Universidade de Aveiro Departamento de Electrónica, Telecomunicações e Informática
2009

Tiago Silvestre Condeixa

AVALIAÇÃO DE CONTROLO DE SESSÕES MULTICAST EM REDES COM CONTEXTO

Universidade de Aveiro
2009
Departamento de Electrónica, Telecomunicações e Informática

Tiago Silvestre Condeixa

AVALIAÇÃO DE CONTROLO DE SESSÕES MULTICAST EM REDES COM CONTEXTO

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Electrónica e Telecomunicações, realizada sob a orientação científica da Prof. Dra. Susana Sargento, Professora auxiliar do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro, e do Prof. Dr. Augusto Neto, Professor adjunto do Instituto de Informática da Universidade Federal de Goiás, Brasil, e colaborador no Instituto de Telecomunicações de Aveiro.

Dedico este trabalho aos meus Pais, Irmã e Namorada.

O júri

Presidente	Prof. Doutor Nuno Miguel Gonçalves Borges de Carvalho Professor Associado do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro.
Orientadora	Prof. Doutora Susana Isabel Barreto de Miranda Sargento Professora Auxiliar do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro.
Vogal	Prof. Doutora Maria João Mesquita Rodrigues da Cunha Nicolau Pinto Professora Auxiliar do Departamento de Sistemas de Informação da Escola de Engenharia da Universidade do Minho.

Agradecimentos

Antes de mais gostaria de agradecer à minha família que sempre me apoiou e me deu força para superar esta etapa tão importante da minha vida.

À minha namorada que esteve sempre presente nos momentos mais difíceis, mostrando ser muito compreensiva e carinhosa.

Ao Nuno Coutinho e ao João Mateiro que me ajudaram imenso através da experiência obtida, estando sempre disponíveis para me ajudar a compreender questões técnicas relativas ao simulador e até mesmo questões mais conceptuais. Ao Rui Valbom que foi um amigo e companheiro com o qual partilhei muitas horas no desenvolvimentos do nosso projecto no Simulador de Redes. Ainda um muito obrigado aos colegas do meu laboratório que se mostraram sempre prestáveis em tirar dúvidas mais genéricas na elaboração do trabalho.

À professora Susana Sargento e ao Augusto Neto que se mostram uns verdadeiros orientadores, estando sempre disponíveis para qualquer dúvida que surgisse. Agradeço a forma como me cativaram e me apoiaram ao longo de todo o trabalho, imprescindíveis para contornar problemas e encontrar soluções.

Finalmente um muito obrigado a todas as pessoas que por diferentes razões, directa ou indirectamente, contribuíram para que esta dissertação fosse realizada

Palavras-chave Multicast, Mobilidade, QoS, IPT, NUM, MTO, CB, Contexto, AP, NS.

Resumo

Os utilizadores pretendem aceder, cada vez mais, a serviços multimédia com requisitos mais exigentes e personalizados. As limitações impostas pelos ambientes existentes (internet, 3G) para fornecer estes serviços levam à procura de melhores soluções, nomeadamente uma gestão eficaz das sessões *multiparty*. Neste tipo de soluções é normalmente utilizado o *multicast*, já que este permite reduzir os recursos utilizados, diminuindo o número de pacotes na rede. Contudo, o *multicast* não está consistente ao nível dos cenários de mobilidade, fundamentais nas redes de próxima geração.

Actualmente existe uma vasta gama de tecnologias de acesso sem fios como WiFi, GPRS, UMTS e WiMAX. No futuro estas tecnologias diferentes complementar-se-ão convergindo numa infra-estrutura heterogénea capaz de fornecer um melhor serviço aos utilizadores, denominadas de redes 4G. A evolução dos terminais móveis também permitirá que estes se liguem simultaneamente a várias redes de acesso. Para uma melhor distribuição dos serviços dos utilizadores pelas redes de acesso disponíveis são necessários novos mecanismos de selecção. Uma nova selecção da rede baseada em informação de contexto (entidades e ambiente) tem tido grande relevo na comunidade científica. Assim, aplicações e rede reagem a alterações de contexto para uma melhor selecção da mesma.

A dissertação apresentada encontra-se no âmbito do transporte *multiparty* com informação de contexto e reserva de recursos, permitindo a entrega do conteúdo de uma forma personalizada e com Qualidade de Serviço a vários utilizadores móveis, independentemente da tecnologia de acesso de cada um e da própria tecnologia da rede. Em suma, é utilizada uma arquitectura de rede baseada em informação de contexto e que reage eficazmente a alterações do mesmo.

De forma a implementar a proposta apresentada recorreu-se à criação de várias entidades no simulador de redes NS-2. Os resultados foram obtidos usando diferentes cenários, avaliando a influência de cada parâmetro individualmente. Demonstrou-se que a arquitectura implementada permite suportar uma entrega dos conteúdos de uma maneira personalizada e independente da tecnologia utilizada. Obteve-se ainda uma boa gestão dos recursos da rede e uma melhoria na experiência percepcionada pelo utilizador através da selecção total da rede com base numa entidade de controlo central. A introdução do *overlay* de transporte *multiparty* melhora o comportamento geral da rede, minimizando as reconfigurações frequentes necessárias.

Keywords Multicast, Mobility, QoS, IPT, NUM, MTO, CB, Context, AP, NS.

Abstract

Nowadays, more and more users want to access multimedia services with strong and personalized requirements. The limitations intrinsic to current environments (Internet and 3G) to provide this type of services motivate the research for an efficient management of multiparty sessions. The solution can also be based on multicast implementation, since it reduces resources utilization, decreasing the number of packets in the network. However, current multicast is not a strong solution in mobility scenarios, essential in next generation networks.

Currently there is a wide range of wireless access technologies such as WiFi, GPRS, UMTS and WiMAX. In the future, these different technologies will converge in a complementary manner forming a heterogeneous infrastructure able to offer a better service to its users, usually named 4G. The evolution of mobile terminals will also allow them to connect simultaneously to several access networks. In order to a better distribution of the users services throughout available access networks, new selection mechanisms are required. A new network selection based on context information (entities and environments) is having a relevant role in scientific community. So, applications and networks react according to context changes, improving network selection.

This Thesis is in the scope of context-aware multiparty transport with resources allocation, allowing the delivery of content in a personalized way with Quality of Service to several users, independently of the technology and the network. Resuming, the solution implements a context-aware network architecture that reacts efficiently to its changes.

In order to implement this architecture, new entities were created in the network simulator NS-2. The results were obtained using different scenarios, evaluating the influence of each parameter independently. It was demonstrated that the integration of several components, allows a delivery of contents in a personalized manner and independently of the technology. The results showed a better management of the network resources and users experience, throughout the total network selection, based on a central control unit. The multiparty transport overlay improves the network behaviour, minimizing the necessary frequent reconfigurations.

Table of Contents

Index of Figures

Index of Tables

Acronyms

	Acronym	Description
A		
	AAA	Authentication, Authorization and Accounting
	ABC	Always Best Connected
	AF	Assure Forwarding
	AHP	Analytic Hierarchical Process
	ALM	Application Layer Multicast
	AMT	Abstract Multiparty Transport
	AP	Access Point
	ASM	Any Source Multicast
	ASN	Access Service Network
B		
	BE	Best Effort
	BS	Base Station
	BT	Bi-directional Tunnelling
	BU	Binding Update
C		
	CB	Context Broker
	CBT	Core Base Tree
	C-CAST	Context-casting
	CID	Communication Identification
	CN	Correspondent Node
	CoA	Care of Address
	CoS	Class of Service
	CS	Circuit Switched
	CSN	Connectivity Service Network
	CTMS	Constraint Tree Migration Scheme

	CxP	Context Providers
D		
	DCF	Distributed Coordination Function
	DHCP	Dynamic Host Configuration Protocol
	DM	Dense Mode
	DMSP	Designated Multicast Service Provider
	DVMRP	Distance Vector Multicast Routing Protocol
E		
	EDCA	Enhanced Distribution Coordinate Access
	EF	Expedited Forwarding
	ESS	Extended Service Set
F		
	FA	Foreign Agent
	FFD	First Fit Decreasing
	FMIP	Fast Mobile Internet Protocol
G		
	GGSN	Gateway GPRS Support Node
	GPRS	General Packet Radio Services
	GW	gateway
H		
	HA	Home Agent
	HC	Hybrid Coordinator
	HCCA	Controlled Channel Access
	HCF	Hybrid Coordination Function
	HMIP	Hierarchical Mobile Internet Protocol
	HMMCT	Hierarchical Mobile Multicast Concept Transfer
I		
	IGMP	Internet Group Management Protocol
	IP	Internet Protocol
	ISP	Internet Service Provider

L

LMA	Local Mobility Anchor

M

MA	Mobile Agent
MAC	Medium Access Control
MADCAP	Multicast Address Dynamic Client Allocation Protocol
MADM	Multiple Attribute Decision Making
MAG	Mobile Access Gateway
MBGP	Multiprotocol Border Gateway Protocol
MBMS	Multimedia Broadcast Multicast Service
MEW	Multiplicative Exponent Weighting
MIP	Mobile Internet Protocol
MIRA	Multi-service Resource Allocation
MLD	Multicast Listener Discovery
MMROP	Mobile Multicast with Routing Optimization
MN	Mobile Node
MobiCast	Multicast Scheme for Wireless Networks
MoM	Mobile Multicast
MOSPF	Multicast Open Shortest Path First
MRIB	Multicast Routing Information Base
MS	Mobile Station
MSS	Multicast Subscription System
MT	Mobile terminal
MTO	Multiparty Transport Overlay

N

NAM	Network Animator
NGN	Next Generation Networks
NRS	Neglected Reservation Sub-tree
NS	Network Simulator
NUM	Network Use Management

O

ON	Overlay Node
OSMAR	Overlay for Source-Specific Multicast in Asymmetric Routing

P

PCF	Point Coordination Function
PDA	Personal Digital Assistance
PDB	Per-domain Behaviour
PDP	Packet Data Protocol
PHB	Per-Hope Behaviour
PIM	Protocol Independent Multicast
PMIP	Proxy Mobile Internet Protocol
PoA	Point of Access
PS	Packet Switched
PTM	point-to-multipoint
PTP	point-to-point

Q

QAP	QoS-Access Point
QoE	Quality of Experience
QoS	Quality of Service

R

RAT	Radio Access Technology
RIB	Routing Information Base
RO	Route Optimization
RP	*Rendezvous* Point
RS	Remote Subscription
RSVP	Resource Reservation Protocol

S

SAM	Scalable Adaptive Multicast
SAW	Simple Additive Weighting
SDU	Service Data Unit

	SF	Service Flow
	SFM	Source Filtered Multicast
	SM	Session Management
	SS	Subscribe Station
	SSM	Source Specific Multicast
T		
	TIM	Traffic Indication Messages
	TNCP	Terminal Network Context Provider
	TOPSIS	Technique for Order Preference by Similar to Ideal Solution
	TS	Traffic Streams
	TSPEC	Traffic Specification
	TXOP	Transmission Opportunities
U		
	UE	User Equipment
	UP	User Priorities
W		
	WLAN	Wireless Local Area Network

1. Introduction

1.1. Motivation

Nowadays, Internet Service Providers (ISPs) focus their efforts in defining new types of services to attract customers, who are more and more demanding. Due to the increasing demand of multimedia content by groups of users, efficient solutions are under investigation, aiming to allow the efficient management of multiparty sessions, such as IPTV, file sharing and push media. The limitation of existing network architectures to efficiently fulfil the strong resource requirements of such real-time multimedia sessions (IPTV, video-conferencing) motivate the research community to propose new network functionalities.

Mobility makes part of our lives, having a more and more relevant role in future networks. Costumers want to receive multimedia content in everywhere at any time, never losing the connectivity, while they move around the world. NGNs have to be envisioned, taking into account totally mobile scenarios, changing to a new configuration at each moment.

Multicast is a good solution to avoid performance degradation and save resources in the network, since the routers in the network just duplicate packets when needed. The integration of multicast and mobility is crucial in future network environments. However, multicast is not yet consistent in mobile scenarios, and this should be solved, since next generation terminals equipments are essentially mobile.

Over the last few years, various access technologies, such as WiFi, GPRS, UMTS and WiMAX, have been deployed and are available or even yet integrated in mobile devices, which are increasingly equipped with several interfaces to the different technologies (multihomed). Due to these developments, the Next Generation Networks (NGNs) are envisaged to support a large range of multimedia sessions independently of the underlying network technologies.

