An Admission Control Scheme for IEEE 802.11e Wireless Local Area Networks

by

Conroy Smith

A thesis submitted to the

Department of Electrical Engineering

University of Cape Town

The University of Cape Town

for the degree of

MASTER OF SCIENCE IN ENGINEERING

Supervisor: Neco Ventura

31 January 2008

The copyright of this thesis vests in the author. No quotation from it or information derived from it is to be published without full acknowledgement of the source. The thesis is to be used for private study or non-commercial research purposes only.

Published by the University of Cape Town (UCT) in terms of the non-exclusive license granted to UCT by the author.

University of Cape Town

Statement of originality

I declare that the work presented in the thesis is, to the best of my knowledge and belief, original and my own work, except as acknowledged in the text, and that the material has not been submitted, either in whole or in part, for a degree at this or any other university.

Conroy Smith

....

31 January 2008

Acknowledgments

I would like to thank the following people for their support and assistance during the course of this project:

My supervisor, Mr Neco Ventura, for his guidance throughout this project.

Telkom SA, NSN, the National Research Foundation (NRF) and the Department of Trade and Industry (DTI), for their financial contributions towards this research.

The past and present members of the Communications Research Group (CRG) at UCT, for their feedback and constructive criticism. Special thanks goes to Vitalis Ozianyi, Eugene Golovins, Dave Waiting, Gabriel Andrews, and Mike Pitman for their their help in the reviewing of this thesis.

My Wife, Cindy, for her constant support and motivation throughout this project.

My parents and family for their support and encouragement.

Finally I would like to thank God for his divine guidance during this project.

Abstract

Recent times has seen a tremendous increase in the deployment and use of 802.11 Wireless Local Area Networks (WLANs). These networks are easy to deploy and maintain, while providing reasonably high data rates at a low cost. In the paradigm of Next-Generation-Networks (NGNs), WLANs can be seen as an important access network technology to support IP multimedia services. However a traditional WLAN does not provide Quality of Service (QoS) support since it was originally designed for best effort operation.

The IEEE 802.11e standard was introduced to overcome the lack of QoS support for the legacy IEEE 802.11 WLANs. It enhances the Media Access Control (MAC) layer operations to incorporate service differentiation. However, there is a need to prevent overloading of wireless channels, since the QoS experienced by traffic flows is degraded with heavily loaded channels. An admission control scheme for IEEE 802.11e WLANs would be the best solution to limit the amount of multimedia traffic so that channel overloading can be prevented.

Some of the work in the literature proposes admission control solutions to protect the QoS of real-time traffic for IEEE 802.11e Enhanced Distributed Channel Access (EDCA). However, these solutions often under-utilize the resources of the wireless channels. A measurement-aided model-based admission control scheme for IEEE 802.11e EDCA WLANs is proposed to provide reasonable bandwidth guarantees to all existing flows. The admission control scheme makes use of bandwidth estimations that allows the bandwidth guarantees of all the flows that are admitted into the network to be protected. The bandwidth estimations are obtained using a developed analytical model of IEEE 802.11e EDCA channels. The admission control scheme also aims to accept the maximum amount of flows that can be accommodated by the network's resources.

Through simulations, the performance of the proposed admission control scheme is evaluated using NS-2. Results show that accurate bandwidth estimations can be obtained when comparing the estimated achievable bandwidth to actual simulated bandwidth. The results also validate that the bandwidth needs of all admitted traffic are always satisfied when the admission control scheme is applied. It was also found that the admission control scheme allows the maximum amount of flows to be admitted into the network, according the network's capacity.

Contents

List of Figures

List of Tables

List of Acronyms

AC	Access Class
ACU	Admission Control Unit
AEB	Average Exponential Backoff
AIFS	Arbitration Inter-Frame Space
AIS	Average Idle Slots
AP	Access Point
API	Application Programming Interface
ARF	Automatic Rate Fallback
BE	Best Effort
BK	Background
BSS	Basic Service Set
CBR	Constant Bit Rate
CFB	Contention Free Bursting
CFP	Contention Free Period
CP	Contention Period
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear to Send
CW	Contention Window
DAC	Distributed Admission Control
DCF	Distributed Coordination Function
DIFS	Distributed Inter-Frame Space

DLL	Data Link Layer
DLP	Direct Link Protocol
ECDA	Enhanced Distributed Channel Access
ESS	Extended Service Set
FTP	File Transfer Protocol
HC	Hybrid Coordinator
HCCA	HCF Controlled Channel Access
HCF	Hybrid Coordination Function
IEEE	Institute of Electrical and Electronics Engineers
IFS	Inter-Frame Space
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control
MLME	MAC Layer Management Entity
MSDU	MAC Service Data Unit
NGN	Next Generation Network
NS	Network Simulator
OSI	Open Systems Interconnection
PCF	Point Coordination Function
PHY	Physical Layer
PIFS	Point Cooordination Inter-Frame Space
QAP	QoS enabled Access Point

QBSS	QoS enabled Base Service Set
QoS	Quality of Service
QSTA	QoS enabled Station
RTS	Request to Send
SI	Service Interval
SIFS	Short Inter-Frame Space
SME	Station Management Entity
TC	Traffic Class
TCP	Transmission Control Protocol
TSPEC	Traffic Specification
TXOP	Transmission Opportunity
UDP	User Datagram Protocol
UTRAN	UMTS Terrestrial Radio Access
VI	Video
VO	Voice
VoIP	Voice over IP
VSTA	Virtual Station
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network

Chapter 1

Introduction

1.1 Background

Recent advancements have seen 802.11 WiFi hotspots become increasingly popular. By using the unlicensed ISM (Industrial, Scientific and Medical) frequency spectrum, Wireless Local Area Networks (WLANs) provide a cheaper alternative for wireless Internet connectivity that achieves relatively high throughput. With the growth of the Internet, home and enterprise WLANs are now being used for applications such as file sharing. More devices, including cellular phones, are being equipped with WiFi capabilities and a significant effort is being put into providing these devices with roaming support. It is envisioned that further growth of WLAN usage will take place and that they will continue to have a major impact on society. WLANs would be able to compete directly with 3G cellular networks as an access technology for multimedia services, since WLAN end users would want to use services like video conferencing and Voice over IP (VoIP) telephony. These services require a certain level of bandwidth guarantees in order meet the performance expected from end users.

Exciting new applications and networked services are putting great demand on Next-Generation- Networks (NGNs). The general idea behind NGN is to provide a multi-service (voice, video and data) platform over an "all-IP" network. Multiple access technologies would be integrated to provide end users with ubiquitous access to network services. WLANs play an indispensable role as an access network technology in NGN deployments. Figure 1.1 shows the typical architecture for Next Generation Networking.

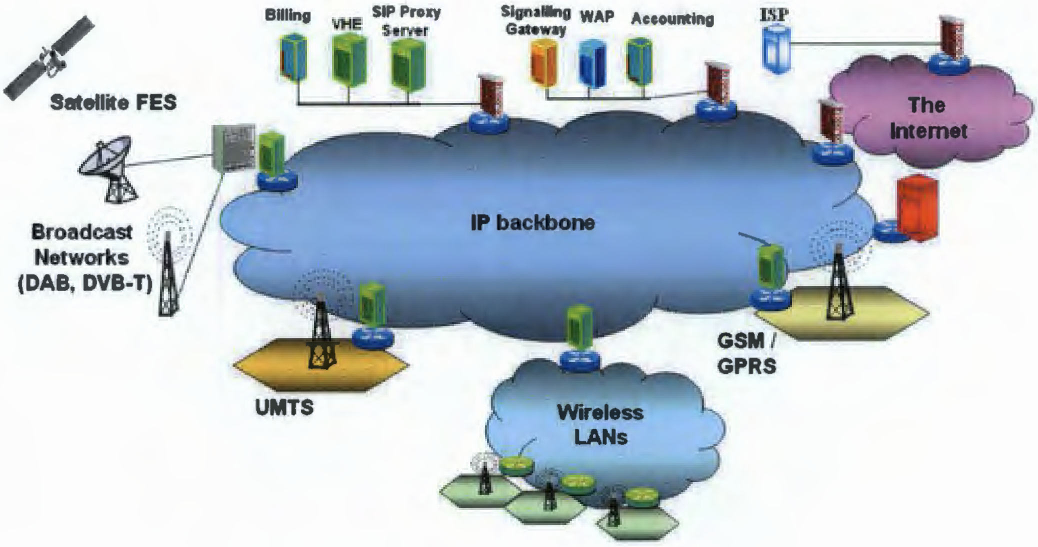


Figure 1.1: Typical architecture of NGNs

An important challenge of NGNs is dealing with the complexity of providing Quality of Service (QoS) support for applications with diverse performance needs. QoS support is mainly implemented in the core of the IP network where resources are assumed to be abundant. While some access networks such as UTRAN, may offer well defined QoS support, others do not provide such support. This is especially the case with IEEE 802.11 WLANs since they traditionally use a "best-effort" medium access technology. For this reason end users of WLANs would not experience predictable network performance.

The IEEE 802.11e enhancement was introduced to overcome the lack of QoS support for legacy IEEE 802.11 WLANs [1]. QoS support is enabled by modifying the Media Access Control (MAC) layer to offer priority-based service differentiation functions, using a multi-queueing model rather than a single queued station described in the original IEEE 802.11 standard. This is achieved by introducing a new coordination function called the Hybrid Coordination Function (HCF). The HCF includes a contention-based channel access scheme known as Enhanced Distributed Channel Access (EDCA), as well as a polling-based channel access function known as HCF Controlled Channel Access (HCCA). EDCA is a mandatory function that extends the Distributed Co-ordination Function (DCF) of the original 802.11 MAC specification. The EDCA supports 4 types of Access Classes (ACs), each with different priorities. Service differentiation is achieved by choosing backoff parameters and inter-frame spaces to give one AC priority over the other. On the other hand, the HCCA is an optional function that provides deterministic channel access scheme by centrally controlling the channel through the Hybrid Coordinator (HC). It supports multiple traffic streams, each having deterministic bandwidth allowances.

The HCCA still requires some major improvements, with the main problem being its failure to cope well with overlapping channels of multiple Access Points (APs). For this reason EDCA is mostly used for QoS support, due to its simplicity and relatively good performance. However, when the channels are heavily loaded the network becomes less capable of satisfying the QoS requirements of time-bounded multimedia traffic. This results in the need for an effective admission control scheme to protect existing traffic flows in the network from new requests, based on resource availability. The need for this effective admission control for IEEE 802.11e is the main motivation behind this thesis.

1.2 Problem Statement

Past work has shown that QoS support can be achieved with the EDCA mode of IEEE 802.11e WLANs [2][3][4]. However, channel overloading still remains a major problem as the network performance is degraded under heavy load. When a new flow is admitted while the network is operating close to full capacity, it may not achieve its required QoS. It may also jeopardize the QoS experienced by other already admitted flows. This is because bandwidth is shared in the physical transmission medium of a WLAN. The effect of channel overloading is undesirable for inelastic traffic from video and voice applications that require a certain level of bandwidth and delay guarantees. For this reason, an efficient admission control mechanism is needed to ensure that admitted flows achieve the required performance. Admission control is especially important for mobile scenarios to aid handover decisions. If the WLAN has insufficient resources to accommodate the traffic flows of the mobile station, the handover request will be rejected by the admission control scheme.

Admission control decisions are based on resource availability in the network. However, it is difficult to quantify the resources within the EDCA due to the probabilistic nature of the MAC layer operations. MAC layer parameters and measurements can be used to estimate the bandwidth available to wireless stations. Thus, it would be advantageous to consider an admission control at the MAC layer, where bandwidth estimations can be made.

Another important concern for WLANs is channel utilization. It is important to maximize the resource utilization, by maximizing the number of admitted flows that can be accommodated by the network capacity.

1.3 Thesis Objectives

The main contribution of this thesis is to present the concept of an admission control scheme that is based on the resource availability in an IEEE 802.11e WLAN MAC layer. It explores the design of this admission control scheme where the requirements are:

- It must be able to guarantee the bandwidth requirements for existing flows admitted into the WLAN.
- It should make effective utilization of the network's resources by accepting the maximum number of flows that can be accommodated by the network's capacity.
- It should be of low computational complexity, so that admission control decisions can be obtained in real-time.
- It must comply with the goals of NGNs i.e., admission of traffic flows should be granted upon request and bandwidth availability.

Furthermore, the thesis will provide the reader with a comprehensive understanding of legacy WLANs and the IEEE 802.11e enhancement as a basis to understanding the project design. Through simulations conducted in NS-2, this thesis will analyze bandwidth statistics at the MAC layer to validate the accuracy and performance of the admission control scheme.

1.4 Scope and Limitations

The principle focus of this thesis is the design and validation of an admission control scheme for IEEE 802.11e WLANs that makes use of bandwidth estimations. A more advanced admission control scheme would involve features such as resource authorisation based on user profiles and network operator specific-policy rules. However, these additional features are handled at higher protocol layers and are thus outside the scope of this thesis.

The IEEE 802.11e amendment recommends that admission control is not required for non-real-time traffic. However, high volumes of best-effort traffic would degrade the performance of real-time flows in the network. For this reason it is important to limit best-effort traffic, however this requirement falls outside the scope of this thesis.

The IEEE 802.11.e enhancement describes two channel access modes, EDCA and HCCA. The HCCA mode is not widely used, whereas the EDCA mode is mandatory and performs reasonably well. For this reason, the scope is limited to the EDCA access mode.

1.5 Thesis Outline

Chapter 2 presents the background that is fundamental to this thesis. The chapter starts with a survey of legacy WLANs, emphasizing the lack of QoS support. It then presents an overview of the IEEE 802.11e amendment that enables QoS support for WLANs. A review of some work related to admission control for EDCA is given. The modelling of WLAN bandwidth is also explored.

Chapter 3 presents the design of a measurement-aided model-based admission control scheme for IEEE 802.11e WLANs. A mathematical analysis for estimating the bandwidth available to EDCA ACs for wireless stations is presented. The relation between admission control, bandwidth estimations and measurements of WLAN conditions is discussed.

Chapter 4 describes the simulation framework for evaluating the performance of the admission control scheme presented in chapter 3. Implementation issues regarding the functional behaviour of an existing simulation framework that supports IEEE 802.11e WLAN capabilities are explored. Extensions made to this existing simulation framework to incorporate the proposed admission control scheme are discussed.

Chapter 5 presents the results obtained from the simulation framework described in chapter 4. The results are analyzed to evaluate the performance proposed admission control scheme. The improved performance of the EDCA due to the introduction of the admission control scheme is validated and discussed.

Chapter 6 draws conclusions based on the findings of this project and simulation results. Possibilities for additional research and recommendations for possible extensions to the work described in this thesis are presented.

Appendix A provide some information about IEEE 802.11 enhancements. Appendix B provides details that are relevant to the implementation of the simulation model and Appendix C describes the contents of the accompanying CD ROM.

Chapter 2

Literature Review

2.1 Legacy IEEE 802.11 Wireless LANs

IEEE 802.11 is a family of specifications for wireless local area networks (WLANs) developed by the Institute of Electrical and Electronics Engineers (IEEE) 802.11 working group. It specifies the operation for the Data Link Layer (layer 2) of the Open Systems Interconnect (OSI) model. It is basically the wireless equivalent of the wired IEEE 802.3 (Ethernet) protocol. 802.11 provides data rates ranging from 2 Mbps extending to 54 Mbps and operates over the unlicensed ISM frequency band. WLANs have a relatively limited range of coverage as compared to the UTRAN of 3G networks. A WLAN link can typically cover up to a maximum range of 100m.

2.1.1 IEEE 802.11 Network Architecture

The 802.11 standard defines two modes of operation: Ad-hoc and Infrastructure mode. The Ad-hoc mode is where a set of 802.11 wireless stations can communicate directly without the use of an Access Point (AP) or any connection to a wired network. The infrastructure mode requires the operation of at least one AP.

Infrastructure Mode

The infrastructure mode is typically used for hotspot deployments and requires the use of at least one AP. An AP is analogous to a hub in an Ethernet network and is able to connect wireless stations to a wired backbone. The wireless stations may not communicate directly without the intervention of the AP. This mode of operation can easily be deployed to provide a WLAN with direct Internet access.

An 802.11 network operating in the infrastructure mode can be arranged as a cellular system where the network is subdivided into cells. Each cell is known as a Basic Service Set (BSS) and is controlled by an AP. An Extended Service Set (ESS) can be formed from two or more BSSs by connecting their APs through a distribution system, typically an Ethernet backbone. The ESS is seen by the upper layers of the OSI model as a single 802.11 network. Figure 2.1 shows a typical ESS.

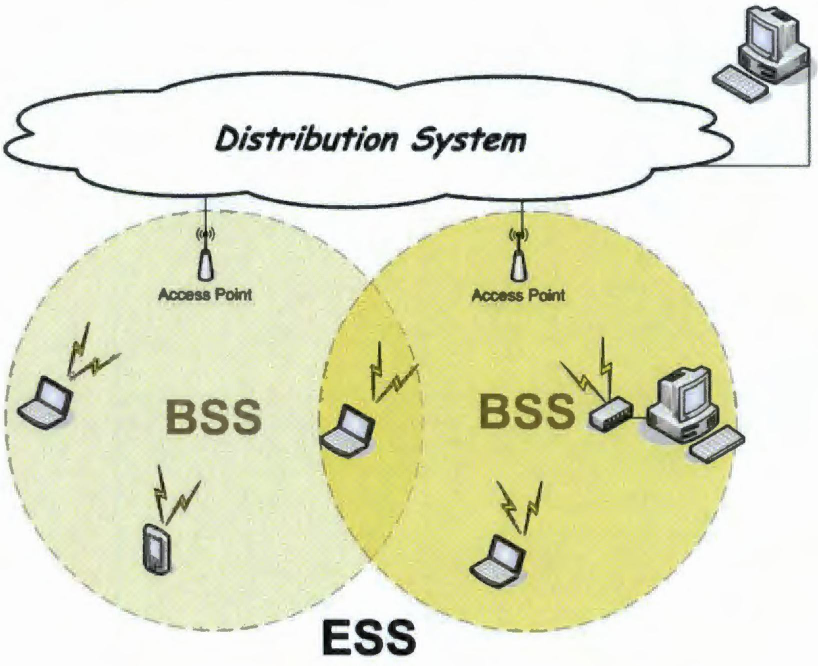


Figure 2.1: Network topology of an ESS

Ad-Hoc Mode

An Ad-Hoc wireless network is a collection of two or more WiFi devices that communicate without the intervention of an AP. Ad-hoc networks are mostly intended for short lived communications between wireless stations, e.g. a file transfer between two notebooks, providing connectivity for participants at a business meeting, etc. An example of an ad-hoc configuration is shown in Figure 2.2.

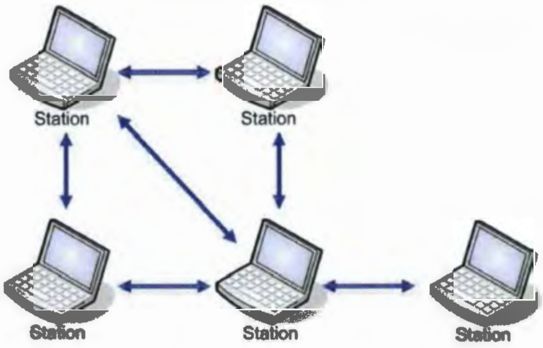


Figure 2.2: An example of an ad-hoc configuration

2.1.2 The Protocol Stack

Figure 2.3 illustrates the components of the protocol stack for the physical and data link layers of the IEEE 802.11 standard. The data link layer consists of the Media Access Control (MAC) Layer and the Logical Link Control (LLC) Layer. The LLC layer provides an interface to the higher layers of the protocol stack.

The MAC layer is responsible for sharing the channel resources in a fair and reliable manner. It is further divided into two sub-layers, the Distributed Coordination function (DCF) and the Point Coordination function (PCF). The DCF specifies a contention based medium access where multiple stations are in "contention" to transmit data frames. The PCF provides a contention free medium access, where the AP polls each station to transmit their frames without contention from the other stations.

The physical layer defines the supported data rates and frequency bands for transmission as well as specifying the encoding and modulations schemes. The modu-

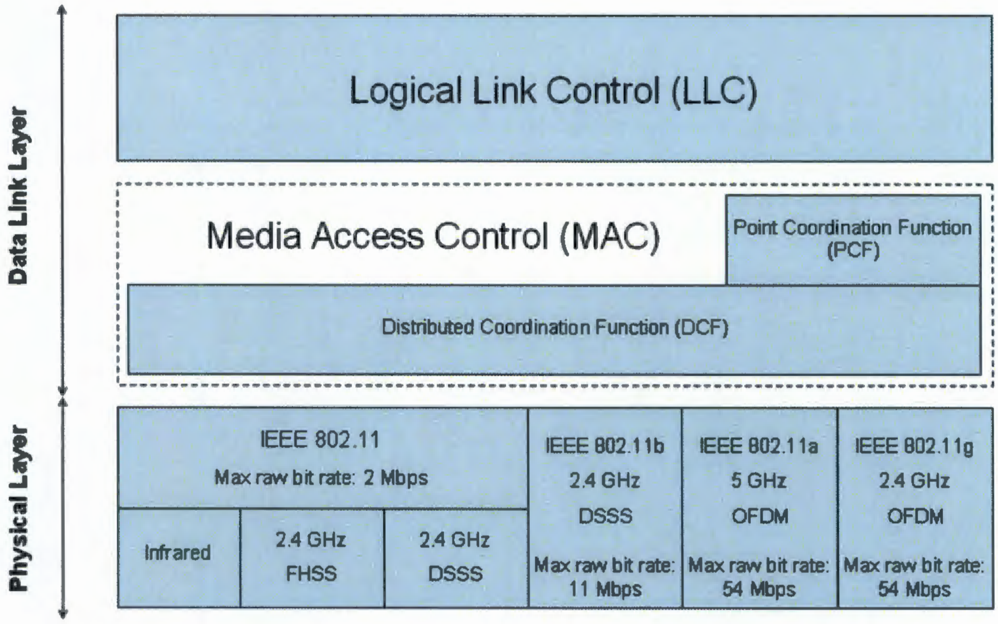


Figure 2.3: The IEEE 802.11 protocol stack

lation schemes defined for original 802.11 standard are Infrared (IR), Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS).

2.1.3 Medium Access

The DCF and PCF define how the stations access the wireless medium. An AP would send beacon frames at regular intervals. These beacon frames will define two periods, the Contention Free Period (CFP) and the Contention Period (CP). The DCF is used during the CP to provide reliable transmission using the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism. PCF is an optional function for WLANs. In the CFP the AP sends Contention Free-Poll (CF-Poll) frames to each station, one at a time, to give them the right to send a frame. The AP is the coordinator that determines which wireless node has the right to transmit. This may facilitate better management of access to the medium. Unfortunately, this mechanism is not widely used due to its problematic behaviour. The unpredictable beacon frame delays and the unknown transmission time of polled stations makes it difficult for the AP to predict and control an effective polling schedule [5]. PCF also doesn't take any QoS parameters into consideration.

