate with each other for safety purposes. DSRC performs better and effective in service differentiation where prioritized services are applicable. In road safety application, vehicle can warn a driver of any danger such as braking, merging traffics, emergency etc [39].

Wireless access is now been developed by the IEEE so as to deploy this technology in vehicular applications. The challenging task about the vehicular network is the range of communication. This will be the task that must be put into consideration, as per how much distance should the vehicles be; to receive messages from other stations, which is an interesting and challenging question.

In this research, we have considered a broadcast network, in which stations can send two types of messages to various stations. In sending of these messages to our stations, those stations can be alerted of any danger.

3.9 Factors influencing Network Performance

Service differentiation is the major difference between EDCF and DCF. Therefore, In order to observe the effectiveness of 802.11e in vehicle/real time applications, the following parameters have effective control over these applications:

- AIFS
- CWmin (Channel access contention window)
- TXOpLimit
- Controlling Lower priority applications

Since 802.11 legacy lacks QoS support for real-time applications, 802.11e introduces an enhanced EDCF which provides differentiated access to the channels by using eight categories of priorities [39]. In our simulation, we have focused on controlling Lower priority applications for the effectiveness of higher priority applications.

3.10 Improvement of QoS

There have been a lot of different schemes that will help is rending QoS on networks.
Various researchers have looked at this from varying angles, and some have come out with their findings and solutions, some of them are reviewed in this thesis, to show what has been done, how it was done, the problems encountered and possible solutions to the problems identified.

A survey was made by [40], of how QoS can be enhanced in WLANs, majority of the works that were reviewed have a limitation of management layer that could dynamically react to continuous fluctuation of radio resources. Also presented was QoS support for mobile ad hoc network, which requires some modifications especially to the link layer, although it is not compatible with the recent IEEE 802.11 link layer [41].

There was comparison from existing QoS-aware middleware systems, with specifications for QoS requirements [41]. Some of the specifications include: QoS translation and compilation, QoS enforcement and adaptation. The model proposed here [41], takes into account, the available framework for inter-device communications like UDP which was designed for guarantee interoperability between devices manufactured by different vendors [41]. Similar work was carried out by IEEE 802.11 TGK working group which focused on Radio Resource management; this was aimed at making collection of measurements at WLAN station to be easier. Furthermore, this model depends on exchanging QoS relevant [41], information and control messages available at the application layer.

Congestion control is currently performed by TCP, both TCP and UDP are protocols used in the transportation of multimedia applications. The later does not perform congestion control, but only the former. New congestion algorithm was proposed by [41], it was developed, analyzed and various numbers of experimental studies and stimulations were carried out. This scheme is meant to envisage into the congestion problem associated with, multimedia application and trying to use a transport protocol through which this problem can be handled. The various schemes available to deploy congestion control were also compared by [10], in varying environments. What is known as the TCP-Friendliness was also introduced; this is an upgrade of TCP feature that is deployable in case of congestion control [42], Contributed to previous knowledge to the current research in multimedia applications by giving a parallel look at the current congestion control algorithms for multimedia traffic and the relevance of deploying both TCP and TCP compatible schemes in wireless networks.

Balachandran et al developed an algorithm that was able to be adaptive to load balancing, this tries to handle services requested by users and readjusting the load across all APs. In this case, if an AP then cannot accommodate the new session request, network suggests a new location for the user. Furthermore, three different types of AP states were defined as: under-loaded, balanced and overload was mentioned by Velayos et al. [24], now proposed a dynamic load balancing scheme that considers QoS users. This scheme is able to handle heavy load, the rate of collisions and the number of transmission escalates [8].

Overloading results to delay in network and affects its throughput, which in turn affects the QoS to be delivered to the network. At AP, it affects the delays experienced by MAC layer .The above mentioned problem is what results to proposing this scheme that will be able to solve this problem in other to achieve the users requested QoS.

Fast collision resolution (FCR) scheme was also recently proposed for the purpose of improving the performance of DCF, static back off threshold and fast back off mechanisms are employed, unfortunately, since it has the inability to support service differentiation, it then cannot provide good performance for multimedia services [43], these new schemes have the aims of exhibiting the followings: improve the performance of multimedia applications, total throughput obtained, and fairness between same priority. This proposed scheme is very useful in the situation when the channel is highly loaded, which definitely will result to much queue for transmission of packet, a medium mechanism is needed in such a scenario.

Distributed admission control (DAC) was proposed by IEEE 802.11e working group for the purpose of protecting QoS flows, although it is not supported by the latest draft, but it still stands as foundation for study admission control. The newly adopted IEEE 802.11e provides a powerful tool for QoS requirements in WLANs. Due to the limitations identified in the previous other two access mechanisms, DCF and PCF, hybrid coordination function (HCF) and contention-based channel access (EDCA) has been introduced to cover up their deficiencies. This new scheme aggregates the functions of both DCF and PCF for data transmission. It still retains the two phases of operations which are the contention period (CP) and contention free period (CFP); HCCA is used in both cases while EDCA is used in CP only.

It was exploited that dynamic Bayesian network (DBN) allow features to be moved during classification, at the cost of decrease accuracy .They also worked on content–based publish/subscribe service with multicast support and video streaming on top of this service. These are all focused of the need for QoS requirements that needs to be fulfilled on wireless networks. V.S.W Eide et al presented this algorithm as an improvement in what has been previously done both in architecture and evaluation. This algorithm allows applications to be independently distributed and parallelized at multiple logical levels. In this paper, QoS is used as a term that means timeliness and accuracy of the outputs of the application; therefore QoS models in the approach include accuracy, resolution, temporal and latency.

3.11 Resource Reservation Protocol (RSVP)

RSVP is one of the protocols used in implementing Intergrated Service .It is a signalling protocol that is responsible for installing and maintaining reservation state in each router.This is an end to end signalling protocol. In this protocol, necessary network information is reserved along its way until it reaches its destination. This reserves resource can be in form of hard or soft state in the router's buffer.

Typically all IP traffic on the Internet is delivered on a best-effort basis. This delivery method does not address the requirements of multimedia applications such as videoconferencing, real-time IP multicasting and Internet telephony. RSVP is an effort to address the performance needs of such applications.

RSVP is a signalling and control protocol that doesn't carry application data. It operates on top of IP in the transport layer of the OSI protocol stack. This reservation information can either be hard or soft in the router's buffer. The well known scalability problem with the reservation approach, limits the solution's domain to small networks. However, soft state can be used to effectively increase the network scale. On the other hand, hard state can not only reduce the amount of signalling but also hard guarantee user's QoS profiles. These trade-offs should be considered together with the practical factors of some particular networks.

RSVP is a transport layer protocol that enables a network to provide differentiated levels of service to specific flows of data. With the fact that different application types have different performance requirements, RSVP acknowledges these differences and provides the mechanism necessary to detect the levels of performance required by different applications and to notify network behaviors to accommodate those required levels. And for further emphasis, RSVP is not a routing protocol, but was designed to work in conjunction with existing routing protocols. Host applications use RSVP to request the necessary QoS (such as guaranteed bandwidth) from the network for specific data flows. The QoS request is sent through all the routers along the path of the data flow on a hop-by-hop basis, and at each device the RSVP process attempts to establish and maintain a reservation state to provide the requested service.

Refresh messages are sent periodically by hosts and routers to maintain this state during the duration of the data transfer. The established state ends when the end host sends an explicit "teardown" message after the application has finished sending the data. RSVP also adapts to routing topology and multicast group membership changes.

3.11.1 RSVP and QoS

RSVP is used to specify the QoS by both hosts and routers. Hosts uses RSVP to request a QoS level from the network on behalf of an application data stream. Routers use RSVP to deliver QoS requests to other routers along the path(s) of the data stream. RSVP supports tunneling, which requires RSVP and non-RSVP routers to forward path messages toward destination address by using a local routing table.

RSVP supports four basic messages: Reservation, path ,error and confirmation and Teardown messages. RSVP supports both unicast and multicast flows, messages and travels along the same path as that of media flow. The sessions are simplex and receiver-oriented and it does not directly control the behavior of the network.

3.11.2 How does RSVP work?

When an application in a host (end system) requests a specific QoS for its data stream, RSVP is used to deliver the request to each router along the path(s) of the data stream and to maintain router and host state to provide the requested service. Although RSVP was developed for setting up resource reservations, it is readily adaptable to transport other kinds of network control information along data flow paths.

A host uses RSVP to request a specific QoS from the network, on behalf of an application data stream. RSVP carries the request through the network, visiting each node that the network uses in carrying the stream. At each node, RSVP attempts to make a resource reservation for the stream.

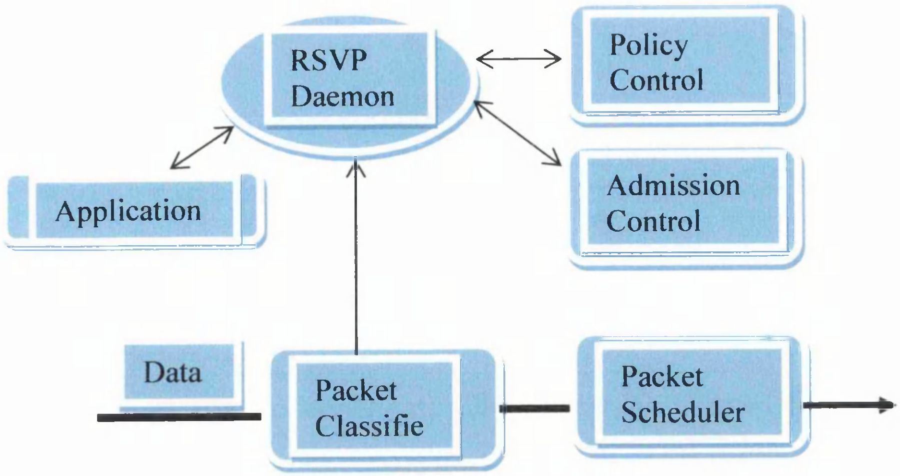

Fig 3.3 Reservation at a node on the data flow path [79]

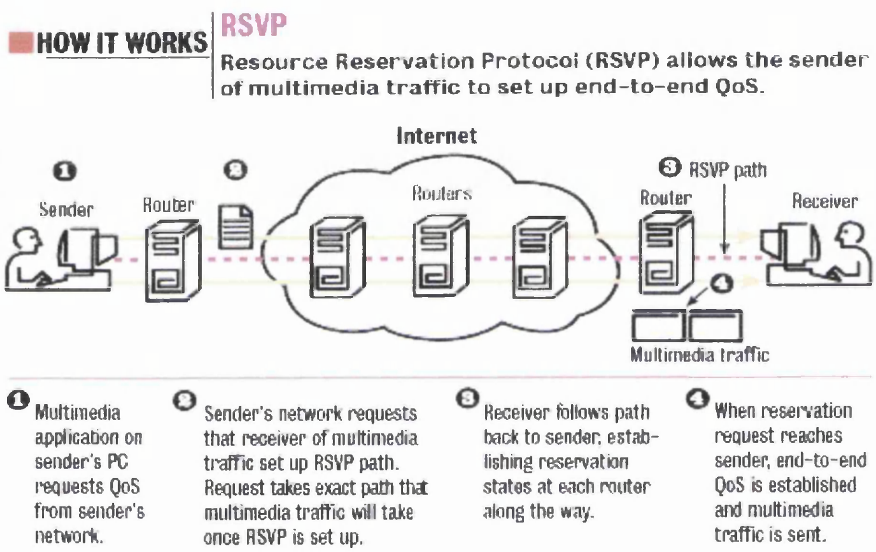

Fig 3.4 How RSVP Works [32]

In order to make a reservation at a node, the RSVP daemon [43], calls two local decision procedures, admission and policy controls. Admission control determines whether the node has sufficient available resources to supply the requested QoS. Policy control determines whether the user has administrative permission to make the reservation. If either check fails, the RSVP program returns an error notification to the application process that originated the request. If both checks succeed, the RSVP daemon sets parameters in a packet classifier and packet scheduler to obtain the desired QoS. The packet classifier determines the QoS class for each packet and the scheduler orders packet transmission to achieve the promised QoS for each stream. The reservation requests are receiver-oriented, and merge when they progress up the multicast tree. The reservation for a single receiver does not need to travel to the source of a multicast tree; rather it travels only until it reaches a reserved branch of the tree.

