JYVÄSKYLÄ STUDIES IN COMPUTING
80

Olli Alanen

Quality of Service for Triple Play Services in Heterogeneous Networks

JYVÄSKYLÄN YLIOPISTO

JYVÄSKYLÄ STUDIES IN COMPUTING 80

Olli Alanen

Quality of Service for Triple Play Services in Heterogeneous Networks

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi yliopiston Liikunnan salissa L304
marraskuun 21. päivänä 2007 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
in Auditorium L304, on November 21, 2007 at 12 o'clock noon.

UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2007

Quality of Service
for Triple Play Services
in Heterogeneous Networks

JYVÄSKYLÄ STUDIES IN COMPUTING 80

Olli Alanen

Quality of Service for Triple Play Services in Heterogeneous Networks

UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2007

Editors
Tommi Kärkkäinen
Department of Mathematical Information Technology, University of Jyväskylä
Irene Ylönen, Marja-Leena Tynkkynen
Publishing Unit, University Library of Jyväskylä

URN:ISBN:978951304-8
ISBN 978-951-39-3044-8 (PDF)

ISBN 978-951-39-2997-8 (nid.)
ISSN 1456-5390

Jyväskylä University Printing House, Jyväskylä 2007

ABSTRACT

Alanen, Olli
Quality of Service for Triple Play Services in Heterogeneous Networks
Jyväskylä: University of Jyväskylä, 2007, 88 p.(+included articles)
(Jyväskylä Studies in Computing
ISSN 1456-5390; 80)
ISBN 978-951-39-3044-8 (PDF), 978-951-39-2997-8 (nid.)
Finnish summary
Diss.

This thesis studies the Quality of Service issues of heterogeneous (wired and wireless) networks and services. Voice over IP and IPTV are the main applications whose requirements, problems and solutions are considered. In the first part of the thesis, the Quality of Service issues in IEEE 802.16 networks are studied. This part deals with the scheduling policy of the base station, contention resolution parameter optimization, multicast polling related issues and parameter based admission control policy. These issues are also studied and verified with the help of NS-2 simulator. In the second part of thesis, the admission control policies and mechanisms regarding multicast applications are studied. The proposed methods are verified in the NS-2 simulator and their applicability is tested in a real Linux router implementation. The thesis is based on the original publications in nine refereed conference proceedings and one journal article.

Keywords: Quality of Service, IPTV, VoIP, 802.16, WiMAX, Multicast, Admission Control

Author Olli Alanen
Department of Mathematical Information Technology
University of Jyväskylä
Finland

Supervisor Prof. Timo Hämäläinen
Department of Mathematical Information Technology
University of Jyväskylä
Finland

Reviewers Prof. Nikolay Sokolov
The Bonch-Bruevich Saint-Petersburg State
University of Telecommunications
Russia

Dr. Yevgeni Koucheryavy
Department of Information Technology
Tampere University of Technology
Finland

Opponent Prof. Gennady Yanovsky
The Bonch-Bruevich Saint-Petersburg State
University of Telecommunications
Russia

ACKNOWLEDGEMENTS

First of all, I wish to express my gratitude to my supervisor Professor Timo Hämäläinen for all the help and guidance throughout the post-graduate studies and the dissertation process. I would also like to thank Professor Nikolay Sokolov and Dr. Yevgeni Koucheryavy for the review of the manuscript and Professor Gennady Yanovsky for acting as an opponent.

I would like to thank all the co-authors who have participated in the research work of the articles included in this dissertation: Timo Hämäläinen, Jyrki Joutsensalo, Juha Karhula, Olli Karppinen, Mikko Ketola, Mikko Pääkkönen and Alexander Sayenko. This work would not have been completed without you. Special acknowledgements are given to Steve Legrand for performing the language review of the dissertation in the last phases of the work.

Acknowledgements are also given to the Department of Mathematical Information Technology of University of Jyväskylä and TeraBitti, PalHaLa, LaiLa, VizTool, and WIMALE projects for the financial support to make this research work possible. The premises of the telecommunication laboratory, provided by the department and the projects, have also been remarkably important.

Nokia Foundation, Jenny and Antti Wihuri Foundation, Ellen and Artturi Nyyssönen Foundation, Finnish Cultural Foundation and Ulla Tuominen Foundation also deserve thanks for the encouragement grants honoured for the dissertation work.

Last but not least, thanks for my parents, siblings and other relatives for their support and love during this work and my life. Johanna, thank you for giving me the time and support to do this "thing". The most special thanks belong to the most important persons of my life: Jesse "Chick Hicks" Alanen, Rasmus "Lightning McQueen" Alanen. You are the ones who make all the other things possible by balancing the life between the time at work and at home.

Jyväskylä November 8, 2007,
Olli Alanen

LIST OF FIGURES

LIST OF TABLES

CONTENTS

LIST OF INCLUDED ARTICLES

PI A. Sayenko, O. Alanen, T. Hämäläinen, and J. Karhula, Ensuring the QoS Requirements in 802.16 Scheduling, *Proceedings of the 9th ACM/IEEE International Symposium on Modelling, Analysis and Simulation of Wireless and Mobile Systems, pp. 108–117, October 2006*

PII A. Sayenko, O. Alanen, and T. Hämäläinen, Scheduling solution for the IEEE 802.16 base station, *to be published in Journal of Computer Networks*

PIII A. Sayenko, O. Alanen, and T. Hämäläinen, Adaptive Contention Resolution for VoIP Services in the IEEE 802.16 Networks, *Proceedings of the 8th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, June 2007.*

PIV A. Sayenko, O. Alanen, and T. Hämäläinen, On Contention Resolution Parameters for the IEEE 802.16 Base Station, *to be published in the Proceedings of the 50th IEEE Global Telecommunications Conference, November 2007.*

PV O. Alanen, Multicast Polling in the 802.16 Networks, *Proceedings of the 10th ACM/IEEE International Symposium on Modelling, Analysis and Simulation of Wireless and Mobile Systems, pp. 289–295, October 2007*

PVI O. Alanen, M. Pääkkönen, T. Hämäläinen, M. Ketola, and J. Joutsensalo, Multicast Admission Control in DiffServ Networks, *Proceedings of the 12th IEEE International Conference on Networks, volume 2, pp. 804–808, November 2004*

PVII O. Alanen, M. Pääkkönen, M. Ketola, T. Hämäläinen, and J. Joutsensalo, Measurement-Based Multicast Admission Control in DiffServ Networks, *Proceedings of the 7th International Conference on Advanced Communication Technology, volume 2, pp. 755–760, February 2005*

PVIII O. Alanen, M. Pääkkönen, M. Ketola,T. Hämäläinen, and J. Joutsensalo, An Enhanced Admission Control Solution for Multicasting in DiffServ, *Proceedings of the 1st Next Generation Networks, pp. 268–273, April 2005*

PIX O. Karppinen, O. Alanen, and T. Hämäläinen, Multicast Access Control Concept for xDSL Customers, *Proceedings of the 3rd IEEE Consumer Communications and Networking Conference, volume 1. pp. 448–452, January 2006*

PX A. Sayenko, O. Alanen, O. Karppinen, and T. Hämäläinen, Analysis and simulation of the signaling protocols for the DiffServ Framework, *Proceedings of 6th International Conference on Next Generation Teletraffic and Wired/Wireless Advanced Networking, Springer; LCNS 4003, pp. 566–579, May/June 2006*

Publication **PI** presents the first version of the Quality of Service scheduler for IEEE 802.16 network base station. The work was done in co-operation with the co-authors and the contribution of the author included the initial planning of the IEEE 802.16 extension for the NS-2 simulator, co-operative help in the design of the scheduler, the analysis of the results and background research on the other studies in the area. In Publication **PII**, a more advanced scheduler with some new features and more efficient functionality is presented together with new simulation scenarios. The contribution of the author is the same as that in the previous one.

In Publication **PIII** an adaptive framework for tuning the contention resolution parameters in 802.16 networks is presented. The idea was to change dynamically the backoff parameters and the size of the contention period, based on the requirements and the number of active subscriber stations. The author assisted with the design of the algorithm and with the analysis of the results.

In Publication **PIV** the tuning of adaptive contention resolution parameters is used with a VoIP application. The delay is considered more thoroughly in this article, and the contribution of the author is similar to that in the previous one.

In Publication **PV** the advantages of and guidelines on the usage of multicast polling in 802.16 networks are presented. The author was in charge of the design and implementation of the simulator, of the creation of the theoretical part and analysis of the results.

In Publications **PVI**, **PVII** and **PVIII** the guidelines for multicast receiver admission control are presented. Three different types of methods for the admission control decisions are also introduced. Both measurement based and parameter based methods are discussed. The author is the main contributor for each of these publications, having designed all the methods and having implemented the basic framework and the first method on the NS-2 simulator. The author is also the main person responsible for analyzing the results.

In **PIX** other facets of multicast admission control methods are studied. The restriction of multicast content to legitimate receivers only is implemented by integrating the network devices and network management software. The author is responsible on designing the integration and the experiments for this part of the research.

In **PX** different QoS signalling protocols used in DiffServ architecture are compared. The article presents the behavior of each protocol and also compares them in terms of the overhead produced. The contribution of the author in this research is in his role of supporting the main author in the analysis of the simulation results.

ACRONYMS

3G	3rd Generation
3GPP	3rd Generation Partnership Project
ACM	Association for Computing Machinery
ADC	Admission Control
AF	Assured Forwarding
AQM	Active Queue Management
ARQ	Automatic Repeat-reQuest
BB	Bandwidth Broker
BE	Best Effort
BS	Base Station
BPSK	Binary phase-shift keying
CATV	Cable Television
CBR	Constant Bit-Rate
CDMA	Code Division Multiple Access
CID	Connection Identification
COPS	Common Open Policy Service
CSMA	Carrier Sense Multiple Access
DAMA	Demand Assigned Multiple Access
DCD	Downlink Channel Descriptor
DiffServ	Differentiated Services
DL	Downlink
DL-MAP	Downlink Access Definition
DOCSIS	Data Over Cable Service Interface Specifications
DSL	Digital Subscribe Line
E2E	End-to-End
ertPS	Extended Real-time Polling Service
EF	Expedited Forwarding
FPS	Frames Per Second
FTP	File Transfer Protocol
GIST	General Internet Signalling Transport
GRIP	Gauge&Gate Reservation with Independent Probing
HDTV	High-Definition Television

IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IntServ	Integrated Services
IP	Internet Protocol
IPTV	Internet Protocol Television
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
LTE	Long Term Evolution
MAC	Medium Access Control
MBAC	Measurement Based Admission Control
MCS	Modulation and Coding Scheme
MPEG	Moving Picture Experts Group
NRS	Neglected Reserved Sub-tree
nrtPS	Non-real-time Polling Service
NS-2	Network Simulator 2
OFDM	Orthogonal Frequency Division Multiplexing
OFDMa	Orthogonal Frequency Division Multiple Access
PBAC	Parameter Based Admission Control
PDU	Protocol Data Unit
PHB	Per Hop Behavior
PHY	Physical layer
PIM	Protocol Independent Multicast
PMP	Point-to-Multipoint
QoS	Quality of Service
RFC	Request for Comments
rtPS	Real-time Polling Service
RSVP	Resource ReSerVation Protocol
RTP	Real-time Transport Protocol
SC	Single Carrier
SDU	Service Data Unit
SLA	Service Level Agreement
SS	Subscriber Station
TCP	Transmission Control Protocol

TDD	Time Division Duplexing
TLV	Type-length-value
UCD	Uplink Channel Descriptor
UDP	User Datagram Protocol
UGS	Unsolicited Grant Service
UL	Uplink
UL-MAP	Uplink Access Definition
VBR	Variable Bit-Rate
VoIP	Voice over IP
WCDMA	Wideband Code Division Multiple Access
WFQ	Weighted Fair Queuing
WiBro	Wireless Broadband
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
XORP	eXtensible Open Router Platform

1 INTRODUCTION

Networks have changed dramatically over the last few years. The driving force behind the change are the new network applications: real-time video and audio applications have a whole new set of requirements to the Internet and other networks that used to be best-effort based simple packet-switched networks. Another big challenge is the huge growth of wireless networks. Wireless networks are always more sensitive to disturbance and therefore more lossy and unreliable. Indeed, it is a challenging task to provide a guaranteed level of service for real-time applications in wireless networks.

The Quality-of-Service (QoS) experienced by the users or customers of the network services depends on several elements and entities on the network. It depends on all the networks and network technologies that a packet traverses during its path from the source to the destination. There is a huge research community concentrating on some of the pieces of the puzzle in order to solve the overall problem. This thesis also focuses on some of the important parts, which are included in the mission to guarantee the service level of new real-time applications like Internet Protocol Television (IPTV) and Voice-Over-Internet Protocol (VoIP).

1.1 Motivation and objectives

Triple play service is a concept that means delivering digital television broadcasts and a telephone and a broadband Internet access to people through a single broadband connection. It is currently a term that is well-known throughout the telecommunication world. All over the world, network operators are introducing their triple play services - in Asia alone there were 2.7 million IPTV subscribers at the end of 2006, which corresponds to an increase of 87.4% from the previous year [44]. Another research from Gartner estimates that, in 2011, 7.5% of North-American households will have IPTV [34]. Naturally the growth will continue. It seems like a reasonable assumption that, in the future only general IP-based wireless access network technologies like WiMAX will be used on the radio waves; on top of them television, radio channels, phone calls and all the other services can traverse inside IP packets.

The delivery of digital television to homes by the Internet (IPTV), however, is not a simple thing to accomplish. First of all, the video encoding must be efficient: for example, when using Moving Picture Experts Group 2 (MPEG2) encoding, one channel can take about 5 Mbit/s of the bandwidth. With a High-Definition Television (HDTV) broadcast MPEG4 must be used, and the bandwidth it uses up is considerable. This can, however, be solved by widening the bandwidth of access networks. Another solution already in use is the delivery mechanism used by IPTV: multicast. Multicast itself is quite an old method. It was introduced by the Internet Engineering Task Force (IETF) already in 1989 [29], but the QoS of multicast connections has not been studied to any great extent so far.

To make things even more complicated, it is not always possible to provide a wired internet access network like Digital Subscribe Line (DSL) or Cable Television (CATV) to the customers. This is often the case in sparsely populated areas, where it would be too expensive to set up wires. For triple play services, wireless access network technology must be used. The wireless access network must be able to provide a low and constant delay and also support the guaranteed bandwidth.

VoIP itself is one of the most difficult applications to handle for the network operator. It is one of the most delay critical network applications, because it is interactive and the users thus experience the problems immediately. VoIP calls have increase drastically, and each network technology should provide an adequate service level for the VoIP connections.

1.2 Problem statement

As described above, the QoS research area in general is challenging. It is important to solve all the small problems and subproblems, to be able to provide true end-to-end (E2E) QoS for heterogeneous applications and services. This thesis focuses on two particular problems in the area.

The first problem chosen for this research is related to a new wireless access network technology (WiMAX) standard 802.16 defined by the Institute of Electrical and Electronics Engineers (IEEE). The standard defines a promising technology that should be able to guarantee QoS for a wide range of network based applications. It does not however define all the details about the implementation of the QoS scheduling. Nor does it define the correct manners to set up all the parameters to be used by all the extra features. The research community has only started to evaluate the features of the 802.16 specification, and some exact methods and simulation studies have been published. These do not however provide complete solutions or evaluations for the area, and therefore, these issues are studied in Chapter 2.

The second problem chosen for this research is the absence of standard admission control policies for multicast traffic. The difference with unicast methods and the concomitant problems should be studied. IETF has published an RFC [11] that deals with the problems combining DiffServ and multicast, and the document in question describes the problems and solutions well. Another solution [73] provides a different kind of framework. Both of these methods, however, leave the definition of actual admission control methodology open. Therefore, this problem is tackled in Chapter 3.

1.3 Research methodology

The research described in this thesis is based on the analytical results from various equations and algorithms presented. Each of the equations and algorithms is then evaluated with a simulation and a deep analysis on the simulation results.

The main research tool employed in these studies has been a network simulator NS-2 that is widely used by the research community. The simulator has been extended with many new features and protocols to study their peculiarities. The network simulator has been the only possible tool in most of the cases, since the new methods proposed in this thesis can not be implemented to real network devices like 802.16 base stations or IP routers.

Some experiments have also been done with Linux-based router implementations. However, inefficiencies in Linux routers and the absence of sufficiently big laboratory network can cause problems in real life experiments. Some of the methods proposed will be investigated with real equipment, when applicable, in further studies.

1.4 Outline of the dissertation

Chapter 2 provides an overview of most of the mechanisms that the IEEE 802.16 technology provides to guarantee QoS for wireless connections. Several studies on the optimal parameters and implementations of open parts of the specification are then presented there. All the proposed methods and parameter optimizations are then evaluated with simulations.

Chapter 3 describes the problems of providing QoS for multicast connections in current QoS architectures. One of the problems, multicast admission control policies in DiffServ architecture, is then tackled by proposing several admission control methods. All of the methods are evaluated with simulation scenarios.

Finally, Chapter 4 concludes this thesis and points out the important results of the thesis. Some of the author’s future research topics are also presented.

2 QUALITY OF SERVICE ON IEEE 802.16 MAC LAYER

In the recent years, wireless network technologies have become more and more popular. The reasons for this include, among the other things, the ease of use and faster and cheaper construction of infrastructure. Wireless hotspots can be found almost anywhere, and all the new laptop computers have a wireless network adapter that can be used to connect to the Internet. Because of its short range, WLAN network is not always suitable. They can never replace the broadband connections to homes, since their maximum range is only a few hundreds of meters. On the other hand, there is an obvious need for this kind of wireless broadband connection and several suggestions regarding the technology standards have been made.

3GPP is trying to convince the industry that Wideband Code Division Multiple Access (WCDMA) based 3rd generation (3G) mobile network technology and its successor Long Term Evolution (LTE), should be used, even though the latter is mainly targeted for mobile phones and other mobile devices. The advantage of LTE is that it can be built on top of the current 3G network. The disadvantage is that the specification is not yet ready, and it will take years before the specification can be employed.

Another broadband wireless network technology has been developed by a company called Flarion, later merged to QualComm. That technology is called Flash-OFDM and provides mobile broadband connections for high speeds and large cell sizes. The technology however is not open, which might slow down its development. In Finland Digita is currently using it. The advantage of the technology is that it operates in lower frequencies at around 450Mhz, which makes it easier to handle bigger cell sizes.

WiMAX is a wireless broadband access network technology. WiMAX Forum is the body responsible for the certification of WiMAX compatible devices. IEEE and its 802.16 working group on their behalf have defined the IEEE 802.16 standard, which is the actual specification of the technolgy. In 2004 the first official standard [42] for fixed subscriber stations was finalized and, shortly after, the e-specification [43] extended it to support mobile users as well. IEEE 802.16 is the best positioned against its main competitors, since it is a public standard and has a few years head start against, for example, LTE. Also, there are already several 802.16 networks in different parts of the world and more are currently under construction.

802.16 is a very promising technology, also in regard to QoS, since it can provide QoS guarantees on the MAC layer, which is not possible in WLAN for example. Even though the 802.11e extension to the WLAN standard does provide priority based QoS to the subscriber stations, strict QoS guarantees can not be always obeyed. The actual QoS experienced by the users is always dependent on the physical layer (PHY), and, especially on wireless links, the nature of the PHY is unreliable. Still, 802.16 provides currently the best means to achieve the necessary level of service when there is enough capacity on the physical layer.

Another broadband wireless technology, WiBro was implemented in South Korea to build a wireless broadband network while the standardization of 802.16 was still unfinished. The WiBro will most probably be compatible with the WiMAX certification in the near future. Still, there is a widely accepted fact that WiBro can not survive as a global technology and that IEEE 802.16 will win this battle.

In this chapter, the functionality of the 802.16 MAC layer QoS is first described in Section 2.1. Then in Section 2.2 the previous studies in the area are discussed. In Section 2.3 our propositions and solutions on how to use the features of the MAC layer are presented. These propositions are then tested with simulations in Section 2.4. Finally, with Section 2.5 the chapter is concluded and some future studies are presented.

2.1 IEEE 802.16 QoS - MAC layer mechanisms

The Quality of Service experienced by the users depends on all the protocol layers used by the application. For example, in case of VoIP the codec used is the first component affecting a call. Usually data are packed to UDP and IP packets. The IP layer might use some QoS architecture, such as IntServ or DiffServ, which can impact on delay, throughput and packet losses. On 802.16 networks IP packets are then handed to the 802.16 MAC layer, where the packets are treated based on the QoS guarantees given for the connection. The MAC layer hands the MAC PDU to the PHY layer that is responsible for delivering the packet to the other end of the wireless channel. Some errors, retransmissions or even complete loss of signals might occur in the process.

Each layer, from the application to the aPHY, makes a difference on transferring the packet. This chapter of the thesis deals only with the possibilities and features of a 802.16 MAC layer that supports QoS. This particular layer has not yet been studied extensively and forms therefore a reasonably interesting research area.

The QoS architecture of IEEE 802.16 is based on the fact that 802.16 is a connection oriented network technology, in which each subscriber station (SS) must create a connection to a base station (BS) and associate it with a certain

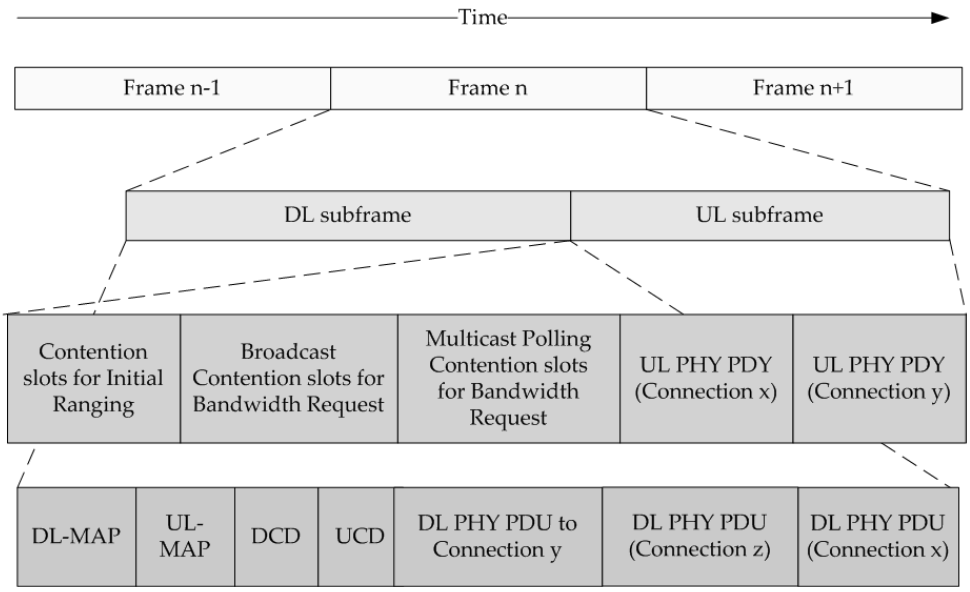


FIGURE 1 A simplified frame structure of 802.16

service class, before sending or receiving any data. The service classes define the QoS level for the connections. Another important principle is that the 802.16 base station schedules the uplink transmissions of SSs in Demand Assigned Multiple Access (DAMA) mode, in which the BS controls the SSs turns to send data. This makes it possible to avoid collisions when necessary.

