Quality of Service (QoS) over 802.11 Wireless Networks

SATYAJIT MUKHERJEE

Doctor of Philosophy

ASTON UNIVERSITY

August 2008

Aston University

Quality of Service (QoS) over 802.11 Wireless Networks

Satyajit Mukherjee

Doctor of Philosophy
August 2008

Thesis Summary

The following thesis presents a comprehensive analysis of the IEEE 802.11 wireless protocol focussing on the operation of the Medium Access Control layer. Extensive background to the protocol is provided and the problems relating to Quality of Service are discussed. 802.11 networks are investigated through computer simulation and practical experimentation, both of which were carried out by the author.

The majority of wireless local area networks in use today are unable to support multiple services with different Quality of Service requirements. Real time traffic such as Voice over Internet Protocol suffers from poor performance, in terms of Mean Opinion Score in the presence of other traffic such as File Transfer Protocol and Hyper Text Transfer Protocol.

Performance of the legacy distributed coordination function is compared with the performance of the enhanced distributed channel access, and it is found that multiple services can be supported under the newer protocol. In addition to simulated results, a real world wireless testbed is designed, from which a noteworthy set of results are generated on the performance of both legacy and enhanced protocols. The work demonstrates through both simulation and real field testing that service differentiation is possible, but not without significantly penalising low priority traffic such as file transfer protocol, hyper test transfer protocol and peer to peer applications.

It is advised that providing quality of service should not just be concerned with prioritising high priority fragile traffic such as Voice over Internet Protocol, but should also look at a wider range of traffic in a network. By altering the default enhanced distributed channel access parameter set, fairness could be established between competing traffic types while maintaining a satisfactory level of service differentiation between competing traffic streams.

Key Words and Phrases

Distributed Coordination Function (DCF), Enhanced Distributed Channel Access (EDCA), Voice over Internet Protocol (VoIP), Transfer Control Protocol (TCP), Frame Loss.

Acknowledgements

Dr Xiaohong Peng for his guidance and advice as supervisor through the duration of my research. Current and previous members of the Adaptive Communication Networks Research Group for the useful discussions during the course of my research.

Ragbir Bassi, Shelly Fevian-Alliston and Andrew Abbot for their help with equipment in both of the laboratories.

Richard Haywood for his help with the Java scripts to process the packet captures for the retransmission distributions and collaborative work on video transmission over 802.11e EDCA.

I would also like to thank my parents, Indrajit and Krishna and my sister Indrani for their support over the course of my research work. Without their help and support it would not have been possible.

List of Contents

List of Figures

List of Tables

List of Acronyms

ACK	Acknowledgment
AIFS	Arbitration Interframe Space
BPSK	Binary Phase Shift Keying
BSS	Basic Service Set
CCK	Complementary Code Keying
CFP	Contention Free Period
CODEC	Compressor/Decompressor
CP	Contention Period
CRC	Cyclic Redundancy Check
CSD	Circuit Switched Data
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
CW	Contention Window
CWmax	Maximum Contention Window Size
CWmin	Minimum Contention Window Size
DCF	Distributed Coordination Function
DiffServ	Differentiated Services
DIFS	DCF Interframe Space
DOCSIS	Data Over Cable Service Interface Specification
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum
EDCA	Enhanced Distributed Channel Access
EDCF	Enhanced Distributed Coordination Function
ESS	Extended Service Set
FCS	Frame Check Sequence
FHSS	Frequency Hopping Spread Spectrum
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GSM	Global System for Mobile
HCCA	Hybrid Coordinator Function Controlled Channel Access
HCF	Hybrid Coordinator Function

HSCSD	High Speed Circuit Switched Data
HSPA	High Speed Packet Access
HTTP	Hypertext Transfer Protocol
IBSS	Independent Basic Service Set
IEEE	Institution of Electronics and Electrical Engineers
IntServ	Integrated Services
IP	Internet Protocol
ISM	Industrial, Scientific and Medical
LAN	Local Area Network
LLC	Logical Link Control
MAC	Medium Access Control
MADWiFi	Multiband Atheros Driver for Wireless Fidelity
MIMO	Multiple Input Multiple Output
MOS	Mean Opinion Score
NAV	Network Allocation Vector
NEGSOB	Negative Sobel
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
PBX	Private Branch Exchange
PC	Point Coordinator
PCF	Point Coordination Function
PDA	Personal Digital Assistant
PHY	Physical
PIFS	PCF Interframe Space
PSNR	Peak Signal to Noise Ratio
QAM	Quadrature Amplitude Modulation
QAP	Quality of Service Enabled Access Point
QBSS	Quality of Service Enabled Basic Service Set
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
QSTA	Quality of Service Enabled Station
RFC	Request for Comments
RTP	Real Time Protocol
RTS	Request To Send

SIFS	Short Interframe Space
SIP	Session Initiation Protocol
STA	Station
TACS	Total Access Communication System
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
ToS	Type of Service
TSPEC	Traffic Specifications
TxOP	Transmit Opportunity
UDP	User Datagram Protocol
UMTS	Universal Mobile Telephone System
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol
WDS	Wireless Distribution System
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
WAN	Wide Area Network
WWW	World Wide Web

1 Introduction

Over the last 20 years wireless communication has found widespread use in the telecommunications industry. Currently wireless communications is one of the fastest growing areas in the industry. Wireless systems such as Global System for Mobile communication (GSM), Universal Mobile Telephone System (UMTS) and Wireless LAN (WLAN) have become essential tools in people's working and personal lives. The popularity of wireless communication systems is due to its inherent advantages over wired communication systems. The most important advantages are the mobility and flexibility that wireless systems inherently provide [1].

1.1 Early Wireless Systems

Initially wireless system conceptions were concerned with the delivery of voice services to mobile users. Early methods adopted analogue techniques such as Frequency Modulation (FM), with each channel operating on a different frequency, as used in Total Access Communication System (TACS) in the 80's. With data transmission being in its infancy, the use of modems over TACS was not commonplace. Analogue systems are now considered "first generation" or 1G. During the 90's the use of digital modulation techniques and time division multiple access (TDMA) resulted in the popularity of the GSM standard. The first digital systems are now regarded as 2G or "second generation". The increased call quality, security and service provided by 2G systems lead to the rapid growth of the sector during the late 90's and early 21st century. GSM inherently supported data transmission at a rate of 9.6 kbps using Circuit Switched Data (CSD). While this was adequate for remote telnet and other low rate applications, web browsing was painfully slow. The advent of high speed circuit switched data (HSCSD) and packet operated General Packet Radio Service (GPRS) raised the

potential speed to over 100 kbps. Since then, so called 3G or "third generation" networks based on the Universal Mobile Telephone Service (UMTS) have brought broadband speeds (384 kbps) to mobile users. Newer enhancements to UMTS, such as High Speed Packet Service (HSPA) have led to data rates of 7.2 Mbps in urban areas. These technologies are seen to be direct competitors to Wireless LAN, which is introduced in the following section.

1.2 Wireless Local Area Networks

In recent years wireless LAN (WLAN) technology has become commonplace in home and work environments [2], bringing the benefits of multi-megabit broadband to mobile users. Traditional local area networks (LANs) suffer from a lack of mobility for the end user. As with regular telephony services, the introduction of the mobile/cellular networks allowed telephone users the freedom to make calls regardless of location. The series of IEEE 802.11 wireless networking standards aim to bring the same level of freedom and connectivity to mobile data users on a local scale. Wireless LAN offers two main advantages over traditional fixed data networks, such as Ethernet, *Mobility* and *Flexibility*. The end user is no longer limited to working at a computer terminal in a fixed location, as the availability of LAN cabling is no longer a limiting factor. For example a typical office worker could access shared files, printers and other networked resources from another desk, meeting room or canteen area, providing they remain within the coverage area of the base station (referred to as Access Point, or AP). Similarly, a home user could browse the Internet or check Email from multiple rooms within their house, or even the garden, where wired networking is traditionally not available. WLAN deployments are also becoming popular in public areas such as coffee shops, hotels, train stations and airport lounges, giving users the ability to access Internet services on the move. The flexible deployment of wireless networks translates into the ability to rapidly deploy the technology across a building where an existing LAN infrastructure

exists. The installation of wired networking points for additional users can be expensive and time consuming [3]. Adding users to a wireless network is a simple matter of configuration. This can be regarded as an edge user technology, providing mobility and flexibility at the edge of a data network to the client. Bandwidth, a measure of data capacity, of a wireless network is limited by the availability of allocated radio spectrum. Wired systems do not suffer from this limitation, resulting in far higher bandwidth capability. Mobility is also rarely required for servers and other equipment such as printers. For this reason the remaining backbone of data networks are dominated by wired mediums such as copper and fibre optic systems and are likely to remain this way for the foreseeable future.

With the rapid growth of IEEE 802.11 WLAN in airports, coffee shops, homes and offices, the need for Quality of Service (QoS) support is increasing. Applications involving the heavy use of multimedia content, such as Video Conferencing, VoIP [4] and Video on Demand are starting to be used across WLAN's. Therefore requirements for bandwidth, error rate and delay are needed in order to provide a usable service [5].

Operating wireless devices in the popular 2.4 GHz ISM band provides some significant technical challenges. The wireless physical layer (PHY) is a much more hostile medium than wired environments. In addition to this the band suffers from overcrowding, with the available spectrum shared with cordless phones, bluetooth, and other proprietary wireless devices making use of the license free status. Water vapour can cause significant attenuation from absorption at 2.4 GHz. In outdoor or point to point WLAN deployments this can be challenging as rain, trees and even humans can have a detrimental effect on the received signal. In older buildings, thick stone walls are an undesirable barrier to WLAN signals. Other obstacles, such as large filling cabinets and K-Glass film coated windows can cause

attenuation in addition to multipath reflections. All of these factors can affect the throughput and delay of a system, which dictates the achievable QoS performance.

1.3 Motivation for Research and Objectives

This work aims to evaluate a number of techniques to provide a satisfactory QoS to the end user over WLAN networks. The work focuses on the operation of the Medium Access Control (MAC) layer in the popular IEEE 802.11 Wireless LAN protocol. Both MAC layer protocols; Distributed Coordination Function (DCF) and the new Enhanced Distributed Channel Access (EDCA) are investigated through computer simulation and experimental testbeds. This research will bring a greater understanding of the operation and functionality of the IEEE 802.11 protocol with real time protocols in a realistic working environment.

The motivation for providing QoS support is to provide an adequate service experience to the end user so that their expectations of that service are met [6]. For example a typical user may be happy to wait a few seconds for a web page to load. If however the same delay was applied to a voice conversation, the user would be dissatisfied. Providing service differentiation is considered essential to the growth of wireless networks in the next 10 years. Network usage is increasing faster than the available wireless bandwidth, so service degradation is likely to be a common occurrence. While newer physical layers featuring Multiple Input Multiple Output (MIMO) technology promise higher data rates, products are not common place due to the slow IEEE standardisation process. In this situation QoS mechanisms can provide greater network utilisation, while providing an adequate service experience with current physical layers. It is for this reason that current WLAN mechanisms, such as DCF and EDCA are investigated for their ability to provide QoS support over WLANs.

1.4 Structure of Thesis

The remainder of the thesis is structured as follows. In Chapter 2 the concept of wireless networking and the popular IEEE 802.11 Wireless LAN family of standards is introduced. The operation of each part of the protocol is discussed, followed by a description of some of the services used over a WLAN. MAC layer operation is detailed in Chapter 3, introducing the different access mechanisms and other relevant features. Chapter 4 introduces the concept of QoS. Provision of QoS on fixed networks is briefly discussed. This is followed by a detailed description of the metrics used to measure and quantify it. The section also contains a summary of related work in this area and some of the recent advances in experimental evaluation. In Chapter 5 the various simulation environments are discussed. OPNET Modeller™ is described in detail and the simulation results presented and discussed. Both DCF and EDCA mechanisms are simulated with various traffic patterns, including HTTP, FTP and VoIP. QoS is measured in terms of throughput and delay in addition to other traffic specific metrics such as Mean Opinion Score (MOS). Chapter 6 introduces the experimental testbed and contains the field testing results and discussions. The challenges of constructing reliable testbed architecture are presented. Using the chosen testbed, an analysis of the different MAC layer mechanisms under a variety of conditions is presented. Network performance in terms of delay, throughput and frame/packet loss rate is measured with varying traffic loads and types. The implications of these factors on the end user experience are discussed. Although practical field testing is much more complicated than simulation, a significant contribution to practical WLAN testing is presented. The thesis is concluded in Chapter 7 and an overview of areas of further research and the recommended modifications to the current protocol set based on the findings are given.

2 Wireless Networking Background

2.1 Introduction

This section aims to provide an overview of the IEEE 802.11 WLAN standard and its functionality. Some of the common services such as HTTP, FTP and VoIP which are used over WLAN networks are introduced. Their behaviour and traffic patterns are discussed.

The IEEE 802.11 protocol suite is a part of the 802 family, which provides the specifications for local area networks (LANs). The 802 family of protocols specify the operation and requirements of the data link layer and physical layer in the Open Standards Interconnection (OSI) model as shown in Figure 2.1.

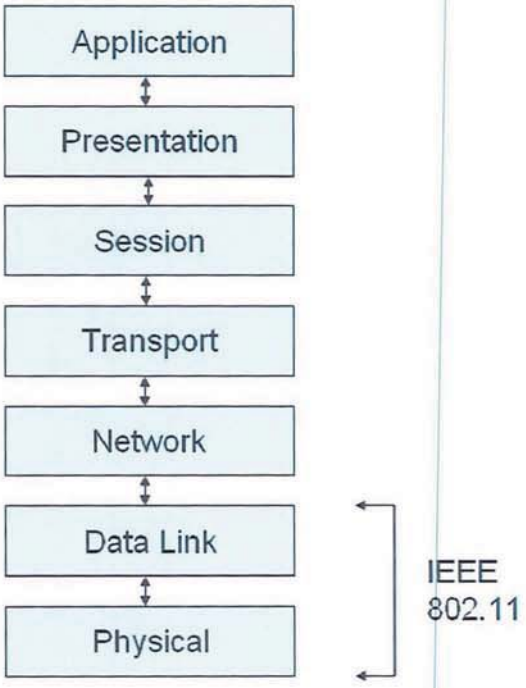

Figure 2.1 - IEEE 802.11 in the OSI Model

2.1.1 Data Link Layer

The data link layer is split into two parts, the upper Logical Link Control (LLC) and the lower Medium Access Control (MAC), which is what we are interested in. The LLC is responsible for error and flow control, however in most TCP/IP networks flow control is handled by TCP at the transport layer. The MAC layer functions include defining the procedure for multiple stations to access the medium, the sending/receiving of data and organisation of data into frames. From a casual view, the 802.11 MAC looks similar to the popular 802.3 Ethernet, in the way that wireless devices have a 48 bit MAC address, the same as wired stations.

The frame structures of both Ethernet and 802.11 are shown below:

Preamble	Destination Address	Source Address	Type	Data	CRC Checksum
8 bytes	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes

Table 2.1 – IEEE 802.3 Ethernet Frame Structure

Table 2.2 – IEEE 802.11 WLAN Frame Structure [7]

The 802.11 MAC is much more complex than Ethernet in order to deal with the shared radio medium. Due to the added complexity, the overheads are much greater. The 802.11 MAC is discussed in detail in Chapter 3.

2.1.2 Physical Layer

A number of different physical layers (PHY) have been defined in 802.11, as listed in Table 2.5. Two PHY types are commonly in use today, Direct Sequence Spread Spectrum (DSSS) and Orthogonal Frequency Division Multiplexing (OFDM).

In DSSS each bit in the original data is represented by a number of chips in the spread signal. The data stream is multiplied by a higher rate pseudorandom sequence known as a chipping code. The resulting stream is modulated and spread across the given frequency band.

OFDM is a type of multi-carrier transmission that divides the given frequency band into smaller sub carriers of a very narrow bandwidth. The data stream is split across the multiple parallel sub carriers for transmission and reconstituted at the receiver. OFDM features a high spectral efficiency and is robust against various sources of interference, making it the best performing PHY type.

DSSS is only used in 802.11b, which operates in the 2.4 GHz band, while OFDM in used in both 802.11g (2.4 GHz) and 802.11a (5 GHz). These physical layers are combined with various modulation schemes to allow a station to operate at different data transmission rates. The higher transmission rates utilise higher rate coding methods in order to fit more data into a given bandwidth channel, at the expense of making them more prone to errors. The two main techniques are based on Phase Shift Keying (PSK) and Quadrature Amplitude Modulation (QAM). PSK can be of the Binary type with two symbols (BPSK) or Quadrature with four symbols (QPSK), both of which can operate in differential mode (DBPSK and DQPSK). Complementary Code Keying (CCK) replaces the Barker Code used in original 802.11b. An overview of the modulation schemes and data transmission rates are shown in Table 2.3 and Table 2.4.

Table 2.3 - IEEE 802.11b Modulation Schemes [7]

Table 2.4 - IEEE 802.11a/g Modulation Schemes [7]

The 802.11a/g OFDM physical layers introduce forward error correction through the use of convolutional coding. This introduces redundancy to the data stream, therefore increasing the probability of a successful transmission. A detailed investigation of different modulation schemes and coding techniques is considered outside of the scope for this thesis.

2.2 Wireless Standards

The success of wireless LAN technology is due to the standardisation of 802.11 protocols by the Institution of Electronics and Electrical Engineers (IEEE). The role of such a standardisation body is to ensure that equipment manufacturers have a guideline to follow to allow interoperability between different devices. The Internet Engineering Task Force (IETF) has also made significant contributions to some of the more recent standards. Working group 11 within the 802 project is responsible for writing and maintaining the wireless LAN standard. This is referred to as IEEE 802.11 or more commonly, wireless LAN. Within the 802.11 group there are a number of smaller task groups, each responsible for a specific part or problem. Some of the important dates and standards from the group are listed in Table 2.5.

IEEE Standard	Date	Description
802.11	1997	Original standard specifies MAC layer, Frequency Hopping Spread Spectrum (FHSS) PHY and Direct Sequence Spread Spectrum (DSSS) PHY. Operates at 1 & 2 Mbps respectively.
802.11a	1999	High speed 54 Mbps Orthogonal Frequency Division Multiplexing (OFDM) PHY for the 5 GHz UN-II band.
802.11b	1999	High speed 11 Mbps DSSS PHY for the 2.4 GHz ISM band.
802.11g	2003	High speed 54 Mbps OFDM PHY for the 2.4 GHz ISM band. Most popular PHY standard in use as of 2008.
802.11e	2005	MAC Layer Quality of Service (QoS) enhancement.
802.11	2007	Roll Up of previous amendments (802.11a/b/g/e and others).

802.11n	2009	High rate 300 Mbps PHY based on OFDM Multiple Input Multiple Output (MIMO) technology with enhanced MAC.

Table 2.5 - IEEE 802.11 Standards

In 2007, the IEEE Standards Association reissued the 802.11 standard, rolling-up all of the amendments following the original issue in 1999.

2.3 Wireless Network Components

Wireless networks consist of three basic items; stations, access points and a backbone or distribution network. These can be arranged in a number of ways to produce distinct network topologies, discussed later in this section.

- **Stations (STA)**

Wireless stations are computing devices equipped with a WLAN interface. Usually these are battery operated and may consist of laptops, personal digital assistants (PDAs) and mobile phones. However, they are not restricted to mobile devices. It is quite common in residential environments for static desktop computers to be connected using wireless adaptors. Most consumer computing devices are equipped with an IEEE 802.11 network interface, with 802.11g being the most common at the time of writing. Legacy devices with no wireless interface or older devices with the 802.11b interface can be retrofitted with an additional card in the form of a PC Card or USB 2.0 adapter.

- **Access Points (AP)**

An access point (AP) is responsible for allowing wireless stations to access external networks. In effect the AP is responsible for bridging the wireless network to a wired network, most commonly with Ethernet. In some cases, discussed later, the AP may bridge multiple segments of a wireless network. Basic APs are equipped with an Ethernet interface and an 802.11 interface. More advanced models will have multiple Ethernet interfaces and multiple radios, allowing support of 802.11b/g and 802.11a simultaneously.

- **Distribution System / Backbone Network**

The distribution network is required to connect multiple WLANs together or more commonly to connect the AP to a larger network or LAN. This is generally referred to as the backbone network, or backhaul, which is responsible for interconnecting different LAN segments. The backbone network in a corporate environment may be Ethernet based, however in home networks, the backhaul is more commonly based on Data Over Cable Service Interface Specification (DOCSIS) or Digital Subscriber Line (DSL). While the backhaul carrier technology varies, Ethernet is usually emulated over the underlying protocol for compatibility.

2.4 WLAN Topologies

There are a number of different ways the components described in Section 2.3 can be arranged. These form distinct topologies, each of which has its advantages and disadvantages.

2.4.1 Independent Basic Service Set (IBSS)

The Independent Basic Service Set (IBSS) is also known as Ad Hoc mode and consists of two of more stations that are in direct communication range of each other. The stations transmit information directly to each other. This topology is popular when there is no infrastructure or backbone network present, for example in a conference room or computer gaming LAN party, where participants wish to exchange files or communicate with others nearby. In order to create an IBSS, the STA devices are required to set their Service Set Identifier (SSID) or network name identically. Due to the network being independent, communication with other LANs or the outside world is not possible. An example of a IBSS is shown in Figure 2.2.

Figure 2.2 - Independent Basic Service Set

2.4.2 Basic Service Set (BSS)

The Basic Service Set (BSS) consists of an access point and one or more stations. This is commonly referred to as an infrastructure network. All communication between stations is sent through the AP. If the destination of the data frame is within the same BSS, the originating station sends the frame to the AP, which then forwards it to the destination station. If the destination is outside of the current BSS, then it is forwarded onto the appropriate Ethernet interface. All stations in a BSS must remain within radio transmission range of the AP in order to communicate. When a station wishes to join a BSS, it is required to select the

SSID to that of the access point. This is usually broadcast periodically by the AP in a beacon frame. Following this the station is "associated" with the access point. BSS networks also include the ability to use power saving features and centralised polling functions as described in Chapter 3. A single BSS is suitable for WLAN coverage in a small office or home environment. In this research the simulation and testing is based on this type of topology because it is the most common type encountered in a home or office environment. An example of a BSS is shown in Figure 2.3.

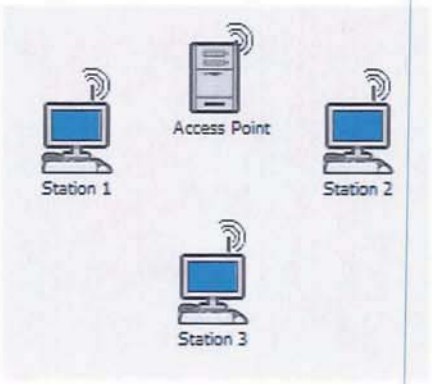

Figure 2.3 - Basic Service Set

2.4.3 Extended Service Set (ESS)

The Extended Service Set consists of a number of Basic Service Sets, linked together using a distribution system, or backbone network. The APs within an ESS all share the same SSID. This allows a single WLAN to cover an area of an arbitrary size, from an entire office to an entire campus. STAs are able to communicate with each other across individual BSS cells, as data frames are routed through the backbone to the destination BSS AP and finally to the destination STA. Extended Service Sets are commonplace in large offices and other large WLAN deployments. STAs are also able to roam in between the constituent BSS cells, but the transition is not seamless due to the disassociation and re-association process. An example of an ESS is shown in Figure 2.4.

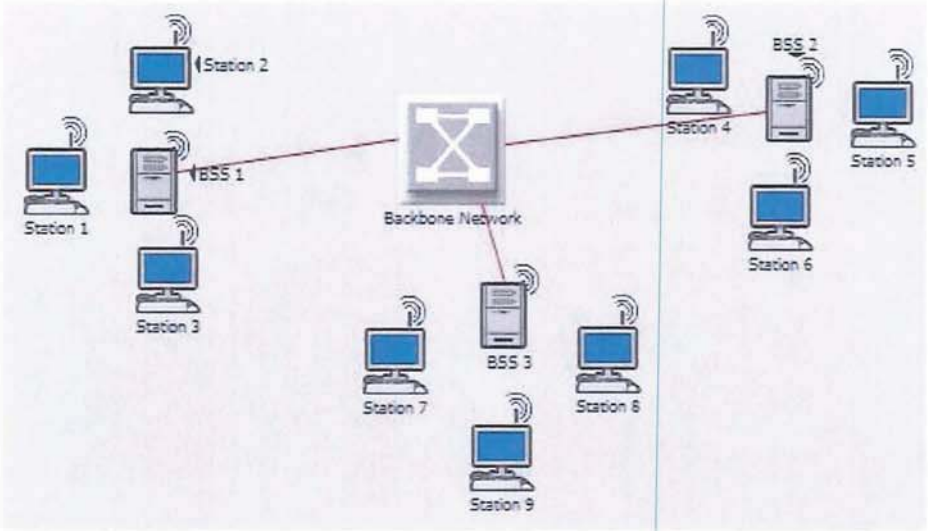

Figure 2.4 - Extended Service Set

2.5 Common Traffic Types

In this section some of the types of traffic that are simulated and tested over 802.11 wireless networks are introduced and discussed. All of these application layer protocols use either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) at the transport layer. TCP is defined in RFC 793 [8] and later amendments RFC 1323, 2018, 2581 and 2988 [9-12]. It can be regarded as a connection orientated service [13] where the client and server have a handshaking procedure before transmitting data packets. TCP provides a reliable ordered delivery of data packets through the use of mechanisms such as flow control and congestion control. Using a positive acknowledgement technique, packets can also be retransmitted if lost. UDP, defined in RFC 768 [14], is a connectionless service [15] which requires no handshaking and data packets are simply transmitted onto the network under this protocol. UDP does not provide any reliability guarantee mechanisms or ordered delivery of data, due to the absence of flow control and congestion control mechanisms. Its streamlined

nature makes it more suitable for delay critical services such as VoIP and Video, where the overhead of TCP would be a problem.

2.5.1 Hypertext Transfer Protocol (HTTP)

Hypertext transfer protocol (HTTP) defined in RFC 2616 [16] is one of the most popular protocols currently in use on the Internet. It is the backbone protocol of the World Wide Web (WWW) used for viewing and browsing internet websites. The WWW was designed by Sir Tim Berners-Lee in 1989 for the exchange of information between geographically separated research establishments. Commercial interests in the WWW lead to a new era of websites from e-commerce such as eBay and Amazon to social networking sites such as MySpace and Facebook. Currently it is estimated that there are over 100 million websites in operation on the WWW [17].

HTTP governs the exchange of data between a web browser and a web server. The underlying transport protocol is TCP. The traffic pattern can be considered as bursty. For example, when a user requests a certain web page and its elements, the contents are downloaded from a server to a client and rendered on the users screen. This is followed by a period of inactivity while the user views the page. This is followed up by a request for a different page and the process repeats. This stop-start nature of HTTP leads to it being regarded as a bursty service. During the page request, a TCP connection will be created between the client and the server. While the contents are transferred to the client, the connection will use all of the available bandwidth. The amount of data transferred will depend on the type of web page being viewed. For example, during image browsing there may be a large amount of data transferred per page, but the viewing/reading time may be short, while a news page containing only text would be the opposite.

HTTP can also be used for downloading of files as an alternative to File Transfer Protocol (FTP). The traffic pattern here changes from bursty to continuous, as the HTTP/TCP connection uses all the available bandwidth to download the file.

The HTTP service is not greatly affected by changes in throughput or delay. However, excessive reduction in throughput can significantly increase the time taken to fully load a webpage, but the service will still be functional. Changes in delay are relatively well tolerated, but excessive delay can increase the object request time, which would directly affect the time taken to fully load a page. This behaviour is regarded as *elastic*.

2.5.2 File Transfer Protocol (FTP)

File Transfer Protocol (FTP) defined in RFC 959 [18] allows a user to access a remote file system to upload and download data files. The user is first required to enter a username and password into their FTP client. The server will then authenticate the user before allowing the transfer of any files. Users can also log on anonymously if the server allows. The control data such as username and password, directory listings and other navigation information are sent over a TCP connection. The actual file data is sent/received over a separate TCP connection. The control channel will use a very small amount of bandwidth as the packets contain very little data. The data channel however will use up as much bandwidth as is available. For this reason FTP is regarded as a "greedy" protocol. The traffic pattern as such will be a continuous TCP stream that will use all available bandwidth for the period of the transfer. The duration of the active connection will depend on the bandwidth available and the size of the files(s) being transferred. Transferring large files over FTP has the effect of saturating the network and is an ideal test for calculating the throughput, discussed in Section 4.2.

The FTP service is not greatly affected by changes in throughput or delay. The passive nature of file transfers and lack of interactivity make changes in delay and throughput almost irrelevant. Excessive reduction in the throughput can increase the time taken for a file transfer, but the service will still be functional. FTP behaviour is referred to as *elastic* due to its flexible operating conditions.

2.5.3 Voice over Internet Protocol (VoIP)

Voice over Internet Protocol is a protocol designed for the transmission of voice over packet switched networks such as the Internet. There is a large migration occurring from the traditional circuit switched architecture to more cost effective packet switched IP solutions. VoIP has gained popularity in business and corporate circles for its lower running cost and implementation (in new buildings). Traditionally data networks were installed in addition to private branch exchange (PBX) lines for telephony services. VoIP allows the use of one heterogeneous network for both services, thus saving costs in management and deployment. The additional functionality of built in telephone directories and other data is an additional incentive to use VoIP systems. In the residential market the biggest motivator for VoIP has been the ability to make cheap rate telephone calls through a broadband connection. In the USA, where long distance calling is expensive, VoIP services such as Vonage have increased the consumer's choice in this competitive market. In other markets such as the UK & Europe, services such as Skype have received much attention for their price undercutting of traditional telephony operators. It must be noted that a number of successful VoIP services such as Skype use proprietary signalling and transmission methods.

In the UK, British Telecom (BT) is currently deploying its 21st Century Network that will see the majority of the circuit switched public service telephone network (PSTN) migrate to a complete IP network.

The VoIP protocol consists of two sections, signalling or control and data. The Session Initiation Protocol (SIP) defined in RFC 3261 [19], is responsible for the control and signalling information required in setting up, connecting and tearing down a VoIP call. Other protocols such as H.323 exist, but are not as widely adopted and supported as SIP. SIP is also used in other types of conversation such as video conferencing; however the discussion is limited to its use in primarily voice applications. The control and signal data in SIP is transported over a TCP connection. The actual voice data is transmitted using Real Time Protocol (RTP) over the UDP transport protocol. Voice data is usually compressed using a COmpressor/DECompressor (CODEC) in order to reduce the bandwidth requirements. Codecs are elaborated on in Section 4.5.

The VoIP service requirements are somewhat more stringent than other *elastic* protocols such as HTTP and FTP. Due to the real time nature of a voice conversation, excessive delay cannot be tolerated; otherwise the intelligibility of a conversation is affected. End to End delay below 150 ms can usually be tolerated [20]. Delays of up to 400 ms affect the Mean Opinion Score (MOS is discussed in Section 4.5), while values above this make conversation almost impossible. The throughput requirements of a VoIP call can vary significantly depending on the CODEC in use (for a list of CODECs please refer to Table 4.2). However, all CODECs require a minimum level of throughput, beyond which the packet loss will seriously affect the MOS. The strict requirements in terms of delay and throughput for the VoIP service must be met, in order for the network to provide an acceptable service. This behaviour is referred to as *in-elastic.*

2.5.4 Video

Video over Internet Protocol is one of the fastest growing services on the Internet at the moment. Traditionally video was transmitted using the television broadcasting network, originally analogue signals on the terrestrial VHF/UHF band. However this has rapidly been replaced by digital equivalents using terrestrial VHF/UHF, Satellite and Cable mediums. This move towards a digital broadcast world has opened up the possibility of transmitting television content through IP networks. There are other popular applications of Video over IP, such as CCTV and video conferencing. In this thesis the focus is on the use of video for the distribution of television/film content.

When video is viewed over the Internet there are two primary systems is use; streaming video and buffered video, both of which are explained in the following subsections.

2.5.4.1 Streaming Video

Streaming video involves a real time connection between the end user and broadcast server/other user. The video data (and accompanying audio stream) are usually sent using a UDP based protocol. Here excessive packet delay or packet loss can have an adverse effect on the end user QoS. Packet delay and loss will commonly result in picture stuttering and a loss of the live stream. This is a particular problem with video conferencing, where the live pictures (and associated audio streams) are essential to the functionality of the service. Without adequate QoS mechanisms in place, the performance of IP video conferencing systems can be affected drastically. It is for this reason many businesses still use multiple bonded ISDN lines in order to interconnect video conferencing systems. Streaming video is referred to as an in-elastic service, as it is not flexible to changes in network conditions.

2.5.4.2 Buffered Video

Buffered video is a more recent concept when video is sent in non real-time or near real-time. The video content is usually embedded in a webpage (commonly using Adobe Flash)., with common user controls such as play/pause and a position bar all appearing within the webpage. Video data and accompanying audio data are encapsulated in a TCP based protocol which is usually proprietary. Upon selecting a video, the embedded client will buffer data for a number of seconds, in order to allow uninterrupted playback of the video in case of packet loss. The added buffering gives a degree of protection against variation in network performance, where delay, bandwidth and packet loss are continually changing. Any losses would be recovered by TCPs retransmission function. However excessive packet loss would cause the video to pause, while the buffer is replenished. This method of TCP buffered video requires a greater bandwidth than an equivalent UDP based stream due to the overhead of having to acknowledge each packet. This overhead also increases the video delay, so true live streaming is not possible, with streams referred to as near real-time. Popular examples of buffered video are YouTube and television catch up services, such as BBC iPlayer, Channel 4oD and ITV on demand. Whilst these services are relatively well protected against variation in packet delay, they can be sensitive to changes in bandwidth. Standard definition streams can require up to 2 Mbps bandwidth; whilst High Definition content can require a much higher 10 Mbps. Frequent reduction of bandwidth would affect the continuity of the stream (as the embedded client waits for the buffer to replenish) and spoil the user experience, resulting in a poor perceived QoS. TCP buffered video is one of the fastest growing services in use on the Internet (due to the growth in TV catch up services) and is increasingly being used across WLANs.

2.6 Conclusions

This Chapter presented an overview of wireless LAN technology. The research work will be focussed on IEEE 802.11b and IEEE 802.11g physical layers, in combination with the original legacy IEEE 802.11 MAC and the enhanced IEEE 802.11e MAC, which are discussed in detail in Chapter 3. The Infrastructure Basic Service Set (IBSS) is the preferred topology for the simulation and field testing, as this is the most popular form of deployment in homes and offices. The popular services currently being used across wireless LAN's are introduced and discussed.

The Chapter concludes that most services can be categorised into either *elastic* or *in-elastic*. Time sensitive traffic such as VoIP and real time video streaming are considered *in-elastic*. This is due to their strict requirements in terms of delay and throughput. Non real time services such as HTTP and FTP are far less sensitive to variations in both delay and throughput and are considered flexible or *elastic*.

3 IEEE 802.11 MAC Layer

3.1 Introduction

This Chapter is introduced as an in depth explanation of the 802.11 MAC layer as specified by the standards document. The MAC layer is responsible for the framing of data, transmission of data over the radio interface and interaction with the higher protocol layers. IEEE 802.11 builds on the Ethernet standard by introducing a Carrier Sense Multiple Access (CSMA) method to control access to the radio transmission medium. Ethernet also uses a Collision Detection (CSMA/CD) mechanism to detect when two transmissions are sent simultaneously and consequently collide with each other. Due to the nature of the wireless medium, collisions cannot be detected (explained in Subsection 3.1.2), so a Collision Avoidance (CSMA/CA) mechanism is used. Some of the problems faced by the MAC layer are discussed, followed by a description of the access modes used in both legacy 802.11 and the new enhanced 802.11e. The access methods investigated in the research are given at the end of this chapter.

3.1.1 Hostile Physical Medium

With wired networks using copper and fibre mediums it is assumed that a data frame transmitted on the medium will arrive at its destination with little chance of error. Wireless radio links are considerably less reliable with Bit Error Rates (BER) in the region of 10^{-5} as oppose to near errorless for a fibre of similar transmission length and speed. Factors such as fading due to multipath interference as well as interference from other devices operating in the same frequency band contribute to the unreliability of the radio medium. In order to combat this problem the 802.11 MAC introduces a *positive acknowledgement* scheme where each data frame sent between two devices must be acknowledged on successful reception. If

the acknowledgement is not received within a specified time, the sender assumes the frame was lost and the retransmission process (described later in this chapter) begins. The acknowledgement (ACK) is only sent if the packet was received correctly. The process is shown in Figure 3.1.

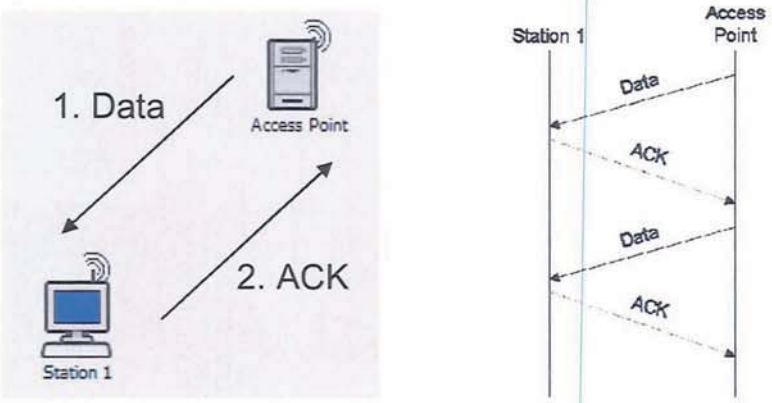

Figure 3.1 - Positive ACK Operation

The positive ACK mechanism is part of the Automatic Repeat Request (ARQ) mechanism. For each positive ACK not received, the transmitting station will attempt to resend the frame. Each frame transmitted contains a Sequence Number field. This is a 12 bit number that ranges from 1 to 4096. The main purpose of the sequence numbering is to identify frames that are being retransmitted by the sender. If a frame is successfully transmitted and a positive ACK received, the sequence number is incremented by one for the following frame. If the ACK is not received within the given *ACK Timeout*, the same sequence number remains static and the retransmission flag set to 1. If unsuccessful this process is repeated n times, where n is the retry limit. After the retry limit is reached, the frame is discarded. The value of the ACK Timeout is vendor specific and can sometimes be set by the end user. Usually the ACK Timeout value will be directly related to the expected coverage area of a wireless network. For example a large network would require a longer ACK Timeout or unnecessary retransmission will occur due to the propagation delay. In the case of smaller networks, a

shorter ACK timeout will enhance throughput as retransmissions can be sent quicker. Excessive retransmissions in either case can have a significant effect on throughput and delay of a network.