There are some problems that will result if RSVP is considered under host mobility, a mobile receiver must wait for a PATH message at its new location before it can send a RESV message back via a new path to the source for reservation, service disruptions occur due to delay encountered or experience during long reservations, which is as a result of handoff scenario and no guarantee that same level of resources will be available under a new point of attachment to which an MN moves.

Handoff event is one of the causes of packet losses on networks, when admission request are been processed. So to avoid this, QoS signaling at handoff should be processed and done quickly. On the other hand, if the time required in restoring flow traffic, after MN receives the beacon that triggers the handoff, is very short, then it might be possible to provide QoS guarantee to some real-time applications in hand with proper transmission buffer.

3.11.3 RSVP over Wireless Networks

In wireless networks, channel capacity and much limited and expensive as compared to wired. Hence there is need for the resource reservation to enhance network utilization as much as it can, to alleviate this problem.

On the other hand, the amount of resource reservation required by RVSP varies according to QoS needs, and can be time-variant because of mobility pattern of mobile users [32]. So it should be ensured that resource reservation in wireless link should be as simple as possible.

3.12 Relationship between 802.11e with QoS

This flavor is able to support QoS since it offers service differentiation, and also with the introduction of backoff instances. It further provides QoS by grouping the applications into four different categories, the associated CFB helps for multiple transmission of stations [44].It supplements and addresses the issue of QoS support in wireless LANs. In order to enhance QoS support in WLANs, it developed the HCF to provide QoS guarantee and uses admission control for resource management which helps in enhancing QoS support for networks. The prioritized channel access mechanism in 802.11e is effective, in which higher priority traffic can get higher throughput and lower MAC access delay [45].

3.13 Queuing Models

The principle behind the prioritization of voice packets over data packets is based on the theory and principles of queuing. This technique is what the channel performs as the traffic sources arrive from both voice and data to the channel to be served. A queuing system can be described as customers arriving for service, waiting for service if it is not immediate, and if have been waiting for service, leaving the system after being served [44]. NS-2 can be used to implement and simulate classical queuing models. In the simplest classical models, the time between packets arrival is random and has some general probability distribution, and the time it takes to transmit a packet is random as well distributed according to some other distributions.

In Queuing theory, the performance parameters are:

- time delay (i.e., time spent in the buffer)
- blocking probability (i.e. how likely an arriving packet is to be blocked)
- packet throughput (number of packets per second that gets through the system)

These parameters depend on:

- packet length
- packet arrival process (i.e., arrival statistics of incoming packets)
- service discipline, e.g. FCFS (≡FIFO), LCFS, or prioritization
- buffer size: Is it finite (as in practice) or infinite?
- nodal processing time

❖ transmission link capacity

3.13.1 Characteristics of Queuing Models

Arrival pattern of customers: This is the input to the queuing system

Service pattern of servers: Can be described as a rate in which customers are served

Discipline: Is the manner by which the customers are selected for service when a queue is performed

System capacity: Refer to limit at which the buffer can accommodate queue

Number of service channels: Refers to number of parallel service stations which can service customers simultaneously

Number of service stages: Refers to different layer or stages in which the queuing discipline occurs.

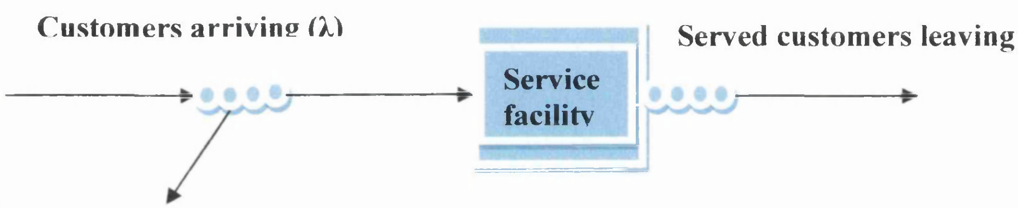

Fig 3.5 Queuing Model

$\lambda < \mu$ where **λ** is the packet arrival rate-, and μ is the transmission **rate.**

There are different ways of implementing queuing model and each has its own peculiar feature attached to it. Some of the queuing mechanisms will be discussed shortly.

3.13.2 Types of Queues

❖ **FIFO, First In First Out**

Packets arrive and leave the queue in exactly the same order. It has simple configuration and fast to operate [12]. There is no priority servicing or bandwidth guarantees possibility.

❖ PQ, Priority Queuing

In this case, traffic is classified into high, medium, normal and low. The principle adopted in this type of queue ensures that high priority traffic is served first, followed by medium, normal and then lastly low priority traffic. It has also been available for years like the former.

❖ Priority Queuing Systems

In this system, priority is given to certain classes of customers. Example in packet switching networks priority may be given to short control packets over normal data packets which are typically of much longer length.

Higher priority traffic can starve lower priority queues of bandwidth. There is no possibility of bandwidth guaranteed. Queuing behavior can be pre-emptive or non-pre-emptive. In a pre-emptive priority queue, service on a lower-priority customer is interrupted and only resumed after all arriving higher-priority customers have been served. On the other hand, in the case of the non-pre-emptive queue, higher-priority customers move ahead of lower-priority ones in the queue but do not interrupt the lower-priority customers already being served.

❖ CBWFQ, Class Based Weighted Fair Queuing

This is a type of queue in which traffic services are rated according to different classes. For example if you have a VoIP packets, which consist of both voice and data, they can be classified vividly as thus.

Class1: Voice

Class2: Data

The principle of operation is similar to that of PQ in which priority is given to a class named as high and so on.

3.14 Poisson Process

The Poisson process is a special type of a Markov process where the probability of an event at time $t+\lambda\ \Delta t$ depends only on the probability at time t.

The Poisson process defines arrivals in the following ways:

- ❖ probability of one arrival in an infinitesimally small interval Δt is $\lambda\Delta t$ where λ is a specified constant , and $\lambda\Delta t << 1$
- ❖ the probability of zero arrival in $\lambda\Delta t$ is $1- \lambda\Delta t$
- ❖ arrivals are memory less: An arrival or event in one time interval is independent of events in previous or future intervals.

Applications of Poisson process can be found in the following areas:

- modelling of telephone traffic, photon generation, photo detector statistics, shot noise processes, Electron-hole pair generation in semiconductors etc
- evaluating the performance of telephone switching systems and computer networks.

4 Network Simulator

4.1 Introduction

This chapter talks about Network simulator popularly called NS-2. It also fully explains how it is used in wireless networks to achieve the expected results in our simulations. It is open source software, so that users can change and extend existed classes very easily.

NS-2 is an object-oriented, discrete event network simulator [46], written in C++ with an OTcl interpreter as a frontend (used to execute user's command script). It uses two languages because the simulator has two different kinds of things it needs to do. C++ is faster and allows you to achieve efficiency in simulation but slower to change making it suitable for detailed protocol implementation.

OTcl on the other hand runs slower but can be changed very quickly which makes it ideal for simulation configuration. The OTcl script provided by the user can be used to define a particular network topology, specific protocols and applications that wish to simulate and the kind of output that you wish to obtain from the simulator.

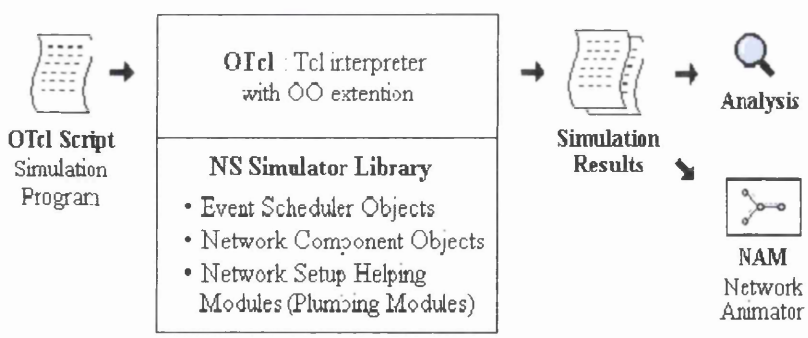

Fig 4.0 Simplified User's View of NS-2

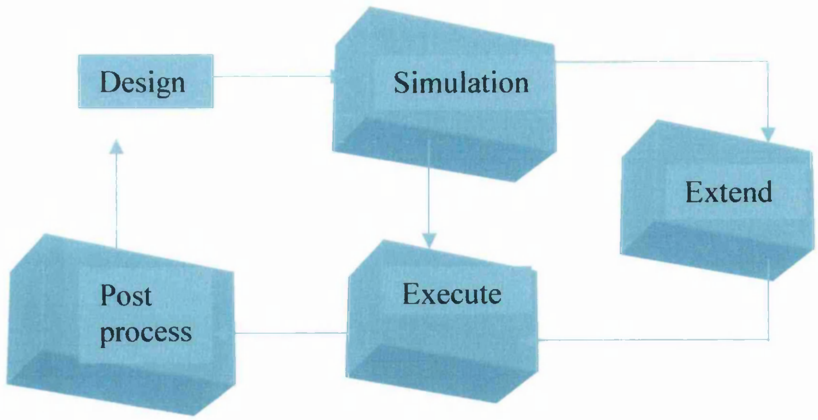

Fig 4.1 Setup of Simulation Model with NS-2

4.2 Why NS-2?

NS-2 support research, it is used for protocol design, traffic studies. It is and open source software, it allows easy comparison of similar protocols . Unlike OPNET it does not require a lot of processing power, and does not consume much time. It is good in routing applications. It is used because of its extensibility and plentiful online documentation.

There are other simulators like OPNET, but we have decided to use NS-2 as a matter of choose and interest, and also based on some of the above reasons, especially for its efficiency in routing application. It eases analysis in the various metric parameters. Although it involves much of coding, but becomes easier to implement when the right syntax and scripts is been used.

4.3 NS-2 and 802.11e Simulation

The other wireless standard which is IEEE 802.11 supports basic NS-2 environment, but it has some limitations in QoS requirements. For example it does not at this moment provide 802.11e HCCA and EDCA standard [46], 802.11 extension implements new 802.11 PHY and MAC layers for NS-2.After the implementation of 802.11 been integrated into basic NS-2 environment, it is possible to associate different network packets with different priority classes, but on the contrary, NS-2 tracing mechanism does not work with the 802.11 module.