It is also possible to use 802.16 in a Mesh mode, where subscriber stations can also send data directly to each other (ad-hoc), but this thesis focuses only on the Point-to-Multipoint (PMP) mode. It is anticipated that the QoS will be much more important in the PMP mode, since it is the mode that is used in all the current implementations.

A simplified frame structure of IEEE 802.16 in time division duplexing (TDD) mode is presented in Figure 1. The time domain is divided into frames, which are further divided into the uplink (UL) and the downlink (DL) parts. Furthermore, both the UL and DL subframes are divided between the SSs and for some special purposes. These special purposes include broadcast, multicast and initial ranging contention slots. Management messages Uplink Channel Descriptor (`UCD`), Downlink Channel Descriptor (`DCD`), Downlink Access Definition (`DL-MAP`) and Uplink Access Definition (`UL-MAP`) define the channel allocation between the subscriber stations in both uplink and downlink directions. In addition to the bursts shown in the figure, other periods, for example synchronization, exist in the frames. These additional periods depend on and vary between the different PHY layers (SC, SCa, OFDM and OFDMa).

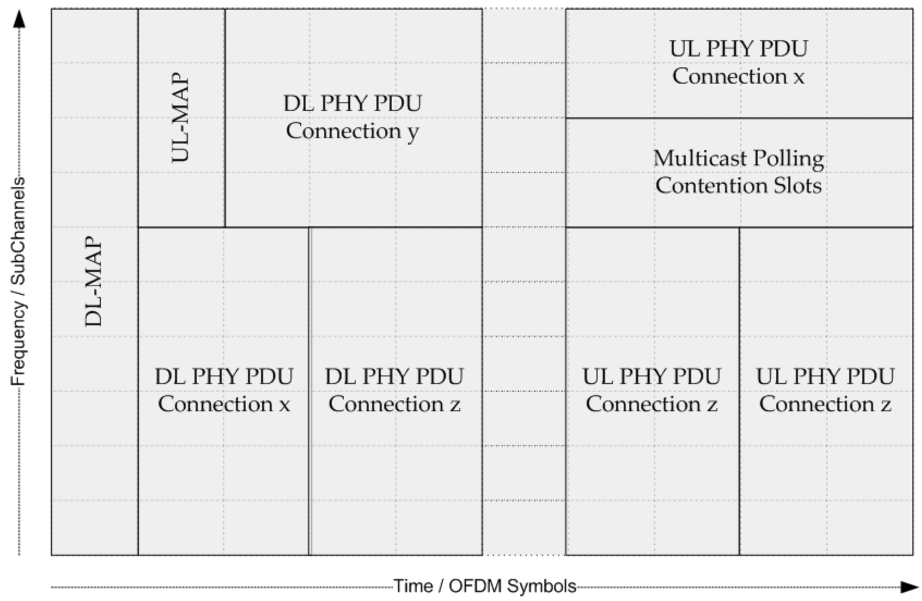


FIGURE 2 An example of OFDMa PHY frame

2.1.1 Scheduling and grants

The most important part of a 802.16 base station, as far as the QoS is concerned, is probably the scheduler of the base station. It is the responsibility of the scheduler to decide how many time slots does each of the connections (both downlink and uplink) get on each frame. The base station then informs with the UL-MAP and DL-MAP messages that explicitly define the slot allocations, the SSs about this order. To make this decision, the scheduler should take into account the QoS parameters (such as bandwidth, packet loss, delay, and jitter), sizes of the downlink queues and the sizes of the bandwidth requests sent by the SSs currently requesting uplink bandwidth. The specification however does not define how this scheduler should be implemented and how it should work. It only states the requirements for it.

The uplink slots allocated for SSs are also referred to as grants. Each grant consists of one or multiple PHY bursts, each of which again consists of one or more slots. The PHY layer defines the structure of the bursts. Depending on the PHY, these can be either consecutive time intervals on the same frequency channel or blocks that span through both time and frequency domains. An example of mapping of MAC PDUs to the OFDMa physical layer frame is shown in Figure 2. When this physical layer is used, the frequency is first divided to subchannels which consist of several subcarriers. The time axis on the other hand, is divided into OFDM symbols. In this case, the MAC layer scheduling decisions must be mapped to the physical layer by allocating rectangular blocks from the frequency-time plane.

The uplink grants are allocated to the basic connections rather than to the actual transport connections. Therefore the subscriber stations also need to implement an uplink scheduler. It is the responsibility of the scheduler to decide how the uplink grants are then divided between the connections with data to send. This research focuses on the scheduler of the base station, since it is expected to be the more important, at least when laptop computers or mobile phones are used as subscriber stations. When using, for example, WiMAX-WLAN routers, the uplink scheduler of the SS will, however, become more important. It is worth mentioning that even though this thesis does not directly concern the SS uplink scheduler, the same equations and implementation principles that are used with the BS scheduler can be applied to SSs.

2.1.2 Service classes

Five service classes are defined in the IEEE 802.16 specification to satisfy the demands of different kinds of applications. During the establishment, each connection is associated with one of the service classes. The parameters of the service class can be modified during the connection but if the type of the service class needs to be changed, a new connection must be established.

The original IEEE 802.16 specification [42] defines four service classes. The service classes are Unsolicited Grant Service (UGS), Real-time Polling Service (rtPS), Non-real-time Polling Service (nrtPS) and Best Effort (BE). The 802.16e standard presents one new service class called Extended Real-time Polling Service (ertPS).

UGS is designed to support guaranteed constant bit-rate flow to fixed-size packets. VoIP without silence suppression or a leased line are examples of applications that shall use the service class. The scheduler of the base station always provides the appropriate amount of uplink bandwidth for UGS connections, even if these have nothing to send. The maximum latency and the variance of the delay (*jitter*) values are also associated with each UGS service flow. The scheduler must also guarantee the provision of the agreed amount of DL resources, when there are packets in the DL queue.

rtPS service class offers support for real-time service flows with variable bit-rate and packet size. Streaming video or variable bit-rate audio codec are the example applications for this class. The QoS parameters for the service class are: Minimum Reserved Traffic Rate, Maximum Sustained Traffic Rate and Maximum Latency. Contention is prohibited for rtPS connections, so unicast polling is the only bandwidth request mechanism allowed.

ertPS was added to the specification in the 802.16e extension. It was suggested and analyzed in [57], [36] and [58]. Its main purpose is to support VoIP applications that use silence suppression. The basic idea is to allocate a constant number of slots while the application is on its active phase. This number is by default indicated with the Maximum Sustained Traffic Rate parameter. When the application does not send anything, the SS needs to send a bandwidth request with a request size of zero. After that it is not allocated with slots any more. During the silent phases the base station can either allocate periodic polling slots or

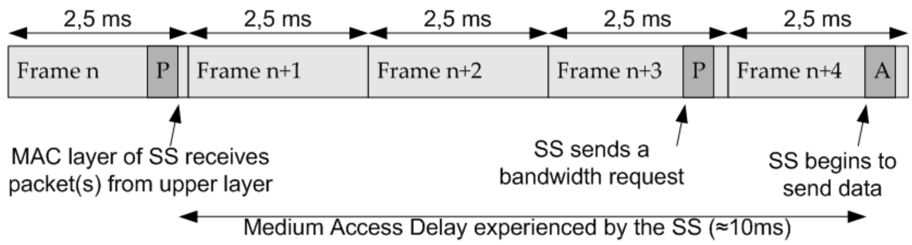


FIGURE 3 802.16 polling mechanism

if it does not, the subscriber station must participate on the contention when it wants to start sending again.

nrtPS service class is designed for non-real-time applications that need some guarantees on the bit-rate, but do not have critical delay limits. It provides periodic polling, but also allows the use of the contention resolution process and Minimum Reserved Traffic Rate. It must be guaranteed that while the connection is requesting bandwidth it is allocated at least slots to satisfy the minimum requirement.

BE is regarded as the worst service class for 802.16 networks. There are no guarantees of service for connections of this class and polling is not allowed. We anticipate that most of the regular user connections will be of the best effort type and therefore it is important to study also the behavior of BE connections using simulation, even though it is not very sophisticated from QoS perspective.

2.1.3 Polling

Polling is a term and a method that is used to provide the connections a guaranteed possibility to request for uplink bandwidth. Most of the service classes do not have a constant uplink bandwidth allocated for them, and therefore a method to request it is necessary. In polling, some slots are allocated for the SSs, even when they do not have anything to send. This allocation can be used to request for bandwidth when needed. The polling interval P_I of the connection defines the interval between the consecutive polling slots allocated for an SS. It can be set to anywhere between 2.5ms and several seconds or minutes. Setting of it has a direct impact on the *medium access delay*, which equals the time that SS has to wait from the moment of time when it has something to send to the time it can start to send data.

An example of polling, polling interval and the medium access delay is illustrated in Figure 3. In that example FPS of 400 is used, and a polling interval of 7.5 ms is used for the SS. This produces a polling slot to be allocated on every 3rd frame. The example presents the worst case polling delay D_{max} for the SS. Equation 1 can be used to calculate the correct polling interval P_I based on the QoS requirements for the rtPS or ertPS connections:

$$P_I = D_{max} - \frac{1s}{FPS}. \tag{1}$$

The value for D_{max} is the maximum tolerated delay in the QoS requirements for the connection.

The polling method also has some drawbacks. Some of the resources are reserved to the SSs even when these do not have anything to send. This naturally wastes some of the network capacity and prevents the best possible utilization. A maximum waste of bandwidth takes place when the connection does not send anything for a long period while being polled. The percentage of the slots used for the polling and thereafter wasted, can be calculated as follows:

$$P_{overhead} = \frac{1}{P_I \cdot USPF \cdot FPS}. \tag{2}$$

where $USPF$ is the slots per frame for user data and FPS is the frames per second in use. Supposing that 151 is the slots per frame for user connection in the example above, the overhead caused by polling is

$$P_{overhead} = \frac{1}{P_I \cdot USPF \cdot FPS} = \frac{1}{0.0075s \cdot 151\frac{slots}{frame} \cdot 400\frac{frames}{s}} = 0.22\%. \tag{3}$$

The parameters of the example are realistic, and result from static UL/DL relation and FPS value of 400. In this case the overhead caused by the polling would be 0,22% of the total link capacity. That is quite a lot since it is the polling overhead of only one SS, and there could be several polled SSs in the network. Therefore it is not optimal to apply polling to all the connections but only to the most important and delay critical ones. Long polling intervals naturally do not cause that much overhead, but they do not results with good medium access delays either. Therefore, for most of the connections, contention resolution mechanism, described in the next subsection should be used.

2.1.4 Contention resolution

The contention resolution process in 802.16 is the period of time during which subscriber stations can compete for the bandwidth. The process is carried out during contention periods, and three different kinds of contention periods exist: initial ranging period, broadcast request transmission period and multicast polling period. The initial ranging period is used by new subscriber stations willing to enter the network. Both the broadcast request transmission period and the multicast polling period behave in a similar fashion to provide an opportunity for SSs to request for uplink transmission possibilities when they do not have any and when they are not polled individually. Polling is always the most reliable way to request for bandwidth, but it also involves extra utilization, since SSs do not always use the slots allocated for polling. The drawback of the contention resolution process is that a collision might take place causing both of the requests to disappear.

The contention periods are divided into transmission opportunities based on the size of the particular request message, the properties of the PHY layer and

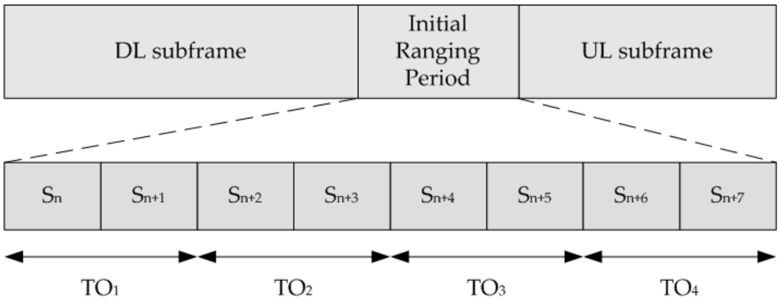


FIGURE 4 An example of request contention period and transmission opportunities

the Modulation and Coding Scheme (MCS) used. An example of a contention period for request transmissions is provided in Figure 4. In this example OFDM PHY and BPSK-1/2 MCS scheme are used resulting in a slot size of 12 bytes and in the size of the request message of 24 bytes. Therefore each transmission opportunity (*TO*) has the size of 2 slots. If, in this case, the base station decides to allocate four initial ranging transmission opportunities for the frame, it needs to allocate 8 slots from S_n to S_{n+7}.

The other parameters that control the usage of contention resolution are backoff start (BO_s) and backoff end (BO_e). These parameters are announced in the UCD management message and may have a value from 0 to 15. When an SS is willing to participate in the contention, it sets its internal backoff window (W) value to 2^{BO_s}. Then SS chooses randomly a value between $[0, W]$ and waits for that number of transmission opportunities (*TO*) before sending its request. These waited transmission opportunities may exist in the current frame or they might also span multiple frames. After sending the request, SS waits for an allocation. If it does not receive an allocation during the specified time interval (`T16`), it increases its internal backoff window to $2 \cdot W$ and repeats the process described before. SS continues the process until $W = 2^{BO_e}$ if it does not receive an allocation. After that the corresponding MAC PDU is dropped.

A base station can adjust BO_s and BO_e values for the desired performance. It can, for example, set the values equal for speeding up the process and for providing smaller access delays. This will naturally result in a larger loss of PDUs. On the other hand it can, for example, set $BO_s = 0$ and $BO_e = 15$, which would result in a minimal amount of packet drops but would create much larger access delays. An example of a contention process is depicted in Figure 5. In this example, there are four subscriber stations participating in the contention, each entering the process on frame n. The backoff start in this example is set to 0 and the backoff end is 2. In the nth frame, each of the SSs have their internal window value equal to 1, so all the requests are sent during the same transmission opportunity and, therefore, all of them are lost. In the frame number n+1, SSs randomly choose TO between one and two, and here SS2 succeeds to transmit the request. In the n+2 frame, SS1 succeeds but SS3 and SS4 are again in a collision. Since backoff window has now reached its maximum value, SS3 and SS4 are obligated

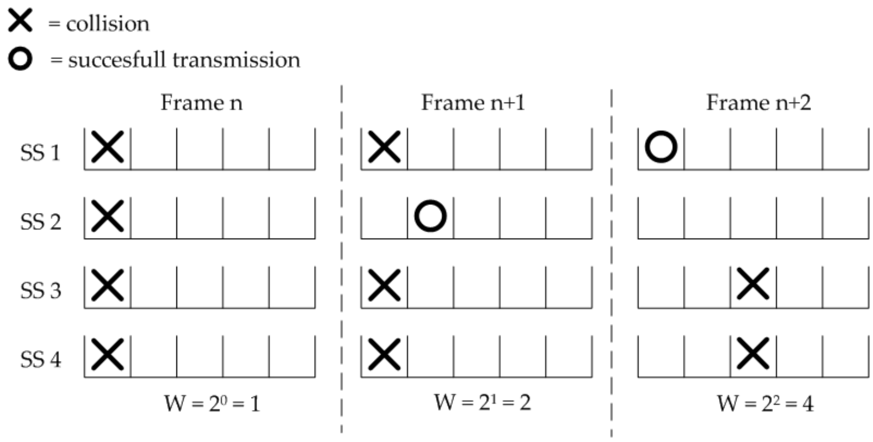


FIGURE 5 An example of contention resolution process

to drop their PDUs. If there are other PDUs waiting in their queues, they can and will start the contention resolution process from the beginning.

2.1.5 Multicast polling

Multicast polling is one of the mechanisms defined by 802.16 standard. It achieves a better or guaranteed quality of service with less overhead when compared to the polling approach. When it is used, a group of SSs is added to a multicast polling group and the slots are assigned to allow these SSs to participate in the contention resolution process during these slots. This way, the probability of collisions during the contention period and the medium access delay are both decreased. Multicast polling was introduced to achieve a tradeoff between a regular contention resolution and unicast polling.

Each SS may belong to one or zero polling groups and the memberships are managed dynamically. Two management messages: Multicast Assignment Request (`MCA-REQ`) and Multicast Assignment Response (`MCA-RSP`) are used to assign and unassign SSs to and from the polling groups. The base station always decides about membership dynamics by sending `MCA-REQ`s, and the SSs reply to changes with a later message. The specification does not clearly define whether the SSs can participate in the broadcast contention while being assigned to a multicast group. We anticipate that the SSs should not participate: this would significantly simplify the calculation of the backoff parameters and also provide means to guarantee QoS in a more reliable manner.

The specification states that multicast polling can be used to poll SSs whenever there is insufficient bandwidth for unicast polling. The specification also states that multicast polling is only allowed to be used with nrtPS, ertPS and BE connections. Since no guarantees are given to BE connections, we expect that the multicast polling should only be used with ertPS and nrtPS connections. Even in the case of nrtPS connections, it is not clear, whether the multicast polling can provide a better Quality of Service, since the nrtPS connections do not have any delay requirements.

However, there are two disadvantages with the multicast polling approach when compared to the broadcast contention resolution. The first one of these is the overhead involved with UL-MAP message, which is caused by the necessity to have a separate information element for each multicast polling group on each UL-MAP message. Each polling group increases the size of the UL-MAP message by 6 bytes (in the OFDM physical layer). Since the UL-MAP is sent with the BPSK-1/2 modulation (12 bytes / slot), adding 3 polling groups increases the overhead by 2 slots. Depending on the used frames per second parameter, three groups would then create an overhead of 0.3 - 3 percent. Therefore, a careful consideration should be given on how many polling groups are used.

The second problem is that there are no separate backoff parameters defined for broadcast contention and multicast polling groups. In practice this means that the multicast polling group members should use the same backoff parameters as the broadcast group members do, as defined in the UCD management messages. If the polling slots of the broadcast and the multicast groups could be scheduled to separate frames, the problem would not arise, but in practice this is not always possible. This problem is also tackled in the latter part of this thesis.

2.2 Other research on IEEE 802.16 QoS

Since 802.16 is quite a new network technology, the research done in the area is also very young. The first research articles about the issues concerning the Quality of Service on the 802.16 MAC layer have been published in 2002 and most of the papers published have appeared after the year 2004. The ones addressing the area that is studied in this thesis, are briefly covered in the following subsections.

2.2.1 802.16 scheduling

As explained in the previous sections, one of the most important unsolved and unstandardized issues on providing QoS guarantees in 802.16 networks is the implementation of the BS scheduler. Although there have been several suggestions for the implementation and architecture of scheduling, our proposal differs from them significantly.

Some of the schedulers suggested previously do not take into account all the service classes and are, therefore, imperfect. Some of them can handle each class, but are way too complex. It must be taken into account that the scheduling decisions must be made for each frame: while the frames per second value can be up to 400, there is not much time for making these decisions. There are also many articles that describe a method to provide guarantees with a very high probability and might provide the desired behavior for some cases but not all. Certain applications do have very strict delay and bandwidth limits that can not be guaranteed with these solutions, even though they might result with the best utilization. This kind of measurement based scheduling is certainly an alternative to a scheduling based on strict parameters, but we consider the hard QoS guarantees to be more important than a slightly more efficient resource utilization.

Most of the publications also quote simulation results produced in a MatLab or a similar general purpose simulator that does not take into account all the details of the 802.16 protocols. All the previous work in the area will now be described briefly.

Article [39] is the first publication made on the subject of the MAC QoS issues in WiMAX. The standard was not yet in place at the time of its writing, but as the QoS standard is based on the Data Over Cable Service Interface Specifications (DOCSIS) the efficiency of WiMAX could be evaluated. The proposed scheduler is WFQ based, but there are no simulation results in the paper.

In [62] a hierarchical scheduler with multiple WFQ based schedulers is presented. The article focuses on delays experienced by connections in different service classes, and, therefore, it is impossible to tell whether this scheduler can guarantee bandwidth.

Article [50] also presents a WFQ based method, but it is mostly about admission control. The article does not describe the scheduler with enough details and the applicability of it cannot therefore be estimated. The traffic is estimated with the token bucket model, which is not the one used in the 802.16 specification.

In [83] a complete scheduling solution is presented and the model is based on a hierarchical scheduler. The implementation however is very complex, and the article lacks proper simulation results.

Each of the articles [23], [25] and [2] presents a scheduling framework rather than a detailed algorithm. Therefore they cannot be considered as complete solutions for 802.16 base stations. In [2] only BE connections are considered.

In [28], a completely different kind of approach is used: the article suggests a modification to the 802.16 standard to use variable size frames instead of static ones. The suggestion runs counter to the fundamental ideas of 802.16 and cannot be considered realistic at this stage.

Publications [21] and [48] discuss higher layer issues about providing QoS to the subscriber stations. These articles discuss the integration of a 802.16 base station with a DiffServ and IntServ based core network.

Articles [65] and [64] present a good stochastic approach, and the authors also present good analytical results on the scheduling method. The work, however, lacks proper simulation results from a network simulator. The traffic is also estimated with the Poisson process, and the scheduler does not provide strict guarantees for traffic.

In [80] the authors present a scheduling solution based on Packet Based Round Robin that provides a good efficiency between a large number of BE connections. The solution does not however take properly into account other than the UGS and the BE service classes.

In [82] a simple yet working solution for a simple scheduler is presented. The analytical results are impressive, but no simulation results are presented.

Article [22] presents probably the best solution for the scheduler of 802.16 base stations. All the service classes are handled properly with a WFQ and DRR based hierarchical scheduler. The negative aspects of the solution are its complexity and the lack of good simulation results.

In [85] a quite complex and memory consuming scheduler is presented. Again simulations are not complete since MatLab was used.

Thus none of the previous suggestions presents a complete scheduling policy with strict QoS guarantees while showing its applicability with a proper network simulator. Our research aims to provide an adequate solution to satisfy this requirement and prove it with good simulation results using a simulation framework NS-2.

2.2.2 Contention resolution process

The contention resolution process defined in the 802.16 standard is based on the exponential backoff algorithm. The same algorithm, under research for the last few years [53], is used in 802.11 networks. WLAN networks differ from the 802.16 ones, however in that in the WLAN networks Carrier Sense Multiple Access (CSMA) mode is used, and an SS must participate in the contention resolution process with each and every packet it sends. In the 802.16 networks, subscriber stations participate in the contention only when they start sending something. Afterwards they can request for more bandwidth by using the capacity they were allocated. Other important difference is that in CSMA the subscriber stations can also sense the collisions, which is not the case with 802.16.

As described earlier, it is possible to use two distinct methods in contention resolution. The first one is the CDMA based contention that can be used with OFDM and OFDMa physical layers. It is quite similar to the one that is used in 3G CDMA networks and the research done in that area is therefore quite well known. At least article [70] has studied these issues.