DCF makes use of the CSMA/CA protocol that uses Inter-Frame Spaces (IFSs) and Contention Windows (CWs) to provide a reliable transport medium for several stations. The DCF protocol defines two access modes; Basic and RTS/CTS modes.

Basic Mode

The basic mode allows stations to first sense the channel for an idle slot before initiating data transmission. If the channel is idle the wireless station waits for a Distributed Inter-Frame Space (DIFS) before transmitting its frame. When the destination node receives the frame it waits for a Short Inter-Frame Space (SIFS) before sending an acknowledgement (ACK) frame. The acknowledgement is necessary to inform the transmitting node that the transmission was successful and that there was no collision with other stations that were also trying to transmit simultaneously. However, if an ACK is not received the transmitting station would have to perform a backoff algorithm before attempting to resend the frame. The backoff algorithm involves setting a timer to a random value. The wireless station would decrease this backoff timer when the channel is idle. When the backoff timer reaches zero the wireless node may sense the channel to determine if it can transmit. The Contention Window (CW) limits the value of the random integer for the backoff counter. The backoff counter is bounded by minimum and maximum values; CWmin and CWmax. This basic mechanism is shown in the Figure 2.4.

RTS/CTS mode

The second mechanism of the DCF protocol is the RTS/CTS (Request to Send/Clear to Send) handshake, and is primarily focused on solving the hidden node problem. The hidden node problem exists when a node is able to sense the access point, but it may not be able to sense other nodes communicating with the access point. The other nodes may then be hidden to the node and the CSMA/CA mechanisms will fail. An example is shown Figure 2.5. In the example, nodes A and B can each communicate with the AP, but are hidden from each other. When node A is transmitting data, node B will still sense the medium as idle. Node B may then

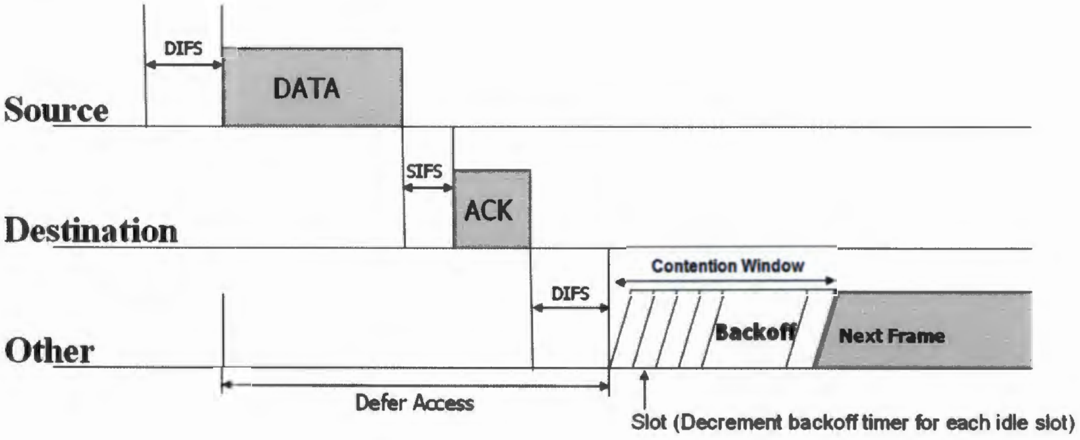


Figure 2.4: Basic DCF mechanism

transmit its own data which would be corrupted along with the data sent by node A.

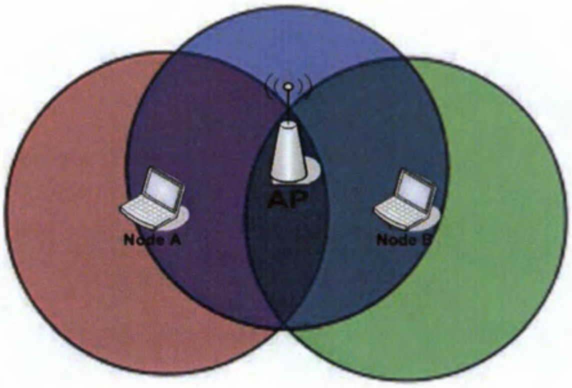


Figure 2.5: The hidden node problem

The solution to this problem involves the transmission of short RTS/CTS frames in order to reserve the channel. When a wireless node wants to transmit frames, it will send a RTS frame to the AP. The AP replies with CTS to acknowledge the RTS frame and to inform all the other nodes to be idle for the required transmission period.

With the RTS/CTS mode, only RTS frames are susceptible to collisions that will trigger the backoff mechanism. This is because stations contend only to transmit RTS frames rather than data frames. Thus, collisions are detected much faster than the basic access mechanism because collisions only occur on the short RTS frames rather than larger data frames. However, the RTS/CTS handshake is not a complete solution to the hidden node problem and will degrade the network's performance due to the additional overhead of RTS/CTS frames.

Shortcomings of the DCF

The main problem with the DCF is that it is virtually impossible to achieve the maximum throughput [6]. A significant percentage of the available raw channel capacity is sacrificed (by the CSMA/CA mechanism) in order to improve the reliability of data transmissions under diverse and adverse environmental conditions [7]. Bandwidth is also lost due to MAC overheads added to MAC layer Service Data Units (MSDUs) that are transmitted over an 802.11 channel. Furthermore, the performance will degrade when channels are heavily loaded because collisions are more likely. When a collision occurs, a portion of the bandwidth is wasted. Collisions also expand the range of contention windows, resulting in larger backoff counter values thus introducing more idle slots. The DCF also has limitations when it comes to QoS support, since the CSMA/CA mechanism operates without any knowledge of high or low priority traffic. Furthermore, once a station is granted access to the medium, it may keep the medium for as long at it is transmitting data. If a station has a low bit rate, it will take a long time to send its frames, hence all other stations will wait longer to transmit their frames.

2.1.4 IEEE 802.11 Wireless LAN Protocols

The original 802.11 standard was released in 1997 and specifies two raw data rates of 1 and 2 Mbps to be transmitted in the ISM frequency band at 2.4 GHz [8]. Further physical layer enhancements has been made to this standard to increase the raw data rates of wireless stations.

IEEE 802.11b

The 802.11b amendment to the original standard was ratified in 1999 [9]. The standard uses the DSSS modulation scheme with advanced encoding techniques to achieve data rates of up to 11 Mbps. Due to the CSMA/CA protocol overhead, in practise the maximum 802.11b throughput that can be achieve is severely reduced as the channels become more congested [10]. 802.11b products appeared on the market on a wide scale mainly due to the dramatic increase in throughput (compared to the original standard) together with substantial price reductions. This led to the rapid acceptance of 802.11b as the definitive wireless LAN technology.

IEEE 802.11a

The 802.11a amendment to the original standard was ratified in 1999 [11]. The 802.11a standard uses the same core protocol as the original standard, but it operates in the 5 GHz frequency band and uses a 52-subcarrier Orthogonal Frequency-Division Multiplexing (OFDM) scheme. It has a theoretical maximum raw data rate of 54 Mbps, however the realistic net achievable throughput is in the range of 20 Mbps. Using the 5 GHz band gives this standard the advantage of having less interference, since the 2.4 GHz is heavily used (Bluetooth, microwaves, etc). However, the high frequency carrier also means that 802.11a cannot penetrate as far as 802.11b since it is absorbed more readily by objects. This restricts the use of 802.11a to only clear line of sight, thus the range of coverage is reduced. 802.11a may require more access points to achieve a reasonable area of coverage than 802.11b. Due to the usage of different frequency bands, 802.11a is not interoperable with 802.11b, except for the case where the equipment implements both standards.

IEEE 802.11g

The 802.11g specification achieved standard status in July 2003 [12]. It is also based on OFDM with a maximum raw data rate of 54 Mbps, while its realistic net throughput is also in the range of 20 Mbps. 802.11g is designed to operate in the 2.4 GHz band so that it can be backward compatible with 802.11b. The 802.11g standard penetrated the consumer world immediately after ratification. Despite its major acceptance, 802.11g also suffers from the same interference as 802.11b due to the heavily used 2.4 GHz frequency bands.

Table 2.1: Parameters of the fundamental 802.11 standards

Protocol	**Release date**	**Frequency band**	**Modulation**	**Maximum data rate**	**Link coverage**
Legacy 802.11	1997	2.4-2.5 GHz	IR	2 Mbps	100m
802.11b	1999	2.4-2.5 GHz	DSSS	11 Mbps	100m
802.11a	1999	5.15-5.35/5.47-5.725/5.725-5.875 GHz	OFDM	54 Mbps	50m
802.11g	2003	2.4-2.5 GHz	OFDM	54 Mbps	100m
802.11n	2003 (draft)	2.4 GHz or 5 GHz bands	DSSS/OFDM	540 Mbps	125m

IEEE 802.11n

In January 2004 IEEE announced that it had formed a new Task Group to develop a new amendment to the 802.11 standard for WLANs [13]. The estimated maximum raw data rate is expected to be around 540 Mbps which is almost 50 times faster than 802.11b, and 10 times faster than 802.11a and 802.11g. 802.11n builds upon previous 802.11 standards by adding Multiple-Input Multiple-Output (MIMO) techniques. MIMO makes use of spatial multiplexing and advanced coding schemes to achieve a high throughput. According to "IEEE 802.11 Working Group Project Timelines", the 802.11n standard is not due for final approval until March 2009 [14]. Table 2.1 shows the fundamental 802.11 standards at a glance:

2.1.5 WLAN Enhancements

Section 2.1.4 explores a set of physical layer specifications that are fundamental to the operation of WLANs. Additional MAC layer enhancements have been defined to address certain shortcomings of the original standard and can be used to enrich these fundamental specifications. A number of IEEE working groups are currently tasked with enhancing the functionality of 802.11-based networks. Appendix A provides some insight on a few significant enhancements that have been released as well as some that are expected to be released in the future.

2.2 The IEEE 802.11e QoS Enhancement

The IEEE 802.11e enhancement was introduced to overcome the lack of QoS support for the legacy IEEE 802.11 standard [1]. It became an approved standard late in 2005, and defines a set of QoS enhancements for WLAN applications. This is imperative for real-time multimedia applications such as video streaming. It specifies enhancements to the legacy IEEE 802.11 MAC layer shown Figure 2.6. A new coordination function called the Hybrid Coordination Function (HCF), controlled by a Hybrid Coordinator (HC), is defined. A HC is situated in every QoS enabled Access Point (QAP). HCF specifies two channel access modes; Enhanced Distributed Channel Access (EDCA) and HCF Controlled Channel Access (HCCA). Both EDCA and HCCA define Traffic Classes (TC) that provide service differentiation. The PCF is an optional element providing contention-free service for those stations that are unable to conform to the HCF of the IEEE 802.11e standard. The DCF is used to provide a reliable transport medium using the CSMA/CA mechanism.

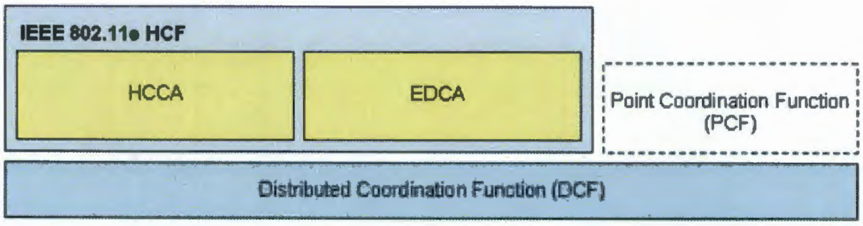


Figure 2.6: MAC enhancement for IEEE 802.11e

2.2.1 Enhanced Distributed Channel Access (EDCA)

EDCA allows service differentiation by supporting 8 different priorities, which are further mapped to 4 Access Classes (ACs) as shown in Table 2.2. The 8 priorities originate from higher layers of the protocol stack depending on QoS mechanisms enforced at the IP layer, such as Differentiated Services (DiffServ) [15]. The DiffServ architecture is a framework for providing QoS support in IP networks and is widely accepted due to its scalability and simplicity. A mapping scheme from 8 DiffServ priorities to the EDCA ACs can easily be implemented through a collaborative architecture [16, 17]. The 4 ACs support voice, video, best-effort and background data traffic. Each AC behaves as a single Enhanced DCF (EDCF) contending entity with dedicated queues as shown in Figure 2.7. A single AC queue can be seen as an individual Virtual Station (VSTA), as they all contend for the shared wireless medium independently. Differentiation is achieved by varying the amount of time a VSTA will sense the channel to be idle and the length of the contention window during backoff. This is achieved by differentiating an Arbitration Inter-Frame Space (AIFS), initial window size and maximum window size for each AC. The AIFS is used for the ACs instead of the DIFS for legacy 802.11 wireless stations. For each $AC[i]$; $(i \in \{0, 1, 2, 3\})$, the minimum backoff window size is $CW_{\min}[i]$, the maximum backoff window size is $CW_{\max}[i]$, and the AIFS is $AIFS[i]$. The values of these parameters are announced by the QAP via periodically transmitted beacon frames. The virtual collision handler is used to resolve internal collisions by allowing the frame with higher priority to be transmitted, while the lower priority VSTA invokes a backoff algorithm. This means that a lower priority internal VSTA will not cause a higher priority internal VSTA to backoff. This makes the IEEE 802.11e enhancement more efficient when handling internal collisions.

Table 2.2: Priority access category mappings

User Priority (UP)		AC	Designation
Lowest	1	0	Background
	2	0	Background
	0	1	Best Effort
	3	1	Best Effort
	4	2	Video
	5	2	Video
	6	3	Voice
Highest	7	3	Voice

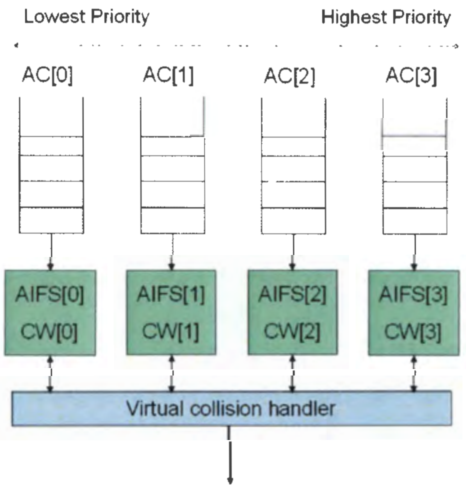


Figure 2.7: EDCA queueing architecture

Both basic access and RTS/CTS modes are supported by the EDCA. Before data transmission, each VSTA has to contend for a Transmission Opportunity (TXOP). Data transmission begins when the medium is idle for more than the AIFS time. The same backoff algorithm is performed when unsuccessful transmissions occur however, different window size parameters are used. A TXOP can be obtained when the backoff timer reaches zero. Figure 2.8 demonstrates the EDCA timing for the basic access mechanism, where three ACs are shown. An AC with smaller $AIFS$, CW_{min} and CW_{max} has a better chance of accessing the wireless medium earlier and will thus experience better QoS.

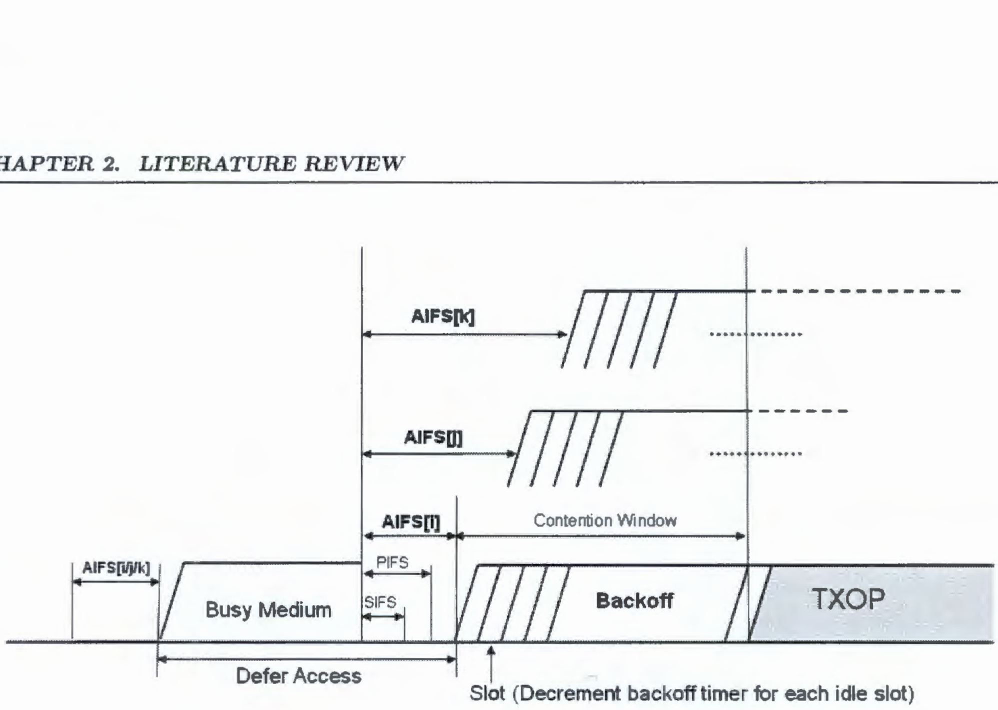


Figure 2.8: EDCA timing diagram

For each AC queue the initial backoff counter will be a random value that is uniformly distributed between zero and $CW_{\min}[AC]$. When the destination station receives the frame, it waits for a SIFS before sending back an ACK frame. The acknowledgement is necessary to inform the transmitting node that the transmission was successful. An unsuccessful transmission is assumed to be caused by a collision with data from other transmitting stations. If a collision occurs the transmitting station will first set its backoff timer to be $random(0,\ (CW_{\min}[AC]+1)\times 2i-1)$ for each retransmission attempt i. In other words, the contention window size is doubled for each retransmission to reduce the probability of a collision. The contention window is also bounded by a maximum value of $CW_{max}[AC]$, thus there is only a finite number of backoff stages where the contention window is doubled.

Contention Free Bursting (CFB)

The IEEE 802.11e standard also specifies an optional medium access transmission mode, where multiple MSDUs are allowed to be transmitted during a TXOP. This is known as Contention Free Bursting (CFB) and the duration of the TXOP is limited for each AC. CFB may be used to improve efficiency by minimizing contention in the network. The basic idea is that an AC may transmit additional data if there is enough time remaining in a granted TXOP. The AC is allowed to resume transmission after a SIFS delay, rather than contending for the medium again. Figure 2.9 shows a timing structure where a TXOP is granted to an AC. The figure shows the transmission of two data frames. The second frame did not have to content to access the medium.

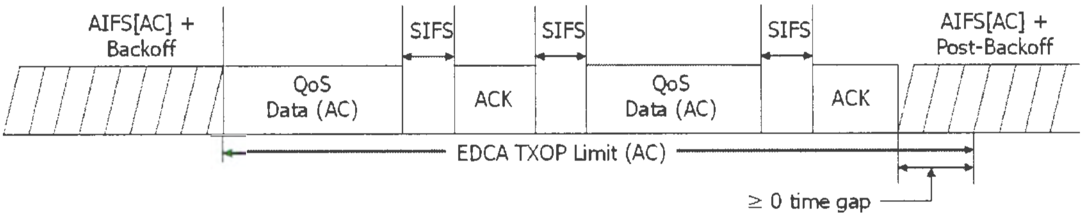


Figure 2.9: CFB timing structure for the wireless medium

The use of CFB increases system throughput without unacceptably degrading other system performance measures [3]. CFB may especially be useful for improving the throughput of 802.11g stations when in the presence of 802.11b devices. An 802.11g station can send more MSDUs during a TXOP than an 802.11b station. In this way, 802.11g stations would not compromise their transmission rates due to the presence of stations with lower transmission rates. The CFB mechanism also allows fair bandwidth allocations for voice and video applications. By default, Larger TXOPs are allocated to the AC(VI) than AC(VO) because video traffic requires more bandwidth than voice traffic.

2.2.2 HCF Controlled Channel Access (HCCA)

The HCF provides deterministic channel access by centrally controlling the channel through the HC (Hybrid Coordinator) [2]. The HCF Controlled Channel Access (HCCA) mode is a major improvement on the legacy PCF contention free channel access. In HCCA the QAP polls the stations for a TXOP duration, which is calculated from reservation requests sent by the stations. The polling schedule and TXOP allocations are based on the requirements of traffic streams. The TXOP is initiated by a poll request from the QAP allowing transmissions to occur in either the uplink or downlink directions. Figure 2.10 shows the multiplexing of HCCA and EDCA channel access schemes. The Service Interval (SI) is the time duration between successive polls for TXOPs. The SI satisfies the delay requirements of each flow, and is a submultiple of the beacon interval duration.

The maximum time spent in HCCA for each SI is limited by the *dot11CAPMax* variable, and the total controlled access time in a beacon interval is limited by *dot11CAPRate* variable. The duration of the controlled access period can be limited using these Management Information Base (MIB) variables.

The HCCA still requires some major improvements, as it does not cope well with overlapping QoS Base Service Sets (QBSSs). Because of the deterministic approach of the HCF, its scheduling algorithm can be efficient only if the traffic being serviced is strictly CBR [18]. For this reason EDCA is mostly used to provide QoS support due to its simplicity and relatively good performance.

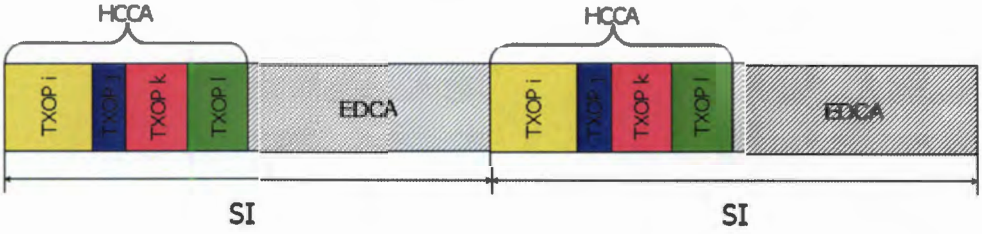


Figure 2.10: EDCA/HCCA multiplexing

2.2.3 Optional Features for the IEEE 802.11e Standard

Many additional features are defined under the 802.11e specification. These enhanced acknowledgement procedures, active power save delivery and a direct link protocol. These features aim to improve the performance of the 802.11e network and are described in this Appendix A.