Furthermore, simulations that uses 802.11e standard needs specially written scenario script which is different from a usual scenario script. NS-2 has the functionality to handle simulations involving multimedia applications with QoS supports.

The critical difference between 802.11 and 802.11e when they exist in same node is that in the original 802.11 standard, there is no support for service differentiation. But with NS-2, an intermediate 802.11 node is transparent in the sense that if a node is able to receive a packet from a 802.11e node, even if the QoS information of the incoming packet is not processed, it will preserve the packet when forwarded to the next hop, which may be 802.11e or not [47].

4.4 NS-2 Structures

The programming language used in NS-2 is structured in the following ways.

- ❖ Back-end C++
  - Defining new agents, protocols and framework.
  - Manipulations at the byte/bit levels.
- ❖ Front-end Otcl (Object-Oriented Tool Command Language)
  - Topologies, scenarios, simulations, ...
  - Script language (easy topology modifications)
- ❖ Split Object
  - Object created in Otcl has a corresponding object in C++

With NS-2 you can create network, create event scheduler, create traffic setup routing, turn on tracing and transmit application –level date. It has four basic components: Application, Agent, Node and Link. With it you can Create simulation, execute and process you results.

OTcl is an object-oriented language an extension of Tcl, it can manipulate existing C++ objects, it is fast to write and change. This language is user friendly because it is flexible for integration, easy to use and it is free.

4.4.1 Tool command language (Tcl)

Tcl means tool command language. It encapsulates the actual instance of the OTcl interpreter, and provides the methods to access and communicate with that interpreter. It provides methods for the following operations: obtain a reference to the Tcl instance, invoke OTcl procedure through the interpreter, retrieve or pass back results to the interpreter, report error situation and exit in a uniform manner, store and lookup "Tcl objects", acquire direct access to the interpreter. Furthermore, TCL is free, easy to use, very flexible and allow a faster development.

4.4.2 Some basic commands of Tcl and OTcl

- **Set** command: This is used in assigning values.

Example: "set b 0" assigns to b the values of 0 which is equivalent to b=0 in C language

- **Expression** command: This is used as a mathematical operation , for example , if you wish to assign to a variable x the sum of values of some variables **a** and **b**, we will write "set x [expre $**a** +$**b**]"
- If we want to **print** a result with this division 1/20 we will write

Puts " [expr 1.0/20.0]"

- The sign **#** starts a command line that is not part of the program, so the tcl interpreter will not execute that line
- To **create a file**, you need to give it a name, and then assign a pointer to it that will be used within the tcl program in order to relate to it. This is written like this: set file1 [open filename w].

Execution of a unix command is done by typing "**exec**" followed by the command. For example , if you want to initiate the display of a curve whose data are given in a two column file named " data" within the simulation , this is done by using the **xgraph** command and is written as: **exec xgraph data &.**

- The structure of an **if** command is like this:

```
If {
<execute some commands>
} else {
<execute some commands>
}
```

It can be nested with other "if"s and with : else's that can appear in the "<execute some commands >" part , when testing equality , you use "==" and not "=" the inequality is written with !=

- Loops have the following form:

```
For [2] [48] [48] {
<execute some commands>
}
```

4.5 NS-2 for windows vista

The installation mode for installing NS2 depending on what operating system you are using which differs for various individuals. For me, I am using windows vista and my installations are aided by two other applications: Ubuntu and VMware. Full details of these softwares and installations will be discussed shortly.

NOTE: NS-2 file names are always given an extension as tcl.

4.6 Simulation overview

The following components exit in NS-2 as seen in the figure below.

- NS , the simulator
- Nam , the network animator, this is for the following scenarios
    - Visualize ns (or other) outputs
    - Nam editor: GUI uses in generating ns scripts
    - Processing: This carry out the task of traffic and topology generation
    - Post processing: This component carry out the following tasks
    - Trace analysis with Unix or GNU/Linux tools like awk, perl or tcl
    - Graphical visualization with graph

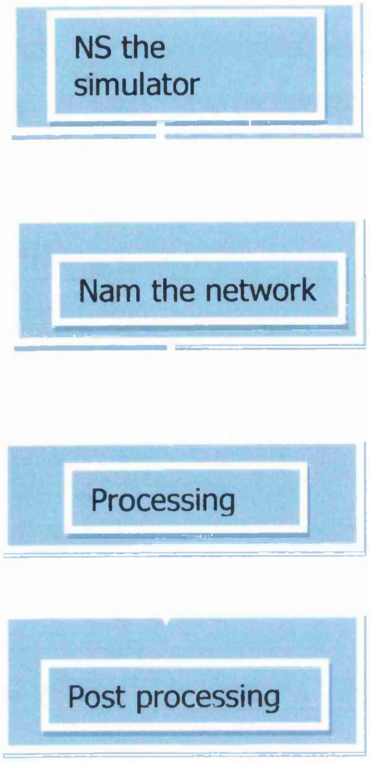

Fig 4.2 NS-2 Simulation overview

4.7 Ubuntu

Ubuntu is an open source operating system built around linux kernel and it supports all of your favorite web-based mail programs like Yahoo(TM) or Gmail (TM).It Includes Mozilla's Firefox 3 as the default browser. Faster, safer and themed browsing for users. It is not difficult to use because of its GUI functionality.

There are many different operating systems that are based in linux: Fedora, Red Hat, Mandriva, Debian, Suse, Gento etc. And ubuntu is now one of the OS contending with the above mentioned ones. And it stands out to have a difference among them.

4.7.1 Why Ubuntu?

Ubuntu creates a distribution that provides and up-to-date and a coherent Linux system for desktop and server computing. It includes a number of carefully selected packages from the

Debian distribution and retains its powerful package management system. It allows for easy installation and clean removal of programme. Considering quality issue, Ubuntu produces a robust and feature-rich computing environment that is suitable for use in both home and commercial environments. It works perfectly with VMware workstation which is one of the popular virtual machines that enables running of NS-2.

4.7.2 Installing Ubuntu

Many options exist on how Ubuntu can be installed, some of the common ways it can be installed and run are: as sole OS (single booting),in addition to another OS (dual booting),within your existing OS (virtualization (usually known as virtual machine),from your CD disc, using Live CD.

Ubuntu can be installed with the graphical CD. Make sure that your computer is set to boot from a CD before a hard drive.

4.8 Virtual Machine ware (VMware)

VMware is one of the non-free virtual machine applications which is compatible with Ubuntu as both a host and guest OS. Several versions of it are available which can be installed on Ubuntu. It is used as a work station in running of NS-2.

5 Methodology

5.1 Introduction

This chapter deals with the applications that were used in our simulation work, which are emergency application (EA) and routine application (RA) and also samples of how NS-2 was run in these simulations.

5.2 Broadcast Application

Broadcasting is the transmission of data or information from one source to all other recipients. In broadcast application, there is no retransmission nor acknowledgment unlike the case of unicast where this occurs, this is because data packets are transmitted without RTS handshaking [39].

In this thesis, we have considered traffics and applications:

- Emergency Application (EA), E.g Voice
- Routine Application (RA) E.g Video

5.3 Network Topology

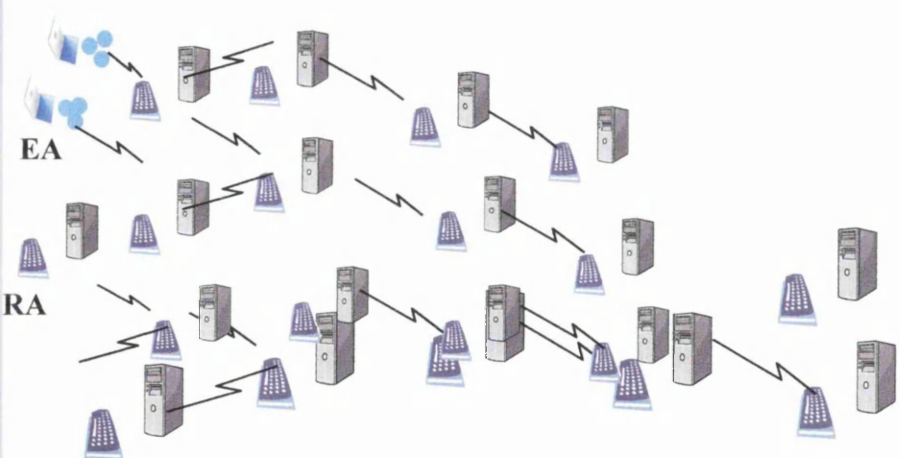

Fig 5.0 Application Setup

5.4 Emergency Applications (EA)

In this application, messages called Emergencies can be sent to various stations. This generates critical safety message events such as notification of collision which has the highest priority and requires reliable and timely transmission. The aim of it is to alert a station for danger, especially for road safety reasons. This is an application deployed in dedicated short range communication (DSRC). This application is designed to provide for both road safety collision warning and avoidance [39]. The very important metric in this type of application is delay. This is because, if the message is not sent and received at the quickest time, it will lead to collision between vehicles. EA as labeled in the figure above is for Emergency stations while RA is for Routine stations, 16 stations in all were simulated in this network. From the figure above, we have just used two different symbols to differentiate between them. Laptops symbols have been used to represent EA while desktop symbols represent RA.

Simulations were run in which numbers of stations for the different applications were changed in different scenarios as can be seen in the parametric tables later. We have also presented below, few samples of how the results appear in NS-2 environment.

5.4.1 Routine Applications

In real time applications, this application is given low priority; routine messages are sent to stations. These applications are assumed to generate some periodic messages such as positive broadcast. Messages are called routine and they are important for collaborative safety but occasional lost of message may not result to distance consequences. Since delay is not a big issue in this type of application, it can tolerate some levels of delay, without having much negative impact on its result. This means that the message but not be sent as fast as possible as in the case of emergency messaging.

5.4.2 High priority Applications (HP)

In 802.11 legacy, we can make an analogy between this and the former. Just like in the case of Emergency application where preference is given to emergency messages as compared to routine messages, in that of legacy, high priority applications have more preferences in transmission and contending for channel resources. One of the means to see the effectiveness of the performance metrics of high priority applications is to control both MAC and traffic generation parameters of low priority applications, this could be by , Changing MAC parameters, varying number of node, packet size and inter arrival time a of lower priority applications. This is what was carried out in these simulations.

5.4.3 Low priority Applications (LP)

These are applications that have less preference or priority in transmission. It has to wait for the higher priority application to transmit before it can do. This time of waiting for its opportunity to transmit increases it delay. The traffic generation and MAC parameters can be controllable. In dealing with 802.11 legacy, the MAC parameters for Low priority applications can be configured but not controlled.

5.5 Metrics

In this work, 3 basic metrics have been used in our analysis:

- **Throughput**, this is usually expressed as a unit of bits per second. It is the minimum end-to-end transmission rate. The formula used in calculating is [expr (($bw0*32*8))/$time]", the explanation of this formula is in the code of my programme which can be seen in appendices.

We took the value of each type of traffic and station, and plotted the average values of the various stations/Traffics. This is done with delay and packet loss as well.