Another contention mechanism is the regular one that can be used with any of the physical layers. There has also been some research done on that area. In [66], [39], [23] and [87] only the size of the contention period was studied, not the backoff parameters. The results were good but incomplete. In [6] only the effect of backoff start is studied.

In [52] an adaptive framework is presented. Connections utilizing nrtPS service class are polled individually when there are free resources, otherwise they participate in the contention. This may prove useful, but it does not solve the problem when the resources are utilized a lot.

In [40] an analytical model for the contention process is presented. The article also presents analytical results for bandwidth efficiency with some parameters.

None of these studies however tackle with the problem of choosing all the contention parameters dynamically and adaptively based on the state of the network. We think that all of these parameters have such a big mutual impact that they cannot be studied separately.

2.2.3 802.16 multicast polling

Multicast polling is a feature that has not been used in previous wireless network standards, and has not been mandated by the WiMAX Forums profile either. Therefore, as a research area, it is new. To the author's knowledge there are only two research groups that have tackled the area and published their results. In [20] and [24] Chang et al. propose a new service class (QrtPS) and a scheme where polling is dynamically switched between the multicast and the unicast mode. Even though impressive numerical results are presented, the work lacks appropriate simulation results.

In [61] the performance of broadcast and multicast polling methods are compared. The analytical model and the simulation results are used to show the efficiency of both methods with different parameters. The efficiency was measured as the utilization of the transmission opportunities, which indeed is an important factor, but not the only one. Currently there are no research articles published about the medium access delay and network utilization efficiency when using multicast polling for some of the connections.

There are also no research articles on how the multicast polling feature should be used and what are the optimal parameters for it. It is obvious that better QoS can be provided by employing that feature.

2.2.4 Others

The admission control methods in 802.16 networks can be divided into certain categories, based on their motivation and fundamentals. In [50] a token bucket based admission control method is presented. The Poisson arrival rate and token bucket rated traffic is assumed, which does not correspond to the specification. Both [22] and [82] present a nice admission control algorithm to be used in conjunction with the schedulers presented in the articles. The incompleteness of the schedulers does not however give the best starting point for the admission control modules.

It is anticipated that the admission control module should work with the same principles as the QoS scheduler: therefore, we will define our own module to support our policy in the most convincing manner.

There are also several other studies and articles in the area of 802.16 QoS. Some of the studies concentrate on the physical layer of 802.16 and some on the features of the MAC layer that are not considered in this thesis. The author of this thesis has also participated in research on active queue management (AQM) in article [55] and on Automatic Repeat-reQuest (ARQ) mechanism in article [69].

2.3 Proposed solutions for QoS in 802.16

Since the 802.16 standard and the 802.16e extension do not define all the functionalities and parameter values needed to support QoS guarantees, we propose several implementations and policies for this. This section presents novel ideas and concrete methods that could be used to achieve a better QoS. The section is based on Publications **PI**, **PII**, **PIII**, **PIV** and **PV** and their results. Some new and yet unpublished studies and their results about admission control and call dropping are also presented.

2.3.1 Scheduling solution

Since the IEEE 802.16 specification does not define how the scheduler of the base station should behave and be implemented, we propose a scheduler in which these matters have been taken into consideration. The scheduling solution with more details is proposed in Publications **PI** and **PII**.

The scheduling solution aims to guarantee the bandwidth requirements in a pure parameter based fashion, not trusting on any stochastic probabilities. There are some advantages in using probabilistic or measurement based scheduling algorithms, but the parameter based approach is the only one that can actually guarantee a service level. Another base for the algorithm is trust in the physical layer. This means that errors and their handling with Forward Error Correction (FEC), Automatic Repeat-request (ARQ) or Hybrid Automatic Repeat-request (HARQ) were not included with the responsibility of the scheduler. FEC and HARQ are invisible for the MAC layer and ARQ was left out for further studies. Some basic guidelines on how to use ARQ are studied in [69] and [68].

The scheduling algorithm is divided into two phases. In the first phase, a minimum number of slots is allocated for each subscriber station and in the second phase, the unallocated *free* slots are allocated between the SSs. The first phase is presumed to be successful in every case. It is the responsibility of the admission control module to take care of it. The admission control model is explained later in Section 2.3.4. The allocation of the minimum number of slots concerns all the connections, except those that are of the BE type.

The purpose of the second phase is to allocate the slots still available after allocating slots for the minimum requirements. In this phase the scheduler has to take into account the maximum bandwidth requirement and bandwidth request size, if they exist. The calculations of both the minimum and maximum number of slots for connections, based on the QoS requirements, are described next.

The following equations can be used to calculate the number of slots that should be allocated to guarantee both the minimum and maximum bandwidth requirements. At first, equations 4 and 5 are used. N_i is the number of slots required by the connection i to satisfy the bandwidth requirement B_i. S_i stands for the slot size of the connection i. As described before, the slot size depends on the PHY layer used and on the MCS scheme resulting in different slot sizes for connections within a frame:

$$N_i = \begin{cases} \dfrac{B_i}{S_i\text{FPS}}, & \frac{B_i}{S_i\text{FPS}} \mod 1 = 0, & \text{(4a)} \\ \left\lfloor \dfrac{B_i}{S_i\text{FPS}} \right\rfloor + \begin{cases} 0, & FC \mod M \neq 0, \\ 1, & FC \mod M = 0, \end{cases} & & \text{(4b)} \end{cases}$$

where

$$M = \left\lfloor \frac{1}{\frac{B_i}{S_i\text{FPS}} - \left\lfloor \frac{B_i}{S_i\text{FPS}} \right\rfloor} \right\rfloor . \tag{5}$$

The 4a form of the equation is used in situations where an integer number of slots can satisfy the requirements of the connection. The 4b form is used when this is not the case. The FC variable stands for a frame counter. It is an integer counter that is increased on every frame. This form of the equation compensates the rounding error caused by a constant slot size.

To take into account the bandwidth request messages utilized by all the service classes except the UGS, the following equation can be used:

$$N_i = \left\lceil \frac{R_i}{S_i} \right\rceil . \tag{6}$$

In this equation, R_i stands for the request size which corresponds to the uplink queue size of the connection in the SS. N_i stands for the number of slots required to satisfy this request and S_i.

Each of the service classes also have their peculiarities, based on their QoS parameters and other behaviors. These issues are considered in the following equations.

In the following equations, C_i denotes the service class of i:th conntection. For the UGS connections, the minimum and maximum bandwidth requirements are the same, and a fixed number of slots, based on this limit should be allocated. For them, Equation 7 is used and works in the same manner as Equation 4:

$$N_i^{min} = N_i^{max} = N(B_i^{max}, S_i), \forall \mid C_i = \text{UGS}. \tag{7}$$

For the connections utilizing the rtPS service class, Equation 8 is used. In rtPS connections, at least one slot is always allocated for polling and, if the connection is requesting for bandwidth ($R_i > 0$), the minimum and maximum number of slots are calculated based on the request:

$$N_i^{min} = \begin{cases} 1, & R_i = 0, & \text{(8a)} \\ N(B_i^{min}, S_i), & R_i > 0, & \text{(8b)} \end{cases}$$

$$N_i^{max} = \min \{ N(B_i^{max}, S_i), R(R_i, S_i) \}, \quad \forall i \mid C_i = \text{rtPS}. \tag{8c}$$

For ertPS connections with polling, one slot is allocated for polling when the connection is not requesting for bandwidth. Otherwise the minimum and maximum number of allocated slots are set to equal, according to the QoS profile:

$$N_i^{min} = N_i^{max} = \begin{cases} 1, & R_i = 0, \quad (9a) \\ N(B_i^{max}, S_i), & R_i > 0, \quad (9b) \end{cases}$$

$$\forall i \mid C_i = \text{ertPS}.$$

In a special case where ertPS without polling is used, the polling slots are not allocated and the number of slots in Equation 9a is 0.

NrtPS is almost identical with the rtPS except that polling is not allowed for it. It results with zero reservation when bandwidth request size equals zero as shown in the following equation:

$$N_i^{min} = \begin{cases} 0, & R_i = 0, \quad (10a) \\ \min\left\{N(B_i^{min}, S_i), R(R_i, S_i)\right\}, & R_i > 0, \quad (10b) \end{cases}$$

$$N_i^{max} = \min\left\{N(B_i^{max}, S_i), R(R_i, S_i)\right\}, \quad (10c)$$
$$\forall i \mid C_i = \text{nrtPS}.$$

BE connections always have a minimum number of slots set to zero. The maximum is then similar to that of nrtPS:

$$N_i^{min} = 0, \quad (11a)$$
$$N_i^{max} = \min\left\{N(B_i^{max}, S_i), R(R_i, S_i)\right\}, \quad (11b)$$
$$\forall i \mid C_i = \text{BE}.$$

A special kind of scheduling is needed for management connections since these do not belong to any service class. We anticipate that the following equation can be used for them:

$$N_i^{min} = N_i^{max} = R(R_i, S_i), \quad (12)$$
$$\forall i \mid C_i = \text{MGMT}.$$

After all the connections have been allotted the number of slots to satisfy their minimum requirements, it is time to move to the phase two. In this phase, maximum requirements based on the previous equations are used if there are enough free slots to do that for every connection. It is often not the case however.

In our scheduling policy, the free slots are divided fairly between the connections requesting bandwidth. If there is a number of slots free that can not be divided fairly, either the priority of the connections or the MCS used by the connections is used as the argument. It is also possible to use the Deficit Round Robin (DRR) method to achieve as fair a resource allocation as possible in these cases. There are pros and cons for all of the solutions.

Delay guarantees for the rtPS and ertPS connections with more efficient polling can be achieved by using an efficient polling policy. Equation 1 can be used first to choose the polling interval based on the QoS requirements. After that Equation 13 is used by the scheduler to choose when to allocate a slot:

$$PC_i \mod \big(\max\{P_I \cdot \text{FPS}, 1\}\big) = 0. \tag{13}$$

In this equation PC_i is the polling counter increased on each frame. The polling slot is allocated in the frame if the modulo is zero. The first sub-equations for rtPS and ertPS classes can then be replaced with this one.

These guidelines naturally apply only to the connections belonging to the service classes that allow polling. ErtPS without polling is the only service class that has minimum delay requirements and that does not use polling. The problem of guaranteeing a delay constraint for these connections is considered in a later section about the contention resolution process and multicast polling.

Because these equations do not take into account any overhead caused by the basic 802.16 header and the extended features, another set of equations and scheduling is needed. The basic mechanism for taking into account the MAC overhead is presented in the original publications. These are however not so important since the 802.16 specification mandates the subscriber stations to estimate the overhead before sending bandwidth requests. It is the responsibility of the base station to do this only for the UGS connections.

Even though these equations and policies are mostly aimed to be used in 802.16 base stations, they can also be applied to the uplink schedulers of the subscriber stations. This becomes extremely important when e.g. WiMAX-WLAN radio routers are trying to provide QoS to the WLAN users by using 802.16 as the backbone network.

2.3.2 Contention resolution

The specification of 802.16 defines how the contention resolution process works and what are the parameters that control the process. It does not however tell anything about how these parameter values should be chosen and set. In Publications **PIV** and **PIII** we present a solution on how to adjust the backoff parameters adaptively to maximize the utilization and still keep the delays under a desired limit. In Publication **PIII** we also considered VoIP as an application for simulations, since it has tight delay requirements and, therefore, imposes certain limitations.

The aim of the parameter tuning is to set the parameters in such way that the number of request transmission opportunities can be minimized while keeping a certain level of service in terms of medium access delay and loss of packets. The equations presented in the publications tune parameters such as backoff start, backoff end and the number of transmission opportunities. Input parameters for the equations are: the number of inactive connections N, Frames per Second FPS, Maximum medium access delay T, the probability for successful transmission on the first attempt p and the overall probability for successful transmission P. The number of inactive connections is known by the BS, and the value expresses the number of connections that could potentially take part in the contention. FPS is a static parameter for the BS. The rest of the parameters should be set based on the QoS requirements and the desired contention behavior. Probabilities p and P are the worst case estimations for probability.

Equation 14 can be used to calculate the value for backoff start. It is presented in Publication **PIV** with more details:

$$S = \begin{cases} \min\left\{ \left\lceil -\log_2\left(1 - 2^{\frac{\log_2 p}{N-1}}\right) \right\rceil, 15 \right\} & N > 1, \quad (14a) \\ 0, & N \leq 1. \quad (14b) \end{cases}$$

Equation 15 is used to choose a value for backoff end:

$$E = \min\left\{ \left\lceil \frac{\log_2(1-P)}{\log_2(1-p)} \right\rceil + S - 1, 15 \right\}. \tag{15}$$

The number of transmission opportunities depends on the delay requirements and can be calculated using Equation 16:

$$N_T = \left\lceil \frac{2^{E+1} - 2^S}{\mathrm{FPS}(T - C(E-S))} \right\rceil. \tag{16}$$

In a certain case where BO_s and BO_e are the same, transmission opportunities can be calculated by using Equation 17. This form of equation is most likely to be used in cases where a small medium access delay is desired, for example, when using VoIP or any other delay critical application:

$$N_T = \left\lceil \frac{2^S}{\mathrm{FPS} \cdot T} \right\rceil. \tag{17}$$

The equations are derived with more details in the original publications.

The base station employs these equations when the number of inactive connection changes.

2.3.3 Multicast polling

Multicast polling is studied in Publication **PV**, and this subsection analyzes the most important results of that publication.

We propose that the common backoff parameter problem described in Section 2.2.3 could be solved by adding two new type-length-value (TLV) encoded parameters to the `MCA-REQ` message (*backoff start* and *backoff end*). The group members would thus get the correct backoff values for the group when joining it. This method has some drawbacks, since it does not allow modifications on the parameters during a connection. On the other hand, it might not be necessary to adjust the parameters that frequently, and the necessary SSs could at first be unassigned from the group and thereafter reassigned with new parameters.

We also expect that the network operators' correct configuration for the usage of multicast polling should be as follows. Each service flow of the ertPS type, with its separate delay and loss requirements, should have separate multicast polling groups. The backoff parameters and the number of polling slots should be based on the requirements and the on number of connections in the group. These parameters can be set according to the equations presented in the previous sections.

The decision about the sizes of the polling groups is also important when setting them up. The same delay limits can be guaranteed with different parameters. For example, the usage of four request opportunities and the value of 3 as the backoff start and end provides the same delay as 2 transmission opportunities and backoff values of 1. So, which one should be preferred? Naturally the latter would result in more collisions. However, it is possible to make 10 SSs to use those 4 request opportunities or to put two groups of 5 SSs to use the smaller ones. As discussed in Publication **PIV** the probability p for a successful transmission for an SS can be calculated with Equation 18, where the sizes of the groups should be set accordingly:

$$p = \left(\frac{W-1}{W}\right)^{N-1}. \tag{18}$$

In the equation, N stands for the number of connections and W is the size of the backoff window, which in our case is the same as the number of request opportunities. It can be seen from the equation, that an increase in the number of the connections always decreases the probability of successful transmission while the number of request opportunities has the opposite effect. This is an open optimization problem and the topic will be discussed further in our future studies. Some guidelines, however, that are based on the experiments, are provided in the simulation section.

2.3.4 Admission control and call dropping

Admission control is an essential part when implementing QoS guarantees in an access network. A scheduling solution can guarantee the service level agreed only if the admission control policy on the base station can restrict the incoming service flows accordingly. This section presents an admission control policy to be used in conjunction with our scheduling algorithm. It uses the same algorithm that is used in scheduling, since the policy is basically the same.

The admission control procedure is launched in the following conditions:

- When Dynamic Service Addition Request (`DSA-REQ`), which creates a new service flow, is received at the base station

- When Dynamic Service Change Request (`DSC-REQ`), which changes the service flow parameters, is received at the base station

- When the MCS of the connection is changed

Each of the above conditions may either increase or decrease the resource demands of the connections. Downgrading is in practice always accepted but upgrading depends on the free capacity of the base station. If there is not enough free capacity, the connection is dropped in the current implementation. In further studies it is, however, possible to create a call dropping module and either to decrease the resource consumption of some service flow with a lower priority or drop it completely.

2.4 802.16 simulations

The quality of service of all the service classes is studied with network simulations in this section. Many of the features that have some additional effect on the QoS were also simulated and analyzed. In this section, the simulation environment is described at first and after that each of the scenarios studied is presented.

2.4.1 Simulation environment and NS-2 enhancements

The NS-2 [81] network simulator was used in this research to study the properties of the 802.16 QoS issues. Since the simulator itself does not have the 802.16 support, an extension (WINSE) was implemented in our research projects. The implementation includes all the important features of the MAC layer and some basic support for the 802.16 PHY. All of the simulation scenarios described in this thesis use the emulation of the OFDM physical layer of 802.16. Emulation of physical layer here means that the correct PHY frame structure that is the essential part for the MAC layer, is used. The physical layer of the extensions is simplified, but based on the simulation results, it seems to be realistic enough for the MAC layer simulations.

Even though some of the 802.16 related parameters were changed between the different scenarios, many of them remained the same. All the parameters that are common to all of the scenarios are listed in Table 1.

All the simulations were run in a scenario consisting of one base station and a varying number of subscriber stations. The topology of this is shown in Figure 6. The topology also includes one wired node that is directly connected to the 802.16 base station. The capacity of the wired link was set to 1 Gbps, to make sure that the wireless link would be the bottleneck of the network. In all the simulation scenarios, applications send and receive their packets between the subscriber stations and the wired node.

TABLE 1 802.16 common parameters

Parameter	Value
PHY	OFDM
Bandwidth	7 MHz
Cyclic prefix length	1/32
Frames per second	400 (2.5 ms per frame)
Slots per frame	75
Duplexing mode	TDD
UL/DL ratio	dynamic
Errors	OFF
Packing/fragmentation	ON
ARQ	OFF
TTG+RTG	160 PS
MAC PDU size	as large as possible

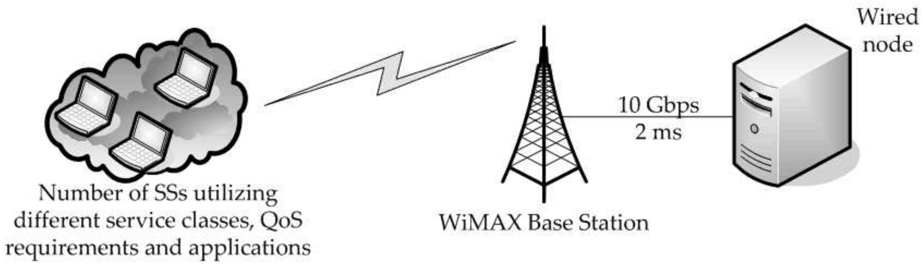


FIGURE 6 The basic topology of 802.16 simulation scenarios

Several different applications were used in the SSs during the simulations. FTP emulation and Pareto distributed ON/OFF traffic generators [26] were used on top of TCP. FTP is a good application to gauge the maximum overall utilization of the network. Pareto traffic on its behalf is used to simulate scenarios where testing of contention resolution is needed. When using FTP, the connections never need to participate in the contention since they can always piggyback the request in their existing allocations. The Pareto distributed ON/OFF application is used to model web traffic with an idle time of 375ms and burst time of 500ms. Due to the nature of the application, there is a need to participate in the contention quite often.

There are many applications tested on top of UDP also. The VoIP simulates the behavior of the G.711 audio codec, which has the highest mean opinion score [46]. The application sends data at the rate of 80kbps and uses a packet size of 300 bytes, which includes the headers of RTP, UDP and IP. Silence suppression is emulated by using active and idle phases of 1.004s and 1.587s respectively [47]. When the application is in an idle mode, it does not send anything whereas in an active mode it sends constantly with previously mentioned rate and packet size. For simulating IPTV traffic, a capture from a real MPEG-4 source was used. The capture included the MPEG packet sizes and time interval between the consecu-

TABLE 2 802.16 Scheduling scenario 1 - Active applications

SS	Simulation time			
	0–5	5–10	10–15	15–20
SS1 – SS3	√	√	√	
SS4 – SS5		√	√	
SS6 – SS13			√	
SS14 – SS15			√	√

tive packets in a random snapshot of the Jurassic Park movie. The capture was then fed to an application capable of reading it and producing the same output to the network. The bit rate of the application fluctuated between 2Mbps and 4.1Mbps. A constant rate traffic generator over the UDP was used in some cases.

2.4.2 Scheduling solution

Several simulation scenarios with different numbers and types of connections were run, and some of them are presented in the original publications. The most interesting scenarios and their results are now considered here. The purpose of these simulations was to show that the scheduler can provide the desired bandwidth guarantees. *Free* resources can then be divided fairly between the other connections.

In **the first scenario**, one BS and fifteen SSs exist. All the SS have one BE connection, and they utilize the connection by using an FTP application. The SSs activate their application periodically, and in the active mode they try to send as much as possible. In the inactive mode, they do not send anything. The activity periods are shown in Table 2.

The results of the simulation are presented in Figure 7. It shows the overall throughput of the network on the upper half of the figure and the throughput for each of the SS in the lower half. Data was gathered from the output interface of the BS towards the wired network. It can be seen that even though the number of the subscriber stations changes dynamically during the simulation scenario, the bandwidth resources are allocated fairly between the connections. The overall throughput is not constant since the number of SSs directly influences the sizes of UL-MAP and DL-MAP messages. When there are more subscriber stations, the sizes of the MAP-messages are larger.

In **the second scenario**, a similar kind of environment with five subscriber stations was simulated. The purpose of this scenario was to test whether the maximum traffic rates can be constrained. SS5 had the maximum bandwidth rate of 1Mbps, rate of the SS4 was limited to 2Mbps and all the others (SS1, SS2 and SS3) had no limitations.