Addressing current limitations of the network, new approaches emerged: context-awareness has recently attracted attention by the research community, since a wide number of information can be available, describing specific characteristics of entities and environments, such as devices, applications and places. This kind of information will have a strong influence on the services and their characteristics. Context-aware applications and networks should react to context changes to efficiently compute decisions according to the environment, session, users/terminals and networks characteristics. Always best connected (ABC) concept takes advantage of the context-awareness to select the best access point considering not only network

resources and application requirements, but also user situation and preferences, environment conditions, etc. In a more traditional networking viewpoint, efficient re-routing can be deployed when changes in context of networks and users/terminals are detected, such as link failures and terminal handovers, respectively. In the envisioned scenarios, preferences of users, their characteristics, location, mobility, and the environment, e.g. weather, noise, can influence the network attachment choice, re-routing and any other changes in the network.

To provide efficient real-time applications based on context information, it is important to create mechanisms in order to deliver personalized multiparty content through the chosen networks taking into account context information, and ensuring Quality-of-Service (QoS) guarantees: to reserve multicast paths and build multicast trees, it is necessary to choose an appropriate Access Point (AP) and the adequate core path, taking into account all context information, not only QoS information, but also users profiles/preferences and environment characteristics. Besides, it is necessary to assure that these mechanisms can be used independently of the core transport technology (IPv4/IPv6 and Unicast/Multicast) and access technology (WiFi, WiMAX, UMTS). Finally, the network needs to deal efficiently with all context changes, providing minimal impact in the network nodes.

1.2. Objectives

This Msc. Thesis is in the scope of the Context Casting (C-CAST) [1] project, more precisely the Context-aware Multiparty Transport and Network Resources Control components of the mentioned project. C-CAST proposes to design a new approach to allow personalized session content delivery to multiple mobile users with guaranteed resources, independent of the underlying network access and transport technologies, and taking into account context sources and information to optimize the content delivery.

In this Thesis, context-awareness is considered to allow the collection and delivery of information about mobile terminals, network and environment. This way, dynamic events can trigger session and network reactions, such as service and network re-configuration, multiparty session content delivery and re-negotiation, and seamless context-aware mobility. Resuming, the aim is to have a cognitive network driven by context, to efficiently react to context information and changes.

The aggregation of components, interfaces and functionalities for context-aware multiparty transport sub-system has to fulfil the aforementioned requirements. This can be made

by including capabilities to collect and make available context information, dynamically match and establish multiparty content sessions, allocate network resources in a scalable manner with support to self-organizing operations for resilience, and control terminal mobility seamlessly.

This thesis implements a new architecture based on a centralized approach, where a centralized intelligent entity performs decisions with respect to the best way to deliver data to users. Another central unit keeps all information (users profile, sources characteristics, environmental conditions and network resources) collected by terminals sensors. It uses an overlay layer to allocate resources and build multicast trees across the selected paths, and another to permit transparency to users in concerns to access technology and core configurations. It then builds the concept of abstract trees to prevent the change of the network due to the change in context: whenever it is possible to perform all required changes just resorting to local reactions, the abstract trees are not changed and the central nodes remain free to support other tasks. This architecture permits not only a correct delivery of the data content with minimum resources as possible and QoS guarantees, but also allows users and network operators to make their decisions according to their own preferences and policies.

In order to evaluate the proposed solution, Network Simulator (NS-2) was used. The use of simulation allows the evaluation of several scenarios with many different characteristics. It allows scalability performance assessment of the developed work which is not always possible with real hardware. Therefore, it was necessary to create and add new entities to NS in order to simulate the proposal architecture.

1.3. Contribution of this work

As a result of the accomplishment of the above proposed objectives, this work provides the following set of contributions:

- The development of a network architecture in the ns-2, which enables a NGN that supports efficient schemes to provide scalable content transport with QoS guarantees to several fixed/mobile terminals simultaneously.

- An evaluation, via simulation, of the global architecture performance in different fields and its response in different situations, in order to test the robustness and reliability of the developed solution.

1.4. Organization of the Thesis

The research work developed in this Thesis is organized in six main chapters. Each one explains briefly the work performed in different phases of the research, introduction, state-of-the-art, conceptual ideas, implementation, evaluation of the architecture and conclusion/future work.

Current chapter contextualizes the thesis in the current situation of the next generation networks paradigms. It also presents the goals and contributions of this Thesis.

The second chapter describes the current state-of-the-art developments in this research field. It consists in an overview of the multicast concepts and protocols, mobile IP and mobile multicast solutions, as well as current work in QoS and context-aware network selection mechanisms. An analysis of the developed work related with this Thesis is also presented.

The third chapter presents the main ideas, concepts, components and architecture of the C-CAST project. It also contextualizes this work in the project with the in-depth exposition of the guidelines and requirements.

The fourth chapter presents the architecture implementation performed in the Network Simulator (NS 2.31). This chapter is divided in sub-chapters, according to the different architecture components.

The fifth chapter presents an evaluation of the implementation made by testing the efficiency of the scheme as well as the performance of the network in several scenarios and conditions.

Finally, the last chapter summarizes the main results and a description of the performed research. It also describes future work to be carried out after this Thesis, issued from an evaluation of the deficiencies and possible improvements.

2. State of the Art

In our days, more and more new multimedia applications have appeared to satisfy different costumer demands, which require high bandwidth, low delay and small losses. As a result, it should be applied multicast in multimedia applications, in order to avoid redundant packets in the network, and consequently performance loss. QoS is strongly required in multimedia application progress, ensuring end-to-end requirements by efficiently distributing the different application flows throughout network resources. Mobility makes part of our lives, and Mobile Internet Protocol in version 4 (MIPv4) or version 6 (MIPv6) has a more and more relevant role in future networks. Recently, the concept of context-aware motivates large interests in scientific community, since it can consider all kind of environment and entities information, like places, applications and devices.

Section 2.1 will describe the concept of multicast as well as the protocols that support its functionalities. Section 2.2 will specially focus in MIPv4/MIPv6 and Multicast Mobility. Section 2.3 is related with network resources allocation in wired and wireless networks and its integration with multicast. Section 2.4 will analyse the existing proposals of network selection mechanisms based on context-awareness. Finally, Section 2.5 resumes this chapter.

2.1. Multicast Concept and Protocols

Multicast is centred in the concept of group, and multicast protocols are responsible for the delivery of information to multiple listeners without the need of sending several times the same data, increasing the efficiency and reducing costs, since it consumes less bandwidth. Listeners need to send a message identifying the multicast group, in order to receive the correspondent datagram that they desire, so the routers in the network just duplicate packets when needed. A unicast connection is based on a flow of information for each request, so if it has many hosts interested in receiving the same data flow, the data source will send many copies, one for each interested host. Obviously, unicast has a worst network performance compared with multicast, thus it is not the best solution for multimedia applications provided to several users simultaneously (Figure 1).

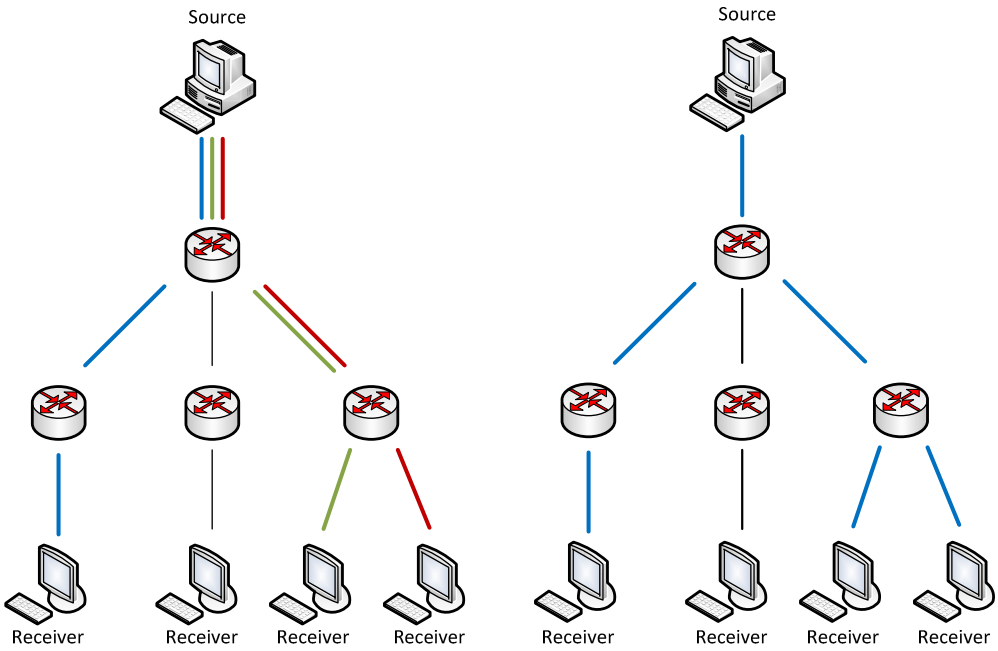

Figure 1- Unicast (left) and Multicast (right) models

Every multicast group is represented by an IP address from a well-defined range. In an IPv4 network, multicast IP uses the addresses of class D (224.0.0.0 to 239.255.255.255), while in IPv6, multicast addresses start with the hexadecimal prefix ff00:: / 8.

In spite of the advantages, the multicast process requires complex control mechanisms between network equipments. First, routers in the network need to support multicast protocols, in order to construct a multicast tree for each group and to forward and replicate multicast packets.

Multicast routing is implemented by protocols such as: Multicast Open Shortest Path First (MOSPF) [2], Distance-Vector Multicast Routing Protocol (DVMRP) [3], Core Based Tree (CBT) [4], and the most used, Protocol Independent Multicast (PIM) [5]. PIM presents two different versions, Sparse Mode (SM) and Dense Mode (DM), from different scenarios. While communication between routers is assured by the protocols mentioned, the communication between routers and hosts, or hosts and routers, is achieved by Internet Group Management Protocol (IGMP) [6] in IPv4 networks, or Multicast Listener Discovery (MLD) [7] in IPv6 networks. With a proper protocol, IGMP or MLD, sources inform their neighbour routers that they will send data to a certain group, and listeners, using the same protocol, inform their neighbour routers that they wish to join that group. By their turn, routers use a configured protocol to create or extend the multicast distribution tree of the desired group. Routers keep information about who

joins a certain group and the respective interfaces that they should use to forward packets to that group. If a user wishes to stop receiving the data flow, he leaves the group by sending an IGMP/MLD prune message to the neighbour router. If this user is the last in the group, the neighbour router informs its above routers, sending a prune message, to stop forwarding packets in its direction.

Recent IGMPv3 [8] or MLDv2 [9] protocols, where listeners can specify the source from which they want to receive, caused the appearance of the new multicast model, named Source Specific Multicast (SSM) [10].

The SSM models were proposed to solve the problems related to access control, address allocation, and handling of well-known sources generated by the Any-Source Multicast (ASM) and its deviation, the Source-Filtered Multicast (SFM). PIM-SSM became the preferred SSM model due to its simple architecture implementation, especially supported by the fact that it does not require a Rendezvous Point (RP). PIM-SSM creates the multicast distribution trees in a receiver-driven approach, based on a routing table called Multicast Routing Information Base (MRIB) [5], and relies on an underlying topology-gathering protocol for its population.

Usually, the unicast Routing Information Base (RIB) is used to get information about the multicast paths; however, they can also be provided by Multiprotocol Border Gateway Protocol (MBGP) [11] or other different protocols. The MRIB aims to provide the next-hop along a multicast-capable path so that any PIM Join message is sent to create the tree. Contrary to the RIB, MRIB gives reverse path information and indicates the itinerary that a multicast signalling packet would take from hosts to the data sources.

Recently, Application Layer Multicast (ALM) [12] [13] appears due to the very limited multicast support in routers within internet, being an attempt to use “multicast”. ALM uses some ideas of IP multicast as it transmits only one copy-packet per flow between end hosts via unicast, and just replicates the packets at end hosts. The ALM approach can be very motivating since it is not required an infrastructure to support intermediate nodes, and it does not cause any modification to the current network. Despite the flexibility and the easy deployment that ALM provides, it introduces performance issues and less stability comparing with multicast distribution trees [14].

The ALM is not scalable in large-scale networks due to its low bandwidth efficiency and heavy control overhead in comparison with a full multicast capable environment, caused by synchronization of transport at end hosts. Besides, it is difficult for an ISP to control member access and measure the bandwidth used by the group, because memberships and multicast

distribution trees are totally managed at end hosts. Consequently, the ALM models have a difficult or even impossible implementation cost [15], being not as efficient as IP multicast.