- **Delay,** this is the average time of transit , it is a sum of processing, propagation and queuing delays
- **Packet loss**, this is the number of packets dropped, also they are packets that never reach its destination or packets that arrives late and hence cannot be used or play its multimedia content. In our result, the packet lost obtained from graphs and results is in bits, we then calculated an equivalent packets of such bits, and this is shown the table below.

5.6 Problem of Legacy and Solution

It was earlier mentioned that 802.11 legacy lacks QoS support for real time applications [39]. This is because DCF mechanism employs carrier sense multiple access with collision avoidance hence cannot offer differentiated services for QoS guarantee. Every station in this legacy transmits at same time without priority given to any type of application. With this problem, it lacks the mechanism to render differentiated services to real time applications such as voice and video for QoS guarantee.

The solution to 802.11 legacy is by using enhanced EDCF mechanism, which supports differentiated services and render QoS guarantee. Given a targeted QoS, it is seen that controlling the LP applications, the HP still achieved its targeted QoS requirements. Furthermore, in controlling the MAC and traffic generation parameters for LP application, we could observe similarities in the differentiated metrics of delay and throughput etc. The effective of 802.11e MAC on provisioning of QoS for HP applications is one the solutions to the problem of legacy.

5.7 Running NS-2

The figure below shows how NS-2 was run throughout the simulation.

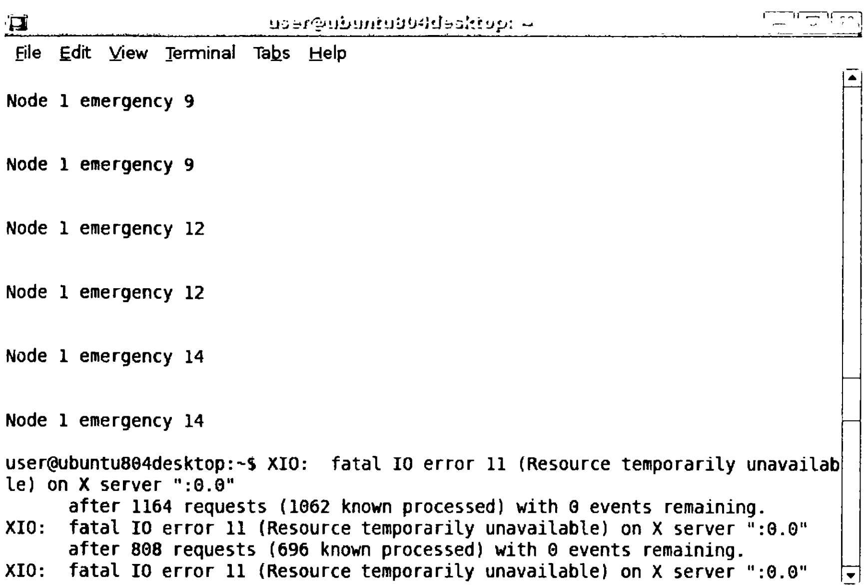

Fig.5.1 Command prompt used in running simulations

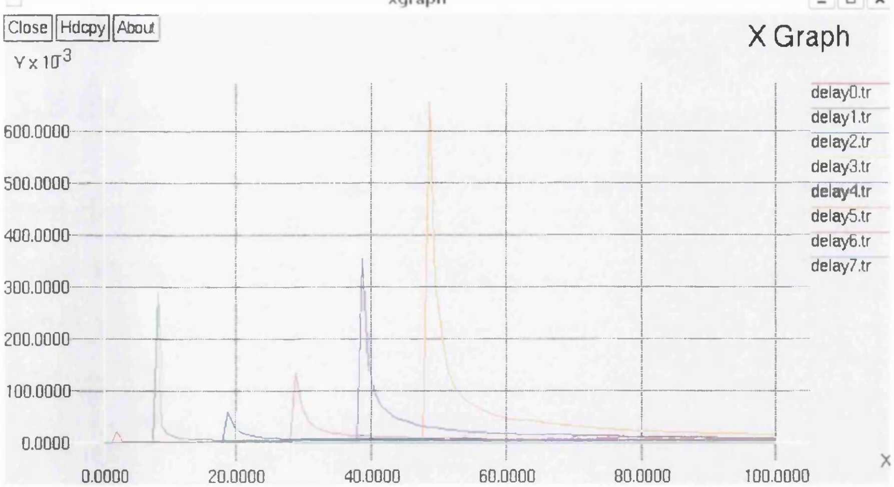

Fig 5.2 Sample of Delay graph

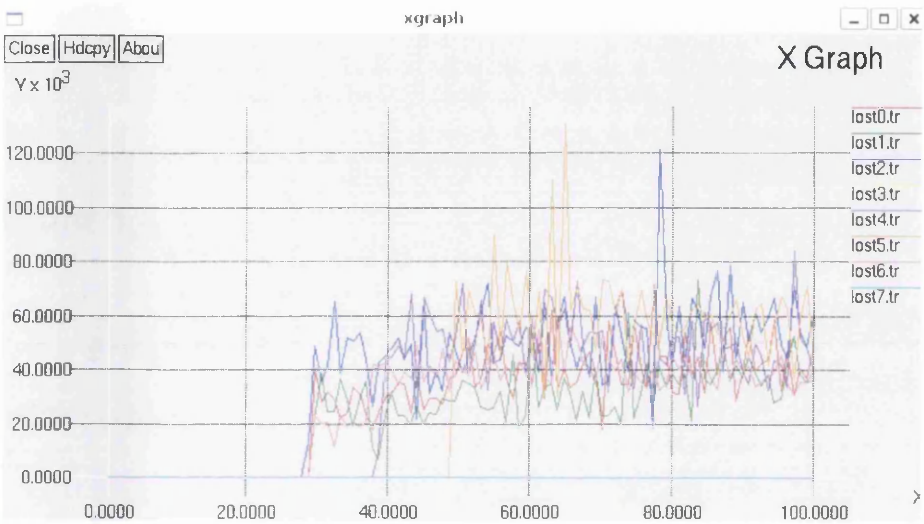

Fig 5.3 Sample of Packet Loss graph

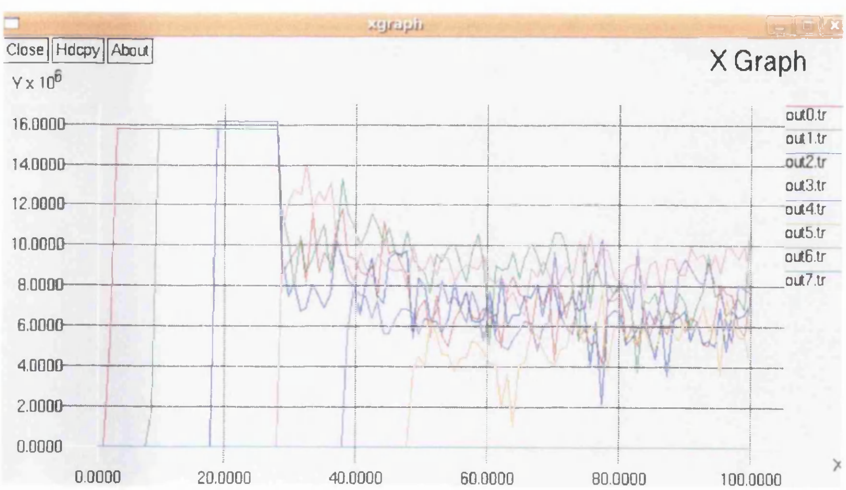

Fig 5.4 Sample of Throughput graph

5.8 Explanation of axes

From the figures above, the X axis is the simulation time, which indicates how long the simulation lasted in seconds, while the Y axis is the values of the metric parameter simulated for. As seen above, Figure 5.2 shows how the delay values are obtained, figure 5.3 shows how packet loss is obtained and figure 5.4 is for Throughput result.

5.9 Simulation Parameters

The table shows the parameters and values that has been use in my all simulation scenarios.

Table 5.0 Mac Parameters for various stations

Simulation Parameters

Broadcast Application (S=Stations)

with same parameters for all stations

MAC Parameters

Scenario 1

S/NO **Parameters**

		HP1	HP2	LP1(8S)
1	AIFS	2	2	4
2	Cw_{min}	7	7	10
3	PF	2	2	2
4	TxOPlimit	0.003	0.003	0.003

Scenario 2

		HP1	HP2	LP1(8S)
1	AIFS	2	2	6
2	Cw_{min}	7	7	15
3	PF	2	2	2
4	TxOPlimit	0.003	0.003	0.003

Scenario 3

		HP1	HP2	LP1(8S)
1	AIFS	2	2	6
2	Cw_{min}	7	7	31
3	PF	2	2	2
4	TxOPlimit	0.003	0.003	0.003

Scenario 4

		HP1	HP2	LP1(8S)
1	**AIFS**	2	2	7
2	**Cw_{min}**	7	7	15
3	**PF**	2	2	2
4	**TxOPlimit**	0.003	0.003	0.003

Broadcast Application

with varying parameters for LP stations

Scenario 1

		HP1	HP2	LP1(8S)
1	**AIFS**	2	2	4
2	**Cw_{min}**	7	7	10
3	**PF**	2	2	2
4	**TxOPlimit**	0.003	0.003	0.003

Scenario 2

		HP1	HP2	LP1(8S)
1	AIFS	2	2	6
2	Cw_{min}	7	7	15
3	PF	2	2	2
4	TxOPlimit	0.003	0.003	0.003

Scenario3

		HP1	HP2	LP1(8S)
1	AIFS	2	2	6
2	Cw_{min}	7	7	31
3	PF	2	2	2
4	TxOPlimit	0.003	0.003	0.003

Scenario4

		HP1	HP2	LP1(8S)
1	AIFS	2	2	7
2	Cw_{min}	7	7	15
3	PF	2	2	2
4	TxOPlimit	0.003	0.003	0.003

Broadcast Application for 802.11e

with varying parameters for LP stations

Scenario 1

		HP(6 Stations)	LP1(6S)	LP2(4S)
1	AIFS	2	4	6
2	Cw_{min}	7	10	15
3	PF	2	2	2
4	TxOPlimit	0.003	0.003	0.003

Scenario 2

		HP(6 Stations)	LP1(6)	LP2(4S)
1	AIFS	2	4	6
2	Cw_{min}	7	10	15
3	PF	2	2	2
4	TxOPlimit	0.003	0.003	0.003

Scenario 3

		HP(6 Stations)	LP1(6S)	LP2(4S)
1	AIFS	2	4	6
2	Cw_{min}	7	10	15
3	PF	2	2	2
4	TxOPlimit	0.003	0.003	0.003

Scenario 4

		HP(6 Stations)	LP1(6S)	LP2(4S)
1	AIFS	2	7	9
2	Cw_{min}	7	31	64
3	PF	2	2	2
4	TxOPlimit	0.003	0.003	0.003

Broadcast Application for 802.11e with reductions of HP Stations(1)

Scenario1

		HP1	HP2	LP1(8S)
1	AIFS	2	2	4
2	Cw_{min}	7	7	10
3	PF	2	2	2
4	TxOPlimit	0.003	0.003	0.003

Scenario2

		HP1	HP2	LP1(8S)
1	AIFS	2	2	4
2	Cw_{min}	7	7	10
3	PF	2	2	2
4	TxOPlimit	0.003	0.003	0.003

Scenario3

		HP1	HP2	LP1(8S)
1	**AIFS**	2	2	6
2	**Cw_{min}**	7	7	15
3	**PF**	2	2	2
4	**TxOPlimit**	0.003	0.003	0.003