2.3 Admission Control in IEEE 802.11e

Despite achieving service differentiation for EDCA ACs, the bandwidth of WLANs is limited meaning that QoS guarantees can only be satisfied when the network is not overloaded. For this reason, the need for admission control has become apparent to prevent QoS degradation due to overloading. The HC is responsible for admission control decisions at the QAP. The IEEE 802.11e standard specifies the use of Traffic Specification (TSPEC) messages for negotiating admission control in IEEE 802.11e WLANs. QSTAs use TSPEC messages to specify their traffic flow requirements such as, packet size, service interval, data rate and delay. The HC may accept or reject a new TSPEC request based on network conditions.

Fig 2.11 shows a typical TSPEC negotiation between a QoS enabled station (QSTA) and the HC. TSPEC negotiation for a new Traffic Stream (TS) request is always initiated by the Station Management Entity (SME) of a QSTA and accepted or rejected by the HC. The SME allows higher layer protocols and applications, such as RSVP, to allocate resources within the MAC layer. The SME of the QSTA indicates its TSPEC to its MAC layer via a MLME-ADDTS (MAC Layer Management Entity-ADDTS) request. The QSTA MAC interface will then forward the ADDTS request to the HC, while starting the ADDTS respond timer. The MAC layer of the HC will then generate the MLME_ADDTS indication for its SME. The Admission Control Unit (ACU) in the HC's SME will decide whether to accept or reject the TS request. Once decided, the HC will notify the QSTA with an appropriate response. If the response times out the request message will be resent.

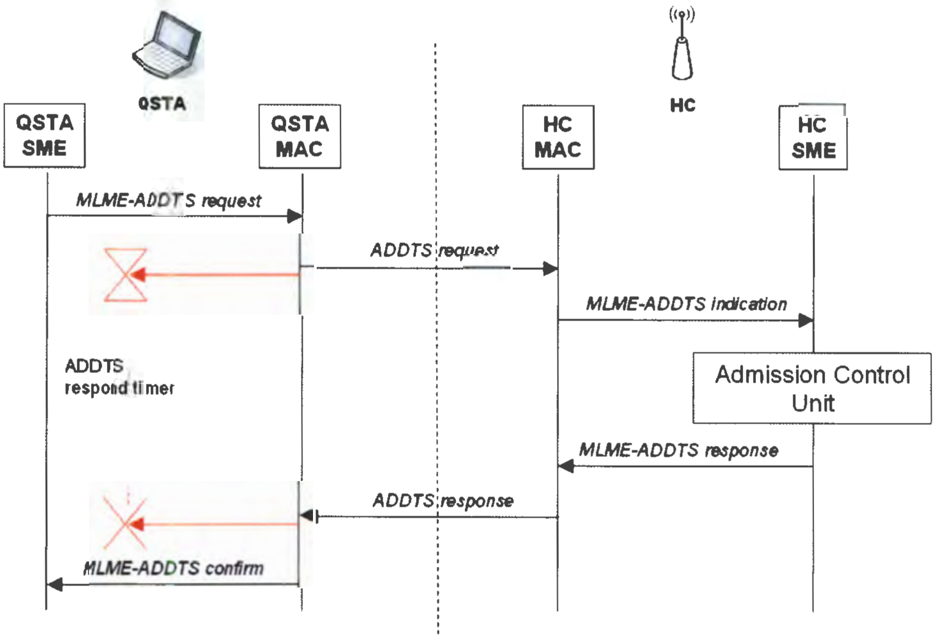


Figure 2.11: TSPEC negotiation

2.3.1 IEEE 802.11e EDCA Admission Control Mechanisms for EDCA

This section presents some fundamental contributions to the research related to admission control for 802.11e WLANs.

Distributed Admission Control (DAC)

A Distributed Admission Control (DAC) scheme was proposed by the 802.11e working group to protect the QoS of active flows [19]. With the DAC, the AP attempts to limit the transmission duration of each AC. The QAP announces a transmission budget for each AC, every beacon interval. The transmission budget is the additional amount of transmission time available for an AC during the next beacon interval. It is calculated by subtracting the measured occupied time, during the previous beacon interval, from the transmission limit of the AC. The transmission limits for the ACs are determined inside the wireless stations. It is based on the successfully used transmission time during the previous beacon period and the transmission budget announced from the QAP. When the transmission budget for an AC is depleted. a new flow would not obtain any transmission time, and existing flows would not be permitted to increase their transmission time.

It was shown that the DAC scheme is able to protect admitted real-time flows in EDCA so that they can achieve the desired bandwidth. However. the DAC scheme can only protect existing EDCA flows when the traffic load is not very heavy. This means that some flow admission requests may be rejected. even though they could be accommodated by the network. Thus the DAC scheme is unable to make optimal use of the network's resources. Another shortcoming of the DAC scheme is the difficulty of avoiding network performance fluctuations, since stations would continuously adjust their transmission parameters during every beacon interval.

Threshold-Based Admission Control

Daquing Gu and Jinyun Zhang proposed a Threshold Based Admission Control scheme [20]. In this scheme, each station needs to measure traffic conditions on the wireless link. The network defines suitable upper and lower bound threshold values that indicate the current network load. The network load can be indicated using either average collision ratios, or relative occupied bandwidth indications. The admission control scheme takes no action when the network load is between the defined upper and lower threshold values. When the chosen metric indicates that the network load is above the higher threshold, the network will stop the transmission of the lowest active AC for the next beacon period. When the network load is below the lower bound threshold value, the inactive AC with highest priority will be resumed during the next beacon period.

The advantage of this scheme is that it can easily be implemented for both ad-hoc and infrastructure mode. However, the threshold values are difficult to set. In addition, since the transmission of data flows are stopped and resumed depending on the network condition, there is no way to guarantee the bandwidth requirements.

Model-Based Admission Control

Dennis Pong and Tim Moors proposed an admission control scheme based on a two-state Markov chain model for IEEE 802.11 Wireless LANs [21]. The scheme estimates the bandwidth that flows would achieve if a new flow with certain parameters were admitted. The new flow is admitted only if it can achieve its required bandwidth, at the same time bandwidth guarantees for all other existing flows should be preserved. The model deals with EDCA parameters, i.e., minimum contention window size and transmission opportunity duration, as well as measured collision statistics. The analytical model is derived under saturation conditions, as admission control usually becomes assertive when the network is saturated [22]. Their work also adjusts the contention window parameters so that the goals of admission control can be achieved.

The advantage of using this model-based admission control algorithm is that it is able to provide quantitative bandwidth guarantees for EDCA. However, accurate estimations can only be obtained if there are no more than one flow admitted per AC for each station. This makes the admission control scheme unable to cope with the diverse needs of new multimedia applications. The work also does not take virtual collisions into consideration. The continuous adjustments of the contention windows may also lead to severe fluctuations of the network's performance and estimates of the achievable bandwidth for flows. Another problem is that the fundamental analytical model used for this admission control scheme assumes that the wireless network is fully saturated. Thus the queues of each station in the network must always be non-empty for the the admission control scheme to be effective. This is not very practical, since a scenario where a WLAN experiences non-saturation conditions occurs often.

However, this work still remains a very promising prospect, as a model-based admission control scheme may lead to the best solution for providing quantitative bandwidth guarantees while making optimal utilization of network resources.

2.4 Modelling the Bandwidth Availability for WLANs

There are two main approaches for estimating available bandwidth within a WLAN [22][23]. Both approaches attempt to model the available bandwidth of a network at saturated level. This means that both analytical models assume that the queues of all stations in the network are always non-empty. The first analytical approach is based on a stochastic (Markovian) process, known as a Bianchi model. The second analytical approach is based on an averaging analysis of the state of the network. The second approach is proved to be less complex; however, the Bianchi model provides more accurate bandwidth estimations. The second approach also fails to incorporate some basic design principles of DCF mechanisms, especially the RTS/CTS access method. For this reason the Bianchi model is more accepted in literature for modelling bandwidth availability within a WLAN.

2.4.1 The Bianchi Model [22]

The Bianchi analytical model was developed for the original 802.11 standard to determine the maximum system throughput at a saturation level. It assumes an error free wireless channel, and that there are no hidden stations present. Thus any erroneous data frames received are assumed to be a result of a collision in the shared wireless medium. When the network is in a stable saturated state the conditional collision probability (p) and the transmission probability (τ) are assumed to be constant and independent for each station. The network is considered to be in a stable saturated state when it is completely congested and all the queues are constantly attempting to transmit data. To facilitate the understanding of this analytical model some notations are defined in Table 2.3.

Table 2.3: Main notations used in the Bianchi analytical model

n	Number of active stations in the WLAN
W	Minimum window size for backoff slots
m	Maximum backoff stage (Maximum window size is $2^{\mathrm{m}}W$)
p	The conditional probability that each frame collides constantly and independently
τ	The probability that a station transmits in a randomly chosen time slot
$b(t)$	The random process of the backoff time counter for a given station
$s(t)$	The random process of the backoff stage for a given station at time t
$b_{\mathrm{i,k}}$	$\lim_{t\to\infty} P\{s(t)=i,\, b(t)=k\}$, $i \in [0,m]$, $k \in [0, W-i]$ This represents the stationary distibution of the markov chain from the Bianchi model
P_{tr}	The probability that there is at least one transmission in a slot
P_{s}	The probability that there is a successful transmission in a slot
T_s	The cycle duration time that the medium is sensed busy due to a successful transmission
T_c	The cycle duration time that the medium is sensed busy due to a collision
S	The normalized channel utilization rate of successful payload transmissions
$E\{P\}$	The average packet payload size used to transmit data over the wireless medium
σ	Slot time

To obtain values for p and τ, a discrete-time Markov chain model that is based on a steady-state stationary distribution of the backoff counter is deployed. The probabilities p and τ can be obtained by numerically solving the following system of non-linear equations:

$$b_{0,0} = \frac{2(1-2p)(1-p)}{(1-2p)(W+1)+pW(1-(2p)^m)} \tag{2.1}$$

$$\tau = \frac{1-p^{m+1}}{1-p} b_{0,0} \tag{2.2}$$

$$p = 1-(1-\tau)^{n-1} \quad ; valid\, for\ p \neq 1 \tag{2.3}$$

In (2.1), $b_{0,0}$ represents the probability that the backoff counter is zero at the first backoff stage. The probabilities P_{tr} and P_{s} can then be calculated using τ as shown in the following equations:

$$P_{\mathrm{tr}} = 1-(1-\tau)^n \tag{2.4}$$

$$\begin{aligned} P_{\mathrm{s}} &= \frac{n\tau(1-\tau)^{n-1}}{P_{\mathrm{tr}}} \\ &= \frac{n\tau(1-\tau)^n}{1-(1-\tau)^n} \quad ; where\ n > 0 \end{aligned} \tag{2.5}$$

The saturation throughput of successful frames can be obtained by:

$$\begin{aligned} S &= \frac{E\{Payload\, Information\, Transmitted\, in\, a\, time\, slot\}}{E\{Length\, of\, a\, time\, slot\}} \\ &= \frac{P_{\mathrm{s}} P_{\mathrm{tr}} E\{P\}}{(1-P_{\mathrm{tr}})\sigma + P_{\mathrm{s}} P_{\mathrm{tr}} T_{\mathrm{s}} + (1-P_{\mathrm{s}}) P_{\mathrm{tr}} T_c} \end{aligned} \tag{2.6}$$

Table 2.4: Cycle duration times of the basic and RTS/CTS access mechanisms for successful and unsuccessful transmissions

Access Scheme	**Cycle**	**Frame sequence in cycle duration**
Basic	T_s	Data frame + SIFS + ACK + DIFS
	T_c	Data frame + DIFS + ACK_Timeout
RTS/CTS	T_s	RTS + SIFS + CTS + SIFS + Data frame + SIFS + ACK + DIFS
	T_c	RTS + DIFS + CTS_Timeout

The cycle duration times for a collision (T_c) and a successful transmission (T_s) are the times required to transmit their associated frame sequences, including preambles and physical layer headers. The time to transmit these frame sequences depends on the medium access mechanism used by the DCF as shown in Table 2.4.

Extensive simulations show that this model is extremely accurate in predicting the system throughput at a saturation level [22]. The simulation results were observed for both basic and RTS/CTS mechanisms.

2.4.2 Extending the Bianchi Model for EDCA

The new features of the EDCA provide a challenge for extending the Bianchi model, e.g., different AIFS, CW and virtual collision handling. Extending the Bianchi model for EDCA involves modelling an AC queue as a Virtual Station (VSTA). An AC queue can be seen as a VSTA because it contends for the shared medium access independently. Since each AC has different parameters (AIFS, CW, TXOP) their collision probabilities and transmission probabilities have to be modelled accordingly. Equations (2.1) and (2.2) are thus modified to:

$$b[\mathrm{AC}]_{0,0} = \frac{2(1-2p[\mathrm{AC}])(1-p[\mathrm{AC}])}{(1-2p[\mathrm{AC}])(W[\mathrm{AC}]+1)+p[\mathrm{AC}]W[\mathrm{AC}](1-(2p[\mathrm{AC}])^{m[\mathrm{AC}]})} \tag{2.7}$$

$$\tau[\mathrm{AC}] = \frac{1-p[\mathrm{AC}]^{m[\mathrm{AC}]+1}}{1-p[\mathrm{AC}]} b[\mathrm{AC}]_{0,0} \tag{2.8}$$

Equations (2.7) and (2.8) incorporate the maximum backoff stage and congestion window parameters for each AC. The collision probabilities for each AC (VO, VI, BE or BK) are modified to:

$$\begin{aligned} p[\mathrm{VO}] &= 1-(1-\tau[\mathrm{VO}])^{n[\mathrm{VO}]-1}(1-\tau[\mathrm{VI}])^{n[\mathrm{VI}]} \\ &\times (1-\tau[\mathrm{BE}])^{n[\mathrm{BE}]}(1-\tau[\mathrm{BK}])^{n[\mathrm{BK}]} \end{aligned} \tag{2.9}$$

$$\begin{aligned} p[\mathrm{VI}] &= 1-(1-\tau[\mathrm{VO}])^{n[\mathrm{VO}]}(1-\tau[\mathrm{VI}])^{n[\mathrm{VI}]-1} \\ &\times (1-\tau[\mathrm{BE}])^{n[\mathrm{BE}]}(1-\tau[\mathrm{BK}])^{n[\mathrm{BK}]} \end{aligned} \tag{2.10}$$

$$\begin{aligned} p[\mathrm{BE}] &= 1-(1-\tau[\mathrm{VO}])^{n[\mathrm{VO}]}(1-\tau[\mathrm{VI}])^{n[\mathrm{VI}]} \\ &\times (1-\tau[\mathrm{BE}])^{n[\mathrm{BE}]-1}(1-\tau[\mathrm{BK}])^{n[\mathrm{BK}]} \end{aligned} \tag{2.11}$$

$$\begin{aligned} p[\mathrm{BK}] &= 1-(1-\tau[\mathrm{VO}])^{n[\mathrm{VO}]}(1-\tau[\mathrm{VI}])^{n[\mathrm{VI}]} \\ &\times (1-\tau[\mathrm{BE}])^{n[\mathrm{BE}]}(1-\tau[\mathrm{BK}])^{n[\mathrm{BK}]-1} \end{aligned} \tag{2.12}$$

The rest of the parameters, being AIFS and TXOP are used to determine the cycle duration times T_c and T_s. Once these variables are determined the system throughput for the four ACs can be obtained by following the procedures described in section 2.4.1.

Equations (2.9) to (2.12) form a set of non-linear equations that can be solved using complex numerical techniques. There has been research work yielding a closed form solution of these non-linear equations in a fairly accurate manner [24, 25, 26, 27]. However, these works focus primarily on accuracy of modelling the bandwidth availability and neglect the computational complexity required for obtaining solutions.

2.5 Discussion

This chapter described the some limitations of the legacy 802.11 MAC layer. These are mainly the bandwidth losses when the wireless channels become heavily loaded and the lack of QoS support. This chapter then described many features of the IEEE 802.11e amendment that provides a platform to support QoS in WLANs for multimedia applications.

Research work on admission control mechanisms for IEEE 802.11e EDCA WLANs were surveyed. The main objectives of admission control set out in this thesis, is to protect admitted flows from new requests while accommodating the maximum amount of flows according to the network's capacity. All the techniques described in this chapter were unable to satisfy both these conditions simultaneously. However, a promising prospect of a model-based admission control scheme was found to satisfy the aims of an effective admission control solution.

Furthermore, this chapter looked at literature on modelling the bandwidth availability for WLANs using analytical models. The most promising model that was investigated is the Bianchi model, because of its ability to be extended to EDCA as well as its ability to adapt to medium access mechanisms of legacy DCF (Basic and RTS/CTS mode), and EDCA (CFB). However, there are several problems that were observed for the extensions of the Bianchi model. The first one is that these models are derived under saturation conditions, assuming that each station always has frames to transmit. This is not always true since a practical scenario of a WLAN often experiences non-saturation conditions. Another major obstacle for utilizing analytical models based on multi-dimensional Markov chain analysis is the high computation complexity of these models. It may not be possible to find a feasible solution for the set of non-linear equations in real-time. Although these models may provide good accuracy, the high computational complexity may prevent them from being used for on-line call admission control algorithms in IEEE 802.11e networks. It is also desirable to model the achievable bandwidth for each VSTA to facilitate an admission control scheme that is able to protect the bandwidth guarantees of all flows. Thus existing models would have to be extended.

Chapter 3

A Measurment-Dependent Model-Based Admission Control Scheme for IEEE 802.11e WLANs

3.1 Introduction

In Chapter 2 a review of literature related to admission control in 802.11e EDCA WLANs was explored. A model-based admission control scheme was identified for providing quantitative bandwidth guarantees. However, an accurate bandwidth estimation requires heavy computational processes that are unacceptable for real-time admission control solutions. This chapter presents a measurement aided model-based EDCA admission control scheme that is a modification to the solution presented in [21]. The analytical model from Bianchi is modified to provide more accurate bandwidth estimations, especially when the AC queues contain multiple flows. Bandwidth estimation techniques for single EDCA Virtual Stations (VSTAs) are incorporated into the admission control scheme to support bandwidth guarantees. The main idea behind this admission control scheme is to make effective admission control decisions based on estimated bandwidth availability. A new traffic flow request may be accepted into the network only if estimation shows that it can achieve its required bandwidth and will not jepordize the bandwidth guarantees of already admitted flows.

The scheme uses network measurements to aid bandwidth estimation for VSTAs. Complex and iterative numerical techniques are required to determine the collision probabilities for each VSTA as discussed in Section 2.4.2. With the proposed admission control scheme, collision statistics are measured at each VSTA to ease the computation of collision probabilities (p). This allows admission control decisions to take place in real-time. The scheme also measures EDCA queue activity so that achievable bandwidth can be estimated for both saturated and non-saturated conditions. This admission control scheme would protect the QoS of admitted flows, while making optimal use of the network's resources.

3.2 Estimating Achievable Bandwidth for EDCA Virtual Stations

The bandwidth estimations are made based on the legacy IEEE 802.11 MAC analytical model presented in [22]. The analytical model is extended so that it can be used for estimating achievable bandwidth for EDCA VSTAs. Each AC queue is modelled as a VSTA, because they contend for the access medium independently. The analytical model is also extended to accommodate non-saturation conditions, since the original Bianchi model only considers saturation conditions. The reason for this is that a completely saturated scenario, where all the queues in the network are always non-empty, rarely exists in real networks. The extended model is aided by the measurement of packet collision probabilities and queue activities. To facilitate the understanding of the bandwidth estimation process, some notations are defined in Table 3.1.

Table 3.1: Notations used for calculating the estimated bandwidth

S_i	Estimated bandwidth for Virtual Station i
$E\{P_i\}$	Average packet payload size at a Virtual Station i
$P(C)$	The probability of a collision in a slot
$P(S)$	The probability of a succesful transmission in a slot
$P(I)$	The probability of an idle slot
$P(Tx)$	The probability of at least one transmission in a slot
$P(S\|VS=i)$	The probabilty of a succesful transmission for Virtual Station i
$T_{col,i}$	The cycle duration time that the medium is sensed busy by Virtual Station i, due to a collision
$T_{suc,i}$	The cycle duration time that the medium is sensed busy by Virtual Station i, due to a sucessful transmission
σ	Slot time
β_i	Queue activity factor for Virtual Station i
W_i	The minimum contention window size for Vitual Station i
m_i	The maximun backoff stage for Virtual Station i (Maximum contention window size is $2^{m_i}W_i$)
n	Number of active Virtual Stations in the WLAN
p_i	The conditional probability that frame from Virtual Station i collides constantly and independently
$\tau_{sat,i}$	The probability Virtual Station i transmits in a randomly chosen slot time, assuming saturation conditions
τ_i	The estimated transmission probability for Virtual Station i
AIS	Average Idle Slots
AEB	Average Exponential Backoff
SI	Service Interval
$AIFS$	The number slot for an Arbitration Inter-Frame Space (AIFS) period

If the transmission probabilities of each VSTA are known, the estimated achievable bandwidth would be given by S_i in (3.1):

$$S_i = \frac{P(S|VS=i)E\{P_i\}}{P(C)T_{col,i} + P(I)\sigma + P(S)T_{suc,i}} \tag{3.1}$$

The denominator in (3.1) is the average cycle duration for a transmission. The

Table 3.2: Cycle duration times of different access schemes

Access Scheme	**Cycle**	**Frame sequence in cycle duration**
Basic	$T_{suc,i}$	Data frame + SIFS + ACK + AIFS[AC = i]
	$T_{col,i}$	Data frame + AIFS[AC = i] + ACK_Timeout
RTS/CTS	$T_{suc,i}$	RTS + SIFS + CTS + SIFS + Data frame + SIFS + ACK + AIFS[AC = i]
	$T_{col,i}$	RTS + AIFS[AC = i] + CTS_Timeout
TXOP	$T_{suc,i}$	TXOP[AC = i] + AIFS[AC = i]
	$T_{col,i}$	Data frame + AIFS[AC = i] + ACK_Timeout

numerator is the average amount of successful data for VSTA i, transmitted during the average cycle. The cycle duration times, $T_{col,i}$ and $T_{suc,i}$, are the times required to transmit the associated frame sequences, including preambles and the physical layer headers. The frame sequences depend on the medium access scheme used and are shown in Table 3.2.

The transmission probabilities of VSTAs $(\tau_1, \tau_2, ..., \tau_n)$ are used to calculate the needed probabilities as shown:

$$
\begin{aligned}
P(S|VS=i) &= \tau_i \prod_{j=1}^{i-1}(1-\tau_j) \prod_{k=i+1}^{n}(1-\tau_k) && (3.2)\\
P(S) &= \sum_{i=1}^{n} P(S|VS=i) && (3.3)\\
P(Tx) &= 1-\prod_{j=1}^{n}(1-\tau_j) && (3.4)\\
P(C) &= P(Tx)-P(S) && (3.5)\\
P(I) &= 1-P(Tx) && (3.6)
\end{aligned}
$$

The following section shows how the transmission probabilities (τ) can be obtained at each VSTA.