3.1.2 Hidden Node Problem

It is common in wireless networks that all the client stations will be out of direct radio range of each other. In the example in Figure 3.2 Station 1 is in range of the Access Point but outside of the range of Station 2. If both stations 1 & 2 attempt to transmit data at the same time, a collision will occur at the AP. This can lead to the *hidden node problem.*

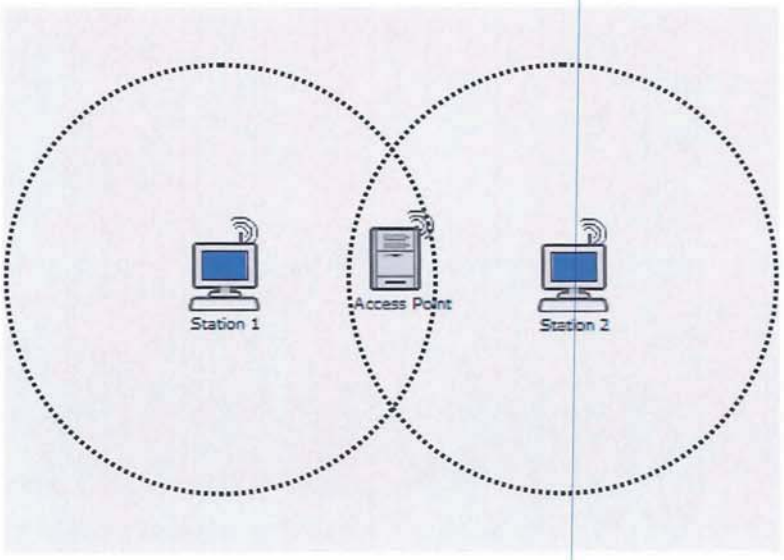

Figure 3.2 - Hidden Node Problem

In order to combat this problem, the standard introduces a Request to Send (RTS) and Clear to Send (CTS) mechanism. When station 1 has a frame to send, it attempts to reserve the radio medium by sending a special RTS frame. Any station within the range that hears the RTS is forbidden from transmitting any data. The AP then responds with a CTS frame, which indicates to station 1 that it can now commence transmission of the waiting data frame.

Station 2 in this case has heard the CTS frame from the AP to station 1, which also forbids any other stations from transmitting. The data frame, when received correctly by the AP is acknowledged with an ACK frame. Once this transaction is complete, other stations may transmit data by sending out a RTS frame.

Hidden nodes are a problem in networks where a large distance exists between stations. In this scenario the RTS/CTS mechanism can be considered helpful, however in other circumstances it is not because of its considerable overhead. In a typical home and office scenarios devices are within radio range of each other, therefore making the RTS/CTS exchange an unnecessary overhead. In the majority of devices on the market, the RTS/CTS feature is disabled by default for standard sized frames.

3.2 MAC Access Modes

The CSMA/CA access mechanism is provided by the basic access mechanism known as Distributed Coordination Function (DCF), which is described in detail later in this chapter. Contention-free access is provided by the Point Coordination Function (PCF) and Hybrid Coordination Function (HCF) from IEEE 802.11e. The IEEE 802.11e standard provides service differentiation and Quality of Service (QoS is discussed in Chapter 4). However before moving into the operation of each of these functions, some key concepts fundamental to the understanding of the access mechanisms should be introduced.

Carrier Sense / Network Allocation Vector (NAV)

In contention based access mechanisms the station wanting to transmit data must first sense the medium to check if it is free. If the medium is busy the station must wait until it is free

before attempting to transmit again. As mentioned previously, it is difficult to physically detect carriers on a radio based medium, so 802.11 introduces a Virtual Carrier Sense – Using the Network Allocation Vector (NAV). The NAV is a timer in microseconds that indicates how long a station expects to need the medium for completing its transmission and appropriate acknowledgement. The duration field is carried in most 802.11 frames, and due to the broadcast nature of the medium, all stations within range receive the frame and set their NAV to the duration value indicated. Frames sent from other stations with a NAV longer than the current value will update the NAV with the longer value. The NAV is then counted down and while it is not zero, the virtual carrier sense mechanism indicates that the medium is busy. Upon the NAV timer reaching zero, the virtual carrier sense indicates that the medium is now free and available for use. The NAV operation is shown in Figure 3.3.

Figure 3.3 - NAV Operation in Combination with the RTS/CTS Mechanism [21]

Interframe Spacing

There are a number of different interframe spaces which are introduced later, defined in the 802.11 standard. By using different sized interframe spaces, certain types of frames can be

transmitted before others as the shorter interframe spacing allows a station to access the medium before others have had a chance. The interframe spacing is defined per PHY in microseconds.

Short Interframe Space (SIFS)

SIFS is the shortest of the interframe spaces and is used for the highest priority frames, such as ACK and RTS/CTS exchanges. As soon as the medium is idle, the high priority frames can be transmitted after one SIFS. Other frames with a longer interframe space will encounter the medium as being busy and will defer transmission.

PCF Interframe Space (PIFS)

PIFS is the second shortest interframe space and is exclusively used for the start of a contention free period in the PCF access method (described in Subsection 3.2.2)

DCF Interframe Space (DIFS)

The DIFS spacing is used for contention based access using the DCF mechanism. Providing the medium is idle for a DIFS, a station may begin transmission of a data frame.

Arbitration Interframe Space (AIFS)

The AIFS does not feature in the original 802.11 MAC specification but is introduced in the 802.11e MAC layer amendment to provide Quality of Service (QoS). With the default DIFS spacing, all stations wait for the same amount of time before attempting transmission. The AIFS value is designed to be of varying lengths for different access categories or traffic types in order to provide service differentiation. As with the intention of different spacing, the categories with smaller AIFS value will seize control of the medium before those with longer

AIFS values. The relationship between interframe spaces is shown in Figure 3.4. This is discussed in further detail later in this chapter.

Figure 3.4 - Interframe Spacing [21]

3.2.1 Distributed Coordination Function (DCF)

The DCF access mechanism is mandatory in all 802.11 implementations. It can be used in both basic service set (BSS or Ad-Hoc) topology as well as infrastructure basic service set (BSS). DCF implements the basic CSMA/CA operation. The DCF operation can be described as the following sequence:

1. Station uses NAV to check if the medium is idle. If the NAV is non zero, then it is counted down in microseconds until zero.
2. The station waits for a DIFS period, once this has elapsed the station may contend for the medium.
3. The *random backoff* function then selects a value from the range [0, CW-1]. This range is referred to as the contention window and is measured in terms of *slots*. Initially the CW is equal to CW_{min}. The *slot time* is defined per PHY. The value chosen from the contention window range is set as the back off counter.
4. While the medium remains idle, the backoff counter is decremented. If the medium is detected as busy anytime during the backoff period, the countdown is paused and only

restarted when the medium is idle for a DIFS. During the backoff period it is possible that another station with a shorter CW may begin transmitting. In this case the station in backoff updates it NAV, and waits until this is 0 before resuming the backoff timer countdown.

5. If the backoff counter reaches zero and the medium is still idle, the station begins to transmit its data frame.
6. The station then awaits the positive acknowledgement (ACK) frame from the destination.
7. If the ACK is received OK, the contention window is reset to CW_{min} and the process described in 1 is repeated.
8. If the ACK is not received within the period of the ACK timeout (again defined per PHY), the backoff procedure is repeated except the contention window is doubled such that a value is chosen from the range

   [0, (2 x CW) – 1].
9. For each unsuccessful retransmission the CW size is doubled, until the upper bound of CW_{max} is reached. The retry counter is incremented by one each time a collision occurs.
10. This process of increasing the CW continues until the retry limit of usually 7 attempts, but can vary in different products and 802.11 implementations. Upon reaching the retry limit the frame is dropped and the CW reset to CW_{min}.

Figure 3.5 - DCF Operation [22]

The DCF process is shown in Figure 3.5 and Figure 3.6. The random exponential backoff process is shown in Figure 3.7, where CW_{min} is 7 and the CW_{max} is 255. The values of CW_{min} and CW_{max} are $(i^2 - 1)$ where i is an integer value. CW_{max} is always greater than CW_{min}.

Figure 3.6 - DCF Process with Multiple Stations [21]

Figure 3.7 - Random Exponential Backoff in DCF [21]

3.2.2 Point Coordination Function (PCF)

PCF is an optional access method defined in the 802.11 standard. The idea behind PCF is to provide a contention free access method for frames requiring a better than best effort service. As PCF was introduced as an optional standard, the majority of access points and client devices choose not to implement it. In order to operate in PCF mode a Point Coordinator (PC) and a PCF STA are required. The PC is responsible for the centralised control of access to the medium. For this reason PCF can only be used in BSS infrastructure networks with an access point (where the PC resides). The overhead and complexity of maintaining the point coordinator at the access point was also a contributing factor in its low popularity.

The PCF contention free service does not provide exclusive access to the medium 100% of the time; it is shared with the contention based access method DCF. When a PC wishes to start a contention free period (CFP), after waiting for a PIFS, it transmits a beacon containing the expected maximum duration of the CFP. This has the effect of reserving the medium ready for the CFP. The PC at the access point maintains a list of stations that require PCF service and sends a CF-Poll frame to the first station, prompting the station to respond after a SIFS with its data frame. As the PIFS will always be less than the DIFS, the PCF access method will always be able to access the medium before any DIFS stations. The PC can acknowledge the receipt of the frame using a CF-ACK frame, which can be combined with a CF-Poll request to the second station. The process is then repeated for the second station, and so on until the end of the contention free period (CFP). Normal DCF operation is then resumed. The operation of PCF is shown in Figure 3.8.

Figure 3.8 - PCF Operation [21]

As mentioned previously, PCF is very rarely implemented in hardware devices and its use in providing QoS has been superseded by the IEEE 802.11e amendment.

3.2.3 Hybrid Coordination Function (HCF)

The Hybrid Coordination Function is part of the latest IEEE 802.11e amendment published in 2005. The aim of the amendment is to provide an effective QoS framework that can support multiple services over the wireless medium. Due to the complexity of the solution, the standard took over 4 years to complete.

HCF provides two functions, a contention based Enhanced Distributed Channel Access (EDCA) and a contention free Hybrid Coordination Channel Access (HCCA). Over the last 2 years, support for 802.11e has grown in hardware devices. However manufacturers have chosen to support a subset of the 802.11e standard called Wireless Multi Media (WMM) supported by the Wi-Fi Alliance. WMM includes EDCA, but not HCCA, as this was still in draft at the time WMM was conceived. The research focuses on EDCA (described in the next section) due to the abundance of hardware support.

3.2.3.1 Enhanced Distributed Channel Access (EDCA)

The enhanced access method EDCA introduces four different access categories (AC) or traffic classes for service differentiation at the MAC layer. These four classes are mapped from the user priority value in the IEEE 802.1D standard. The mapping table from 802.1D to 802.11e EDCA categories is not linear. This is shown in Table 3.1.

Table 3.1 - User Priority Mapping [23]

Service differentiation is provided by the following methods.

Arbitration Interframe Space (AIFS)

This is similar to the DIFS used in DCF, except the AIFS can vary according to the access category. The lower priority categories are given longer AIFS and the higher priority categories shorter AIFS. The idea is that categories with shorter AIFS will be able to contend for the medium before others have a chance, this is shown in Figure 3.9.

Figure 3.9 - AIFS Illustration [23]

Variable Contention Window

By giving high priority traffic smaller contention windows (CW_{min} and CW_{max}), less time is spent in the back-off state, resulting in more frequent access to the medium. Lower priority categories are given larger contention windows, giving rise to less frequent access to the wireless medium. Also with smaller window sizes, the MAC delay can be reduced as the smaller counters are able to decrement quicker than categories with large counters.

Transmission Opportunity (TxOP)

This allows a station that has access to the medium to transmit a number of data units without having to contend for access to the medium. Legacy DCF only allows a single data frame and associated acknowledgement per contention event. EDCA allows multiple data frames and ACKs up to the TxOP limit, defined in microseconds. In effect this is a form of frame bursting. The TxOP limit is defined per traffic class.

Multiple AC queues can co-exist on a single station, contending with each other for the physical medium. If multiple queues exist, the backoff and contention are conducted internally, with the higher priority category gaining access to the real physical medium. This is referred to as virtual contention and is illustrated in Figure 3.10.

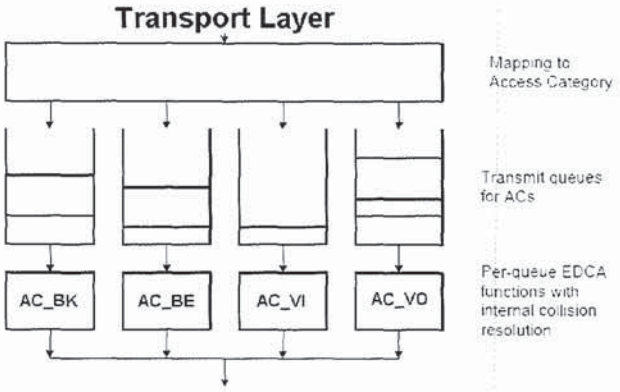

Figure 3.10 - EDCA Virtual Contention

Virtual collisions occur when two internal queues back off simultaneously and attempt to access the real medium at the same time. In this case the higher priority queue will win access to the real medium first. The losing queue, then doubles it CW as if a real collision had occurred, and starts the back off process again. Virtual collisions are discussed in further detail in [24].

As mentioned previously the four categories are differentiated by their contention window size and TxOP length. These values are derived from the CW_{min} value which is specified per PHY. The EDCA parameter set for both the OFDM and DSSS PHY are shown in Table 3.2 and Table 3.3.

Table 3.2- 802.11a/g OFDM EDCA Parameter Set [23]

Table 3.3- 802.11b DSSS EDCA Parameter Set [23]

"QoS aware" or 802.11e enabled stations are referred to as QSTAs and access points as QAPs. Similarly an 802.11e infrastructure basic service set is referred to as a QBSS. In a QBSS it is possible to have different EDCA parameter sets for the QAP and QSTA. Usually the QAP will distribute the parameter set to be used in its beacon frames to all associated QSTA's inside the QBSS.

As shown in Chapter 6, contention based access mechanisms can suffer from service degradation when overloaded. The 802.11e standard introduced Admission Control as a way to limit the amount of stations served with a given priority. Admission control in EDCA is possible through the use of a Traffic Specifications (TSPEC). When a station wishes to use

one of the "premium" access categories such as AC_VO or AC_VI (shown in Table 3.1), it sends its required TPSPEC to the QAP that it is associated to. The TSPEC is a list of the traffic flow requirements for that particular station in terms of packet size, data rate, delay etc. The QAP will then check the current channel conditions to see if the request can be satisfied. If admission is possible, the QAP will allocate the resources internally and send an ADDTS (Add TSPEC) frame to the QSTA. In the case that resources are not available, the TSPEC is denied and the QSTA is not permitted to use the access category it applied for and must use one of the lower AC_BE or AC_BK categories. Usually admission control will only be used on the premium access categories such as AC_VI and AC_VO; however it can also be used on the lower AC_BE and AC_BK categories.

The use of admission control is optional and the exact implementation in hardware devices may vary from vendor to vendor. From experience with hardware from Proxim, Netgear and Linksys, this is not implemented.

3.2.3.2 HCF Controlled Channel Access (HCCA)

The HCCA mechanism employs a Hybrid Coordinator (HC) which resides within a QAP, similar to the PC in PCF. The basic operation is centred on granting of Transmission Opportunities (TxOPs) to stations within the QBSS using a polling process, which is known as a polled TxOP as oppose to the EDCA TxOP mentioned earlier.

With HCCA, the HC has the ability to allocate TxOPs to itself and other QSTA at any point in the cycle and is not limited to contention free periods (CFP). Optionally, the HC can introduce a specific CFP, but normally the HCCA mechanism operates on top of the standard EDCA. Operation of HCCA is similar to that of PCF, where stations are polled for a TxOP. If

a QSTA has data to send, it continues to transmit until the TxOP had expired or there is no more data to send. In the case of no data waiting, the QSTA responds with a QoS Null frame. The QoS Null frame is also used to prematurely end the TxOP, returning unused resources back to the HC and increasing medium utilisation. Higher priority stations can be granted longer TxOPs, while lower priority stations can be granted shorter TxOPs.

Admission control is also possible using HCCA in combination with TSPEC, but the 802.11e standard does not go into a specific detail and the implementation of such a mechanism is left to device vendors.

3.3 Block ACK

The Block Acknowledgement feature was designed to improve the channel efficiency of the existing positive ACK system. When using Block ACK, several acknowledgement frames can be aggregated into a single Block ACK frame. There are two types of Block ACK defined, immediate and delayed Block ACK.

In order to use Block ACK, the originating station sends out an ADDBA request. If the destination QSTA supports Block ACK, it responds with an ADDBA response. Upon receipt of this response the QSTA may begin transmitting its QoS Data frames, once the data sequence is complete; the originator requests a Block ACK Request. In the immediate system, the data series is acknowledged in the next frame, while the delayed version the receiver has the option of delaying the Block acknowledgement. This is illustrated in Figure 3.11.

Figure 3.11 - Immediate Block ACK Operation [23]

Upon completion of a Block ACK exchange, the feature is turned off or "torn down" by the sending of a DELBA frame. Normal positive ACK operation is then resumed. The frame exchange is shown in Figure 3.12.

Block ACK has the potential for considerably increasing the efficiency of the MAC in good signal environments. In poorer or more hostile environments, the overhead of retransmitting large sequences of frames may lead to a significant reduction in overhead on system throughput.

Figure 3.12 - Block ACK Frame Sequence [23]

3.4 No ACK

The No ACK policy removes the requirement for the positive acknowledgement at the MAC layer. This obviously reduces the reliability of frame transmission as erroneous frames will not be retransmitted. The advantage of using No ACK is that the transactional delay and jitter of the transmission sequence is reduced, as the receiving station is not required to wait for a SIFS and send an ACK. This can be beneficial to delay sensitive traffic.

When the No ACK policy is used, it is advised that a high level recovery mechanism, such as TCP be used to address the issue of errors at the MAC layer.

3.5 Frame Check Sequence

In order to check the integrity of frames received at the MAC layer the 802.11 standard implements a frame check sequence (FCS). This forms the last part of a MAC frame and is 32 bits long. The FCS implements a form of Cyclic Redundancy Check (CRC), details of which can be found in the frame formats section of the 802.11 standard. The FCS is calculated by the sender on the header and data parts of the frame and appended as a 32 bit value to the end of each frame. The receiver also calculates the FCS from the header and data fields and compares it to the value appended to the frame. If the FCS is the same, the frame can be regarded as valid and a positive ACK is sent. If the FCS values differ, then the received frame is considered invalid as the header or data has been corrupted. In this case the frame is not acknowledged, it will be discarded without being passed to the higher layer.

3.6 Conclusions

In this chapter the operation of the 802.11 MAC layer access protocols DCF, PCF, EDCA and HCCA are described. Although the IEEE standards specify operations rules and parameters for all four schemes, only DCF and more recently EDCA have been implemented by equipment vendors in hardware devices at the time of writing. Simulation tools such as NS-2 [25] and OPNET Modeller™ [26] have implemented many of the features of these schemes but full support for the features offered by both legacy 802.11 and the enhanced 802.11e is a long way away. Open source initiatives such as the Multiband Atheros Driver for WiFi (MADWiFi) [27] has given researchers invaluable access to hardware based testing platforms for their work with EDCA. Support for the Windows based platforms is restricted to DCF and partial EDCA functionality through vendor specific utilities and supplement programs.

The research is concentrated on the DCF and EDCA access mechanisms that are prevalent in current simulation tools and hardware devices. Future work may address the functionality of HCCA and other emerging access protocols.

4 Quality of Service (QoS)

4.1 Introduction

Quality of Service (QoS) can be defined as the ability to provide selective treatment to different services or users in the most efficient way. It is a collective term for the methods, standards and protocols designed to prioritise different traffic streams in a packet switched network.

Internet Protocol (IP) is now the standard for the transmission of data services, such as HTTP, FTP and real time services such as VoIP and Video Streaming. The majority of IP networks function with a best effort approach. The large bandwidth available in these networks allows real time services such as VoIP to co-exist with HTTP and FTP without any type of special treatment. If there are problems, it is easier to simply increase the bandwidth of the link. In wireless networks the radio resources are usually limited, so the option of increasing the bandwidth is not available. Resources have to be managed to ensure that network users have access to an acceptable service.

The way in which QoS is implemented and at what layer in the protocol stack varies by the network type and topology. For example a network may only provide QoS on certain hops in an Internet Protocol (IP) network, but not for an end to end transfer from source to destination.

Within the typical home/office environment, it is now common to have a wireless router acting as the last hop before the client device. In this research work the focus is on evaluating QoS on the "wireless last hop" in a wireless IP network. Referring back to the introduction in

Chapter 2, the primarily optical and copper based backbone network features low error rates compared to their wireless counterparts. Wireless networks suffer from a hostile radio channel which makes providing QoS a challenge.

In this chapter an overview of the types of QoS mechanisms used in a fixed network are presented. The discussion moves focus to a number of QoS parameters or metrics and their relevance to commonly used services.

QoS methods on wired networks are considered a mature technology. Most large LANs and backbone networks will implement some form of QoS in order to differentiate and protect different types of traffic from each other. This is approached in two different ways, integrated services and differentiated services commonly better known as *IntServ* and *DiffServ* respectively.

IntServ (defined in RFC 1633 [28]) is a method of providing guaranteed QoS on a multihop network. Network resources can be reserved for certain flows. Individual flows have to request a certain level of QoS. The routers can then admit the flow or reject it if there are not enough resources; this is a form of *call admission.* HCCA Polling in 802.11e works on a similar principle of call admission as does the optional admission control in EDCA. The system requires that each router in the path keeps a state table of each active flow. While this may work on a small scale, the resources required to maintain such information along the entire route make it unsuitable for larger networks.

The DiffServ architecture (defined in RFC 2475 [29]) is somewhat different to that of IntServ in that service differentiation is provided on a group or class basis as opposed to a per flow method. Traffic is categorised into different classes through the Differentiated Services Code

Point (DSCP) field in the IP header. Routers can use this class information to manage groups of traffic flows, providing preferential treatment for higher priority classes. As class control is provided on a per hop, per router basis, it is much simpler to implement than IntServ. The operation of DiffServ can be compared to that of EDCA in 802.11e.

One of the major drawbacks of the DiffServ architecture is that once a packet travels outside of its DiffServ domain (usually a company's LAN/WAN, or an ISP's backbone) the information on its class type is lost as routers that don't support the tagging may simply rewrite the value as zero. The destination network cannot recover the original priority value, and is usually treated as Best Effort.

Both systems discussed, IntServ and DiffServ, are generally only applied to the networks over which the owner has control. In a network as large as the Internet, this becomes difficult as coordination is required between edge and backbone network operators. Corporations and other large network operators may be able to negotiate certain levels of QoS through the use of Service Level Agreements (SLA's). Here the network operator specifies performance guarantees for the service provided for a certain percentage of the active time. This is similar to some of the *Soft QoS* techniques mentioned in Subsection 4.10. Small businesses and end users don't have this facility for a strict SLA and are at the mercy of the service provided by their chosen Internet Service Provider.

The QoS mechanisms on wired networks may be mature but the coordination and implementation aspects require more work on a global scale. However, further investigation into this topic is outside of the scope of this thesis. The reader is referred to [30] for more information.

4.2 Throughput

Throughput is one of the most common metrics used for judging performance in a network. It is the amount of useful data received per second, usually quoted in kbps (kilobits per second) or Mbps (megabits per second). In its simplest form it can be defined as the amount of data transferred divided by the time taken to transfer it. This definition is an application layer measurement and is sometimes referred to as the goodput. For example if we have a file of size L that takes a time t seconds to download, the throughput $\eta_{application}$ can be defined as:

$$\eta_{application} = \frac{L}{t} \tag{4.1}$$

For example, a 7MB ZIP file takes 4 seconds to download; the throughput is calculated as:

$$\frac{7 \times 1024^2 \times 8}{4} = 14.68 \; Mbps$$

Note that the conversion in the above calculation from bytes to bits as 1MB is equal to 1048576 bytes, giving an overall throughput of 14.68 Mbps in the example.

The throughput can be calculated at different layers in the protocol stack (refer to Figure 2.1). In the majority of the simulations and fields tests, the application layer throughput is referred to, which includes any reductions due to protocol overheads. For example, the maximum data transmission rate of an 802.11g wireless LAN is 54 Mbps, but the maximum achievable application layer throughput is in the region of 25 Mbps. The largest overheads are from the ARQ mechanism, MAC layer timing and contention for the wireless medium.

The Iperf utility [31] that is used in some of the tests measures the transport layer throughput. The reported value however is the throughput of the data payload, so is effectively the application layer data throughput. This is true for both TCP and UDP payloads and the specifics are discussed further in Subsection 6.2.3.2

Physical layer conditions can directly affect the throughput capability of a wireless network. One of the main indicators of the quality of the radio link is Signal to Noise Ratio (SNR). This is a ratio of the signal power against the noise power in a given channel. In order for a device to transmit at higher speeds, a higher SNR is required. This is investigated in Sections 6.4 and 6.6.

Throughput is the most important metric in measuring the performance of a network. Every service, in one way or another, is affected by changes in the throughput. Services such as FTP and HTTP are flexible to changes in throughput, but can be crippled if the throughput is excessively low. For example, referring to Equation 4.1, a halving of the throughput can result in the time taken for a file transfer to double. VoIP requires a minimum throughput to provide an acceptable service. If this is not adhered to, the resulting packet loss can significantly affect the MOS.

4.3 Delay

Delay is the time taken for a data packet to cross a network from sender to receiver. The total delay has a number of components described below.

Processing Delay

The processing delay, $\tau_{processing}$, is the time taken to read a frame or packet's header information and direct it to the correct interface or queue. It also includes other checks that may have to be performed on the packet/frame such as the Frame Check Sequence (FCS is discussed in Section 3.5). Processing delay for the transport layer and below is usually small and lower than a millisecond.

Queuing Delay

The multiple access nature of radio medium means that frames can only be sent one at a time, resulting in frames being placed in a queue. In DCF (discussed in Subsection 3.2.1) there is only a single queue. EDCA (discussed in Subsection 3.2.3.1) features four queues for prioritisation. Depending on the network load, the queuing delay, $\tau_{qucuing}$, can vary significantly from zero to a number of milliseconds.

Transmission Delay

This is the time required to transmit the frame onto the physical link. A frame of length L bits, and a data transmission rate of R bits/second, the transmission delay $\tau_{transmission}$ can be defined as:

$$\tau_{transmission} = \frac{L}{R} \tag{4.2}$$

For example, take an 802.11 frame of length 1572 bytes and a data transmission rate of 54 Mbps, the transmission delay is:

$$\frac{1572 \times 8}{54 \times 10^6} = 0.233\ ms$$

This is a relatively small amount, but it can increase to 2.096 ms when the data frame is transmitted at 6 Mbps; the lowest supported 802.11g OFDM rate (refer to Table 2.4).

$$\frac{1572 \times 8}{6 \times 10^6} = 2.096\ ms$$

Propagation Delay

After the data has been transmitted onto the physical link, it will propagate to the destination.

The distance between the transmitter and receiver can be d meters. The propagation speed is s meters/second. The propagation delay $\tau_{propagation}$ can be defined as:

$$\tau_{propagation} = \frac{d}{s} \tag{4.3}$$

With wireless links it is assumed that the propagation speed in air is equal to that of light at 3×10^8 m/s. For example, in a typical wireless link of 50m; the propagation delay is calculated to be:

$$\frac{50}{3\times10^8} = 0.167\ \mu s$$

In the deployment of a long distance 802.11 link, the delay involved can be significantly greater. For a 50km link, the propagation delay will be:

$$\frac{50\times10^3}{3\times10^8} = 167\ \mu s$$

The increase is proportional to the distance of the link. However the 802.11 MAC layer was not designed to operate over such large distances and problems can occur with the ACK Timeout being too short. This is discussed in Subsection 3.1.1.

The total delay or end to end delay is the cumulative total of all of the components mentioned:

$$\tau_{total} = \tau_{processing} + \tau_{queuing} + \tau_{transmission} + \tau_{propagation} \tag{4.4}$$

The effects of each of the different delay components can be compounded in multi-hop wired/wireless networks. However, in this research the focus is on the single hop wireless last link, in which queuing, transmission and to some extent processing delay are the only significant components.

Delay is one of the most important metrics when referring to the performance of real time services such as VoIP and Video Streaming. As discussed in Subsection 2.5.3, VoIP requires an end to end delay of less than 150 ms to function acceptably [20]. Services such as HTTP and FTP are unaffected by changes in delay, but HTTP interactivity can adversely effected if the delay increases excessively in the region of seconds.

4.4 Jitter

Jitter can be defined as the variation in packet delay, discussed in Section 4.3. Due to the packet switched network, data packets generated a constant rate may not arrive at the destination at the same rate. As discussed, the end to end delay has a number of components and their effects can be compounded with each hop. In this scenario; a last hop wireless link with static wireless clients, the largest contributor to the delay is the queuing delay. For example, a VoIP call using the G.711 codec with a data rate of 64 kbps, packets with a payload of 160 bytes are generated approximately every 20 milliseconds. Depending on the other traffic present on the network, the packets will be queued, which will mean that they do not arrive constantly at an interval of 20 milliseconds. For example, if the first packet transmitted from the voice source to the wireless destination arrives at an AP with no background traffic it will be transmitted to the destination almost straight away with minimal queuing delay. The second packet generated 20 ms after the first then arrives at the AP which now has a large queue from other background traffic. Due to the queuing delay introduced from the extra traffic load, the second packet will now arrive at the wireless destination more than 20 ms after the first packet was received. This variation is referred to as the packet (at the network layer) or frame jitter (MAC layer).

Jitter is a common occurrence in packet switched networks; however the extent of its effect is directly related to the number of hops in the packets journey. As discussed earlier, the major factor in jitter is the queuing delay which is directly related to the background traffic present on a link.

The occurrence of jitter is usually combated by the use of sequence numbers in higher layer protocols, such as RTP, in addition to time stamping each individual packet. Using this time stamp, a packet that arrives outside of the jitter threshold can be discarded. Any error correction or concealment is then left to the higher layer protocol. Time sensitive services such as VoIP and Video Streaming are sensitive to jitter, which can lead to interruptions in the service provided, should excessive jitter occur.

4.5 Mean Opinion Score (MOS)

The mean opinion score (MOS) is a numerical scoring system to evaluate the perceived quality of a call made using VoIP. The MOS is expressed as a range of numbers from 1 to 5, where a score of 5 is considered the best quality possible, and 1 the poorest quality. This is shown in Table 4.1.

Table 4.1 - Interpretation of MOS Scores [32]

The MOS can be affected by a number of different factors. One of the major influences on the value will be the codec (compressor/decompressor) used to compress the vocal content. The idea of compression is to reduce the bandwidth required for transmission of the content. The best codec will provide the highest quality with the maximum compression. Achieving this perfect balance is difficult, Table 4.2 below shows some of the common codec's currently used in VoIP and their achievable MOS.

Table 4.2 - Codec MOS Comparison [33]

The compression methods are expressed as follows:

Type	Name
PCM	Pulse Code Modulation
ADPCM	Adaptive Differential Pulse Code Modulation
LD-CELP	Low-Delay Code Excited Linear Prediction
CS-ACLEP	Conjugate-Structure Algebraic-Code-Excited Linear-Prediction
ACELP	Algebraic Code Excited Linear Prediction

Table 4.3 - Codec Compression Methods

The compression delay is also another factor that can affect the MOS. The more complex codec's that allow for greater compression with little loss in quality often require greater processing loads on both ends. This processing capability is not always available, especially in the case of low powered embedded devices such as VoIP phones.

The majority of VoIP deployments will aim for a MOS value of 3 to 4. In this research this range is chosen as an acceptable level of service. The G.711 codec is the most popular standard in Integrated Services Digital Network (ISDN) and Digital Private Branch Exchange (dPBX). It is for these reasons that in the majority of the simulations G.711 is used as a preferred codec due to its high quality and popularity.

4.6 Peak Signal to Noise Ratio (PSNR)

The peak signal to noise ratio (PSNR) is a ratio between the maximum possible power of a signal and the power of corrupting noise that affects its representation. It is used extensively in image and video compression for measuring the quality of an image or video stream. In this

research the focus is on the use of the PSNR as a QoS metric for video streaming. Higher PSNR values relate to a higher quality video. A video that is transmitted perfectly with no compression or losses will have an infinite PSNR. In a compressed video using a modern codec such as H.264 [34], PSNR values of 30 to 50 dB are expected. For example in the testing (see Section 6.7) the achieved PSNR values are compared to the infinite PSNR possible when there are no losses.

Other measures such as Perceptual Evaluation of Video Quality (PEVQ) [35] and negative sobel (NEGSOB) have been proposed. The PEVQ provides a perceptual grading system similar to that of the MOS (Section 4.5). NEGSOB uses edge detection to identify video artefacts. A discussion of these technique is outside the scope of this thesis and the reader is referred to further information in [35] and [36].

The diagram below shows a typical video frame that has suffered a loss, resulting in the classic "blocking effect", in which artefacts can be seen in the right hand edge and right lower quadrant. These artefacts have a direct effect on QoS measures such as PSNR and NEGSOB.

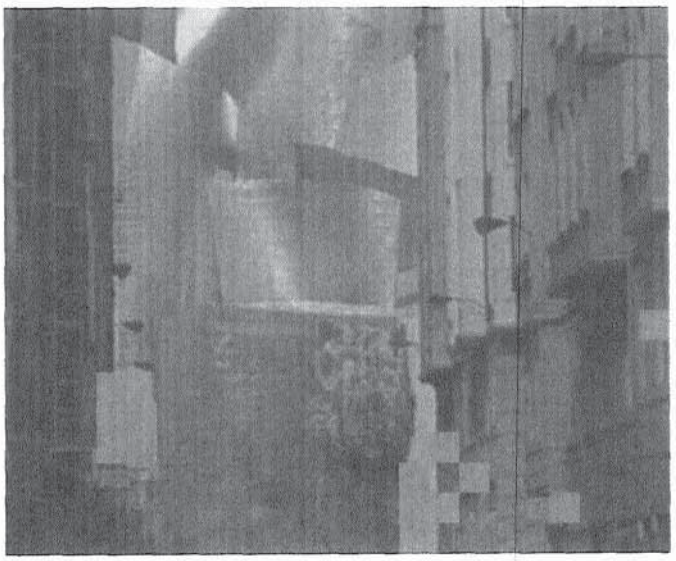

Figure 4.1 - Typical Video frame with Block Artefacts

4.7 Differential Services Code Point and 802.11e

The Differential Services Code Point (DSCP) value [37], mentioned previously, is sometimes referred to as the Type of Service (TOS) field. This is the one of the most common ways of categorising packets for 802.11e. This field consists of an 8 bit value which is located within the Internet Protocol header; this is illustrated in Figure 4.2 from a Wireshark capture of a single packet. As most applications do not have control over any layers below the Network, there is a need for a mechanism to transfer the required priority of a packet to the lower layers. The majority of implementations of 802.11e or Wireless Multi Media (WMM) will use this value to map packets onto a MAC layer priority class.

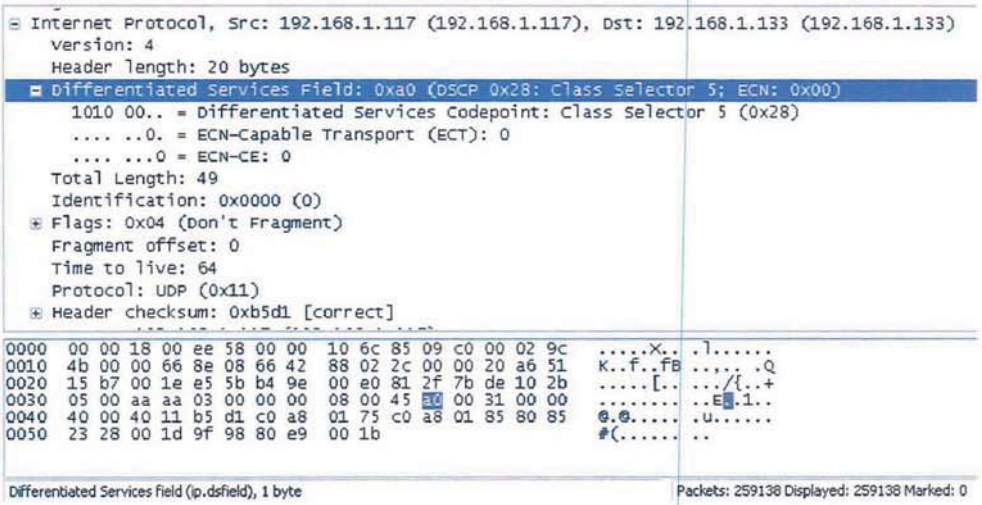

Figure 4.2 - DSCP Field in IP Header

The problem arising here is that there is no standardised way of dealing with this mapping procedure from DSCP to the 802.11e EDCA access categories. In a number of the trial testbed implementations there was a significant difference between the ways systems dictated the mapping between DSCP and 802.11e EDCA access category. The mapping for the MADWiFI testbed is described in Chapter 6 and shown in detail in Table 6.2, located in Chapter 6. A specific DSCP value in one vendor's system will more than likely map onto a

different access category in another's implementation. This makes application design for QoS difficult as the DSCP value is required to be set on a per application per system basis which significantly reduces portability.

Wireless Device / OS	DSCP Value (decimal)	EDCA Access Category
Proxim AP4000 Vx Works	32	AC_BE (Best Effort)
MADWiFi 0.94 Linux	32	AC_BK (Background)
DD-WRT v24 Linux	32	AC_BE (Best Effort)
Tomato Firmware v1.19	32	AC_BK (Background)

Table 4.4 - DSCP Mapping Variations

Table 4.4 shows the different ways in which a specific DSCP value can be regarded by different wireless EDCA implementations. In the Proxim based testbed there was some control over the DSCP to EDCA mapping, however during testing an appropriate solution to allow us to utilise all of the EDCA access categories was not found. The Proxim mapping is shown in Figure 4.3.