The results of the simulation are presented in Figure 8. It can be seen that the constraints are satisfied and both SS4 and SS5 get the correct amount of throughput, and the free capacity is then divided fairly between the other SSs. The ability to constrain BE traffic is an important feature: it is likely that network opera-

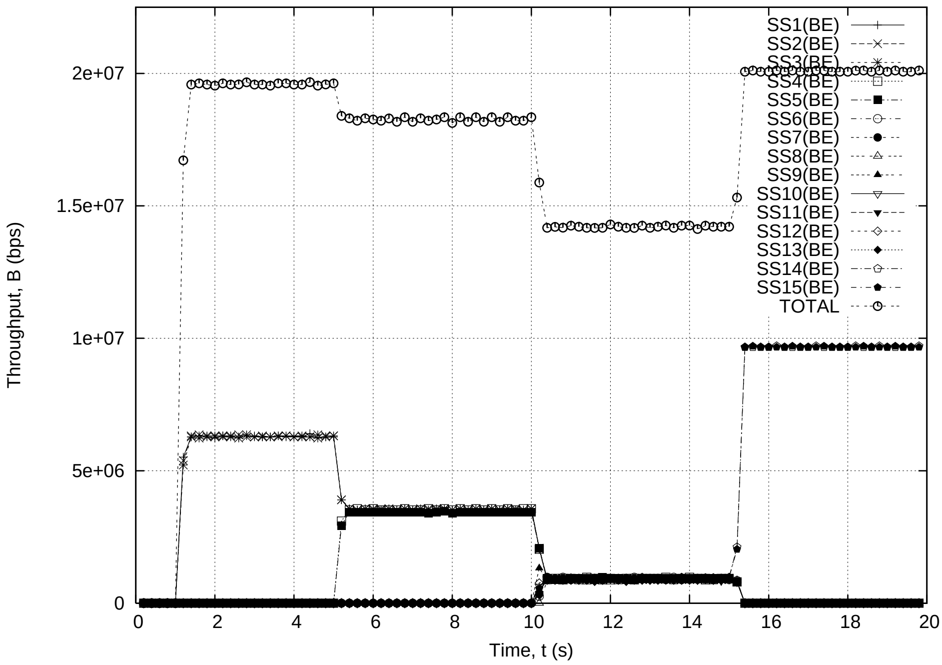


FIGURE 7 802.16 Scheduling scenario 1 - Throughput

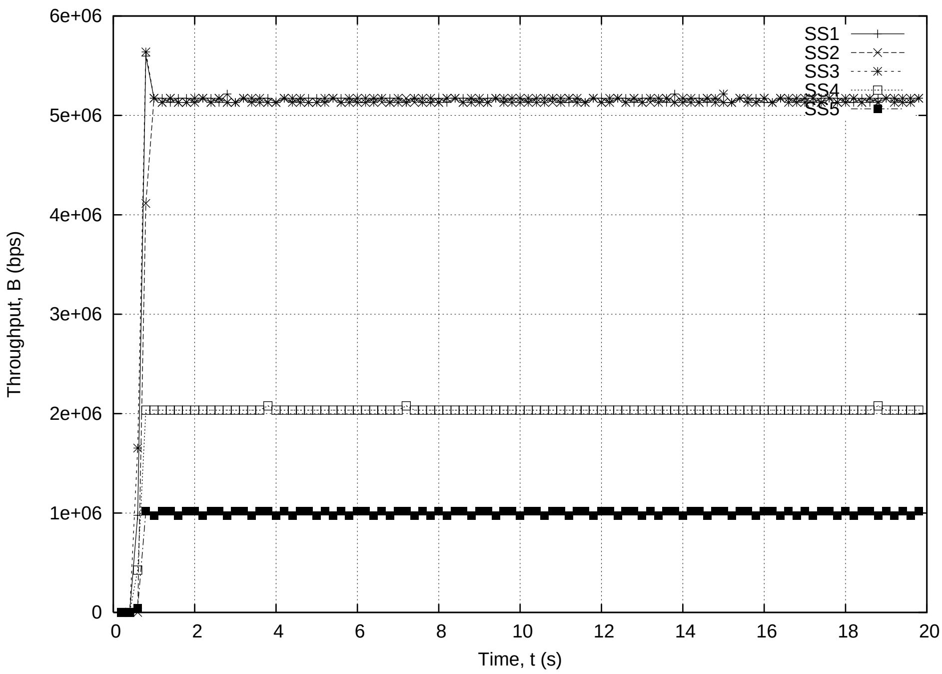


FIGURE 8 802.16 Scheduling scenario 2 - Throughput (maximum bandwidth limits)

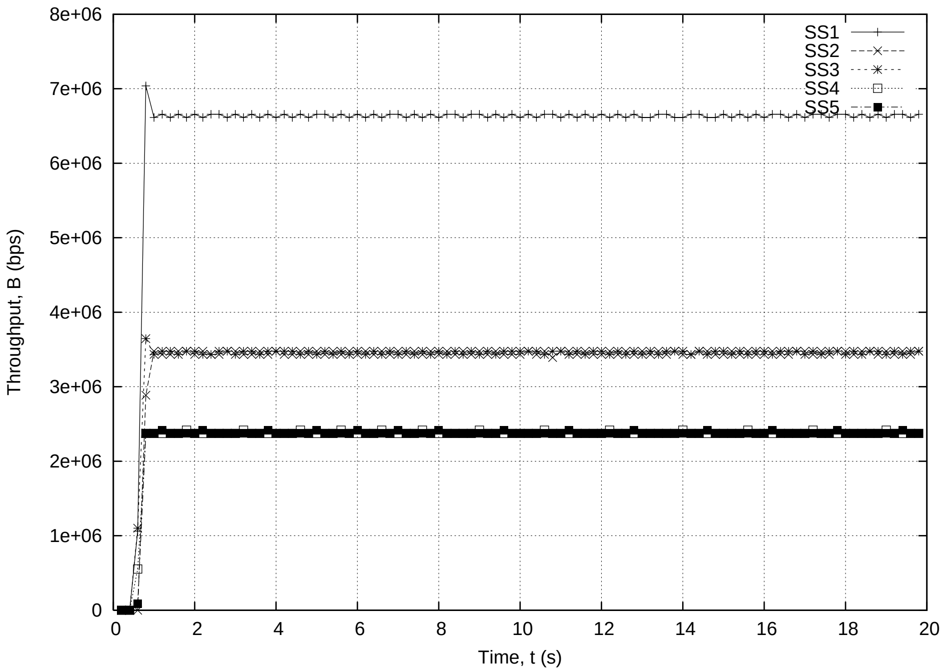


FIGURE 9 802.16 Scheduling scenario 3 - Throughput (traffic priority subcase)

tors are willing to constrain the traffic in order to offer connections with different speeds.

In **the third scenario**, another possible feature that could be used with BE connections is tested. It is the traffic priority parameter, associated to each service flow. In this scenario, there were again five subscriber stations, but now instead of setting the maximum throughput constraints, the priorities were set. SS1 was assigned the highest priority with the value of 2, SS2 and SS3 had a lower priority with the value 1 and SS4, and SS5 had the lowest priority of 0.

Figure 9 presents the results from the scenario. It can be seen that the subscriber stations with same priorities are treated fairly, and a separation is done between the priorities.

In **the fourth scenario**, other service classes in addition to the Best Effort service class were also simulated. The scenario consists of one base station and six subscriber stations. The application types, service classes and the bandwidth requirements for each connection are presented in Table 3.

Figure 10 presents the results from the scenario. It is shown that each of the connections retrieves the service that it is supposed to get in the form of bandwidth requirements. The throughput graph of UGS is depicted on top of the figure. The graph shows that the UGS connection utilizes four mega-bits per second throughout the simulation. The rtPS-connection utilizes the network with varying traffic profiles, caused by the variable-bit-rate nature of the MPEG video application. This is not shown in the figure, but it is definitely worth mentioning

TABLE 3 802.16 Scheduling scenario 4 - Traffic types and QoS requirements

SS	Traffic type	Service class	Packet size [B]	Bandwidth [bps]	
				min	max
SS1	UDP/CBR	UGS	500	4,000,000	
SS2	UDP/VBR	ertPS	300	0	80,000
SS3	UDP/VBR	rtPS	1378	2,054,400	4,108,800
SS4	UDP/VBR	rtPS	1378	2,054,400	4,108,800
SS5	TCP/FTP	nrtPS	1060	1,500,000	2,000,000
SS6	TCP/FTP	nrtPS	1060	1,500,000	2,000,000
SS7	TCP/FTP	BE	200	–	

TABLE 4 802.16 Scheduling scenario 5 - Used MCS

SS	Simulation time			
	0–5	5–10	10–15	15–20
SS1	64-QAM3/4	64-QAM3/4	64-QAM3/4	QPSK3/4
SS2	64-QAM3/4	64-QAM2/3	64-QAM2/3	QPSK3/4
SS3	64-QAM3/4	16-QAM3/4	64-QAM2/3	QPSK3/4
SS4	64-QAM3/4	16-QAM1/2	64-QAM2/3	QPSK3/4
SS5	64-QAM3/4	QPSK3/4	QPSK3/4	QPSK3/4
SS6	64-QAM3/4	QPSK1/2	QPSK1/2	QPSK1/2

that no packet loss is experienced during the simulation. That means that the scheduler handles the bandwidth requests from the SSs correctly. The nrtPS connections always get the maximum bandwidth allocation, since the network is not overutilized in this example. The bit rate of the BE connection on the other hand depends on the variance of the rtPS connections, since those are the only meaningful variable bit rate connections in this scenario. The throughput of the ertPS connection is shown by the bottom line in the figure. Since the ertPS connection is utilized by a VoIP application generating 80kbps on the active phases and zero on idle phases, slots are allocated to it accordingly. It is worth mentioning that ertPS connections do not experience any loss of packets. This is guaranteed by using polling for the connection.

The fifth scenario is supposed to illustrate the scheduler's ability to handle MCS dynamics. The modulation and coding scheme is changed periodically with the intervals presented in Table 4. The subscriber stations SS1 – SS5 establish UGS connections with a bandwidth guarantee of 1 Mbps and use the CBR UDP application generating that amount of traffic. The sixth subscriber station uses a BE connection and an FTP application on top of it. The purpose of this is to utilize the rest of the free capacity.

The results of this scenario are presented in Figure 11. As the results indicate, regardless of the MCS used, UGS connections are always allocated a correct number of slots to satisfy their requirements. The throughput of the BE connection (SS6) is explained by the MCS changes within the other subscriber stations.

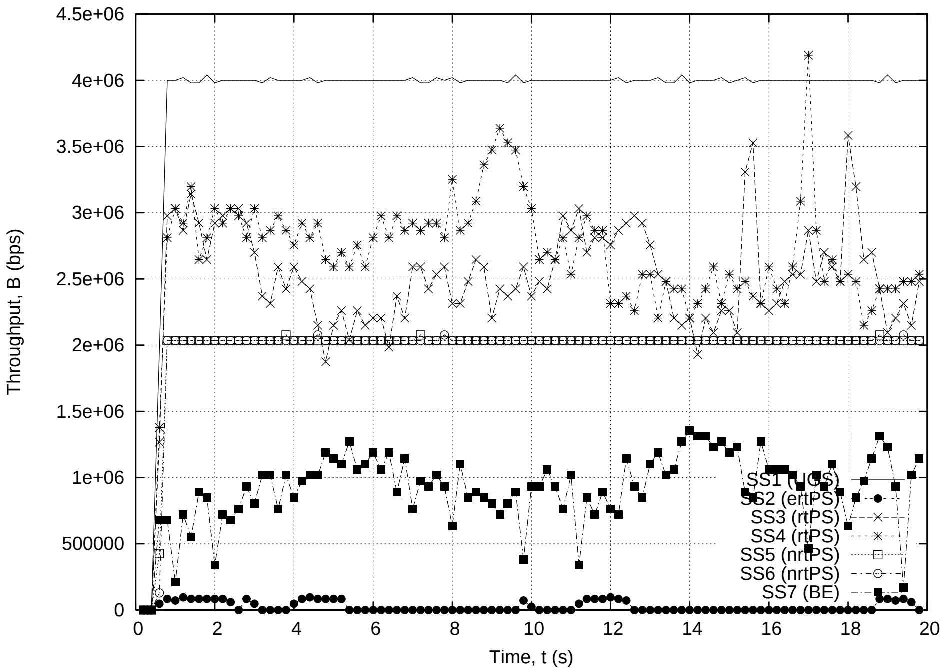


FIGURE 10 802.16 Scheduling scenario 4 - Throughput

For example at the simulation time of 15 seconds all of the UGS connections begin to use the less robust QPSK3/4 MCS: less slots are left available for other connections, and therefore SS6 can send a traffic volume of 500 kbps.

The sixth scenario on the scheduler is designed to illustrate whether the scheduler can allocate resources fairly to BE connections with different modulation and coding schemes. The schemes are the same ones as those used in the previous scenario and presented in Table 4, but all the connections in this case were BE ones using FTP applications.

The results of the scenario are presented in Figure 12. Analyzing the figure reveals that the scheduler does indeed behave as expected.

The overall conclusion regarding all of the scenarios is that the proposed scheduler can serve bandwidth guarantees for all of the service classes. The scheduler also takes into account the MCS utilized by the subscriber stations and MAC overhead for the UGS connections. BE connections are also served fairly in all of the cases.

2.4.3 Contention resolution

In the simulation part of Publication **PIV**, the behavior of the adaptive solution is studied. The exact simulation parameters and setups can be found from the original publication, but the basic idea was to test four different sets of backoff parameter combinations and compare them to the adaptive method. In the adap-

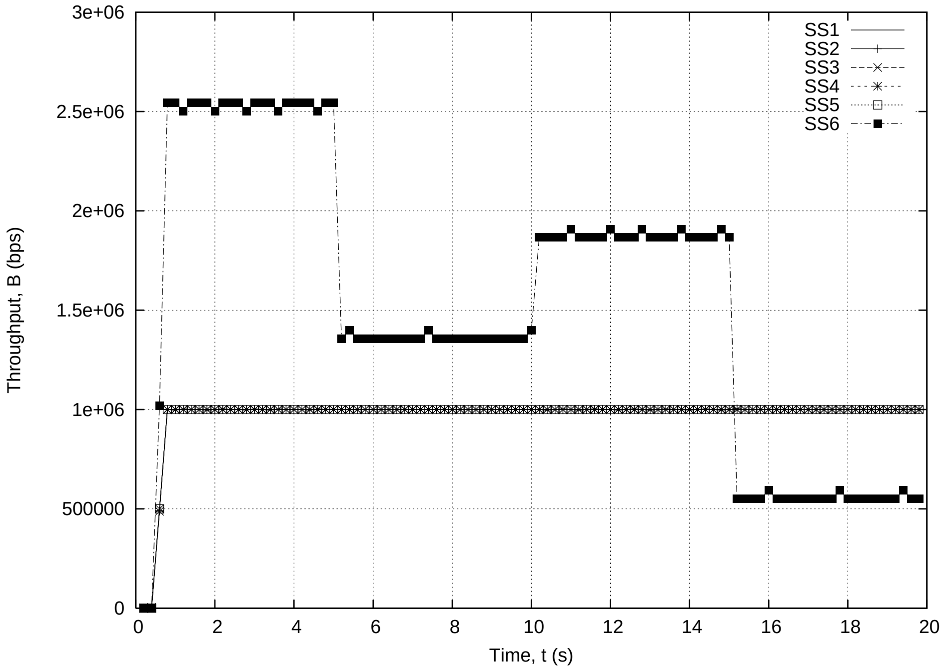


FIGURE 11 Throughput (802.16 Scheduling scenario 5 - Throughput)

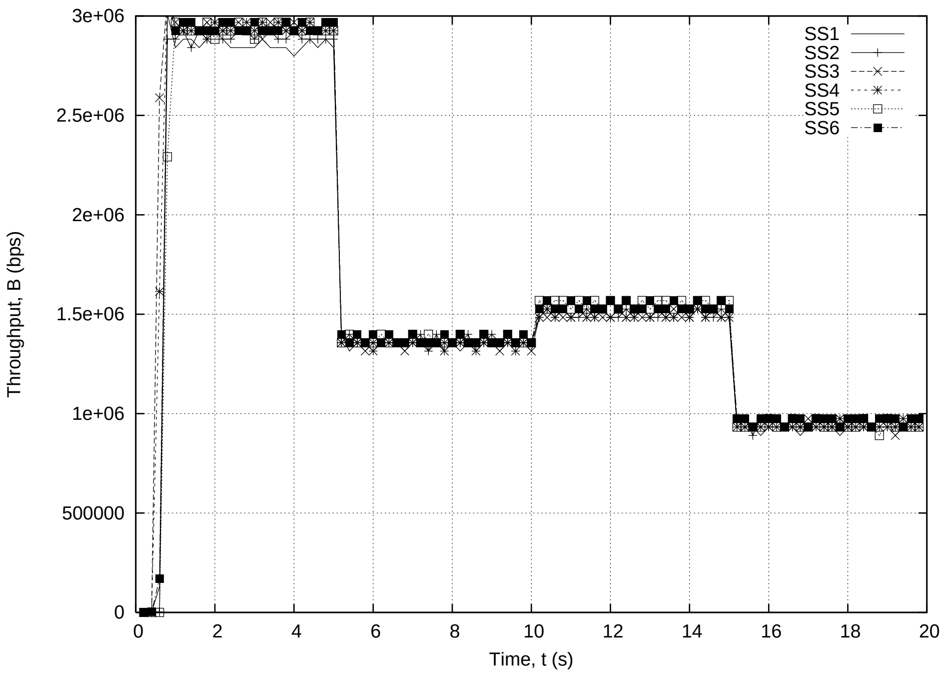
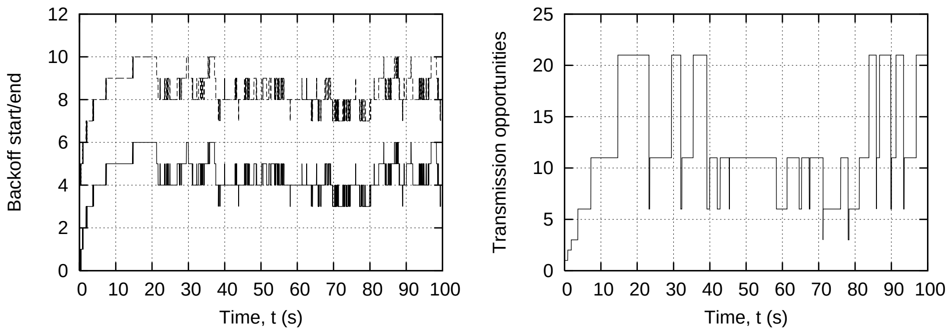


FIGURE 12 Throughput (802.16 Scheduling scenario 6 - Throughput)



(a) Backoff start/end (b) Transmission opportunities

FIGURE 13 Dynamically calculated parameters

	Backoff Start	Backoff End	Transm. opp.	Data (MB)	Max.access delay [s]	Loss (%)
I	0	15	1	58.610	68.52	0
II	6	15	1	82.566	72.90	0
III	6	10	21	165.352	1.58	0.004
IV	p=0.1, **P**=0.35, T=2			181.905	1.69	0.017
V	6	10	30	156.503	1.05	0.001

TABLE 5 Simulation results

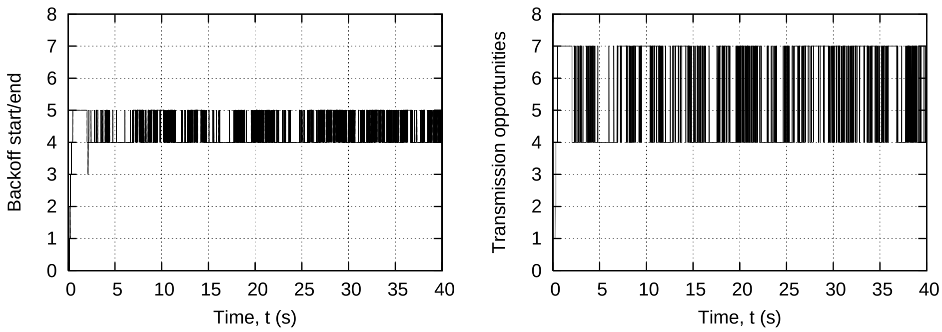
tive case, the adaptive algorithm adjusted the number of transmission and backoff parameters based on the number of inactive connections, maximum access delay T and the desired worst-case loss probabilities p and P set statically.

One BS and 100 SSs with BE connections with Pareto application were used. An application that generates traffic on a periodic basis was chosen, to make sure that there are several SSs taking part in the contention resolution process all the time. The number of inactive connections varied between 15 and 90 during the simulation period. The total simulation time was 100 seconds and SSs joined the network gradually from the beginning of the simulation. At the simulation time of 20 seconds, all the applications were started.

The number of transmission opportunities and the backoff parameters chosen by the algorithm are presented in Figure 13.

The utilization of the network, loss of packets and maximum medium access delay were measured and the most important results of the scenario are presented in Table 5.

The simulation Cases I and II were used to examine whether it makes sense to set the number of transmission opportunities as low as possible while allowing long contention process with backoff values. The results from Table 5 show that in these cases maximum access delay can be very long and, furthermore, the bandwidth is not utilized very well. This follows from the fact that while being in the middle of contention process, SS can not send any application data and



(a) Backoff start/end (b) Transmission opportunities

FIGURE 14 Dynamically calculated parameters

therefore no data is sent to the network. Backoff parameters and the number of transmission opportunities in Cases III and V were set as good as possible to limit the access delay but still to give a good utilization. Even though Case IV with the adaptive method gives better results in terms of utilization, the maximum access delay is still kept within the constraint (2s).

In the second simulation scenario presented in Publication **PIII**, VoIP is used as an application. The target upper limit for delay is 30ms, and 30 VoIP connections are emulated. The simulation setup is again presented with more details in the original publication. The target of this simulation scenario was the same as in the previous one, except for a lot tighter delay requirement. In this scenario, the first case was run by using unicast polling while the second and the third utilized static backoff parameters. In the fourth and the last one of the cases, the adaptive backoff algorithm was used. The resulting adaptive parameters are presented in Figures 14(a) and 14(b).

Parameters and results from the scenario are presented in Table 6. The results are as expected. Polling does not allow any packet drops and provides small and static access delay. On the other hand, the overall utilization of the network is very moderate in this case. The static parameters can be adjusted to either maximize the utilization, as is done in Case II. In this case the maximum access delay can however grow too high. Another static parameter set in Case III is adjusted to support the delay guarantees, but in this case the network is not maximally utilized. The adaptive method in Case IV follows as the best tradeoff between guaranteeing the delay while utilizing the network as well as possible.

The medium access delays experienced by the users in the adaptive backoff case are presented in Figure 15. It is shown in the figure that the delays are distributed to 5ms phases, which is caused by the frame duration of 5ms. The medium access delay of 5ms is experienced in cases where the contention resolution is successful in the first possible frame, 10ms in the second frame and so on.