3.2.1 Determination of Transmission Probabilities (τ)

Using derivations presented in [22], it is possible to calculate the transmission probability of VSTA i assuming saturation conditions:

$$\tau_{sat,i} = \frac{2(1-p_i)}{(1-p_i)(W_i+1)+p_iW_i(1-(2p_i)^{m_i})} \tag{3.7}$$

The collision probabilities of each VSTA are measured at each station, while the minimum window sizes and the maximum backoff stages are static variables. As mentioned earlier the Bianchi analytical model assumes that the wireless network is always saturated, hence $\tau_{sat,i}$ denotes the transmission probability for VSTA i if its queue is always non-empty. If the queue activity can be measured at each VSTA, the actual transmission probability can be estimated as follows:

$$\tau_i = \beta_i \tau_{sat,i} \tag{3.8}$$

In (3.8), β_i is the measured queue activity factor for VSTA i. The measurement of the collision probabilities and the queue activity factors is described in the following sections.

Measuring of Collision Probabilities (p)

As seen in (3.7), the measured collision probably (p_i) is required from each VSTA. Each VSTA keeps a counter to monitor the number of collisions ($\#Collisions$) as well as the number of successful transmissions ($\#SuccessfulTransmissions$). Assuming a reliable (approximately error free) wireless channel, the number of retransmissions should be the same as the number of collisions. The collision probability is calculated every update period using an exponentially weighted average to smooth out short term fluctuations due to varying channel conditions:

$$p_i = (1-\alpha)p_{i,current} + \alpha p_{i,prev} \tag{3.9}$$

The update period is chosen to be the beacon period, and α is chosen to be 0.8. The values chosen for these two parameters are considered to be effective for removing short term fluctuations and maintaining a good long term trend. The sample update of the collision probability can be calculated as follows:

$$p_{i,current} = \frac{\#Collisions}{\#Collisions + \#SuccesfulTransmissions} \tag{3.10}$$

The counters are reset at the end of each beacon period. The channel is assumed to be error free; hence, when a frame is unacknowledged it is assumed to be caused by a collision. For the basic access mechanism the collision counter is incremented whenever an acknowledgement frame times out. When an acknowledgement is received the counter for successful transmissions is incremented. When Contention Free Bursting (CFB) is used the counters are only allowed to be incremented for the first frame in the allocated TXOP. This is because of the fact that only the first frame of the VSTA has to contend for the shared wireless medium. For the RTS/CTS access scheme the collision counter increments whenever an CTS message times out. This is because collisions can only occur on RTS messages. The successful transmission counter is incremented whenever a CTS message is received.

It is important to note that errors may not always be a result of a collision. Bit errors often occur due to bad wireless channel conditions. It is important that these kind of errors are minimized. Thus it is recommended that appropriate error control techniques be used. For example, the Automatic Rate Fallback (ARF) algorithm used in WaveLAN-II products from Lucent is a simple algorithm where the transmission bit rate is adapted by the sender depending on the number of missing acknowledgement frames [28]. It should be noted that error control techniques are outside the scope of this thesis.

Measuring Queue Activity Factors (β)

The queue activity factor can be interpreted as the percentage of time that the queue is non-empty during a beacon period. For each beacon period the time spent when a VSTA's queue is non-empty can be measured using a timer. This timer is stopped whenever the queue is empty and resumed again when the queue is non-empty. The queue activity factor for the current beacon period can then be calculated as:

$$\beta_{i,current} = \frac{timer\,value}{beacon\,period} \tag{3.11}$$

The timer value is reset at the end of every beacon period. To smooth out fluctuations an exponential weighted average of the current and previous values of β are used as indicated in (3.12).

$$\beta_i = (1-\alpha)\beta_{i,current} + \alpha\beta_{i,prev} \tag{3.12}$$

3.2.2 Transmission Probability (τ) for a VSTA Requesting a New Flow

If a new flow is admitted into an AC the queue utililization factor for that queue is expected to increase. Since the new flow will cause the queue to be non-empty for an additional MAC delay period of the new flow, the queue activity factor would be updated accordingly. For a given VSTA, the MAC delay of the new flow can be calculated as follows:

$$MAC\,Delay = \frac{AIS\sigma}{P(I)} \tag{3.13}$$

To compute the Average Idle Slots (AIS) for the VSTA, the following formula is used:

$$AIS = AEB + AIFS + P(Tx) \times AEB \times AIFS \tag{3.14}$$

It is considered that the number of transmissions observed by the VSTA during its backoff is $P(Tx) \times AEB$. This implies that an extra number of idle slots awaited by the VSTA is equal to $P(Tx) \times AEB \times AIFS$, since an Arbitration Inter-Frame Space (AIFS) period is waited before restarting the countdown of the backoff timer.

The Average Exponential Backoff (AEB) can be interpreted as the average number of backoff slots required for each transmission attempt. Based on derivations from [22] AEB can be computed as the inverse of the saturation transmission probability:

$$AEB \approx \frac{1}{\tau_{sat}} \tag{3.15}$$

The reason the saturated transmission probability is used is that an upper bound for the MAC delay can be computed. This conservative approach ensures that the bandwidth guarantees are still met if the flow is accepted.

Once the MAC delay is known, the new queue activity factor can be computed as:

$$\beta_{new} = \beta_{prev} + \frac{MAC\ Delay}{Packet\ Interval} \tag{3.16}$$

The packet interval can be obtained from the *minimum service interval* parameter from the TSPEC of the new flow. The new transmission probability can then be computed using (3.8).

Even though an upper bounded value is used for the MAC delay there is still a problem that the collision probabilities used to compute the transmission probabilities for all VSTA are from the previous state. This means that the collision probabilities used are those computed before the acceptance of the new flow. This introduces inaccuracies to the bandwidth estimation, since the collision probabilities are likely to increase after the acceptance of a new flow. Thus, the inaccuracies are likely to cause over-estimations of bandwidth. Over-estimating achievable bandwidth may have an unacceptable effect on the network, since it may lead to accepting more flows than the network can handle.

3.2.3 Scaling of Bandwidth Estimations

A problem identified in the previous section was that the collision probabilities for the previous state (the state before a flow is accepted) are used to evaluate whether a flow is to be accepted or rejected. When the new flow is accepted the collision probabilities for each VSTA are likely to increase, due to increased contention. Thus the QoS enabled Access Point (QAP) is likely to over-estimate the achievable bandwidth for each VSTA.

Over-estimating the achievable bandwidth for VSTAs may lead to the acceptance of a flow that may jeopardize the bandwidth requirements of some VSTAs. This conflicts with the primary goal of admission control, i.e., to protect the QoS for admitted flows in the network. On the other hand, by under estimating the achievable bandwidth QoS can be guaranteed, but optimal use of the network resources would not always be maintained. It can be argued that it is better to make sure that QoS is guaranteed at the cost of bandwidth under-utilization. Thus it is recommended that the estimated achievable bandwidth be scaled down so that QoS can be guaranteed.

The scaling of the estimated achievable bandwidth should depend on the medium access mechanism used and its ability to effectively utilize the network's bandwidth. It was found that when no hidden stations are present the basic access mechanism outperforms the RTS/CTS handshake mechanism in terms of bandwidth utilization [29]. Improved bandwidth utilization is expected for the CFB mechanism due to its ability to reduce contention in the WLAN. Thus, the RTS/CTS mechanism should have the estimated achievable bandwidth scaled down most and the CFB mechanism scaled down least. Another factor to consider is that higher priority ACs are favoured and should be scaled down less than lower priority ACs. The chosen scaling factors for the estimated achievable bandwidth are shown in Table 3.3. These scaling factors are used in the evaluation process that will be described in later chapters. It is the author's belief that these scaling factors would reasonably ensure bandwidth guarantees with little effect on the total bandwidth utilization of the network.

Table 3.3: Chosen scaling factors for the estimated bandwidth

	AC(VO)	AC(VI)
CFB	0.975	0.950
BASIC	0.950	0.925
RTS/CTS	0.925	0.900

3.3 Functional Behaviour of the Proposed Admission Control Scheme

3.3.1 Wireless Station Behaviour

Once a station joins the WLAN and is authenticated it would perform certain procedures that contribute to the overall function of the admission control scheme. It is important that all stations communicate the transmission probabilities for all their ACs during every beacon interval. The procedure followed for a given wireless station to achieve this would be as follows:

1. All four VSTAs within the station, would measure collision statistics as well as the AC queue activity. The number of collisions and successful transmissions are measured, so that the collision probability (p_i) can be calculated for a particular VSTA. The queue activity factor (β_i) for each VSTA can be calculated using timers. These procedures are described in Section 3.2.1.
2. Once p_i and β_i are known for VSTA i, the saturation and estimated transmission probabilities, $\tau_{sat,i}$ and τ_i, can be calculated from equations (3.7) and (3.8).
3. These transmission probabilities are then forwarded to the QAP using the highest priority access class, AC(VO). The information is sent to the head of the AC(VO) queue to ensure that it is transmitted with minimal delay.

When a station wishes to initiate a flow it has to first send a request to the QAP and indicate its QoS requirements. This request procedure is done via a TSPEC negotiation and it includes the required information that is needed by the QAP. The station will then wait for a TSPEC response from the QAP to determine whether the flow is accepted or rejected.

Some important fields in TSPEC are:

- Minimum Data Rate: the lowest data rate (in bits per second) to transport MSDUs.

- Mean Data Rate: the average data rate (in bits per second) to transport MSDUs.
- Peak Data Rate: the maximum allowable data rate (in bits per second) to transport MSDUs.
- Minimum PHY Rate: the desired minimum physical rate for this traffic stream.
- Maximum MSDU: the maximum size, in octets, of MSDUs belonging to the traffic flow under this TSPEC.
- Minimum Service Interval: the minimum interval, in microseconds, between the transmission of two successive payload frames.
- Maximum Service Interval: the maximum interval, in microseconds, between the transmission of two successive payload frames.

3.3.2 QoS enabled Access Point Behaviour

The QAP stores information about the bandwidth required for each active VSTA. It also collects and stores all the transmission probability information sent by the wireless stations during every beacon period. Figure 3.1 shows the admission control signalling using TSPEC, as described in Section 2.3.

Admission control decisions take place in the Admission Control Unit (ACU) of the QAP. When stations initiate sessions they state their bandwidth requirements using TSPEC as defined in [1]. The QAP will then attempt to increase the required bandwidth at the corresponding VSTA because it would have to accommodate an additional flow. The QAP is able to estimate the achievable bandwidth for each VSTA as described in Section 3.2. The admission control scheme should accept a new flow only if the required bandwidth for all VSTAs can be guaranteed (i.e., estimated achievable bandwidth is more than or equal to the required bandwidth for each VSTA). If Any VSTA cannot achieve their required bandwidth, then the new flow should be rejected. Once the process is completed the ACU will send a MLME-ADDTS (MAC Layer Management Entity-ADDTS) response message containing the decision of whether the new flow is accepted or rejected.

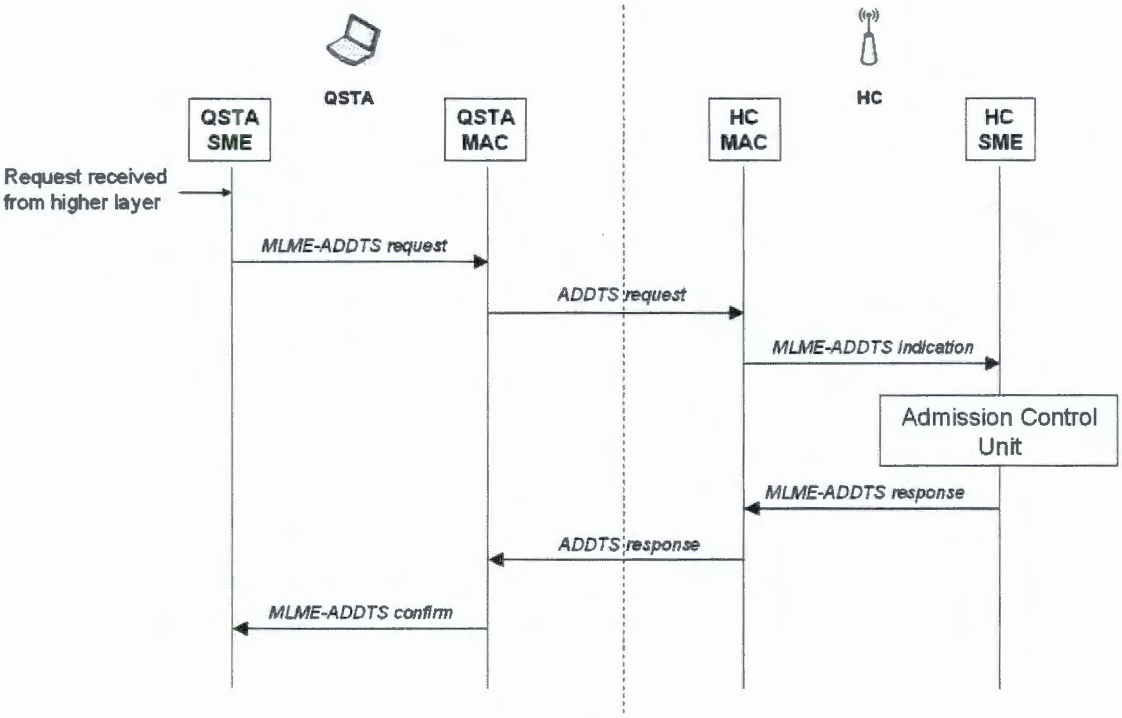


Figure 3.1: Admission Control signalling using TSPEC

3.4 Signalling Overhead

The proposed admission control scheme requires the transmission of information from each active wireless station to the QAP. The information sent are the transmission probabilities that are needed for the QAP to compute the bandwidth estimates for each VSTA. Each wireless station has to send both τ and τ_{sat} variables for all four ACs (Virtual Stations). To transmit the transmission probability for one VSTA requires 16 bits of data, represented as a float. Thus the signalling message contains 128 bits of information to send both τ and τ_{sat} for four ACs.

The bandwidth required for these signalling messages depends on the beacon interval and the number of active stations in the network. The required bandwidth for these signalling messages is:

$$B_{sig} = n_s \frac{128}{T_{beacon}} \ (bps) \tag{3.17}$$

where n_s is the number of active wireless stations in the network and T_{beacon} is the beacon period.

3.5 Discussion

This chapter introduced a theory for estimating the achievable bandwidth for EDCA VSTAs. It detailed how these bandwidth estimations can be used for admission control EDCA WLANs. The the major shortcoming of the admission control scheme, described in Section 2.3.1, is that admitted flows aren't protected when making good use of network resources. The proposed admission control scheme is capable of overcoming these shortfalls, because it is able to estimate achievable bandwidth resources for each VSTA. It requires specific functional modifications to standard WiFi stations and Access Points. The main concepts of the proposed admission control scheme can be summarised as follows:

- Each station measures the collision statistics and queue activity for each of its four VSTAs; this takes place during every beacon period.
- Using these measured parameters the station can estimate the transmission probabilities for each of its four VSTAs and forwards this information to the QAP. The computation of these transmission probabilities is achieved using an extension of the Bianchi analytical model that is aided by the measured parameters.
- Once the QAP has captured all the transmission probabilities of the active VSTAs in the WLAN, it can estimate the achievable bandwidth for them. The bandwidth estimations are obtained using the modified Bianchi analytical model.
- When the QAP receives a new flow request with the required bandwidth, it will estimate the achievable bandwidth for all active VSTAs in the WLAN. A new flow is accepted only if all VSTAs would still achieve their required bandwidth, otherwise the request is rejected. This can be determined by comparing the required bandwidth of a VSTA (sum of the required bandwidths for its servicing flows) and the estimated achievable bandwidth.

Chapter 4

Implementation of the Evaluation Framework

4.1 Introduction

This chapter describes the design of an evaluation framework used to evaluate the proposed admission control scheme. The implemented evaluation framework supports all the required functionality needed to analyse the admission control scheme. The requirements of the evaluation framework will be considered and discussed. This chapter also describes basic simulation environments in which the evaluation framework will be utilized.

4.2 Simulation Platform Information

The evaluation experiments were conducted in a software simulation environment, rather than a hardware-based testbed. This is because it was easier to change the functionality of IEEE 802.11e functions in software as compared to hardware. This is primarily due to limited access to driver code or APIs. However, in a software simulation environment the functionality and network components can easily be modified. Furthermore, the scale and complexity of experiments is not limited by cost or availability of resources when using an open source simulation environment.

The NS-2 simulator was chosen as a simulation platform to evaluate the proposed admission control Scheme [30]. NS-2 simulator was designed specifically for network research. It is a discrete event-driven object-oriented simulator written in C++ together with an OTcl (Object-oriented extension of Tcl) interpreter. The distribution is entirely open source and is freely available for most operating systems. In this thesis simulations and programming were performed using the Fedora Core 6 Linux platform.

The impact of NS-2 on networking research has been considerable, making it arguably the largest simulation tool set for research on Internet protocols. New protocols and wireless modules are regularly contributed by the research community. During the standardization the IEEE 802.11e standard, simulation models were developed by the Mosquito group for the NS-2 simulator [31]. In 2003 the Telecommunication Networks (TKN) Group from the University of Berlin, developed an EDCA module for NS-2.26 based on a draft version of IEEE 802.11e [32, 33]. Boggia et al. investigated feedback-based scheduling algorithms based on their own HCCA implementation[34]. Cicconetti et al. also implemented a pure HCCA mechanism [35], but failed to implement any proper EDCA support. Ni Qiang et al. implemented both HCCA and EDCA models as well as various enhancements for adaptive contention parameter tuning and fair resource allocation [36, 37, 38]. However, this implementation is based on an old version of NS-2 (NS-2.17b) and is also based on a draft standard of IEEE 802.11e.

Lacage et al. from INRIA (l'Institut National de Recherche en Informatique et en Automatique), a French institute in Sophia Antipoli, developed a new model including the legacy 802.11 MAC functionality, standadized 802.11e EDCA and HCCA functionality, as well as multi-rate support [39]. The model is available and is intended to be integrated into the coming release of the Network Simulator version 3 (NS-3). This simulation model was chosen to be used for this research, because it supports all the necessary fundamental support required to implement and evaluate the proposed admission control scheme.

4.3 Simulation Objectives

The primary aim of this simulation study is to quantitatively evaluate the performance of the proposed admission control scheme. The assessment is based on the ability to protect the bandwidth guarantees for admitted flows in the network, while making effective use of network resources by accommodating as many flows as possible. Another aim of the simulation experiment is to evaluate the accuracy of bandwidth estimations that is fundamental to the operation of the admission control scheme. The implementation must be shown to work accurately for the three fundamental EDCA access mechanisms:

- Basic mode
- RTS/CTS handshake
- Contention Free Bursting (CFB)

4.4 Simulation Framework Requirements

To be able to test the concept of the proposed admission control scheme the simulation framework needs to support the mandatory aspects of the IEEE 802.11e enhancement. The major features required are:

1. Access differentiation through Access Classes (EDCA support)
2. TSPEC negotiation mechanisms (Admission control signalling support)

These features are implemented in the contributed module as described in [39]. Further requirements include the implementation of the actual admission control scheme. This should include the QoS enabled Access Point (QAP) functional behaviour described in Section 3.3.2, as well as the station behaviour as described in Section 3.3.1. The simulation environment would provide approximately error-free channel conditions so that accurate bandwidth estimations can be obtained. The overall simulation framework would extract bandwidth statistics that can be analyzed to evaluate the performance of the proposed admission control scheme. The measured bandwidth metrics would indicate the accuracy of the bandwidth estimations used by the admission control scheme. It would also show the efficiency of using the network's resources and indicate weather bandwidth requirements are met for real-time traffic flows. Furthermore, the admission control decisions should be recorded to a log file so that these decisions can be observed.

4.5 IEEE 802.11e WLAN Implementation

The 802.11e contributed NS-2 module from INRIA was modified to integrate the proposed admission control functionality. The original contribution from INRIA was implemented in a modular fashion. The 802.11a standard was used for the fundamental MAC and PHY layer specifications. This section presents relevant implementation details about the original 802.11e contributed module. It provides insight about the MAC and PHY layer architecture as well as the TSPEC implementations.

4.5.1 The MAC Architecture

The MAC architecture supports both legacy and 802.11e WLAN support. Figure 4.1 shows the overall architecture of the IEEE 802.11e WLAN implementation from INRIA, while Figure 4.2 shows the architecture of a Virtual Station (VSTA).

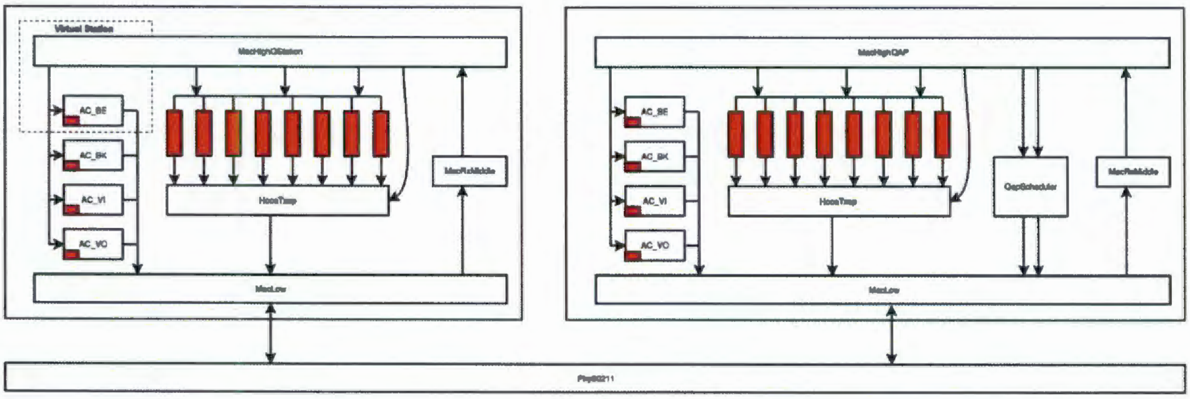


Figure 4.1: Overall framework of the MAC implementation from INRIA

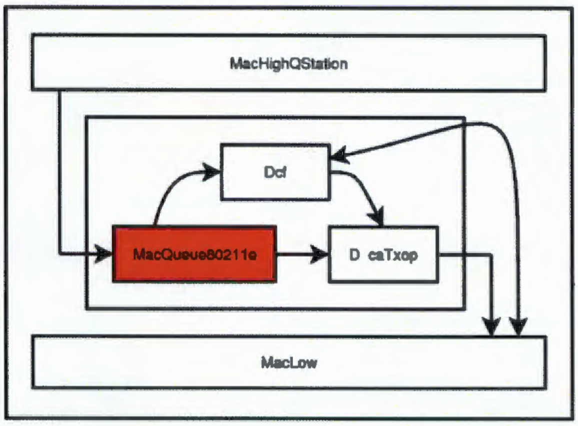


Figure 4.2: Architecture of a Virtual Station (VSTA)

The MacHigh entity handles all of the functions related to Management frames and interfaces to the Logical Link Control (LLC) Layer . There are two specific implementations of the MacHigh entity; MacHighQStation and MacHighQAP. MacHighQAP implements QAP specific functions while MacHighQStation implements station specific functions. The station-specific MacHigh associates with the QAP and synchronizes with the beacons. The QAP-specific MacHigh generates the beacon frames and handles associated stations. An 802.11e enabled AP MacHigh contains the Hybrid Coordinator.