Scenario4

		HP1	HP2	LP1(8S)
1	**AIFS**	2	2	7
2	**Cw_{min}**	7	7	31
3	**PF**	2	2	2
4	**TxOPlimit**	0.003	0.003	0.003

Broadcast Application for

802.11e

with reduction of HP stations(2)

Scenario1

		HP	LP1(10S)	LP2(4S)
1	**AIFS**	2	4	6
2	**Cw_{min}**	7	10	15
3	**PF**	2	2	2
4	**TxOPlimit**	0.003	0.003	0.003

Scenario2

		HP	LP1(10S)	LP2(4S)
1	**AIFS**	2	4	6
2	**Cw_{min}**	7	10	15
3	**PF**	2	2	2
4	**TxOPlimit**	0.003	0.003	0.003

Scenario3

		HP	LP1(10S)	LP2(4S)
1	**AIFS**	2	6	9
2	**Cw_{min}**	7	15	31
3	**PF**	2	2	2
4	**TxOPlimit**	0.003	0.003	0.003

Scenario4

		HP	LP1(10s)	LP2(4S)
1	**AIFS**	2	7	9
2	**Cw_{min}**	7	31	64
3	**PF**	2	2	2
4	**TxOPlimit**	0.003	0.003	0.003

Table 5.1 Traffic generation parameters for various stations

Traffic Generation Parameters

Broadcast Application with same parameters for all stations

Scenario1

	HP1	HP2	LP1(8Stations)	LP2(4 Stations)
Pkt size	200	200	100	120
Arrival rate	0.02	0.02	0.04	0.03
Scenario 2				
Pkt size	200	200	140	180
Arrival rate	0.02	0.02	0.04	0.03
Scenario 3				
Pkt size	200	200	160	1500
Arrival rate	0.02	0.02	0.02	0.012
Scenario 4				
Pkt size	200	200	120	1464
Arrival rate	0.02	0.02	0.04	0.01

Broadcast Application

with varying parameters for LP stations

	HP1	HP2	LP1(8 Stations)	LP2(4 Stations)
Pkt size	200	200	100	120
Arrival rate	0.02	0.02	0.04	0.03
Scenario 2				
	HP1	**HP2**	**LP1(8 Stations)**	**LP2(4 Stations)**
Pkt size	200	200	140	180
Arrival rate	0.02	0.02	0.04	0.03

Scenario 3

	HP1	HP2	LP1(8 Stations)	LP2(4 Stations)
Pkt size	200	200	140	180
Arrival rate	0.02	0.02	0.04	0.03

Scenario 4

	HP1	HP2	LP1(8 Stations)	LP2(4 Stations)
Pkt size	200	200	160	1500
Arrival rate	0.02	0.02	0.02	0.013

Broadcast Application for 802.11e with varying parameters for LP Stations

Scenario1	HP(6 Stations)	LP1(6 Stations)	LP2(4 Stations)
	200	240	160
Pkt size	0.02	0.03	0.01
Arrival rate			

Scenario2	HP(6 Stations)	LP1(6 Stations)	LP2(4 Stations)
	200	1464	100
Pkt size	0.02	0.012	0.01
Arrival rate			

Scenario3	HP(6 Stations)	LP1(6 Stations)	LP2(4 Stations)
	200	1500	100
Pkt size	0.02	0.01	0.01
Arrival rate			

Scenario4	HP(6 Stations)	LP1(6 Stations)	LP2(4 Stations)
	200	1500	250
Pkt size	0.02	0.01	0.05
Arrival rate			

Broadcast Application for 802.11e

with reduction of HP stations

Scenario1	HP(4 Stations)	LP1(8 Stations)	LP2(4 Stations)
	200	240	160
Pkt size	0.02	0.03	0.01
Arrival rate			

Scenario2	HP(4 Stations)	LP1(8 Stations)	LP2(4 Stations)
	200	1464	100
Pkt size	0.02	0.012	0.01
Arrival rate			

Scenario3	HP(4 Stations)	LP1(8 Stations)	LP2(4 Stations)
	200	1500	150
Pkt size	0.02	0.01	0.05
Arrival rate			

Scenario4	HP(4 Stations)	LP1(8 Stations)	LP2(4 Stations)
Pkt size	200	250	100
Arrival rate	0.02	0.05	0.05

Broadcast Application for

802.11e

with reduction of HP stations

Scenario1	HP(2 Stations)	LP1(10 Stations)	LP2(4 Stations)
Pkt size	200	240	160
Arrival rate	0.02	0.03	0.01

Scenario2	HP(2 Stations)	LP1(10 Stations)	LP2(4 Stations)
Pkt size	200	1464	100
Arrival rate	0.02	0.012	0.01

Scenario3	HP(2 Stations)	LP1(10 Stations)	LP2(4 Stations)
Pkt size	200	1500	150
Arrival rate	0.02	0.01	0.05

Scenario4	HP(2 Stations)	LP1(10 Stations)	LP2(4 Stations)
Pkt size	200	250	100
Arrival rate	0.02	0.05	0.05

Table 5.2 Traffic types

Applications and Traffic types Broadcast Application with same parameters for all stations			
NO of stations	Applications	Type	Priority
4	EA	Voice	HP
8	RA	Video	LP1
4	RA	Video	LP2

Broadcast Application with varying parameters for LP stations			
NO of stations	Applications	Type	Priority
4	EA	Voice	HP
12	RA	Video	LP1
			LP2

Broadcast Application for 802.11e			
with varying parameters for LP station			
NO of stations	Applications	Type	Priority
6	EA	Voice	HP
6	RA	Video	LP1
4	RA	Video	LP2

Broadcast Application for 802.11e			
with reduction of HP station (1)			
NO of stations	Applications	Type	Priority
4	EA	Voice	HP
8	RA	Video	LP1
4	RA	Video	LP2

Broadcast Application for 802.11e			
with reduction of HP station (2)			
NO of stations	Applications	Type	Priority
2	EA	Voice	HP
10	RA	Video	LP1
4	RA	Video	LP2

5.10 Network scenarios and Results

Task 1

This task consists of four scenarios as seen in the tables above. In this task, the followings were configured: packet size, inter arrival time for both High and Low priority applications to be same. Also, MAC layers for both LP and HP are the same in all cases. The parametric settings used are

AIFS, Cw_{min}, PF and TXOPlimit. The parameter table also shows the number of stations used for both LP and HP in all scenarios.

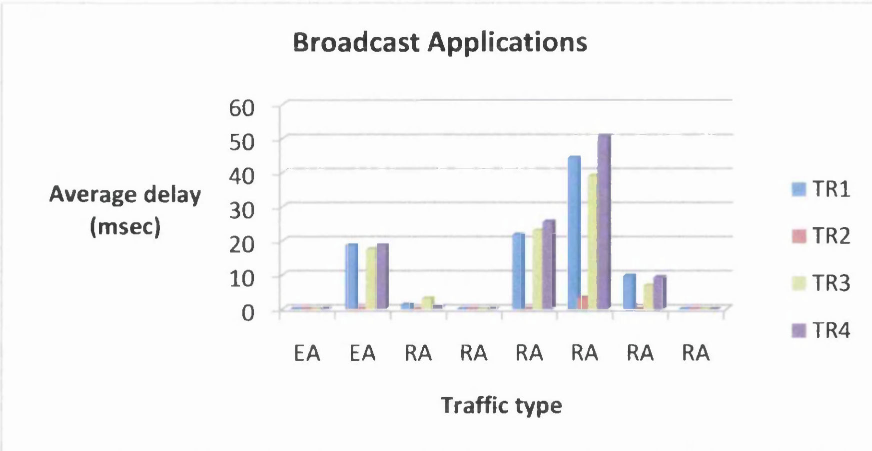

Fig 5.5 Average Delay for LP Stations with Varying Traffic rate

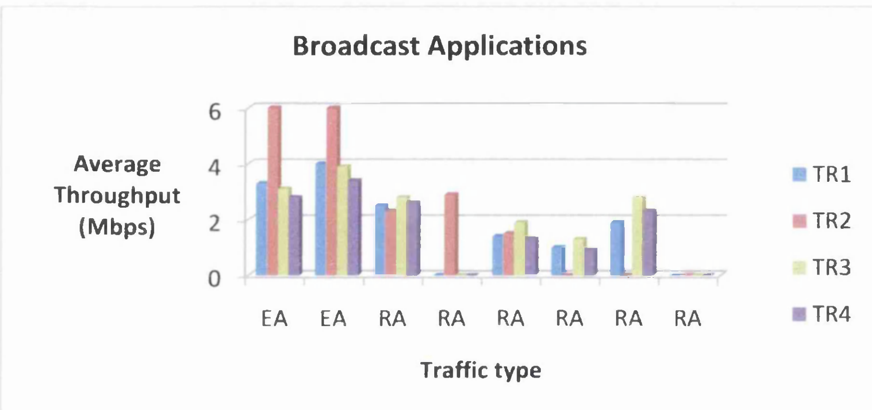

Fig 5.6 Average Throughput for LP Stations with Varying Traffic rate

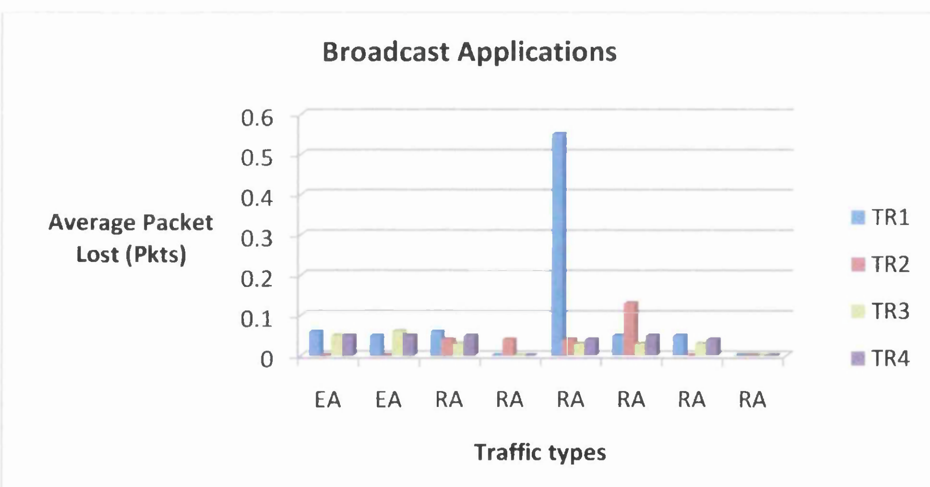

Fig 5.7 Average Packet Loss for LP Stations with Varying Traffic rate

UNIVERSITY OF WALES SWANSEA LIBRARY

5.10.1 Discussion of result for task 1

Figures 5.5-5.7 are the simulated result for controlling MAC layers parameters for LP stations and then a fixed traffic generation and MAC parameters for HP stations. In this scenario, the result shows the effectiveness of controlling LP traffic. Results also show the differentiated values of delay, throughput and packet loss for various applications and similar performance when the same MAC and Traffic generation parameters are used. In all cases, it is observed that the delay is brought under control so that the ITU-T standard for these applications are kept to. None of it exceeded 150ms, but has a very low delay which can be effectively utilized in road safety application and vehicular network.