TABLE 6 Simulation results

Value	Polling	Static backoff		Adaptive backoff
		Case I	Case II	
Parameters	1 slot/ frame	E/S=4, TO=2	E/S=5, TO=7	p=0.25, T=30ms
BE data (MB)	6.984	15.288	13.406	14.031
VoIP data (MB)	4.528	4.308	4.427	4.350
Total data (MB)	11.512	19.596	17.833	18.381
VoIP loss (%)	0	0.89	0.39	0.69
Max.delay (ms)	–	42.18	28.2	27.67

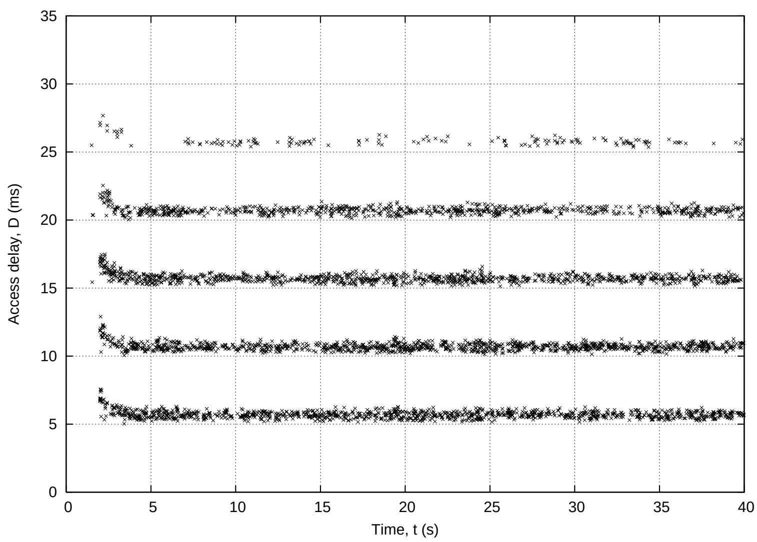


FIGURE 15 VoIP medium access delay (adaptive backoff case)

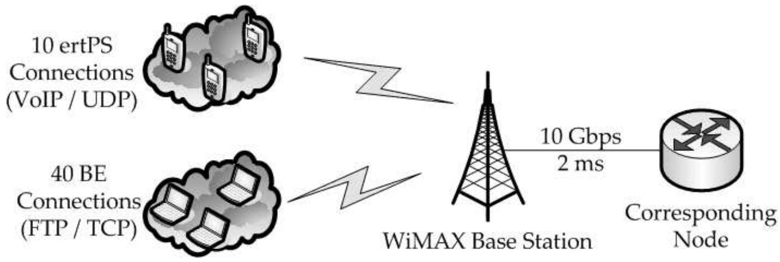


FIGURE 16 Topology of the Multicast Polling (Scenario 1)

2.4.4 Multicast polling

Multicast polling was studied by implementing the feature to the WINSE simulator. The implementation included all the details from the 802.16 specification and additionally the possibility to indicate SSs on separate backoff parameters with `MCA-REQ` management messages. The purpose of the simulations was to study the effect of the multicast polling in terms of bandwidth utilization and medium access delay experienced by real-time application users. This part is based on Publication **PV**.

All of the three scenarios were run in a topology that included one 802.16 base station and varying number of subscriber stations connected to it. The service classes and applications of the subscriber stations were also changed in the scenarios. The subscriber stations had either a VoIP application using an ertPS connection, an FTP application using a BE connection or an on/off TCP traffic to model web browsing. Each of the SSs established exactly one transport connection in both directions.

The base station was connected to one wired router with a large capacity link. This was done to make sure that the wireless link always remained as the bottleneck link for the connections. All the subscriber stations communicated with the wired node.

In the **first simulation scenario**, several polling methods are compared with each other in a fixed set of SSs. One BS and 50 SSs are connected. For the sake of simplicity, each SS establishes one transport connection and runs one application on top of it. Of the SSs, 40 use the BE service class and the Pareto application over TCP. The Pareto application is used to model web traffic with an idle time of 375ms and burst time of 500ms. Due to the nature of the application, there is a need to participate on the contention quite often. The rest 10 of the SSs establish an ertPS connection and use simulated VoIP as an application. The VoIP simulates the behavior of the G.711 audio codec, which has the highest mean opinion score [46]. The application sends data at the rate of 80kbps and uses a packet size of 300 bytes, which includes the headers of RTP, UDP and IP. Silence suppression is emulated by using the active and idle phases of 1.004 and 1.587 respectively [47]. When the application is in an idle mode, it does not send anything. In an active mode it sends constantly with previously mentioned rate and packet size.

The bandwidth guarantee is set to 80 kbps and the scheduler then allocates the appropriate slots for each connection. VoIP applications usually can handle delays of 100 - 200 ms, and therefore it is important to minimize the delay on the wireless link. In this simulation scenario the parameters are adjusted to see what kinds of delay limits can be achieved with them. The topology of the scenario is presented in Figure 16.

There are six subcases considered under this simulation scenario. The purpose of them is to compare the efficiency of polling mechanisms. These subcases are defined as follows:

I Only 10 VoIP connections and no BE connections. Here the aim is to find out how much bandwidth do the VoIP connections take when they are not disturbed by other connections. Unicast polling is used for the bandwidth requests.

II 50 BE connections are added in this scenario and then observed. The VoIP connections still use unicast polling with 1 polling slot in ertPS. In this case, the BE connections should not affect the VoIP connections at all. The efficiency of the ertPS with polling approach can be seen with this scenario.

III The VoIP connections are made to exclude ertPS polling and to use regular broadcast contention mechanism. The backoff parameters are adjusted to minimize packet loss, with the price of lost delay guarantees.

IV The case is like the previous one, except that the backoff parameters are changed to serve smaller MAC delays with the cost of decreased utilization.

V The VoIP connections are made to use Multicast Polling instead of the broadcast one. The backoff parameters are now adjusted to guarantee 15ms MAC delays.

VI This case is exactly like the previous one, except that the MAC delay of 20ms is now guaranteed.

The exact delay limits and contention parameters are presented in Table 7. The table also presents some results from the scenario. It can be seen that while the ertPS with unicast polling (Cases I and II) gives the best performance for the VoIP connections, it does not utilize the network very well. The solution allows only about 70 % of the BE traffic when compared with the other cases. The table also shows that the multicast polling based approaches utilize the network more efficiently than the broadcast based ones. Of the Cases IV and V, while the same delay limits are being guaranteed, the latter utilizes network more efficiently.

Figure 17 presents the MAC delays from subcases III to VI. Cases I and II are not presented since the unicast polling was used and SSs did not need to participate on the contention, resulting in a small constant MAC delay. It can be seen from the figure that Cases IV and V indeed do result in similar MAC delays. It is worth reminding that the approach with multicast polling (V) resulted with a

TABLE 7 Multicast polling (Scenario 1) parameters and results

Case	Broadcast Request Opp.	Broadcast BackOff Start	Broadcast BackOff End	Multicast Request Opp.	Multicast BackOff Start	Multicast BackOff End	Sent [KB] VoIP	Sent [KB] BE	Sent [KB] Total	VoIP Loss
I	8	0	32768	-	-	-	15345	0	15345	0%
II	8	0	32768	-	-	-	15345	231438	246783	0%
III	8	0	32768	-	-	-	14583	325058	339640	0.43%
IV	8	7	7	-	-	-	11318	260021	271338	4.39%
V	4	0	32768	4	3	3	13113	293042	306154	2.10%
VI	4	0	32768	4	7	7	13915	292189	306104	1.30%

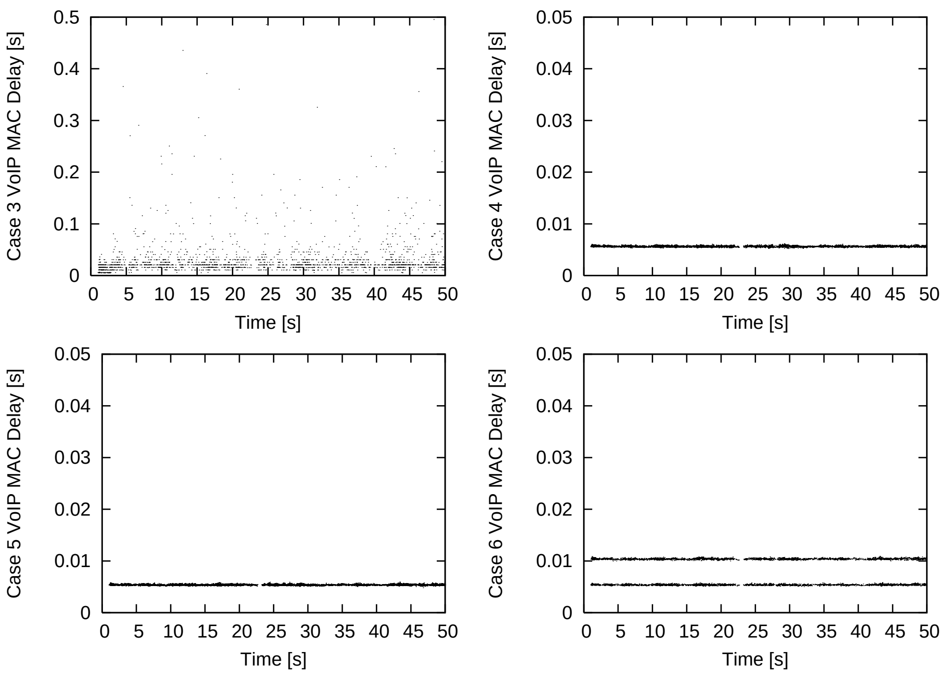


FIGURE 17 Multicast polling (Scenario 1) MAC delays

TABLE 8 Multicast polling (Scenario 2) simulation parameters

Case	Groups	SSs per Group	Req. Opp.	Backoff Start	Backoff End	Sent [KB] VoIP	Sent [KB] BE	VoIP Loss	Max. Delay [ms]
I	1	24	8	7	7	31341	516560	3.10%	6.62
II	2	12	4	3	3	31730	517123	2.96%	6.72
III	4	6	2	1	1	32295	516154	2.65%	6.88
IV	8	3	1	0	0	33659	513074	2.05%	7.05

better utilization. In Case VI a bit larger delay limit (20ms) was set, and the limit was kept.

It is also worth mentioning that even though each individual QoS guarantee can be satisfied without multicast polling, by adjusting the backoff parameters, not all of them can be at the same time. The final result from this scenario indicates that multicast polling is a nice advantage for guaranteeing QoS.

In **the second scenario**, a comparison is made between the use of smaller and bigger polling groups. Four subcases are run, and in each of them there are 24 VoIP users that use the same application parameters as in the previous scenario, and there is also one BE FTP user. The purpose of the FTP background application is to fill the available network utilization capacity, based on the free capacity. FTP is a good application for this purpose due to its greedy nature.

In the first case, there is only one multicast polling group with eight request opportunities. In the second one there are two groups with four opportunities each, and in the third one there are four groups and two opportunities each. In the fourth and the last case, there are four groups with only one opportunity for each. The backoff parameters are adjusted, so that the SSs can try to send a bandwidth request only once and if it does not succeed, the PDU is discarded. The exact parameters are presented in Table 8.

The effect of the group size should be examined in theory first, but from the experiments we can see that in this case a smaller group equals fewer collisions and thereafter incurs less packet loss. It must be also taken into account that on increasing the number of groups the size of the UL-MAP is also increased. This can be seen from the bytes sent by the BE class, especially in Case IV. It is also worth mentioning that the groups' size does not really have any effect on the MAC delays. This is predictable since the backoff parameters are adjusted to guarantee the delay.

The effect of the group size depends on the relation of the request opportunities and the number of connections in the group. Our future studies will investigate this issue more carefully.

In **the third simulation scenario** it is shown that the network operator can provide different delay limits and drop percentages to different applications / SS-connections. This is shown by using four VoIP classes with different delay requirements. Each class here has 5 VoIP applications and backoff parameters and the request opportunities are adjusted based on that. The backoff start and end values are passed to the SSs in the `MCA-REQ` messages as defined in Section

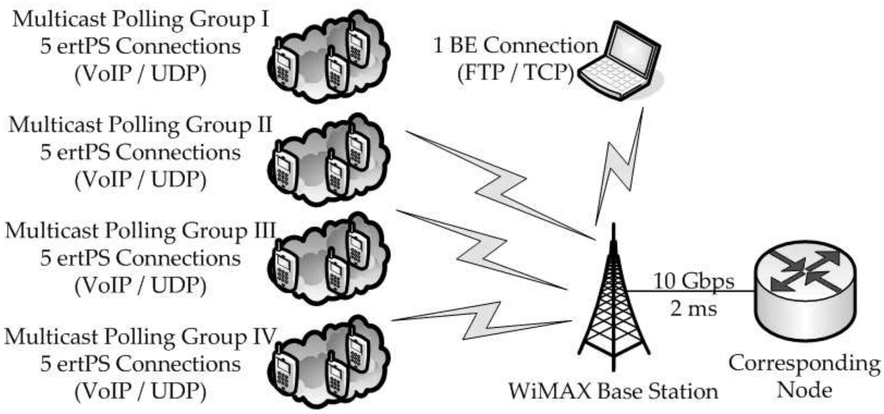


FIGURE 18 Topology of the multicast polling (Scenario 3)

TABLE 9 Multicast polling (Scenario 3) parameters

Polling Group	Req. Opp.	Backoff Start	Backoff End	Delay Req.	Packet Loss
I	2	1	1	15ms	1,455%
II	2	3	3	20ms	1,085%
III	2	7	7	30ms	0,884%
IV	4	3	3	15ms	0,106%

2.3.3. The network structure of this scenario is presented in Figure 18.

The contention parameters and delay requirements for each service class are explained in Table 9. Each class, except the fourth one, is allocated two multicast polling contention slots, and the backoff start and end are adjusted based on the delay requirements of the connections, based on Equation 1. The fourth class has more request opportunities per frame, since we want to see how this affects the loss percentage of the connections.

The resulting MAC delays from each class of VoIP connections are presented in Figure 19. It can be seen that the delays are always below the desired limit presented in Table 9. It follows from the contention parameters that for the first class there is only one opportunity in the first frame where bandwidth request can be sent, and therefore the delay is almost static. With the second class, there are two possible frames and with the third one, four. If a bandwidth request results in a collision and there are no more opportunities, the packet is dropped. Since the first class only has one opportunity, the number of dropped packets is naturally higher than with the others. The losses for each class are presented in Table 9. By increasing the number of contention slots per frame, the loss percentage can be decreased, as can be seen with the class 4. The decrease between Cases I and IV is actually quite dramatic.

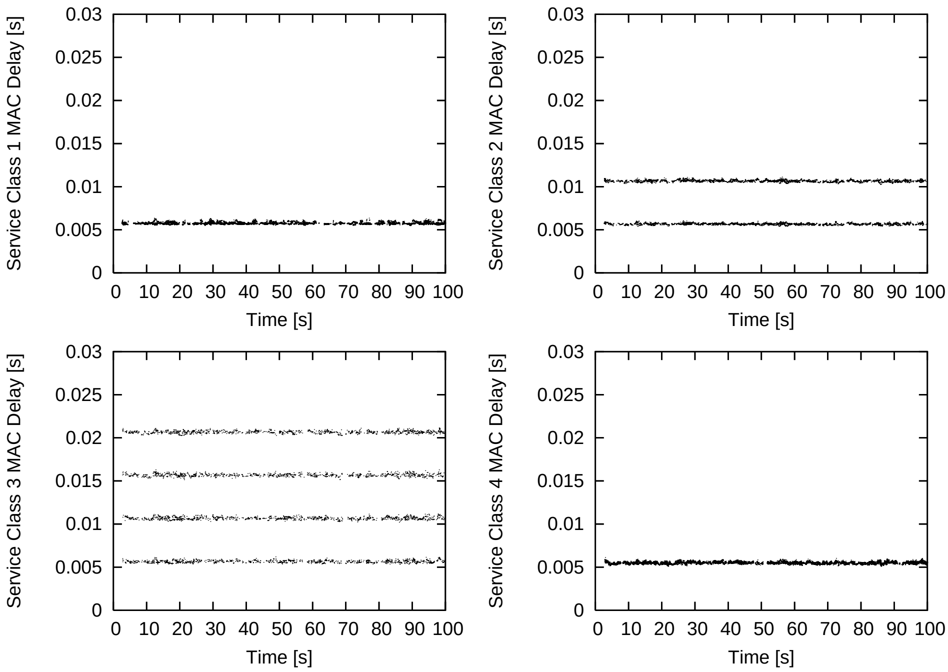


FIGURE 19 Multicast polling (Scenario 3) MAC delays

2.5 Summary

802.16 is a very promising technology for future wireless broadband access networks. One of the most interesting features of 802.16 is the support for Quality of Service on the MAC layer. The standard does not however define all the features needed to achieve it. Some of the features also depend on the correct parameters that are not part of the standard.

In this chapter of the thesis several novel ideas have been presented to support QoS on 802.16 base stations. A scheduling algorithm was defined to support all the service classes and their QoS requirements. Guidelines for setting the contention resolution parameter and an adaptive algorithm to tune them in real-time were presented. Multicast polling parameters were also studied and a modification to the standard was proposed.

All of the studied items were also tested in an NS-2 simulator. The results of the simulations clearly show the correctness and the advantages of our methods and parameter sets.

3 MULTICAST ADMISSION CONTROL

IPTV is a service with a huge potential: it is a widely accepted fact that the number of IPTV customers all around the world will grow quickly as the triple-play concept spreads out. Nevertheless, the Quality of Service of multicast flows has not been studied as much as it might be expected. This chapter describes the existing problems with multicast QoS and then focuses on the certain problem of multicast admission control. Therefore, some basic principles of admission control in general and the current quality of service architectures are presented at first.

3.1 Admission control

Admission control mechanisms are used for two reasons. The first reason is to restrict access to some resource to legitimate users only. When admission control restricts the content or flows to the legitimate users only, it may be referred as access control. Access control for unicast flows is a trivial task and, is usually done on the end systems (servers) to be dynamic enough. For multicast connections, it is not however as simple, since the server cannot control the access at all. After the server has sent the packets to the network, it has no knowledge of who is receiving it.

We studied the issues on these problems in Publication **PIX**. That article presents some practical results from work with this kind of real implementation. In [59, 17, 45] the authors present several methods to handle multicast admission control by either extending the IGMP protocol or by creating a new layer over the IGMP layer. These ideas seem good, but if implemented, many changes to the multicast routers would be needed. Our main idea was to create a method that could be used with the current network devices.

Some studies [4, 38] have suggested that the access control of the multicast flows could be affected by simply encrypting the content. The encryption and group key management mechanisms are feasible, but they cannot replace the access control. Replacing access control with encryption would have a major impact on the QoS issues also. The problem with multicast flows would be that useless multicast flows with large bit-rates would be forwarded to the network to drop down the QoS of the legitimate users of the network.

3.1.1 QoS based admission control

The second reason for admission control is to make sure that resources are not overloaded and existing users can be served with some quality of service. This mechanism is one of the most important ones when trying to guarantee QoS to the users. It may include the admission of new users, connections or flows and also some call-dropping functionality that is responsible on dropping existing users from the resources to allow a more important user to enter it. When QoS admission control is discussed, the terms that define whether the new flow can enter the network or not are the quality of service requirements of the new flow and of the existing ones. Someone or something in the network must make the decision, either to accept or to reject, based on the current information of the existing flows and the specification of the new flow. Traditionally the admission control methods have been divided into parameter based (PBAC) and measurement based (MBAC) mechanisms.

The selection of proper admission control module depends on the QoS architecture in use. There have been two main suggestions for the architecture and many variations of them, and these are now described briefly.

3.1.2 QoS architectures

The purpose of the QoS admission control module is always the same, but the implementation is tightly coupled with the QoS architecture used. The admission control procedures used in different architectures are briefly described here.

IntServ

When IntServ [13] architecture was presented by the IETF, instead of being the best effort model, was to create a framework where resources would actually be reserved. The signalling protocol to be used with the framework is not mandated, but Resource ReSerVation Protocol (RSVP) [84] is the best and only reasonable candidate. RSVP is used by the clients willing to establish a connection with another client or server. The RSVP message includes the traffic profile of the new flow, and is examined by all the routers on the path. Each router decides, whether it can accept the new flow, and if even one of the routers rejects it, the flow is rejected. Therefore, RSVP itself defines the admission control on the network.

The use of RSVP based signaling on each of the routers indeed does result as guarantees on the bandwidth basis and low delay when necessary. However, the reason why IntServ has never gained a wide acceptance, lies in its scalability. This aspect was criticized since, for example, in the core of the Internet there are millions of flows active all the time. The number of reservations in the memory of all those routers cannot scale well enough.

The IntServ model was rejected shortly after by the research community, because of these scalability issues. This thesis does not therefore directly deal with it. However, the IntServ model has been later proposed to be used on within another architecture [5].

DiffServ

The scalability issues having been left unresolved in the IntServ architecture, IETF created another architecture called Differentiated Services (DiffServ) [9]. Unlike in the rejected architecture, no reservations are made in DiffServ and the traffic is handled in aggregates rather than by flows. The idea was to move the complicated functionalities to the edges of the domains and keep the core routers simple and therefore efficient.

In the DiffServ architecture, there are three main service classes or Per Hop Behaviors (PHB). In [41] Assured Forwarding (AF) PHB is defined. The purpose of AF is to provide a better than best effort treatment and some bandwidth guarantee. Another per hop behavior called Expedited Forwarding (EF) is defined in [27]. The purpose of EF is to provide a service with a low delay, low jitter, low loss and guaranteed rate. In addition to these, the regular BE aggregate must be handled by the routers.

DiffServ by itself does not guarantee any service level for specific flows and, therefore a certain external entity is needed for this purpose. In [63] a framework with an entity called Bandwidth Broker (BB) is introduced. The purpose of the BB is to handle the dynamic admission control by replying to the admission control requests. BB must be aware of the flows existing in the network to make this decision. In [18] and [71] the framework is extended with a policy based management model. This framework also makes it possible to configure routers dynamically, based on the existing flows. In practice this means that the scheduling weights, service classes and queue lengths can be adjusted dynamically.

The bandwidth broker specification does not define an implementation for the framework, but Common Open Policy Service (COPS) was introduced in [30] and [19] for it. The signalling between the COPS server and the routers is based on the COPS, but the signalling from hosts to others can be done with several ways. RSVP, Aggregated RSVP [3] or GIST [16] might be used, for example. The applicability of each of these has been studied extensively in [67]. In Publication **PX** we have presented each of these technologies and their advantages and disadvantages. The publication also compares the protocols in terms of overhead caused by them. Basically, the purpose and behavior of each of them is quite similar, and any of them could be used.

After extending the DiffServ with some of the previous flow-specific proposals, it seems clearly better than the IntServ approach, in terms of providing QoS guarantees and scalability. Therefore, we concentrate on the DiffServ approach for the rest of this chapter.

3.1.3 Parameter based admission control

In parameter based admission control, the decision of whether the flow is accepted or rejected is based on the resource reservations made for existing flows and the specification of the new flow. This information might include, for example:

- Minimum, maximum and average bandwidth requirement
- Maximum burst size
- Average and maximum delay
- Average and maximum jitter
- Average and maximum loss percentage of packets

After taking into consideration these or at least some parameters, the admission control module must then decide whether the requirements can be handled properly for the new and existing flows. For example in IntServ architecture a token bucket based flow specification (TSpec) is used [84]. The parameters in this solution include token bucket rate, token bucket size, peak data rate, minimum policed unit size and maximum packet size. Other solutions on defining the bandwidth of the flow include leaky bucket and simple peak or average rate of the flow.

The strength of a parameter based solution is in that strict QoS requirements can be guaranteed. A weakness of these methods is that it is assumed that the entity responsible for the admission control has the full knowledge about each flow in the network, although this is not often the case in the current networks. Parameter based methods will usually also lead to scenarios where over-provisioning is done and some of the utilization of the network is wasted.