2.2. Mobility

The internet architecture is structured in protocol stack, which one of the most important protocols/layer is the IP. IP addresses are associated with the identification and localization of a terminal connected to the internet. This is the big problem that should be addressed with mobility concepts and ideas, trying to dissociate localization from identification. Networking base technologies were created on the assumption that the terminals would be stationary. If the terminal is connected to its home network and it wants to move to a new network, it is needed a reconfiguration of the IP address and gateway based on a new location, losing the network connections and communications during the process.

The NGN offers a heterogeneous environment focusing in the widespread of the mobile terminals (MT), always requiring constant network connectivity. Concerning these future environments, ABC services require an efficient mobility protocol to assure that their decision mechanisms can be executed seamlessly without downgrading the service provided.

This section will describe the current state-of-the-art of the Mobility, with special attention to Mobile IP (v4 and v6) and their solutions to multicast environments.

2.2.1. Mobile IP

The MIP protocol was first developed in the context of IPv4 [16] and presented as the first solution for the global mobility issue, being suitable for large movements. The architecture of this protocol is composed by Mobile Node (MN), Correspondent Node (CN), Home Agent (HA), Foreign Agent (FA) and the addresses Home Address (HoA) and Care-of Address (CoA). MN is the terminal that moves through the different networks, changing its access network. CN is the terminal that communicates with the MN. HA is typically a router in the home network of MN, which is responsible for registering the MN location, and FA is also a router, which is visited by the MN. HoA is the MN IP address in its home, and CoA is a temporary IP address acquired when the MN visits the foreign network.

In this protocol we have to use two different IP addresses, in order to maintain the MN reachable in the visited network. The home address is necessary when other hosts want to

communicate with the MN and it is permanently associated to it. The aim of the MIP protocol is to redirect, through IP tunnels, the packets received in the home network, to the foreign network, where the MN is temporary located.

IP-in-IP tunnels (in MIPv4) are dynamically managed, in order to allow the mobile host to appear accessible from its home address. MIP permits that applications designed for the traditional non-mobile Internet will continue to work even in mobile environments. The purpose of MIP protocol is to allow applications to keep communications between hosts, while roaming between different IP networks. While in standard IPv4 a movement would result in a loss of connectivity to the mobile host's, with MIP only a short disruption is perceived.

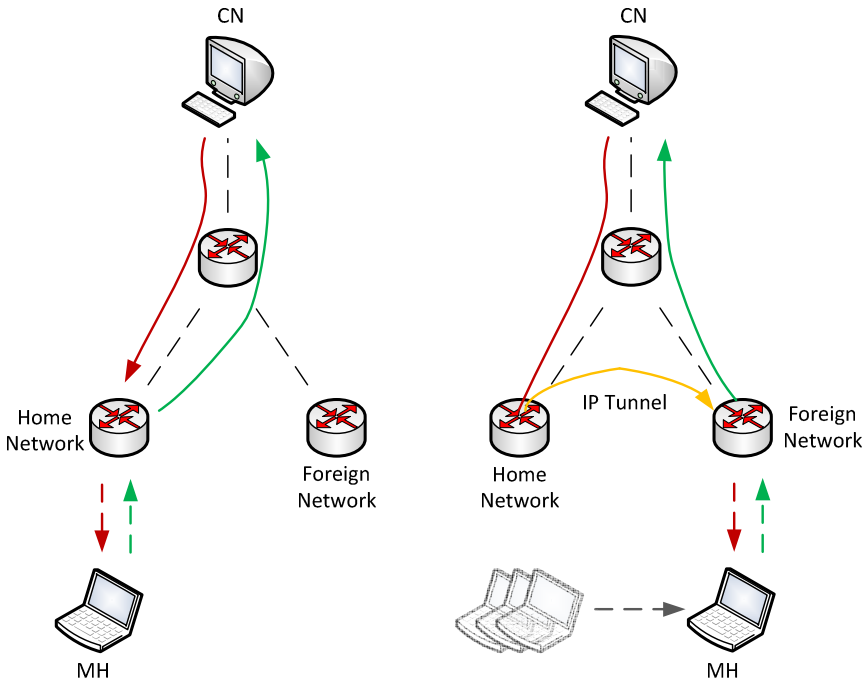

Figure 2 - MIP scenario

When a MN moves to a foreign network, the packets have to continue to be delivered to home network, and the receptive HA is responsible for sending them to the FA through an IP tunnel. When MN receives the packets, it replies to CN directly from its new location, creating a triangle routing (Figure 2). This is a weakness concerning the performance of MIP protocol, which can be solved by introducing a feature in the original protocol, named Route Optimization (RO) [17]. In original MIP scenario, CN never knows if MN moves from its home network, but with RO, CN gains the capacity of communicating directly with the MN. MN moves to a foreign network

and it sends a Binding Update (BU) message to the CN and the current location to HA at the same time.

In order to know the current location of MNs, CN needs to create a database with all CoAs of MNs, named Binding Cashes. If MN's CoA does not appear in CN database, CN uses the original process by sending all information to the HA of the MN.

The introduction of the RO feature causes a loss of transparency in the process (CN always knows current MN IP address), but it increases the efficiency and reduces delays and resources allocation.

The MIPv6 protocol [18] was developed in combination with IPv6, to solve the lack of efficiency caused by no native MIPv4 in the IPv4. This protocol is based on the same MIPv4 concepts, but with a better performance, due to the improvements of IPv6, comparing with IPv4, and also with the inclusion of RO as a native solution to the triangle routing. Besides, it does not require the FA to detect if it is in a foreign network, due to the simple use of IPv6 router advertisements. MN generates by itself the CoA when it moves to another network, using the stateless auto-configuration mode. This process is a new IPv6 feature that automatically obtains the needed information so that the MN may connect automatically when arriving to foreign network.

The MIPv6 is adopted as a standard solution for the global mobility support in the NGN, since it is an efficient solution that provides security and optimization features.

2.2.2. Multicast Mobility Solutions

Standard multicast protocols do not implement mobility in a native way, being necessary to use turn-around solutions to integrate mobility and multicast. This problem is solved with the introduction of minimal standard solutions as the Bi-directional Tunnelling (BT) and Remote Subscription (RS). Several publications propose a mixture of both solutions, implementing BT for source mobility and the RS for listener mobility. These mixed approaches, named Agent-based solutions, are the preferred ones by the research community to develop Mobile Multicast solutions [19].

BT solution proposes that mobile multicast source (MN) uses tunnels to redirect multicast data flow to its HA. When the HA receives the multicast packets from the tunnel, it sends packets using IP Multicast Routing on behalf of the mobile multicast source. This mobile multicast solution has the advantage of hiding all mobile multicast source movements, since the HA and multicast

trees remain static. Besides the transparency of BT with mobile multicast listeners and sources, this solution has a loss of performance due to its overhead on the network and a large delay of data delivering.

The RS strategy adopts an opposite solution that delivers all movement reconfiguration to multicast routing, in order to create/expand the multicast tree to new MN IP address.

When a MT enters a foreign network, it re-subscribes to its desired multicast group and the respective foreign multicast router has to join the multicast group to the multicast tree. This strategy offers an optimum routing: the multicast packets are sent directly to the respective local multicast router by an IP multicast. However, this solution could lead to significant overheads due to the reconstruction of the delivery multicast tree in case of frequent handovers.

This strategy forces the mobile node to re-initiate multicast distribution subsequent to handover. This approach of tree discontinuation relies on multicast dynamics to adapt to network changes, resulting in a rigorous service disruption and leading to mobility-driven changes of source addresses. In result, RT cannot be the solution to support session persistence under multicast source mobility.

Thereby, since these both approaches have their disadvantages, Agent-based solutions attempt to balance between the two mechanisms. Static agents typically act as local tunnelling proxies. Different types of Multicast Agent (MA) approaches have been proposed in order to reduce the reconstruction of the multicast tree. These agents join the multicast group on behalf of the multicast listeners along the different networks, providing multicast source movement transparency. When a multicast source moves and changes its current IP address to a new CoA, the multicast tree only needs to be re-established from the MA to the multicast source. Therefore, this reduces the multicast tree reconstruction, and consequently, the service disruption time. Unlikely, many of the proposed protocols are based on foreign agents and also on Mobile Ipv4 paradigm. As the Mobile IPv6 does not have any foreign agents, these protocols cannot be directly derived to IPv6 multicast mobility scenarios. There are some alternatives or extensions to the basic Mobile IP and IP multicast interoperability approaches proposed by the IETF. Each one of these examples improves the basic mechanisms, but further refinement is needed before these solutions can be widely deployed.

For the specific case of the multicast listener mobility, new approaches appear attempting to solve the related problems, dividing into Agent Assistance, Multicast Encapsulation and Hybrid Architecture.

Agent Assistance:

Agent assistance proposals use host-based mobility, since it complements the unicast real-time mobility existing infrastructures of Fast MIPv6 (FMIPv6) [20] and Hierarchical MIPv6 (HMIPv6) [21], becoming Multicast-FMIPv6 (M-FMIPv6) [22][23] and Multicast-HMIPv6 (M-HMIPv6)[24]. These solutions presume that the context information is saved in a node accessible before and after the movement. However, when a MN moves from one operator to another, it loses contact with the previous network, and it is necessary to find a solution to recover from loss of connectivity and context based on the node alone.

Proxy MIPv6 (PMIPv6) is a network based on mobility management that becomes multicast transparent in the sense that the MN experiences a point-to-point home link fixed at its (static) Local Mobility Anchor (LMA). This virtual home link is composed of a unicast tunnel between the LMA and the current Mobile Access Gateway (MAG), and a point-to-point link connecting the current MAG to the MN. A PMIPv6 domain thereby inherits MTU-size problems from spanning tunnels at the receiver site. Besides, some avalanche problems can be easily identified. The LMA may be required to tunnel data to a large number of MAGs, while a MAG may be needed to forward the same multicast stream to many MNs via individual point-to-point links. Future optimizations and extensions to share links preferably adapt native multicast distribution towards the edge network, possibly using a local routing option, including context transfer between access gateways to assist IP-mobility-agnostic MNs.

Multicast Encapsulation:

Encapsulation of multicast data packets is a recognized method to shield mobility and to enable access to remotely located data services, like streams from the home network. Applying generic packets tunnelling in IPv6 using a unicast point-to-point method will also allow multicast-agnostic domains to be transited, but does inherit the tunnel convergence problem and may result in traffic multiplication.

Multicast enables environments to take advantage of point-to-multipoint encapsulation, such as generic packet tunnelling, using an appropriate multicast destination address in the outer header. Such multicast-in-multicast encapsulated packets similarly enable reception of remotely located streams, but do not suffer from the scaling overhead from using unicast tunnels.

The tunnel entry point performing encapsulation should provide fragmentation of data packets, to avoid issues resulting from MTU size constraints within the networks supporting the tunnels.

Hybrid Architectures:

There has been recent interest in seeking methods that avoid the complexity at the Internet core network, like application layer and overlay proposals for (mobile) multicast. The possibility of integrating multicast distribution (overlay) into the network layer is also being considered by the IRTF Scalable Adaptive Multicast (SAM) Research Group (RG).

An early hybrid architecture using reactively operating proxy-gateways located at the Internet edges was introduced by Garyfalos and Almeroth [25]. The authors presented an Intelligent Gateway Multicast as a bridge between mobility-aware native multicast management in access networks and mobility group distribution services in the Internet core, which may be operated on the network or application layer. The Hybrid Shared Tree approach [26] introduced a mobility-agnostic multicast backbone on the overlay.

Current work in the SAM RG is developing general architectural approaches for hybrid multicast solutions [27] that will require a detailed design in the future work.

Mobile Multicast (MoM) Protocol:

MoM Protocol [28][29] is based on BT approach and it focus on solving the tunnel convergence trouble with the development of the Designated Multicast Service Provider (DMSP).

Each multicast group is associated with a particular DMSP, that is a HA between several HAs that forward packets to the visit network with the specific multicast IP group, and it is chosen by foreign network.

Mobile Multicast with Routing Optimization (MMROP):

MMROP [30] is supported by RS and it has a better routing efficiency and no packet roaming losses, since it applies a Mobility Agent (MA), which is a FA that forwards (via IP tunnel) lost packets to neighbouring networks.

Constraint Tree Migration Scheme (CTMS):

CTMS [31] is a new global multicast protocol based on the development of Core Based Tree to allow a dynamic multicast configuration. CMTS is applied to mobile multicast listeners and it automatically changes multicast trees to better ones, while maintaining the QoS guarantees specified by mobile users.