The MacLow entity handles the low-level transmission functions. It generates the RTS, CTS and ACK frames. It also handles the proper Inter-Frame Space timing as well as the timing for CFB.

The DcaTxop entity handles retransmissions, fragmentation, and bursting. It is notified by the Dcf entity whenever access to the medium has been granted. The legacy 802.11 DCF is used to calculate when to grant access to the transmission medium. The CSMA/CA mechanism is used to provide reliable access to the wireless medium.

The MacRxMiddle in Figure 4.1 performs defragmentation and handles duplicate frames.

4.5.2 The PHY Architecture

The physical layer models are implemented in the Phy80211 sub-classes of the module code. The important concerns are the modelling of the over-the-air propagation and the reception of data frames. These models are important for determining erroneous frames.

A Signal-to-Noise Ratio (SNR) Threshold-based model is used to model the reception of packets. The SNRT (Signal-to-Noise Ratio Threshold) based model uses the SNR and compares it with a SNR threshold (SNRT). It then accepts only those signals whose SNR values were above the SNRT at any time during reception. It was found that this reception model has good accuracy while and low computational cost. This is desirable since the wireless medium is intended to be heavily loaded in the simulation environment.

Another important factor is to model the path loss during signal propagation. The free space model is used as a basic reference. It is considered to be an idealized propagation model, which is desirable for an error free channel condition. A further discussion of various PHY simulation models, used in various simulators, can be found in [40].

4.5.3 TSPEC Implementation

The TSPEC frame formats are all defined in the contributed model as recommended in the 802.11e enhancement. The TSPEC requests that are initiated by the wireless stations are generated in the OTcl code. As described in Section 2.3 the request is processed at the admission control unit in the QAP. This is implemented at the MacHighQAP. The response will be received by the wireless station and handled in the OTcl code. If the request is accepted then the traffic flow will be initiated in the OTcl code. If the response is rejected then no traffic will be sent. Appendix B shows how TSPEC operations are handled in OTcl code.

4.6 Implementation of the Measurement-Aided Model-Based Admission Control Scheme

This section describes how the proposed admission control scheme was integrated into the 802.11e module from INRIA. The functional behaviour of the QAP and the wireless stations are described in Section 3.3.

The collisions and successful transmissions are measured at the DCF of each VSTA and used to calculate its collision probability. The queue activity factor is measured at the queue of the VSTA (MacQueue80211e). The saturation and estimated transmission probabilities can be calculated at the DCF of each VSTA, as described in Section 3.2.1. The MAC-High module will extract this information for all active ACs and send it to the QAP using AC(VO). This information is put at the head of the queue in AC(VO) to ensure that it gets to the QAP quickly and reliably during each beacon period.

When the station wants to request a new flow it first formulates a TSPEC request. At the QAP all TSPEC requests are evaluated in the Admission Control Unit (ACU) of the Mac-High module in the QAP, where the admission control decisions are made. The algorithm for making admission control decisions when a new TSPEC request is received is described in Section 3.3.2. The pseudo code for this algorithm is shown below:

```
Estimate the transmission probabilities considering the new flow request();
Calculate Markovian probabilities();
Estimate achievable bandwidth for each Virtual Station();

bool OK = true;
//Run the algorithm to see if bandwidth guarantees can be met and set 'OK' accordingly
for (int i = 1; i < number of active Virtual Stations + 1 ; i++)
{
    if (Requested_Bandwidth[i] < Estimated_Bandwidth[i])
    {
        OK = false;
```

```
        }
    }

    if (OK)
    {
        admit the flow:
    }
    else
    {
        reject the request;
        restore the required bandwidth for the requesting Virtual Station:
        restore the transmission probabilities for all Virtual Station:
    }
```

4.7 Simulation Environment

4.7.1 Topology Configuration

The focus of the performance evaluation is specifically for the shared EDCA Wireless medium. Thus, only the wireless access network was considered in the simulation. Figure 4.3 shows the topology of the WLAN segment used for simulation experiments. All the wireless stations are are spaced 13 m away from the QAP. This is considered to be within good range of the QAP for good signal strength. There were no obstacle and no hidden nodes in the configuration. This facilitates the approximate error free conditions required for the simulation environment.

of a collision in the case of larger MSDUs is longer than for smaller MSDUs. Thus more time is wasted due to collisions for larger MSDUs.

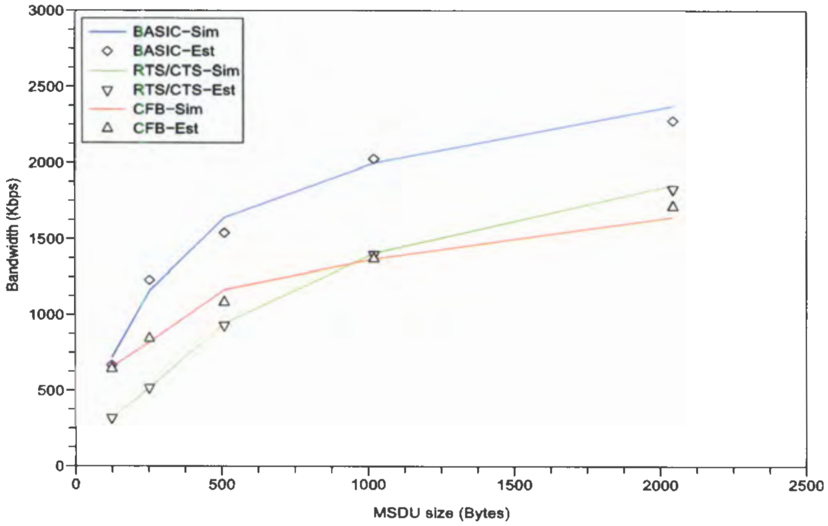


Figure 5.1: Comparison between the estimated and simulated bandwidth for AC(VO)

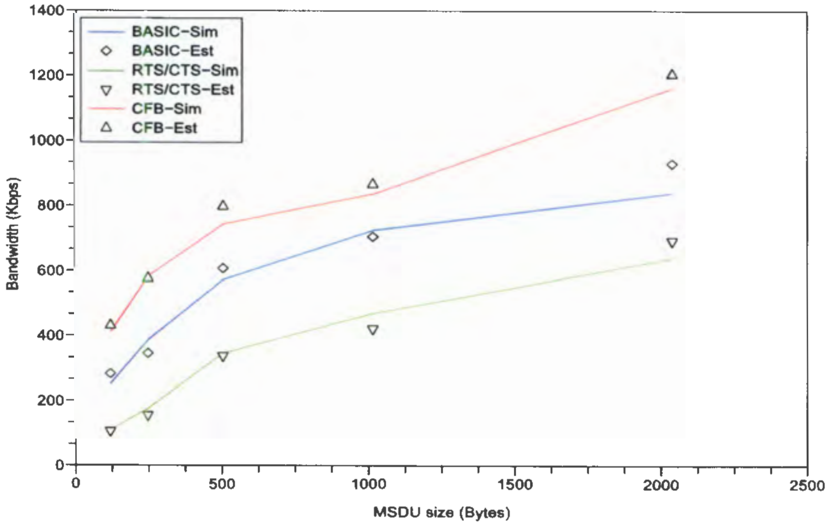


Figure 5.2: Comparison between the estimated and simulated bandwidth for AC(VI)

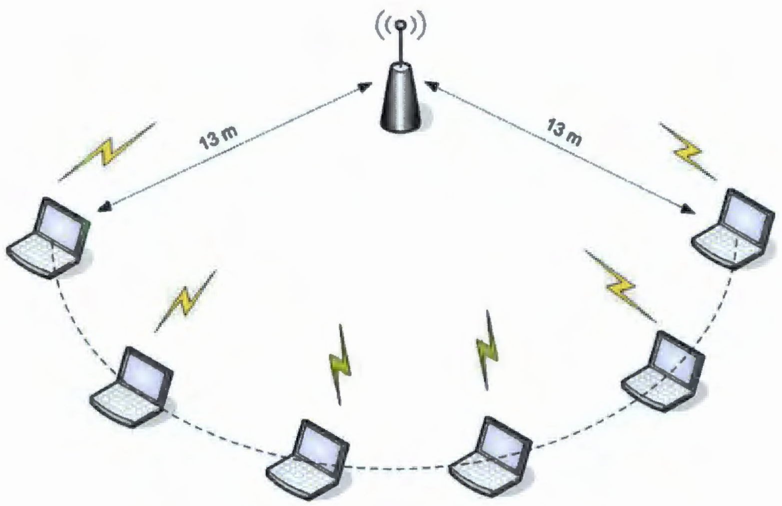


Figure 4.3: Topology of the WLAN segment

4.7.2 WLAN Parameters

The 802.11a standard was used by the 802.11e contributed model for MAC and PHY layer specifications. The parameters for the slot time and Inter-Frame Spaces are shown in Table 4.1 and is configured for the the 802.11a standard.

Table 4.1: Slot time and Inter-Frame Space parameters

Slot time (σ)	$9\,\mu s$
SIFS	$16\,\mu s$
PIFS	$25\,\mu s$
DIFS	$34\,\mu s$

Default values for the EDCA parameters are used during simulation experiments, as indicated in Table 4.2.

Table 4.2: Default values for the EDCA parameters as used in the simulations

	AC(VO)	AC(VI)	AC(BE)
AIFS (slots)	2	2	3
CW_{min} (slots)	3	7	15
CW_{max} (slots)	7	15	1023

4.7.3 Transmission Rates for Wireless Stations

The data rate of all the stations are set at 18 Mbps complying with the 802.11a physical layer standard. Even though the maximum transmission rate is 54 Mbps for 802.11a, a lower rate of 18 Mbps is considered to be more reliable and reduces the likelihood of bit errors. All the control frames, such and RTS and CTS frames are transmitted at 6 Mbps for even higher reliability.

4.7.4 Traffic Considered for Simulations

In simulations three of the EDCA Access Classes are used: AC(VO), AC(VI) and AC(BE). Thus, the traffic considered for the simulations would include voice, video and best-effort traffic. Both video and voice traffic are Constant Bit Rate (CBR) applications that transmit packets using Real-Time Protocol (RTP) [41] session over an User Datagram Protocol (UDP) [42] connection. CBR traffic is used so that the bandwidth required by CBR flows can easily be obtained. This is needed by the admission control scheme, since admission control is required for video and voice traffic. With VBR traffic, it would be difficult to observe whether the instantaneous bandwidth requirements are met.

A typical PCM voice coding scheme G.711 is simulated for voice flows with a required bandwidth of 64kbps at the application layer. RTP typically transmits at a packet interval of 10ms, thus the payload size is chosen to be 82 bytes (64kbps×10ms). This means that the MSDU size for the voice traffic is 122 bytes, which includes the 82 byte payload and 40 bytes of overheard for RTP, UDP and IP headers. Thus the bandwidth required at the MAC layer for a single voice flow is 95.3125kbps (122 bytes÷10ms).

CBR MPEG4 video streaming traffic are simulated for video flows with a required bandwidth of 750kbps at the application layer. For a packet interval of 10ms the payload size was chosen to be 960 bytes (750kbps ×10ms). This means that the MSDU size for video traffic is 1000 bytes once the 40 bytes of overhead is added for RTP, UDP and IP headers. Thus the bandwidth required at the MAC layer for a single video flow is 781.25kpbs (1000 bytes÷10ms).

The File Transfer Protocol (FTP) application is used to simulate best-effort traffic over a Transport Control Protocol (TCP) [43] connection. The MSDU size for the

FTP traffic is 1040 bytes. This traffic does not require any admission control, but it is included to make the scenarios more realistic. The set up of all the simulated traffic in OTcl code is shown in Appendix B.

Chapter 5

Results, Evaluations and Analysis

5.1 Introduction

This chapter presents an evaluation of the proposed measurment-aided model-based admission control scheme using the simulation architecture presented in chapter 4. The admission control scheme is evaluated for three medium access mechanisms (Basic, RTS/CTS and CFB). The metric of concern is the bandwidth utilized by real-time traffic. The bandwidth utilization will indicate whether bandwidth guarantees are met. It can also indicate the efficiency of usage of network resources. In all experiments traffic was transmitted only in the uplink direction. Downlink traffic consisted only of the required signalling for MAC and higher layer operations. This was done to improve bandwidth utililization so that the effect of admission control can be fully observed. If traffic was generated for both directions then more bandwidth usage would be observed for uplink traffic due to unfairness. This is because all downlink traffic is transmitted by only one contending Access Point (AP), whereas uplink traffic is transmitted by multiple contending wireless stations. Thus, the admission control scheme would have to reject uplink flows in order to protect downlink flows and the maximum total bandwidth utilization would not be observed. The traffic used for voice, video and best-effort data is described in Section 4.7.4. All results displayed are extracted during simulations within the OTcl code as shown in Appendix B. The next section evaluates the accuracy of the bandwidth estimations for the proposed admission control scheme.

5.2 Accuracy of Bandwidth Estimations

Since bandwidth estimations are fundamental to the proposed admission control scheme the accuracy of the estimations was tested by simulating a network scenario as flows: The network consists of 1 QAP and 6 wireless stations. For each wireless station 3 ACs are active for voice, video and best-effort data. Three of these stations have unlimited UDP data to send and their queues would always be non-empty. The other three stations each service one video and voice flow, and one FTP session. This means that the network is not completely saturated. The original Bianchi analytical model was shown to be accurate only for saturation conditions. However, the modifications made to the Bianchi model does consider non-saturation conditions. One of the saturated stations is monitored so that the actual simulated bandwidth of AC(VO) and AC(VI) can be compared to what is estimated at the QAP. Since the monitored station sends unlimited data in the uplink direction, its estimated achievable bandwidth is expected to be the same as its simulated bandwidth. The bandwidth estimations are not scaled down because new traffic requests are not anticipated. The signalling bandwidth required for bandwidth estimation in this scenario can be calculated from equation (3.18). A beacon period of 1 second is used for all simulations; thus, this signalling bandwidth is calculated to be 768 bps. The signalling bandwidth is considered to have a negligible effect on the overall bandwidth utilization. From equation (3.1) it can be observed that the estimated achievable bandwidth is dependent on the packet payload size used at Virtual Stations (VSTAs). Thus, five simulations were conducted with varied MAC Service Data Unit (MSDU) sizes (128 bytes, 256 bytes, 512 bytes, 1024 bytes and 2048 bytes).

As seen from Figure 5.1, accurate bandwidth estimations can be obtained for AC(VO) traffic using the measurement-aided model-based approach. A similar conclusion can be drawn for AC(VI) by observing Figure 5.2. In all cases the bandwidth utilization is much higher when larger MSDUs are used. This is because more time is spent transmitting data rather than contending for the frame to be sent. Each frame has a fixed MAC header size thus using larger MSDUs is more efficient because the user data-to-overhead ratio is higher. As the MSDU size increases it can be observed that bandwidth utilization increases at a lower rate. This is because bandwidth wasted due to collisions. The average duration

The basic access scheme performs better than the RTS/CTS mechanism. This is primarily due to the bandwidth wasted by additional RTS and CTS overhead frames. For video traffic the CFB mechanism is able to utilize the most bandwidth as compared to other access modes. On the other hand it utilizes less bandwidth than the basic access mode for voice traffic. When using an MSDU of more than 1024 bytes it even utilizes less bandwidth than the RTS/CTS mechanism for voice traffic. This is because of the additional bandwidth allocated to the video traffic via TXOP allocations. Longer TXOPs are allocated to AC(VI) thus AC(VO) spends more time waiting for AC(VO) to finish transmitting data.

5.3 Performance of the Proposed Admission Control Scheme

The experiments in this section focus on the performance of the network and real-time traffic flows. A comparison will be made between a scenario where no admission control is applied on the network and a scenario where the proposed admission control scheme is applied.

The simulation scenarios consist of one QAP and 5 wireless stations. After 3 seconds from start each station initiates one voice flow, one video flow and one FTP session. At 8 seconds one wireless station requests a voice flow via a TSPEC request, and the response from the QAP is recorded to a log file. A new voice request is generated every 4 seconds afterwards from different wireless stations. At 10 seconds a wireless station will request a new video flow and the response is also recorded to the log file. Afterwards, more video requests are made every 4 seconds from different wireless stations. This means that a TSPEC request has to be processed every 2 seconds at the QAP when admission control is applied.

The signalling bandwidth required for making bandwidth estimations in this scenario is 640 bps, and is considered to have a negligible effect on the overall bandwidth utilization. It is expected that the bandwidth required for each admitted flow is reasonably guaranteed when the admission control scheme is applied. The total bandwidth utilization will also be analysed to evaluate the efficiency of using the network bandwidth when handling traffic requests.

5.3.1 Basic Access Mode

Figure 5.3 shows the bandwidth usage for 3 monitored flows without the presence of admission control, while Figure 5.4 shows the bandwidth usage of these flows with the proposed admission control implemented in the network. Figure 5.5 displays the log text file that indicates whether TSPEC requests are accepted or rejected. It is clear that the bandwidth share of the flows diminishes as the load in the network increases. However, when the admission control scheme is asserted it is found that the network provides the required bandwidth for these flows.

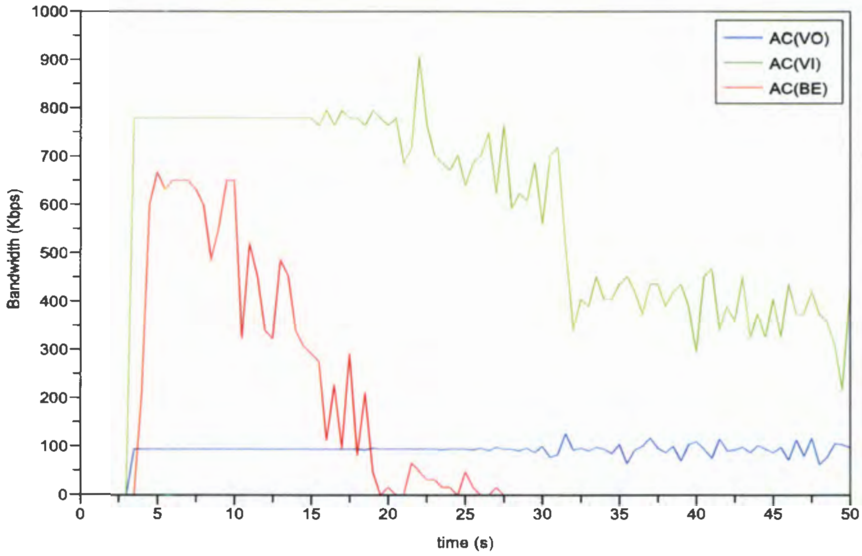


Figure 5.3: Bandwidth usage for the basic access mechanism without admission control (monitoring a single flow per AC)

In Figure 5.3 it can be seen that the bandwidth of the video flow fluctuates rapidly after 18 seconds. This is attributed due to collisions and random backoff. This is because a new video flow is accepted into the network at about 18 seconds, causing the bandwidth utilization to be degraded for the video flow. The situation is different when the admission control scheme is applied, because the video requests are rejected after 18 seconds as indicated in Figure 5.5. An extra voice flow is accepted after 20 seconds, because it doesn't use as much bandwidth as video flows and the admission control scheme determined that it would not degrade the

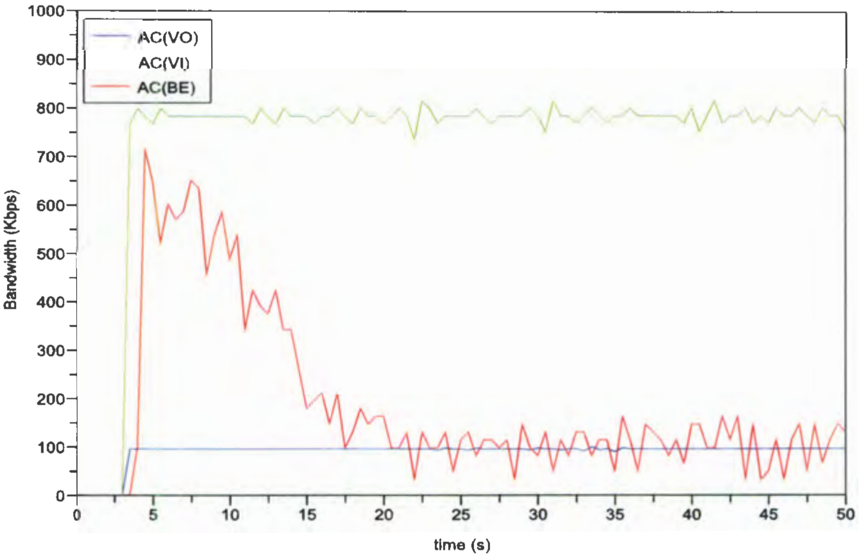


Figure 5.4: Bandwidth usage for the basic access mechanism with admission control enabled (monitoring a single flow per AC)

```
8.0098347285768003 tspec granted for sta 1 AC_VO
10.008850742743927 tspec granted for sta 1 AC_VI
12.004309499658442 tspec granted for sta 2 AC_VO
14.002144098414895 tspec granted for sta 2 AC_VI
16.012304803628158 tspec granted for sta 3 AC_VO
18.007201232676426 tspec refused for sta 3 AC_VI
20.010544889676343 tspec granted for sta 4 AC_VO
22.006300430891979 tspec refused for sta 4 AC_VI
24.005270479832241 tspec refused for sta 5 AC_VO
26.006332976047624 tspec refused for sta 5 AC_VI
28.009557512535025 tspec refused for sta 1 AC_VO
30.007001281045000 tspec refused for sta 1 AC_VI
32.007355464573415 tspec refused for sta 2 AC_VO
34.012014753717203 tspec refused for sta 2 AC_VI
36.002300529478283 tspec refused for sta 3 AC_VO
38.005768351152390 tspec refused for sta 3 AC_VI
40.008574054833517 tspec refused for sta 4 AC_VO
42.007966216357630 tspec refused for sta 4 AC_VI
44.010569198606788 tspec refused for sta 5 AC_VO
46.007009113887634 tspec refused for sta 5 AC_VI
```

Figure 5.5: TSPEC request log (basic access mechanism)

bandwidth utilized by the admitted flows. With no admission control the voice flow only becomes unstable after 30 seconds, when 11 video flows and 11 voice flows are already accepted into the network. The reason that voice flows are more stable than video flows is that the AC for voice has the highest priority.