Parameter based methods depend heavily on the QoS architecture used. In IntServ networks, the architecture itself defines the admission control. In the DiffServ networks, the parameter based methods are not mandated by the RFCs. Therefore, the implementation of the parameter based admission control has been studied for example in [32]. It uses network calculus [12] to define an admission control mechanism, which makes it possible to guarantee QoS for the flows. The model is studied both in an analytical and simulative manner.

3.1.4 Measurement based admission control

The need for parameter based admission control is obvious when strict QoS guarantees are necessary. Many real-time applications do need this kind of behavior, but there are also many applications with different kinds of requirements. Basic TCP connections utilized by web browsing, e-mail and file transfers are examples of these. The usage of parameter based admission control with these applications will most likely result with many admission rejects and inefficient overall network utilization. Some of the measurement based admission control algorithms should be used with them. Another important reason for implementing measurement based admission control is that some traffic sources can not be estimated with Token Bucket or other models well enough without over-provisioning. In practice it is also often a case that applications do not estimate the utilization of themselves at all.

When using measurement based approach, the decision is done based on the measurements on the network. The measurements should result with some information on the current state of the network. The measurements can be based on some weighted average values from the history or be actual measurements from a specific moment of time.

The measurement based methods can also be divided into the active and passive ones. In this thesis the active methods are defined to be those that generate some extra packets (probe packets) to the network that are then used to measure the state of the network. The passive ones on the other hand only monitor the traffic of the network and do the measurements from the existing traffic. Both of the methods have their advantages and disadvantages.

The advantages of the active measurements usually include yielding more accurate results, at far as delay, jitter or packet loss are the parameters concerned. On the other hand, the extra packets always change something on the state of the network and therefore might also show up as a change on the results. The extra packets also always result with some extra utilization on the network and should not be therefore used when the capacity of a network is very limited. Active measurements also capture the state of the network only from the actual moment when probing is done, and cannot therefore adapt very well to networks with quickly varying utilization.

One active measurement based method for unicast admission control has been proposed in article [7], where a Gauge&Gate Reservation with Independent Probing (GRIP) protocol is described. It uses E2E probe packets to achieve a reliable admission control for AF PHBs. The basic idea of GRIP is to send probe packets to the destination node and wait for the replies. The admission control decision is then done based on the lost probe packets.

The advatageous features of passive methods are different from those of the active ones. They do not affect the utilization of the network and may sometimes result with more accurate results. Usually the results can also be averaged with some history results, and therefore give better view to the network with rapid utilization changes. The delay, jitter and loss can also be measured with these methods if the traffic measured is provided with enough details. For example, when measuring RTP-based traffic, the header fields of an RTP packet could be used. This naturally also requires clock synchronization between the source and destination of the measurement.

The authors of [15] compare several passive measurement based admission control methods and draw a conclusion that each of them can give almost exactly the same performance. In [14] the same authors conclude that the current measurement based methods are good enough in terms of their accuracy. The methods could be still developed to be more fair between the connections.

3.1.5 Comparison of different admission control approaches

When deciding whether to use an admission control based on parameters or on measurements, the QoS architecture usually imposes many limitations on the choice. Were these limitations ignored, the choice should be done taking into account the following:

Parameter based methods are good in providing strict QoS guarantees. The guarantees can actually be guaranteed. On the other hand, some of the bandwidth is not always utilized if complete guarantees must be given. A full knowledge of all of the flows in the network is also assumed, which is not always the case.

The measurement based methods usually utilize the network more efficiently. Strict guarantees can not always be given. This has been shown, e.g., in [49].

The methods can be divided into centralized and distributed ones. The problematics in the placement of the admission control modules are discussed in [35] and [51].

A combination of parameter and measurement based methods is the best solution in general. In [54] and [56] an admission control combining both parameter and measurement based methods is presented. The parameter based method is applied to EF flows, while measurement based approach is applied to AF flows. This kind of solution would be the most suitable for DiffServ networks. Both of these methods are studied in this chapter.

3.2 Multicast QoS in DiffServ domains

DiffServ is the best QoS architecture currently known, and with the correct extensions it can be used to provide QoS guarantees for the flows. Multicasting, however, is not as simple task in the DiffServ domain. Although the basic principles and mechanisms of DiffServ do work with multicast flows also, there are some provisioning related things that must be taken into consideration. As described in [11], [73], [76] and [1] the problems of using multicast flows in DiffServ domains can be divided into three or four parts, depending on the opinion. The fourth problem of DiffServ multicast are the multicast groups that include several senders. This makes things even more complicated, and most of the publications do not deal with the issue at all.

3.2.1 Heterogeneous multicast trees

The first one of the problems has to do with the issue of heterogeneous multicast trees. It follows from the scenario where there are several receivers in a multicast group, the receivers belonging to different PHB groups. One of the biggest problems is that it is not trivial to sort the PHBs in any absolute order. This again makes the generation of heterogeneous trees difficult or even impossible. One of the solutions to this problem is to create separate multicast groups for each offered service level. It naturally solves the problem but does not provide any optimal solution in terms of bandwidth utilization. Another simple solution is to offer best service level for all the receivers. It might be a more optimal solution in terms of utilization, but is not very practical from the viewpoint of an operator trying to get more profit from a better service level.

A solution for providing heterogeneous multicast trees, has been tried to be proposed in [8], [88], [78], [79] and [74].

The correct way to solve the problem would be to extend the functionality of multicast routers to support re-marking of the DSCP field in the packets when replicating them [8]. In this solution, routers would separate different service levels on the branching points of the multicast tree. The main problems in this solution are the sorting of the service classes and the scalability problem described later in this section. Another problem in this solution is the so-called "Good Neighbor Effect", which is illustrated in a scenario, where a regular IPTV receiver is paying for a cheap best effort service for its TV-channel. His neighbor has bought the best service level for the content and therefore the multicast content is transported to the switch of the building with the highest service level. Only after that the DSCP of the packets is degraded for the best effort customer. Even though the "Good Neighbor Effect" would be an interesting research item, it is left out of scope of this thesis. The overall problem of heterogeneous QoS has also been studied sufficiently, and it is not considered any further in this thesis.

3.2.2 Scalability of multicast

The second issue forms a fundamental rather than practical problem. The basic principle of DiffServ is that the core routers must be kept stateless, while multicast expects that all the routers forwarding multicast traffic must keep the state for each group. Providing heterogeneous trees further increases the problem, since the core routers also need to handle the remarking of packets on the branching points, which can be the core routers.

When trying to solve this problem, there are basically three different approaches available. The first solution is not to do anything. In [11], it is stated that this is not a problem at all and can be left as it is. Currently the number of multicast flows in the routers is indeed low, and therefore this opinion is justified.

The second solution is to change the existing multicast routing protocols and functionalities to more scalable ones. Several propositions have been made in [60], [75] and [74]. Even though these solutions do seem to be good and scalable, they would basically change everything in the current multicast protocols. It is unlikely that this kind of change could take place.

The third solution for the scalability issues, is to aggregate multicast flows to bigger groups, and let the core nodes handle the multicast aggregates only rather than individual flows. This kind of solution is presented at least in [31]. The solution does what it claims, but the applicability of it is uncertain.

Based on these considerations, it can be stated that the scalability issue is not searching for solutions by the time being, since the current scalability of the multicast is sufficient. However in future more efficient methods might be needed.

3.2.3 Neglected Reserved Sub-tree (NRS)

The third and probably the most important issue in the integration of DiffServ and multicast, is the Neglected Reserved Sub-tree (NRS) problem. It is described and analyzed quite thoroughly in [11] and [73]. The problem occurs when a new receiver joins an existing group G: the new subtree should not be neglected, but rather an admission control function should be performed. Although RFC 3754 [11] about DiffServ multicast has been published by the IETF, it does not solve all the issues of the NRS problem. The solution provides a framework that can handle that problem but relies on an external admission control method to do the actual admission control decision. The framework relies on the basic idea that, when a new receiver joins a multicast group, it should be grafted to the tree with a per hop behavior lower than BE [10]. After that, the actual admission control decision should be done. Afterwards, were the admission control decision positive, the DSCP of the receiver and its new branch would be increased.

In [37] another solution for the NRS problem is presented. Here the solution includes a QoS multicast routing algorithm and a BB based admission control method. The simulations are driven with NS-2, but the analysis of the results is not very detailed.

In [78] a solution presented can be used in IntServ over DiffServ kind of architectures with COPS server. Naturally the approach relies on the RSVP admission control criteria. The solution is good for IntServ over DiffServ architecture, but it is not applicable for other QoS architectures.

The EBM protocol presented in [74] also provides a solution for the NRS problem. In this solution, the core routers of the DiffServ domain have been left stateless and multicast-unaware. EBM would, however, replace the current multicast protocols completely.

Following from the previous work, it can be stated that if traditional IP multicast is to be used in the DiffServ domain, RFC 3754 [11] provides the best framework for it. The actual implementation of multicast admission control policy however needs to be defined and handled before the framework can be utilized in real DiffServ networks.

3.3 Multicast admission control

The RFC 3754 and the DSMCast protocol do provide good frameworks to handle the problems of delivering multicast in DiffServ domains. As described earlier, they do not however define the actual admission control method, and therefore we concentrate on creating one.

One could ask whether there exists a need for a separate admission control method for the purpose of multicast, or whether we need another one? The most important reason why the admission control must behave differently for multicast flows is that in unicast the sources must be controlled whereas in multicast the receivers must be controlled. This makes the decision making very different in these two cases. For a further analysis, we define a node called *Branching Node*. In multicast admission control, the new branch containing the new receiver is added to that node. Multicast admission control is supposed to take place for this branch only, not for the path from the source to the receiver. Another important thing is that in the current routers multicast packets are not forwarded with the same efficiency as in unicast, and therefore receive different kind of treatment. This makes most of the active measurement based admission control methods unusable for multicast purposes.

3.4 Proposed methods for multicast admission control

To overcome the NRS problem described in the previous section, we propose guidelines on how to manage the admission control for multicast flows. We also present some exact methods on how to do it. These methods are not supposed to be perfect: rather, they illustrate the strengths and weaknesses of each type of methodology and show the basic principles that should be taken into account when designing a multicast admission control method.

Since most of the current multicast applications are real-time applications, the EF class of the DiffServ architecture is the one under consideration in this thesis.

The methods are designed to be used in a distributed mode, but could also be implemented to work with a centralized admission control module such as COPS with RSVP. All of the methods have to three distinct phases each of which could be replaced with another more suitable one for the QoS architecture in use. It is worth mentioning that each of the phases has to be implemented with some method if true QoS is to be served.

The methods influence only the edge nodes of the domains, so they work according to the basic principles of the DiffServ architecture. The basic idea is to filter the unwanted join requests sent by the customers. Some additional leave requests also have to be generated when necessary. The idea is to reject some of the requests, to keep the QoS of the existing receivers acceptable. It is also checked whether a new receiver can get the service level required.

The admission control procedures begin when the egress edge router receives a join request from a potential new receiver R_N trying to join group G (Figure 20). The join request *Join(S,G)* is extended to include a third parameter (*QoS*). The whole message, *Join(G, S, QoS)* then includes the group address, source address and the QoS constraints that the receiver demands. The constraints are all or some of the following: maximum delay, average delay, maximum jitter, av-

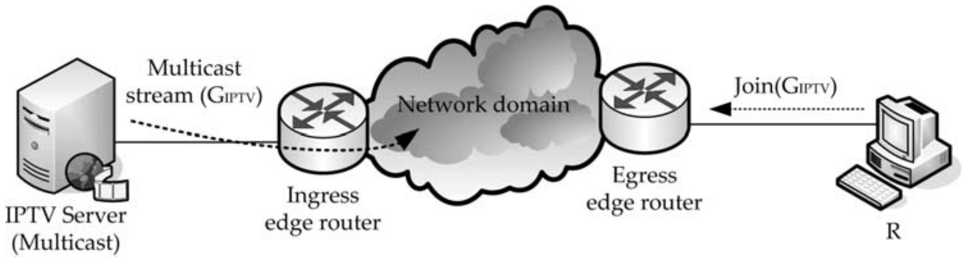


FIGURE 20 The beginning of the admission control procedure

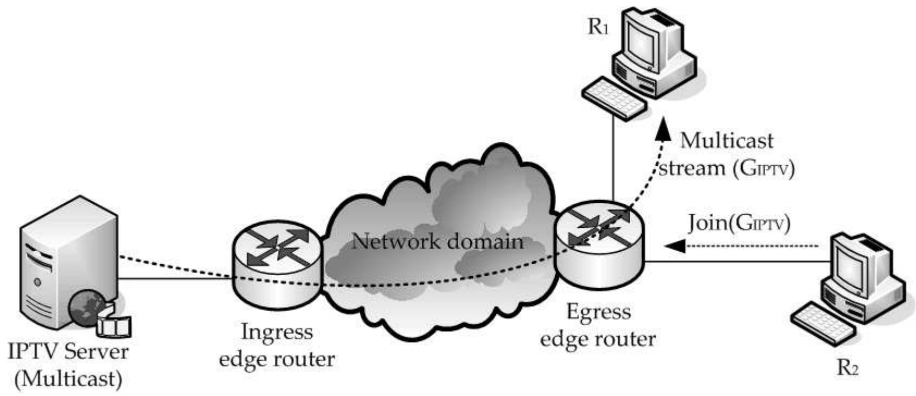


FIGURE 21 Multicast admission control - Edge test

erage jitter and average loss of packets. The constraints may be defined by the customer or they might be pre-defined in the SLA between the customer and the service provider. If IntServ over DiffServ is the architecture used in the domain, the QoS requirements would be sent in the RSVP or GIST protocol at the same time as the join message is generated.

3.4.1 Phase 1 edge test

When multicast admission control is performed, the first phase should always be the "Edge Test". The purpose of this test is to examine whether the egress edge of the domain is already forwarding the particular multicast group. If it is forwarding it, the join attempt should always be accepted. A possible scenario for edge test is presented in Figure 21. In this example, multicast receiver R_1 is already watching an IPTV channel transmitted in multicast group G. At that point another client R_2 is willing to join the same group. At the egress edge router and based on the edge test it should make a decision to accept the new receiver without continuing to the rest of the admission control tests.

Naturally the capacity and free resources on the link between the edge node and the receiver needs to be examined to make the decision whether the flow can be admitted. This has been left out of scope on this thesis however, since we only consider the resource management of a single domain.

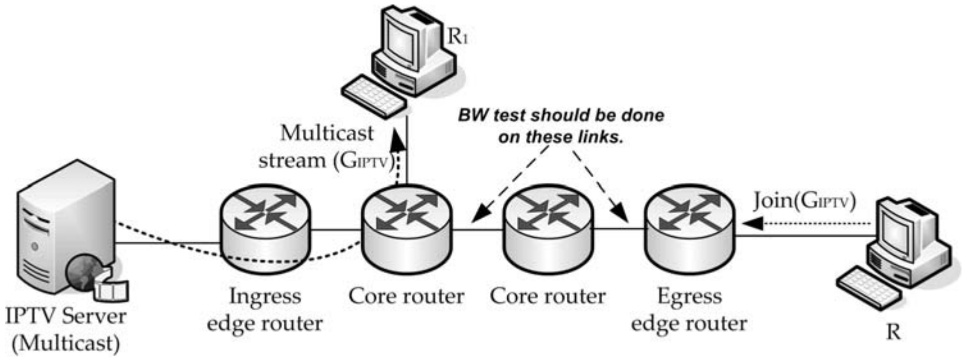


FIGURE 22 Multicast admission control - Bandwidth Test

3.4.2 Phase 2 bandwidth test

The implementation of the bandwidth test depends on the QoS architecture used. In the case of IntServ, RSVP would be the natural choice as it already supports this kind of functionality. Also a request to a COPS server or to a bandwidth broker might be sent if one of them is used in the network. In the case of aggregated RSVP, RSVP would be used again. Regardless of the QoS architecture, the bandwidth requirements need to be transferred to the elements responsible for reserving the bandwidth. In our methods, the bandwidth requirement is attached to the multicast join message.

When implementing the bandwidth test it is important to take into consideration the set of links where reservation or measurement should be made. Figure 22 shows these links in one example scenario.

All of our proposed methods either measure or calculate the available bandwidth in these links. In the parameter-based method, Equation 19 is used to calculate the free bandwidth on each of the link between the egress edge node and the branching node:

$$B_i^{free} = (w_i \cdot B_{tot}) - \sum_{j=0}^{N} B_j^{max}. \tag{19}$$

In the equation, w_i equals the weight of the class i where i is the service class of the multicast flow. B_{tot} is the total bandwidth of the link, N is the number of flows in the class, and B_j^{max} is the peak rate of the flow i. The flow specific peak rate here is assumed to be caught from a bandwidth broker.

The measurement based methods constantly measure the throughput on their links and then estimate the average utilization of the links. In practice, this functionality already exists on the routers. For retrieving this information to the egress edge responsible on the decision, MGRIP-based [7] [8] protocol is used. MGRIP works in quite the same manner as RSVP and could therefore be replaced with RSVP also. The idea behind these methods is to send a special GRIP packet containing the bandwidth requirements of the new flow to the branching node of the group. On the way to the destination, each router makes an independent decision about whether the new flow can be accepted or not. If the GRIP packet is received back by the sender, the flow is considered accepted and therefore the bandwidth test is accepted. Two different kinds of methods were used in our simulations: the first compared the requirement of the new flow to the overall available bandwidth and the second to the available bandwidth in the service class of the flow.

3.4.3 Phase 3 delay and jitter tests

The third phase of the admission control method is supposed to check that the delay and jitter requirements for the new flow can be guaranteed. Delay and jitter experienced by the packets usually depends highly on the network technology used, but some basic guidelines on how to test it for multicast flows are presented.

The parameter based method proposed, calculates the estimated delay with Equation 20 based on the calculations in [72]:

$$D_i = \frac{\sigma_i}{\rho_i} + \sum_{j=1}^{k} \left(\frac{F_j - \phi_{i,j} + L_i}{r_j} \right) - \frac{L_i}{\rho_i} + \sum_{j=1}^{k+1} p_i^j. \tag{20}$$

In Equation 20, D_i is the end-to-end delay estimation for the new flow in class i. σ_i and ρ_i are the Token Bucket parameters for the class that the new flow belongs. F_j defines the frame size of the node j; $\phi_{i,j}$ is the size of the frame for class i in node j; L_i is the maximum packet size for the class; and r_j is the outgoing link capacity on node j. The last sum is the total propagation delay for the path from the branching node to the receiver.

When measurement based admission methods try to solve whether delay or jitter can be guaranteed, there are two ways for doing it. In the easier solution the edge nodes have to do active measurement on packets by sending probe packets to the branching node and then by examine the results.This creates some additional overhead to the network. The other solution is to use the flow waiting for an admission itself. This has several advantages compared with the first solution. Multicast packets are usually treated differently from the unicast ones on the routers. As a results there is a difference on the measurements between multicast and unicast test packets. This approach assumes that delay measurements can be done on real packets handled with the help of the fields of the RTP header. The edge node joins the multicast groups, waits for the 20 first packets and then calculates the average delay of those packets. If the calculated delay is below the limit, joining of the new receiver is accepted.

The delay and bandwidth tests are done concurrently, and if even one of them fails, the new flow is rejected. The overall procedure is presented in the original publications.

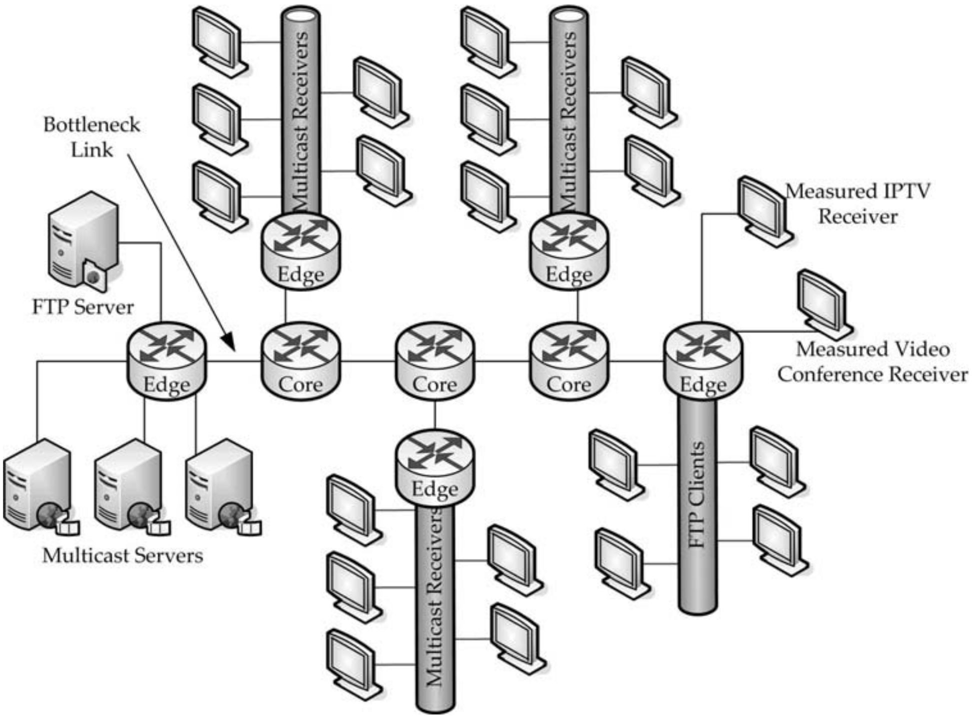
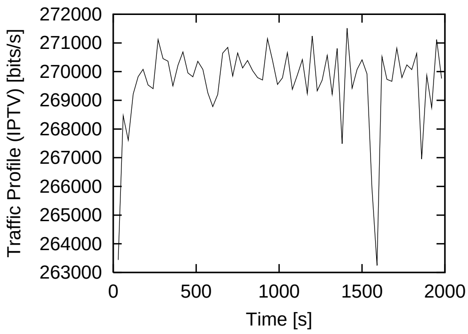


FIGURE 23 The topology in multicast admission control scenarios

3.5 Simulations

This section presents the simulation scenarios where all of the methods described in previous section were tested. The simulations are described with more details in Publications **PVI**, **PVII** and **PVIII**. The simulations were run in a network simulator NS-2 [81] with the DSMCast extension [77]. All of the simulation scenarios were run in a network topology shown in Figure 23.