Task 2

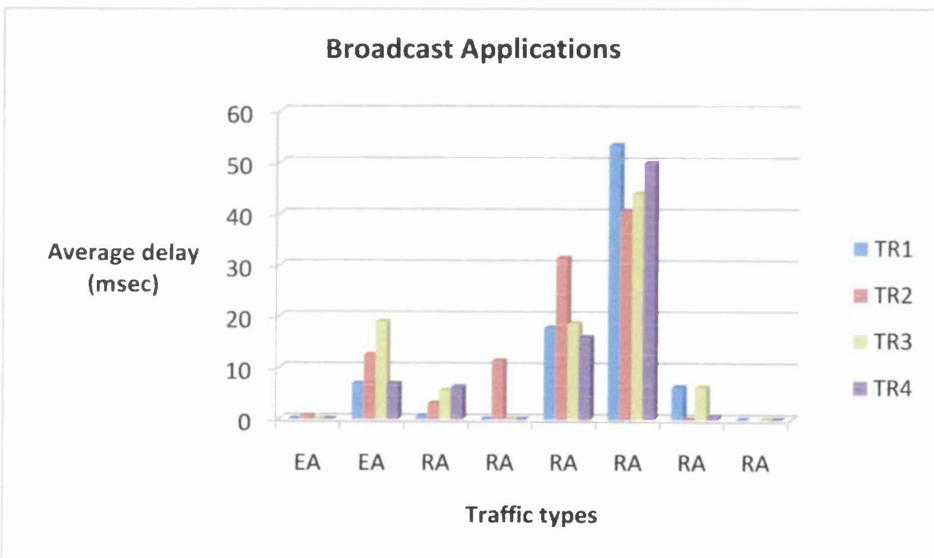

Fig 5.8 Average delay for Stations with same MAC Layer

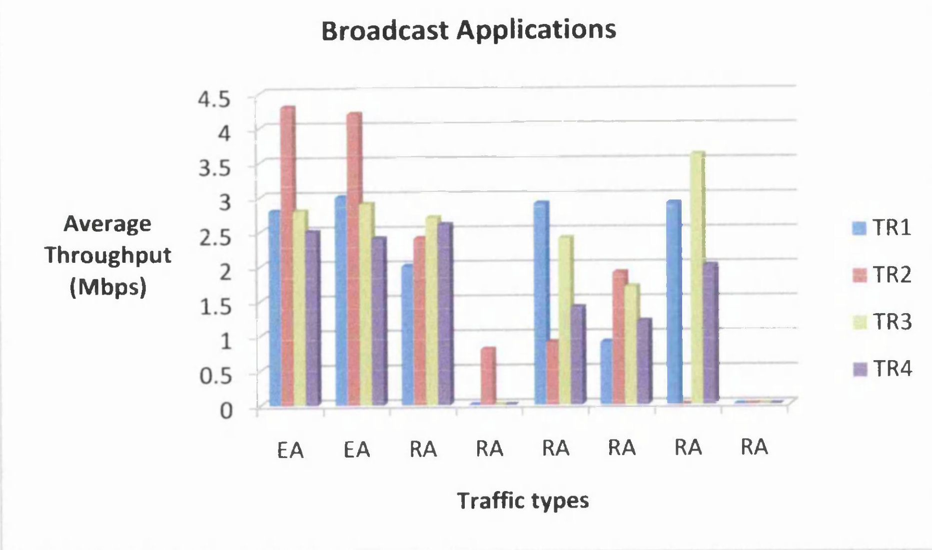

Fig 5.9 Average Throughput Stations with same MAC Layer

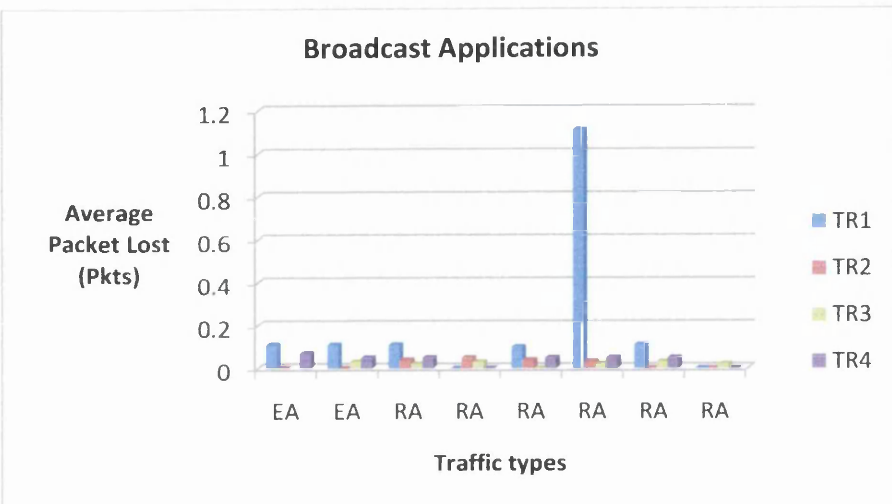

Fig 5.10 Average Packet Loss for LP Stations with same MAC Layer

5.10.2 Discussion of result for task 2

In Figures 5.8-5.10 all our MAC and traffic generation parameters are configured to be same, for both HP and LP stations .In this scenario, it can be observed that although the values of the metrics differs but they have similar delay , throughput and packet loss values. This is because, using same MAC parameters and traffic rate, the applications do not really have a priority in transmission and hence every application sends packets without priority.

Task 3

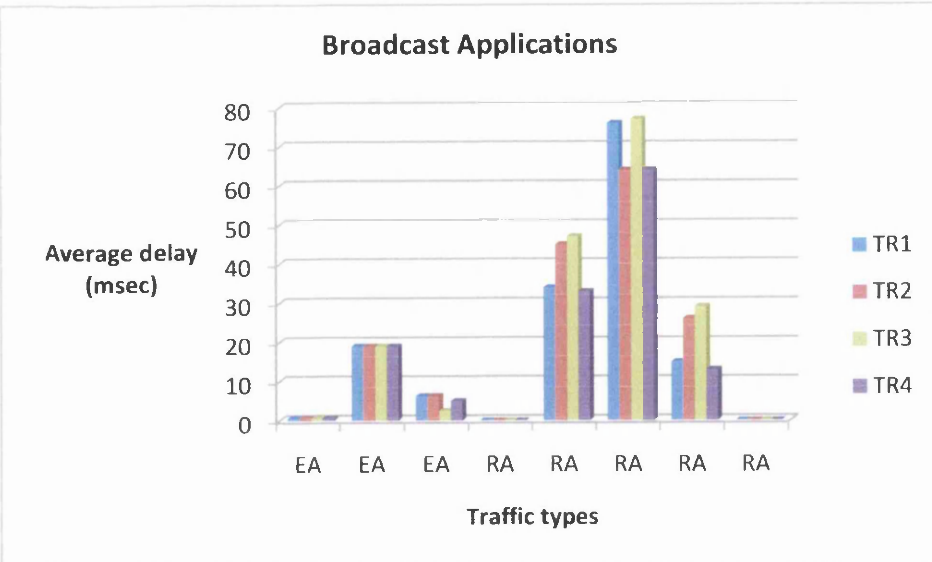

Fig 5.11 Average delay for Stations with fix MAC for HP

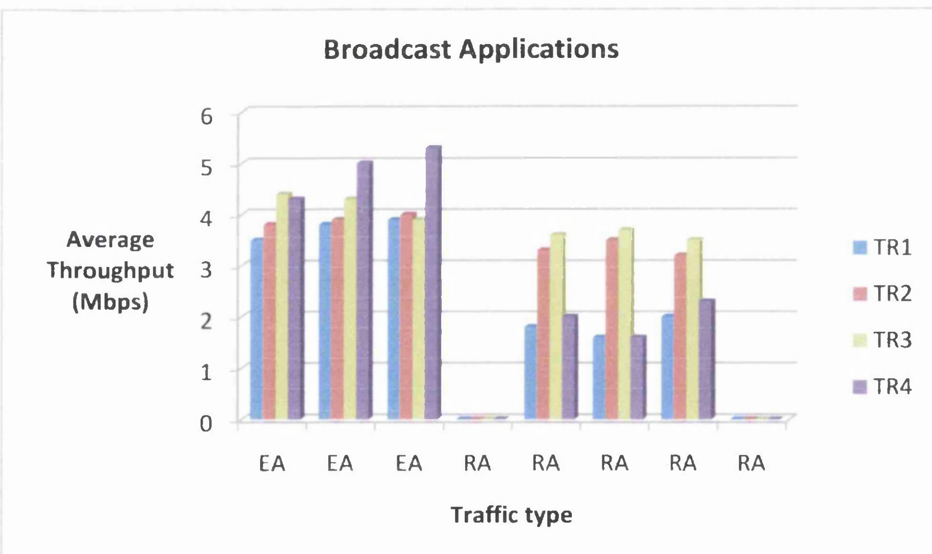

Fig 5.12 Average Throughput for Stations with fix MAC for HP

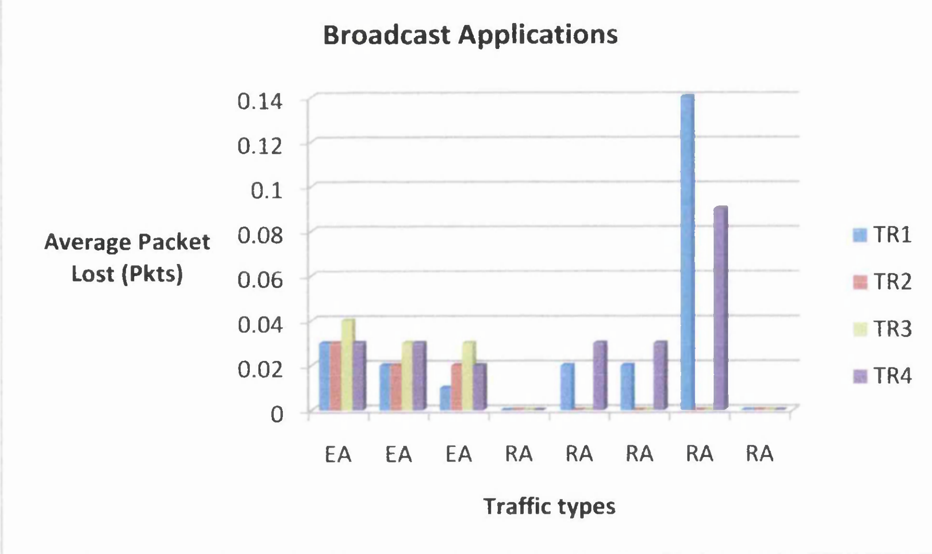

Fig 5.13 Average Packet Loss for Stations with fix MAC for HP

5.10.3 Discussion of result for task 3

In figures 5.11- 5.13, we have configured same Mac and traffic rate for HP applications and the then varying it for LP stations. In this scenario, these parameters are controlled so as to ensure the performance of HP applications. The result shows that HP stations are able to attain its QoS requirements when the LP applications are controlled.