Multicast Scheme for Wireless Networks (MobiCast):

MobiCast [32] is based on RS and its key extension is the introduction of the Domain Foreign Agent (DFA), which serves many small adjacent wireless cells. A hierarchy is introduced with small cells being organized into one Dynamic Virtual Macrocell (DVM). Therefore, micro mobility is hidden from the global multicast mechanism, which does not require reconfiguration when handovers occur within the same DVM.

Mobile IPv6 Multicast with Dynamic Multicast Agent:

Mobile IPv6 Multicast with Dynamic Multicast Agent [33] approach tries to solve the problems of delivering IPv6 multicast traffic to MN. This approach combines the advantages of BT and RS, selecting a new multicast agent based on both movement and distance dynamically, and the new selected agent is responsible for forwarding multicast data to the MN. Such design optimizes the multicast routes and reduces handoff frequency. Besides releasing triangle route problem and diminishing the influence of handoff to multicast, it can also provide global mobility without limitations of the network topology.

Hierarchical Mobile Multicast Context Transfer (HMMCT):

HMMCT [34] is a new approach to reduce the signalling cost and reduce the packet loss, especially in case of macro mobility. This solution integrates HMIPv6 for the intra-domain mobility, with Mobile context transfer for the inter-domain mobility. The design assumes that the foreign network is a HMIPv6 environment so there will be a special router called Mobility Anchor Point (MAP), responsible for controlling the group membership for multicast listeners and receive the multicast packets intended to the mobile node then the it encapsulates them to the MN. HMMCT provides seamless handovers and reduces the disruption for the mobile nodes whether they move within the same or different MAP domains, and it allows MN to efficiently receive the packets during the handover, especially in real-time services and applications.

2.3. QoS

QoS is crucial to any network architecture and given the challenges envisioned for the NGNs, the provision of QoS in these environments will be a complex task. The implementation of this concept is achieved by increasing the priority of some flows and limiting the priority of other flows. Congestion management tools are able to distinguish flows with different priorities and

dispose them in different queues that have different ways of treatment. The queue management mechanism avoids congestion of queues by dropping lower-priority flows before higher-priority flows. Policing and shaping are also important QoS features to provide priority to a flow by limiting the throughput of other flows. Link efficiency tools limit large flows to show a preference for small flows.

Service levels refer to the actual end-to-end QoS capabilities, meaning the ability of the network to serve, according to agreed insurances, a specific kind of traffic from the source to the terminal or edge to edge. The services differ in their level of QoS strictness, which describes how tightly the service can be bound by specific bandwidth, delay, jitter, and loss characteristics.

To assure QoS in the network, it is deeply necessary to implement mechanisms to allocate and control resources. This section will particularly explain mechanisms to allocate multicast resources in wired networks, and also gives a brief overview about this thematic in wireless networks.

2.3.1. Multicast Resource Allocation Mechanisms

Multicast resource allocation is the set of methods that control the assignment of available multicast paths to correctly transport the incoming flows throughout multicast distribution trees. The control functions to create multicast distribution trees are usually receiver-driven encompassing messages which traverse a multicast-capable path. These messages carry multicast control information, which is the support to setup the packet replication on each node along the reverse-path of the Join messages, so that the data flows along the multicast-capable path. Before building a multicast distribution tree, it is necessary to allocate a multicast IP address to indentify the group. Multicast IP addresses can be dynamically allocated by using standard solutions, such as the Multicast Address Dynamic Client Allocation Protocol (MADCAP) [35]. MADCAP efficiently controls the dynamic allocation of multicast IP addresses, operating similarly to Dynamic Host Configuration Protocol (DHCP). However, MADCAP under SSM environments has significantly optimization problems of multicast address allocation, being well-known with many issues in multi-source scenarios.

The allocation of multicast resources in IP multicast is implemented in a per-flow basis, meaning that a multicast distribution tree is allocated to each micro-flow and created on-demand (e.g. for each Join received). The dependence of the number of flows poses scalability limitations to IP multicast in large-scale systems. For instance, the routing operation and forwarding slow

down with the increasing number of multicast state, due to the saturation of memory in the routers. Moreover, the excessive control overhead of IP multicast increases the bandwidth consumption and overloads CPU processing in each network node [36]. IP multicast has another barrier with regard to the competition of multicast groups, which leads to address space constraints in network layer protocols, such as IPv4.

In order to efficiently deploy QoS-aware multicast communications, it is required to implement solutions to control the allocation of QoS and multicast network resources, which is generally implemented separately, due to contradicting deployment concepts. With regard to multicast solutions, IP multicast is more deployed over the Internet and feasible for large-scale environments than ALM. The integrated deployment of differentiated services (DiffServ) [37] and IP multicast is promising, since the former allows a scalable QoS approach while the latter saves the bandwidth utilization by preventing packet duplication [37]. However, the integration of DiffServ and multicast is not trivial as will be described.

Whereas in the DiffServ model the scalability is achieved by pushing unavoidable complexity to network edges and maintaining per-class state in core nodes, multicast operates on a per-flow basis throughout the network. Furthermore, the dynamic addition of new members of the multicast group using DiffServ can adversely affect other existing traffic if resources were not explicitly allocated before use. This problem, called the Neglected Reservation Sub-tree (NRS), endangers or even violates the quality of the session in communication paths toward other receivers with previous correct reservations. Another reason that makes DiffServ and multicast integration difficult, deals with the reluctance of ISPs to deploy and provide multicast [15]. In spite of allowing the reduction in bandwidth utilization, many technical and marketing reasons make IP multicast (and its performance improvement extensions, such as multicast aggregation) still far from being widely deployed over the Internet. The most critical reasons include:

- The state scalability problems in large-scale networks;
- The lack of support in access control;
- The requirement of global deployment of multicast-capable IP routers;
- The lack of appropriate pricing models.

The deployment of real-time group communications with efficient use of network resources implies that multicast data should always travel in the best possible path. To accomplish this, routing asymmetries, as well as QoS requirements, should be considered when building multicast trees. However, these requirements are not accomplished by most IP multicast routing protocols. One of the reasons is that those protocols build multicast trees from the receivers to

the sender, while data travels in the reverse direction. The result is that data are forced to travel in a path that is not optimized and sometimes not even suitable (Figure 3). This fact may lead to a loss of performance and to the failure to deliver the quality levels expected by the users.

The routing asymmetries that cause this situation are a usual presence in the Internet [38] and can happen due to distinct factors, such as different paths for each direction, same path but different bandwidth for each direction in the same link, as well as quality of service or network access restrictions. Routing policies and traffic engineering may also cause routing asymmetry [39].

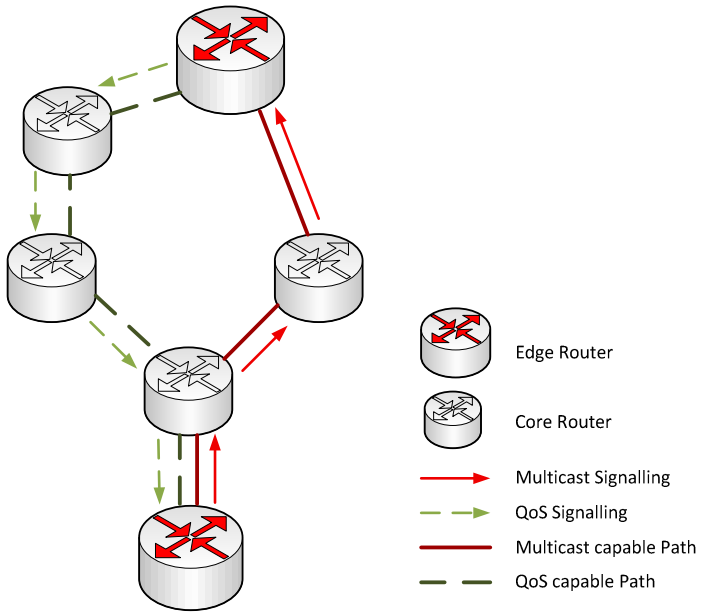

Figure 3 – Asymmetric routing influence in QoS-aware multicast distribution trees

The limited functionalities supported by DiffServ to provide QoS guarantees require the implementation of external resource allocation mechanisms, since resource reservation and admission control is required at least to deploy Per-Domain Behaviour (PDB) and services based on the Expedited Forwarding (EF) Per-Hop Behaviour (PHB). However, the integration of DiffServ and resource allocation mechanisms introduces performance issues. On one hand, the scalability achieved in DiffServ, allowing per-class control, is adverse to the performance degradation taken by per-flow resource allocation mechanisms currently deployed in the Internet through Resource Reservation Protocol (RSVP)[40]. On the other hand, the addition of new mechanisms increases system complexity and endangers its performance, which is not desirable. DiffServ was originally

conceived for wired networks, but its aggregation QoS control concept was also extended for wireless networks.

Aiming to solve some issues related to QoS-aware multicast communications, it will be given a brief explanation of two mechanisms that will be used in this work to control resources allocation and multicast trees. The first one is the Overlay for Source-Specific Multicast in Asymmetric Routing environments (OSMAR) [39], which focus on asymmetric routing problem and propose a solution to solve this situation like an overlay for SSM protocols. The second mechanism is the Multi-service Resource Allocation (MIRA) [41] that controls Class-of-Service (CoS) resources and multicast tree at the same time, considering also the asymmetric routes through the OSMAR over PIM-SSM as the multicast routing protocol.

OSMAR [39] aims to be used as an overlay for source-specific multicast protocols, such as PIM-SSM, enabling them to deal with network asymmetries and to provide QoS-aware content distribution, while maintaining their specifications and state machine. To accomplish this, OSMAR changes the values of the MRIB tables, used by the multicast routing protocol to build the multicast tree considering the path from source to receivers (data path) contrary to the greatest existing multicast protocols. OSMAR allows the creation of multicast branches according to the connectivity and the QoS characteristics configured for each source-receiver data path. OSMAR works with asymmetric routes, either intra-domain or inter-domains, that increase the scalability of this protocol. Additionally, it allows the adaptation of SSM protocols to asymmetric routes in a distributed manner, in which most of the functionality is done by OSMAR agents residing in edge routers. Also, OSMAR ensures an easy deployment, avoiding any changes in the state machine of the multicast routing protocol and either in terminals. Furthermore, OSMAR can be progressively implanted, because it does not require the installation of agents in all network domains at the same period.

MIRA [41] is a possible solution to control the resources of CoSs and multicast trees in a synchronized manner taking into account the problem of asymmetric routes. MIRA assures the quality level requested for each flow of a multi-user session, by adjusting the resources of the selected CoS. Besides, MIRA supports the construction of QoS-aware multicast trees for each session-flow by manipulating the MRIB. The CoS bandwidth and the MRIB are updated in a single-pass operation from the ingress to the egress located in the direction of the access-router of the receiver that asked for the session. In the ingress-router and in each interior router, the configuration of the selected CoS is done in the outgoing interface indicated by the unicast RIB. After configuring the CoS, MIRA updates the MRIB with the IP address of the previous visited

router. In an egress-router, MIRA configures the selected CoS taking into account the SLS established with the neighbour network, and triggers PIM-SSM after configuring the MRIB. Edge-agents store the definition of session-flows, characterized by different kinds of information, such as available CoSs (e.g., tolerance to loss and delay), the edge-to-edge per-class reservations and the list of interior-routers involved in the reservation-paths. While the edge-to-edge per-class information is used for fast admission control and to support QoS mapping and adaptation functionalities, the list of interior-routers increase the flexibility of process. Updated information about the edge-to-edge per-class state is acquired periodically by querying network resources associated with each class, inside a network or by checking SLSs between networks. Although edge-agents are overloaded with processing and information, this makes possible interior-agents store only per-class reservation state for a trivial control and consequently packet forwarding procedure optimization.

The first real demonstrated architecture, containing QoS and mobility of multicast sessions in heterogeneous environments, was developed under the framework of IST FP6 Daidalos II project [42]. This proposal is characterized by a hierarchical structure to support QoS, and extends the current Media Independent Handover standard IEE 802.21 to seamlessly integrate mobility and QoS [43], to enable the support of multicast services in unidirectional technologies, the Multicast Subscription System (MSS) protocol was introduced: this mechanism needs a return channel only for subscription.

A new algorithm based on ant colony optimization for QoS mobile multicast routing is presented in [44]. Ant colony optimization algorithm is a new optimization method proposed recently. The algorithm does not rely on mathematical description of the specific issues, but it has a strong global optimization performance. It has gotten better results in solving NP-complete problem such as the Travelling Salesman Problem. According to the general scope of the search path, a suitable orthogonal table is chosen to confirm the effect of the QoS parameters. Thus, the volatility of pheromone is rectified dynamically to speed up the constringency rate and the optimal multicast tree which meets multiple QoS constraints is set up.