The aim of the simulation scenarios was to show that it is necessary to have some admission control method to be able to guarantee a proper quality of service for multicast receivers. The advantages and disadvantages of each type of method also need to be highlighted. QoS experienced by two multicast customers in the network were measured to indicate the feasibility of the admission control. Those two measured receivers joined to the multicast groups in the beginning of the scenarios and were kept as members till the end of those scenarios. The other multicast receivers were continuously joining and leaving the groups and therefore utilizing the admission control module on the edge nodes. The joins and leaves were randomized with certain random distributions. The duration of the memberships was simulated with exponential distribution and after leaving a group, the receivers waited for a Pareto distributed time interval. In addition to the multicast receivers, there were two multicast servers sending video traffic to



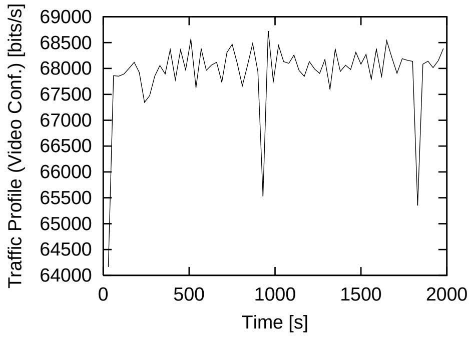


FIGURE 24 The profiles of the measured traffic

TABLE 10 Simulations traffic

Traffic	**Bandwidth**	**Packet-size**	**DSCP**	**Delay Max.**
Control messages	-	-	5	-
Video conference	~68kbit/s	~800Bytes	6	400ms
IPTV	~270kbit/s	~950Bytes	10	250ms
FTP	-	900Bytes	99	-

ten multicast groups. An FTP server and clients were also added to create background traffic and to utilize the free capacity of the network. The maximum bit rate of the FTP servers was regulated in the scenarios to see how the amount of background traffic influences the QoS of the multicast receivers.

The video streams produced by the multicast servers were captured from real H.263 video streams transferring the "Jurassic Park" movie [33]. The first stream was used to model IPTV traffic with an average throughput of 270 kbit/s and the second one was modelling a video conference application with an average rate of 68kbit/s. Sample traffic profiles of both sources are shown in Figure 24. Both of the sources were used for 10 multicast groups making up 20 multicast sources and groups altogether.

The realtime multicast traffic was classified as EF PHBs on the ingress edge of the network. The core routers of the domain then forwarded the traffic according to a WRR scheduler with the weights listed in Table 11. The weights of each class were set a bit lower than the actual bitrate of the multicast traffic, since the admission control module should show its capabilities here.

Three simulation scenarios are now presented to show the strengths and weaknesses of each method. In the first scenario, network is not utilized by the background traffic to any great extent. The motivation behind this scenario is to show that the admission control methods do not reject any request. The next scenario simulates a situation where the network and its bottleneck link are very highly utilized. This scenario shows that the admission control can still provide

TABLE 11 PHB definitions

Application	PHB	WRR Weight	Queue length
Control messages	EF	0.01	25
Video conference	EF	0.14	50
IPTV	EF	0.47	100
FTP	BE	0.38	300

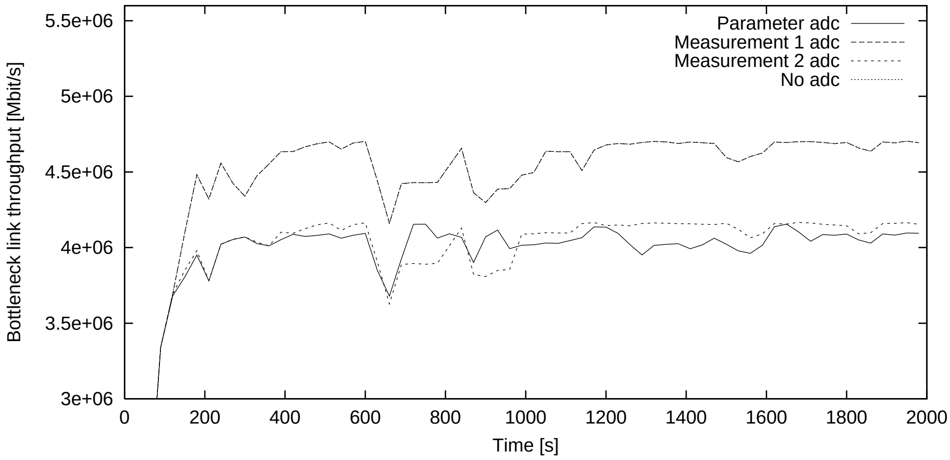


FIGURE 25 Bottleneck link's throughput in low utilization scenario

a good QoS to the receivers by rejecting some of the new receivers. In the third scenario, all the interesting results from the previous scenarios are examined as a function of the background traffic volume.

3.5.1 Low utilization scenario

In this scenario, it was tested whether the admission control method has a negative impact on the network utilization when it should not have. In this scenario the links were lightly loaded and the queues were not full at any time. The bandwidth of the FTP link was restricted to 1.325Mbps.

Figure 25 demonstrates the throughput on the bottleneck link. It shows that when not using any admission control or when using method 1 that is measurement based the throughput of the bottleneck link is exactly the same. This is due to the low load on the network causing no requests being rejected and therefore maintaining the number of multicast receivers the same. On the other hand, when using method 2 or parameter based admission control, the bottleneck link is less utilized, although there would still be bandwidth available on the link.

The reason for not utilizing the bandwidth completely derives from the differences in admission control methods. As mentioned earlier, the measurement based method 2 and parameter based method base their admission decision based on the available bandwidth within each class, not within the whole link. A

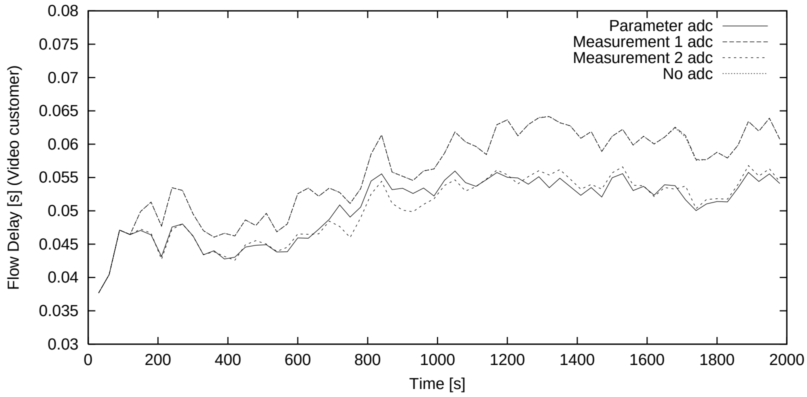


FIGURE 26 IPTV delay in low utilization scenario

certain class might have used all the bandwidth available for that class already. Therefore all the new requests would be rejected, although there would still be bandwidth available on the link.

The effects of these methods to the delay can be seen in Figure 26. The figure shows the end-to-end delay experienced by the video stream receivers in this lightly loaded scenario. It can be seen clearly that the parameter based ethod and the measurement based method 2, which were wasting bandwidth by rejecting join requests, provide shorter end-to-end delays. This is just a simple consequence from the fact that with less traffic in the network the delays remain low, because the packets are handled faster.

3.5.2 High utilization scenario

The results here are from a simulation where the utilization of the network was much higher. The bandwidth of the FTP's link in this simulation was 2.775Mb/s. This scenario is much more interesting than the first one, because in this case the advantages of admission control are needed. At first it can be seen from Figure 27 that each of the methods start to deny some of the connections, as the FTP applications cannot send at a full rate.

In Figure 28, the utilization of the bottleneck link is shown. This Figure shows that methods others than the measurement based method 1 utilize the network in its entirely. This is due to the greedy nature of FTP applications; they utilize their share of the capacity and, therefore, do not allow multicast connections to enter the network later. This conclusion indicates that the measurement based method 1 does not work very well.

In Figure 29 the delays experienced by the multicast customers are shown. It shows that all the admission control methods can limit the end-to-end delay to a decent size, except when not using any admission control.

The overall result from this scenario is that the measurement based method 2 and the parameter based method do work well also in a high utilization sce-

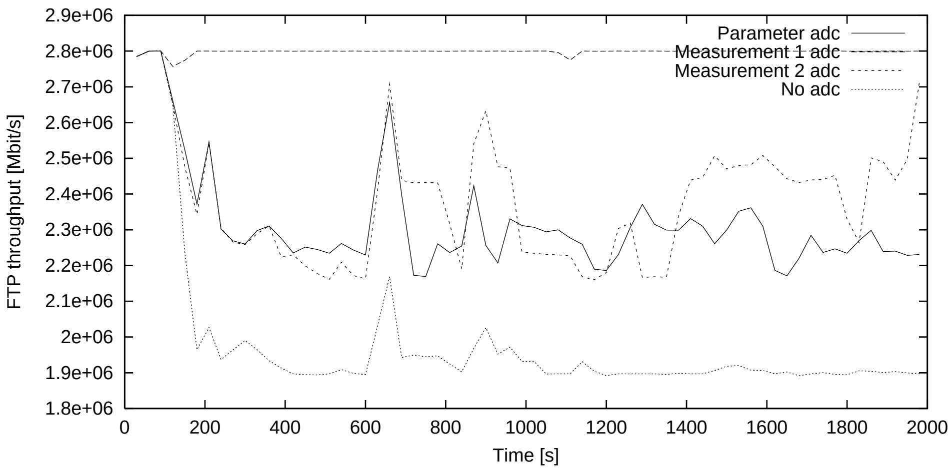


FIGURE 27 FTP throughput in high utilization scenario

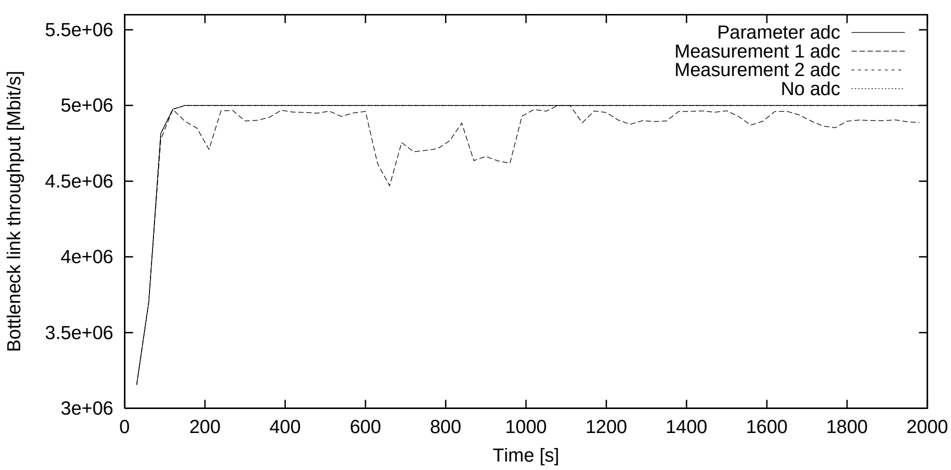


FIGURE 28 Bottleneck link's throughput in high utilization scenario

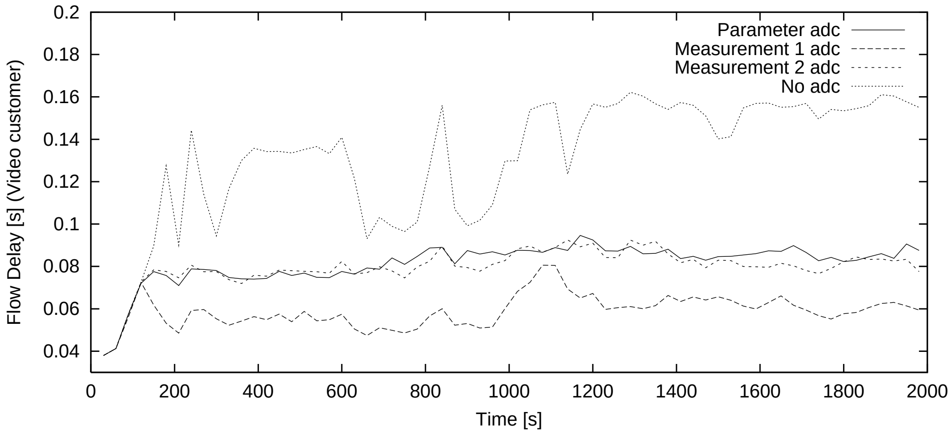


FIGURE 29 IPTV delay in high utilization scenario

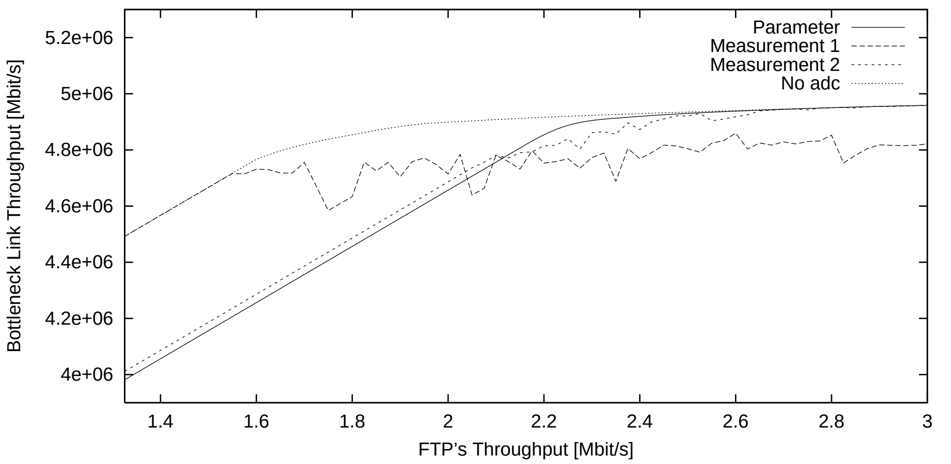


FIGURE 30 Bottleneck link's utilization as a function of the background traffic

nario.

3.5.3 The effect of the utilization

For this Subsection, a total of 70 simulations were run, every round increasing the amount of the background FTP-traffic. In Figure 30 it can be seen how the bottleneck links' utilization increases as a function of the FTP-traffic from 1.325Mb/s all the way up to 3.025Mb/s.

As the amount of background traffic increases, the bottleneck links' utilization level increases as well. It can be seen that the maximum utilization is reached when not using any admission control, which is expected. The figure also shows the goodness of the methods, when compared to the overall network utilization. The measurement-based method 1 produces quite a good network utilization in

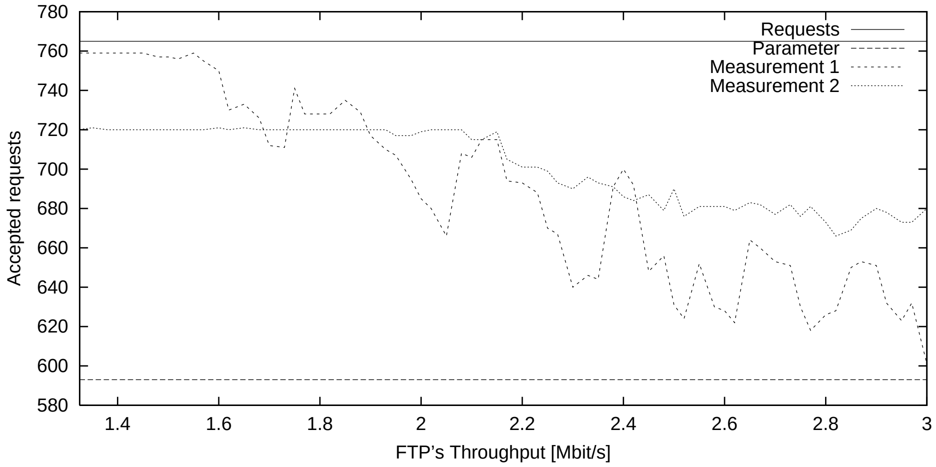


FIGURE 31 Accepted requests as a function of the background traffic

all the cases. The other two methods have a more positive effect when the network is more utilized.

Figure 31 shows the number accepted join requests in each of the scenarios. Here it can be seen that the parameter based method always produces the same number of accepts, which is as expected. The measurement based methods however produce different numbers of requests. The first one of the measurement based methods results with a decreasing number of accepted requests while the second one succeeds to stabilize the number. This again indicates that the second method is more reliable and suitable.

Also the maximum delay experienced by the multicast receivers is reached at 1.9 Mbit/s. This is the point where the background traffic has used all the bandwidth dedicated to it. In this case of no admission control, the network is very well utilized from the very beginning.

The measurement based method 1 starts to reject joining requests at 1.6 Mbit/s. From this point onward, the utilization level does not increase significantly. There will be more rejects on the video customers than on the conference customers because of the stricter QoS requirements for the former. This is shown in Figures 32 and 33. The delay remains low throughout the simulation because the admission control maintains the number of multicast receivers at a low level all the time.

On the other hand, when using method 2 or the parameter-based method, the utilization level reaches the maximum possible at 2.4 Mbit/s - from this point onward the available bandwidth is used also in the case of no admission control. This can be explained as follows. At 2.4 Mbit/s the background traffic has used all the bandwidth of its own plus the bandwidth left over from the multicast receivers. As mentioned earlier, these two methods tend to leave some amount of bandwidth dedicated to that class unused. It can be seen from Figure 34 that at 2.2 Mbit/s the delays increase very steeply due to the packets being queued until

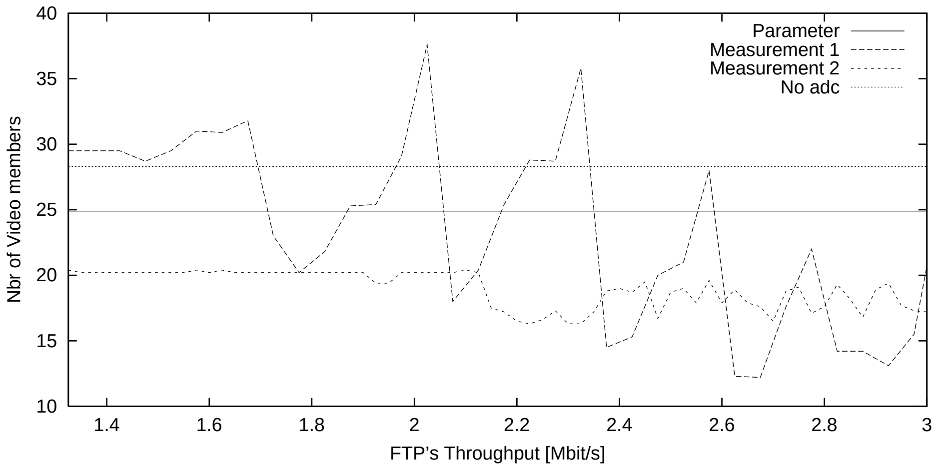


FIGURE 32 The number of IPTV customers throughout the simulation

the point at 2.4 Mbit/s. After that the delays settle down to a certain value. This means that the multicast receivers have reached their maximum queuing delay, the amount of background traffic being at its maximum.

In the parameter based method the number of video and conference customers remains the same all the time, as it does in case no admission control is used. The other two remaining methods do change the number and the relation of the different types of multicast receivers. The number of accepted requests is depicted in Figure 31. In the end the number of video receivers will have decreased while the number of conference receivers will have increased. This is because of the stricter QoS requirements for the video receivers. The variation of conference -and video customers during the simulations is shown in Figures 32 and 33.

As mentioned earlier, the parameter based and measurement based 2 approach 'wastes' bandwidth. That is why the utilization level starts from such a low level in comparison with cases of no admission control or with the measurement based method 1 (Figure 30).

As an overall conclusion drawn from the results, it can be stated that either the parameter based or the measurement based method 2 could be used as an admission control method. Both of them provide QoS for the customers and still utilize the network well in all the cases.

3.6 Implementation issues

To see whether the admission control methods would be applicable for a real router environment, one of the methods was implemented to Linux-based routers in a laboratory network. The functionality of the edge router and some helping

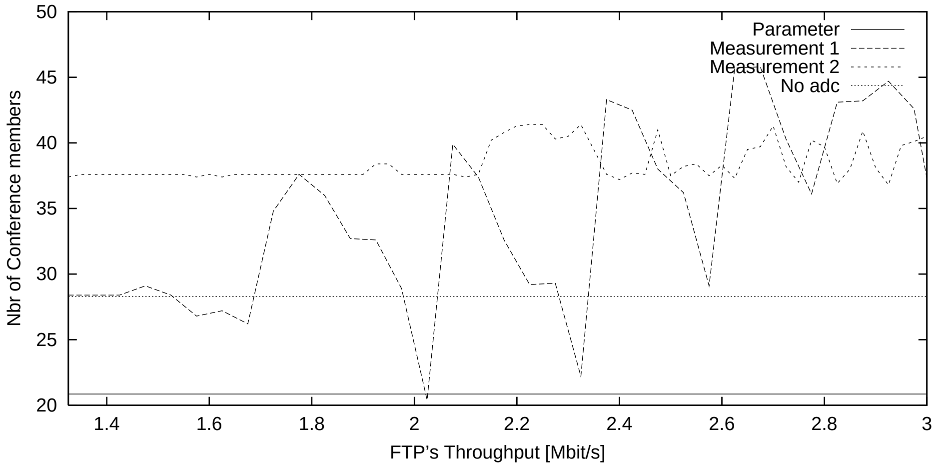


FIGURE 33 The number of video-conference customers throughout the simulation

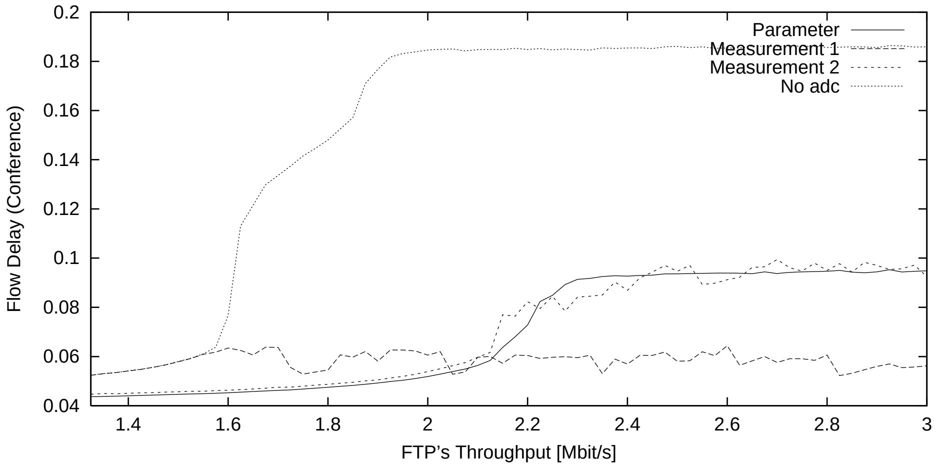


FIGURE 34 End-to-end delay of a conference customer as a function of background throughput

applications like multicast QoS monitor were implemented. The added functionality of the edge router was used with a Linux routing software XORP [86].

The edge nodes admission control method (measurement based method 1) was implemented with the help of Linux firewall software IPtables. Its task was to capture all the IGMP join messages received from the customers in order to base the admission control decision on those messages. When an admission is rejected, the edge routers generate an IGMP leave message to itself causing the XORP framework to generate an appropriate PIM prune message towards the core network. The IPtables rules used in this implementation were the following:

```
iptables -t mangle --flush
iptables --flush
iptables -t mangle -A PREROUTING -p IGMP -d 230.0.0.0/8 -j QUEUE
iptables -A OUTPUT -d 230.0.0.0/8 -p IGMP -j QUEUE
```

Since the laboratory network did not have a sufficient number of computers for the tens or hundreds of multicast receivers, a software called Shadow Node was also implemented. The task of the Shadow Node was to behave as a certain number of multicast receivers leaving and joining the multicast groups with the intervals used in the simulation part. The scenario tested with the implementation was also similar to the one in the simulation part, shown in Figure 23.