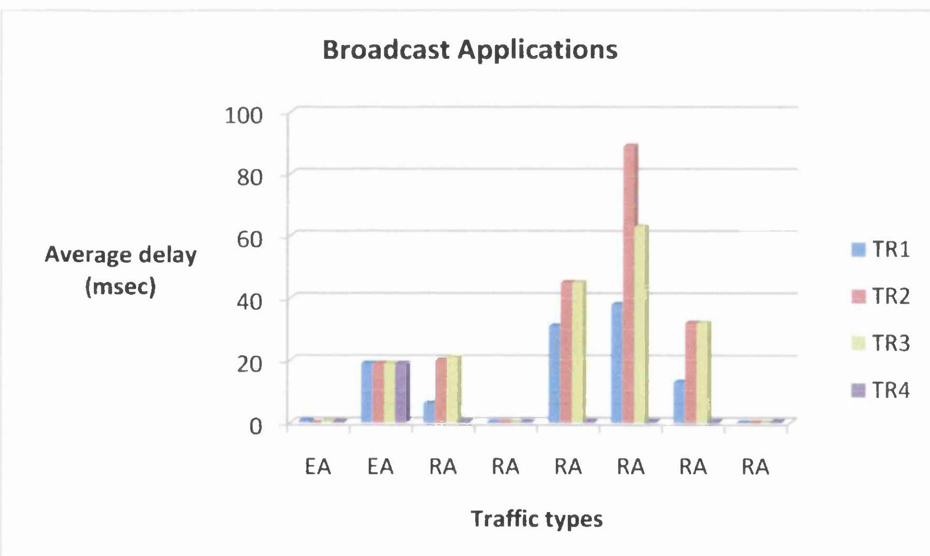

Fig 5.14 Average delay for 802.11e with control of MAC HP Stations

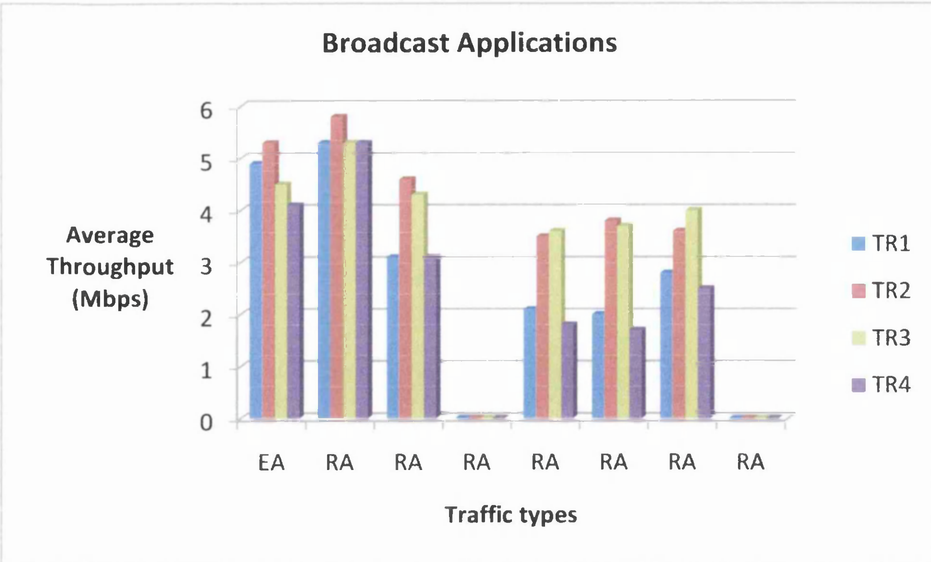

Fig 5.15 Average Throughput for 802.11e with control of MAC HP Stations

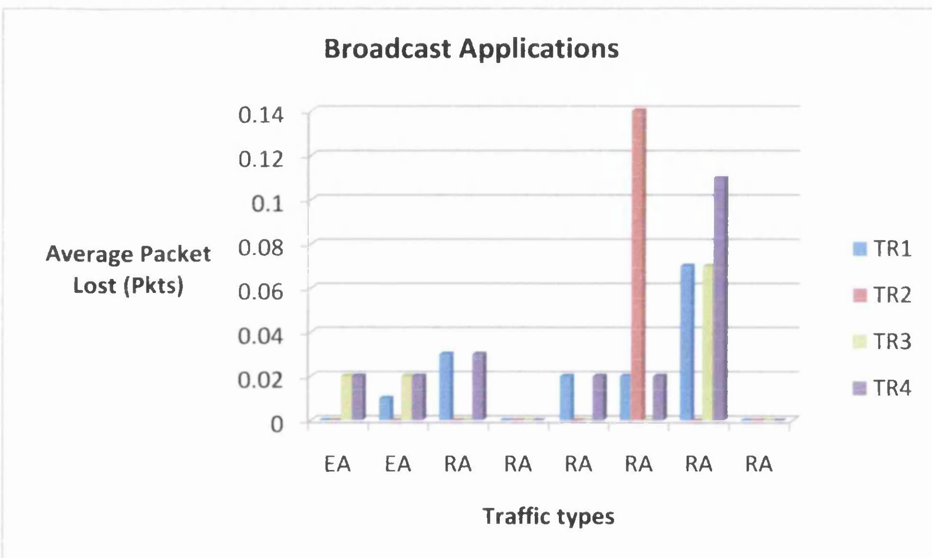

Fig 5.16 Average Packet Loss for 802.11e with control of MAC HP Stations

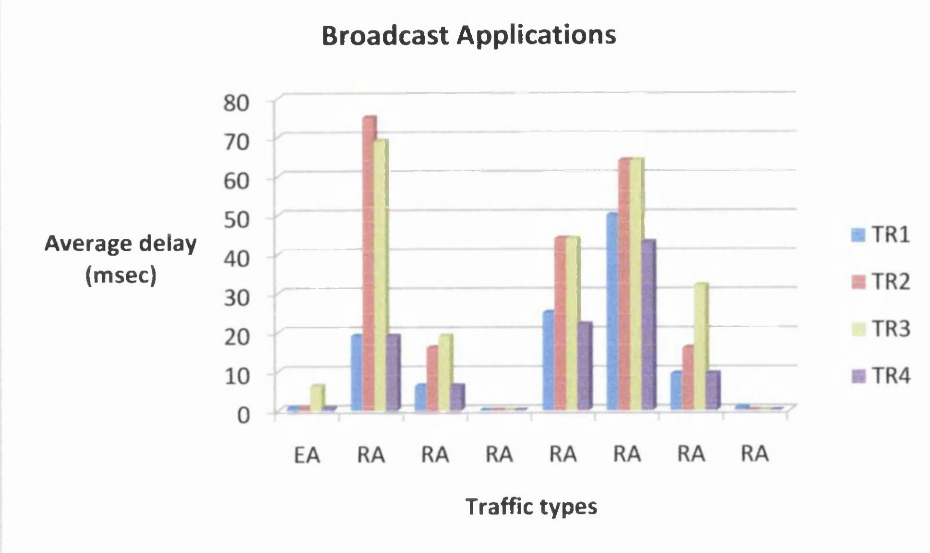

Fig 5.17 Average delay for 802.11e with reduced HP Stations

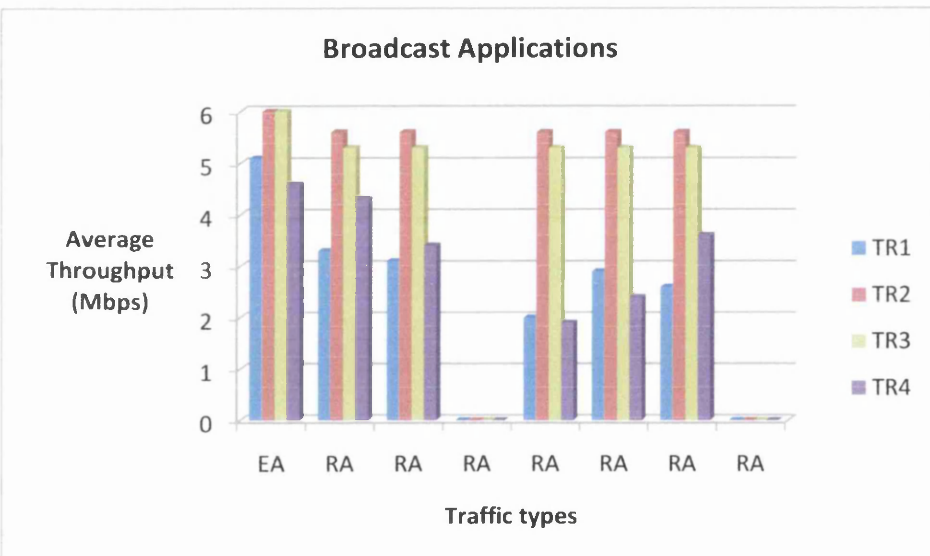

Fig 5.18 Average Throughput for 802.11e with reduced HP Stations

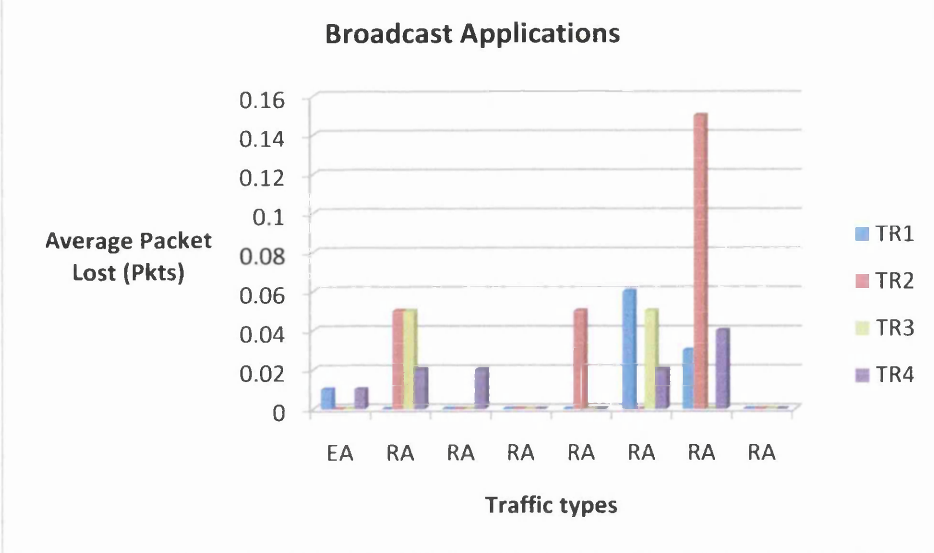

Fig 5.19 Average Packet Loss for 802.11e with reduced HP Stations

5.10.4 Discussion of result for task 3b

Furthermore, in figures 5.14-5.16, these stations are configured with fix values of MAC parameters for HP stations while traffic generation parameters were varied. In this simulation, values of EA have better delays to support this type of application as compared to RA. The result also shows differentiated values of throughput and packet losses, that is they are similar in both EA and RA. This can be seen if compared to the result obtained in Figures 5.5-5.7.

And finally in Fig 5.17-5.19, we further reduced the number of HP applications to see if the QoS requirement will still be attained, and yes it did. This is can be seen from the graphs plotted and can be observed that the increase of LP stations and reduction of HP applications didn't affect the metric performance. The reduction of LP stations also provide more channel capacity for HP stations/traffics, hence improving it performance. You can see the Throughput value increasing to about 6Mbps as oppose to the preceding scenario of about 5.3Mbps. The delay is reduced up to about 8ms as against 20ms in the preceding scenario.