Figure 5.6 shows the total bandwidth used in the network for the voice, video and best-effort traffic when no admission control is applied. Initially the total bandwidth usage increases as the number of admitted flows increase. However, when the network becomes overloaded the utilized bandwidth fluctuates and fails to increase according to the bandwidth needs of the admitted traffic. This phenomena is observed after 18 seconds when a new video flow is admitted into the network. After 23 seconds the bandwidth utilization for video traffic decreases due to the bandwidth loss during collisions. The best-effort traffic receives little bandwidth after 25 seconds.

Figure 5.7 shows the total bandwidth usage when the admission control scheme is applied. It is clear a good decision was made to reject the video request at 18 seconds. It can also be observed that no requests are rejected before 18 seconds, the period during which the network shows predictable performance. Thus, effective utilization of network resources occurs. The bandwidth requirements are still met, even when an extra voice flow is accepted after 20 seconds. It is expected that any additional flows that are accepted into the network would result in failure to meet bandwidth requirements. This can be seen from Figure 5.8 where an extra video flow is accepted after 18 seconds and an extra voice flow is accepted after 24 seconds.

In the graph displayed in Figure 5.8 it is clear that the network is unable to cope with bandwidth demands for video traffic. Only an average of 6065 kbps can be allocated to video traffic after 24 seconds; however, the bandwidth required is 6250 kbps. When the admission control is applied the bandwidth is guaranteed for the 5468.75 kbps required for video traffic, as seen in Figure 5.7. Figure 5.9 shows the effect the admission of the extra flows has on the monitored traffic flows. In this situation the voice flow is allocated its required bandwidth. However, it is clear that the bandwidth utilized by the video flow is less than what is required.

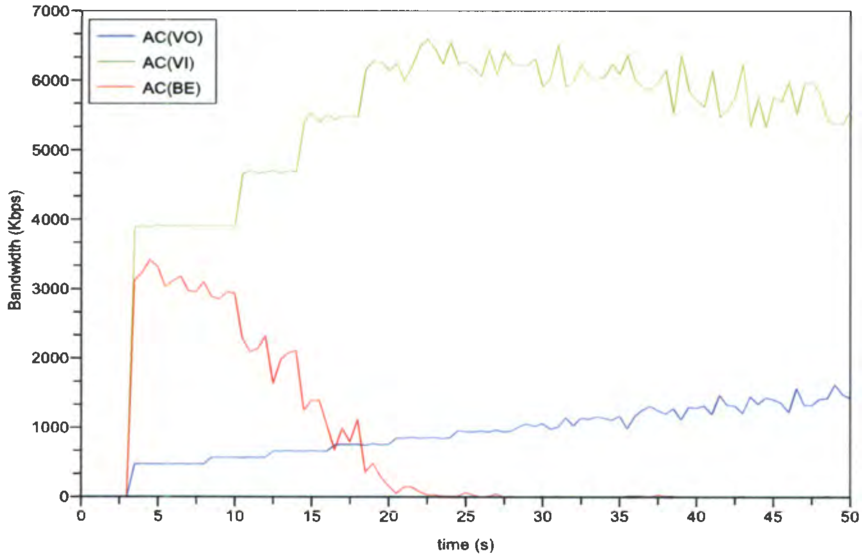


Figure 5.6: Bandwidth usage for the basic access mechanism without admission control (total bandwidth)

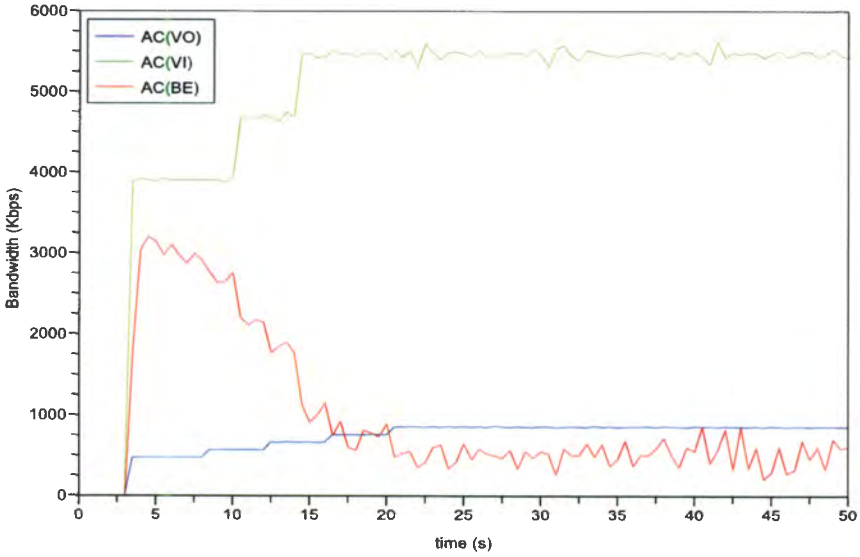


Figure 5.7: Bandwidth usage for the basic access mechanism with admission control enabled (total bandwidth)

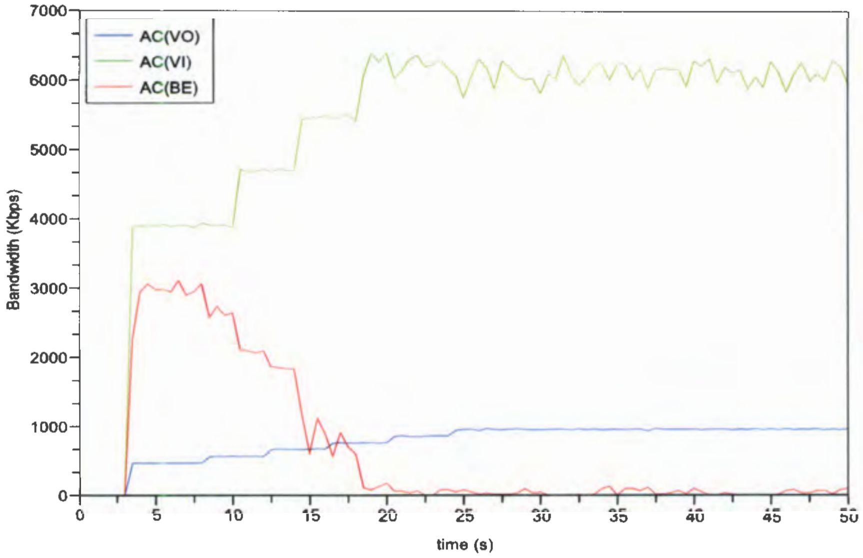


Figure 5.8: Bandwidth usage for the basic access mechanism after admitting 2 extra flows (total bandwidth)

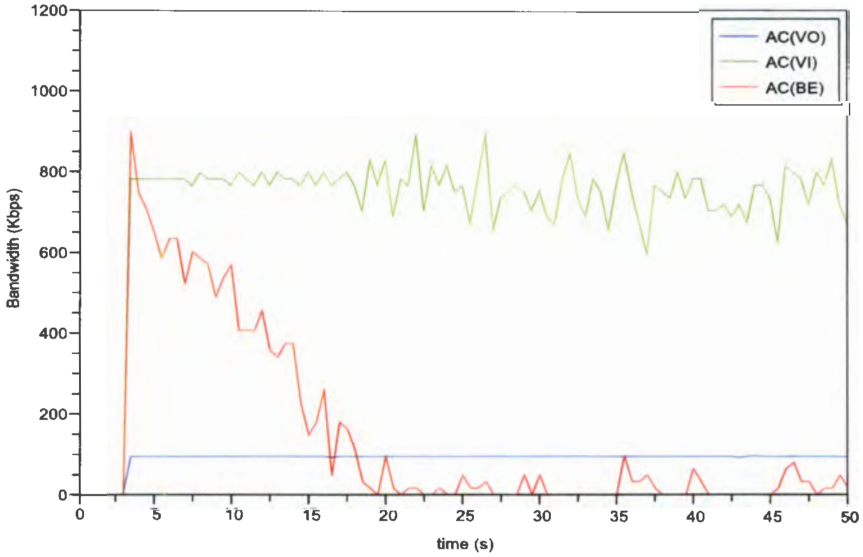


Figure 5.9: Bandwidth usage for the basic access mechanism after admitting 2 extra flows (monitoring a single flow per AC)

5.3.2 RTC/CTS Access Mode

Figure 5.10 shows the bandwidth usage for 3 flows without admission control, while Figure 5.11 shows the bandwidth usage of these flows with the proposed admission control scheme implemented in the network. Figure 5.12 displays the log text file for the flow requests. Once again it is found that the admission control scheme is able to protect the bandwidth needs of the flows by preventing the network from becoming overloaded.

In Figure 5.10 it can be seen that the bandwidth utilized by the monitored video flow diminishes after 12 seconds, due to collisions and random backoff. This is because a new voice flow is accepted into the network at 12 seconds, causing the bandwidth usage for the video flow to degrade. The situation is different when the admission control scheme is applied, because all the requests are rejected after 12 seconds as indicated in Figure 5.12. With no admission control the monitored voice flow only becomes unstable after 28 seconds, when 10 video flows and 11 voice flows are already accepted into the network. It is important to observe that with the basic access mechanism, rejection of flows start at 18 seconds, whereas with the RTS/CTS mechanism rejection starts at 12 seconds. This is because of the bandwidth loss due to the additional overhead of RTS/CTS frames, thus less flows are accommodated. Thus, If hidden stations can be avoided it is not recommended to use the RTS/CTS handshake mechanism.

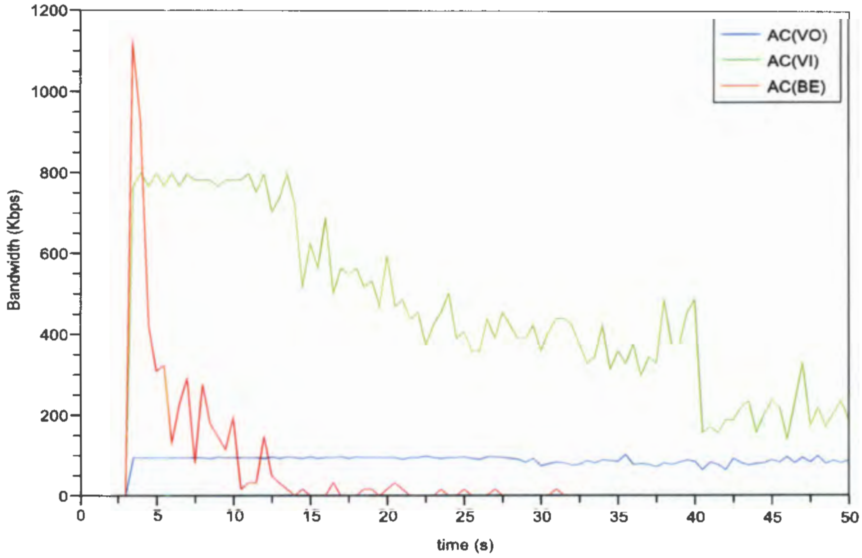


Figure 5.10: Bandwidth usage for the RTS/CTS access mechanism without admission control (monitoring a single flow per AC)

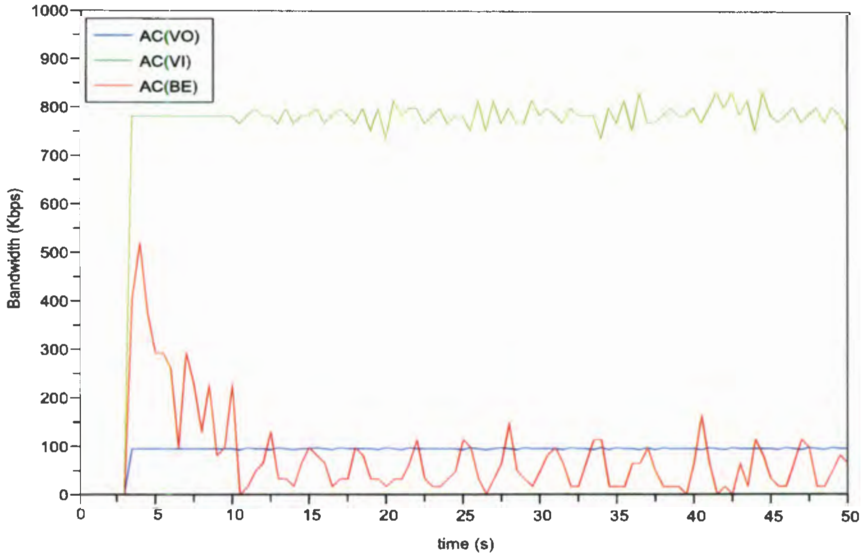


Figure 5.11: Bandwidth usage for the RTS/CTS access mechanism with admission control enabled (monitoring a single flow per AC)

```
8.0147225344013311 tspec granted for sta 1 AC_VO
10.006465113573427 tspec granted for sta 1 AC_VI
12.003898681561960 tspec refused for sta 2 AC_VO
14.002095280001848 tspec refused for sta 2 AC_VI
16.003696754148866 tspec refused for sta 3 AC_VO
18.004906648270975 tspec refused for sta 3 AC_VI
20.005448194496633 tspec refused for sta 4 AC_VO
22.009193796704352 tspec refused for sta 4 AC_VI
24.008157988093629 tspec refused for sta 5 AC_VO
26.006583784754135 tspec refused for sta 5 AC_VI
28.019921245140630 tspec refused for sta 1 AC_VO
30.001022560726547 tspec refused for sta 1 AC_VI
32.009425161852796 tspec refused for sta 2 AC_VO
34.006511046493031 tspec refused for sta 2 AC_VI
36.009531864202302 tspec refused for sta 3 AC_VO
38.005655610958392 tspec refused for sta 3 AC_VI
40.001848483046068 tspec refused for sta 4 AC_VO
42.012921420613502 tspec refused for sta 4 AC_VI
44.010119499747248 tspec refused for sta 5 AC_VO
46.003825651188194 tspec refused for sta 5 AC_VI
```

Figure 5.12: TSPEC request log (RTS/CTS access mechanism)

Figure 5.13 shows the total bandwidth used in the network for voice, video and best-effort traffic when no admission control is applied. Initially the total bandwidth usage increases as the the number of admitted flows increase. However, when the network becomes overloaded the bandwidth usage fails to increase according to the bandwidth needs of the admitted traffic. When the voice flow is allowed into the network at 12 seconds, the utilized bandwidth for video traffic fluctuates. The bandwidth allocated to video traffic fails to increase to what is required when the video flow at 14 seconds is accepted into the network. In fact the bandwidth utilized for video traffic decreases after 20 seconds. though more traffic has to be serviced. This is once again due to the nature of WLAN's contention-based MAC. When the wireless medium becomes overloaded poor utilization is made of the network's bandwidth. Furthermore, it can be observed that utilized bandwidth for voice traffic fluctuates after 25 seconds. The best-effort traffic receives little bandwidth after 20 seconds.

Figure 5.14 shows the total bandwidth usage when the admission control scheme is applied. It is clear that a good decision was made to reject the voice request at 12 seconds, so that the network can guarantee the 4687.5 kbps required for video traffic at that stage. A higher bandwidth utilization is achieved when admission control is applied. even though less traffic is admitted into the network. Thus effective usage is made of the network's resources, while the bandwidth requirements for all admitted flows are still met.

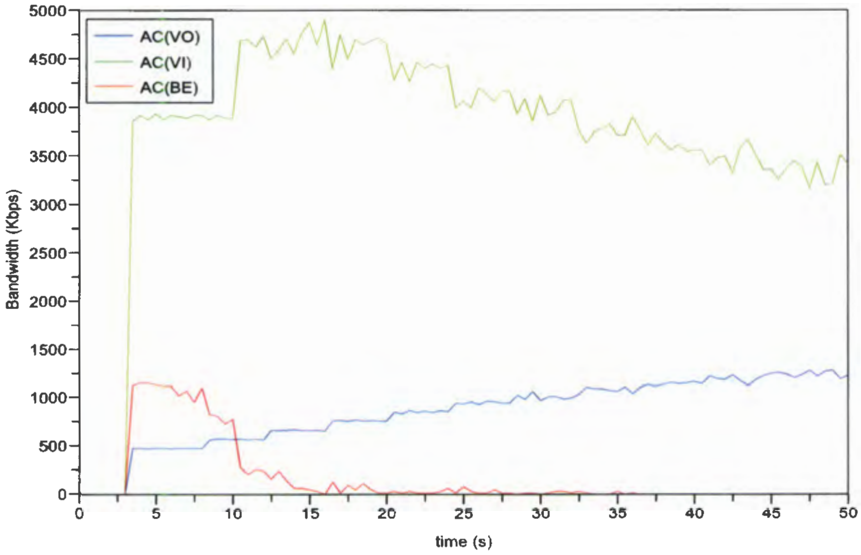


Figure 5.13: Bandwidth usage for the RTS/CTS access mechanism without admission control (total bandwidth)

Figure 5.15 shows the total bandwidth usage, when an additional voice flow is accepted after 12 seconds and an additional video flow is accepted after 14 seconds. In the graph it is clear that network is unable to cope with the bandwidth demands for video traffic. Only an average of 4778 kbps can be allocated to video traffic after 14 seconds; however, the bandwidth required is 5468.75 kbps to service the 7 video flows. Figure 5.16 shows the effect that the admission of extra flows has on the monitored traffic flows. Even though the voice flow is allocated the required its bandwidth the video is not.

5.3.3 Contention Free Bursting (CFB)

Figure 5.17 shows the bandwidth usage of 3 flows without admission control, while Figure 5.18 shows the bandwidth usage of these flows when the proposed

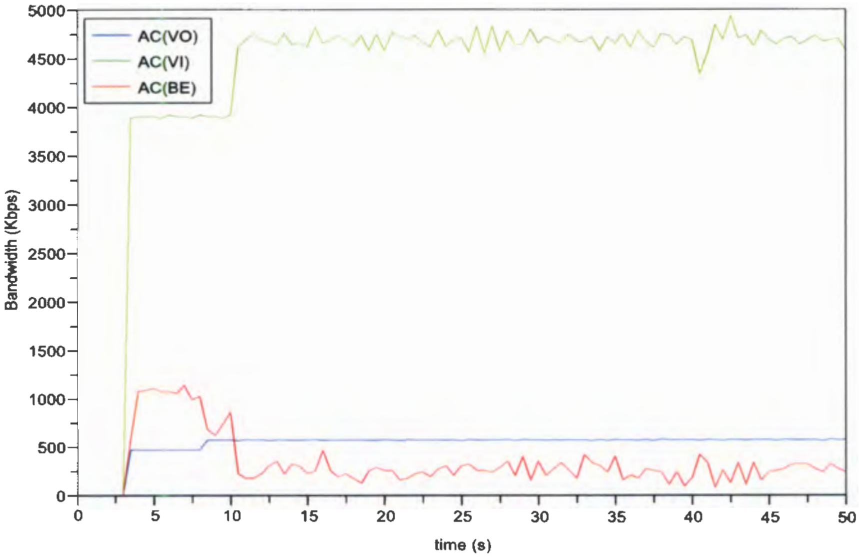


Figure 5.14: Bandwidth usage for the RTS/CTS access mechanism with admission control enabled (total bandwidth)

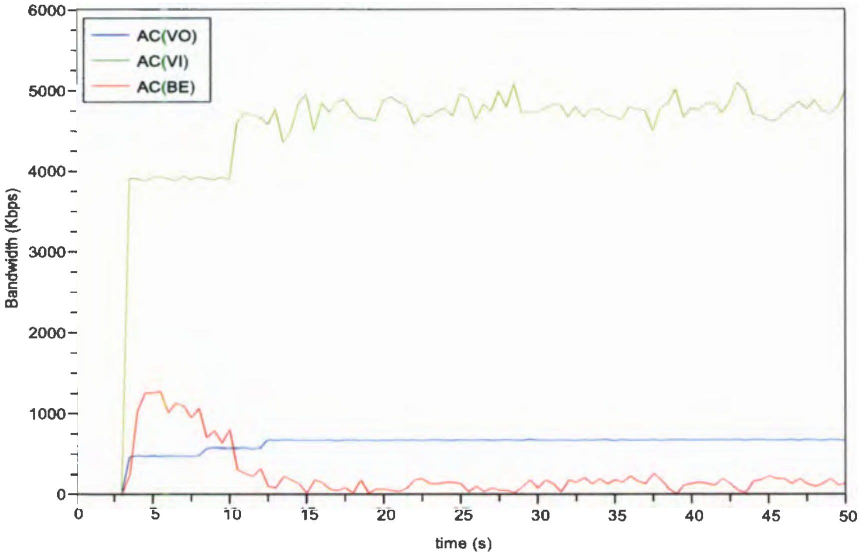


Figure 5.15: Bandwidth usage for the RTS/CTS access mechanism after admitting 2 extra flows (total bandwidth)

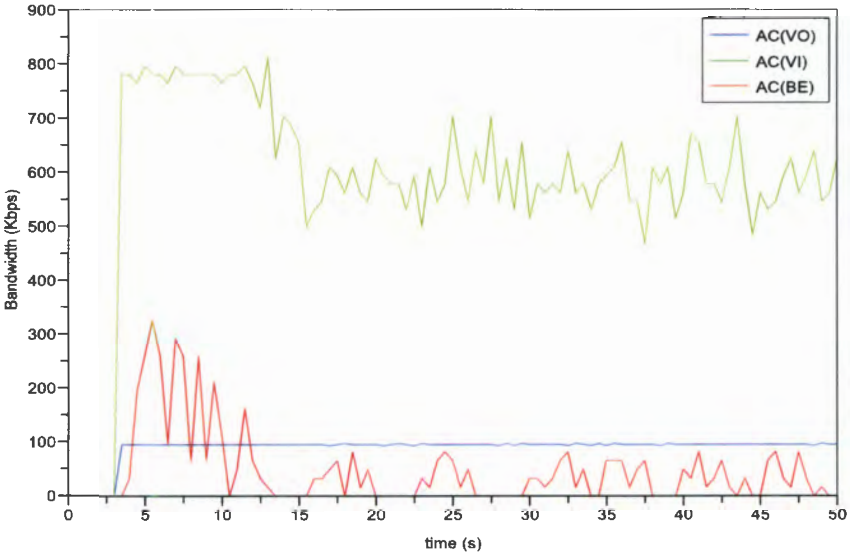


Figure 5.16: Bandwidth usage for the RTS/CTS access mechanism after admitting 2 extra flows (monitoring a single flow per AC)

admission control scheme is asserted in the network. Figure 5.19 displays the log text file for the flow requests. Once again, it is found that the admission control scheme is able to protect the bandwidth needs of the flows by preventing the network from becoming overloaded.