Two measured clients were also implemented. Their purpose was to receive the multicast traffic and measure the QoS. The measurements were based on the RTP headers and the delay, jitter and loss were calculated.

A scenario comparable to the one in the simulation part was then run. The results of the implementation did not appear to be as good as in the simulations. The reason for this was the small delay in the real network. Therefore the bandwidth test was the only one resulting in rejects. Another problem was the fact that, e.g., 10Mbps Ethernet did not actually produce the maximum throughput of 10Mbps but approximately 9Mbps. This caused the admission control module to accept request also in cases where no more flows could enter to the network. Before real results from a practical implementation can be expected, some calibration needs to be done. Some delay generator could also be added to the network links to utilize the delay test also.

The overall result from the implementation point of view was positive, since the method could actually be implemented to the routers and they do provide better performance for the flows.

3.7 Summary

This chapter has discussed some of the problems when providing QoS for multicast flows. These problems include the management of heterogeneous multicast trees, scalability, many-to-many multicast and the neglected reserved sub-tree (NRS) problem. All of these problems have been studied quite thoroughly in

RFC 3754, and solutions for each problem have been proposed. The document, however, leaves the question of the actual multicast admission control method open. For this reason, basic guidelines and exact methods for solving the problem have been presented here. Probably the most important instructions when creating a multicast admission control method is that only the path between the branching node and the new receiver should be examined in the bandwidth test. In the delay tests, the same applies to the active measurements. Passive methods, on the other hand, do provide more accurate results when multicast is considered. This is because the addition of new multicast group for the measurements increases the load of the network. Also, passive measurements of the unicast traffic do not provide enough accurate results, because multicast traffic is usually treated differently in the routers. The methods do provide good instructions on how to implement a multicast admission control policy for a DiffServ network.

The methods indicate that separate policies for handling multicast admission control are needed and by using some method, the QoS can be provided for multicast receivers. It is also worth mentioning that the existing unicast admission control methods are not enough for multicast purposes.

4 CONCLUSIONS AND FUTURE RESEARCH

The search for true end-to-end Quality-of-Service for real-time applications in the Internet continues. To build a world-wide network with a possibility to guarantee the service level for all the users is still a dream, but it is getting closer all the time. The fixed-mobile convergence of the access networks has also been making the task of E2E QoS more complicated. Also the existence of real-time network applications provide their own limits and challenges for QoS architectures. Many pieces on this puzzle are waiting for solutions, and this thesis has presented some of them. Based on the previous research and the studies presented in this thesis, the goal can be reached, but it will still take some time.

It has also been said sometimes that there is no need for QoS in the networks and that traditional best effort with enough capacity is enough. Right now this might be true, but with the use of video and other bandwidth consuming services becoming more common the traffic will grow in the future. Also the competition over the market shares will grow and quality will probably be one of the important competitive factors for network and content providers.

The particular issues considered in this thesis included QoS on IEEE 802.16 access networks and admission control for multicast traffic. Both of them are very important issues on providing triple play services to both wired and wireless networks. The 802.16 studies in Chapter 2 have presented several concrete methods to improve the service level of users while still maximizing the utilization of the network and minimizing the overhead produced by the over-provisioning. Multicast admission control dealt with in Chapter 3 includes general guidelines and policies that should be taken into account when designing or implementing a multicast admission control method. These results and conclusions can be used on any QoS architecture with some small modifications.

Studies on the 802.16 QoS issues are currently being continued by us and more results will appear for the research community soon. The specific topics that will be studied next include:

- Pricing based scheduling for maximizing the revenue of a network operator
- Multicast polling with adaptive backoff parameter tuning

- Admission control simulations
- Uplink scheduler for subscriber stations
- Integration of 802.16 network to core QoS architecture, such as DiffServ, IntServ or IntServ over DiffServ
- Validation of the VoIP simulation results with the MOS calculations

YHTEENVETO (FINNISH SUMMARY)

Tässä väitöskirjassa käsitellään palvelunlaatua monimuotoisissa langattomissa ja kiinteissä verkoissa. Pääasiassa käsitellyt sovellukset ovat Internet-puhelut ja Internet-televisio ja tutkimuksessa on keskitytty niiden asettamien vaatimusten, ongelmien ja ratkaisuiden käsittelyyn.

Väitöskirjan ensimmäisessä osassa on kerrottu WiMAX-nimisen uuden verkoteknologian toiminta ja ominaisuudet, joiden avulla kyseisissä verkoissa kyetään takaamaan käytäjille aitoa päästä päähän palvelunlaatua. Myös tekniikan määrävän IEEE 802.16 standardin avoimeksi jättämiä kohtia on ratkaistu ja esitelty oikeita käyttötapoja eri ominaisuuksille. Kaikki tässä työssä esitellyt menetelmät on todettu hyviksi analyyttisen tarkastelun sekä laajojen simulaatioiden avulla. Menetelmät sisältävät skedulointi-algoritmin tukiasemalle, kilpavaraustekniikkaan liittyvien parametrien optimoinnin sekä *Multicast Polling* ominaisuuden parametrien optimoinnin. Luvun tulokset mahdollistavat WiMAX-verkkojen asiakkaille paremman palvelunlaadun ja operaattorin optimaalisen kaistan käytön.

Väitöskirjan toisessa osassa on esitelty ryhmälähetystekniikan ja eriytettyjen palveluiden arkkitehtuuriin liittyvä ongelmakenttä. Koska yhteen ongelmista, eli ryhmälähetysvastaanottajien pääsynhallintaan, ei aiemmin ole esitetty varsinaista pääsynhallinta-algoritmia, tässä työssä annetaan ohjeta sellaisen luomiseen. Tutkimuksessa on esitelty myös muutamia vaihtoehtoisia mentelmiä, sekä niiden heikkouksia ja vahvuuksia simulaatio-tulosten perusteella. Tämän osan tulokset ovat tärkeitä varsinkin Internet-televisiolähetysten kannalta.

REFERENCES

[1] A. Agarwal and K. B. Wang. Supporting quality of service in IP multicast networks. *Computer Communications*, 26:1533–1540, Sep 2003.

[2] H.S. Alavi, M. Mojdeh, and N. Yazdani. A quality of service architecture for IEEE 802.16 standards. In *Proceedings of the Asia-Pacific Conference on Communication*, pages 249–253, Oct 2005.

[3] F. Baker, C. Iturralde, F. Le Faucher, and B. Davie. Aggregation of RSVP for IPv4 and IPv6 reservations. IETF RFC 3175, Sep 2001.

[4] A. Ballardie. Scalable multicast key distribution. IETF RFC 1949, May 1996.

[5] Y. Bernet. Format of the RSVP DCLASS object. IETF RFC 2996, Nov 2000.

[6] B.N. Bhandaril, R. V. R. Kumar, and S.L. Maskara. Performance of the IEEE 802.16 MAC protocol with varying request backoff start. In *Proceedings of the IEEE Region 10 Conference TENCON*, pages 1–4, Nov 2006.

[7] G. Bianchi and N. Blefari-Melazzi. Admission control over assured forwarding phbs: a way to provide service accuracy in a diffserv framework. In *Proceedings of the IEEE Global Telecommunications Conference*, volume 4, pages 2561–2565, Nov 2001.

[8] G. Bianchi, N. Blefari-Melazzi, G. Bonafede, and E. Tintinelli. QUASIMODO: quality of service-aware multicasting over diffserv and overlay networks. *IEEE Network*, 17:38–45, Jan/Feb 2003.

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

[10] R. Bless, K. Nichols, and K. Wherle. A lower effort per-domain behaviour (PDB) for differentiated services. IETF RFC 3662, Dec 2003.

[11] R. Bless and K. Wehrle. Ip multicast in differentiated services (ds) networks. IETF RFC 3754, Apr 2004.

[12] J.-Y. Le Boudec and P. Thiran. *Network Calculus*. Springer, 2001.

[13] R. Braden, D. Clark, and S. Shenker. Integrated Services in the Internet Architecture: an Overview. IETF RFC 1633, Jun 1994.

[14] L. Breslau, S. Jamin, and S. Shenkers. Measurement-based admission control: What is the research agenda. In *Proceedings of the Seventh International Workshop on Quality of Service*, pages 3–5, May/Jun 1999.

[15] L. Breslau, S. Jamin, and S. Shenkers. Comments on performance of measurement-based admission control algorithms. In *Proceedings of the Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies*, volume 3, pages 1233–1242, Mar 2000.

[16] M. Brunner. Requirements for signaling protocols. IETF RFC 3726, Apr 2004.

[17] G. Chaddoud and V. Varadharajan. Efficient secure group management for SSM. In *Proceedings of the 27th Annual IEEE Conference on Local Computer Networks*, volume 3, pages 1436–1440, Jun 2004.

[18] K. Chan, R. Sahita, S. Hahn, and K. McCloghrie. Differentiated services Quality of Service policy information base. IETF RFC 3317, Mar 2003.

[19] K. Chan, J. Seligson, D. Durham, S. Gai, K. McCloghrie, S. Herzog, F. Reichmeyer, R. Yavatkar, and A. Smith. COPS usage for policy provisioning (COPS-PR). IETF RFC 3084, Mar 2001.

[20] B.-J. Chang and C.-M. Chou. Adaptive polling algorithm for reducing polling delay and increasing utilization for high density subscribers in WiMAX wireless networks. In *Proceedings of the 10th IEEE Singapore International Conference on Communication systems*, pages 1–5, Oct 2006.

[21] J. Chen, W. Jiao, and Q. Guo. An integrated QoS control architecture for IEEE 802.16 broadband wireless access systems. In *Proceedings of the IEEE Global Telecommunications Conference*, volume 6, pages 3330–3335, Nov/Dec 2005.

[22] J. Chen, W. Jiao, and H. Wang. A service flow management strategy for IEEE 802.16 broadband wireless access systems in TDD mode. In *Proceedings of the IEEE International Conference on Communications*, volume 5, pages 3422–3426, May 2005.

[23] D.-H. Cho, J.-H. Song, M.-S. Kim, and K.-J. Han. Performance analysis of the IEEE 802.16 wireless metropolitan area network. In *International Conference on Distributed Frameworks for Multimedia Applications*, pages 130–136, Feb 2005.

[24] C.-M. Chou, B.-J. Chang, and Y.-F. Huang. Dynamic polling access control for high density subscribers in wireless WiMAX networks. In *Proceedings of the Taiwan Network Conference*, Nov 2006.

[25] G. Chu, D. Wang, and S. Mei. A QoS architecture for the MAC protocol of IEEE 802.16 BWA system. In *Proceedings of the IEEE International Conference on Communications, Circuits, and Systems*, volume 1, pages 435–439, Jun/Jul 2002.

[26] M. E. Crovella and A. Bestavros. Self-similarity in world wide web traffic: Evidence and possible causes. *IEEE/ACM Transactions on Networking*, 5:835–846, Dec 1997.

[27] B. Davis, A. Charny, J.C.R. Bennett, K. Benson, J.Y. Le Boudec, W. Courtney, S. Davari, V. Firoiu, and D. Stiliadis. An expedited forwarding PHB (per-hop behavior). IETF RFC 3246, Mar 2002.

[28] L.F.M. de Moraes and P.D. Maciel Jr. Analysis and evaluation of a new MAC protocol for broadband wireless access. In *International Conference on Wireless Networks, Communications, and Mobile Computing*, volume 1, pages 13–16, Jun 2005.

[29] S. Deering. Host extensions for ip multicasting. IETF RFC 1112, Aug 1989.

[30] D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, and A. Sastry. The COPS (common open policy service) protocol. IETF RFC 2748, Jan 2000.

[31] A. Fei, J. Cui, M. Gerla, and M. Faloutsos. Aggregated multicast: an approach to reduce multicast state. In *Proceedings of the IEEE Global Telecommunications Conference*, pages 1595–1599, Nov 2001.

[32] M. Fidler and V. Sander. A parameter based admission control for differentiated services networks. *Computer Networks*, 44:463–497, Mar 2004.

[33] F. Fitzek and M. Reisslein. Mpeg-4 and h.263 video traces for network performance evaluation, Nov/Dec 2001.

[34] Gartner. Forecast: Iptv subscribers and service revenue, North America, 2005-2011, Jul 2007.

[35] S. Georgoulas, P. Trimintzios, and G. Pavlou. Admission control placement in differentiated services networks. In *Proceedings of the Ninth International Symposium on Computers and Communications*, volume 2, pages 816–821, Jun/Jul 2004.

[36] T. Kwon H. Lee and D.-H. Cho. Extended-rtPS algorithm for VoIP services in IEEE 802.16 systems. In *Proceedings of the 10th IEEE Singapore International Conference on Communication systems*, volume 5, pages 2060–2065, Oct 2006.

[37] M. El Hachimi, A. Abouaissa, P. Lorenz, and R. Sathya. Control algorithm for QoS based multicast in diffserv domain. In *Proceedings of the International Conference on Communication Technology*, volume 1, pages 225–230, Apr 2003.

[38] H. Harney and C. Muckenhirn. Group key management protocol (gkmp) architecture. IETF RFC 2094, Jul 1997.

[39] M. Hawa and D.W. Petr. Quality of service scheduling in cable and broadband wireless access systems. In *Proceedings of Tenth IEEE International Workshop on Quality of Service*, pages 247–255, May 2002.

[40] J. He, K. Guild, K. Yang, and H.-H. Chen. Modeling contention based bandwidth request scheme for IEEE 802.16 networks. *IEEE Communications Letters*, 11:689–700, Aug 2007.

[41] J. Heinanen, F. Baker, W. Weiss, and J. Wroclawski. Assured forwarding PHB group. IETF RFC 2597, Jun 1999.

[42] Air interface for fixed broadband wireless access systems. IEEE Standard 802.16, Jun 2004.

[43] Air interface for fixed broadband wireless access systems - amendment for physical and medium access control layers for combined fixed and mobile operation in licensed bands. IEEE Standard 802.16e, Dec 2005.

[44] In-Stat. Iptv in asia: Carriers start the battle, May 2007.

[45] N. Ishikawa, N. Yamanouchi, and O. Takahashi. An architecture for user authentication of ip multicast and itsimplementation. In *Proceedings of the Internet Workshop*, pages 81–87, Feb 1999.

[46] Pulse code modulation (PCM) of voice frequencies. ITU-T recommendation G.711, 1988.

[47] Artificial conversational speech. ITU-T recommendation P.59, 1993.

[48] Q. Guo J. Chen, W. Jiao. Providing integrated QoS control for IEEE 802.16 broadband, wireless, access systems. In *Proceedings of the IEEE 62nd Vehicular Technology Conference*, volume 2, pages 1254–1258, Sep 2005.

[49] S. Jamin, B. Danzigp, S. Shenkers, and L. Zhang. A measurement-based admission control algorithm for integrated services packet networks. *IEEE/ACM Transactions on Networking*, 5:56–70, Feb 1997.

[50] C.-H. Jiang and T.-C. Tsai. Token bucket based CAC and packet scheduling for IEEE 802.16 broadband wireless access networks. In *Proceedings of the 3rd IEEE Consumer Communications and Networking Conference*, volume 1, pages 183–187, Jan 2006.

[51] Y. Jiang, A. Nevin, and P.J. Emstad. Implicit admission control for a differentiated services network. In *Proceedings of the 2nd Conference on Next Generation Internet Design and Engineering*, Apr 2006.

[52] S.-J. Kim, W.-J. Kim, and Y.-J. Suh. An efficient bandwidth request mechanism for non-real-time services in ieee 802.16 systems. In *Communication Systems Software and Middleware, 2007. COMSWARE 2007. 2nd International Conference on*, pages 1–9, Jan 2007.

[53] B.J. Kwak, N.O. Song, and L.E. Miller. Performance analysis of exponential backoff. *IEEE/ACM Transactions on Networking*, 13:343–355, Apr 2005.

[54] J. Lakkakorpi. Simple measurement-based admission control for diffserv access networks. In *Proceedings of International Conference on Internet, Performance & Control of Networks*, Jul 2002.

[55] J. Lakkakorpi, J. Moilanen, J. Karhula, A. Sayenko, and O. Alanen. Active queue management for reducing downlink delays in WiMAX. In *Proceedings of the 66th IEEE Vehicular Technology Conference*, Sep/Oct 2007.

[56] J. Lakkakorpi, O. Strandberg, and J. Salonen. Adaptive connection admission control for differentiated services access networks. *IEEE Journal on Selected Areas in Communications*, 23:1963–1972, Oct 2005.

[57] H. Lee, T. Kwon, and D.-H. Cho. An efficient uplink scheduling algorithm for voip services in IEEE 802.16 BWA systems. In *Proceedings of the IEEE 60th Vehicular Technology Conference*, volume 5, pages 3070–3074, Sep 2004.

[58] H. Lee, T. Kwon, D.-H. Cho, G. Lim, and Y. Chang. Performance analysis of scheduling algorithms for voip services in IEEE 802.16e systems. In *Proceedings of the IEEE 63th Vehicular Technology Conference*, volume 3, pages 1231–1235, May 2006.

[59] R. Lehtonen and J. Harju. Controlled multicast framework. In *Proceedngs of the 27th Annual IEEE Conference on Local Computer Networks*, pages 565–570, Nov 2002.

[60] Z. Li and P. Mohapatra. QoS-aware multicasting in diffserv domains. *ACM SIGCOMM Computer Communication Review*, 34:47–57, Oct 2004.

[61] L. Lin, W. Jia, and W. Lu. Performance analysis of IEEE 802.16 multicast and broadcast polling based bandwidth request. In *Proceedings of the IEEE Wireless Communications and Networking Conference*, pages 1854–1859, Mar 2007.

[62] N. Liu, X. Li, and B. Young C. Pei. Delay character of a novel architecture for IEEE 802.16 systems. In *Proceedings of the Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies*, pages 293–296, Dec 2005.

[63] K. Nichols, V. Jacobson, and L. Zhang. A two-bit differentiated services architecture for the Internet. IETF RFC 2638, Jul 1999.

[64] D. Niyato and E. Hossain. Joint bandwidth allocation and connection admission control for polling services in IEEE 802.16 broadband wireless networks. In *Proceedings of the IEEE International Conference on Communications*, volume 12, pages 5540–5545, Jun 2006.

[65] D. Niyato and E. Hossain. Queue-aware uplink bandwidth allocation and rate control for polling service in IEEE 802.16 broadband wireless networks. *IEEE Transactions on Mobile Computing*, 5:668–679, Jun 2006.

[66] S.-M. Oh and J.-H. Kim. The analysis of the optimal contention period for broadband wireless access network. In *Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications Workshops.*, pages 215–219, Mar 2005.

[67] A. Sayenko. *Adaptive scheduling for the QoS supported networks*. PhD thesis, University of Jyväskylä, Finland, 2005.

[68] A. Sayenko, V. Tykhomyrov, H. Martikainen, and O. Alanen. Performance analysis of the IEEE 802.16 ARQ mechanism. In *Proceedings of the 10th IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, Oct 2007.

[69] A. Sayenko, V. Tykhomyrov, H. Martikainen, O. Alanen, and T. Hämäläinen. Performance evaluation of the WiMAX ARQ mechanism. In *Proceedings of the 7th International Conference on Next Generation Teletraffic and Wired/Wireless Advanced Networking*, Sep 2007.

[70] J.-B. Seo, N.-S. Lee, N.-H. Park, H.-W. Lee, and C.-H. Cho. Performance analysis of IEEE 802.16d random access protocol. In *Proceedings of the IEEE International Conference on Communications*, volume 12, pages 5528–5533, Jun 2006.

[71] Y. Snir, Y. Ramberg, J. Strassner, R. Cohen, and B. Moore. Policy Quality of Service (QoS) information model. IETF RFC 3644, Nov 2003.

[72] D. Stiliadis and A. Varma. Latency-rate servers: a general model for analysis of traffic scheduling algorithms. *IEEE/ACM Transactions on Networking*, 6:611–624, Oct 1998.

[73] A. Striegel. *Scalable approaches for DiffServ multicasting*. PhD thesis, University of Notre Dame, Nov 2002.

[74] A. Striegel, A. Bouabdallah, H. Bettahar, and G. Manimaran. EBM: a new approach for scalable diffserv multicasting. *Lecture Notes in Computer Science*, 2816:131–142, Feb 2004.

[75] A. Striegel and G. Manimaran. A scalable approach for diffserv multicasting. In *Proceedings of the IEEE International Conference on Communications*, volume 8, pages 2327–2331, Jun 2001.

[76] A. Striegel and G. Manimaran. Dynamic DSCPs for heterogeneous QoS in diffserv multicasting. In *Proceedings of the IEEE Global Telecommunications Conference*, volume 3, pages 2123–2127, Nov 2002.

[77] Aaron Striegel. Genmcast software extension for the NS-2 simulator. `http://www.cse.nd.edu/striegel/GenMCast/`.

[78] H.-C. Su and R.-H. Hwang. Multicast provision in a differentiated services network. In *Proceedings of the 15th International Conference on Information Networking*, pages 189–196, Jan/Feb 2001.

[79] A.S. Sudhir, G. Manimaran, and P. Mohapatra. Heterogeneous QoS multicast in diffserv-like networks. In *Proceedings of the 14th International Conference on Computer Communications and Networks*, pages 139–144, Oct 2005.

[80] D. Tarchi, R. Fantacci, and M. Bardazzi. Quality of service management in IEEE 802.16 wireless metropolitan area networks. In *Proceedings of the 10th IEEE Singapore International Conference on Communication systems*, volume 5, pages 3070–3074, Sep 2004.

[81] UCB/LBNL/VINT. Network simulator ns-2, 1997. `http://www.isi.edu/nsnam/ns`.

[82] H. Wang, W. Lei, and D. Argawal. Dynamic admission control and QoS for 802.16 Wireless MAN. In *Proceedings of the Wireless Telecommunications Symposium*, pages 60–66, Apr 2005.

[83] K. Wongthavarawat. IEEE 802.16 based last mile broadband wireless military networks with quality of service support. In *Proceedings of the IEEE Military Communications Conference*, volume 2, pages 779–784, Oct 2005.

[84] J. Wroclawski. The use of RSVP with IETF integrated services. IETF RFC 2210, Sep 1997.

[85] S.A. Xergias, N. Passas, and L. Merakos. Flexible resource allocation in IEEE 802.16 wireless metropolitan area networks. In *Proceedings of the 14th IEEE Workshop on Local and Metropolitan Area Networks*, pages 1–6, Sep 2005.

[86] XORP Project. Xorp - extensible open router platform, 2007. `http://www.xorp.org/`.

[87] J. Yan and G.-S. Kuo. Cross-layer design of optimal contention period for IEEE 802.16 BWA systems. In *Proceedings of the IEEE International Conference on Communications*, volume 4, pages 1807–1812, Jun 2006.

[88] B. Yang and P. Mohapatra. Diffserv-aware multicasting. *Journal of High Speed Networks*, 13(1):37–57, Jan 2004.