2.3.2. Network Resources Allocation in Wireless Networks

Wireless Local Area Network (WLAN) is widely deployed as an effective and alternative solution to the LAN and cellular networks from the perspective of bandwidth and mobility. As users experience the convenience of wireless connectivity, they begin to demand support for the

same applications they run over today's wired networks. Contrarily to wired networks, the wireless medium has restricted bandwidth availability and higher packet-error rates with high packet overheads. This could potentially limit the use of WLANs for delivering traffic for real-time applications such as VoIP telephony and multimedia applications. End-users expect not only the mobility provided by WLANs but also the QoS support for new multimedia applications. Nowadays, the IEEE 802.11e (WiFi) [45] and IEEE 802.16e (WiMAX) [46] are distinguished as the two better WLAN technologies that provide broadband access and traffic forwarding with QoS guarantees. In WiFi and WiMAX networks, multicast support is implemented at the MAC layer. The following section has the purpose of giving a brief explanation about QoS support and how resource reservation can be provided in WiFi, WiMAX and 3GPP networks, as much as the multicast support.

IEEE 802.11e (WiFi)

The IEEE 802.11 standard [45] is used by WiFi networks to provide secure, reliable and fast wireless connectivity. The IEEE 802.11 Task Group E (802.11e) has defined enhancements to the original 802.11 Medium Access Control (MAC) to provide QoS. The 802.11e standard introduces the Hybrid Coordination Function (HCF), which combines functions from Distributed Coordination Function (DCF) and Point Coordination Function (PCF) with enhanced QoS-specific mechanisms and frame types. HCF has two modes of operation: Enhanced Distribution Coordinate Access (EDCA) and HCF Controlled Channel Access (HCCA). The EDCA is used to deliver Traffic Streams (TS) based on differentiating User Priorities (UPs). The HCCA is a centralized access mechanism controlled by the Hybrid Coordinator (HC), which resides in the QoS-Access Point (QAP). The QAP can take control of the medium, whenever needed, in order to allocate Transmission Opportunities (TXOPs) to TSs, which guarantee medium access with parameterized QoS. The setup of TS is requested by triggering the QAP with an Add Traffic Stream (ADDTS) Request message containing the Traffic Specification (TSPEC). The main purpose of the TSPEC is to reserve resources within the HC and modify the scheduling behaviour of it. The TSPEC must include at least the following parameters: mean data rate, nominal Service Data Unit (SDU) size, minimum PHY rate, delay bound and maximum service period. The QAP may accept or reject a new TSPEC request through admission control verifications implemented, based on the network conditions. The HC calculates the TXOP having as support the minimum data rate derived from the TSPEC.

The IEEE 802.11 inherits multicast address mapping concepts from 802.3. In infrastructure mode, an AP operates as a repeater, only bridging data between the Base (BSS) and the Extended Service Set (ESS). A mobile node submits multicast data to an AP in point-to-point acknowledge unicast mode. An AP receiving multicast data from a MN simply repeats multicast frames to the BSS and propagates them to the ESS as unacknowledged broadcast. Multicast frames received from the ESS presents a similar treatment. As an unacknowledged service it offers limited reliability. Frames loss arise from interference, collision, or time-varying channel proprieties. Data distribution may be delayed, as unicast power saving synchronization via Traffic Indication Messages (TIM) does not operate in multicast mode. APs buffer multicast packets while waiting for a larger DTIM interval, whenever stations use the power saving mode. Multipoint data may cause congestion, because the distribution system floods multicast, without further control. All APs of the same subnet replicate multicast frames.

IEEE 802.16 (WiMAX)

The IEEE 802.16 standard [46], known as WiMAX, is a new broadband network Access technology to provide data rates from 32 up to 130 Mb/s for wired environments. Recently, this standard has been extended to the IEEE 802.16d and IEEE 802.16e standards, for fixed and mobile access respectively. The former was designed to support video or audio streaming with class-based QoS assurance, and in the latter the QoS is granted and maintained by the MAC layer, where the flows are assigned with a Service Flow (SF) scheduling. The Communication Identifications (CID) of all transport connections must be associated with a SF, which is the unidirectional service MAC transport that provides a particular QoS on either the uplink or the downlink. The traffic specifications in WiMAX represent the QoS requirements used to establishment a SF, which can be described by: QoS parameter set type; Traffic priority; Maximum sustained traffic rate; Minimum reserved traffic rate; Service flow scheduling; Tolerated jitter; Maximum latency; and Fixed length versus variable length SDU indicator. The WiMAX Forum defines the WiMAX network reference model between the Mobile Station/Subscriber Station (MS/SS) and the Base Station (BS) as Access Service Network (ASN) and Connectivity Service Network (CSN). ASN manages the WiMAX radio links and consist of one or several ASN Gateways and BSs, supplying WiMAX radio coverage to a geographical area. In some cases the ASN is also used as a proxy, such as proxy MIP. CSN defines a set of network functions that provide IP connectivity to WiMAX subscriber stations. The CSN is destined to high level management,

containing gateways for Internet access, routers, servers or proxies for AAA, IP-allocation, user databases, and internetworking devices.

To invoke a multipoint data channel, the BS assigns a common CID to all SS in the group. For selecting group member, a BS may implement IGMP/MLD snooping or proxy as foreseen[46]. A SS will send multicast data to a BS as a point-to-point unicast stream, which –in the presence of the IPv6 CS- is forwarded to the upstream access router. The access router (IP over Ethernet CS) or the BS may return multicast data to the downstream BS by feeding into a multicast service channel. On reception, a SS cannot distinguish multicast from unicast streams on the link layer. Multicast CIDs are unidirectional and available only in the downlink direction. Thus a native broadcast-type forwarding model is not available. CID collisions for different multicast groups are very likely due to the short ID space. As a consequence, multicast data transmission may occur in joint point-to-multipoint groups of reduced selectiveness.

3GPP

The 3GPP system architecture spans a circuit switched (CS) and a packet switched (PS) domain. The latter General Packet Radio Services (GPRS) incorporates the IP Multimedia Subsystem (IMS) [47]. The 3GPP PS is connection-oriented and based on the concept of Packet Data Protocol (PDP) Contexts. PDPs define point-to-point links between the MT and the Gateway GPRS Support Node (GGSN). Internet service types are PPP, IPv4 and IPv6, where the recommendation for IPv6 address assignment associates a prefix to each (primary) PDP context [48]. Current packet filtering practice causes inter-working problems between Mobile IPv6 nodes connected via GPRS [49].

In order to receive a QoS level other than the default QoS level, a service data flow needs to be bound to what we refer to as a QoS bearer. A QoS bearer is associated with an uplink binding state in the User Equipment (UE) for the uplink traffic, and a downlink binding state in the gateway (GW) for the downlink traffic. The binding state creates the mapping of a service data flow to a QoS bearer. When multiple bearers are established between UE and a GW, then it is the uplink binding states of the QoS bearers that “steer” the aggregate uplink traffic into the right bearers, and likewise the downlink binding states in the GW for the aggregate downlink traffic. For a specific network that the UE connects to there is at most on bearer without uplink and downlink binding states. This bearer is referred to as the default bearer. It is important that each QoS bearer connecting to a specific network is associated with well defined uplink and downlink binding states to ensure an unambiguous mapping of packets to the QoS bearers.

In UMTS Rel. 6 the IMS was extended to include Multimedia Broadcast and Multicast services (MBMS) [ref]. A point-to-multipoint GPRS connection service is operated on radio links, while the gateway service to Internet multicast is handled at the IGMP/MLD-aware GGSN. Local multicast packet distribution is used within the GPRS IP backbone resulting in the common double encapsulation at GGSN: global IP multicast datagrams over GTP (with multipoint TID) over local IP multicast.

In 3GPP2, the MBMS has been extended to the Broadcast and Multicast Service (BCMCS) [50], which on the routing layer operates very similar to MBMS. In both 3GPP and 3GPP2 multicast can either be sent using point-to-point (PTP) or point-to-multipoint (PTM) tunnels, and there is support for switching between PTP and PTM. PTM uses as unidirectional common channel, operating in unacknowledged without adjustment of power levels and no reporting in lost packets.

2.4. Context-Aware Network Selection

Nowadays, ABC [51] paradigm is becoming more popular, since it enables users to distribute their application flows throughout the most suitable combination of different access points and access technologies, regarding their preferences and network resources. Network access selection is the main functional block of the ABC solutions, enabling not only a choice based on QoS, but also founded on users/applications context. Many algorithms emerged to tackle better solutions as we will see along this section.

ABC best solution depends on several different constraints associated to the network entities (user, network and environment) at different levels. The best in the user perspective does not necessarily match with the best in the network operator perspective. However, the main goal of the ABC service provider is to offer a better experience to users, remembering always network operator capacities and policies.

The network selection problem can be seen by several perspectives, so several proposals appear, trying to solve this problem. However, before introducing the network selection solution, it is important to understand all important contexts that can be used in the network selection. Many proposals appear with the same base of the user's context information and it tries to question users about what is the more important to them. Personnel, preference, social, accessibility, knowledge, location, velocity, devices, network and calendar are the most

considered user's context information in the literature. Besides this new metrics to choose the AP to users, it is also necessary to consider the QoS parameters in selection.

Besides user's context, the access point context must also be considered, regarding not only technology characteristics but also resources availability, performance among other parameters. Related proposals, beyond QoS parameters, emerge other relevant context information, such as security, cost and handover effort.

More recently, it has appeared a context related with session's requirements and characteristics [52]. Due to session context and availability of codecs support in the terminal, users may need to be sub-grouped in different sessions with different codecs, but with the same content. Parameters such as codecs or content requirements are included in session context in order to provide better access network selection decisions. Resuming, all information that can be collected and used to a better network selection and a better service to the client is welcome.

Before performing network selection itself, it is necessary to collect all the information important to the decision. This context acquisition process is not only related with usual link quality but also with information from different levels and entities [53]. New proposals consider this context-awareness dividing it into static and dynamic for both, network and mobile devices [54]. The network context information takes into account resources availability, load status and QoS that is being perceived. However, related with mobile devices, much more information is important to a better selection such as preference, application requirements, reachable APs and real time devices status. Even though, the integration of user context in network selection process is just a small part of a wide range of context information that can be used.

Despite the application of context-aware selection decision, two main different problems arise, concerning the handling of all context information. The first problem is related with the distribution of this information along several components in the network. Besides this information dispersion, it is also dynamic and needs constant update to perform efficient network selection decisions. When all information is organized and updated, the second problem appears: what to do with this information to efficiently select the access network [53] [54]. Information only is precious when we know how to filter and use it to our own benefit. The information collected is not usually in a suitable condition to be used and processed, so it is necessary to format it in a proper way. In this sense, cost function solution [55] appears to convert the context information into a suitable form.

New metrics related with the quality perceived by users when accessing a service, Quality of Experience (QoE), are also introduced under this subject, enabling the evaluation of user

experience. Measuring end-user perception is very complex given the number of parameters (context, network, activity, device …) that can influence this perception. QoE can be seen not only as an output parameter, but also as an input value for a better choice in the next selection.

The following paragraphs describe some of the most known network selection algorithms.

J. Yliato et al. [56] presents an interface selection mechanism for multihomed mobile terminal based on protocols that support handovers between interfaces of different technologies. The solution proposed innovates, concerning mobility of already established traffic flows. Since the different flows of the same application usually have different requirements, this approach provides a simultaneous set of access networks which respectively satisfy the needs of each flow. In the article, interface selection is the local routing of packets through local interfaces in a multihomed terminal. This system has 5 components with different characteristic and functions: entities, action, policy, credentials and mechanisms. The decision process relies on a user-policy database (user-centric decision) which should be dynamically updated due to the constantly changes in context information. The actions in a policy are ordered by a priority so as to define which should be first searched and matched. Although being made an implementation, no simulation results are presented, a reason for not being able to determine the efficiency of this policy-based approach.

A comparison of heterogeneous network selection algorithms is achieved in [57], aiming to evaluate the performance of four algorithms: Multiplicative Exponent Weighting (MEW), Simple Additive Weighting (SAW), Technique for Order Preference by Similarity to Ideal Solution (TOPSIS), Grey Relational Analysis (GRA). Several proposals in the literature model network selection as a fuzzy problem. Fuzzy logic is suitable to represent constraints or preferences that are not well defined and difficult to measure. In order to use this information, it is necessary to convert fuzzy data into numbers and then use a Multiple Attribute Decision Making (MADM) method to obtain a ranked list of the candidate networks. SAW and TOPSIS are two different methods of MADM. The first, determines the overall score of an alternative network through the weighted sum of all its attributes. TOPSIS selects the candidate having the closest distance to the ideal solution and the farthest from the worst scenario.