In Figure 5.17 it can be seen that the bandwidth usage of the video and voice flows experiences fluctuations after 24 seconds. This is because a new voice flow is accepted into the network at about 24 seconds, causing a degradation in the bandwidth usage for the video flow. The situation is different when the admission control scheme is applied, because all the requests are rejected after 24 seconds as indicated in Figure 5.19.

It is clear that when no admission control is applied the utilized bandwidth for both voice and video flows fluctuates after 24 seconds. In the cases for the Basic and RTS/CTS access modes the voice flow only fluctuates later in the simulation when more flows are active in the overloaded network. This is because with CFB the voice traffic is assigned a shorter TXOP than video traffic. It is also clear that more traffic can be admitted into the network as compared to the Basic and RTS/CTS access schemes. This is because less bandwidth is wasted on collisions and random backoff, which is due to reduction in contention for access to the medium.

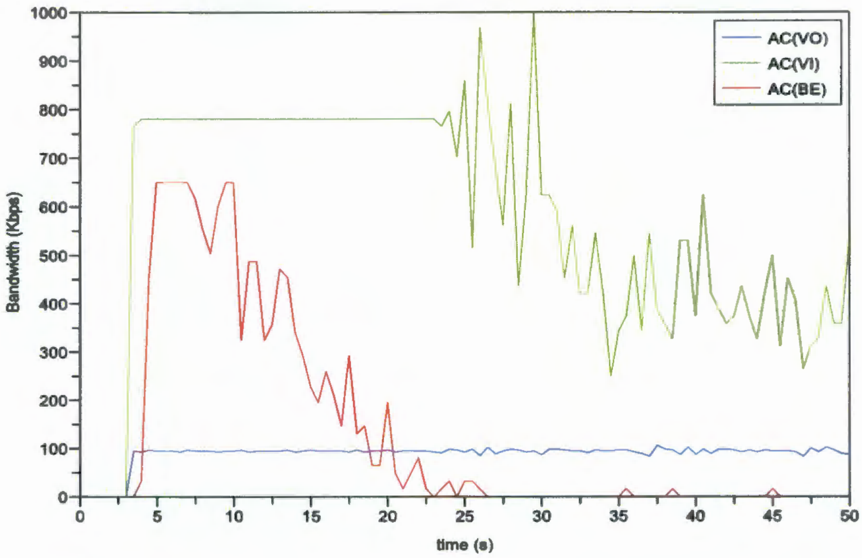


Figure 5.17: Bandwidth usage for the CFB access mechanism without admission control (monitoring a single flow per AC)

Figure 5.20 shows the total bandwidth used in the network for voice, video and best-effort traffic when no admission control is applied. Initially, the total bandwidth utilization increases as the the number of admitted flows increase. However, when the network becomes overloaded the utilized bandwidth fails to increase according to the bandwidth needs of the admitted traffic. When the voice flow is allowed into the network at 24 seconds the utilized bandwidth for both voice and video traffic fluctuates. The bandwidth utilized for video traffic decreases after 28 seconds, even though more traffic has to be serviced. The best-effort traffic receives little bandwidth after 26 seconds.

Figure 5.21 shows the total bandwidth usage when the admission control scheme is applied. A good decision was made to reject all the requests after 24 seconds. When the admission control scheme is asserted the bandwidth requirements for all admitted traffic flows are met. It is observed that no requests are rejected before 24 seconds, the period during which the network shows predictable performance.

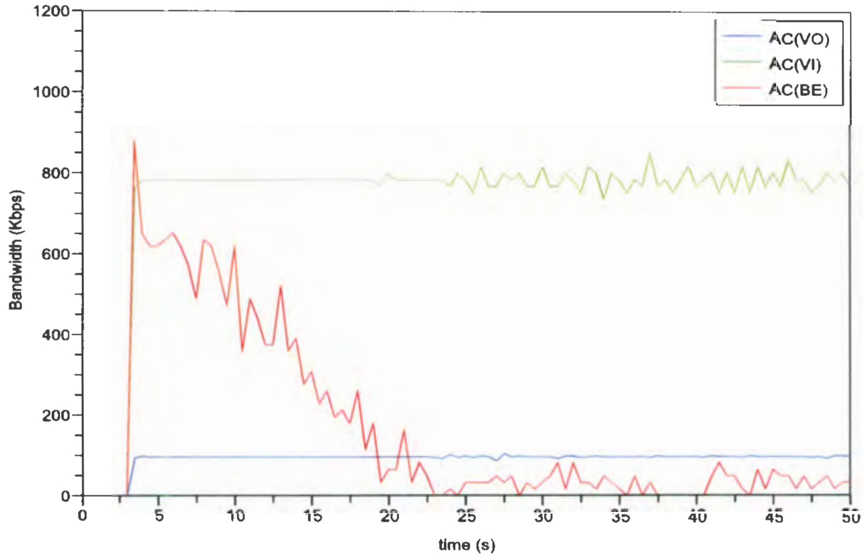


Figure 5.18: Bandwidth usage for the CFB access mechanism with admission control enabled (monitoring a single flow per AC)

```
8.0142358335842800 tspec granted for sta 1 AC_VO
10.003294060309599 tspec granted for sta 1 AC_VI
12.007150867529406 tspec granted for sta 2 AC_VO
14.019395389207382 tspec granted for sta 2 AC_VI
16.011330010502235 tspec granted for sta 3 AC_VO
18.005839046985017 tspec granted for sta 3 AC_VI
20.014087667643569 tspec granted for sta 4 AC_VO
22.002548483639075 tspec granted for sta 4 AC_VI
24.029950385989078 tspec refused for sta 5 AC_VO
26.019105791525547 tspec refused for sta 5 AC_VI
28.029904641960101 tspec refused for sta 1 AC_VO
30.007929501029370 tspec refused for sta 1 AC_VI
32.030545341087333 tspec refused for sta 2 AC_VO
34.029654742328503 tspec refused for sta 2 AC_VI
36.003626438315770 tspec refused for sta 3 AC_VO
38.010642284532373 tspec refused for sta 3 AC_VI
40.015623929618243 tspec refused for sta 4 AC_VO
42.010762347239307 tspec refused for sta 4 AC_VI
44.001977513157414 tspec refused for sta 5 AC_VO
46.006608924214724 tspec refused for sta 5 AC_VI
```

Figure 5.19: TSPEC request log (CFB mechanism)

Thus, the maximum number of traffic flows are accommodated by the available network bandwidth.

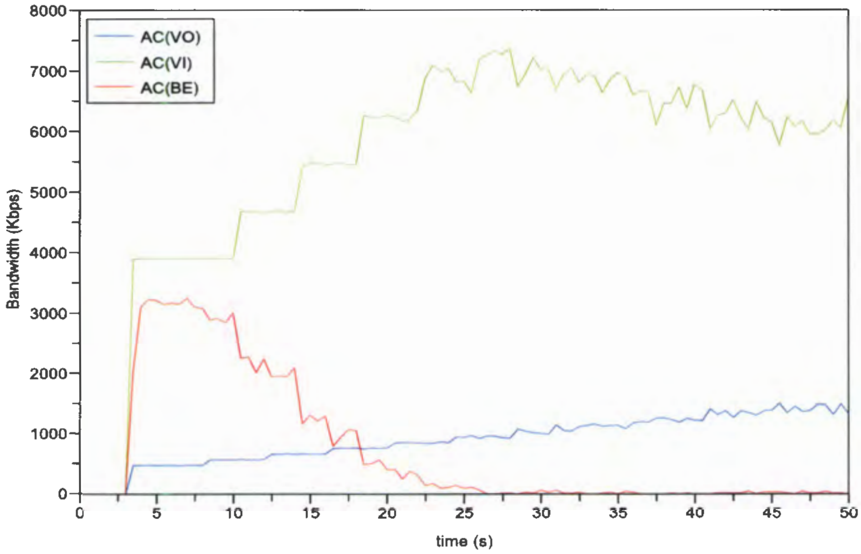


Figure 5.20: Bandwidth usage for the CFB access mechanism without admission control (total bandwidth)

Figure 5.22 shows the total bandwidth utilization when an additional voice flow is accepted after 24 seconds, and an additional video flow is accepted after 26 seconds. In the graph, it is clear that the network is unable to cope with the bandwidth demands for both voice and video traffic after 26 seconds. Only an average of 7215 kbps can be allocated to video traffic; whereas the bandwidth required is 7812.5 kbps to service 10 video flows. An average of 903.125 kbps can be allocated to voice traffic, while the bandwidth required is 953.5 kbps to service 10 voice flows. Figure 5.23 shows the effect the admission of the extra flows has on the traffic. Both the voice and video flows are unable to maintain the required bandwidth after 24 seconds.

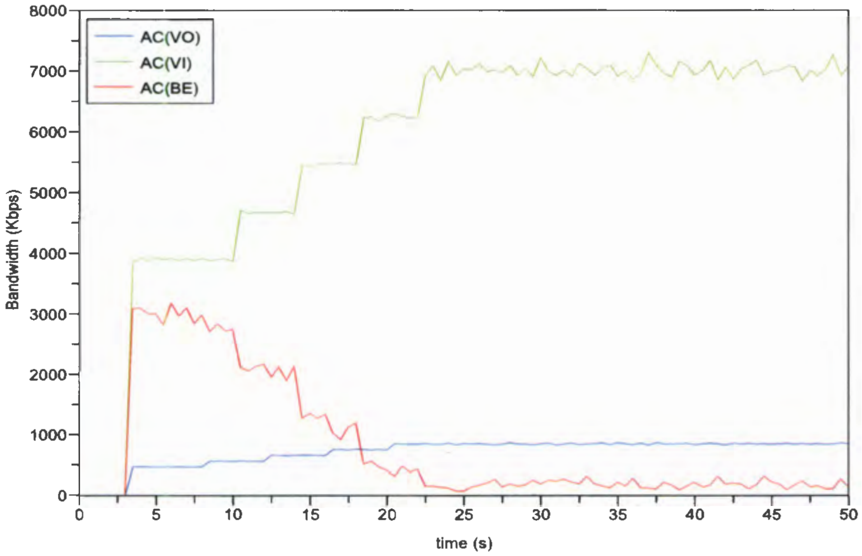


Figure 5.21: Bandwidth usage for the CFB access mechanism with admission control enabled (total bandwidth)

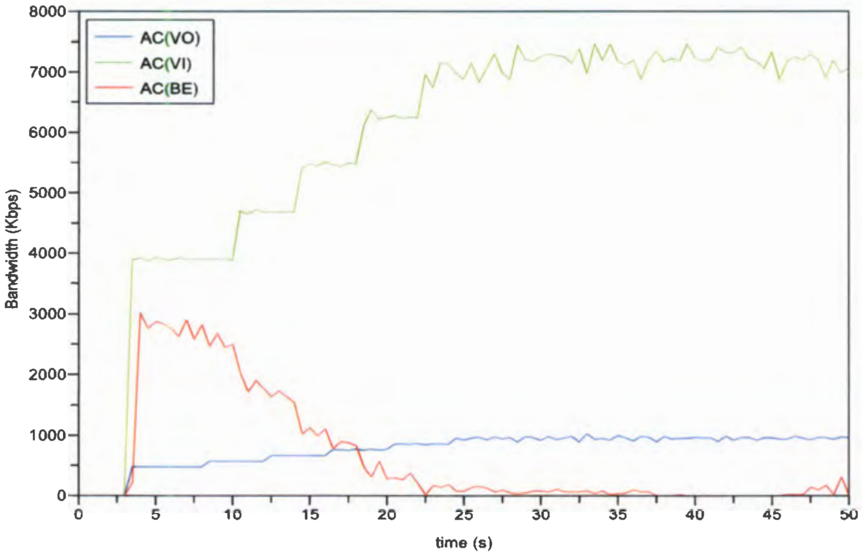


Figure 5.22: Bandwidth usage for the CFB access mechanism after admitting 2 extra flows (total bandwidth)

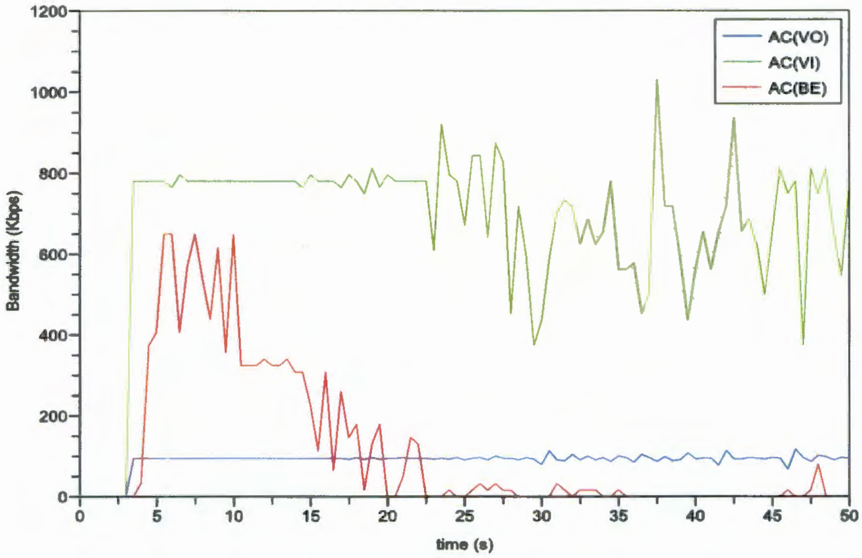


Figure 5.23: Bandwidth usage for the CFB access mechanism after admitting 2 extra flows (monitoring a single flow per AC)

5.4 Discussion

In this chapter it was found that the bandwidth estimations for Virtual Stations, used by the admission control scheme, were fairly accurate. The concept of using the proposed admission control scheme was evaluated for three medium access mechanisms. In all cases bandwidth requirements for all admitted flows were met when the proposed admission control scheme was applied. It was also shown that the network's resources were effectively utilized since maximum flows were accommodated by the network's capacity. Any additional traffic that was not permitted by the admission control scheme, jeopodized the bandwidth guarantees for admitted traffic. Thus, the goals of the admission control scheme set out in this thesis were satisfied.

It was observed that bandwidth utilization is different for the three medium access mechanisms. As a result the amount of traffic flows that can be accommodated were different depending on the medium access mechanisms used. Figure 5.24 shows the number of admitted flows that could be accommodated by the network, for the three medium access mechanisms, when the proposed admission control scheme was applied. It is clear that the RTS/CTS mechanism accommodates the least amount of voice and video flows, due to the bandwidth wasted by the overhead of RTS and CTS frames. The CFB mechanism was able to accommodate two more video flows than the basic access mechanism. This is mainly due to bandwidth saved by the reduced contention.

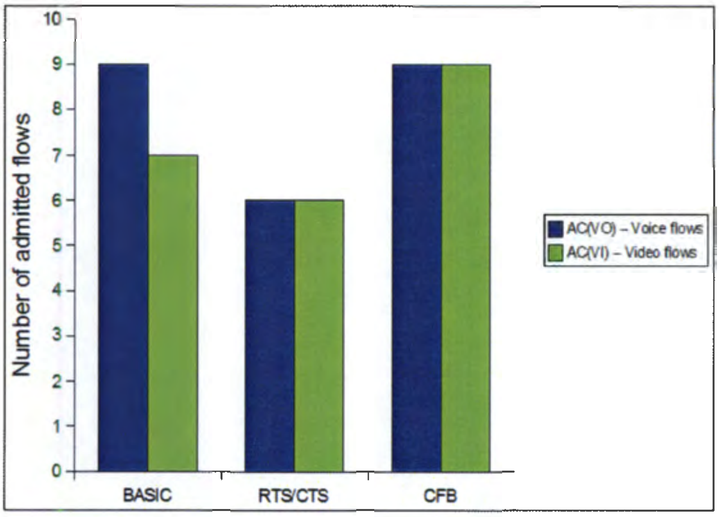


Figure 5.24: Number of admitted flows for the medium access mechanisms

Chapter 6

Conclusions and Recommendations

6.1 Conclusions

The IEEE 802.11e EDCA is able to provide relatively good QoS support for wireless users. However, QoS for real-time flows is heavily degraded during saturated network conditions. This study investigated admission control techniques relating to specific goals set out in this thesis. These goals were to guarantee all bandwidth requirements for the real-time traffic admitted into the network, and to make effective use of the network's resources by accomodating as many flows as possible. It was found that a number of admission control schemes identified in the literature were unable to satisfy both these goals.

A promising prospect for admission control was identified, where the bandwidth of all wireless stations can be estimated to aid admission control decisions. This thesis proposed a measurement-aided model-based admission control scheme that is able to satisfy the bandwidth requirements of all admitted real-time flows, while making effective use of the network's resources. Admission control decisions are based on bandwidth estimations that are obtained by using a developed EDCA analytical model. The analytical model is aided by the measurement of collision statistics on the shared wireless medium and transmission queue activities.

A simulation framework was implemented successfully, using the NS-2 simulator.

The framework was used to evaluate the proposed admission control scheme for three medium access mechanisms (Basic, RTS/CTS and CFB). A number of simulations were performed on topologies that were adjusted specifically to evaluate the proposed admission control scheme. Based on the simulations and the findings within this thesis. the following conclusions are drawn:

- The bandwidth estimations for EDCA VSTAs are reasonably accurate. This enables the proposed admission control scheme to make effective admission control decisions.
- When the proposed admission control scheme is applied to the network all bandwidth requirements are met for admitted real-time flows due to good admission control decisions. Flows are rejected only if it is estimated that their admission would cause bandwidth guarantees of admitted flows to be violated.
- The proposed admission control scheme is able to make optimal use of network resources when the network becomes overloaded with real-time traffic requests. A maximum number of flows whose bandwidth requests can be satisfied are accommodated by the network's resources. Any additional flows accepted into the network would violate bandwidth requirements of some admitted flows and introduced bandwidth instabilities. Thus, the proposed admission control scheme satisfies the goals that are set out in this thesis.
- The Contention Free Bursting (CFB) medium access mechanism, specified in the IEEE 802.11e standard, was introduced to improve bandwidth utilization for the EDCA. It was found to achieve the intended purpose as it is able to maintain a higher bandwidth utilization of the shared wireless channel than the basic or RTS/CTS access mechanism. The proposed admission control scheme can admit more real-time traffic into the network when this medium access mechanism is used.
- When there are no hidden stations present in the WLAN the RTS/CTS mechanism maintains a lower bandwidth utilization compared the CFB and the basic access mechanism. The admission control scheme admits less real-time traffic into the network when this medium access mechanism is used.

6.2 Recommendations and Future Work

This study encompasses a broad spectrum of networking concepts and technologies. These range from admission control techniques for real-time application in WLANs to bandwidth estimation techniques for IEEE 802.11e EDCA WLANs. While conducting this research, a number of issues that can be addressed became apparent. The following is a list of recommendations that arise from these issues:

- The CFB medium access scheme should be used whenever possible, because of its good bandwidth utilization and fairness towards real-time applications.
- The RTS/CTS medium access should be avoided since it was shown to utilize WLAN resources in a poor manner compared the the basic or CFB medium access mechanisms. It is recommended that the possibilities for hidden nodes be reduced by using alternative methods such as increasing the transmission power of wireless stations.
- The bandwidth utilization of a combined RTS/CTS and CFB medium access mode was not investigated in this thesis. It is recommended that further investigation be done for this mode and the performance when admission control is applied. This mode can be used when hidden stations are unavoidable. This medium access mode will allow good CFB features, while managing hidden nodes.
- Further investigation into modelling the achievable bandwidth may be done. The proposed admission control requires signalling procedures to communicate transmission probabilities, based on measured collision statistics and queue activities, to the QAP. This makes it hard for standard WLAN devices to co-operate with the admission control scheme. Further investigation should be taken to model these collision probabilities at the QAP with an acceptable computational cost. The main benefit is that only the QAP needs to be modified to implement the proposed admission control. Another benefit is that no signalling bandwidth would be required for bandwidth estimations.
- The effects of error control techniques are not explored in this thesis. The proposed admission control scheme requires that the bit error rates, due to

bad channel conditions, be minimized. Thus it is highly recommended that error control techniques such as Automatic Rate Fallback (ARF) be used in conjunction with the proposed admission control scheme.

- The real-time traffic used in the evaluation framework was strictly CBR for simpler evaluation purposes. Further studies can be done on VBR traffic to evaluate the effect of the admission control. Traffic engineering tools (e.g. leaky bucket) can be applied to reduce the burstiness of VBR traffic so that predictable bandwidth utilization can be maintained.

- The IEEE 802.11e standard specifies that admission control can only be applied for real-time traffic. However, too many unsuccessful best-effort data transmissions can degrade the existing voice and video flows, since these data transmissions may cause many collisions. In this way, real-time traffic can become vulnerable to best-effort data traffic. Further study needs to be taken to investigate methods where best effort traffic is limited to protect the bandwidth guarantees of real-time traffic. One way to achieve this is to dynamically control the EDCA parameters for the best effort ACs so that the number of collisions are kept relatively small. This can be done by increasing the initial contention window size and inter-frame spaces. For further details on this "second-level" protection method, the reader is referred to [44].

Bibliography

[1] IEEE Std 802.11e, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment: Medium Access Control (MAC) Quality of Service Enhancements," 2005.

[2] D. He and C. Shen, "Analysis of IEEE 802.11e for QoS Support in Wireless LANs," in *IEEE Wireless Communications Magazine, Special Issue on Evolution of Wireless LANs and PANs*, July 2003.

[3] S. M. S. Choi, J. Prado and S. Shankar, "IEEE 802.11e contention based channel access (EDCF) performance evaluation," in *IEEE International Conference Communications (ICC)*, (Anchorage, AK), pp. 1151–1156, 2003.

[4] D. He and C. Shen, "Simulation Study of IEEE 802.11e EDCF," *The 57th IEEE Semiannual Vehicular Technology Conference (VTC)*, vol. 1, pp. 685–689, April 2003.

[5] A. Lindgren, A. Almquist and O. Schelen, "Evaluation of quality of service schemes for IEEE 802.11 wirelessLANs," in *6th Annual IEEE Conference on Local Computer Networks (LCN)*, pp. 348 – 351, 2001.

[6] Jangeun Jun, Pushkin Peddabachagari, Mihail Sichitiu., "Theoretical maximum throughput of IEEE 802.11 and its applications," in *Second IEEE International Symposium on Network Computing and Applications*, pp. 249 – 256, 16-18 April 2003.

[7] M. Heusse, F. Rousseau, G. Berger-Sabbatel, A. Duda, "Performance Anomaly of 802.11b," in *INFOCOM 2003: Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 2, (San Francisco, California, USA), pp. 836– 843, 30 March-3 April 2003.

[8] ANSI/IEEE Std 802.11, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 1999.

[9] IEEE Std 802.11b (Supplement to ANSI/IEEE Std 802.11 1999 Edition), "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band," 1999.