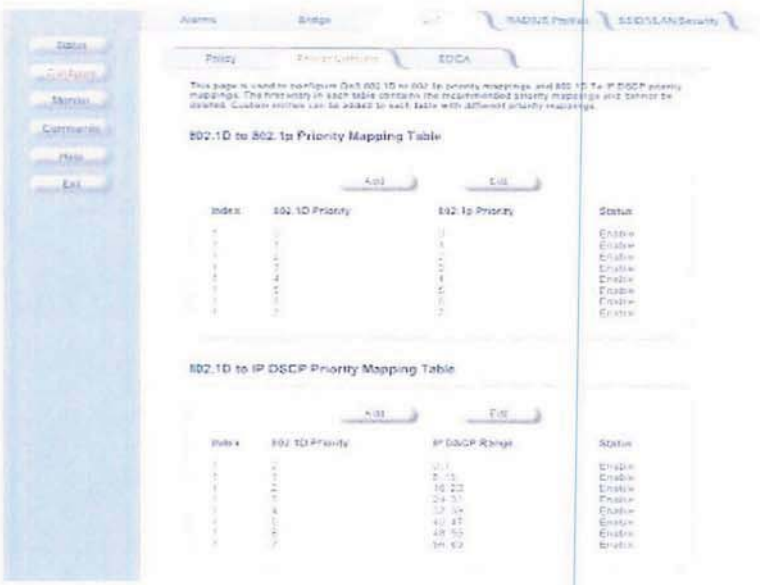

Figure 4.3 - Proxim AP4000 DSCP Mapping

This lead to the use of the MADWiFi based testbed described in Subsection 6.2.3. Although hard coded into the driver, the mapping was based on specific single DSCP values which corresponded to the EDCA access categories as opposed to a range of values with the Proxim equipment (shown in Figure 4.3).

4.8 Related Work

In this Section some of the related work in the field of Quality of Service over wireless networks is introduced. Since the conception of the original wireless LAN standard in 1999 there has been a significant amount of research into the performance and optimisation of the standardised protocols. This section aims to deliver an overview of the work completed in both legacy and enhanced protocols with a particular focus on experimental work with the EDCA protocol. The review is organised such that legacy DCF is discussed first, followed by other suggested ideas for providing QoS using modified DCF. The focus then moves on to work relating to the standardised EDCA protocol, and some alternative suggested enhancements. The Section is concluded with a review of the latest work being conducted using real hardware testbeds.

4.9 Related Work in Legacy Protocols

It is generally accepted that the initial work in the analysis of the IEEE 802.11 MAC layer was conducted by Bianchi in [38] and later in [39]. Both contributions use a Markov chain model to calculate the saturation throughput using the DCF mechanism. Bianchi later refined his original model based on Bidirectional Markov chains [38], with a simpler model based on conditional probability arguments. The original Bidirectional Markov model was complex to solve with its many variables. Kuppa in [40] proposes splitting the Bidirectional chain into two one dimensional chains, which simply the analysis and reduce the number of variables. Bianchi's model in [38, 39] does not account for the retry limit, so overestimates the saturation throughput. This shortcoming was addressed by Wu in [41] which takes into account the retry limit. Both studies accounted for a perfect wireless channel, which is not representative of a real world scenario. Cali in [42] devises a p-persistent variant of DCF,

assuming constant and independent per-slot transmission probability. Chatzimisios introduced the modelling of transmission errors in [43]. A packet drop rate was calculated, based on the packet length, header length and bit error rate of the transmission speed. Chatzimisios later expands the work in [44] to take into account both transmission errors and retry limits. The mathematical model proposed in [44] is validated using OPNET Modeller and shown to be accurate. In [45], Zheng expands on the imperfect channel model to account for varying traffic loads and queue lengths. Fu-Yi further enhances the mathematical model by accounting for the hidden node problem (discussed in Subsection 3.1.2) in [46]. Oliveira introduces an analysis in [47] that incorporates differing frame lengths, a common occurrence in a real world wireless network. Given the complexity in modelling a wireless channel mathematically, it is felt that accounting for all these different parameters in analytical approaches is vital to making the models more applicable to real world scenarios. While the DCF mechanism can be considered a legacy protocol, work still continues on modelling. Jo-Hoon in [48] models the performance of DCF with the Automatic Rate Fallback (ARF) mechanism over a lossy channel. Frame losses in the wireless network with various transmission rates are investigated in Section 6.6 of this Thesis.

Raptis in [49] produces some noteworthy results on delay analysis with the DCF mechanism. In this thesis, both the delay distribution and retransmission distribution for DCF and EDCA are investigated in Sections 6.4 and 6.5. In later work [50], Raptis furthers the analysis of DCF by evaluating the performance using common metrics such as throughput, average delay, jitter and packet loss. Raptis proposes a bursting mechanism at the AP to increase the performance of streams using legacy DCF. Although the work by Raptis in [49, 50] is based on mathematical models validated through simulation, their accuracy could be further enhanced by incorporating empirical testing results, as demonstrated in Chapter 6 of this Thesis.

4.10 Related Work in Enhanced Protocols

Soon after the release of the original DCF specification it was established analytically that the DCF mechanism was unable to support multiple services simultaneously [51]. With the popularity of real time applications such as VoIP and Video Streaming over WiFi, there was a surge in solutions being suggested to this problem of providing QoS over DCF. In [52] the authors suggest the Blackburst scheme, which involves the use of so called "Blackbursts" (BB) where the station contends for the medium. The lengths of the bursts are proportional to the time that the nodes have been waiting for the channel to become idle [52]. After the initial settling period, stations in the Blackburst BSS become synchronised, after which real time stations transmit using smaller Blackbursts than lower priority stations.

At the same time there was an interesting approach to providing *"soft QoS "* [53] where the ranges of acceptable values are specified, in terms of service requirements, as opposed to hard limits. The non real-time services discussed in this thesis, such as FTP, HTTP (elastic) do not require strict QoS requirements. The VoIP application (non-elastic) requires far tighter bounds for QoS in terms of delay and minimum throughput, but is still able to function over a range of values, up to acceptable limits, i.e., 150 ms for delay [20]. The main deficiency in providing a soft QoS service is the management requirements to oversee the operation. Similar to other centrally controlled schemes, it would need to be implemented at the network edge, i.e. on the access point of a BSS. Similar to PCF and HCCA, the added complexity of implementation is not favoured by hardware manufacturers and therefore remains a research concept. Ideas on how to provide service differentiation and prioritisation in wireless networks were floated through the research community. Deng [51] suggested establishing differentiation through changes in the backoff window, while Aad suggested in [54] that

differentiation could be achieved through modifications to the interframe spacing (discussed in Section 3.2). Veres [55] took the idea of using the windows size a step further by introducing variations in the minimum and maximum windows size, what is now known as CW_{min} and CW_{max}. Simultaneously, the IEEE 802.11e working group were working on standardising an approach to providing service differentiation and prioritisation over DCF. The main protocol being discussed at the time was Enhanced DCF better known as EDCF. EDCF was later renamed to EDCA, both terms are used interchangeably in this review.

Based on Bianchi's original work [38, 39], Xiao [56, 57] extended the Markov chain based analytical model to account for the changes in the window sizes and backoff window increasing factor. This was later extended further by Xiao in [58] to model the EDCF draft protocol. The model in [58] accounted for changes in the initial window size and the AIFS length. The saturation throughput and delay were derived and it was found that changes in the initial window size had a greater effect on differentiation than changes on the AIFS value. Bianchi later refined a mathematical model (not based on Markov chains) to include changes in the AIFS [59] which was found to be more accurate than previous works.

Leading up to the finalisation of the 802.11 standard [23] a number of other performance studies [60-70] of EDCA have been conducted using simulation and analytical models in both saturation and non saturation conditions. Del Prado Pavon also looked at the centralised HCCA functionality in [61, 64]. However due to complexity of managing such schemes these are not elaborated further in this Thesis. Also there is very little interest from the major equipment vendors, with the focus being on distributed schemes such as EDCA.

Following the extensive research into the performance of EDCA using simulation and analytical tools, there has been some pioneering work in experimental testing by a number of

groups. As shown in the research work, vendor implementations in hardware devices of the 802.11 standard can differ significantly. As shown in [71, 72], the behaviour and operation of client hardware devices is shown to vary considerably. Di Stefano shows in [71] that factors such as delay and throughput can be affected by non standard implementations. The assumed fairness of DCF as prescribed in the IEEE standard is not guaranteed, as some devices are tested to have shorter interframe spaces and CW_{min} sizes. The operation and implementation of the *auto rate fallback* mechanism, which is not explicitly defined in the standard, also shows variation between vendors. Bianchi [72] while investigating various hardware, concentrates on the backoff mechanism and finds variations, as none of the cards actually perform as they should as specified by the standard [21]. The cards tested in [72] were all certified by the WiFi Alliance, yet major differences are found by the author. One reason behind this may be that manufacturers are using non standard values for the DCF parameters in order to get better performance. In Section 6.4 the analysis of the retransmission pattern of some cards will show the use of non standard values for the retry limit. It is for these reasons the same Atheros client cards are used across all of the client terminals in the experimental testbed.

Looking now at studies concerned directly with 802.11e, some promising empirical work has been conducted over the last two years. The lack of hardware support for the EDCA protocol meant evaluation and analysis could only be conducted through simulation or mathematical models. EDCA hardware has recently become mainstream and operating system support is increasing with open source initiatives like the MADWiFi project [27].

The authors in [73, 74] focus on a non saturated model to analyse the fairness between competing TCP streams over a wireless network. They suggest the use of lower AIFS and CW_{min} values in addition to a variable TxOP for the TCP acknowledgement packets in order

to enforce a level of fairness between streams. However, this work only concerns traffic presented in a single EDCA class. In this thesis the fairness aspect between multiple access classes is investigated. The same group looks at improving VoIP capacity [75] through the modification of the EDCA parameters. Using a hardware testbed similar to that presented in this Thesis (described in Subsection 6.2.3, page 120), Clifford [76] investigates the competing TCP fairness problem thoroughly through mathematical analysis, simulation and experimentation. Using the same testbed setup, Dangerfield [77] investigates the VoIP capacity in both DCF and EDCA networks experimentally. The author provides valuable data on the inability of DCF to support real time services in the presence of TCP data traffic. EDCA parameters, in particular the AIFS, are optimised to support VoIP in the presence of other TCP data traffic. Measurements of the one way delay are provided from experimental results. The research in this thesis utilises the retransmission distribution to generate a delay distribution, which demonstrates the prioritisation effect of EDCA in the experimental testbed. This delay distribution, which is elaborated on later, shows the entire range of delay figures for each traffic class in EDCA. The work conducted in [77] is advanced further by Dangerfield in [78], in which the effects of different buffer sizes and TxOP lengths on VoIP throughput and delay are investigated.

The authors in [79] investigate MAC layer frame losses and their effect on VoIP traffic. The losses are classified into either congestion losses or channel losses to aid the operation of the auto rate fallback mechanism. The work is conducted through simulation and would be even more valuable if repeated experimentally in order to asses real channel losses. In Section 6.6, the effect of frame losses at different data transmission rates is investigated.

Some promising recent work conducted experimentally in [80] investigated the effect of varying the TxOP parameter on the video quality when using data partitioning. The TxOP

parameter allows for a station to send a burst of data frames in a single contention attempt. This benefits streams, such as video, where the packets are dispatched in bursts. The investigation in Section 6.7 focuses on the allocation of video data to different access classes and not on optimisation of a single class.

4.11 Conclusions on QoS and Related Work

In this Chapter the concept of Quality of Service and some of the most important metrics used to measure and quantify it are introduced. The operation of QoS mechanisms used on fixed networks, IntServ and DiffServ, were discussed. IntServ suffers from problems with scalability due to its complex resource reservation based approach. DiffServ is simpler than IntServ to implement as it operates on a per flow basis, providing QoS to groups of traffic. However, flow tagging problems and cooperation between ISP's limit its use to traffic domains, but is not always available for end to end communication.

The main performance metrics; throughput, delay and jitter are discussed in detail. Almost all services are affected, to some extent, by variations in throughput. FTP and HTTP can operate using a wide range of values. VoIP requires a minimum throughput to provide an acceptable MOS. Delay must also be within acceptable limits in order for VoIP to function correctly. Excessive delay can affect the intelligibility of conversations. HTTP and FTP are insensitive to changes in the delay. However an interactive HTTP session involving frequent page requests can be adversely affected by a large delay in the order of seconds. It is also concluded that QoS should not just be concerned with prioritising the most important traffic, but should also consider the fairness between competing traffic streams. This is investigated further in Section 6.5.

The related work section presented a summary of the previous and current work in the area of IEEE 802.11, with a strong focus on the EDCA mechanism. While a lot of the work conducted has been based on multidimensional Markov chain models, as originally proposed by Bianchi in [38, 39] for DCF, these have been expanded to account for the multiple classes of EDCA [56-58]. Simulation methods have also proved popular. However, many of these do not account for the losses that readily occur over a wireless channel. Losses are accounted for by Zheng in [45], which bring the models closer to a real world scenario. Experimental work, such as that conducted in [78, 80, 81] is essential to verify the accuracy of mathematical and simulation models. It is a fact of the physical world that frame losses and errors are an integral part of transmission sent over wireless networks. The work in Section 6.4 will show that frame losses are a regular occurrence even in good channel conditions. Frame loss is also investigated by Malone in [82] through experimental methods. Further experimental work is required to enhance the understanding of the effects of a lossy wireless channel on higher layer protocols and end to end QoS metrics.

5 Simulation Results and Data Analysis

5.1 Introduction

In this Chapter the simulation platform, results and data analysis are presented. Section 5.2 describes some of the simulation tools used in this research, ns2 [25] and OPNET Modeller™ [26]. The results from simulation are introduced with the initial evaluation of the legacy DCF based MAC layer with a single service. This is followed by the performance demonstration in the presence of multiple services and the lack of service differentiation in legacy systems. The focus then moves to PCF in a typical network.

5.2 NS-2 and OPNET Simulator

This research work has spanned a number of years and through this time there have been a number of new developments in the way of simulation tools. Currently there are two popular packages being used, within the research community to simulate wireless networked environments, ns2 [25] and OPNET Modeller™ [26].

Ns is a discrete event simulator targeted at networking research. Originally being a variant of the REAL simulator [83], it has been modified substantially to its current state, ns version 2. Ns provides substantial support for simulation of UDP/TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks, running in most Linux/Unix environments. Its use is limited to mainly academic circles, where it's free license and open source code are seen as advantages. Many researchers publish code for ns2 on their websites, but implementations are often difficult to integrate into a generic build, due to the customisations made by the original programmer. The package is based on C++ and OTcl, with a script driven interface. Traffic patterns and other important simulation parameters are

parsed through additional files. An example of an ns2 script is shown in Figure 5.1. This sets up a simple two node network with a duplex 1Mb/s link connecting them.

Figure 5.1 - Simple ns2 Script [84]

Some GUI interfaces to ns2 have been written but are in an early stage of development, which makes them unreliable for research use. Extensive description of the main simulator is provided in a 392 page PDF file, but tutorials and other help are limited to a few websites. Due to its license free status there is no technical support provided other than newsgroups and message boards run by other end users and academic institutions.

OPNET Modeller™ is a commercial software package originating from works done at MIT and was commercialised in 1987. Within Industry OPNET Modeller™ is the leading software

package for network modelling and simulation. There are an increasing number of universities, particularly in the USA, now using OPNET for their teaching and research work. A free university license is available that is renewable every 6 months and includes technical support via email which is free of charge. OPNET runs on both Windows and Sun Solaris environments as well as Linux in the latest versions. Extensive documentation on functionality is provided along with a comprehensive set of tutorials. Protocols and Process can be modified on a number of different levels. There is also direct access to the C/C++ source code that is used for implementing the models featured in the program. The standard model library also includes many hardware devices in addition to pre-defined traffic models for popular applications such as HTTP, FTP, VoIP, and Video Conferencing. Wireless network simulation is supported through the use of the Wireless Module, now integrated into the main Modeller program as the Wireless Suite.

Initially Network Simulator was used for the basic simulations using a few clients. However the setup was just a point to point system and did not account for the contention on a LAN/WLAN, in addition to multi layer interaction and wireless medium contention. The progress with implementing simulations in ns2 was slow, with the wireless module lacking extensive documentation, so OPNET Modeller™ was chosen as an alternative simulation platform.

OPNET Modeller™ features an intuitive GUI interface, shown in Figure 5.2 that is an integral part of the core software. The GUI shows a wireless network with 10 clients and a single access point.

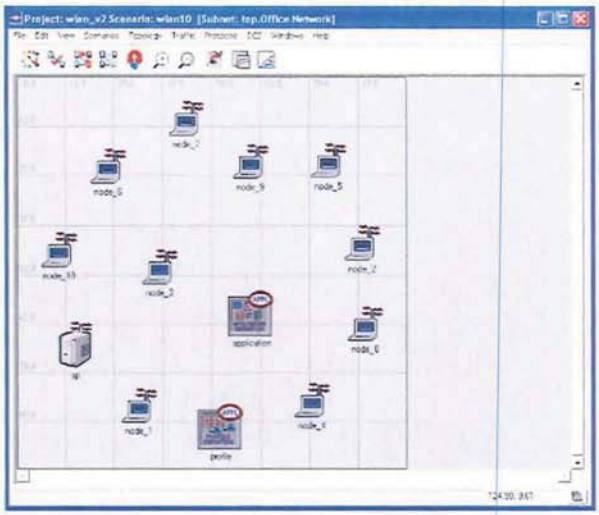

Figure 5.2 - OPNET GUI

The Wireless Module allows the design and simulation of multiple scenarios' which can be scaled up to 100's of clients. Built in traffic models were useful, as they provided a basis for modelling real world traffic on a Wireless LAN. Results can be presented in a variety of methods, though the graphical view proved most useful. An example of a throughput graph is shown in Figure 5.3. This shows the Wireless LAN throughput on a per station basis versus time in minutes. Each station has a different packet inter-arrival time, resulting in different throughput values. It must be noted that the results were generated from a different network topology to that illustrated in Figure 5.2.

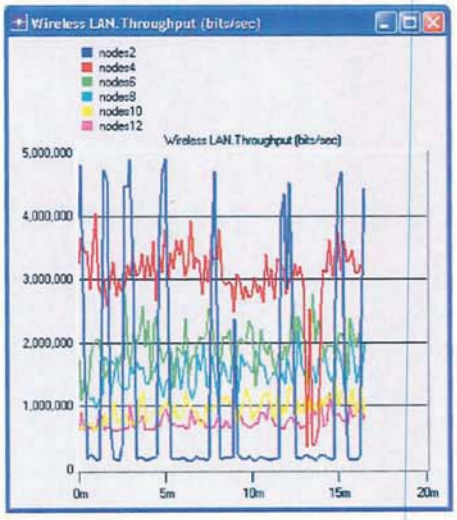

Figure 5.3 - OPNET Graphical Result Output

If required the graph data can be exported to a spreadsheet program such as Microsoft Excel. This allows added flexibility if the OPNET output format is not suitable or further calculations are required on the data gathered from the simulation.

5.3 Legacy DCF and PCF Results

In this section the simulation work is presented. This aims to show the inability of the legacy 802.11 DCF MAC to support multiple services and provide service differentiation between them. Initially the performance in terms of throughput and delay with a single traffic type is shown. This is later expanded to show the results in a network with multiple traffic patterns. To conclude the section the results from some simulations in a PCF enabled network are presented.

5.3.1 Single Traffic HTTP DCF Performance

In this example a simple network in OPNET is simulated using the DSSS 802.11b PHY. The network is configured as a BSS with a single access point and the number of clients being varied from 1 to 80. The wireless parameters used in OPNET are shown in Figure 5.4. There is no mobility simulated and all clients are static throughout the duration of the simulation. Clients are all situated within a 20m radius of the AP.

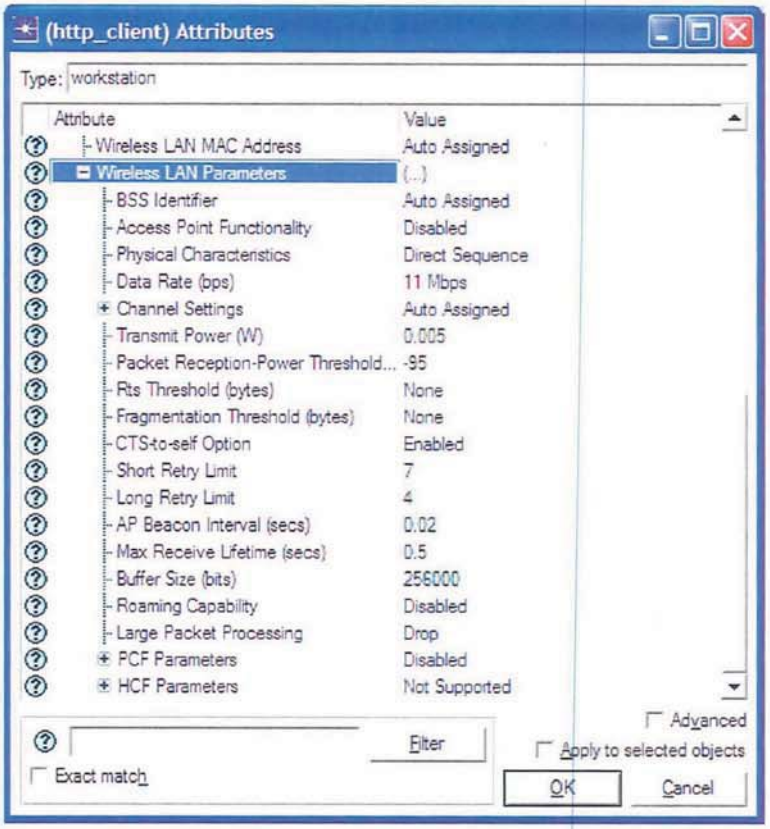

Figure 5.4 - OPNET DCF 802.11b Parameters

The HTTP 1.1 protocol, typically used in web browsing, is configured on each of the stations to simulate web browsers connecting to a web server outside of the wireless network via the backbone network. There is no simulated background traffic on the backbone link. The HTTP page properties are shown in Figure 5.5. The standard values for the DCF parameters (802.11b PHY) were used for the simulations, as prescribed by the IEEE 802.11 standard. These are shown in Table 5.1 below.

Parameter	Value
Slot Time	20μs
SIFS Time	10μs
CW_{min}	31
CW_{max}	1023

Table 5.1 - 802.11b PHY Settings

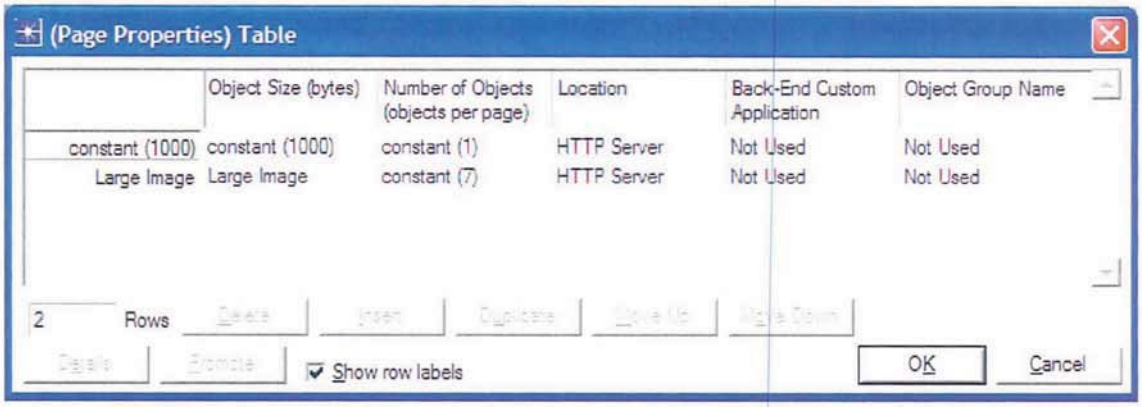

Figure 5.5 - Simulated HTTP Page Properties

The page consists of the hypertext markup language (HTML) element of 1000 bytes and seven large images of size 2000 bytes to 10000 bytes (distributed uniformly). The page requests are modelled on an exponential distribution with a mean of 10 seconds.

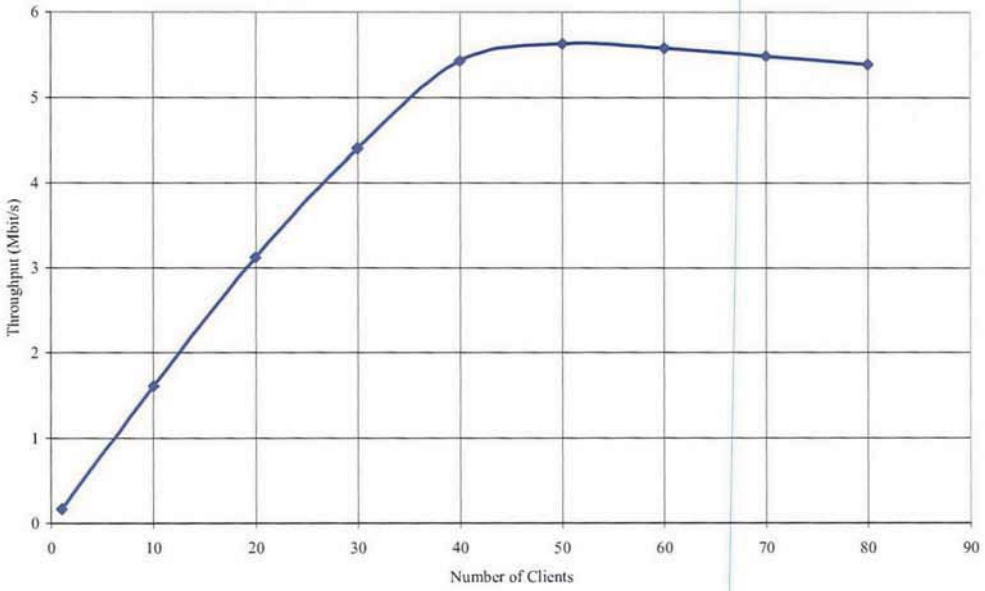

Figure 5.6 - Throughput vs. Number of Clients with HTTP 1.1 Traffic

In Figure 5.6 the overall HTTP throughput over the wireless network is shown as the number of clients is increased in multiples of 10. Due to the bursty nature of HTTP traffic, the average throughput over the course of the simulation is relatively low. The first data point, with a

single client, the throughput is 160 kbps. As the number of clients is increased, the overall throughput increases until approximately 50 clients, after which the throughput starts to drop off. At the point of 50 clients the network has reached its capacity and is unable to support any more HTTP clients at the typical individual throughput. This effect is clearly shown in Figure 5.7 where the individual client throughput is slowly reduced.

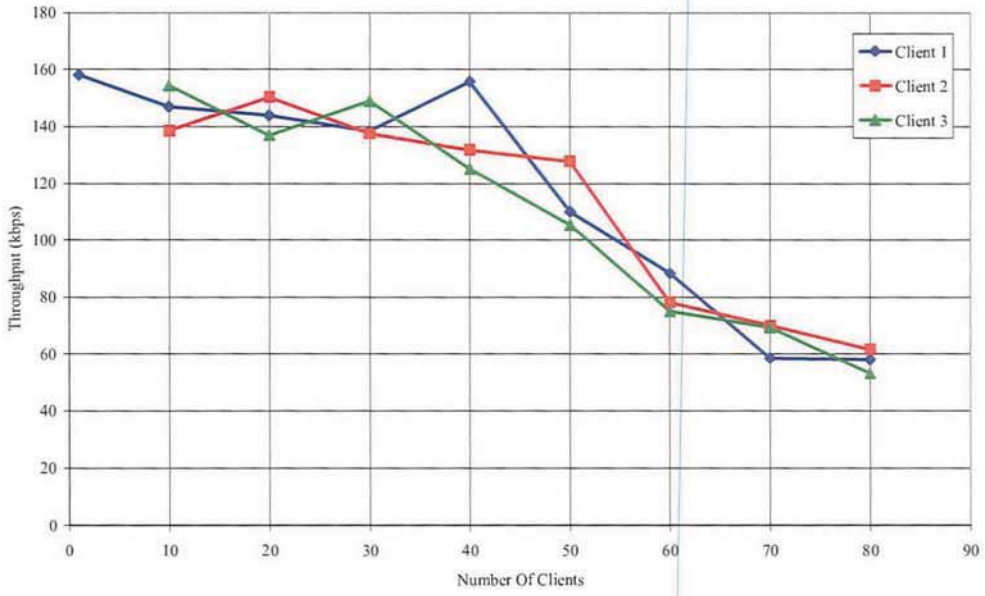

Figure 5.7 - Individual HTTP Client Throughput

The end user will most likely experience slower web browsing in terms of page loading time. In Figure 5.8 the End to End HTTP delay is shown, measured from client to server over the wireless network.

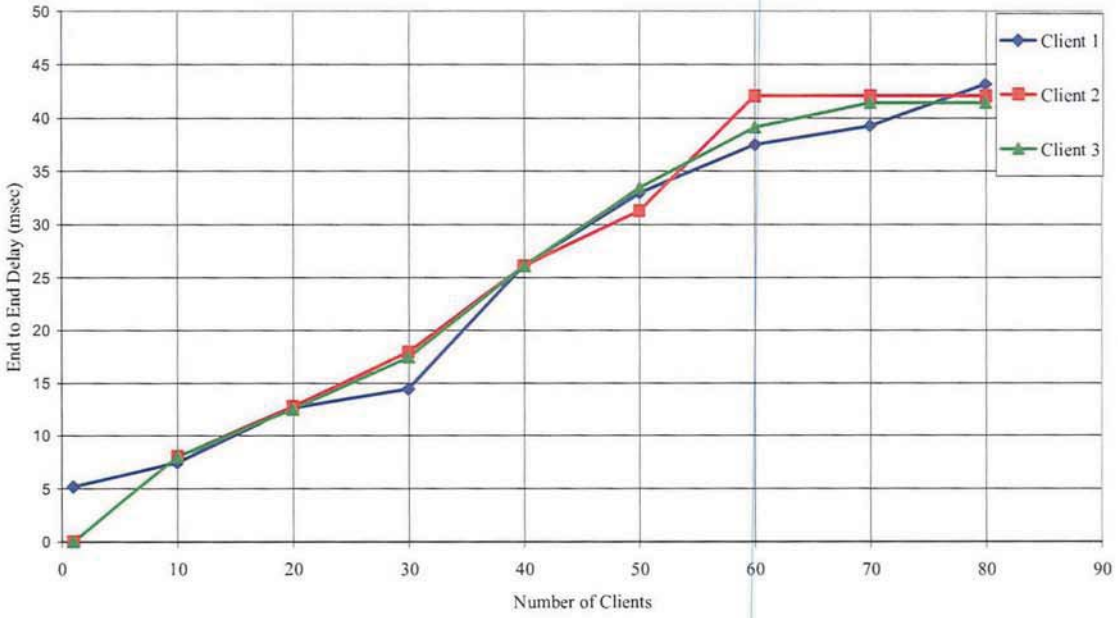

Figure 5.8 - End to End Delay vs Number of Clients with HTTP 1.1

As specified in Section 4.3 the delay has little effect on the end user experience with HTTP. It can be seen from the graph that delay increases almost linearly with the number of clients. The increase in delay in the range shown, i.e. 10's of milliseconds, is unlikely to impact the end user experience, although a delay in the 100's of milliseconds would be noticeable.

Figure 5.9 shows the total number of TCP retransmissions at the transport layer. A TCP retransmission is caused when the MAC layer is unable to send a frame within the given timeout limit at the TCP transport layer. As the number of clients increase, there is greater contention for the wireless medium. This results in individual HTTP packets waiting for too long before they are transmitted over the wireless medium. As mentioned above, under the condition of high loads the TCP connection will time out and trigger a TCP retransmission. It can be seen that the number of TCP retransmissions begins to increase significantly after reaching 32 clients. The effect of TCP retransmissions on a wireless LAN is investigated in

[85]. Excessive retransmissions can have a negative impact on delay and throughput, both of which are important metrics in quality of service.

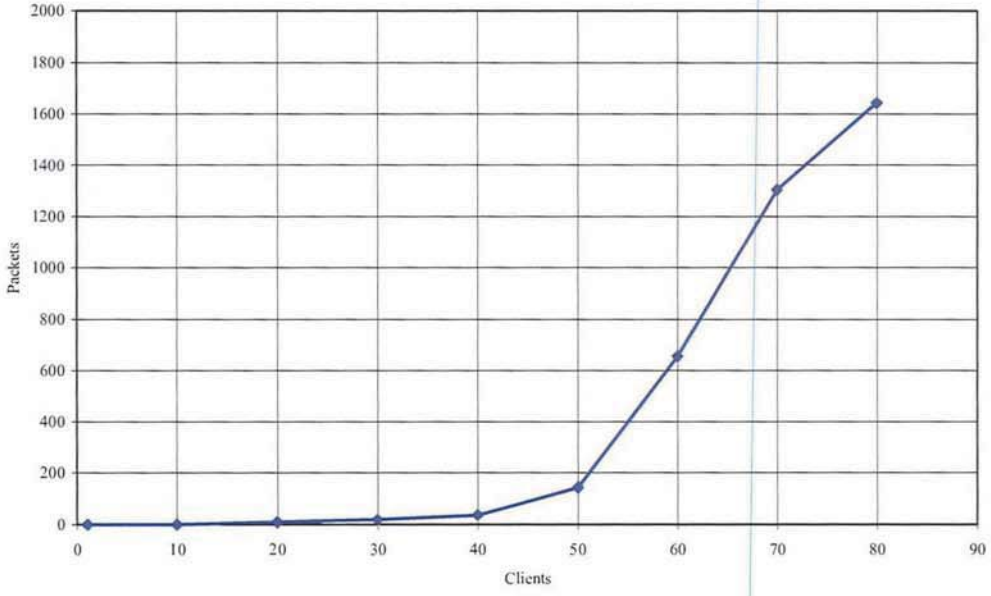

Figure 5.9 - TCP Retransmissions vs. Number of Clients with HTTP 1.1

5.3.2 Multiple Traffic DCF Performance

In this section multiple traffic types are introduced into a DCF wireless network to demonstrate the best effort operation of the legacy MAC protocol. In addition to TCP based HTTP and FTP traffic, VoIP traffic is introduced, which is UDP based traffic. As described in Subsection 2.5.3, VoIP traffic is regarded as delay sensitive. The voice quality measure Mean Opinion Score (MOS) is introduced, which is calculated from the gathered data. In the first example, a BSS network is simulated with both FTP traffic and real time VoIP. The wireless parameters are kept the same as illustrated in Figure 5.4. The FTP profile represents general FTP use, while the VoIP profile is representative of a G.711 CODEC with no silence suppression. The specific details of the traffic configuration are shown in Figure 5.10 and Figure 5.11.

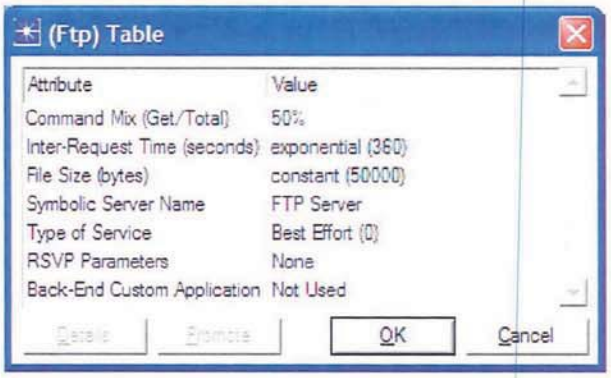

Figure 5.10 - OPNET FTP Traffic Parameters

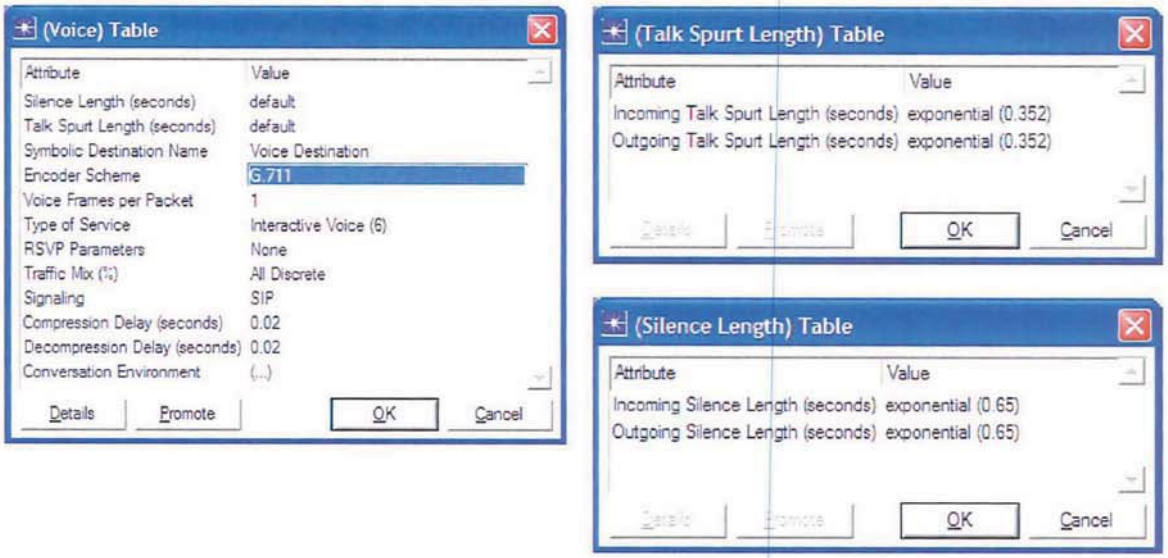

Figure 5.11 - OPNET VoIP Traffic Parameters

The talk spurt is the length for which the user actually speaks. This is modelled on an exponential distribution with an expected mean of 0.352 seconds. The corresponding silence is also modelled on the exponential distribution with an expected mean of 0.65 seconds. FTP traffic is modelled on file requests having an exponential distribution with a mean of 360 seconds and a file size of 50000 bytes. The upload and download mix is set at 50%, so both occur in equal numbers during the course of the simulation. Both services are set to run concurrently on each client station from the start of the simulation. The average values from the simulation runs were taken and plotted them in the figures shown below.