The GRA method selects the best solution through grey relationship with the ideal one. The MEW algorithm is another method of MADM, where the network selection problem is modelled by a matrix representation. Each row of the matrix is the access network and each column concerns an attribute, as in [58]. The score of a network is obtained by the weight product

of the different metrics. All the algorithms concerned in the comparison study need a relative importance of each metric, which vary accordingly to QoS needs.

From the results obtained it is possible to conclude that SAW, TOPSIS and MEW provide similar results for all types of traffic considered. GRA method provides higher average bandwidth for interactive applications. However for the remaining applications using the GRA algorithm had increased the delay observed.

The work presented by X. Bo and V. Nalini [59] also deals with ABC service. The access selection problem, in author's vision, consists in mapping all traffic flows through the available access networks in order to accomplish the following requirements: satisfy user preferences and maximize the number of traffic flows in the network, while satisfying QoS needs. To model this problem, a variant of the well-known bin packing problem was used, proposing approximation algorithms derived from the First Fit Decreasing algorithm (FFD) in order to obtain near-optimal solutions and reduce computational effort. The mathematical model used allows the description of flows and access networks using several characteristics. A new constraint introduced in this work is the power consumption cost that determines the power consumed by a specific flow. It is also introduced a dissatisfaction metric that measures how far the assign access does not match with the preferred. The selection algorithm itself has as goal to minimize the average cost and dissatisfaction of a given flow distribution, regarding other constraints such as maximum bandwidth and acceptable delay. The FDD algorithm in its original state always attends the biggest item in the list to the smaller one. In order to deal with multiple constraints in an ABC scenario extends, the presented solution extends the algorithm, ordering the flows in the wait list, decreasing preference and bandwidth order. Features as substitution, flow partitioning, load-awareness and reallocation are added to the original algorithm and then compared through simulation. From the performance evaluation improvements of each mechanism are notorious, comparing to the random scenario.

The network selection algorithm purposed by S. Qingyang and A. Jamalipour [60] is one of the most cited works under this subject. It focuses only the algorithm itself not concerning mobility and QoS support mechanisms as well as access discovery or context gathering features. The algorithm specifically takes into account just an integration of WLAN and cellular system (UMTS), applying mathematical and computational techniques to model the network selection problem. The constraints considered in this approach are network conditions, service application,

and user preference for QoS. To deal with these parameters, this solution proposes an integrated Analytic Hierarchy Process (AHP) and a Grey Relational Analysis (GRA). GRA was the first method used to find the best solution of a complex problem by dividing it into sub-problems and then integrates them with relative dominances, which after synthesizing will provide a weight for each alternative. A new set of QoS related parameters is introduced as decision constraints. The author divides QoS components in throughput, timeliness, reliability, security and cost. Each one of these factors is then divided into the traditional metrics (packet loss, delay, latency ...) being assigned specific weights to each, depending on the scenario. The assigning of these weights may be the disadvantage of this approach, due to the number of constraints considered. The decision process is always considered a trade-off between network performance and users preferences. Through the simulations and scenarios used in the evaluation of the mechanism this idea is very explicit, despite the existence of few network alternatives.

N. Coutinho et al. [61] presents a performance study of a traffic control mechanisms that is able to perform context-aware and personalized network selection to determine the best access connection for each terminal and service. This work focus on the access selection process to optimize network performance when considering multi-technology and multihomed environments, using any-constraint algorithm, based on parameters related to context, preferences, and terminal and network characteristics, combining this knowledge to enable the optimization of both terminal and network point of view[51].

The results show the benefits of using such an algorithm in the network performance, mainly in terms of QoS in these multiservice technologies, and address the influence of specific criteria and constraints considered in the decision process.

2.5. Summary

In this chapter a brief overview of the multicast concepts and related concepts was presented, with emphasis on its importance in the NGN, reducing network load and increasing overall efficiency. Multicast is centred on the concept of group which is a set of nodes interested in a common data flow. Sources only send one copy of each packet and network replicates it only when necessary, presenting great benefits in the network performance. Mobility section begins with the explanation of MIP basic concepts and then details the integration of mobility with multicast. However, much work is still needed regarding multicast mobility despite the current

approaches described: MoM, MMROP, CTMS, MobiCast and HMMCT. Other important mentioned subject is the QoS in multicast environments to ensure a reliable delivery of content to end users. Since QoS for multicast has associated some problems, as asymmetric routing, some solutions like MIRA and OSMAR were studied. A brief description of QoS in the wireless environments was presented and associated with multicast concept, specially focused to WiFi, WiMAX and 3GPP. Finally, it was addressed the context-aware network selection problem, analysing the usefulness of using context not only for network optimization purposes but also to offer personalized services.

3. Context-aware Multiparty Transport and Network Resources Control

The proposed solution evaluated in this thesis addresses the context-aware multiparty transport, supporting context-aware network selection and guaranteeing the network resources control. Recent real-time application requirements and network heterogeneity call for new strategies to efficient deliver multimedia content to several users in a pervasive manner. This section detail described the evaluated architecture.

Section 3.1 explains the main ideas of the architecture proposed and contextualize them in the NGN. Section 3.2 begins with the definition of each architecture component and then the description of the entire architecture, focusing on mechanisms and process to understand how it works. Section 3.3 describes the algorithm and information used to select the AP to each request flow in a context based way. Finally, Section 3.4 resumes the entire chapter.

3.1. General Concepts and Ideas

The main purpose of Context-aware Multiparty Transport framework [62] is to provide techniques in order to use context to efficiently support dynamic group-based content delivery, considering context information (network, users and services) to optimize the delivery process network in a mobile multihomed scenario. As it is intended to deliver data to multiple receivers, IP multicast was the best solution to be adopted, since its bandwidth-constrained scheme allows packet duplication only as needed. Despite optimizing bandwidth consumption, IP multicast cannot provide bandwidth assurance to QoS-constrained sessions, such as video/audio conferences and IPTV. Consequently, it is necessary to associate IP multicast with QoS control schemes, in order to assure access control and bandwidth to prevent degradation service quality. Nevertheless, such integration is not trivial due to scalability problems and divergence in architectural design. In the envisioned scenario, dynamic and mobile, changes of context influence the sessions and network, with constant re-configurations. So it is necessary to create a network multiparty control framework that is able to react in a scalable way to these context changes without damaging the quality of experience perceived by the users and optimizing network resources.

It is important to emphasize that the current technologies are not globally available and still insufficient, making it very difficult in practice to provide seamless and pervasive group communications. Indeed, it is almost impossible to deliver the content in the same form to all group members due to their individual heterogeneous aspects, such as link capacity, network conditions, device capabilities, mobility and environmental circumstances. Such requirements reinforce the need to support dynamic resource adaptations, in order to optimize network performance and guarantee users satisfaction. In order to fulfil such requirements, current Internet requires optimizations practically at all levels of its protocol stack.

3.2. Components and Architecture

In this chapter it is explained the entire architecture evaluated in this thesis, beginning by clarifying the function of each component [63]. After understanding each element, it is necessary to explain the interaction between elements as well as their place in the network scenario.

Session Management (SM):

SM is the key to control both, user-to-content and content-to-user relationship. SM works as an overlay between applications and networks, being agnostic to the access technologies. SM is responsible for session control, more specifically, establishments, re-negotiation and termination. Furthermore, group members can be split into sub-groups, corresponding to different media encodings of the same content, with the objective of providing the better solution to each application. Additionally, SM creates the session context, which describes the characteristics of the sessions, such as codec, delay, loss rate, jitter and ID of the members of the group. Since the SM plays a role of intermediary between users and their machine content, it needs to trigger the link between traffic applications and receivers. The SM enables the content to be transmitted with necessary QoS for the given session by using specific signalling in order to interact with NUM and IPT.

When a user intends to join or leave a multiparty group, SM is required to trigger the appropriate network resource control. This requirement may be differentiated according to the type of networks, the terminal capabilities and the context information. Furthermore, due to the networks dynamics as well as user situation modifications which can lead to a new type of media, such as new audio or video stream, SM must be capable of re-negotiating the content leading to

modified or even new sessions. SM participates in dynamic changes, such as switching between different content, achieving a dynamic SM nature for the context-aware, heterogeneous system.

Internet Protocol Transport (IPT):

The IPT component aims to select a communication path (unicast or multicast) to connect Overlay Nodes (ONs), as well as further allocating network resources in the nodes between the ONs to allow a propagation of multiparty content sessions, with QoS guaranteed over the time, to a group of users. The main requirements of IPT in heterogeneous networks include the support of scalable QoS control, efficient IP multicast control, fast resilience operations, setup of network resources and QoS mapping.

IPT handles network resources aggregately (per-class) to overcome the performance shortcomings of existing per-flow approaches. For instance, the wide used Resource Reservation Protocol (RSVP), a standard solution that places excessive signalling/state, thus processing overhead, to configure and maintain resources for each micro flow. Also IP aims to avoid too much centralized control, such as in TISPAN, for scalability and fault tolerance. In the scope of multiparty transport, IP multicast is not efficient due to the high signalling and state overhead placed by the per-flow basis of legacy multicast protocols (eg. PIM and SSM), as well as the lack of QoS support and access control, which is essential.

The performance limitations of the existing proposals motivated to design IPT with support of distributed per-class resource control, thus whereas session establishment can be requested in a per-flow basis, resources are configured per-aggregations. As input, IPT takes session context and collects network context directly from devices or QoS-Context Providers (CPs) (CP with QoS information about nodes, paths …) via a well defined API. In order to obtain an efficient operation, IPT has tools to interact with network elements (packet scheduling mechanisms, QoS approaches for mapping, unicast/multicast routing protocols …) of several network technologies to deploy resources allocations and build delivery trees in heterogeneous environments.

Besides IPT functionalities, we can list admission control, per-class resource reservation in different QoS models, control of IP multicast trees and detection of re-routing conditions. IPT tries to be seamless as possible in resilience operations, since it attempts to reconfigure multicast trees without changing multicast groups address. This measure prevents user's re-subscription and enables to local changes, a re-configuration of tree with appropriate requirements and does not need to interact with other components (Network Use Management (NUM) and SM) to take a

decision, it only informs them. This process has several benefits in different types of metrics, such as energy user's consumption, session handovers disruption (signalling and processing overhead), user's satisfaction, etc. So, IPT only triggers other elements when strictly needed. For instance, when doesn't exist a path between ONs, it is necessary to trigger NUM in order to reconfigure transport connections with others ONs and paths.

Context Providers (CxP):

In order to support the context required in the architecture proposal, it is necessary to create entities to obtain context information from entire network elements, providing this information in a useful manner to other components. Such entities, named Context Providers (CxP), are capable of reporting sensed and network information according to control mechanism, triggering events on other components (using notify/subscription mechanisms).

Terminal Network Context Provider (TNCP):

TNCPs were developed with the main purpose of collecting information related with user terminal. This entity collects information about user profile and user interfaces and sends them to CB. Besides collect information, TNCP also measures QoE for each received flow and it sends this information to NUM, in order to guarantee the always best connection for each user flow.

Context Broker (CB):

CB as can be described as the context database of the network, so CB periodically receives the information of the CxP and keeps them. CB not only interacts with CxP but also delivers information to the decision entity (NUM), when NUM sends a request message with pretended information. CB contains context information about traffic applications, users, network, etc.

Multiparty Transport Overlay (MTO):

The main objective of using a MTO is to provide a generic transport service for multiparty applications in order to support several existing and future multiparty applications in a heterogeneous networking environment (eg. WiFi, 3G and WiMAX). MTO is based on the new concept of applying the overlay paradigm at the transport layer, while the most of the existing multiparty overlay solutions, whether in the conceptual stage or deployed in today's networks, either use some form of IP tunnelling (eg. MBMS or AMT) or specify application layer protocols.

With the study of the related work, it was found a lack in generic MTO providing abstract transport trees. Some multiparty technologies are application dependent or do not support IP multicast. Besides, it was found the lack of the dynamic transport group management functionalities, considering networking changes and environmental contexts.