[10] Y. Wang and J. Garcia-Luna-Aceves, "Modeling of Collision Avoidance Protocols in Single-Channel Multihop Wireless Networks," tech. rep., Department of Computer Engineering, University of California, Santa Cruz, CA 95064, USA.

[11] IEEE Std 802.11a (Supplement to ANSI/IEEE Std 802.11 1999 Edition), "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher Speed Physical Layer (PHY) in the 5 GHz band," 1999.

[12] IEEE Std 802.11g (Amendment to IEEE Std 802.11-1999 Edition (Reaff 2003) as amended by IEEE Stds 802.11a-1999 802.11b-1999 802.11b-1999/Cor 1-2001 and 802.11d-2001), "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band," 2003.

[13] IEEE 802.11n, "Wireless LAN Medium Access Control MAC and Physical Layer PHY specifications. IEEE 802.11n-D1.0," 2006.

[14] IEEE 802.11 Working Group, "OFFICIAL IEEE 802.11 WORKING GROUP PROJECT TIMELINES." `http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm`.

[15] D. Black, S. Blake, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "An Architecture for Differentiated Services." IETF RFC 2475, December 1998.

[16] B. Selvig, A. Bai, T. Skeie, and P.E Engelstad, "Differentiated Services in 802.11e WLANs," in *Norwegian Network Research Seminar (NNRS)*, 27-28 October 2005.

[17] Seyong Park, Kyungtae Kim, D.C Kim, Sunghyun Choi, Sangjin Hong, "Collaborative QoS Architecture between DiffServ and 802.11e Wireless LAN," in *The 57th IEEE Semiannual Vehicular Technology Conference (VTC)*, vol. 2, pp. 945–949, 22-25 April 2003.

[18] S Mangold, S Choi and G.R Hiertz, "Analysis of IEEE 802.11e for QoS support in Wireless LANs," in *IEEE Wireless Communications*, vol. 10, Issue: 6, pp. 40–50, December 2003.

[19] Y. Xiao and H. Li, "Evaluation of Distributed Admission Control for the IEEE 802.11e EDCA," in *IEEE Communications Magazine*, vol. 42, Issue: 9, pp. 20–24, September 2004.

[20] D. Gu and J. Zhang, "A New Measurement-based Admission Control Method for IEEE 802.11 Wireless Local Area Networks," tech. rep., Mitsubishi Elec. Research Lab, October 2003.

[21] D. Pong and T. Moors, "Call Admission Control for IEEE 802.11 Contention Access Mechanism," in *IEEE GLOBECOM'03, vol. 1*, (San Francisco), pp. 174–178, December 2003.

[22] G. Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function," in *IEEE Journal on Selected Area in Communications*, pp. 535–547, March 2000.

[23] Y. Tay and K. Chua, "A Capacity Analysis for the IEEE 802.11 MAC Protocol," in *Wireless Networks archive*, vol. 7, Issue 2, pp. 159–171, April 2001.

[24] J. Hui and M. Devetsikiotis, "Performance analysis of IEEE 802.11e EDCA by a unified model," in *Proc. of IEEE Globecom*, (Dallas, Texas), pp. 754–759, November 2004.

[25] B. B. Z. Kong, D.H.K. Tsang and D. Gao, "Performance Analysis of IEEE 802.11e Contention-Based Channel Access," in *IEEE Journal on Selected Area in Communications*, vol. 22, no.10, pp. 2095–2106, June 2004.

[26] J. Robbinson and T. Randhawa, "Saturation Throughput Analysis of IEEE 802.11e Enhanced Distributed Coordination Function," in *IEEE Journal on Selected Area in Communications*, vol. 22, no.5, pp. 917–928, June 2004.

[27] Y. Xiao, "Performance analysis of IEEE 802.11e EDCF under saturation condition," in *Proc. of IEEE ICC*, (Paris, France), pp. 170–174, June 2004.

[28] A. Kamerman and L. Monteban, "WaveLAN-II: A High-Performance Wireless LAN for the Unlicensed Band," in *Bell Labs Technical Journal*, pp. 118–133, 1997.

[29] R. Bruno M. Conti and E. Gregori, "IEEE 802.11 Optimal Performances: RTS-CTS Mechanism versus Basic Access," in *The 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, (IT Inst., CNR, Pisa, Italy), pp. 1747– 1751 vol.4, September 2002.

[30] "The Network Simulator - NS-2." `http://www.isi.edu/nsnam/ns/`.

[31] Priyank Garg, Rushabh Doshi, Russell Greene, Mary Baker, Majid Malek, and Xiaoyan Cheng, "Using IEEE 802.11e MAC for QoS over Wireless," in *Proc. of IPCCC*, pp. 537–542, 9-11 April 2003.

[32] IEEE 802.11e WG, "Medium Access Control (MAC) Quality of Service (QoS) Enhancements, P802.11e/D2.0a," November 2001.

[33] IEEE 802.11e WG, "Medium Access Control (MAC) Quality of Service (QoS) Enhancements, P802.11e/D4.3," May 2003.

[34] Gennaro Boggia, Pietro Camarda, Luigi Alfredo Grieco, and Saverio Mascolo, "Feedback-based bandwidth allocation with call admission control for providing delay guarantees in IEEE 802.11e networks," in *Computer Communications, special issue*, pp. 325–337, February 2005.

[35] Claudio Cicconetti, Luciano Lenzini, Enzo Mingozzi and Giovanni Stea, "A Software Architecture for Simulating IEEE 802.11e HCCA," in *Proc. of IPS-MoMe*, pp. 14–15, March 2005.

[36] L. Romdhani, Qiang Ni, and Thierry Turletti, "Adaptive EDCF: Enhanced Service Differentiation for IEEE 802.11 Wireless Ad Hoc Networks," in *IEEE Wireless Communications and Networking Conference (WCNC 2003)*, (New Orleans, Louisiana, USA), March 16-20 2003.

[37] M. Malli, Qiang Ni, Thierry Turletti, and Chadi Barakat. "Adaptive Fair Channel Allocation for QoS Enhancement in IEEE 802.11 Wireless LANs," in *IEEE International Conference on Communications (ICC 2004)*, (Paris), June 2004.

[38] Pierre Ansel, Qiang Ni, and Thierry Turletti, "FHCF: A Simple and Efficient Scheduling Scheme for IEEE 802.11e," in *Journal on Mobile Networks and Applications (MONET)*, vol. 11, Issue 3, pp. 391–403. June 2006.

[39] Mathieu Lacage and Thomas R. Henderson, "Yet Another Network Simulator," in *Proceedings from the Workshop on ns-2: the IP Network Simulator*, (Pisa, Italy), October 10 2006.

[40] Mineo Takai , Jay Martin , Rajive Bagrodia, "Effects of wireless physical layer modeling in mobile ad hoc networks," in *2nd ACM international symposium on Mobile ad hoc networking and computing*, (Long Beach, CA, USA), pp. 87 – 94, 04-05 October 2001.

[41] H. Schulzrinne et al., "RTP: A transport protocol for real-time application." IETF, RFC 1889, January 1996.

[42] J. Postel, "User Datagram Protocol." IETF. RFC 768, August 1980.

[43] Information Sciences Institute, University of Southern California, "Transmission Control Protocol." RFC: 793, September 1981.

[44] Yang Xiao, Haizhon Li, Sunghyun Choi, "Protection and guarantee for voice and video traffic in IEEE 802.11e wireless LANs," in *INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. Volume 3, pp. 2152 – 2162 vol.3, 7-11 March 2004.

Appendix A

WLAN Enhancements

A.1 IEEE 802.11e Amendments

A.1.1 IEEE 802.11e

IEEE 802.11e is concerned with providing QoS support for multimedia transmissions over 802.11 networks. The enhancement is of great importance to delay-sensitive applications, such as VoIP and streaming multimedia applications. Section 2.2 provides more details on the IEEE 802.11e enhancement.

A.1.2 IEEE 802.11f

This enhancement is concerned with improving the performance of roaming between APs and ensuring interoperability between vendors. The protocol is designed to aid the handoff process through a secure exchange of a station's security context between the current AP and the new AP. This enforces a unique association throughout an ESS.

A.1.3 IEEE 802.11i

This enhancement defines security improvements to overcome the shortcomings of the original 802.11 standard's security mechanisms.

A.1.4 IEEE 802.11p

This enhancement is referred to as Wireless Access for the Vehicular Environment (WAVE). This will allow for data exchange between high-speed vehicles and between the vehicles and the roadside infrastructure. The enhancement will provide support for Intelligent Transport Systems (ITSs) applications, such as toll collection, vehicle safety services, and commerce transactions via cars. The 802.11p standard is scheduled to be published in April 2009.

A.1.5 IEEE 802.11Q

This enhancement specifies a mechanism that allows multiple bridged networks to transparently share the same physical network link. This amendment is of particular importance for bridging 802.11e WLANs to 802.3 Ethernet segments without losing QoS information. This is done by encapsulating frame overheads between bridged segments.

A.1.6 IEEE 802.11r

This enhancement specifies fast BSS transition. This is of great importance to mobile real-time multimedia applications.

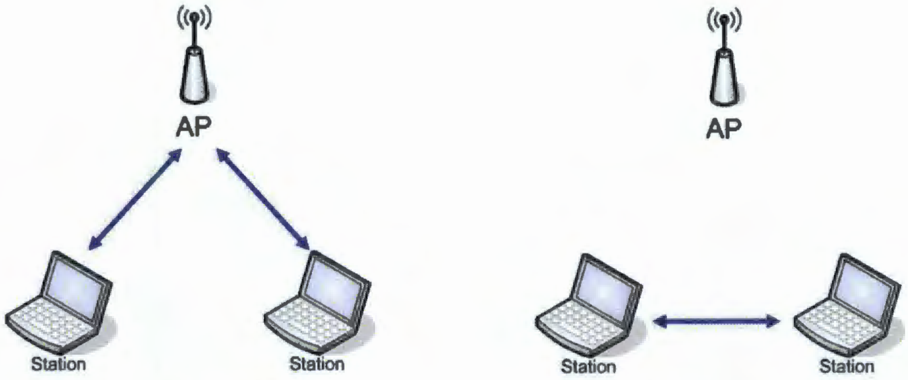
A.2 Optional IEEE 802.11e Features

A.2.1 Enhanced Acknowledgement Procedures

To further improve the channel efficiency, the IEEE 802.11e amendment offers Block Acknowledgements that allow an entire TXOP to be acknowledged in a single frame. This will provide less protocol overhead compared to the legacy IEEE 802.11 standard, where the receiver acknowledges each data frame individually. The IEEE 802.11e amendment also allows the disabling acknowledgements. This can be utilized by real-time application, to avoid the retransmission of time-critical data.

A.2.2 Direct Link Protocol (DLP)

The Direct Link Protocol (DLP) in 802.11e provides a mechanism that allows direct communication among QoS enabled stations (QSTAs) without traversing through the QAP. The DLP will save bandwidth in the network, because data is transmitted once over the air, instead of twice (QSTA-to-QAP and QAP-to-QSTA). DLP requires the communicating QSTAs to be within range of each other. This is designed for consumer use, where station-to-station transfer is more commonly used. Figure A.1 demonstrates the difference between a scenario where DLP is absent and one where DLP is used.



(a) without DLP (b) with DLP

Figure A.1: Communication set-up with and without DLP

A.2.3 Automatic Power Save Delivery (APSD)

Automatic Power Save Delivery (APSD) allows efficient power management that is especially useful for battery-operated devices. It is an enhancement of the legacy 802.11 power saving mechanisms that allows a station to set up a 'schedule' for delivery of frames, based on a repetitive pattern for specified number of beacon intervals. A time period within interval can be specified, allowing a number of stations to enter a doze state when they are not active. The AP will buffer the frames of stations for the number of beacon intervals specified in an APSD setup. APSD operations are invoked by TSPEC negotiations with the APSD flag set.

Appendix B

NS-2 Implementation Issues

B.1 Topology Set-up

This section displays the set up of the wireless stations and their posisioning in OTcl. The topology consists of one access point and 6 wireless stations. The 'x' and 'y' coordinates are specified so that the wireless stations are spaced approximately 13 metres from the QAP.

```
set nodeConstructor [new NodeConstructor];

set interfaceConstructor_WiFi [new TclNetInterfaceConstructor80211];

set channel_WiFi [new TclFreeSpaceBroadcastChannel];


#Setting up the wireless stations and AP

for {set i 0} {$i < 6} {incr i} {

    set nodes($i) [$nodeConstructor create-node];

}


#Setting the position of the nodes

$nodes(0) set-position 0.0 0.0 0.0

$nodes(1) set-position 1.0 12.961481400 0.0
```

```
$nodes(2) set-position 2.0 12.845232580 0.0
$nodes(3) set-position 3.0 12.649110640 0.0
$nodes(4) set-position 4.0 12.369316880 0.0
$nodes(5) set-position 5.0 12.000000000 0.0

#Setting up the interface for the QAP
$interfaceConstructor_WiFi set-qap;
set interfaces_WiFi(0) [$interfaceConstructor_WiFi create-interface];

#Setting the wireless stations
$interfaceConstructor_WiFi set-qsta 1;
for {set i 1} {$i < 6} {incr i} {
    set interfaces_WiFi($i) [$interfaceConstructor_WiFi create-interface];
}

#Adding/Connecting interfaces for the wireless nodes
for {set i 0} {$i < 6} {incr i} {
    $nodes($i) add-interface $interfaces_WiFi($i) $channel_WiFi
}
```

There are situations where only 5 wireless stations are required for simulations. In this case node(5) is not added to the set up.

B.2 Applications Used in NS-2

This sections shows the OTcl procedures required to generate the voice, video and ftp traffic used for simulation experiments.

```
#Set up voice stream
```

```
proc generate-voice-traffic {node sink} {
    global ::ns
    set now [$ns now]

  ##################################################
    # Voice Stream
    #
    # This is the canonical PCM coding for telephony networks:
    # sampling frequency is 8kHz, sample size is 1 byte, total
    # bandwidth required is thus 64kb/s and the required end-to
    # end delay is 125ms.
    #
    # RTP typically transmits at a packet interval of 10ms
    # Thus the payload size is 64kbps*10ms = 82 bytes
    #
    # This means that the size of each packet is:
    # 82 (payload) + 40 (ip+udp+rtp) + 34 (MAC header) = 156 bytes
    # MSDU = 82+40 = 122 bytes.
    # Thus, the Data Rate at the MAC level is:
    # 122bytes/10ms = 12200bytes/s
    #

    set source [new Agent/UDP];
    $node attach-agent $source;
    set cbr [new Application/Traffic/CBR];
    $cbr attach-agent $source;
    $cbr set packetSize_ 122
    $cbr set interval_ 0.01
```

```
    $source set class_ 0;
    $source set prio_ 7

    ip-connect $source $sink
    $ns at $now "$cbr start"
}


#Set up video stream
proc generate-video-traffic {node sink} {
    global ::ns
    set now [$ns now]

 ##################################################
    # CBR Video Stream (MPEG4)
    #
    # This is an MPEG4 Video Stream, with a data rate of 750 Kbps
    #
    # RTP typically transmits at a packet interval of 10ms
    # Thus the payload size is 750kbps*10ms = 960 bytes
    #
    # This means that the size of each packet is:
    # 960 (payload) + 40 (ip+udp+rtp) + 34 (MAC header) = 1034 bytes
    # MSDU = 960+40 = 1000 bytes.
    # Thus, the Data Rate at the MAC level is:
    # 1000bytes/10ms = 100000bytes/s
    #
```

```
    set source [new Agent/UDP];
    $node attach-agent $source;
    set cbr [new Application/Traffic/CBR]:
    $cbr attach-agent $source;
    $cbr set packetSize_ 1000
    $cbr set interval_ 0.01
    $source set class_ 0;
    $source set prio_ 5

    ip-connect $source $sink
    $ns at $now "$cbr start"
}


#Set up ftp traffic
proc generate-ftp-traffic {node sink} {
    global ::ns
    set now [$ns now]

 #################################################
    # FTP Application
    #
    # segment = 1040 bytes
    #
    # packet size = segment size - tcp overhead
    # = 1040 - 40 = 1000 bytes
    #
```

```
        set source [new Agent/TCP];
        $node attach-agent $source;
        set ftp [new Application/FTP];
        $ftp attach-agent $source;
        $ftp set packetSize_ 1000
        $ftp set maxpkts_ 10000000
        $source set class_ 0;
        $source set prio_ 1

        ip-connect $source $sink
        $ns at $now "$ftp start"
    }
```

B.3 TSPEC Set-up and Handling in NS-2

The OTcl code below shows how the voice and video TSPEC request are are set up according the the required traffic parameters shown in B.2.

```
    #Setting Up the TSPEC for Voice
    set tspec0 [new TclTspec]
    $tspec0 set-minimum-service-interval 0.01     ;# ms
    $tspec0 set-maximum-service-interval 0.01     ;# ms
    $tspec0 set-delay-bound 0.125     ;# ms
    $tspec0 set-nominal-msdu-size 122     ;# bytes
```

```
$tspec0 set-mean-data-rate 12200     ;# bytes per second
$tspec0 set-peak-data-rate 12200     ;# bytes per second
$tspec0 set-access-policy EDCA
$tspec0 set-user-priority 7

#Setting up TSPEC for Video
set tspec1 [new TclTspec]
$tspec1 set-minimum-service-interval 0.01     ;# ms
$tspec1 set-maximum-service-interval 0.01     ;# ms
$tspec1 set-delay-bound 0.125     ;# ms
$tspec1 set-nominal-msdu-size 1000     ;# bytes
$tspec1 set-mean-data-rate 100000     ;# bytes per second
$tspec1 set-peak-data-rate 100000     ;# bytes per second
$tspec1 set-access-policy EDCA
$tspec1 set-user-priority 5
```

The example below shows how video and voice request can be generated by station 1 during a random interval between 10 seconds and 10.01 seconds.

```
$ns at [expr 10 + rand()*0.01]
"$interfaces_WiFi(1) addts $tspec0 addts-granted-callback0 addts-refused-callback0”

$ns at [expr 10 + rand()*0.01]
"$interfaces_WiFi(1) addts $tspec1 addts-granted-callback1 addts-refused-callback1"
```

The request message contains an entry point to a callback procedure within the OTcl code. The actual procedure that is called depends on the response from the QAP. The section of OTcl code bellow, demonstrates four procedure calls, where video and voice flow requests are accepted or rejected depending on the response from the QAP:

```
#Allow Voice Stream
proc addts-granted-callback0 {tspec tsid sta} {
    global ::ns
    global ::nodes
    global NumVO sinkVO log

    set now [$ns now]     ;#get the current time
    set sinknum [expr $NumVO + 1]

    #start the new flow
    $ns at $now "generate-voice-traffic $nodes($sta) $sinkVO($sinknum)"
    puts $log "$now tspec granted for sta $sta AC_VO"
    incr NumVO ;#increments the number of admitted Voice flows
}


#Refuse the Voice Stream
proc addts-refused-callback0 {tspec tsid sta} {
    global ::ns
    global log

    set now [$ns now] ;    #get the current time

    puts $log "$now tspec refused for sta $sta AC_VO";
}
```

```
    #Allow Video Stream
    proc addts-granted-callback1 {tspec tsid sta} {
        global ::ns
        global ::nodes
        global NumVI sinkVI log

        set now [$ns now]     ;#get the current time
        set sinknum [expr $NumVI + 1]

        $ns at $now "generate-video-traffic $nodes($sta) $sinkVI($sinknum)"
        puts $log "$now tspec granted for sta $sta AC_VI"
        incr NumVI
    }


    #Refuse Video Stream
    proc addts-refused-callback1 {tspec tsid sta} {
        global ::ns
        global log

        set now [$ns now]     ;#get the current time

        puts $log "$now tspec refused for sta $sta AC_VI"
}
```

B.4 Recording Bandwidth Statistics in NS-2

This section shows how bandwidth statistics are extracted to a form where they can easily be used to display graphs. Output files are required to be opened for writing the statistics. The following lines displays how this is done in the beginning of the Tcl script.

```
#To gather bandwidth statistics for three monitored traffic sources
set f0 [open throughput0.tr w]
set f1 [open throughput1.tr w]
set f2 [open throughput2.tr w]

#To gather the total bandwidth statistics for three three Access Classes
set f3 [open throughputAC_VO.tr w]
set f4 [open throughputAC_VI.tr w]
set f5 [open throughputAC_BE.tr w]
```

The following OTcl procedure shown bellow is used to gather statistics for the total bandwidth and the bandwidth for 3 monitored traffic flows. This procedure reads the number of bytes received from the the traffic sinks. Then it calculates the bandwidth (in MBit/s) and writes it to the appropriate output files together with the current time. The procedure ends by resetting the bytes_ values gathered during a 0.5 second period and then it re-schedules itself.

```
#Recording bandwidth statistics
proc record {} {
    global sinkVO sinkVI sinkBE f0 f1 f2 f3 f4 f5

    #Get an instance of the simulator
    set ns [Simulator instance]

    #Set the time after which the procedure should be called again
    set time 0.5
```

```
#Set the amount of bytes gathered during the 0.5 second period
#(Monitored 3 flows)
set bw0 [$sinkVO(1) set bytes_]
set bw1 [$sinkVI(1) set bytes_]
set bw2 [$sinkBE(1) set bytes_]

#Initializing the total bandwidth variables
set bw3 0
set bw4 0
set bw5 0

#calculating bw3, bw4 and bw5
for {set i 0} {$i < 20} {incr i} {
    set tmp3 [$sinkVO($i) set bytes_]
    set tmp4 [$sinkVI($i) set bytes_]
    set tmp5 [$sinkBE($i) set bytes_]
    incr bw3 $tmp3
    incr bw4 $tmp4
    incr bw5 $tmp5
}



#Get the current time
set now [$ns now]

#Calculate the bandwidth (in B/s) and write it to the files
puts $f0 "$now \t[expr $bw0/$time]"
puts $f1 "$now \t[expr $bw1/$time]"
```

```
    puts $f2 "$now \t[expr $bw2/$time]"
    puts $f3 "$now \t[expr $bw3/$time]"
    puts $f4 "$now \t[expr $bw4/$time]"
    puts $f5 "$now \t[expr $bw5/$time]"

    #Reset the bytes_ values on the traffic sinks
    for {set i 0} {$i < 20} {incr i} {
        $sinkVO($i) set bytes_ 0
        $sinkVI($i) set bytes_ 0
        $sinkBE($i) set bytes_ 0
    }

    #Re-schedule the procedure
    $ns at [expr $now+$time] "record"
}
```

Appendix C

Accompanying CDROM

The contents of the accompanying CD ROM are as follows:

- An electronic copy of this thesis document in PDF format.
- The LyX source files used for generating this document.
- The source code of the simulations used for the evaluation process.
- Relevant electronic material that were used during the research of this thesis.