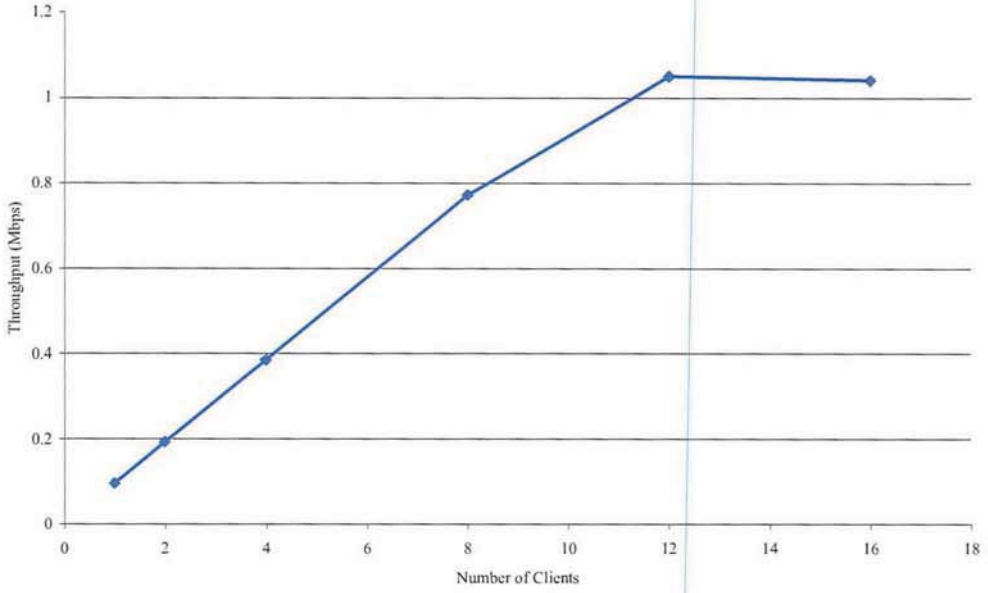

Figure 5.12 - DCF Throughput with Mixed FTP/VoIP Traffic

Figure 5.12 shows that as the number of clients on the network are increased, the offered load increases linearly until 12 clients.

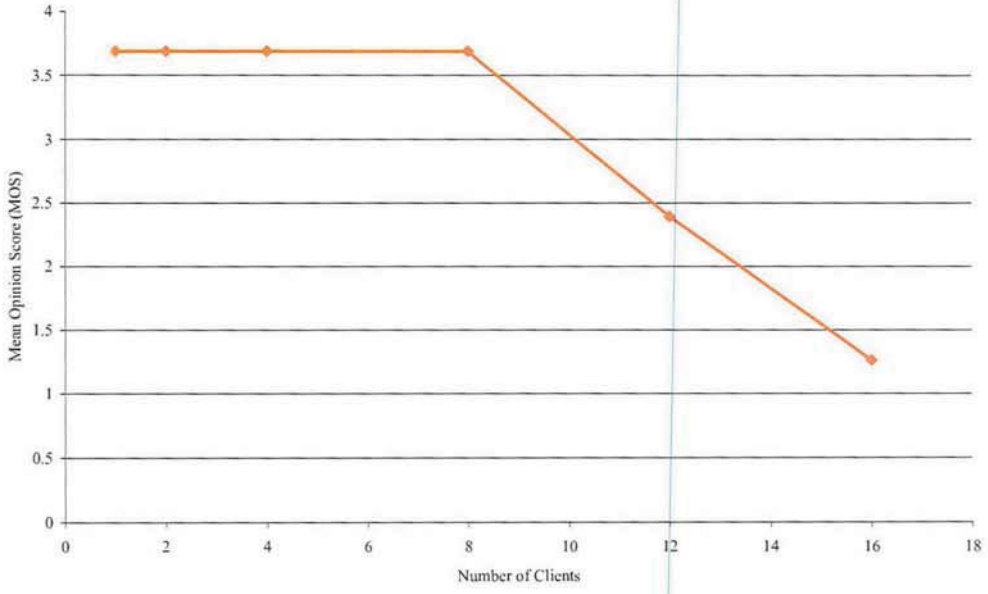

Figure 5.13 - DCF MOS with Mixed FTP/VoIP Traffic

Similarly, it can be seen from Figure 5.13 that the mean opinion score reduces significantly after 8 clients. Referring back to Table 4.1 that shows the interpretation of MOS scores, after eight clients the majority of users would be dissatisfied with the call quality with a MOS below 3.4. This can be regarded as the VoIP capacity for the network with this particular type of background traffic. It is shown in this chapter that the VoIP capacity of a DCF based network can vary depending on the other traffic streams present. In the case where there is heavy traffic it is expected that the VoIP capacity will be lower; and in the cases where background traffic is lower, higher VoIP capacity is expected. The findings on the VoIP capacity of a network are in line with the investigations conducted in [86], where heavy traffic reduces VoIP capacity.

5.3.3 PCF Performance

Although PCF is rarely implemented in any hardware devices, the simulation tool OPNET had support for this mechanism. Referring back to Subsection 3.2.2 where the operation of PCF is described, it would seem true that the access mechanism does not scale well. The network was configured such that the total number of stations was split 50% VoIP and 50% FTP. For example in the scenario with eight clients there were four VoIP and four FTP, similarly with a total of 16 clients, eight were VoIP and eight FTP. The traffic patterns are as prescribed in Figure 5.10 and Figure 5.11. In Figure 5.14 where the individual throughput is plotted against the number of clients, it can be seen that the effect of the polling mechanism of PCF has on the throughput.

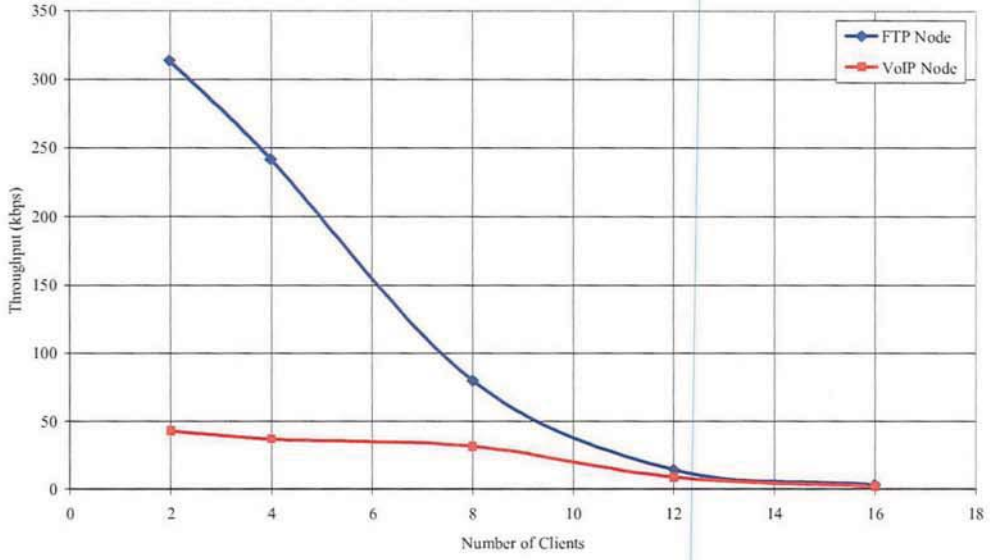

Figure 5.14 - PCF Throughput with FTP/VoIP Traffic

Recalling that PCF operates in a round robin fashion in which each station associated with the AP is polled one by one through the use of the CF-Poll frame. As the number of clients increases, the AP has more stations to poll, resulting in poor operational efficiency at large client loads. The initial throughput of the VoIP stream is much lower than that of FTP due to the nature of the traffic with FTP having much larger packet sizes when compared to VoIP.

In Figure 5.15 the end to end delay of both an FTP Client and a VoIP client is shown. The increased delay introduced by the PCF at high loads is clearly visible. The FTP delay increases steeply after four clients, while the VoIP delay increases after eight clients. This difference may be due to the FTP packets being considerably larger in size than those of VoIP. This would allow the client station to transmit the smaller packet quicker than a larger packet and allow the AP to move on to poll the next client with a minimal delay. At approximately 10 total clients, five VoIP and five FTP, the delay for the VoIP clients has reached the delay threshold, which will affect the call quality.

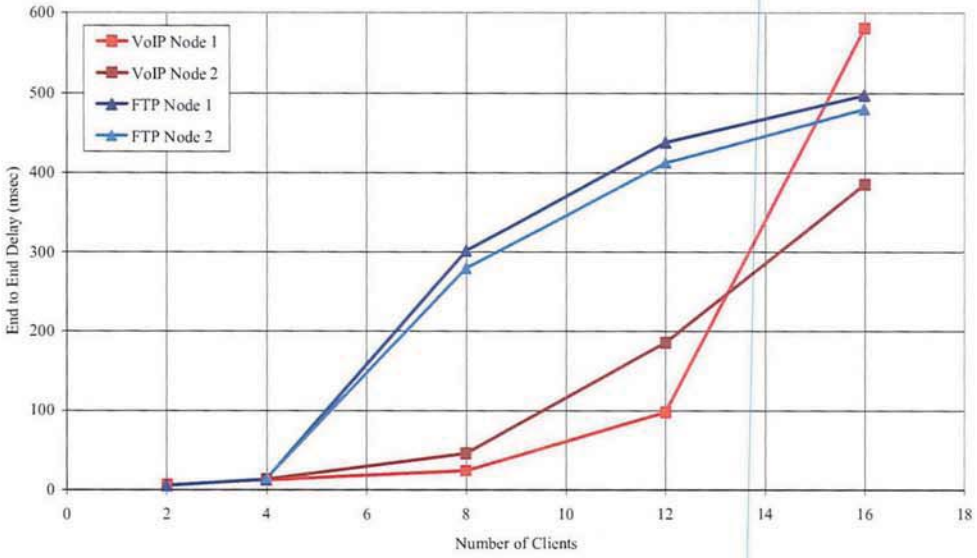

Figure 5.15 - PCF End to End Delay with FTP/VoIP Traffic

The facility to measure the MOS for VoIP was not available in the earlier version of OPNET Modeller used to generate the results for PCF.

5.4 Enhanced EDCA Results

This section aims to provide a comprehensive analysis of the EDCA access mechanism based on simulation results. Initially some comparisons of legacy DCF against EDCA are shown using similar traffic patterns. Following this the service differentiation ability of EDCA with both TCP and UDP based traffic is introduced.

In the first example an earlier simulation is repeated to demonstrate the service differentiation capability of EDCA over DCF. Referring back to Figure 5.12 and Figure 5.13 the same settings and traffic patterns are used (as prescribed in Figure 5.10 and Figure 5.11) except with the EDCA access mechanism enabled instead of the legacy DCF. The EDCA parameters set is kept as prescribed in Table 3.3 with no modification to any values. The default positive

acknowledgement scheme is used. The legacy DCF results are also included in Figure 5.16 and Figure 5.17. Referring to the MOS in Figure 5.16, it can be seen that EDCA is able to provide an adequate service in terms of VoIP quality at the presented traffic loads shown in Figure 5.17. The traffic classification or allocation is given in Table 5.2.

Traffic Type	EDCA Traffic Class
Voice over IP (VOIP)	AC_VO (Voice)
File Transfer Protocol (FTP)	AC_BE (Best Effort)

Table 5.2 – Simulation Traffic Class Assignment

As introduced in Subsection 3.2.3.1, the shorter AIFS and contention window of the AC_VO category will allow the VoIP stream to access to the medium before others. Others competing streams, in this case the AC_BE used for FTP will back off for a longer time given the VoIP traffic with greater priority.

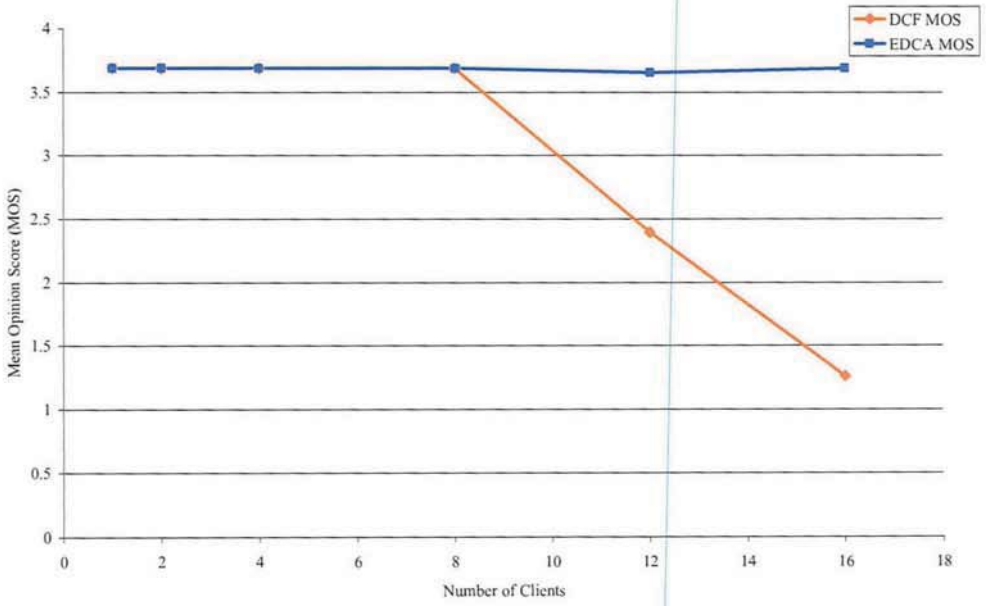

Figure 5.16 - EDCA/DCF MOS with FTP/VoIP Traffic

It can also be seen from Figure 5.17 that EDCA has a slightly higher overall throughput than DCF with the same traffic pattern. This effect can be attributed to the better medium utilisation by the enhanced MAC layer. With multiple stations using different contention window sizes, the probability of collision is less than that with DCF where all stations use the same window size.

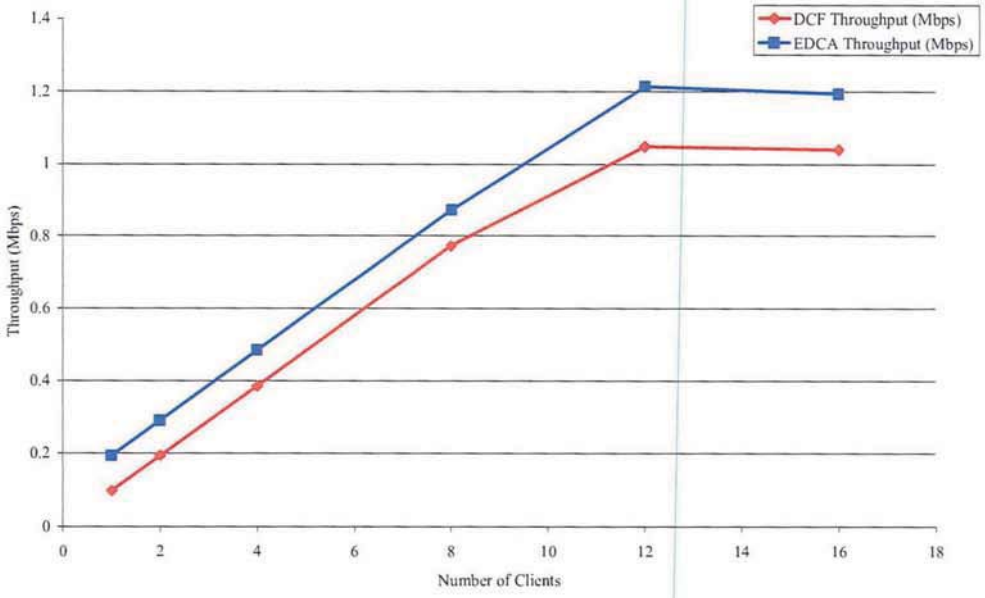

Figure 5.17 - EDCA/DCF Throughput with FTP/VoIP Traffic

In the next simulation example, another BSS network is simulated with both the DCF and EDCA access mechanisms. This simulation introduces HTTP traffic in addition to the real time service VoIP. The network is scaled in terms of the number of clients, higher than previously shown. The class assignment is shown in Table 5.3.

Traffic Type	EDCA Traffic Class
Voice over IP (VOIP)	AC_VO (Voice)
Hyper Text Transfer Protocol (FTP)	AC_BE (Best Effort)

Table 5.3 - Simulation Traffic Class Assignment (2)

The services are split equally across the total number of clients. For example when the total number of clients is four, there are two HTTP clients and two VoIP clients. This is shown in Figure 5.18. As with the previous example, the EDCA parameter set is kept as prescribed in Table 3.3 with no modification to any values. The default positive acknowledgement scheme is used. In this example the G.726A codec is used in addition to silence suppression which reduces the data rate by stopping transmission during silent periods in the conversation. The specific settings are shown in Figure 5.19.

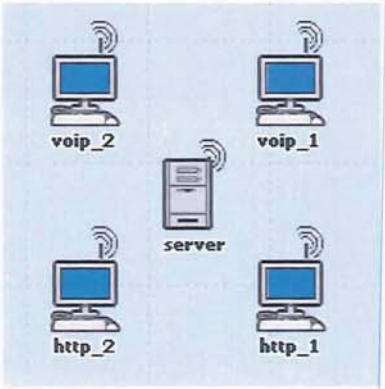

Figure 5.18 - Service Allocation in a Mixed Network

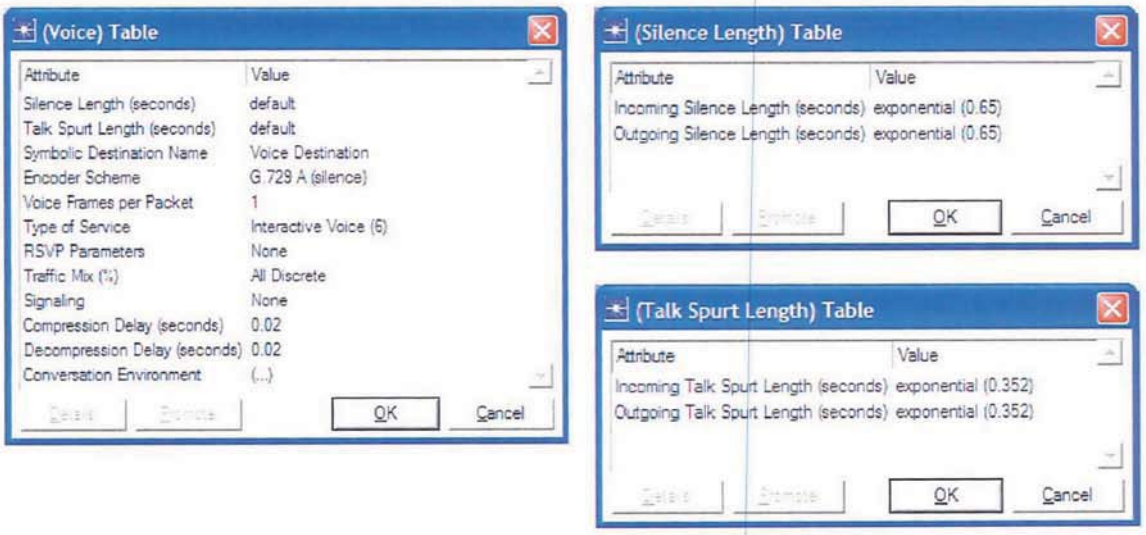

Figure 5.19 - OPNET G.729A VoIP Traffic Parameters

The talk spurt and silence lengths are kept the same, modelled with an exponential distribution with a mean of 0.352s and 0.65s, respectively.

In Figure 5.20 the overall network throughput as the total number of clients is increased from 4 to 36 is shown. Traffic is split 50/50, with a network of four clients having two VoIP and two HTTP. As expected the throughput increases gradually as the load is increased on the network. At the data point of 20 clients, the throughput peaks at just under 3 Mbps, indicating that the maximum network capacity has been reached with this traffic pattern. As the number of clients in increased further, the network throughput starts to drop off sharply as the throughput saturation point has been reached.

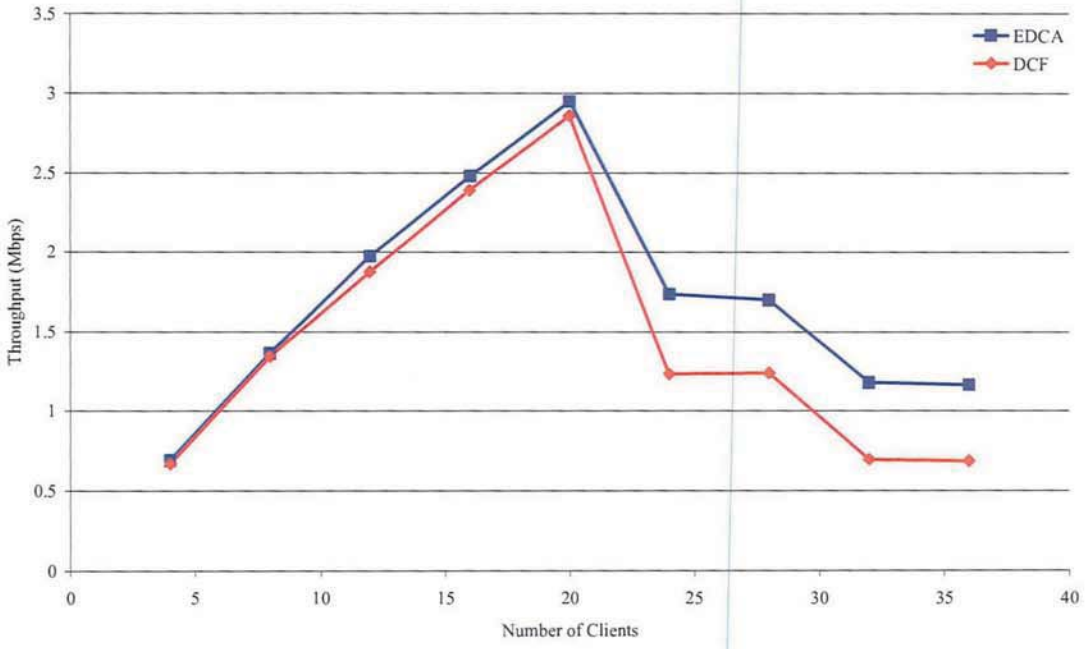

Figure 5.20 - Overall Throughput with HTTP/VoIP Traffic in a DCF/EDCA WLAN

The total network capacity for both DCF and EDCA are almost identical in these cases. In line with previous results, the greater efficiency of EDCA sees a slightly higher numerical value than DCF for a given number of clients; however this is more apparent at higher loads.

Comparing the overall throughput in Figure 5.20 with the HTTP Delay in Figure 5.21 it can be seen as the network approached its maximum throughput at 20 clients, the HTTP delay increases considerably. Although as mentioned in Subsection 2.5.1, the HTTP service is not particularly sensitive to changes in delay, although changes in the region of 100's of milliseconds could have an impact on the end user experience. The increased HTTP delay is illustrated by reduced responsiveness and greater time between clicking a hyperlink and the page beginning to render on screen. In Figure 5.21 both EDCA and DCF follow the same pattern, with HTTP delay increasing as the number of client stations increase. As the HTTP traffic is placed in the AC_BE (Best Effort) class, it receives a similar service to that of DCF, with no prioritisation.

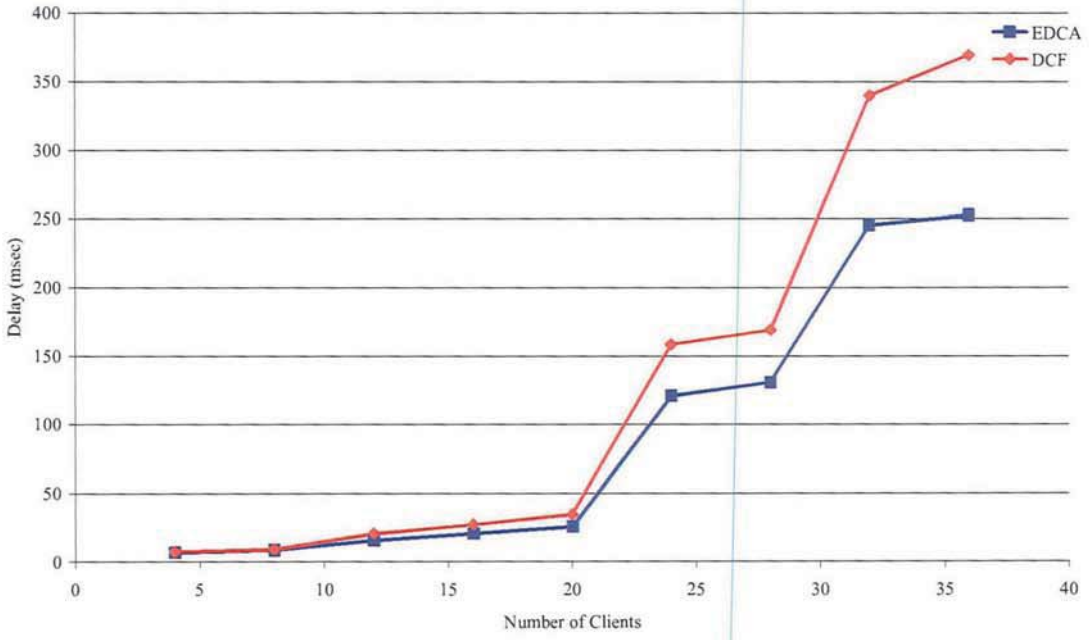

Figure 5.21 - HTTP Delay with HTTP/VoIP Traffic in a DCF/EDCA WLAN

Figure 5.22 shows the VoIP client delay, it illustrates a different trend to that in Figure 5.21 of HTTP delay. As shown in Table 5.3, the VoIP traffic is assigned to the AC_VO (Voice) category and HTTP to the AC_BE (Best Effort) category. The prioritisation mechanism and

service differentiation in EDCA is clearly evident, as the higher priority VoIP stations have a substantially lower delay than those using HTTP in the AC_BE category. The VoIP delay under DCF rises rapidly with load and again shows the inability of DCF to support time sensitive services under heavy network loads. The EDCA access mechanism manages to restrict the delay to below the 150 ms threshold [20] for VoIP traffic before the MOS is affected.

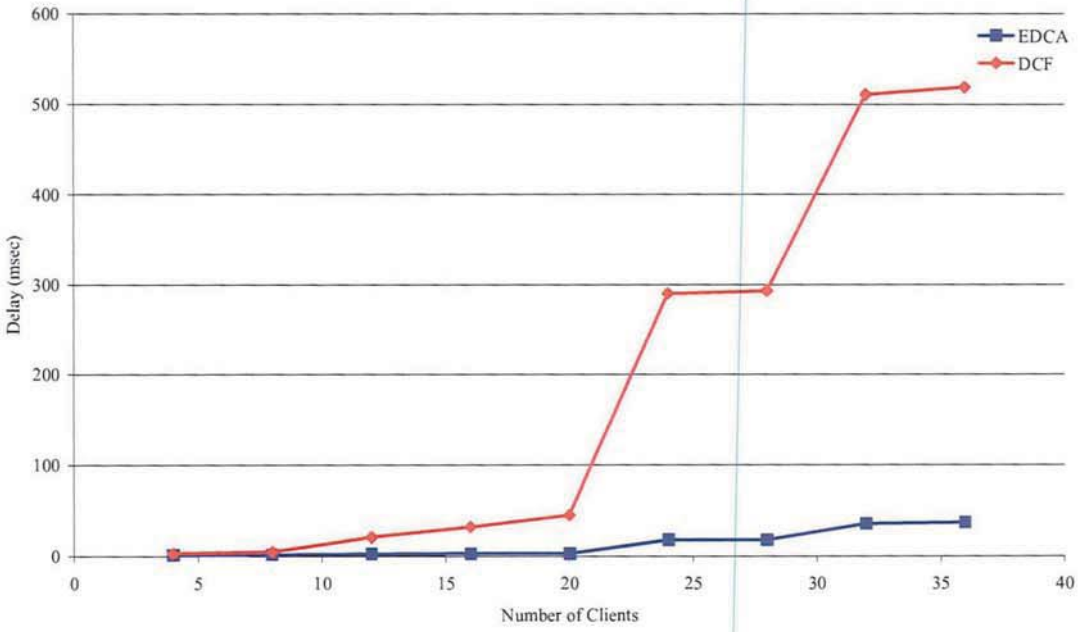

Figure 5.22 - VoIP Delay with HTTP/VoIP Traffic in a DCF/EDCA WLAN

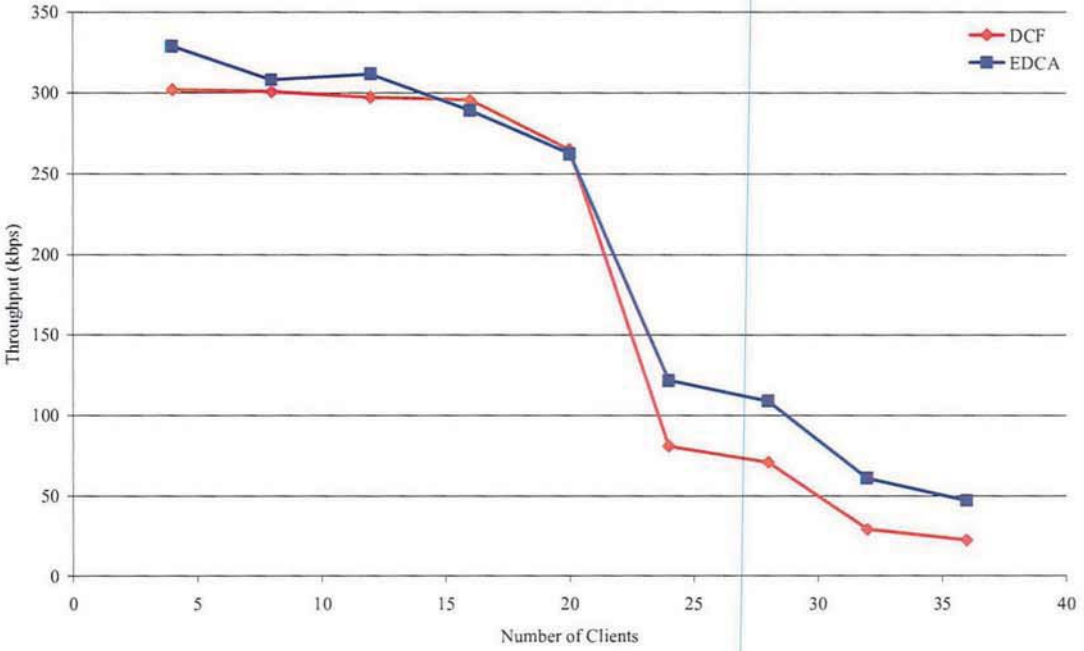

Figure 5.23 - Individual HTTP Throughput with HTTP/VoIP Traffic in a DCF/EDCA WLAN

In Figure 5.23 showing the HTTP client throughput, it can be seen how the lower priority traffic is gradually throttled back as the network load is increased. This is true for both DCF and EDCA, which is using the AC_BE (Best Effort) category for HTTP traffic. This reduction of HTTP throughput would be signified by web pages requiring a longer time to be displayed on a user screen. Modern web pages can contain a large number of graphical elements in addition to textual content. For example, the BBC News front page contains over 20 graphical images in addition to textual information [87]. Slower HTTP throughputs, while not critical to the operation of the service, would have an impact on the end user experience as demonstrated later in Figure 5.28.

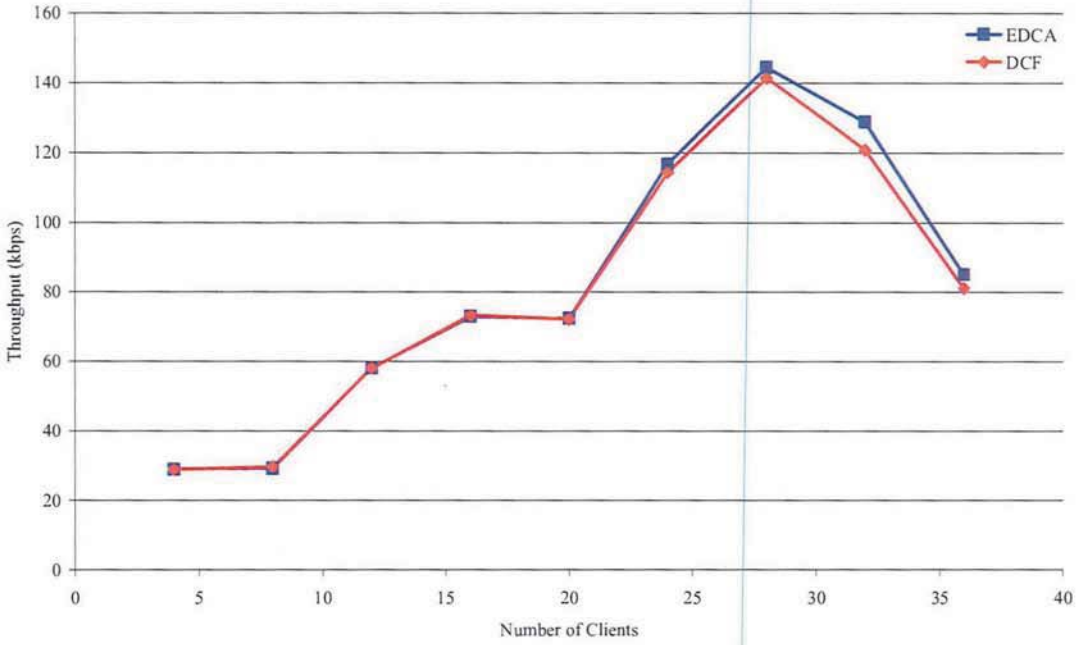

Figure 5.24 – Individual VoIP Throughput with HTTP/VoIP Traffic in a DCF/EDCA WLAN

In Figure 5.24 it can be seen the VoIP throughput increases as the number of clients increases. The graph is significantly different from that of HTTP in Figure 5.23, as the VoIP load is increasing as the number of clients is increased. This is due to the increasing number of simultaneous VoIP calls being made. The HTTP traffic model is one that represents a typical client server operation, where the traffic is mostly downstream from server (in this case AP) to client. The VoIP traffic is more representative of a client to client or more popularly known as Peer to Peer model. Looking at the individual throughput, it is a constant rise until the VoIP traffic peaks at approximately 28 clients. However, from this data it is difficult to see if the individual call throughput is reduced in the presence of other traffic (VoIP and HTTP), so the MOS value in Figure 5.26 is consulted. Both DCF and EDCA perform similarly here in terms of throughput, but looking at Figure 5.22 the delay is significantly lower in EDCA than legacy DCF. Also referring back to Section 4.3 the reader is reminded that VoIP traffic is much more sensitive to delay than to throughput.

Another factor in VoIP call quality is the jitter, which is effectively the difference between successive delay values. In Figure 5.25 the delay jitter for both EDCA and DCF is shown. As observed from the values the majority of the jitter was positive and less than one millisecond. Although DCF has a higher average jitter than EDCA, both are well within acceptable bounds and show no cause for concern.

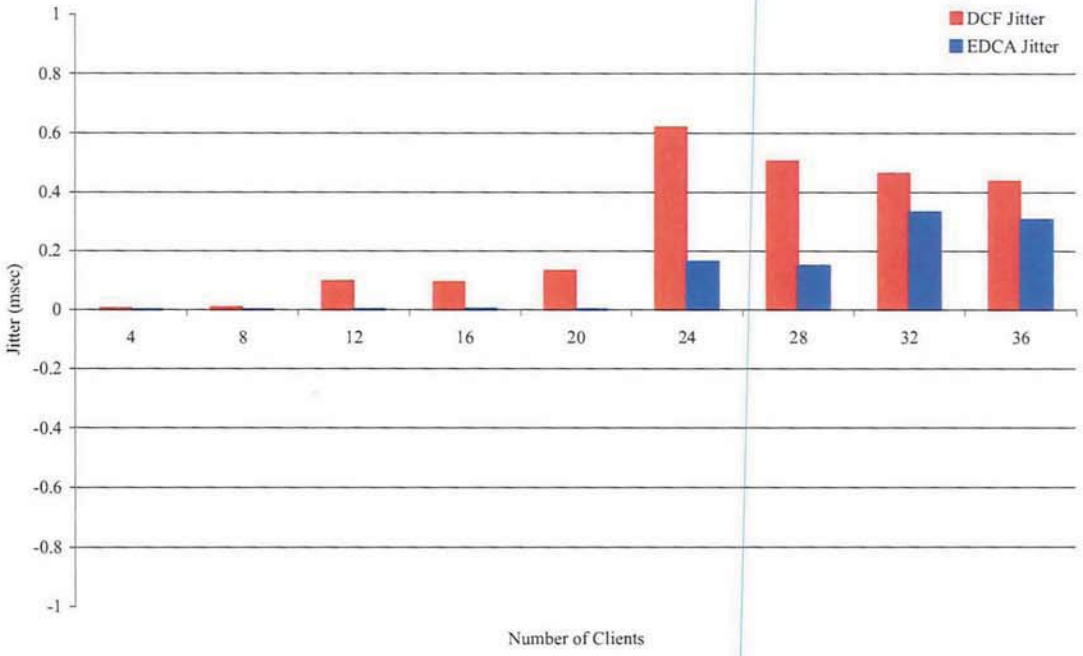

Figure 5.25 - VoIP Jitter with HTTP/VoIP Traffic in a DCF/EDCA WLAN

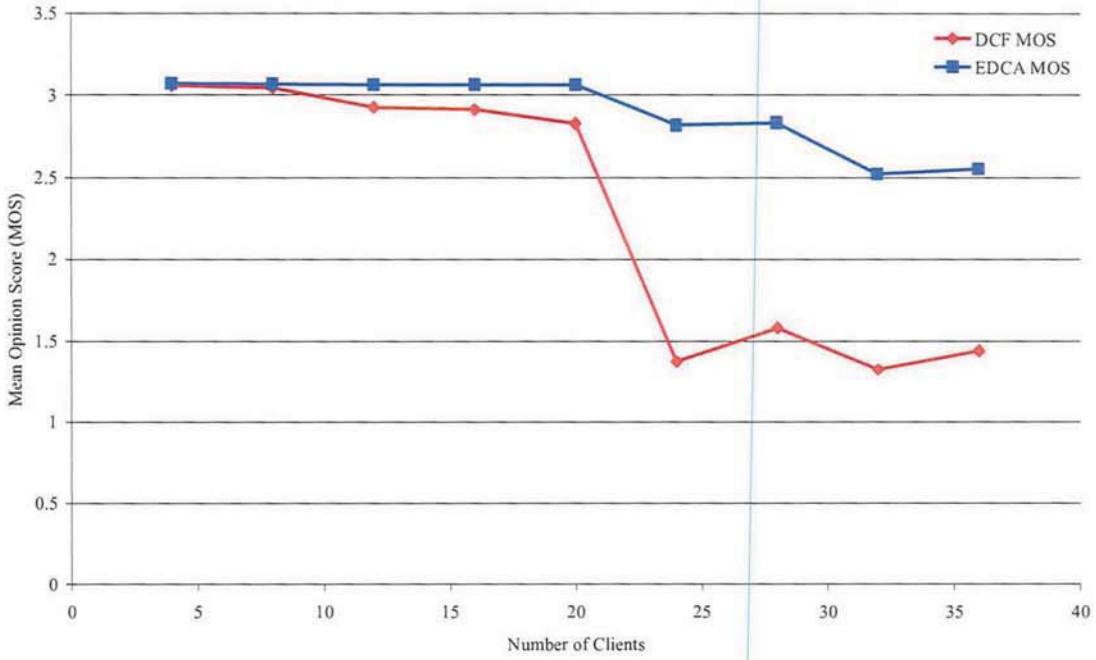

Figure 5.26 – MOS with HTTP/VoIP Traffic in a DCF/EDCA WLAN

Looking now at Figure 5.26 the most important result of the simulation, which shows the mean opinion score for both the DCF and EDCA tests, a considerable difference is observed. A MOS value below three would be regarded as poor quality. With the DCF access mechanism the MOS slips below three at approximately 10 clients, while EDCA is able to keep the MOS intact at above three up to 20 clients. By using different access categories for different traffic types, EDCA is able to provide a greater quality of service to the VoIP users. Also in terms of network utilisation, EDCA is allowing support of a greater number of clients under the given traffic conditions. As mentioned previously this priority is not without a reduced service to HTTP.