MTO fragments the concept of Abstract Multiparty Transport (AMT) in order to introduce the concept of sub-AMT. Sub-AMTs can be seen as sub-networks embraced between two Overlay Nodes. Sub-AMT concepts increases the scalability and reliability of the network, since it is possible to change only a sub-AMT instead of creating a new AMT when a failure or modification occurs. Figure 4 presents 2 AMTs (AMT1 and AMT2) for different users that want to receive from 2 different sources (S1 and S2). The AMT2 is divided in 2 sub-AMTs, the sub-AMT 4 and sub-AMT5, in order to hide the lack of multicast support in the nodes of the network between ON1 and ON3. MTO is very helpful in heterogeneous environments, guaranteeing the content reception, independently of technology used.

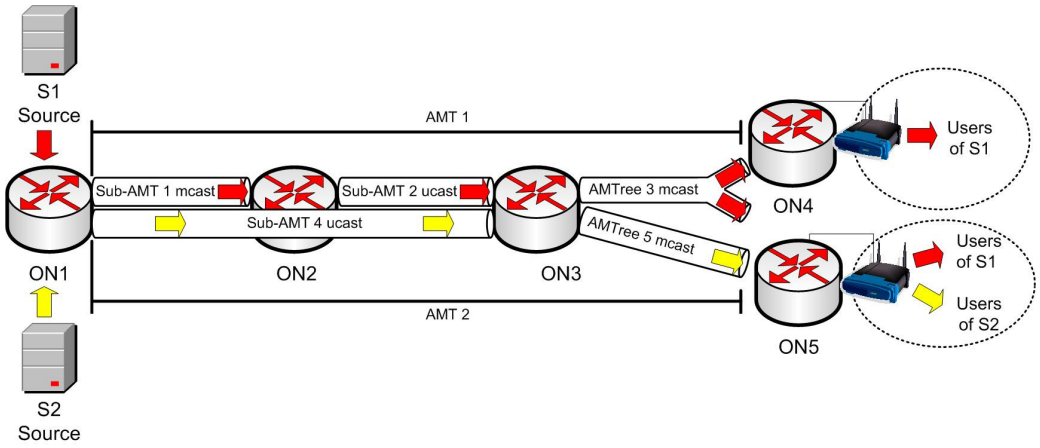

Figure 4 - End-to-End AMTs and interiors Sub-AMTs [64]

MTO should be developed as a scalable and reliable generic solution, transparent to communication layers below and above the transport layer. This overlay solution also provides a dynamic multiparty transport group management service, adaptable to the networking and environmental context. Context-aware transport group management paradigm is a key feature of the MTO and it represents a set of operations performed at the transport layer on the whole multiparty group or individual groups of users. This is a new concept with no substantial background technical literature. MTO concept is tightly related to the management of multiparty transport connections (creation, update and deletion operations) according to the changing networking and environmental context.

Conceptually, an MTO is an abstract transport tree made up of overlay nodes (ONs). The root of the tree represents the multiparty source (eg. application server) and the leaf of the tree is the closest node to the receiver (eg. AP). To properly deliver multiparty packets from the source to the receivers over the overlay tree, each overlay node has to maintain mapping information between the multiparty transport connection ID (unicast source address and port, and a unicast or multicast destination address and port) and the IDs of associated multicast and unicast transport connections forming the branches of the abstract transport tree. Multiparty data routing (unicast or multicast) from the source to ON, between ONs, and from ON to receivers is handled by IPT. Figure 4 shows an example of multiple abstract transport trees, maintaining a multiparty transport connection with multicast and unicast connections.

The transport management operations along with the related MTO tree updates are triggered by networking and environmental contexts, captured by the NUM and translated by IPT for MTO in terms of commands via the IPT-MTO interface. MTO also provides an efficient transport framework able to optimize the use of network resources (e.g. maximizing the use of IP multicast when possible) while adapting to the specific context of each group member (e.g. using IP unicast where multicast is not available). In terms of context-awareness networking, the MTO component also maintains adaptive transport reliability (eg. adaptive FEC) based on the link quality.

Network Use Management (NUM):

NUM can be described as the brain of the entire architecture, since it provides intelligent context-aware network selection to select IP routing paths, not only in the core network, but also in access network. The main purpose of the NUM is to maintain all multihomed terminals always best connected, offering best QoS trough a heterogeneous system while it achieve enhanced network capacity and performance. Besides, context-based reactions of NUM allow the mobile terminals switched between its interfaces, to prevent quality degradation according to user context, network conditions, transport modes and devices.

NUM was designed based on the limitations of the existing multihomed mobility solutions. For instance, the SCTP protocol is not able to provide information about the best path selection, while the HIP protocol does not provide information about technologies and QoS attributes of local network interface. For the network selection functionality, objective and profit functions are not transparent to the users since they are asked for data in order to make a

decision. Consumer surplus uses a user-centric approach, which may not be good for load balancing. Stochastic programming is designed to support a single common service with a fixed bandwidth, which is not flexible.

The context-aware network selection of NUM is being designed to overcome the limitations of the existing solutions, by considering user, environment, session and network context. Consequently, it is expected to achieve a more efficient use of the available heterogeneous radio resources, as well as more uniform distribution of the load between the different radio access technologies (RATs), while satisfying the requested QoS to the users.
The network selection algorithm aims to anticipate and prevent undesirable situations like overloading or underutilizing of RATs, not only with entire information, but also with the feedback of the users about their QoE. The heterogeneous tendency of the future Internet requires routing decisions that take into account all the relevant information of the users and sessions, as well as the environmental information.

AMT&MTO Controller:

This component is an element that belongs to NUM entity and it can be described as a database and an interface to interact with IPT and MTO in order to construct sub-AMTS and configure ON with proxy information. This entity has its own messages to interact with other network elements, maintaining the correct function of the entire network.

After explaining the components of the architecture, it is important to understand the architecture taking into account the way that different elements interact to support the context-aware multiparty service delivery. First, it is necessary to perceive the distribution of the components in a scenario for a better comprehension of the interactions between them. The NUM and SM components are shown as belonging to a central station, for simplification purposes, and IPT is placed on all nodes of the network. As described, the ONs implement an overlay agent for proxy functions, and can be implemented in strategic nodes, such as between IPv4 and IPv6 domains or between Multicast and Unicast areas, or everywhere (depending on the network operator decision). The SM and NUM must be supplied with information about the CB, all available ONs and the network attached to the egress ONs (APs). Beyond controlling multiparty communications to keep mobile users ABC, context-based adaptation of the multiparty delivery aims to enable pervasive access to the group communication as well as its seamless continuity

despite mobility of group members, re-grouping, or context changes that require change in session or network conditions. Figure 5 shows how components can be placed at edge and core routers and how they interact in a general environment.

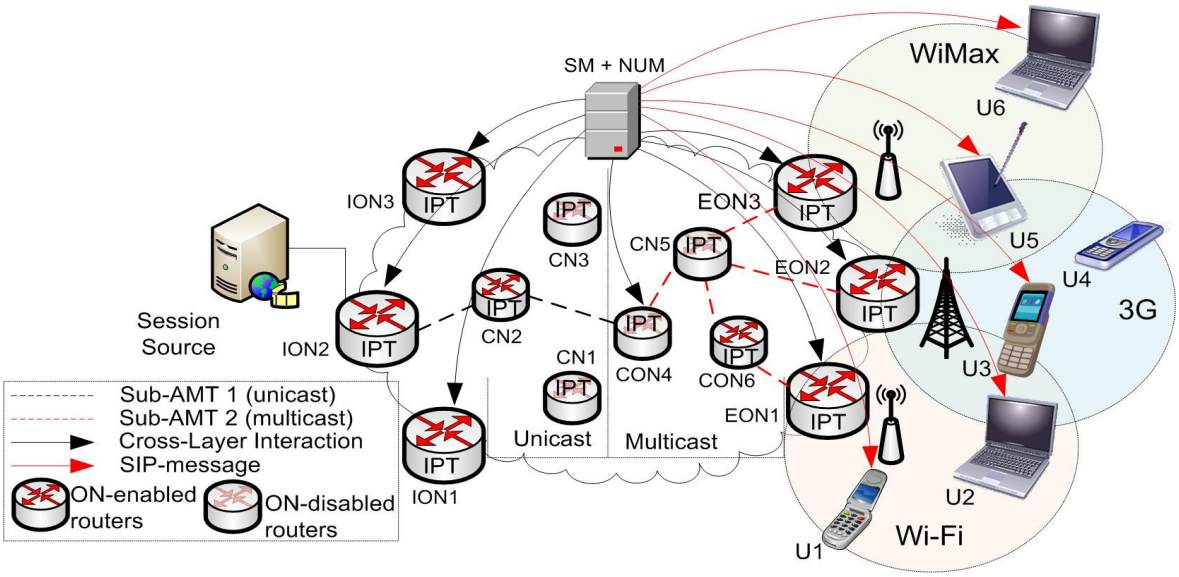

Figure 5 – General project scenario [64]

Whenever a session is to be established, SM first performs grouping/sub-grouping and composes each session based on users contexts. Then, SM triggers NUM for the session establishment. The Session Setup functionality defines a set of operations that must be deployed to establish a session within a network. In addition, the session setup is also used in resilience operations, where new paths require the setup of a new session. Obviously, such operation must be skipped when the indicated sessions are already activated, preventing thus redundant configuration. The session Setup operations are illustrated in Figure 6 , and take into account general environment.

Session Setup:

The main important instruction in the entire architecture is the Session Setup, since it allows users to receive data packets with QoS, trough a selected core path and AP. Session Setup is a complex process with several components, so it will be explained in detail with help of diagrams.

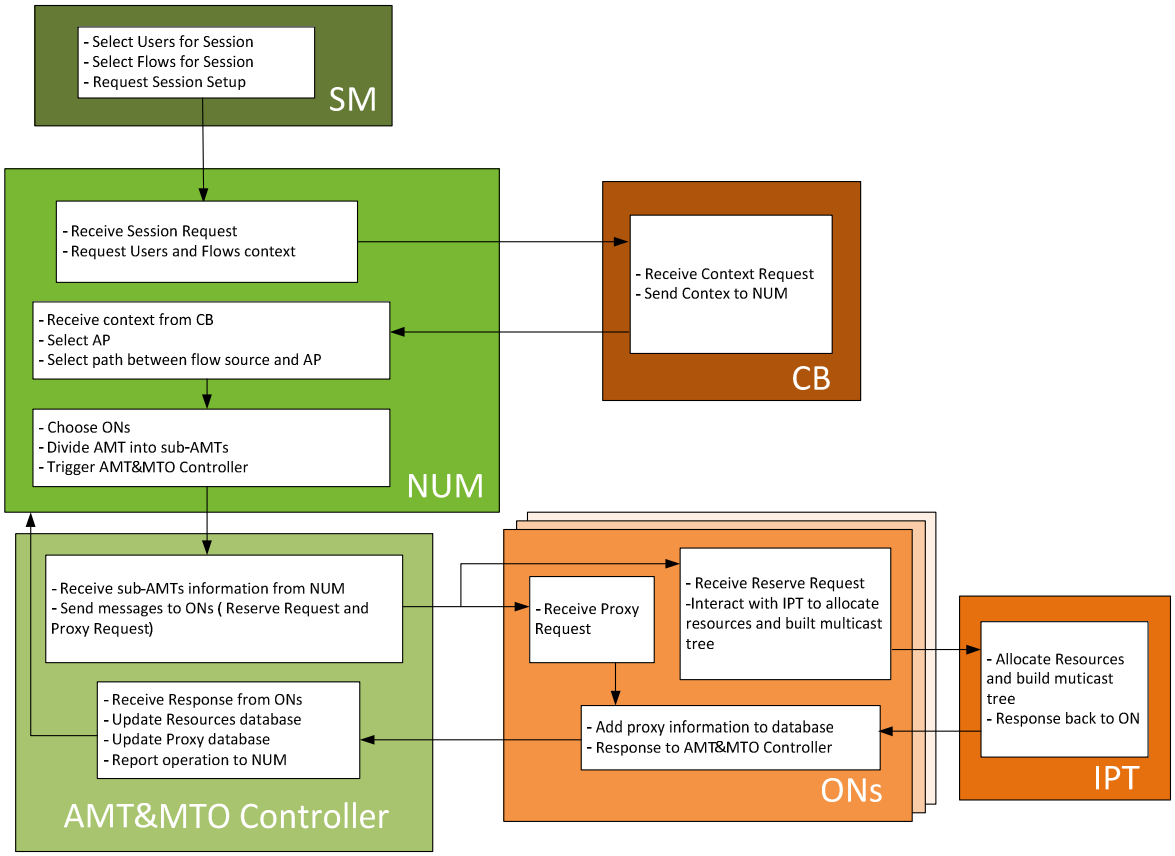

Figure 6 - Successful Session Setup Request

Upon receiving the Session Setup Request trigger from SM, carrying session context and information about the related group, NUM triggers the CB with a list of users IDs to get context about each indicated user and a list of data flows to get each indicated flow context (eg. QoS parameters). After receiving the list of user contexts and list of flow contexts from CB, NUM processes each flow of each user independently. NUM also needs to choose the best AP to each flow of each user with an access network selection process, taking into account the requirements the CoS of the flow (3.3). After AP decision, the next step is to find a path with QoS parameters adequate to the flow between the flow source and the AP selected. NUM selects the path and the ONs, based on links QoS characteristics (delay and bandwidth). After the entire reflected selection process, it is important to proceed with the network elements configuration. Since NUM already decides the path and the ONs to use, it divides the AMT into sub-AMTs. Each sub-AMT begins and ends in ONs, and AMT begins in flow source and ends in Receiver AP, both ONs. Then NUM interacts with AMT&MTO controller to send information to ONs, since AMT&MTO controller works as an output interface and a database to keep the information. After AMT&MTO Controller received information from NUM, it forwards packets to the involved ONs in the selected path,

with QoS information to allocate resources and information to build the multicast trees (Figure 8). This information is enough to configure the ONs proxy database to change data traffic between different multicast trees.