5.11 General Discussion

The results in our simulation work shows that controlling parameter for both MAC and traffic generation rates, EA will be able to used in road safety applications, since the differentiated values of delay in all cases are low, so that emergency messages can be received in very short duration to alert other stations of danger ahead. It also further shows that varying MAC and traffic generation parameters the various stations have differentiated values of throughput and packet loss, they are similar to each other, the difference between them is not very much. The control of both MAC and traffic generation parameters are to ensure QoS guarantee for HP applications, since these applications are given priority compared to the others. In these simulations, HP is same with EA, because much preference is given to those stations for transmission, while RA and given Low priority hence known as LP stations.

Because of problem of legacy which lacks provision of QoS for real time applications, differentiated services of 802.11e for HP stations deals with these issues, and these were configured so that HP stations can achieve this goal to provide QoS for his stations.

In conclusion, voice application is given HP which is EAs in our simulation; this is because, voice cannot withstand much delay compared to video applications (RA) which is given low priority.

THIS

PAGE

IS

LEFT

BLANK

THIS

PAGE

IS

LEFT

BLANK

THIS

PAGE

IS

LEFT

BLANK

6 Conclusion and Future Work

6.1 Introduction

The issue has been that 802.11 legacy lack QoS support for real time applications. It uses DCF mechanism and there is no services differentiation. To help this situation, another legacy is adopted to support this type of application.

Many have worked on enhanced EDCF as in the literature on how to achieve QoS guaranteed in wireless networks. Different approaches have been adopted to handle this issue.

In carrying out these simulations, the followings were observed:

- you can only see the differences in the different applications for these legacies when more than one application is used
- is not that 802.11 legacy does not provide some level of QoS but it is limited, and lack guarantee
- packet losses in both cases does not really show any difference.

In this research the followings have been achieved

- the essence of our simulations were to control LP applications so that HP can retain, improve and meet QoS requirements
- in all our results, we have controlled LP applications so as to ensure QoS guarantee for HP applications, and this is achieved
- we have also ensured that performance metrics are brought as low and never exceeded the recommendation standard. Delay and packet losses in all our simulations are quit low and never exceeded standard values
- real time applications are sensitive to delay and hence is value must be as low as possible, we have ensured that our network achieved that
- one of the applications of this legacy is in road safety application and vehicular networks, in road safety application, messages are sent to other vehicles to alert them of danger etc. In our simulations, we have been able to achieve this by

sending Emergency and routine messages, our emergency messages are sent at the quickest possible time, to avoid collision, while routine messages could tolerate some certain delays. All of these have been achieved in this simulation.

6.2 Conclusion

Our simulations show the performances differences with DCF and EDCF mechanisms. From our results, controlling LP applications will result to effective performance of HP applications. It also shows that EDCF has better performance due to differentiated services compared to DCF where all stations have equal opportunity to transmit.

6.3 Future work /Recommendation

We are continuing research in this area, especially in DSRC and vehicular network. So that we can see the effect of other MAC parameters on HP and LP applications like transmission opportunity. Because in our simulations, it was kept constant in all cases, but what will the performance of the network be if it is changed and other MAC parameters added? If anyone is working on this, we will recommend the person handles this task.

ITU-T recommendations for the different applications have been considered and none of the results exceeded the recommended value for any of the traffics.

List of Acronyms

QoS	Quality of Service
WLAN	Wireless Local Area Network
UMTS	Universal Mobile Telecommunication System
WIMAX	*Worldwide Interoperability*
3G	Third Generation
4G	Forth Generation
HSDPA	High-Speed Downlink Packet Access
IP	Internet Protocol
BER	Bit Error Rate
WCDMA	Wideband Code Division Multiple Access
FEC	Forward Error Correction
GSM	Global System for Mobile network
VoIP	Voice Over Internet Protocol
MAN	Metropolitan Area Network
BSS	Basic Service Set
DC	Distributed Coordinator
DCF	Distributed Interframe Space
EDCF	Enhanced Distributed Cordination Function
HCCA	HCF controlled channel Access
HCF	Hybrid Cordination Function
MAC	Media Access Control
PCF	Point Cordination Function
EDCA	Enhanced Distributed Cordination Access
CBR	Constant Bit rate
PSTN	Public Switch Telephone Network
ATM	Asychronous Transfer Mode
SIP	Session Initiation Protocol
ISO	International organisation for Standardization

ITU	International Telecommunications Union
MPEG	Moving Picture Expert Group
UDP	User Datagram protocol
TCP	Transmission Control protocol
AEDCF	Adaptive EDCF
HC	Hybrid Coordinator
CF	Contention free
CFP	Contention free Period
QAP	QoS Access Point
QSTA	Qos Station
CFB	Contention Free burst
Acs	Access Categories
AIFS	Arbitrary interframe space access category

REFERENCES

1. T.Rudolf, T., Jason, *WCDMA Requirements and Practical Design.* 2004.
2. M.Michael, *Voice-Quality Monitoring and Control for VoIP.* IEEE Internet Computing, 2005.
3. S. Murayama, F.T., *Multimedia data transmission over wireless network with interference*
4. A.Zakhor, W.W., *Multipath Unicast and Multicast Video Communication over Wireless Adhoc Networks.*
5. Balakrishan, N.F.a.H., *Packet Loss Recovery for streaming video.*
6. D. Pong , T.M., *Call Admission Control for IEEE 802.11 Contention Access Mechanism.* 2003.
7. S.A Hussain, K.Z., M.T Khan, S.Ahmad,U.Farooq, *Dynamic Contention Window for Quality of service in IEEE 802.11 Networks.* National conference on Emerging Technologies 2004.
8. Y.Lin .W.S Vicent Wong, *Saturation Throughput of IEEE 802.11e EDCA Based on Man Value Analysis.*
9. D.D. Demarch, L.B.B., *Evaluating the IEEE 802.11e Reference Scheduler for Firm Real-time Traffic.*
10. B.Aladdin Al-Gazzar , M.E.A.-E., A.Ahmad Al-farra, S.Shady Al-Atrash, *Congestion Control and Queue Management in IEEE 802.11e.*
11. S.Choi, J.d.P., S.Shankar, S.Mangold, *IEEE 802.11e Contention-Based Channel Access (EDCF) Performace Evaluation.*
12. V.A.Siris, C.C., *Resource Control for the EDCA Mechanism in Mult-Rate IEEE 802.11e Networks.*
13. Wong, Y.L.W.S.V., *An admission Control Algorithm for Multi-hop 802.11e based WLANs.*
14. D.Gao.C.Heng, C.H.L., K.N.Ngan, *Improving WLAN VoIP Capacity through Service Differentiation.* IEEE Transactions on Vehicula Technology, 2007. **X**.
15. A.Alkhoraidly, K.S.a., *An OPNET-based Simulation Approach for Deploying VoIP*
16. B.Selvig, B.A., T.Skeie, P.Engelstad, *Differentiated Services in 802.11e WLANs.*
17. Dixon., R., *Internet video conferencing.*
18. Zarki, H.L.a.M.E., *Adaptive source rate control for real-time wireless video transmission.*
19. K. Chandra, A.R.R., *Modeling one-and Two-layer Variable Bit Rate Video.* IEEE Transactions on Networking,. **7**.
20. Kroon, R.C.a.P., *Low bitrate speech coders for multimedia communications.* IEEE **34**(12).
21. S.Dhar.R.Bera, K.M., *Wireless LAN to support multimedia Communications using spread spectrum technology.*

22. H.Sameh Ghwanmeh, A.R.A.-Z., *Wireless Network Performance Optimization Using opnet Modeler.* Information Technology, 2006.
23. A.Pertrck, B.O.H., *The IEEE 802.11 Handbook :A Designer's Companion.* IEEE, 2005.
24. N.Qiang, *A survey of QoS Enhancements for IEEE 802.11 Wireless LAN.* Journal of Wireless Communications and Mobile Computing, 2004. **4**(5): p. 547.
25. 2006, B., *Wireless Local Area network(WLAN).* 2006.
26. C.Eklund, J.K., C. Weil,D.R Smith, *Advances in wireless networking Standards.* IEEE.
27. P.Larcheri, R.L.C., *Scheduling in 802.11e:Open-Loop or Cloed-Loop.*
28. G.Pavou, D.A.a., *Distributed Multimedia in Telecommunications service Engineering Using the Distributed Component Object model.*
29. K.Pahlavan, *Principles of Wireless Networks.*
30. M.Kavehrad, *Trends in Local Wireless Networks.*
31. F. Babich , M.D.o.a.F.V., *Video Quality Estimation in Wireless IP Networks: Algorithm and applications.* ACM Transaction on Multimedia Computing and Applications, 2008. **4**(1).
32. A. Wei, S.B., *A new PCF scheme for multimedia traffic in IEEE802.11 wireless-LAN.* .
33. L.Anthony, G.H., I.Niemegeers, *Performance Evaluation of MPEG-4 Video Streaming over UMTS Networks using an Integrated Tool Environment.*
34. V. S. Wold , O.C.G., F. Eliassen and J..A. Michaelsen, *Real-time Content Analysis:QoS –Aware Application Composition and Parallel Processing.* ACM Transactions on multimedia Computing Communications and Applications, 2006. **2**(2).
35. Zarki, H.L.a.M.E., *An adaptive delay and synchronization control scheme for WI-FI based audio/video conferencing.*
36. S.Abraham, M.P., C.Michael , H.Zhang, *The Capacity of VoIP over 802.11.* Bell Labs Technical journal, 2007.
37. Pavlou, D.A.a.G., *Distributed Multimedia in Telecommunications Service Engineering Using the Distributed Component Object Model.*
38. M. Ryu, Y.K.a.H.P., *Systematic QoS Class Mapping Framework for Application Requirement over Heterogeneous Networks.*
39. J.He, Z.T., T.O'Farrell,T.Chen, *Performance Analysis of DSRC Priority Mechanism for Road Safety Applications in Vehicular Networks.* 2009.
40. D. Wu. QoS, *QoS provisioning in wireless networks* 2005.
41. Chuang, H.K.W.a.P.H., *Dynamic QoS Allocation for Multimedia AD Hoc Wireless Networks.*
42. H. Luo, S.L., B Bhargavan, J Cheng and G. Zhong *A packet scheduling Approach to QoS support in Multihop wireless Networks.* 2000.
43. Dhesikan, S., *H.323/RSVP Synchronization for video over*

44. A.Banchs, X.P.-C., D.Qiao, *Providing Througput Guarantees in IEEE 802.11e Wireless LANs.*
45. D.He, Q.C.S., *Simulation Study of IEEE802.11e EDCF.*
46. V.Kataev, *Video Simulation through 802.11e Using NS-2 Documentation.* 2008.
47. P.Pablo Garrido, P.M.M., T.Carlos Calafate, *Evaluation of 802.11 models under ns-2 and OPNET Modeler simulation tools in MANET networks.*
48. C.Ohio, P.C.M.S.a., *Performance Measurement and analysis of H.323 Traffic.*
49. R.Alturki, K.N., R.Mehmood, *End to End Wireless Multimedia Service Modeling over a Metropolitan Area Network.* IEEE UKSIM 2009.