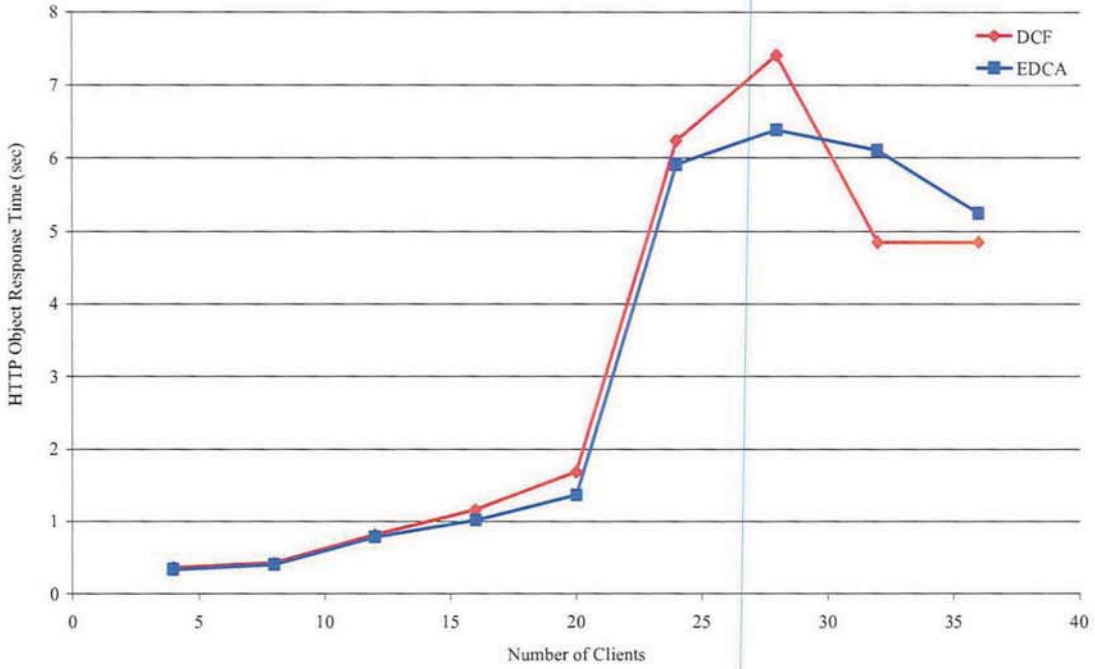

Figure 5.27 - HTTP Object Response Time

In Figure 5.27 the HTTP Object Response Time is shown. This metric is generated by OPNET Modeller™ to gauge HTTP performance in real terms. A HTTP object or element can be anything embedded inside a HTML page, usually an image, sound or animation. The object response time is the average amount of time taken to download each element in a page. The results clearly show a rapid increase in the time taken after the network reaches peak throughput at 20 clients. Under high load EDCA performs worse than DCF, due to the prioritising mechanism, with VoIP in the AC_VO gaining access to the medium before HTTP in the AC_BE category. In DCF all stations are treated equally, so both HTTP and VoIP have equal chances of accessing the medium to transmit.

The HTTP Object Response metric is expanded on by showing the HTTP Page Response Time in Figure 5.28. As the name implies, this is the time taken for the client to download a

web page and all its included elements or objects. The values encountered here are significantly higher than those in Figure 5.27 as there are multiple objects in a single page.

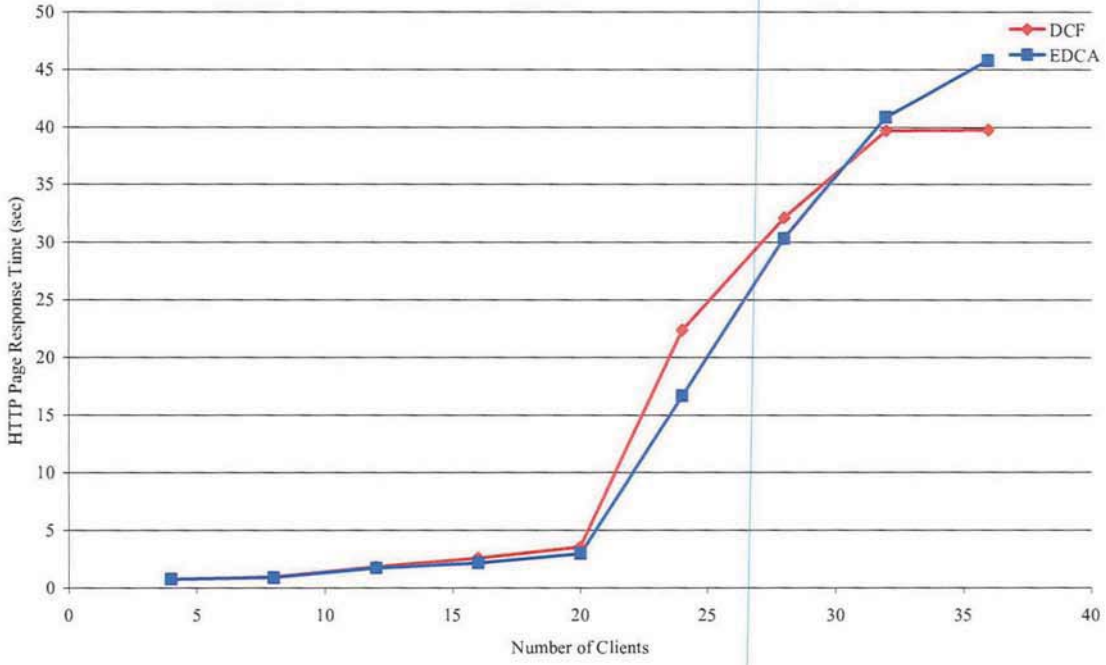

Figure 5.28 - HTTP Page Response Time

From the result in Figure 5.28 the difference between DCF and EDCA is much lower. However, attention must be paid to the numerical values. At 20 clients the page response time is under 5 seconds. This is more than acceptable and considered very good performance. However, as soon as the number of clients is increased above 20, the page response time rises sharply. A response time of 10 – 15 seconds for a large page would be acceptable for a typical wireless connection over a broadband wireless connection (see paragraph below). Under high loads, the HTTP service provided with both access mechanisms is not acceptable.

The acceptable value for page response is very much dependent on the backhaul or LAN technology being used. For example, using a narrowband dial up connection at 56 kbps page response times of 30 seconds would be considered normal. As discussed in Section 2.3, the

most common form of backhaul used in homes and offices is xDSL or DOCSIS (Cable) which run at speeds of up to 50 Mbps. In the simulation environment bottlenecks or contention on the backbone/backhaul network are not modelled. All the effects shown are due to the wireless network. Any additional limitations on the backbone network would only compound the effects seen.

5.5 Conclusions

In this chapter the simulation platform based on OPNET Modeller™ is discussed, which was used to generate results of the performance of the DCF and EDCA MAC layers.

The initial investigation into the capacity of WLAN showed that the maximum throughput using the HTTP service was 5.5 Mbps on an 802.11b WLAN. Recall that the physical layer speed of 802.11b is 11 Mbps, this shows that the achievable throughput is half of the quoted physical layer speed. Network designers should consider the maximum throughput achievable when designing wireless networks

The initial investigation of the DCF Mac layer showed an inverse relationship between throughput and delay. When a network was heavily loaded, the delay for individual clients increased. Quality of Service guarantees in such scenarios are not possible and real time services are shown to suffer. For example in Figure 5.13 the MOS of a VoIP call drops rapidly as the number of clients increase. The implications of this is that the DCF MAC layer is unable to simultaneously support real time services such as VoIP in the presence of non real time traffic such as HTTP or FTP.

The simulations of the EDCA MAC layer show that service differentiation is possible. The shorter AIFS and contention window of real time streams under EDCA give priority when accessing the medium. In Figure 5.16 FTP traffic is simulated simultaneously with VoIP. The results show that EDCA is able to support both real time and non real time services, without

degradation to the VoIP MOS value. Similarly other metrics such as delay remain low for real time traffic, while delay for non real time traffic increases. Further investigation into the priority of real time services shows that the gains of priority are not without sacrifice to non real time services. In the simulation example, VoIP is run simultaneously with HTTP traffic (representative of a typical modern web page such as BBC News). Page response times and object response times are both affected by the VoIP prioritisation when the network is mildly loaded. This has a number of implications as HTTP is generally regarded as a non real time service and is tolerant of variations in delay. However the longer page loading times as shown by simulation would start to affect the end user web browsing experience. Such delays can be further exaggerated by delay and/or congestion on other parts of the network.

It is felt that QoS should be viewed as a requirement across *all* network services and not just those that are considered real time like VoIP. This Chapter has shown that commonly used, non real time services such as HTTP also have constraints in terms of delay and throughput in order to provide an acceptable service. The issue of fairness and priority is discussed further in Subsection 6.5

6 Experimental Results and Data Analysis

6.1 Introduction

In this chapter the experimental research work conducted in the evaluation and implantation of QoS mechanisms in 802.11 wireless local area networks is discussed. The performance of DCF and the enhanced EDCA is investigated through field testing. Service differentiation and fairness aspects of EDCA are compared and contrasted and the effect of frame loss investigated. The Chapter is concluded with the most recent work based on the effect of frame losses on QoS and an application of video streaming over EDCA.

6.2 Field Testing Environment

As with the early simulation work, field testing has spanned a number of years and through this time there have been a number of new developments and changes to the testing environment. Initially the testbed was limited to the legacy 802.11b devices with support for only DCF. As mentioned in Subsection 3.2.2, PCF was very rarely implemented in hardware devices, leaving us limited to simulations only. Technical support was contacted for two major device manufacturers, Proxim and Cisco, both responded that PCF was an optional access method and there were no plans to support it in any of their current products.

6.2.1 Early 3Com DCF 802.11b Testbed

Initially the research was conducted in a wireless laboratory using 802.11b hardware. This consisted of a single 3Com AP8000 access point supporting basic DCF operation. The access point had basic functionality with limited additional features. The AP was connected to the LAN using Ethernet (10 Mbps). The dimensions of the lab were approximately 25m x 8m. As

shown in Figure 6.1 the brown strips indicate the laboratory bench worktops, and the grey marking indicates the position of the 3Com AP8000.

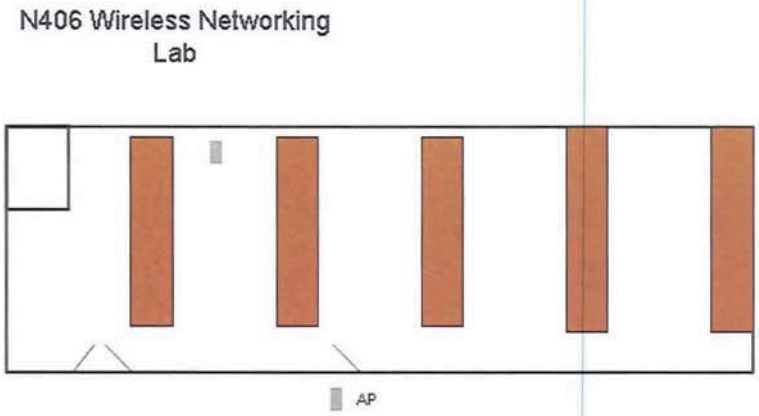

Figure 6.1 - Wireless Laboratory N406 Phase 1

The client machines were Toshiba Tecra laptops (mid specification), equipped with internal 802.11b mini-PCI wireless cards. These client cards were based on the popular PRISM 2 chipset manufactured by Intersil.

This initial testbed was only used for a short period of time at the start of the research and was soon replaced by the designs described in Subsection 6.2.2 and 6.2.3.

6.2.2 Proxim EDCA/DCF 802.11a/b/g Testbed

Due to new hardware becoming available on the market the original testbed was expanded from the basic 802.11b setup to one that supported the full range of PHY layers 802.11a/b/g. The new access points supported a much wider range of functions useful such as:

- Transmit Power Control
- Data Transmission Rate Control

- Advanced Encryption System support through WPA/WPA2
- Partial 802.11e EDCA support through the Wireless Multi Media (WMM) specification.

6.2.2.1 Hardware Environment

Two Proxim AP4000 were configured and installed in the wireless laboratory, shown in Figure 6.2. The dimensions of the lab were the same as measured in Subsection 6.2.1. The brown strips indicate the laboratory bench worktops, and the grey markings the positions of the access points. The older 3Com AP8000 used in Phase 1 of the testbed was removed and no longer used in any testing.

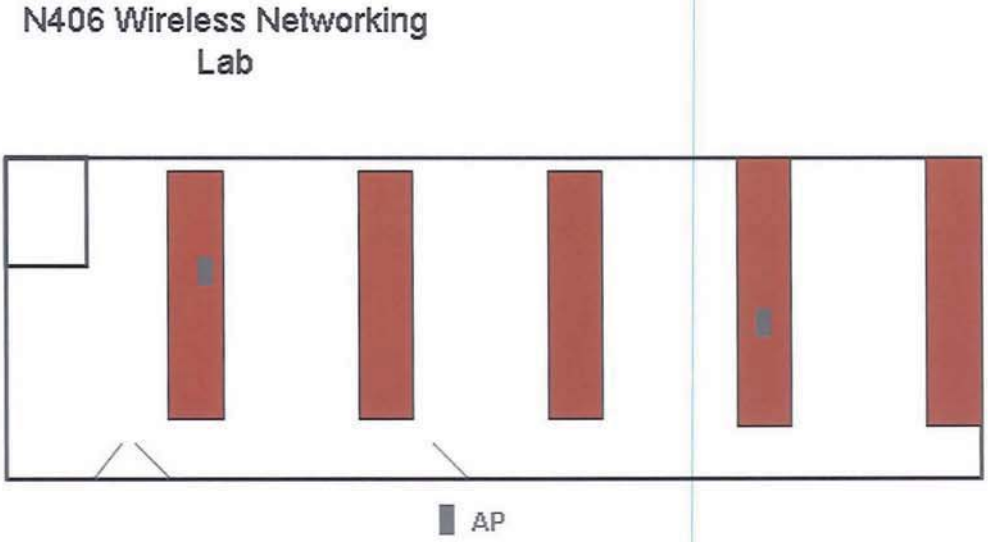

Figure 6.2 - Wireless Laboratory N406 Phase 2

The access points were configured in an Extended Service Set (ESS) configuration on different wireless channels (6 & 11) to prevent any co-channel interference. Fast Ethernet (100 Mbps) connected the APs to the LAN. All of the PHY's, 802.11a, 802.11b and 802.11g were enabled on both access points. This configuration allowed us to disable one of the access

points when required, reverting the topology to a Basic Service Set (BSS), which was used in some of the tests.

The client devices remained the same as described in Subsection 6.1.2.1 with the addition of some devices supporting the newer PHY's. The newer devices consisted of:

- Dell Latitude D600 laptops, which were mid specification featuring mini-PCI 802.11b/g PHY with the Intel BG2200 chipset.
- Proxim ORiNOCO® 11b/g PC Cards based on the Atheros AR5001+ chipset, supporting 802.11a/b/g PHY layers.

The additional PC Cards allowed us to "upgrade" the wireless interface on the Toshiba client laptops, allowing us to use a greater number of clients for tests using the latest OFDM PHY's. In such scenarios, the internal mini-PCI wireless cards were disabled to avoid any conflicts.

In various tests the position of the client stations were moved around the lab area to test a number of different channel conditions. The typical signal to noise ratio (SNR) distribution in the laboratory with both access points is shown in Figure 6.3. The legend for the colour scale is shown in Figure 6.4. Both results were measured using the Ekahau Site Survey tool [88] described in Subsection 6.2.2.2

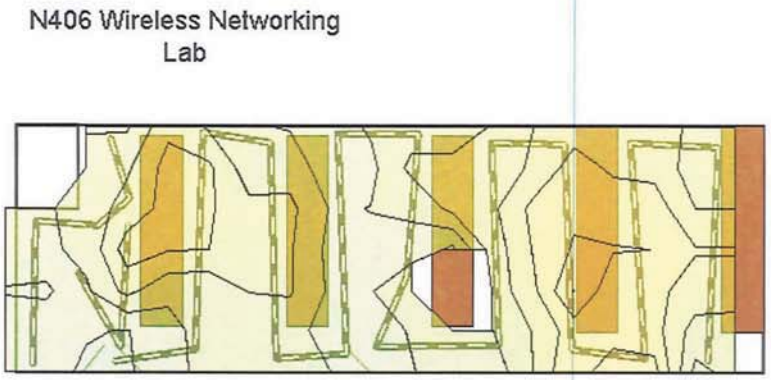

Figure 6.3 - Signal to Noise Ratio Distribution (Dual AP, ESS)

20.0..22.9	22.9..25.7	25.7..28.6	28.6..31.4	31.4..34.3	34.3..37.1	37.1..40.0
40.0..42.9	42.9..45.7	45.7..48.6	48.6..51.4	51.4..54.3	54.3..57.1	57.1..60.0

Figure 6.4 - Signal to Noise Ratio Legend

Figure 6.5 and Figure 6.6 below show the Signal to Noise Ratio (SNR) distribution for the scenario when only a single access point was used, reverting the configuration to a BSS from an ESS. The colour scale is identical to that in Figure 6.4.

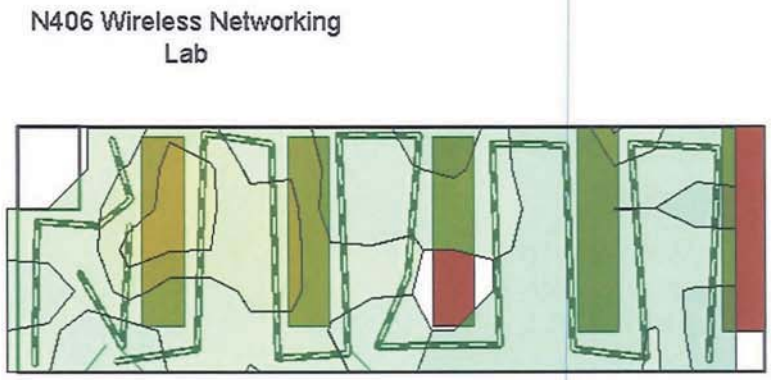

Figure 6.5- Signal to Noise Ratio Distribution (Single Left AP, BSS)

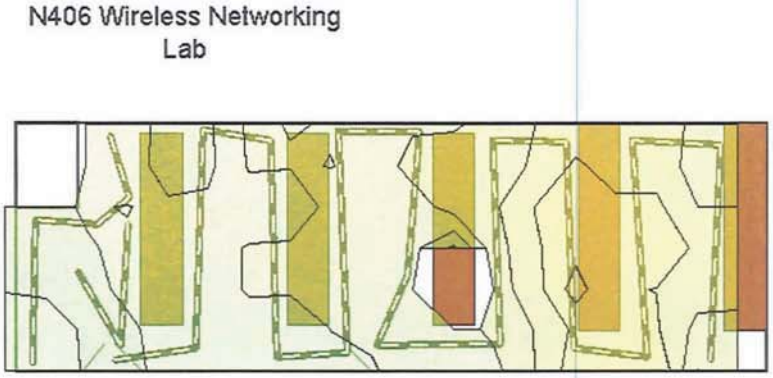

Figure 6.6- Signal to Noise Ratio Distribution (Single Right AP, BSS)

6.2.2.2 Software Environment

QoS metrics such as throughput were measured using the AirMagnet Wireless Analyser [89]. This is a custom software package that runs a laptop using a compatible wireless PC Card, in this case the Proxim ORiNOCO® 11b/g mentioned earlier. The AirMagnet software was used to view details such as:

- Network Throughput and Utilisation
- Signal to Noise Ratio
- Frame Error Rate (CRC errors)

Figure 6.7 shows screen capture of the AirMagnet interface.

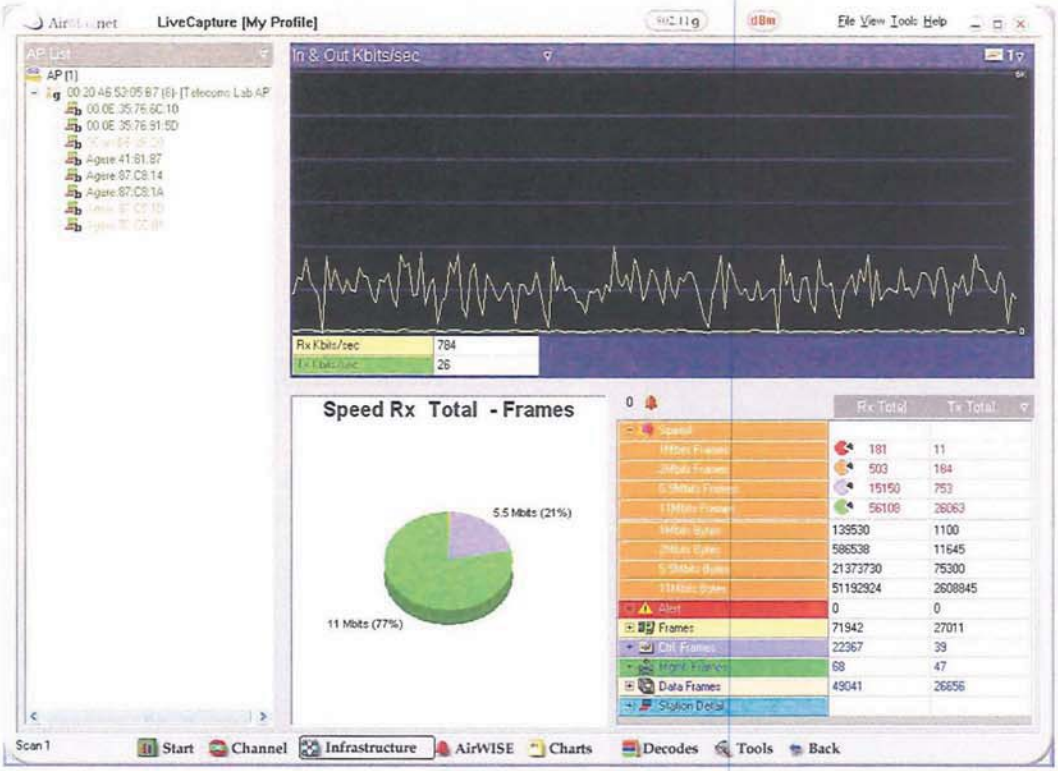

Figure 6.7 - AirMagnet Interface

TCP traffic used for testing was generated by using the HTTP protocol to download a compressed file from a server located on the same LAN. The server was connected to the wireless network via a 100 Mbps Ethernet, so contention on the backbone links was not an issue.

Another software tool used in the testing was the Ekahau Site Survery [88] tool. This is a comprehensive tool than can provide information on Signal Strength and Interference in a real time display. In order to gauge the performance of the testbed setup, the Ekahau software was used to test the signal strength across the wireless laboratory, results of which are shown in Subsection 6.2.2.1 on page 113.

The software runs on a standard laptop equipped with an approved wireless card. The Proxim cards are rated as some of the most reliable and were featured in the Ekahau approved list for use with Site Survey. The site survey interface is shown in Figure 6.8.

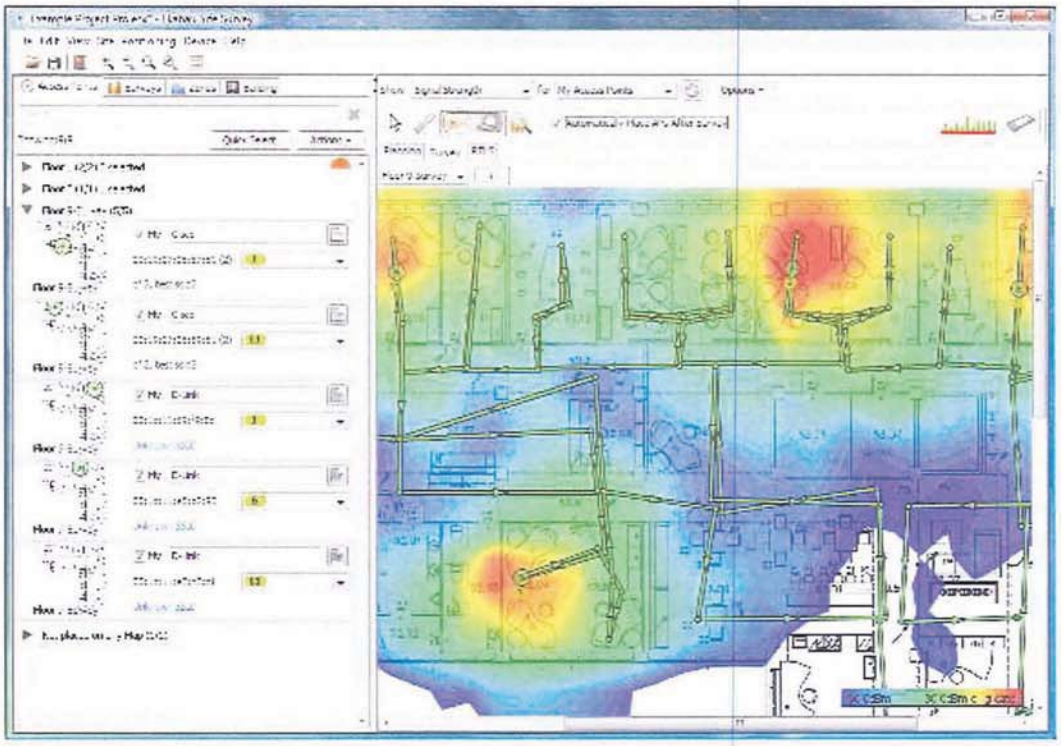

Figure 6.8 - Ekahau Site Survey

As the survey device is moved around, it logs all received signals strengths from APs in range. From this data the site survey the software is able to calculate the following information:

- Signal Strength (dB)
- Noise Power (dB)
- AP availability
- AP dead spots
- AP positioning requirements

The coloured visualisations of the site survey tool were very useful for signal strength measurements as well as indicating areas of co-channel interference.

Another tool used in the testing was the Yellow Jacket Analyser [90] , shown in Figure 6.9.

Figure 6.9 - Yellow Jacket Analyser

This is a combination of custom hardware and software running on a Pocket PC PDA. The device is able to state typical information such as Signal to Noise Ratio (SNR), Access Point details, etc. in addition to a few more specialised measurements like Multipath and Delay Spread. The most useful feature in this device was the portable spectrum analyser function which can show any sources of interference in the 2.4 GHz ISM band. As mentioned previously, interference from other sources can cause significant problems for wireless devices in terms of quality of service.

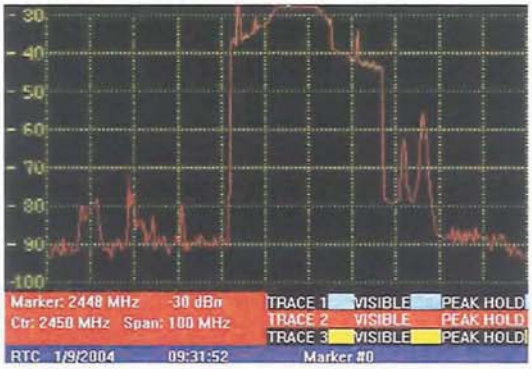

Figure 6.10 - Wideband Interference in the 2.4GHz Band

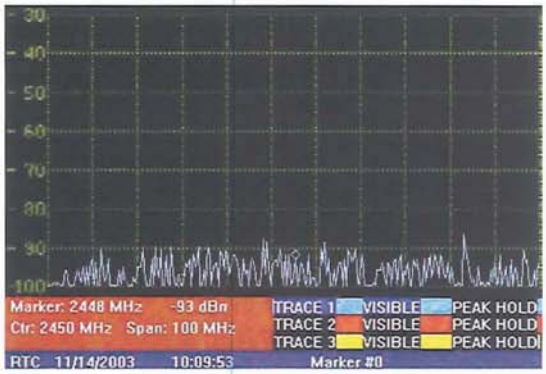

Figure 6.11 - Normal Spectrum in the 2.4GHz Band

In Figure 6.10 a capture from the Yellow Jacket's spectrum analyser mode is shown. The x-axis is the total channel bandwidth in the 2.4 GHz ISM band, the centre point of which is 2.45 GHz. The red line indicates a considerable wideband interference source, effectively blocking out signals from any wireless stations operating on Channel 4 and above. In testing, wireless clients were unable to associate successfully with the access point in the vicinity, leading to a coverage black spot or dead region. It must be noted at this point the interference pattern in Figure 6.10 did not occur in any of the testing laboratories, but at another site where site surveys were being conducted. It was later established that the wideband interference source was a Passive Infrared Detector (PIR) for an intruder alarm system. Figure 6.11 shows a normal frequency spectrum without any interference sources. This reading was taken in the research laboratory.

6.2.3 MADWiFi Linux EDCA/DCF 802.11a/b/g Testbed

Towards the latter part of the research the wireless laboratory was relocated to another floor within the departmental building. The room layout is open plan with a Linux based software access point at a typical desk height of 1m above ground. Using the Yellow Jacket [90] portable spectrum analyser described in Subsection 6.2.2 the test area was checked for any spurious interference that may have affected the experiments. The area was found to have a typical noise power of -85 dBm to -95 dBm, which was within the bounds for an office

environment. There were a number of other wireless networks detected in the near vicinity; however the networks with a high signal power of -50 dBm were operating on channels 1 & 11, while ours operated on channel 6. The other AP's operating on channel 6 had a signal power of less than -80 dBm, giving a SNR of less than 10 dB. The presence of other wireless networks in the testing environment reflected a more typical home/office scenario where other access points are likely to be operating, thus making the testbed more representative of a real world environment.

6.2.3.1 Hardware Configuration

A BSS wireless LAN was established within the research laboratory using a Linux based software access point. A standard desktop PC (specifications given in Table 6.1) was used, which was configured with the Debian Linux operating system (Kernel version 2.6.12). Using a Texas Instruments PCI to PCMCIA adaptor bridge, a Proxim Orinoco 802.11a/b/g card (PCMCIA type) was installed in the desktop PC. This was identical to the type discussed in the previous testbed. Compared to Windows, driver support for wireless devices in Linux has been poor. The cards used were based on the popular Atheros AR5001+ chipset. This allowed us to use the open source Multiband Atheros Driver for WiFi (MADWiFi) to control the radio hardware from the operating system. MADWiFi was originally written by Sam Leffler for the FreeBSD system. Later this was ported to Linux and the source code placed in the public domain. Since then MADWiFi has become one of the most advanced wireless drivers available in Linux [27].

CPU	System RAM	Hard Disk
Pentium 4 2.8 GHz	256 MB	20 GB

Table 6.1 - Linux AP Specifications

The MADWiFi 0.94 drivers were used in Master mode to create a soft access point. Under MADWiFi, the Proxim client card could be used as a conventional Access Point. The laptop clients were also fitted with Proxim ORiNOCO 11a/b/g PC Cards, so the radio hardware was consistent between all devices on the network. RTS/CTS and specific enhancement features such as Turbo G and extended range were disabled.

The data transmission rate was fixed at 54Mbps (64-QAM modulation) using the 802.11g PHY, disabling the auto fallback mechanism. The data transmission rate was fixed (unless stated otherwise) for the tests in order to eliminate any ambiguity introduced by the 802.11 auto-fallback mechanism. For example multiple stations could be operating at different transmission rates, thus making a fair comparison between them difficult. In later tests the effect of altering the data transmission rate in a WLAN on QoS is shown. The testbed setup is illustrated in Figure 6.12.

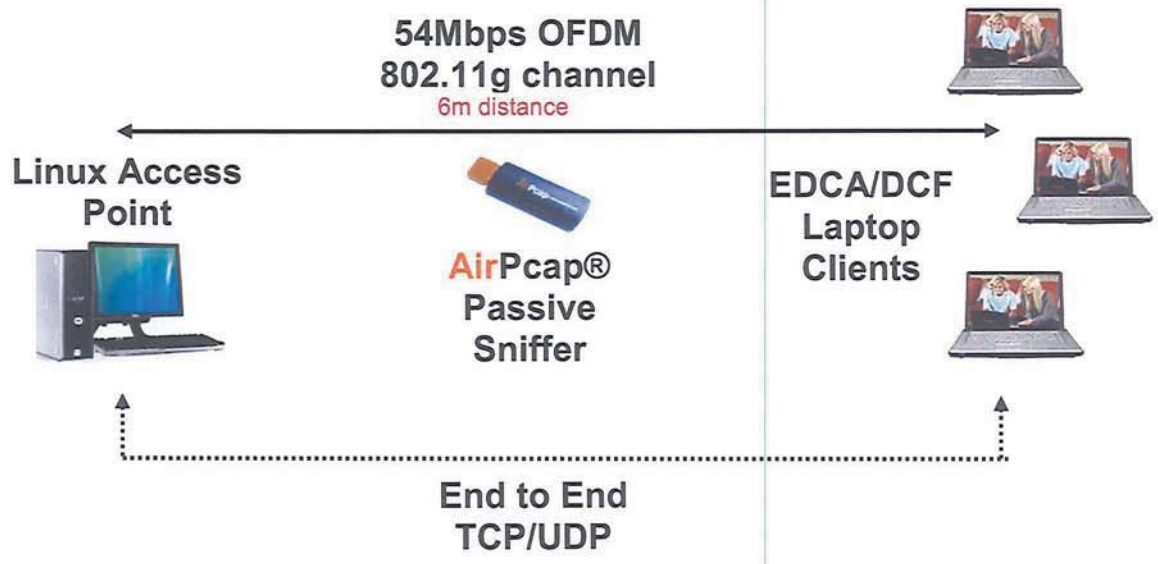

Figure 6.12 - MADWiFi Linux Based Testbed Setup

Figure 6.12 shows the basic testbed setup, on the left is the Linux "soft" AP with three wireless clients. The AirPcap device shown in the diagram is described in the following section. EDCA parameters on the access point were left as default as shown in Table 3.2 and Table 3.3. The Proxim wireless card was bridged with the built in Ethernet interface to allow data frames to be exchanged between the two. The CPU load was measured on the software access point using the *top* command, and the CPU load rarely exceeded 40% under fully loaded traffic conditions. This ensured that the software nature of the access point was not a bottleneck in the testbed.

6.2.3.2 Software Configuration and Integration

The soft access point and clients were both running Debian Linux (2.6 kernel) using the MADWiFi 0.94 drivers. In order to test TCP connections over the testbed, the Iperf utility [31] was used. Iperf is a cross platform traffic generator, for testing the TCP/UDP performance over IP networks. It is capable of reporting the Bandwidth, Delay Jitter and Datagram Loss from traffic generated by itself across a real network. During testing version 2.02 was used under Linux with the default value of 64 k for the TCP receive window, and 1460 byte dummy payloads. UDP settings were also kept at the default of 8 k for the receive buffer with 1470 byte dummy payloads. Traffic streams were categorised into their respected traffic classes by setting the Type of Service (ToS) field in Iperf. This is also known as the Differentiated Services Code Point (DSCP) which is a sub field within the IP header. Using this DSCP code, the MADWiFi driver maps the appropriate DSCP value into one of the four wireless access categories. The classification does not function on a range basis, but on the specific values located in a case statement in the MADWiFi driver source code. The multiple classes and their respective DSCP decimal and hex values are shown in Table 6.2.

Category	Name	DSCP Value (Decimal)	DSCP Value (Hexadecimal)
AC_BK	Background	8/32	8/20
AC_BE	Best Effort	All others	All Others
AC_VI	Video	40/160	28/A0
AC_VO	Voice	48/224/136/184	30/E0/88/B8

Table 6.2 - MADWiFi DSCP to AC Mapping

The AirPcap device was used in conjunction with the Wireshark protocol analyser to capture all of the raw packets from the ether during testing. This is a custom made hardware device manufactured by CACE Technologies [91]. Similar in size to a USB Wireless Adaptor it allows the user to capture raw 802.11 packets (including data, management and control frames) from the wireless medium. The device is completely passive and has the ability to function on all 802.11b and g channels. Before commencing a capture the user is required to select a single channel from which to capture from. More than one channel can be captured by aggregating data from multiple AirPcap devices. Low level headers such as the 802.11 Radio Tap are made available to the user, which is not possible using normal wireless cards, even in *monitor mode*.

To avoid any interaction with the testing procedure, the device was used on a separate high specification desktop PC. The AirPcap device integrates into the popular network protocol analyser Wireshark [92], through the WinPcap [93] libraries. Wireshark's powerful filtering ability allowed us to isolate the required data packets effectively and derive metrics such as delay, throughput and frame loss directly from the captured data. This is done by analysing

the 802.11 sequence numbers, which are used to derive a retransmission distribution for each of the traffic streams. The process and model for this are described later in Subsection 5.3.2.

6.3 Single Traffic FTP DCF Performance

The 3Com testbed was used in a basic BSS configuration using 802.11b DCF. Due to constraints with the amount of equipment available to us, the field testing work could not scale to the levels possible with OPNET. However the effect of the increased load on a network can be demonstrated in this example. The number of clients was increased while a separate machine was used to record the throughput at both Client and AP using the AirMagnet tool. The medium was saturated using the FTP protocol which runs on a TCP transport layer, by downloading a large 4GB compressed image from a server located on the LAN.

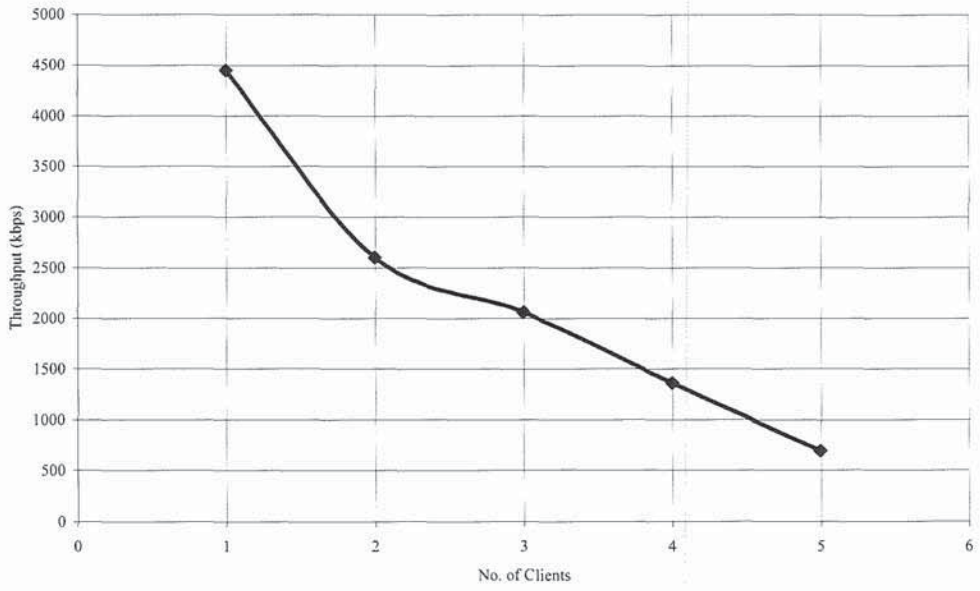

Figure 6.13 - Client Throughput with FTP Traffic

Figure 6.13 shows the FTP throughput of a client in the wireless network. With a single client the throughput is approximately 4.5 Mbps. When another FTP client is added to the network,

the individual throughput is reduced to 2.6 Mbps, just under a half as expected. Due to the shared nature of the wireless medium the available bandwidth is distributed equally amongst all of the stations in the network. Figure 6.14 shows the overall FTP throughput as measured at the access point by AirMagnet. It can be seen that the overall throughput is fairly constant at approximately 5.3 Mbps. This is referred to as the maximum capacity [94] of the wireless network and is similar to that found through simulation in Figure 5.6.

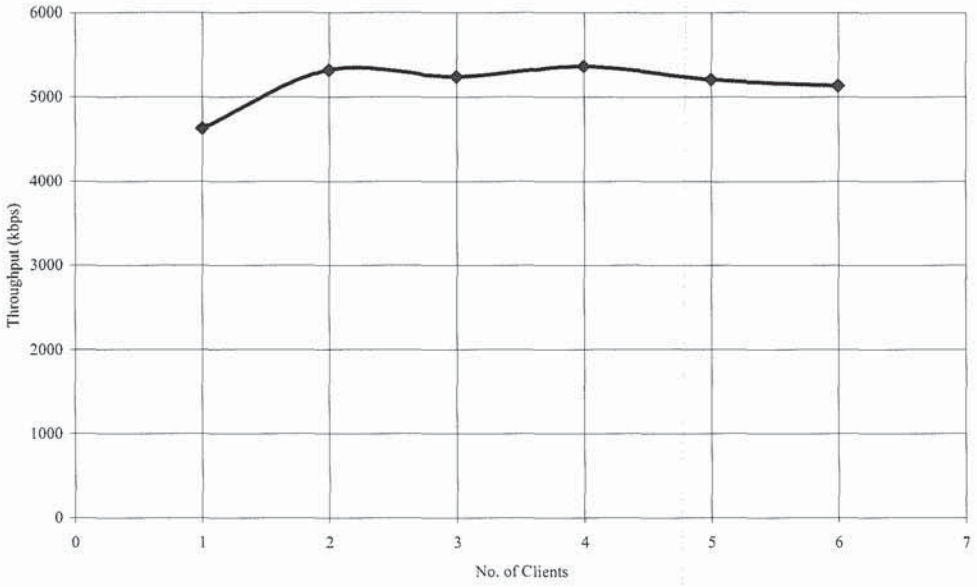

Figure 6.14 - AP Throughput with FTP Traffic

The value of the maximum network capacity is expected to be constant across the same physical layer due to the modulation, framing and spacing overheads being constant in the 802.11b PHY. However the capacity can be affecting by varying channel conditions and any co-channel interference. This is noticeable in Figure 6.14 as the saturated throughput varies slightly as the number of clients increases.

6.4 Effect of Frame Loss on QoS with DCF/EDCA Single Traffic

In this section the effect of frame loss in a wireless LAN on QoS metrics such as throughput and delay is presented. All work is carried out experimentally in real world conditions typical of wireless LAN deployment as depicted in Subsection 6.2.3. The AirPcap device was used in conjunction with the Wireshark protocol analyser to capture all of the raw packets from the ether during testing. The capture file was analysed using a combination of custom scripts and filters. Metrics such as Throughput, Delay and Frame Loss were derived from the capture data.

As described in Subsection 6.2.3 a Linux based AP was used to establish a wireless network in the testing environment. Data transmission rate was set to 54 Mbps, with all enhancement features such as Turbo G and Extended Range turned off.

In Section 4.2 the measure of throughput is introduced as a metric for the quality of service. To date various methods have been developed and introduced to measure throughput at different layers in a protocol stack. MAC layer throughput can be measured with an application such as AirMagnet described in Subsection 6.2.2.2. Transport layer throughput can be measured with a software tool such as Iperf, used extensively in later testing. In this section a new way of deriving the throughput directly from a raw 802.11 frame stream capture is introduced. By capturing all of the 802.11 frames passively during the test using the AirPcap device, then using Wireshark, the required stream is isolated by filtering traffic between the two required MAC addresses. Based on this capture, a combination of filters and custom scripts were used to determine the following:

- Total number of frames sent (at the MAC layer), N.

- Frame retransmission distribution, $R(i)$.
- Frame arrival delay, τ.

The frame arrival delay is defined as the time elapsed between successive data frames at the MAC layer.

The time duration of the data capture, T, was derived from the timestamps in the capture file.

Let $R(i)$ ($i = 1,2,.....n$) be the number of frames being retransmitted i times before they are accepted at the receiver, where n is the retry limit for the device (in this case a value of $n = 10$ is used, as some of the hardware had a non-standard retry limit). If a frame was retransmitted it is assumed that it was lost due to noise, collision or failure to pass the frame check sequence (FCS) at the receiver (discussed in Section 3.5). From this, the total number of frame losses N_l during T is calculated as:

$$N_l = \sum_{i=1}^{n} iR(i) \tag{6.1}$$

The loss rate λ in percent is given by:

$$\lambda = \frac{N_l}{N} \times 100 \tag{6.2}$$

Let N_r denote the total number of frames passed to the higher layer at the receiver. Given the TCP data payload size L_{TCP}, the average TCP throughput η during T can then be worked out by:

$$\eta = \frac{N_r L_{TCP}}{T} = \frac{(N - N_l)L_{TCP}}{T} = \frac{\left(N - \sum_{i=1}^{n} iR(i)\right)L_{TCP}}{T} \tag{6.3}$$

This calculation was based on the assumption that the last retransmission was successful. The captured value of N_r was compared with the calculated result N - N_l as given in (6.3) and (7.1), and it was found that they were identical.

In the first test using TCP traffic, the performance of both DCF and EDCA MAC layers are tested while increasing the number of wireless clients. The wireless clients had an average signal to noise ratio (SNR) of 46 dB at a fixed 3m distance from the access point. Figure 6.15 shows the average individual and overall TCP throughput.

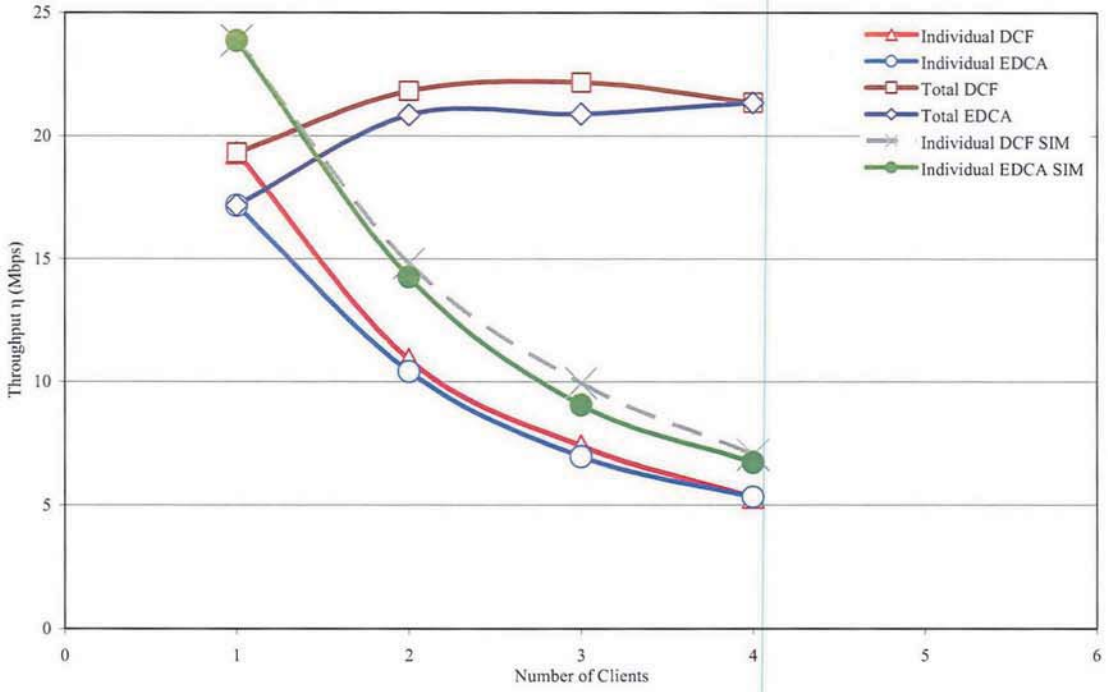

Figure 6.15 - Total and Individual TCP Throughput

As expected, there was a significant drop in individual TCP throughput as the number of clients increase. This is due to the shared medium in 802.11 and the distribution of radio resources amongst the contending clients. There is also a 5% difference in performance between DCF and EDCA with a single client. This difference is attributed to the larger default contention window for the Best Effort traffic class. The empirical test was also simulated in OPNET Modeller™, focussing only on the effect of contention, using a perfect channel. From the result in Figure 6.15 it can be seen that the simulated throughput is higher than that found through experimentation. This reinforces the point that frame losses are present even in good channel conditions. As shown later in this section, frame losses can be directly responsible for

the throughput over a wireless network. When a loss occurs, the sender does not receive a positive ACK (discussed in Section 3.2), resulting in the ARQ mechanism retransmitting. The overhead of retransmitting data reduces the efficiency of the system.

A single retransmission can be regarded as the effect of independent random errors on the channel. This could also be attributed to the increased contention effect created by increasing the number of stations. Burst errors are classified by retransmission of two or more consecutive frames of the same sequence number.

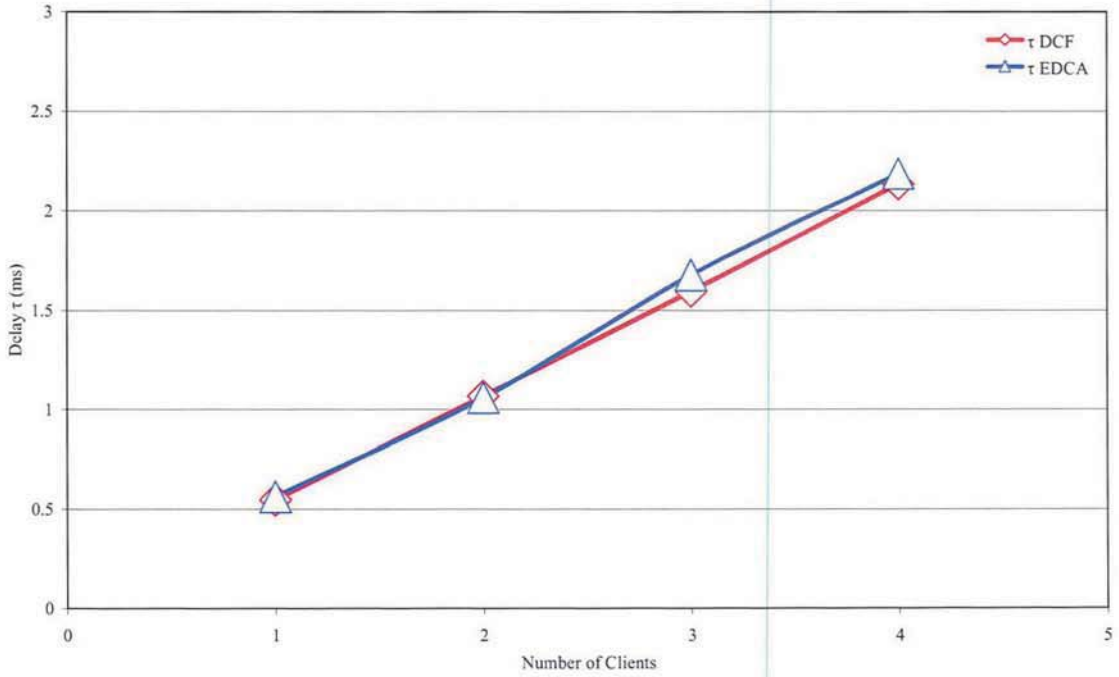

Figure 6.16 - MAC Delay with Increasing Load

In Figure 6.16, the effect on the MAC layer delay τ is shown as the number of TCP wireless clients is increased. This was calculated by averaging the time difference between successive accepted frames on the passive frame capture. A clear linear relationship is observed between MAC delay and the number of clients. The model can be extrapolated to predict the MAC delay for more than 4 clients. Note that this is only a measure of the MAC layer delay and does not include any processing delay.

Moving on to the second test, the correlation between signal to noise ratio (SNR) and throughput is shown. This test involved moving the client device, further away from the AP, therefore reducing the SNR. The test results exhibit a positive correlation between SNR and throughput as shown in Figure 6.17. In the field test the throughput dropped to 0 at the point around 17dB. The received power below this point was below the receiver sensitivity.

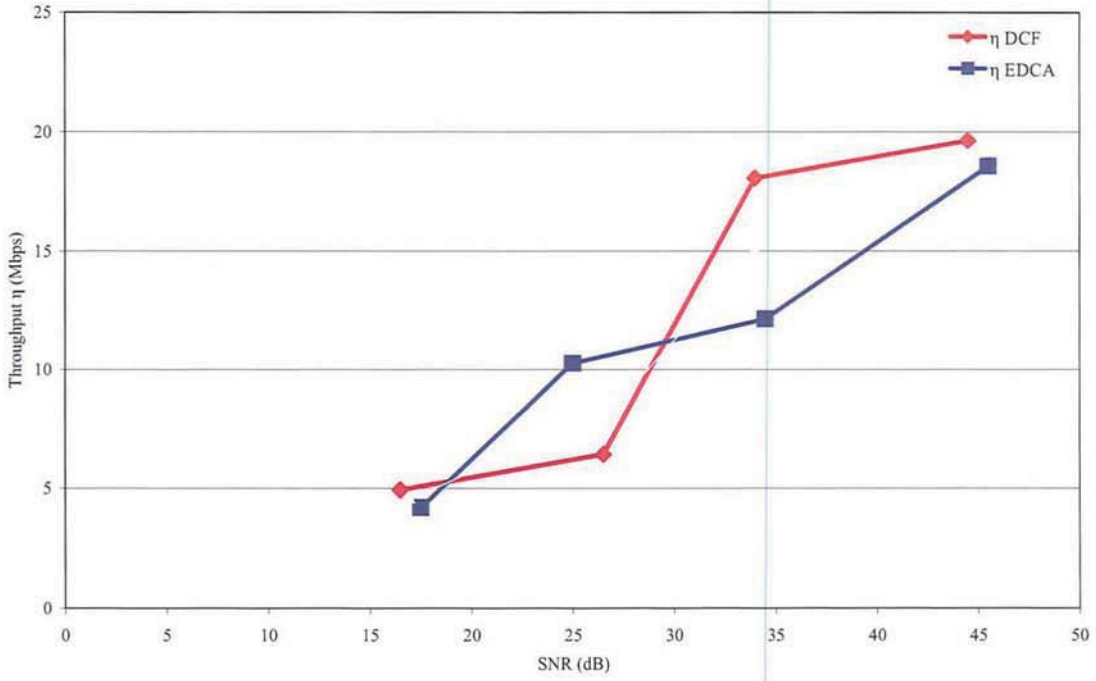

Figure 6.17 - SNR vs. Throughput

The result in Figure 6.17 is specific to the 64QAM modulation scheme for the data rate at 54 Mbps (discussed in Subsection 2.1.2). If the AP is set to a slower PHY (e.g. 9 Mbps BPSK), it can be expected to communicate at a lower SNR at the expense of throughput. This is due to the lower spectral efficiency of the modulation scheme. This is an area of further work that is mentioned later in this chapter. QoS requirement for throughput at a higher layer can be converted into physical layer requirements such as SNR. This can be useful for planning and

design of a WLAN where the requirement at the higher layer (e.g. throughput) and lower layers (e.g. SNR) will be jointly considered.

The retransmission distributions $R(i)$ for different scenarios in terms of distance or SNR are shown in Figure 6.18 & Figure 6.19. Lower SNR at the receiver as the distance from the AP increases causes frames to be lost or corrupted. This in turn triggers the ARQ mechanism to retransmit the frame a number of times. In Figure 6.18 & Figure 6.19, it can be seen that when SNR is high, a frame is mostly retransmitted once or twice if required, while the number of retransmissions required increases significantly with distance when the SNR is lower. The differences between the distributions for EDCA and DCF are attributed to varying channel conditions as the tests were conducted sequentially. Also there is little to differentiate between the two access mechanisms as the TCP streams were sent in the AC_BE (Best Effort) for EDCA, providing no prioritisation. Later in this chapter the test is expanded to show the distribution in different access categories.

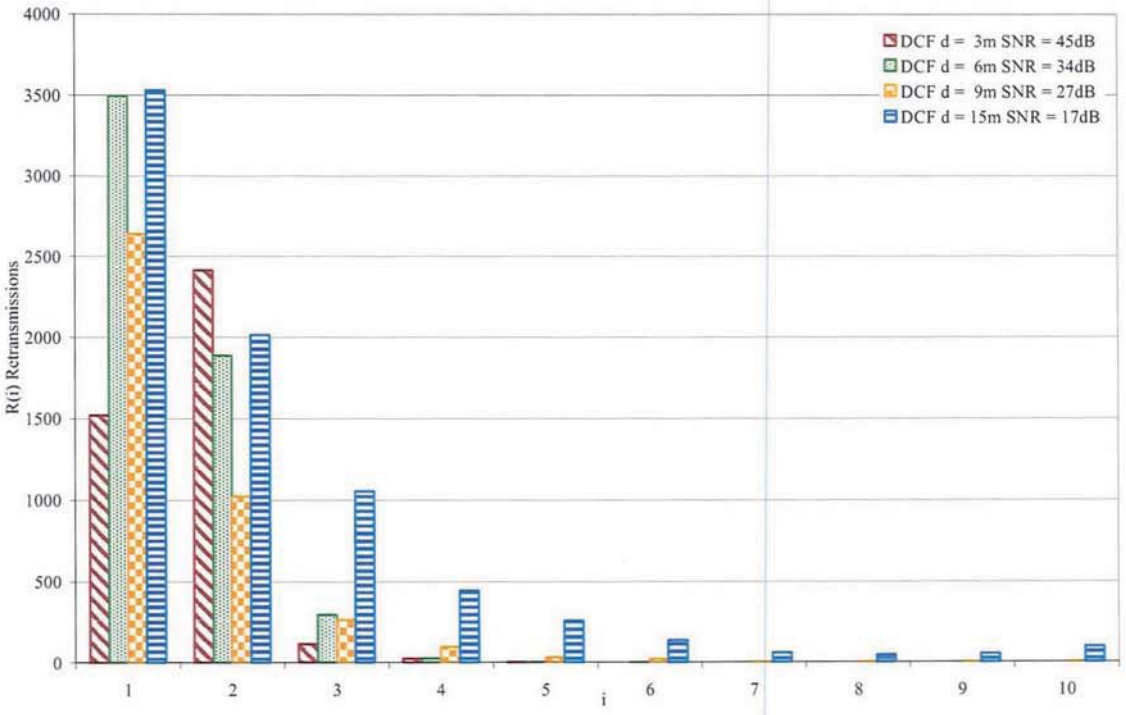

Figure 6.18 - DCF Retransmission Distribution

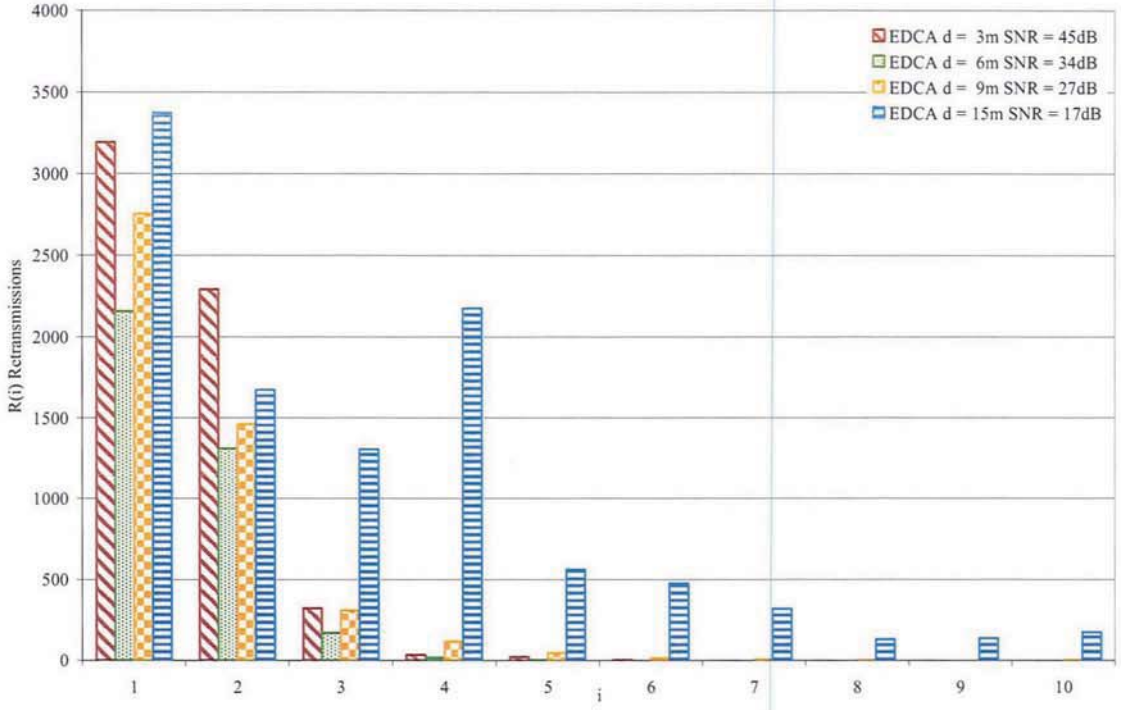

Figure 6.19 - EDCA Retransmission Distribution

In the final test the effect of frame loss on a 2Mbps UDP traffic stream is demonstrated. The stream is indicative of a high quality MPEG video being streamed from a server to a client via UDP. The payload size is set to a default value of 1470 bytes. Both DCF and EDCA MAC protocols are tested. Note that no background traffic was present on the link during the test. The UDP throughput η, was calculated using the same principle as in (6.3) for TCP except for the default payload size: L_{UDP} = 1470 bytes as given by:

$$\eta = \frac{\left(N - \sum_{i=1}^{n} iR(i)\right)L_{UDP}}{T} \tag{6.4}$$

As there was no fragmentation, the calculated UDP throughput η, from (6.4) was identical to that measured at the transport layer by iPerf. The total frame length (UDP payload and headers) is defined as: L_{FRAME} = 1572 bytes. The data transmission rate γ, which includes the retransmitted frames, is defined by:

$$\gamma = \frac{N L_{FRAME}}{T} \tag{6.5}$$

From the data in Figure 6.20 it can be seen that the UDP throughput η remains relatively constant at 2 Mbps for both MAC protocols. However, the UDP data transmission rate γ increases rapidly at low SNR values, due to the increased number of retransmissions through the ARQ mechanism. At high SNR values, there are far fewer retransmissions required, so the difference between the data transmission rate and UDP throughput is significantly reduced.

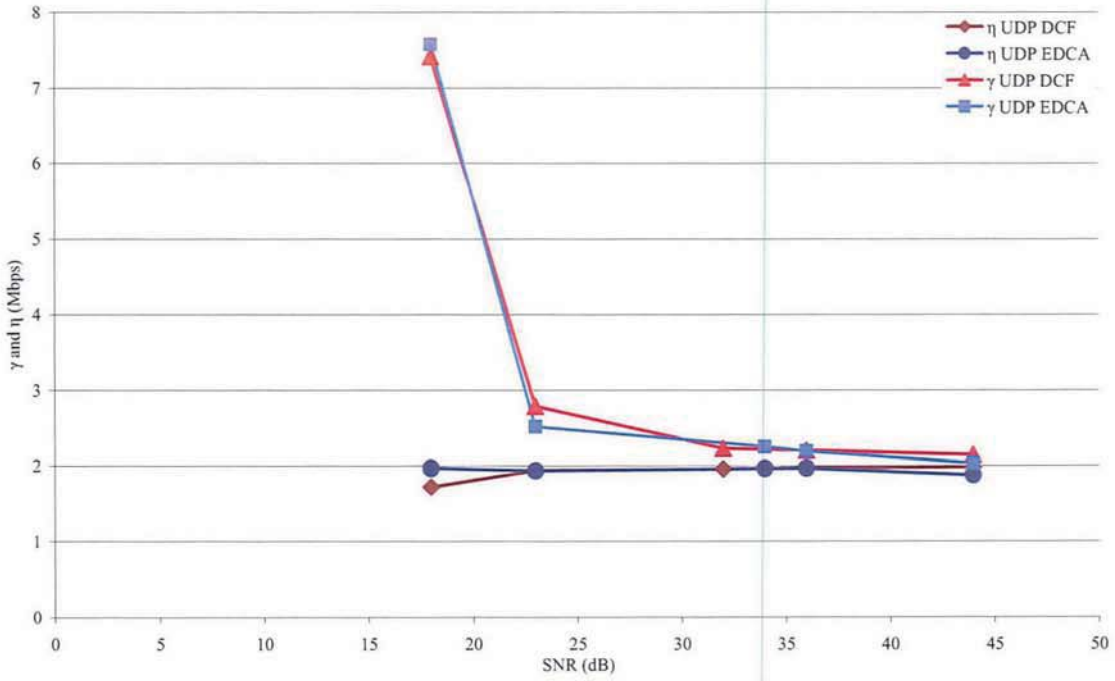

Figure 6.20 - UDP Transmission Rate and Throughput

Figure 6.21 shows the frame loss rate for the UDP test. The frame loss rate shown in Figure 6.21 is synonymous with the transmission rate shown in Figure 6.20. In Figure 6.22 the packet loss rate at the transport layer for the corresponding SNR values is given.

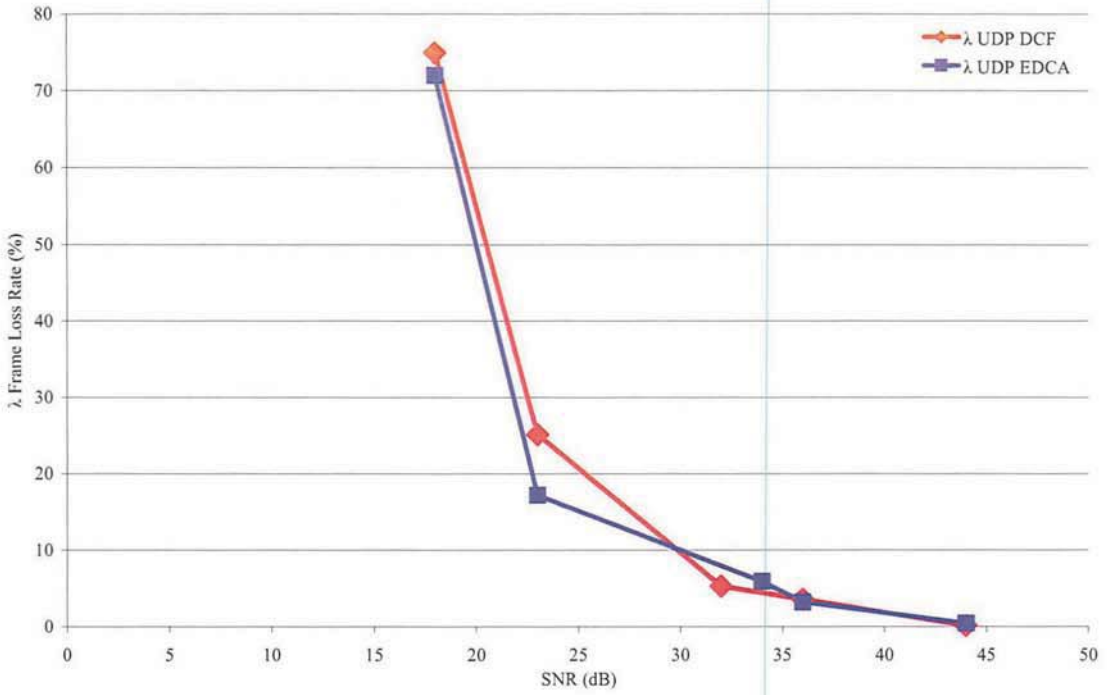

Figure 6.21 - UDP Frame Loss Rate

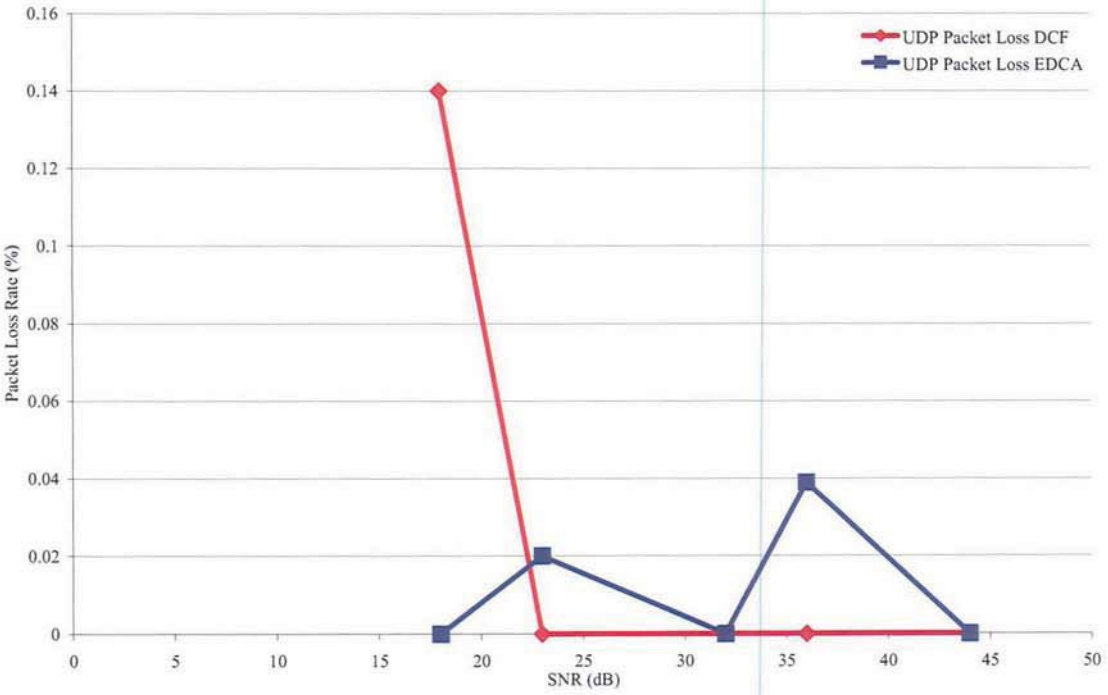

Figure 6.22 - UDP Packet Loss Rate

The most striking result to emerge from the data is that the large frame error rate has a very small effect on packet loss rate, even at low SNR values. The ARQ function at the MAC layer

is able to retransmit the majority of the lost frames with the relatively low rate UDP stream of 2 Mbps.

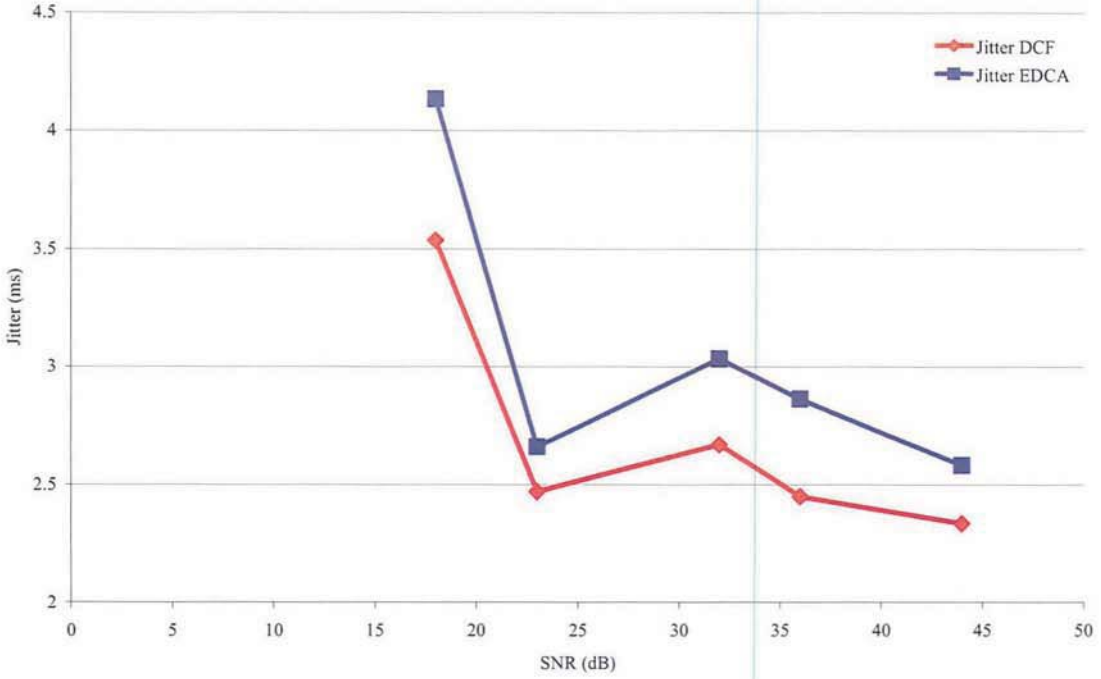

Figure 6.23 - UDP Jitter

However, the packet jitter (variation in delay) in Figure 6.23 shows an increase at low SNR values. Although the packet losses are small they can have considerable effect on a video stream, causing video corruption or frame freezing. More information on video streaming over wireless networks is presented in the later in Section 6.7. In the case of higher bit rate UDP streams, the MAC layer is unlikely to be able to cope with a large number of retransmissions; and consequently large scale packet loss is likely.

The tests in this section have shown that TCP throughput was greatly affected by frame loss caused by low SNR values. With a single TCP stream, legacy DCF and EDCA were both affected by retransmissions and shown to have similar performance, with little difference between them. Multiple TCP streams of different priority are tested in the following section.

The effect on relatively low rate UDP streams was limited as the ARQ mechanism in the MAC layer was able to recover the majority of losses. Further work needs to be done to establish whether the MAC layer can recover from losses in a high bit rate UDP stream, without affecting delay and jitter.

6.5 Investigation of EDCA Service Differentiation and Fairness

Previously in the simulation results presented in Section 5.4, it was shown how the EDCA MAC layer has the ability to prioritise real time traffic over non real time traffic. In the simulation example VoIP traffic was sent in the highest AC_VO (Voice) category, while HTTP traffic was sent in the AC_BE (Best Effort) category. As the network resource i.e. traffic capacity of a network is fixed, the prioritisation of VoIP must come at an expense to other lower priority traffic. The aim of the EDCA MAC protocol was to provide service differentiation between different classes of traffic. This goal is achieved, but in a manner considered to be *unfair* to lower priority traffic. Fairness in terms of service differentiation can be defined as the ability to provide a service to all access categories, without starving or denying a particular type.

In this section it is shown that traffic in the AC_BE (Best Effort) and AC_BK (Background) categories are throttled back vigorously in order to accommodate traffic in the higher AC_VO (Voice) category. There should be a balance between providing service differentiation and ensuring fairness across *all* traffic categories in the network. This section focuses on the fairness and differentiation between the different EDCA access categories as described in Table 3.1. As described in Subsection 6.2.3, the testbed is based on the MADWiFi setup using a software AP running Debian Linux. The TCP testing parameters remain consistent with other tests, a 64k receiver window combined with the TCP-Reno flavour. The DSCP field (as

described in Table 6.2) is used to control the priority of the TCP flows generated by the Iperf application. Throughput is measured directly from the Iperf application and screen output logged and imported into the spreadsheet application Microsoft Excel. The frame capture method described previously, is used to calculate the throughput as shown in Equations (6.1-6.3) in the previous section.

Figure 6.24 shows the effect of service differentiation on three concurrent TCP streams, each set with a different access category.

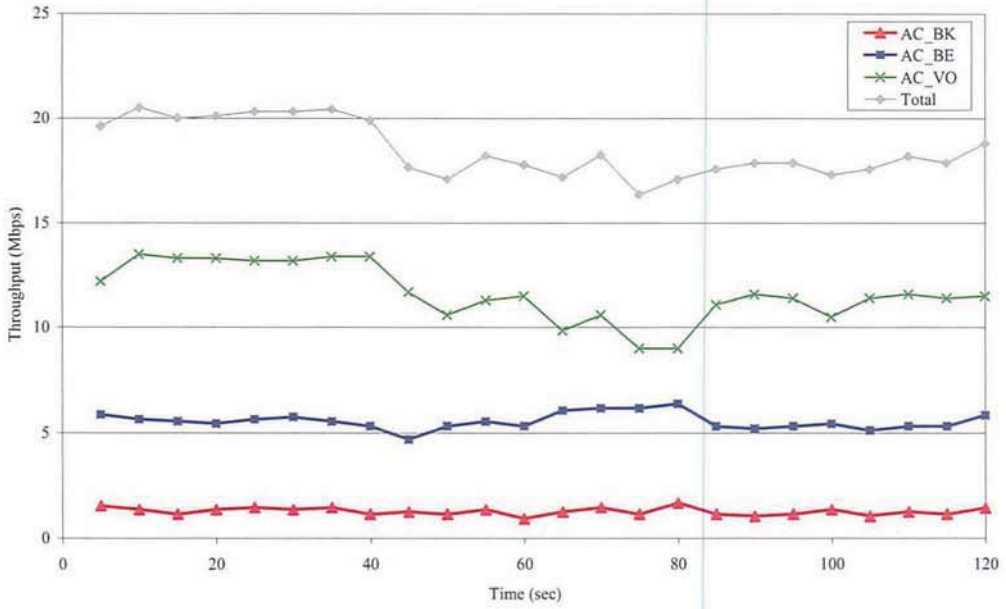

Figure 6.24 - TCP Throughput in Different Access Categories

The results are limited to three access categories instead of the total four, as only three EDCA capable Atheros wireless cards were available at the time of testing. As can be seen from Figure 6.24, the voice category (AC_VO) has the highest throughput, followed by Best Effort (AC_BE) and then Background (AC_BK). This is a direct result of the contention window sizes and interframe spacing dictated in the standard. The service differentiation function of

EDCA is clearly visible, allowing multiple services to be supported with varying levels of QoS in terms of TCP throughput.

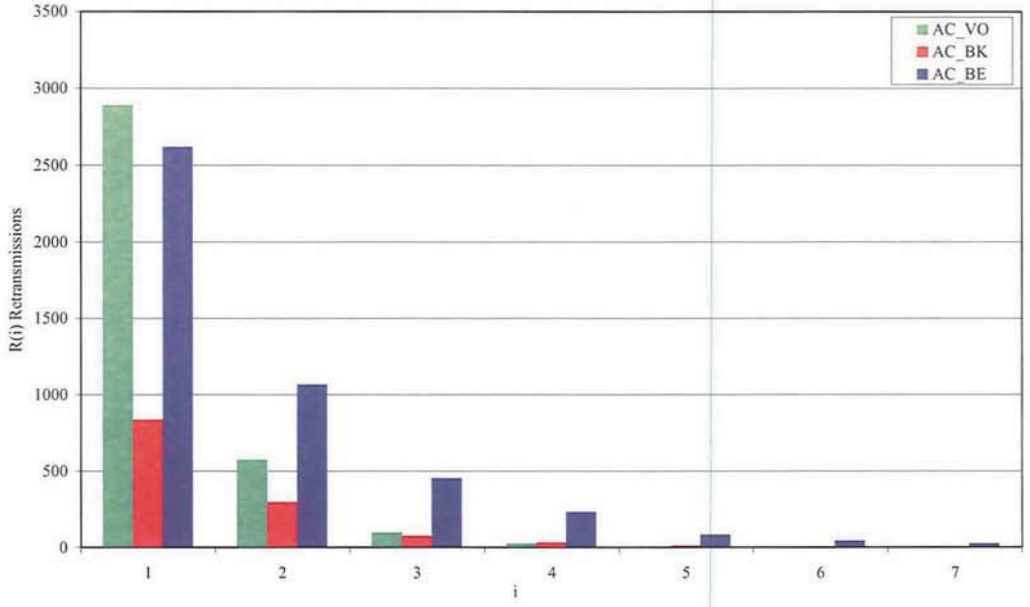

Figure 6.25 - EDCA Retransmission Distribution

Figure 6.25 shows the retransmission distribution from the same test shown in Figure 6.24. This was derived by capturing all the frames and their sequence numbers transmitted on the wireless channel. Using a custom script a frame retransmission distribution is produced, showing the number of frames retransmitted on a per stream basis. As seen from the distribution in Figure 6.25 the AC_VO category has the greatest number of frames accepted with a single retransmission. The lower priority streams, AC_BE and AC_BK suffer from multiple retransmissions, resulting in a lower overall throughput.

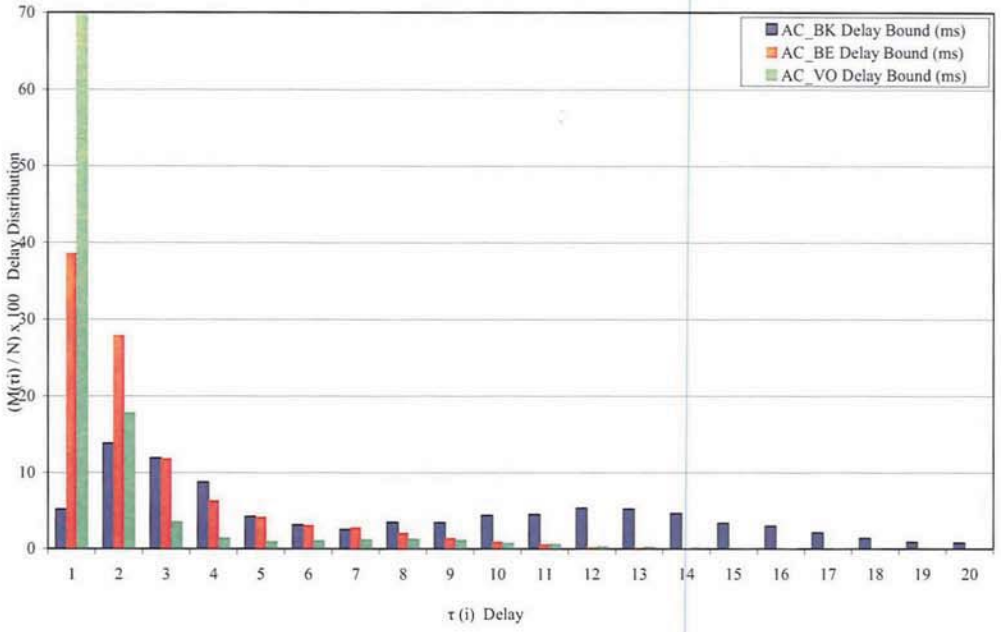

Figure 6.26 - EDCA Delay Distribution

By using the microsecond timestamps on each frame in Wireshark, a delay distribution, as shown in Figure 6.26 is produced. Again the effect of prioritisation on the MAC layer delay is observed. The highest priority AC_VO spends the least time contending for the medium; hence almost 70% of the total frames have a MAC delay of less than 1ms. Comparing this to the lowest priority AC_BK which contends for the medium longer, a much wider distribution of delay is observed. About 35% of AC_BK frames fall into the 2ms to 4ms range. More significantly the spread of delay, i.e. the jitter, is far greater in lower priority streams. This can have a considerable effect on time sensitive applications such as VoIP. From the delay distribution the MAC delay expectation per access category is calculated. Here $M(\tau_i)$ is the total number of frames sent within delay bound τ_i, while N is the total number of frames sent.

$$E(\tau) = \sum_{i}^{n} \left(\frac{M(\tau_i)}{N} \tau_i \right) \tag{6.6}$$

Using equation (6.6) the delay distribution can be calculated to give the expected frame delay per access category as shown in Table 6.3.

Category	Name	Expected Frame Delay (τ)
AC_BK	Background	9.03 ms
AC_BE	Best Effort	2.65 ms
AC_VO	Voice	1.84 ms

Table 6.3 - Expected EDCA Delay

The expected frame delay as shown in Table 6.3 is critical in the performance of time sensitive applications such as VoIP and interactive video. Higher delay figures at the MAC layer can translate into much larger values at the application layer, causing significant problems in the operation of any interactive applications.

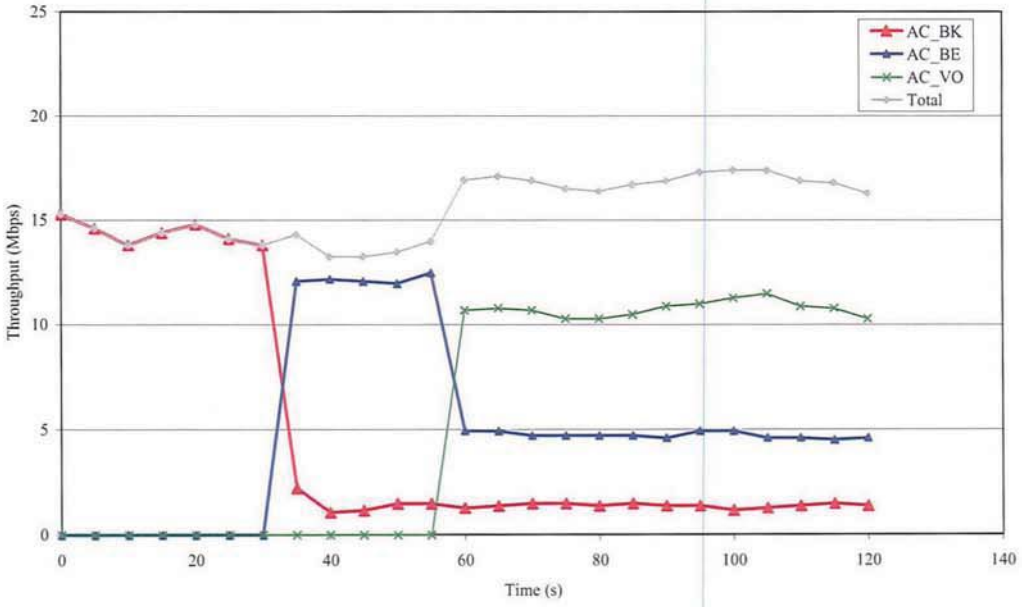

Figure 6.27 - Individual EDCA TCP Throughput

In Figure 6.27, with a background TCP stream (AC_BK) already in operation, a higher priority (AC_BE) TCP stream is introduced at t = 30 second. The previous background stream is now throttled back substantially as it contends for the medium with the AC_BE priority stream. TCP bandwidth is reduced from 14 Mbps to approximately 1 Mbps. At t = 60 second,

when the highest priority AC_VO stream is started, again the prioritisation occurs, as the AC_BE stream is throttled back. An interesting aspect of this is that the overall throughput is increased in the presence of the AC_VO stream. This is due to the smaller minimum contention window size (CW_{min}) allowing for greater medium utilisation. The background category, AC_BK suffers greatly in terms of both throughput and MAC delay. AC_BE is less affected, but still suffers a considerable drop in throughput.

While the AC_BK category is intended for low priority non time sensitive traffic, and AC_BE for best effort, a throughput reduction of such magnitude could significantly effect data intensive applications such as peer to peer (P2P) and streaming TCP video such as YouTube and BBC iPlayer. In the latter case of streaming TCP video, which has become very popular in recent years [95], end users would experience longer initial buffering delays and possible breaks in playback due to the limited bandwidth available. The recommendation is that only low throughput services such as VoIP be placed in the AC_VO category, to limit the effect on lower priority streams. In the case of multiple high priority streams and/or stations, the throttling effect is expected to be even greater.

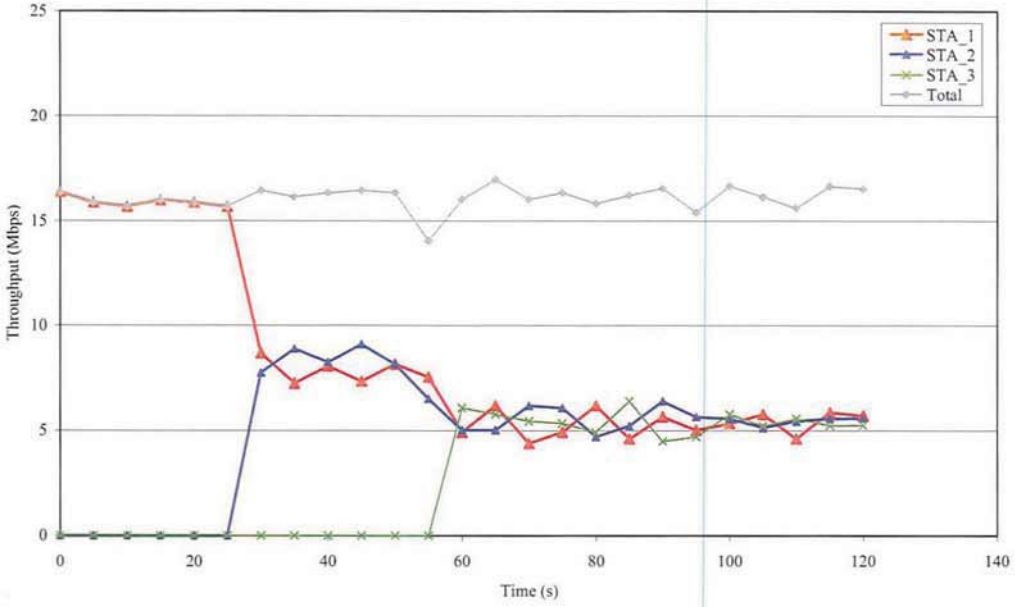

Figure 6.28 - Individual DCF Throughput

Figure 6.28 demonstrates the effect of introducing 3 TCP streams using legacy DCF at t = 30 and t = 60 seconds. It can clearly be seen that the lack of service differentiation results in the individual stations sharing the available bandwidth equally. The overall bandwidth remains relatively constant at just over 15 Mbps. The retransmission distribution for the DCF test is shown in Figure 6.29. All 3 stations have similar retransmission characteristics, resulting in similar throughput and delay figures.

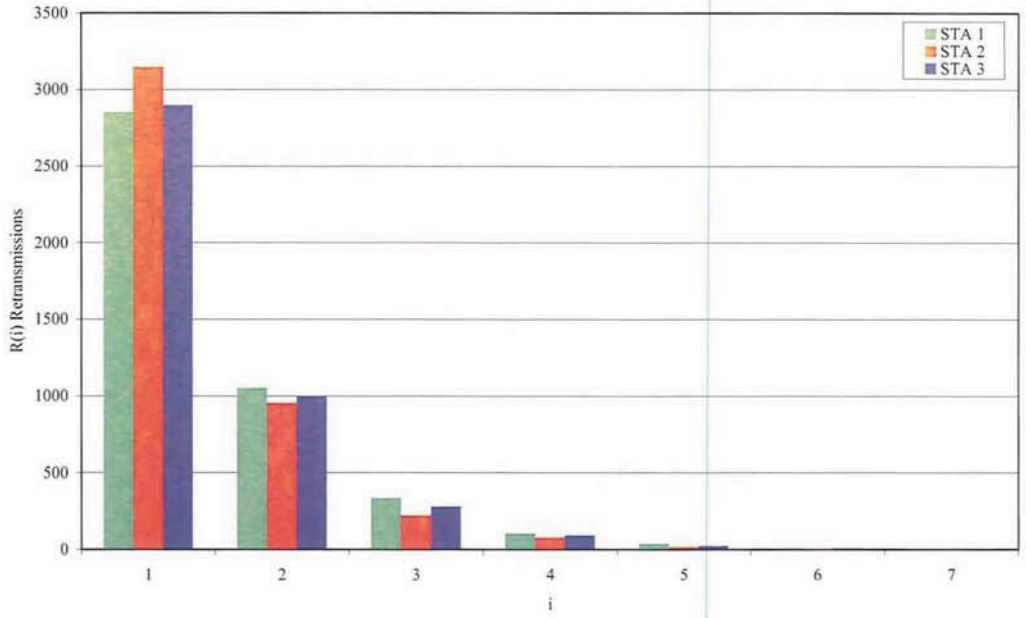

Figure 6.29 - DCF Retransmission Distribution

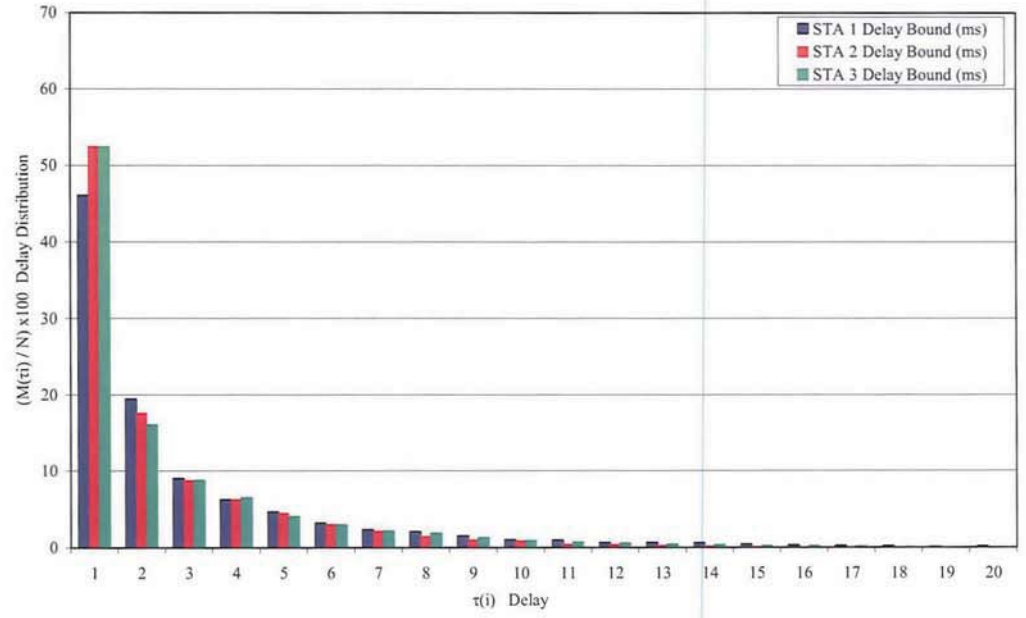

Figure 6.30 - DCF Delay Distribution

Again using equation (6.6) and the delay distribution in Figure 6.30 calculated for the stations in the DCF test, the expected frame delay is derived and shown in Table 6.4.

Name	Expected Frame Delay (τ)
Station 1 (STA 1)	3.00 ms
Station 2 (STA 2)	2.48 ms
Station 3 (STA 3)	2.65 ms

Table 6.4 - Expected DCF Delay

Comparing the performance of EDCA to DCF, it can be seen that the AC_BE, best effort category has similar characteristics to the results in DCF in terms of MAC delay and throughput. The AC_BK category suffers from considerably worse performance than DCF in the presence of other higher priority streams. For example, the lowest priority stream in the AC_BK category suffers from 80% lower throughput and 300% higher delay when compared with DCF. A possible solution to this would be to modify the EDCA contention window timings to introduce more fairness between the four access categories.

In this section the service differentiation capability of IEEE 802.11e EDCA in a real world wireless network has been presented. The experimental work has demonstrated that guaranteed QoS, in terms of delay and throughput can be provided to high priority traffic at the expense of the performance of lower priority traffic.

The results from the testing show that high priority traffic using the EDCA can reduce MAC delay by 30% and maintain a throughput of over 10 Mbps in the presence of two lower priority streams. The negative aspect of this is that the lowest priority stream in the AC_BK category suffers considerably in both throughput reduction and delay increase, compared to the results in DCF under a similar mixed traffic scenario. While EDCA and the AC_VO

category is shown to provide excellent performance and differentiation, the use of this category for "bandwidth heavy" services such as FTP, P2P and HTTP for Downloading could have dire consequences for the QoS across the network. The services mentioned are TCP based, resulting in all available network bandwidth being used up on one category i.e. an unfair distribution of network resources. Users of lower priority AC_VI, AC_BE and AC_BK would see their available bandwidths severely throttled, resulting in a degraded QoS, through excessive retries and higher layer timeouts.

The recommendation is to strictly reserve the use of the highest priority AC_VO category for low data rate, time sensitive traffic, i.e. VoIP based protocols. This would ensure that the VoIP packets are treated with the highest priority, while their relatively small size would ensure that other lower priority users get a fair share of the network resources. The use of the AC_VO category for other TCP based traffic has the effect of throttling throughput significantly for the other access categories, resulting in unfairness and a poor overall network QoS. Further work is required to assess the number of VoIP calls that can be carried in the AC_VO category, before service degradation occurs to other lower priority network users.

6.6 Transmission Rate versus Frame Loss Analysis

In this section a short investigation into the relationship between frame loss and throughput with different data transmission rates is presented. As discussed in Subsection 2.1.2 the 802.11 standard specifies a number of different physical layers that use different frequencies and modulation techniques. In this investigation the focus is on the 802.11g specification that utilises OFDM on the 2.4 GHz ISM band.

The 802.11g protocol features an auto fallback mechanism in order to select the best transmission rate for the given channel conditions. As discussed in Subsection 2.1.2 each transmission rate, shown in Table 2.4 uses different forms of modulation and coding. The higher transmission rates utilise higher level modulation and higher rate coding methods in order to fit more data into a given bandwidth channel, at the expense of making them more prone to errors. The fallback mechanism reduces the data transmission rate to a lower but more robust rate if there are excessive errors on a channel.

The MADWiFi testbed is used as described in Subsection 6.2.3 with one change. Previously in tests the data transmission rate was fixed at 54 Mbps at the access point to intentionally disable the auto rate fallback mechanism as this would interfere with the measurements of throughput. In this series of tests the data transmission rate at the access point is altered. This is instrumented by a simple command line instruction to the MADWiFi driver. The wireless client was stationary approximately 5m from the access point with near line of sight on the radio path. Signal to Noise ratio (SNR) was constant throughout the tests.

As with previous sections, the throughput is measured from the Iperf application in addition to calculating the throughput from the retransmission distribution. The typical frame error rate per data transmission rate is also calculated.

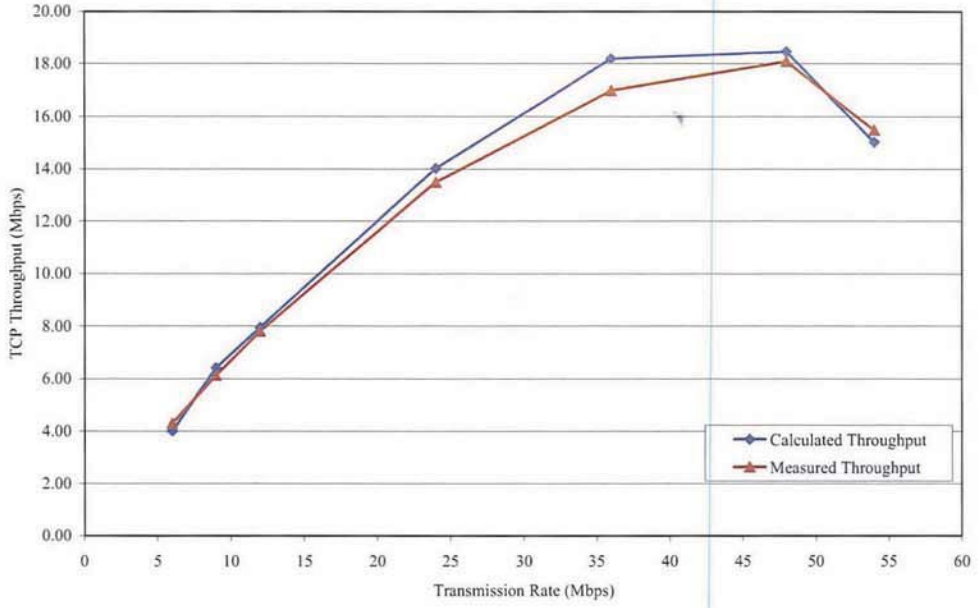

Figure 6.31 - TCP Throughput with Varying Transmission Rate

In Figure 6.31 the TCP throughput is shown against the standard 802.11g data transmission rates. As expected the TCP throughput is directly related to the data transmission rate as the higher transmission rates have a greater spectral efficiency. From the results the calculated throughput is compared against that shown by the Iperf software. Both are very similar with the small difference being allocated to the fact that the AirPcap device may not have been able to capture every frame. It is interesting to note that the trend is not completely linear and that the TCP throughput at the 54 Mbps transmission rate is lower than that with 48 Mbps and 36 Mbps. For more clarification the reader is referred to Figure 6.32.

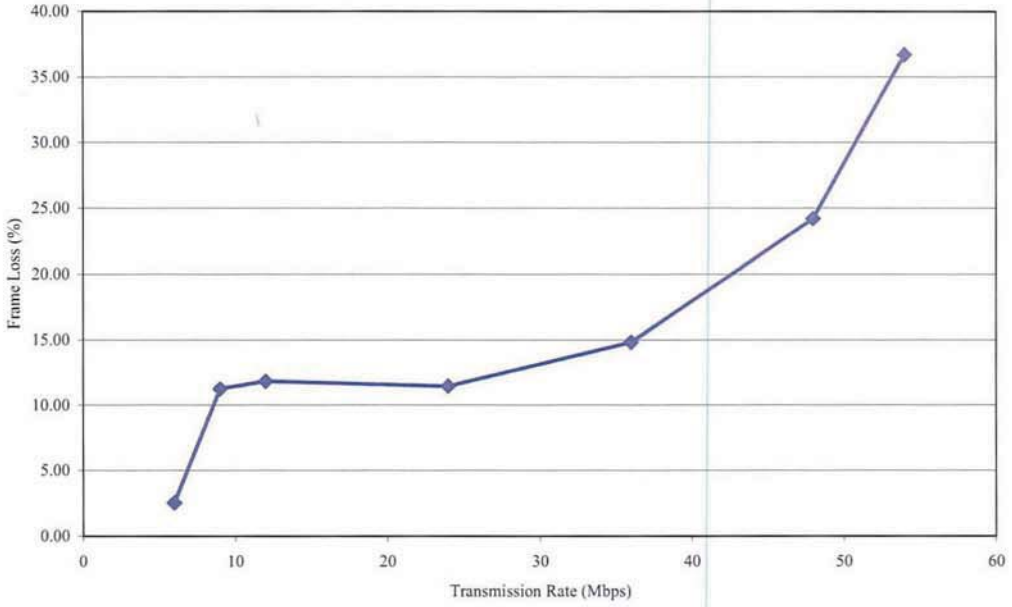

Figure 6.32 - Frame Loss vs. Transmission Rate

In Figure 6.32 the frame loss percentage for each transmission rate is shown. The loss represents frames that either had to be retransmitted or failed to pass the frame check sequence. The 54 Mbps transmission rate has a frame loss of approximately 37% compared with a loss of 24% for the 48 Mbps rate. As shown in Table 2.4, the modulation scheme used in both is 64 QAM but the 48 Mbps rate has a convolutional coding rate of 2/3 as opposed to the 3/4 rate of the 54 Mbps. This extra error correcting information makes the 48 Mbps rate more robust against any errors that may occur. The overhead of the extra redundancy outweighs the advantage of the 54 Mbps transmission rate as shown in Figure 6.31 and Figure 6.32.

This result is specific to the channel conditions in the wireless laboratory. In a better channel environment with a higher SNR it is expected that the 54 Mbps data transmission speed would perform better. The testing environment is typical of a home/office wireless network and the tests were performed with a client at a distance of 5m. In order to improve the channel condition, i.e. the SNR, more than they were the client would be required to be less than 5m

away from AP, which is not a realistic scenario that would normally occur is a wireless environment.

6.7 H.264 Video Data Partitioning over IEEE 802.11e

In this section we introduce the most recent work that experimentally demonstrates the concept of using the EDCA access mechanism to stream H.264 video over the wireless testbed described in Subsection 6.2.3. Discussions of the specifics of the operation of H.264 are beyond the scope of this thesis and the reader is referred to the standard [34] for further information.

6.7.1 H.264 Background

In normal H.264 encoding, the raw video is encoded into a set of frames called a Group of Pictures (GOP). Every GOP sequence starts with an instantaneous decoding refresh (IDR) frame, also called a key frame, which is self contained and can be decoded independently of any other frame types. The remainder of the frames in a GOP are predicted frames. During the encoding process, compression is achieved by removing the repetition between successive predicted frames.

Data Partitioning is a part of the extended profile within the H.264 group of standards and splits the predicted frames into three partitions A, B and C, which are intended to be transmitted as individual packets. Partition A contains the most important information, with Partition B & C containing enhancement information. If Partition A is lost, the entire frame is discarded, but if Partition A arrives with either Partition B and/or C, the frame prediction quality is improved. The loss of an IDR frame can cause errors to propagate through the remainder of the GOP. This is visible to the user as picture corruption and would have a negative effect on the perceived QoS as discussed in Section 4.6

Each partitioned frame, A, B or C is encoded into a network abstraction layer (NAL) unit. These in turn are encapsulated into RTP/UDP/IP packets for transmission over the wireless network. The NAL unit header contains information that identifies the content of the packet allowing us to implement our cross layer approach described later in this section.

6.7.2 Cross-Layer Approach

A cross-layer approach was used by providing an indication of the packet's importance to lower layers in the protocol stack (Figure 2.1). This is achieved through the use of the DSCP field within the IP header. The DSCP field was set from our video serving application based on the packet payload. Using the knowledge about the contents of the packet from the NAL unit header, we set the DSCP value such that when the packet is passed down to the MAC layer of the stack, the DSCP field is then mapped to the EDCA access categories defined in Table 3.2. In our cross-layer approach, termed QoS Arch, the control information is assigned to AC_VO. IDR frames and Partition A is assigned to AC_VI, with Partitions B & C assigned to AC_BE.

6.7.3 Video Testbed Setup

The hardware for our testbed used for our video application was similar to that described in Subsection 6.2.3.1. The three laptops were placed approximately 5m away from the access point, without direct line of sight, but with no major obstacles, such as walls, in the way. Data transmission rate was fixed at 54 Mbps with RTS/CTS disabled and specific enhancement features such as Turbo G and Extended Range disabled. EDCA parameters within the MADWiFi setup were kept as prescribed in the EDCA standard, shown in Table 3.2. The combined testbed network is shown in Figure 6.33.

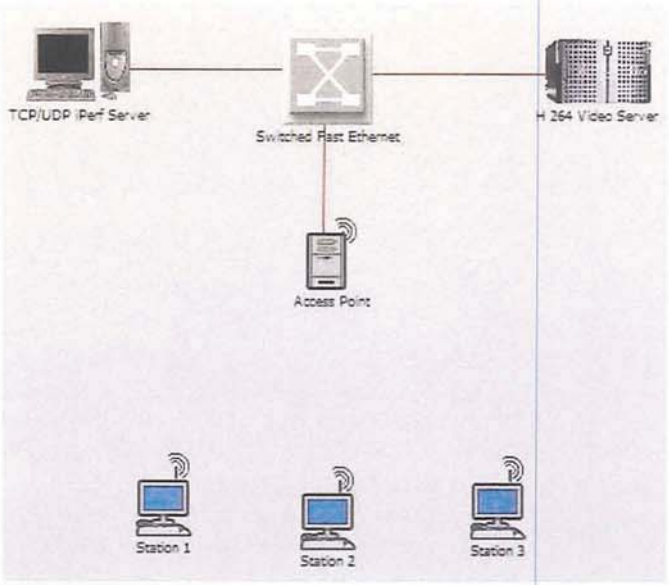

Figure 6.33 - Combined Testbed Network

Using JM v13.2 [96] a 10 minute video was encoded into a sequence of real time protocol (RTP) packets. The video sequence was CIF size (352 x 288) at frame rate of 25 fps, content was from the opening sequence of James Bond – Goldeneye. The video was encoded with a GOP length of 36 frames. The custom video server took the pre encoded RTP packets and assigned them a DSCP value according to the contents (extracted from the NAL header).

Underlying TCP traffic was generated using Iperf and allocated to the AC_BE (Best Effort) access class. As with the previous TCP experiments, TCP Reno was used with a 64K receiver window and dummy payloads of 1460 bytes. This traffic profile generated is indicative of a bandwidth hungry protocol such as FTP. The TCP traffic was present for the duration of each video test from start to beginning.

The raw 802.11 data frames were captured from the wireless channel in a similar fashion to our previous experiments. We reverted to the command line tool tshark, instead of the GUI based Wireshark, to capture the frames because of the increased memory requirements of

capturing 10 minutes of 802.11 data in real time. Wireshark was then used to filter the UDP/RTP video stream from the background TCP traffic. From this we were able to produce the MAC layer retransmission distribution for the video stream. This was done using a custom script.

We conducted a series of experiments to stream the video over the wireless network to a single client. The experimental procedure is described in the steps below:

1. All wireless stations were positioned and tested for wireless connectivity.
2. Background TCP streams, generated using Iperf were initiated on all stations.
3. Video stream was initiated from the video server
4. At the same time as Step 3, the passive capture of the wireless channel was started.
5. After the video stream has terminated, the video stream and packet captures were processed and analysed.
6. The process was repeated three times (with the mean result presented) for each combination detailed below.

The TCP traffic described previously was running on all three clients simultaneously. Firstly the video was streamed over the network using only the legacy DCF protocol. All the video and TCP traffic contended equally for the medium. Secondly, the video traffic was assigned to each of the four EDCA access categories individually, e.g. all in AC_BK, all in AC_BE, all in AC_VI and all in AC_VO. TCP traffic was always sent in AC_BE regardless of the allocation of the video traffic. Finally we partitioned the video data across the EDCA access categories according to importance. This is referred to as QoS Arch., shown in Table 6.5.

Assignment	DCF	AC_BK	AC_BE	AC_VI	AC_VO	QoS Arch.
AC_BK		All Video				
AC_BE			All Video			Partition B & C
AC_VI				All Video		IDR & Partition A
AC_VO					All Video	Control
DCF	All Video					

Table 6.5 - Access Category Assignment

In Figure 6.34 we show the number of each type of packet in the 10 minute video sequence and the average size in bytes.

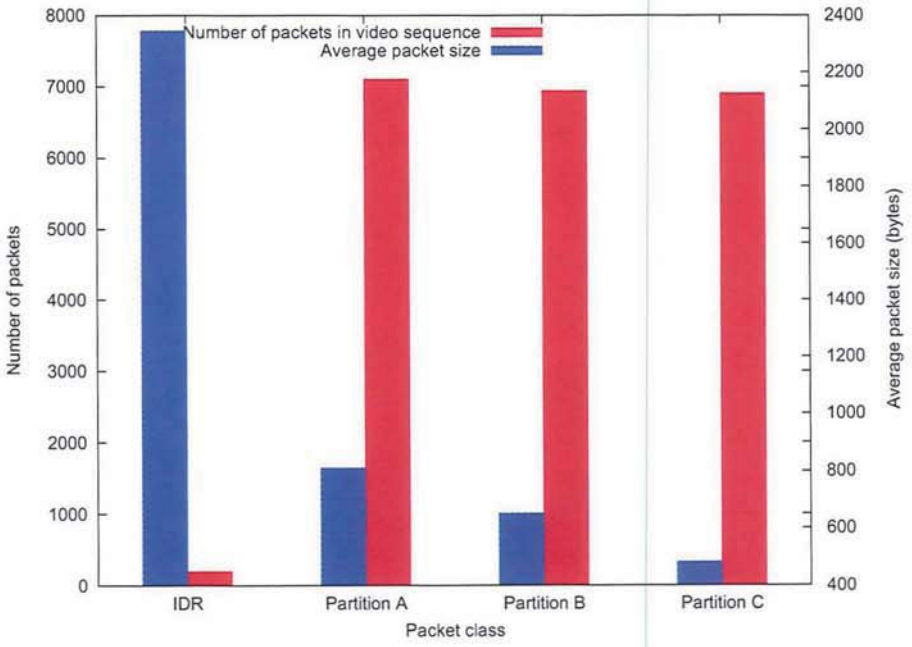

Figure 6.34- Number and Size of Video Packets

The IDR packets being completely self contained and independent are by far the largest and least common as there is only one for every GOP. The number of Partition A, B & C packets is evenly distributed and they range from 4000 bytes to 6000 bytes in size. These make up the bulk of the video data.

6.7.4 Testing Results

Table 6.6 shows the throughput for the TCP traffic generated by Iperf, which was run in the AC_BE (Best Effort) class on each client station. The peak throughput was achieved when the video and TCP traffic were both sent in the AC_BE category. The worst TCP throughput was experienced when the video was placed in the AC_VO category.

Assignment	Average TCP Throughput
AC_VO	10.23 Mbps
AC_VI	13.19 Mbps
AC_BE	14.10 Mbps
AC_BK	13.44 Mbps
QoS Arch.	13.35 Mbps
DCF	12.28 Mbps

Table 6.6 - TCP Throughput in AC_BE

In Figure 6.35 we show the improvement in Peak Signal to Noise Ratio (PSNR) over DCF when any EDCA class except AC_BK is used. All the assignments are compared against the maximum PSNR value achievable of a video decoded without any losses. In the case of AC_BK, the decoder was unable to fully decode the video sequence, as not enough control information was received for the video decoder to operate. The reason for this is the larger

AIFS and contention window in the AC_BK class, resulting in poor throughput in the presence of background TCP traffic in the higher AC_BE class.

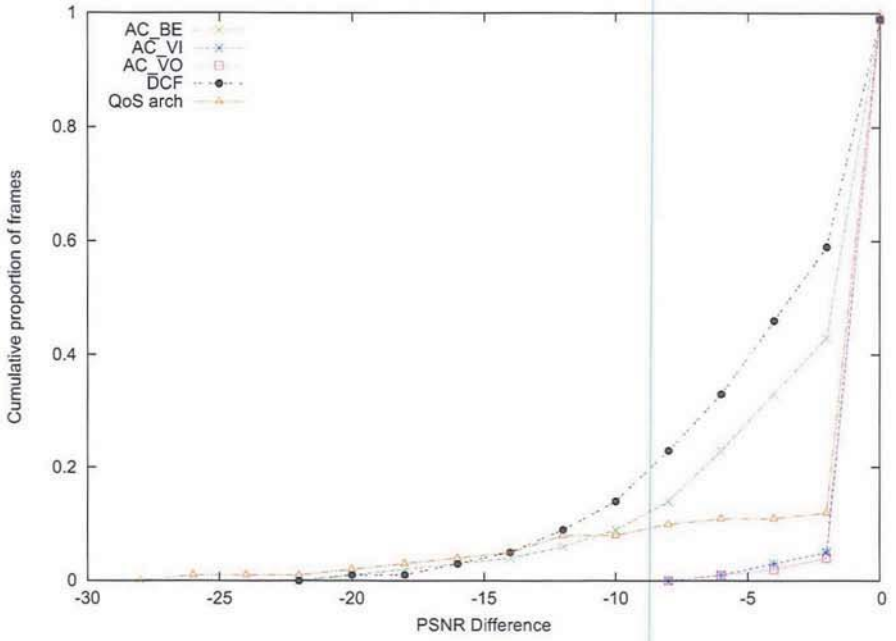

Figure 6.35 - PSNR Difference Compared to Loss Free Video

Of the individual classes, assigning the packets to the background class produces the biggest drop in picture quality. A reduction in the PSNR value would be clearly visible to a user viewing the video stream. Due to hardware limitations the video stream could not be rendered in real time at the receiving client, so it was reconstructed from the incoming packet stream following the completion of the experiment. Typical artefacts that appeared in the reconstructed video were pixilation/blocking effect and freeze frames, due to the loss of packets during the transmission. We also see that when the video is allocated to AC_VO or AC_VI the video quality is better than when using the QoS arch assignment.

	IDR	Part. A	Part. B	Part. C	Total
AC_VO	100.00%	99.972%	99.986%	99.971%	99.980%
AC_VI	100.00%	99.986%	99.986%	99.986%	99.990%
AC_BE	99.502%	99.390%	98.905%	99.662%	99.000%
AC_BK	99.834%	99.948%	99.914%	99.947%	99.930%
QoS Arch.	99.834%	99.972%	99.894%	99.947%	99.950%
DCF	98.673%	99.127%	98.910%	99.102%	99.050%

Table 6.7 - Percentage Packets Transmitted by AP

	IDR	Part. A	Part. B	Part. C	Total
AC_VO	100.00%	99.897%	99.962%	99.720%	99.860%
AC_VI	100.00%	99.944%	99.957%	99.710%	99.870%
AC_BE	99.171%	99.277%	98.656%	99.570%	98.890%
AC_BK	99.171%	99.803%	99.726%	99.715%	99.750%
QoS Arch.	99.171%	99.122%	81.369%	87.312%	99.510%
DCF	98.673%	99.122%	98.905%	99.092%	99.040%

Table 6.8 - Percentage Packet Received by Client

Table 6.7 highlights the issue of virtual contention at the access point, which displays the percentage of packets actually transmitted by the access point. It can clearly be seen that in the cases where the TCP and Video traffic are sent in the same category (i.e. AC_BE and DCF), the percentage of video packets dropped by the access point is higher than in any of the other assignment cases. These losses at the access point are far larger than the number of packets corrupted within the wireless network. In the cases where all the packets are sent in

different classes the largest loss of packets occur in the wireless network and are not dropped due to virtual contention at the access point. This problem of virtual contention could also be caused by the internal buffers within the access point becoming saturated, due to the traffic all being transmitted in one class, resulting in dropped packets.

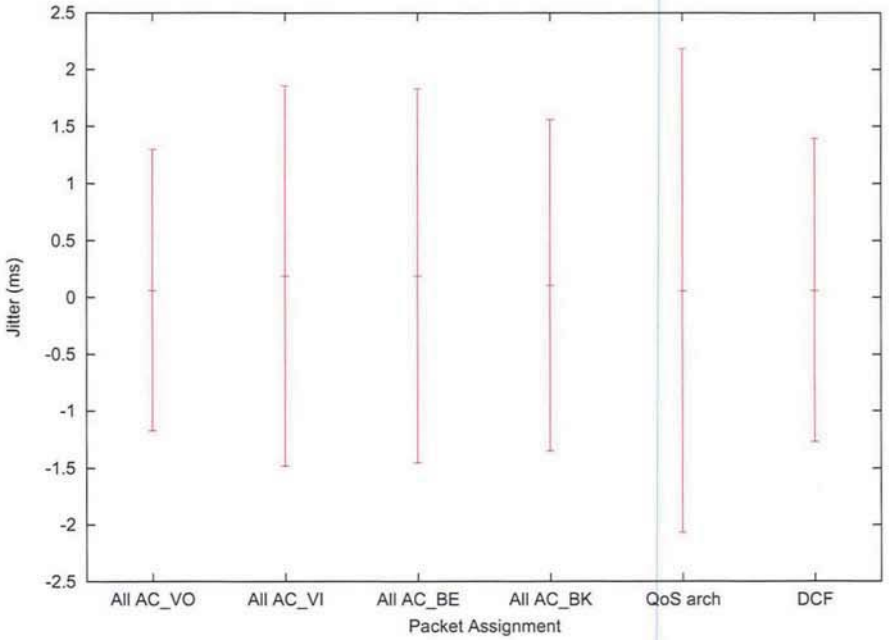

Figure 6.36 - Average Jitter with Standard Deviation

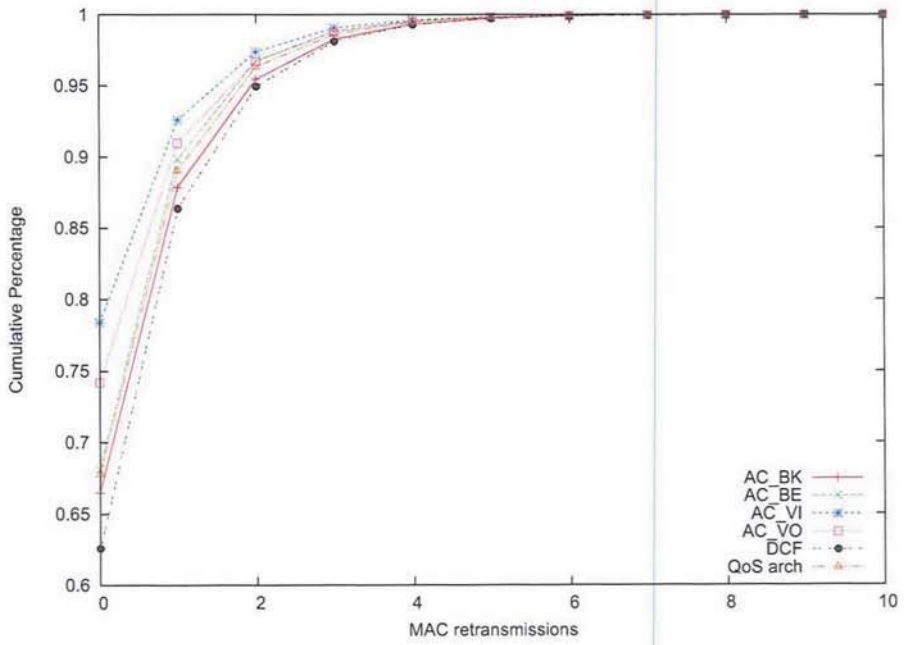

Figure 6.37 - Cumulative MAC Retransmissions

In Figure 6.36 we show the average jitter received by the video stream. The jitter values are within ±2ms, the lowest jitter is experienced when the video is streamed in the AC_VO class. Figure 6.37 shows that AC_VO requires more retransmissions than the AC_VI case; however we have already seen it has the lowest jitter. The reason AC_VO has a lower jitter than AC_VI, is because of its shorter contention time between successive attempts to access the medium. However excessive MAC layer retransmissions may well have a direct impact on higher layer QoS, shown through metrics such as PSNR and Jitter.

To conclude, from our results we have shown that assigning video to either AC_VO or AC_VI provides a visible improvement to the client compared to using AC_BE or DCF. We also tested the proposed QoS Arch. assignment scheme. While this provides an improvement over assigning packets to the AC_BE class, it does not provide any improvement over assigning the video to AC_VO or AC_VI. We have also shown the effect of virtual contention, which is often overlooked, but as out results have shown the losses can be higher than those occurred from corruption in the wireless network. These losses could be due to a buffer saturation issue at the access point, as the greatest losses occurred at the AP when the TCP background traffic and the video traffic were transmitted in the same class.

Future work in this area will be centred on examining the circumstances the QoS Arch assignment scheme can proved to be beneficial. This is likely to involve different hardware devices with different EDCA parameter sets and differing background traffic loads. In addition to this the potential buffer saturation issue at the AP should be investigated further, to establish if this is the cause of the greater losses seen at the AP.

6.8 Conclusions

In this Chapter the bulk of the experimental work based on the real world testbed was presented. Initially testing was limited to the 802.11b physical layer using DCF, but this was later expanded to a platform supporting 802.11a/b/g with both DCF and EDCA MAC layers. Results captured using a testbed provide a realistic view of typical conditions encountered something not possible using a simulation tool such as OPNET. A limitation of the testbed was however the inability to scale to large network. With enough machines this would be possible, but the process of managing such a large test would be cumbersome. It is felt that results generated using an empirical testbed have a greater value than that generated through simulation, as they more closely represent physical network conditions in terms of noise, interference and contention and other factors that cannot be realistically modelled.

In one of the first experiments the capacity of an 802.11b WLAN is shown experimentally to be close to 5.3 Mbps, which is close to the value of 5.5 Mbps found through simulation in Section 5.3. The slightly lower value is attributed to the noisier channel conditions and potential co-channel interference from other access points in the vicinity of the test environment.

The expanded testbed utilises open source software running on a Linux platform. Results are generated from a passive capture of the wireless channel. In the analysis in Section 6.4 it is shown that the number of MAC layer retransmissions is inversely related to the Signal to Noise Ratio (SNR) at a given distance. The built-in Automatic Repeat Request (ARQ) mechanism is shown to recover frames at the MAC layer in the majority of cases, but at low SNR values, packet loss does occur. The low packet loss rate could have a negative effect on real time streaming applications involving video and voice. Packet loss would normally lead

to a video stream momentarily pausing or becoming pixelated, or a voice conversation missing words. Frame acknowledgements and repeat request mechanisms are highlighted as an area of further research as improvements in this area would be beneficial to all services running over wireless LANs.

One of the critical areas of the empirical investigation is on the issue of service differentiation and fairness when utilising the EDCA MAC layer. Real time services are shown to benefit from EDCA when placed in the high priority AC_VO (Voice) category. The AC_VO category is shown to have the highest throughput, whilst maintaining a low MAC delay. However, this priority is not without sacrifice to lower priority queues such as AC_BE (Best Effort) and AC_BK (Background). It is shown that the throughput of an AC_BK stream drops dramatically from 15 Mbps to 1 Mbps in the presence of a TCP AC_VO stream. This could have major implications for modern non real time bulk TCP services, such as BBC iPlayer and YouTube, which may be operating in the AC_BK category. Typically, users would experience longer buffering delays while viewing the video content and, in some cases, interruption to the service, as the available bandwidth is throttled back. As shown in the experimental results, a constant TCP stream will utilise as much bandwidth as available on a network path. In order to ensure fairness across an EDCA WLAN, it is proposed that the highest priority AC_VO category be reserved for low rate, non TCP traffic. The use of any TCP-based service in the AC_VO has the effect of starving lower priority streams of traffic. By adhering to such self regulation, it is possible to balance the need for service differentiation with fairness and provide an adequate QoS and experience to all users of a network, without penalising or starving a particular type of traffic.

Our application of streaming partitioned video over the EDCA MAC layer in combination with H.264 yields some promising results.. The QoS Arch partitioned assignment provides

benefit over DCF, AC_BE and AC_BK assignments, however it is bettered by assigning the video to the higher AC_VI and AC_VO classes. Our work shows that the number of frames dropped through virtual contention and buffer saturation at the AP is often higher than those lost over the wireless channel. This is an area of further research, and that better algorithms and buffer mechanisms for dealing with virtual contention would be beneficial.

7 Thesis Conclusions

7.1 Overview

This thesis presents a comprehensive analysis of the IEEE 802.11 WLAN MAC protocols, DCF and EDCA. Extensive background to the operation of the protocol is provided and the issues of QoS over wireless networks are discussed. The performance and behaviour of both DCF and EDCA are investigated through computer simulation and practical experimentation.

The performance of legacy DCF is compared and contrasted with that of the newer EDCA. The findings indicate that EDCA is able to support multiple services across a WLAN, while maintaining a good QoS for the highest priority traffic. The findings through simulation are similar to those established through experimental methods using the real world testbed. Service differentiation is shown to be possible using EDCA across a WLAN, but not without penalising/starving low priority traffic streams. This behaviour of crippling low priority traffic schemes is unfair and that QoS should be concerned with the network as whole and not just high priority real time traffic such as VoIP. QoS should encompass all types of traffic across a WLAN, and provide service differentiation as necessary, while ensuring that the network has a degree of fairness between different categories of traffic.

7.2 Summary of Contributions

7.2.1 Extensive Analysis of DCF and EDCA through Simulation

The commercial simulation tool OPNET Modeller™ is used to produce an extensive analysis of the operation of both DCF and EDCA MAC layers. As opposed to using static traffic generators, this work utilises real services as defined within the main software that provides a more realistic approach to service modelling. Individual traffic models, for example HTTP,

are altered, in terms of size and elements to represent a typical modern webpage such as BBC News. QoS results obtained from the simulator allow us to perceive the delays and object load times realistically, defining acceptable limits for a service that is difficult to measure.

7.2.2 Design and Implementation of a Real World QoS Testbed

The hardware testbed provides an insight into the operation of the DCF and EDCA MAC layer protocols in a realistic working environment. Using standard commercial off the shelf (COTS) hardware, and open source software based on the Linux operating system, a testbed is designed tests the performance of the protocols in a number of different physical scenarios. QoS metrics such as Throughput and Delay are derived directly from a passive capture of the physical channel. Further offline manipulation of the channel capture could yield more metrics.

7.2.3 Contrasting Balance between Service Differentiation and Fairness

Simulation and experimental results have shown that service differentiation is possible using EDCA over a WLAN. However, while it is possible to provide good QoS to a high priority stream, low priority streams are throttled back aggressively to the point where they are starved of bandwidth. As mentioned in the results, popular bulk data applications such as P2P, BBC iPlayer and YouTube would be adversely affected by this action. In the case of the video applications users would experience pauses in the video stream and increased buffering delays, affecting the perceived QoS.

7.3 Summary of Results

The results in this thesis have been generated through both common simulations platforms and practical real field testing. While there are considerable works on Wireless LAN based on simulation and analytical models, real world testbeds are less common. A practical robust testbed was designed which was based upon freely available open source software in order to investigate QoS using both legacy DCF and the newer EDCA mechanisms in a realistic environment (typical of a home/office setting). Throughput and delay results were derived from a passive packet capture of the channel and validated by results reported by the testing software.

The initial simulations and experimental testing involved a BSS 802.11b WLAN. Using DCF and elastic traffic types such as FTP and HTTP, it is shown that the maximum number of clients that can be supported is limited. The bursty nature of HTTP traffic allows a greater number of clients to be supported than bandwidth hungry FTP. While both services are able to operate with reduced throughput, the file transfer times with FTP are significantly greater with increased network loads. With a single traffic type, it is shown that the application throughput of an 802.11b WLAN is 4 to 5.5 Mbps, almost 50% of the maximum data transmission rate of 11 Mbps. This is attributed to the overheads from the transport and MAC layer. Actual achievable throughput should be considered when deploying wireless networks.

Simultaneous use of elastic services such as HTTP and FTP, with a non-elastic service VoIP, exposes the inability of the legacy DCF MAC layer to provide service differentiation. The VoIP call quality, measured using the MOS value, is shown to drop significantly as the amount of non real time traffic increases. The DCF mechanism is unable to differentiate between the sensitive VoIP traffic and the bulk TCP based traffic. A brief section on the

performance of PCF is also presented. The polling operation is shown to lack scalability as the network load is increased. This is characterised by an increase in delay and a reduction in throughput.

It is shown that the EDCA access mechanism has the ability to support real time traffic in the presence of background traffic such as HTTP and FTP. In the simulation of FTP and VoIP traffic (Section 5.4), the EDCA mechanism is able to support VoIP with a MOS of more than 3.5 with 16 clients. Referring back to Table 4.1, a MOS greater than three is desired for an acceptable service. Using DCF with the same load yields a MOS of 3.5 up to 8 clients, after which it decreases to less than 1.5. The VoIP capacity is doubled when using EDCA in this scenario. However as FTP is tolerant of reduced throughput and increased delay, the effect of the EDCA VoIP prioritisation on the elastic service is difficult to gauge.

HTTP described in Subsection 2.5.1 on page 29, can operate with varying levels of throughput and delay, but is more susceptible to changes in these than FTP. Prioritisation is not without an impact on the bulk service(s), such as HTTP. In the combination of HTTP and VoIP, EDCA is shown to benefit the VoIP traffic with MOS of 3.1 for up to 20 clients, while DCF drops below 3.0 at just 10 clients. HTTP object response time and page response time are valuable metrics to judge HTTP performance realistically. At high loads both the object and page response times increase to tens of seconds, making the service unusable. At this load level, the performance of HTTP using EDCA is shown to be worse than that of DCF.

In the analysis of frame loss, a unique way of calculating throughput directly from a raw frame capture of the wireless medium is shown. Using a custom script a retransmission distribution per station or stream basis is derived. The investigation shows the effect of frame loss on QoS metrics, such as throughput and delay. Physical layer parameters such as SNR

are shown to be directly related to higher layer metrics such as frame loss throughput. These findings can be used in the design and planning of wireless networks where a minimum level of QoS is required.

The EDCA mechanism is also investigated experimentally and shown to have some drastic effects. Traffic placed in the low priority classes such as AC_BK (Background) and AC_BE (Best Effort) are heavily penalised in the presence of traffic in the AC_VO (Voice) class. In one example, using 802.11g the throughput of the TCP traffic (representative of FTP or HTTP downloading) for AC_BK is shown to reduce from 14 Mbps to 1 Mbps. This could have a significant effect on data intensive services. Applications such as YouTube and BBC iPlayer, which both use TCP, would experience increasing buffering delays and possible breaks in playback, thus seriously affecting the service performance. Delay performance in the lowest classes is also shown to be worse than when using DCF. While prioritisation is one of the goals of EDCA, the gross unfairness between categories causes lower priority traffic to be starved of bandwidth.

This research has also shown that the classification of traffic into the appropriate EDCA categories is problematic with current hardware. The non standard mapping from the DSCP field in the IP header (Layer 3) to EDCA at the MAC (Layer 2) between equipment vendors, makes QoS aware applications more difficult to design. The success of WMM and EDCA is dependent on equipment vendors cooperating to adopt a universal approach.

An application for the EDCA based testbed is found in the area of video streaming. The use of the AC_VI (Video) and AC_VO (Voice) classes in EDCA is shown to improve the PSNR (representative of the video quality) when compared to DCF. However the partitioning of video data into different EDCA classes only shows benefit over the lower DCF, AC_BE and

AC_BK assignments. Further research is recommended into the effect of Virtual Contention and possible buffer saturation under the EDCA MAC protocol.

7.4 Future Work

In the conclusions a number of issues with the existing EDCA mechanism as defined in IEEE 802.11e have been raised. While the EDCA mechanism was designed to provide service differentiation between competing traffic streams, it is shown in the case of TCP traffic, the highest priority AC_VO can block out the lower priority AC_BE and AC_BK classes. QoS should not just be concerned with prioritising high priority fragile traffic such as VoIP, but look at the wider aspect of QoS for *all* traffic. In the example two popular applications are cited; YouTube and BBC iPlayer, that use TCP with a buffer for transferring video content for display within a web browser. TCP traffic such as this requires as much bandwidth as possible until the buffering is completed. In Figure 6.27, page 141 the AC_BK throughput is shown to reduce from 14 Mbps to 1 Mbps. Lower throughput figures can lead to breaks in the video playback while the buffer is replenished, thus severely affecting the service quality. It is advised that amendments to the EDCA parameter may solve this issue. In particular, smaller AIFS values and CW sizes for the AC_BE and AC_BK may result in better performance and fairness for low priority traffic, in the presence of higher priority streams using the AC_VO and AC_VI classes. Fairness can also be increased by increasing the default AIFS value and CW sizes for the AC_VO and AC_VI class. Through experimentation using the testbed, different settings for the EDCA parameters can be tested to increase fairness, while maintaining a level of service differentiation.

The changes suggested will aid the goal of providing Quality of Service on the large-scale whole network basis as oppose to just prioritising services such as VoIP and Video. Video

traffic sent over a buffered TCP is becoming increasingly popular and must be taken into account when providing QoS to the whole network.

The behaviour of the wireless channel and effects of frame losses using different data transmission rates is also proposed as an area of expansion. In Section 6.6 a single scenario is investigated where the highest transmission rate of 54 Mbps is not the optimal choice given the channel conditions present. A wider investigation into a variety of transmission scenarios, including both line of sight and non line of sight, with varying distance, will give a better understanding of the loss characteristics in these environments. The findings of this work can be used in the planning and design of wireless networks, where optimal data transmission rates can be defined for the given channel environment.

7.5 Publications

Mukherjee, S., et al. *The Digital Patient Push - Using Location to Streamline the Surgical Journey.* in *Advances in Medical, Signal and Information Processing, 2006. MEDSIP 2006. IET 3rd International Conference On.* 2006. [97]

Mukherjee, S. and X.H. Peng. *Experimental Investigation of IEEE 802.11e EDCA.* in *2nd IEEE International Symposium on Advanced Networks and Telecommunication Systems* 2008. Mumbai, India: IEEE. [98]

Mukherjee, S., X.H. Peng, and G. Qiang. *QoS Performances of IEEE 802.11 EDCA and DCF: A Testbed Approach.* in *Wireless Communications, Networking and Mobile Computing.* 2009. Beijing, China: IEEE. [99]

Haywood, R.H., S. Mukherjee, and X.H. Peng. *Investigation of H.264 Video Streaming over an IEEE 802.11e EDCA Wireless Testbed.* in *IEEE International Conference of Communications.* 2009. Dresden, Germany: IEEE. [100]

List of References

1. Gast, M., *802.11 wireless networks : the definitive guide*. 2nd ed. ed. 2005, Beijing ; Farnham: O'Reilly. xxi, 630 p.
2. Schwartz, M., *Mobile wireless communications*. 2004, New Jersey Cambridge: World Scientific Publishing Co. Pte. Ltd. Cambridge University Press. xi, 457 p. ill.
3. Roshan, P. and J. Leary, *802.11 Wirelss LAN fundamentals*. 2003, Indianapolis, Ind. ; [Great Britain]: Cisco. xviii, 281 p.
4. Geier, J.T., *Deploying voice over wireless LANs*. Networking technology series. 2007, Indianapolis, Ind.: Cisco Press ; [London : Pearson Education, distributor]. xvii, 248 p.
5. Wong, K.D., *Wireless Internet telecommunications*. Artech House mobile communications series. 2005, Boston, Mass. ; London: Artech House. xiii, 250 p.
6. Gómez, G. and R. Sánchez, *End-to-end quality of service over cellular networks : data services performance and optimization in 2G/3G*. 2005, John Wiley: Chichester. p. 8 - 9.
7. IEEE-SA, *IEEE 802.11 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. 2007.
8. DARPA. *RFC 793: Transmission Control Protocol*. 1981.
9. Jacobson, V., R. Braden, and D. Borman. *RFC 1323: TCP Extensions for High Performance*. 1992.
10. Mathis, M., et al. *RFC 2018: TCP Selective Acknowledgment Options*. 1996.
11. Allman, M., V. Paxson, and W. Stevens. *RFC 2581: TCP Congestion Control*. 1999.
12. Paxson, V. and M. Allman. *RFC 2988: Computing TCP's Retransmission Timer*. 2000.
13. Kurose, J.F. and K.W. Ross, *Computer networking : a top-down approach featuring the Internet*. 2003, Addison-Wesley: Boston, Mass. ; London. p. 12 - 13.
14. Postel, J. *RFC 768: User Datagram Protocol*. 1980.
15. Kurose, J.F. and K.W. Ross, *Computer networking : a top-down approach featuring the Internet*. 2003, Addison-Wesley: Boston, Mass. ; London. p. 13 - 14.
16. Fielding, R., et al. *RFC 2616: Hypertext Transfer Protocol - HTTP/1.1*. 1999.
17. Domain-Tools. *Domain Tools*. 2008; Available from: http://www.domaintools.com/internet-statistics/.
18. Postel, J. and J. Reynolds, *RFC 959: File Transfer Protocol*. 1985.
19. Rosenberg, J., et al. *RFC 3261: SIP: Session Initiation Protocol*. 2002.
20. Kurose, J.F. and K.W. Ross, *Computer networking : a top-down approach featuring the Internet*. 2003, Addison-Wesley: Boston, Mass. ; London. p. 542.
21. IEEE-SA, *IEEE 802.11 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. 1999.
22. Pattara-Atikom, W., P. Krishnamurthy, and S. Banerjee, *Distributed mechanisms for quality of service in wireless LANs*. Wireless Communications, IEEE [see also IEEE Personal Communications], 2003. 10(3): p. 26-34.
23. IEEE-SA, *IEEE 802.11e Amendment: Medium Access Control (MAC) Quality of Service (QoS) Enhancements*. 2005.
24. El Masri, M. *IEEE 802.11e: The Problem of the Virtual Collision Management Within EDCA*. in *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*. 2006.
25. Breslau, L., et al. *Network Simulator 2*. 2008; Available from: http://www.isi.edu/nsnam/ns/.

26. OPNET-Technologies. *OPNET Modeller*. 2008; Available from: http://www.opnet.com/solutions/network_rd/modeler.html.
27. Leffler, S. and G. Chesson. *Multiband Atheros Driver for Wireless Fidelity*. 2008; Available from: http://madwifi.org/.
28. Braden, R., D. Clark, and S. Shenker. *RFC 1633: Integrated Services in the Internet Architecture: an Overview*. 1994.
29. Blake, S., et al. *RFC 2475: An Architecture for Differentiated Services*. 1998.
30. Oodan, A.P., *Telecommunications quality of service management : from legacy to emerging services*. [New ed.] / Antony Oodan ... [et al.] ed. IEE telecommunications series 48. 2003, London: Institution of Electrical Engineers. xxxiii, 602 p.
31. NLANR/DAST. *Iperf - TCP/UDP Bandwidth Measurement Tool*. 2008; Available from: http://dast.nlanr.net/Projects/Iperf/.
32. ITU-T. *Telecommunication Standardization Sector*. 2008; Available from: http://www.itu.int/ITU-T/.
33. Cisco-Systems. *Codec Mean Opinion Score*. 2008; Available from: http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a00800b6710.shtml#mos.
34. ITU-T. *H.264 : Advanced video coding for generic audiovisual services* 2008; Available from: http://www.itu.int/rec/T-REC-H.264/e.
35. Barkowsky, M., et al. *Temporal registration using 3D phase correlation and a maximum likelihood approach in the perceptual evaluation of video quality*. in *Multimedia Signal Processing, 2007. MMSP 2007. IEEE 9th Workshop on*. 2007.
36. OPTICOM. *PEVQ: Perceptual Evaluation of Video Quality*. 2008; Available from: http://www.pevq.org/.
37. Nichols, K., et al. *RFC 2474: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*. 1998.
38. Bianchi, G., *IEEE 802.11-saturation throughput analysis*. Communications Letters, IEEE, 1998. 2(12): p. 318-320.
39. Bianchi, G., *Performance analysis of the IEEE 802.11 distributed coordination function*. Selected Areas in Communications, IEEE Journal on, 2000. 18(3): p. 535-547.
40. Kuppa, S., N. Shun-Chen, and R. Prakash. *IEEE 802.11 DCF performance evaluation using one-dimensional discrete time chains*. in *Vehicular Technology Conference, 2006. VTC 2006-Spring. IEEE 63rd*. 2006.
41. Wu, H., et al. *Performance of reliable transport protocol over IEEE 802.11 wireless LAN: analysis and enhancement*. in *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*. 2002.
42. Cali, F., M. Conti, and E. Gregori, *Dynamic tuning of the IEEE 802.11 protocol to achieve a theoretical throughput limit*. Networking, IEEE/ACM Transactions on, 2000. 8(6): p. 785-799.
43. Chatzimisios, P., A.C. Boucouvalas, and V. Vitsas, *Influence of channel BER on IEEE 802.11 DCF*. Electronics Letters, 2003. 39(23): p. 1687-9.
44. Chatzimisios, P., A.C. Boucouvalas, and V. Vitsas. *Performance analysis of IEEE 802.11 DCF in presence of transmission errors*. in *Communications, 2004 IEEE International Conference on*. 2004.
45. Zheng, Y., K. Lu, and D.W. Fang, *Performance Analysis of IEEE 802.11 DCF in Imperfect Channels*. Vehicular Technology, IEEE Transactions on, 2006. 55(5): p. 1648-1656.

46. Fu-Yi, H. and I. Marsic. *Analysis of Non-Saturation and Saturation Performance of IEEE 802.11 DCF in the Presence of Hidden Stations*. in *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*. 2007.
47. Oliveira, R., L. Bernardo, and P. Pinto. *IEEE 802.11 Delay Analysis for Multirate Variable Frame Length*. in *Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on*. 2007.
48. Ji-Hoon, Y., *Throughput analysis of IEEE 802.11 WLANs with Automatic Rate Fallback in a lossy channel*. Wireless Communications, IEEE Transactions on, 2009. 8(2): p. 689-693.
49. Raptis, P., et al. *Packet delay distribution of the IEEE 802.11 distributed coordination function*. in *World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a*. 2005.
50. Raptis, P., et al. *Voice and Data Traffic Analysis in IEEE 802.11 DCF Infrastructure WLANs*. in *Advances in Mesh Networks, 2009. MESH 2009. Second International Conference on*. 2009.
51. Deng, D.J. and R.S. Chang, *A priority Scheme for IEEE 802.11 DCF access method*. IEICE Trans Commun, 1999. E82-B (No 1): p. 96 - 102.
52. Sobrinho, J.L. and A.S. Krishnakumar, *Quality-of-service in ad hoc carrier sense multiple access wireless networks*. Selected Areas in Communications, IEEE Journal on, 1999. 17(8): p. 1353-1368.
53. Hanan, L., et al., *Issues in Managing Soft QoS Requirements in Distributed Systems Using a Policy-Based Framework*, in *Proceedings of the International Workshop on Policies for Distributed Systems and Networks*. 2001, Springer-Verlag.
54. Aad, I. and C. Castelluccia. *Differentiation mechanisms for IEEE 802.11*. in *INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*. 2001.
55. Veres, A., et al., *Supporting service differentiation in wireless packet networks using distributed control*. Selected Areas in Communications, IEEE Journal on, 2001. 19(10): p. 2081-2093.
56. Xiao, Y., *A simple and effective priority scheme for IEEE 802.11*. Communications Letters, IEEE, 2003. 7(2): p. 70-72.
57. Xiao, Y. *Backoff-based priority schemes for IEEE 802.11*. in *Communications, 2003. ICC '03. IEEE International Conference on*. 2003.
58. Xiao, Y. *Enhanced DCF of IEEE 802.11e to support QoS*. in *Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE*. 2003.
59. Bianchi, G. and I. Tinnirello. *Analysis of priority mechanisms based on differentiated inter frame spacing in CSMA-CA*. in *Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th*. 2003.
60. Lindgren, A., A. Almquist, and O. Schelen. *Evaluation of quality of service schemes for IEEE 802.11 wireless LANs*. in *Local Computer Networks, 2001. Proceedings. LCN 2001. 26th Annual IEEE Conference on*. 2001.
61. del Prado Pavon, J. and P. Wienert, *IEEE 802.11e Performance Evaluation*. 2003, Phillips.
62. Sunghyun, C., et al. *IEEE 802.11 e contention-based channel access (EDCF) performance evaluation*. in *Communications, 2003. ICC '03. IEEE International Conference on*. 2003.
63. Xu, K., W. Quanhong, and H. Hassanein. *Performance analysis of differentiated QoS supported by IEEE 802.11e enhanced distributed coordination function (EDCF) in WLAN*. in *Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE*. 2003.

64. del Prado Pavon, J. and S.N. Shankar. *Impact of frame size, number of stations and mobility on the throughput performance of IEEE 802.11e.* in *Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE.* 2004.
65. Jie, H. and M. Devetsikiotis. *Performance analysis of IEEE 802.11e EDCA by a unified model.* in *Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE.* 2004.
66. Jong-Deok, K. and K. Chong-Kwon, *Performance analysis and evaluation of IEEE 802.11e EDCF: Research Articles.* Wirel. Commun. Mob. Comput., 2004. 4(1): p. 55-74.
67. Paal, E.E. and N. Olav, *Non-saturation and saturation analysis of IEEE 802.11e EDCA with starvation prediction*, in *Proceedings of the 8th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems.* 2005, ACM: Montreal, Quebec, Canada.
68. Paal, E.E. and N. Olav, *Analysis of QoS in WLAN.* Telektronikk, 2005. Vol. 1.
69. Tantra, J.W., et al. *Throughput and delay analysis of the IEEE 802.11e EDCA saturation Throughput and delay analysis of the IEEE 802.11e EDCA saturation.* in *Communications, 2005. ICC 2005. 2005 IEEE International Conference on.* 2005.
70. Xi, W.H., et al., *Modeling and Simulation of MAC for QoS in IEEE 802.11e Using OPNET Modeler.* 2005, Department of Electrical & Electronic Engineering: Bristol.
71. Di Stefano, A., et al. *An experimental testbed and methodology for characterizing IEEE 802.11 network cards.* in *World of Wireless, Mobile and Multimedia Networks, 2006. WoWMoM 2006. International Symposium on a.* 2006.
72. Bianchi, G., et al. *Experimental Assessment of the Backoff Behavior of Commercial IEEE 802.11b Network Cards.* in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE.* 2007.
73. Leith, D.J. and P. Clifford. *TCP fairness in 802.11e WLANs.* in *Wireless Networks, Communications and Mobile Computing, 2005 International Conference on.* 2005.
74. Leith, D.J., et al., *TCP fairness in. 802.11e WLANs.* Communications Letters, IEEE, 2005. 9(11): p. 964-966.
75. Clifford, P., et al. *On improving voice capacity in 802.11 infrastructure networks.* in *Wireless Networks, Communications and Mobile Computing, 2005 International Conference on.* 2005.
76. Clifford, P., et al. *Modeling 802.11e for data traffic parameter design.* in *Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, 2006 4th International Symposium on.* 2006.
77. Dangerfield, I., D. Malone, and D.J. Leith. *Experimental Evaluation of 802.11e EDCA for Enhanced Voice over WLAN Performance.* in *Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, 2006 4th International Symposium on.* 2006.
78. Dangerfield, I., D. Malone, and D.J. Leith. *Understanding 802.11e Voice Behaviour via Testbed Measurements and Modeling.* in *Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks and Workshops, 2007. WiOpt 2007. 5th International Symposium on.* 2007.
79. Huang, C.W., et al. *Link Layer Packet Loss Classification for Link Adaptation in WLAN.* in *Information Sciences and Systems, 2006 40th Annual Conference on.* 2006.
80. Cranley, N., T. Debnath, and M. Davis. *An Experimental Investigation of Parallel Multimedia Streams Over IEEE 802.11e WLAN Networks Using TXOP.* in *Communications, 2007. ICC '07. IEEE International Conference on.* 2007.
81. Malone, D., P. Clifford, and D.J. Leith, *On buffer sizing for voice in 802.11 WLANs.* Communications Letters, IEEE, 2006. 10(10): p. 701-703.
82. Malone, D., P. Clifford, and D.J. Leith, *MAC Layer Channel Quality Measurement in 802.11.* Communications Letters, IEEE, 2007. 11(2): p. 143-145.

83. Cornell. *REAL Simulator*. 1997; Available from: http://www.cs.cornell.edu/skeshav/real/overview.html.
84. Greis, M. *Tutorial for the Network Simulator "ns"*. 2008; Available from: http://www.isi.edu/nsnam/ns/tutorial/.
85. Taank, R. and X.H. Peng. *Impact of Error Characteristics of an Indoor 802.11g WLAN on TCP Retransmissions*. in *In Proceedings of 4th IEEE International Conference on Wireless Communications, Networking and Mobile Computing*. 2008. Dalian, China.
86. Patodia, S. and P. Xiao-Hong. *Implementation and analysis of VoIP services in WLANs*. in *3G Mobile Communication Technologies, 2004. 3G 2004. Fifth IEE International Conference on*. 2004.
87. British-Broadcasting-Corporation. *BBC News Website*. 2008; Available from: http://news.bbc.co.uk/.
88. Ekahau-Inc. *Ekahau Site Survey*. 2008; Available from: http://www.ekahau.com/?id=4601.
89. AirMagnet-Inc. *AirMagnet Laptop Analyser*. 2008; Available from: http://www.airmagnet.com/products/laptop_analyzer/.
90. Berkeley-Varitronics-Systems. *Yellow Jacket*. 2008; Available from: http://www.bvsystems.com/Products/WLAN/YJ802.11bg/YJ802.11bg.htm.
91. CACE-Technologies. *Cace Technologies: AirPcap*. 2008; Available from: http://www.cacetech.com/products/airpcap_family.htm.
92. Combs, G. *Wireshark*. 2008; Available from: http://www.wireshark.org/.
93. Varenni, G., et al. *WinPcap: The Windows Packet Capture Library*. 2008; Available from: http://www.winpcap.org/.
94. Gast, M. *When Is 54 Not Equal to 54? A Look at 802.11a, b, and g Throughput*. 2009; Available from: http://www.oreillynet.com/pub/a/wireless/2003/08/08/wireless_throughput.html.
95. Digital-Spy. *BBC iPlayer use grew 22% in April*. 2008; Available from: http://www.digitalspy.co.uk/broadcasting/a96400/bbc-iplayer-use-grew-22-percent-in-april.html.
96. SÜhring, K. *JM Reference Software*. 2008; Available from: http://iphome.hhi.de/suehring/tml/.
97. Mukherjee, S., et al. *The Digital Patient Push - Using Location to Streamline the Surgical Journey*. in *Advances in Medical, Signal and Information Processing, 2006. MEDSIP 2006. IET 3rd International Conference On*. 2006.
98. Mukherjee, S. and X.H. Peng. *Experimental Investigation of IEEE 802.11e EDCA*. in *2nd IEEE International Symposium on Advanced Networks and Telecommunication Systems* 2008. Mumbai, India: IEEE.
99. Mukherjee, S., X.H. Peng, and G. Qiang. *QoS Performances of IEEE 802.11 EDCA and DCF: A Testbed Approach*. in *Wireless Communications, Networking and Mobile Computing*. 2009. Beijing, China: IEEE.
100. Haywood, R.H., S. Mukherjee, and X.H. Peng. *Investigation of H.264 Video Streaming over an IEEE 802.11e EDCA Wireless Testbed*. in *IEEE International Conference of Communications*. 2009. Dresden, Germany: IEEE.