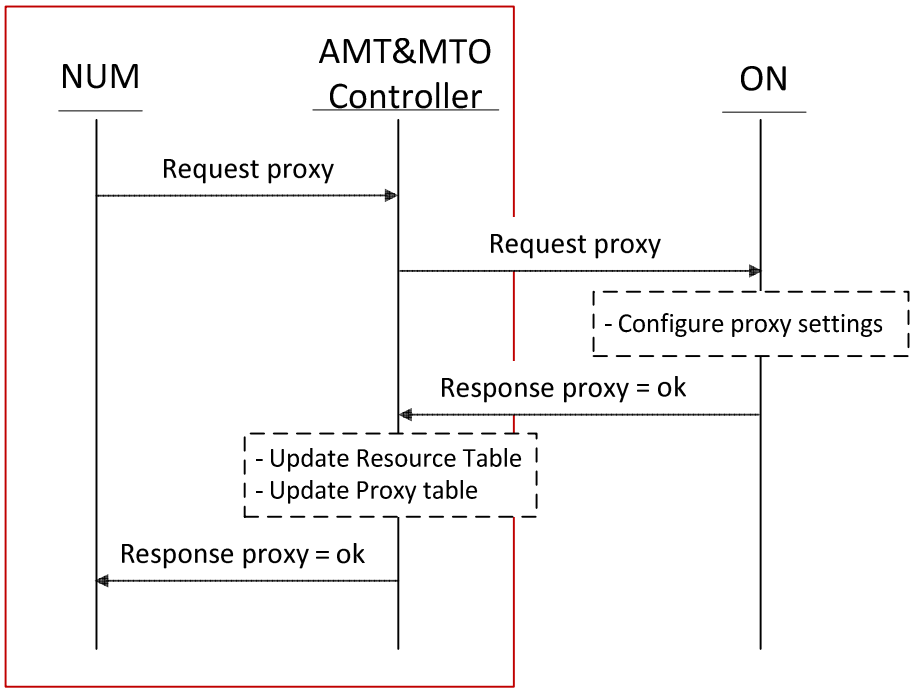

Figure 7 - Successful ON proxy configuration (add or remove)

The AP ON does not allocate resources in the path to MT, so it needs a different message, proxy message (Figure 7), only to configure the proxy settings to forward data to the final multicast tree, which the user receives. When an AP ON receives the *Request proxy* message, it only updates its own database with information received, adding or removing IP source and IP destiny to a certain flow. Then, the ON uses response proxy message to report the success to AMT&MTO Controller that, after receiving it, updates its databases with proxy information.

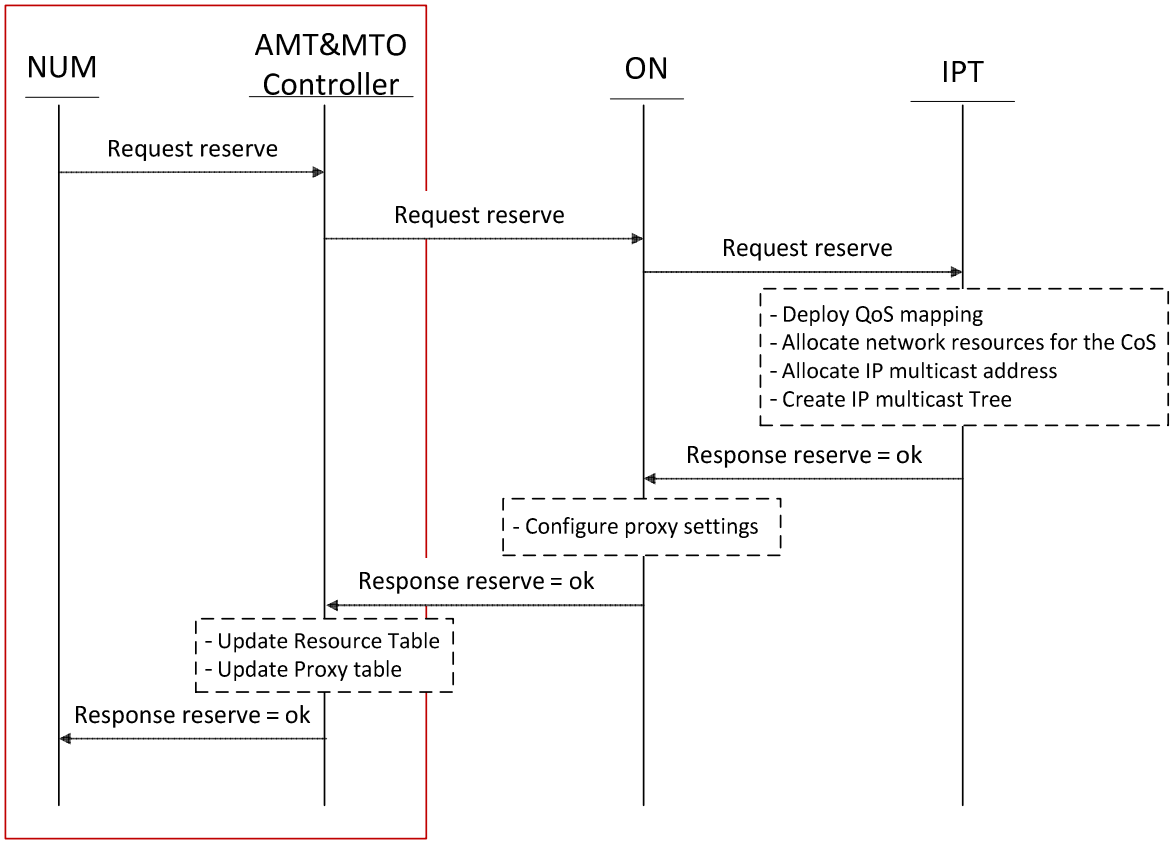

Figure 8 – Successful reservation of resources and build of multicast tree

The case of the ON configuration, when it is not an AP is very different, beginning with the interaction with IPT in order to obtain a multicast tree with allocation of resources (Figure 8). So, ON activates reservation message in the IPT at the same node, and the IPT sends a signalling message across the path between the ONs. The going message allocates bandwidth for the respective CoS in all path nodes and the return message builds the multicast tree using the same path. When the return message is received by the IPT node, it initiates the signalling message, and IPT reports the operation to same node ON. Subsequently, ON configures proxy database in order to forward data packets to the new multicast tree. Then, ON uses the Response reserve message to report the operations to AM&MTO Controller, which updates its proxy and resources databases and delivers message information to NUM.

User Movement:

As soon as MT perceives that it will lose connection in one of the interfaces that are receiving data packets, it is necessary to warn NUM, to maintain the good QoE perceived by user as good as possible. This flow handover should be done as fast as possible and with minimum

packet losses. When NUM receives the *warn move* message, the path selection begins. First, NUM needs to interact with CB, in order to receive updated context information to a better network selection. Then, NUM finds a new AP to forward data packets, and then tries to choose a new path in core network. In the new core path it is important that whenever possible the new path is similar to the old path, in order that changes are as short as possible. After this process, NUM will deliver information to AMT&MTO Controller with ONs and sub-AMTs needs, as explained in Session Setup and observed in Figure 8. The main difference of session setup is that it is necessary to release the allocation resources and destroy the multicast tree in the old path.

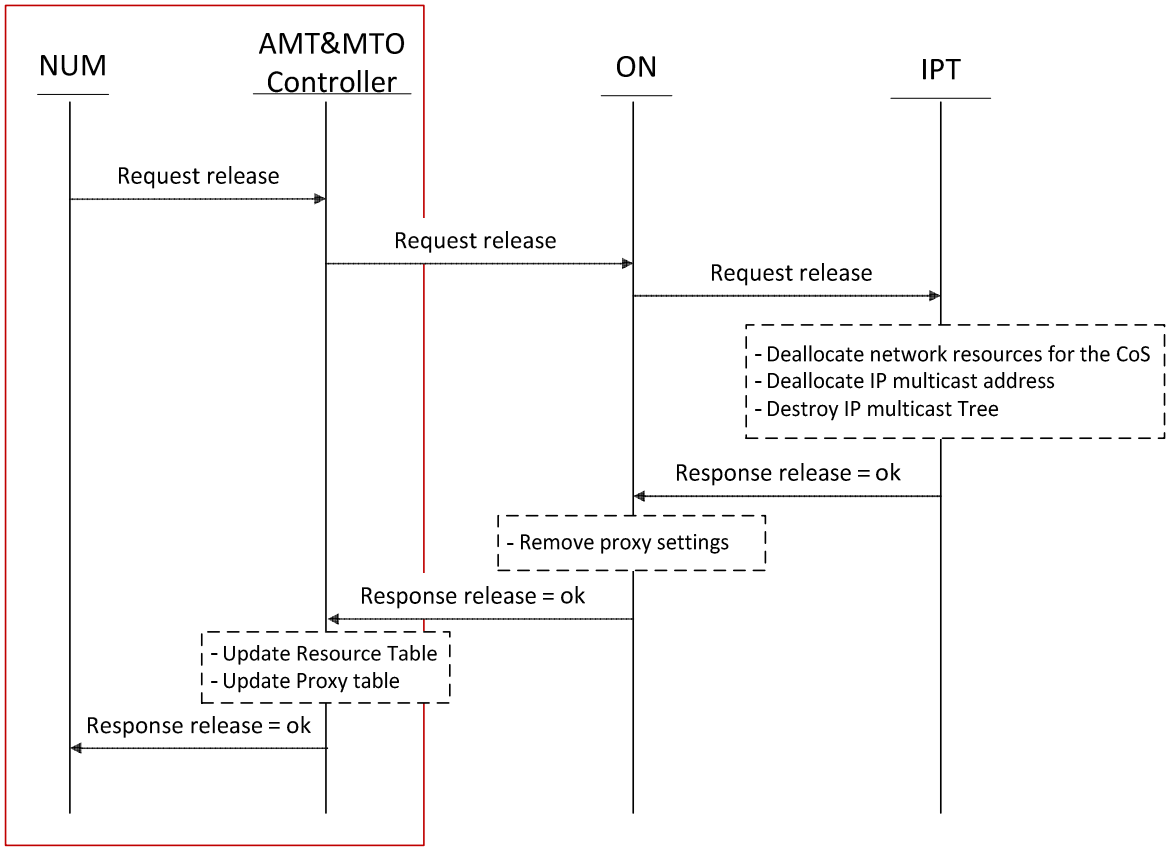

Figure 9 - Successful release of resources and remove of multicast tree

NUM informs to AMT&MTO Controller the sub-AMTs that it needs to be removed and the proxy ON databases that it needs to be updated. Then, AMT&MTO Controller sends *request release* messages to ON with information to remove resources and prune multicast tree or *requests proxy* messages to update proxy database. Besides the AP ON, that it only needs to update its database according Figure 7, the other ONs need to receive *request release* messages. In this case, ON then triggers IPT do de-allocate resources for respective CoS and remove the

multicast tree. After IPT signalling trough the path between ONs, it reports the operation success to ON back. Since ON receives information of signalling from IPT, it configures its proxy database with new information, removing the IP source and leads to the respective flow. Then, ON uses a *response release* message to report information to AMT&MTO Controller that updates its proxy and resources database according to the received information and forwarding them to NUM.

User Bad QoS Report:

This instruction is useful when a user begins to receive under the CoS minimum QoS requirements. It is very similar to the User Movement process, although the main difference is that it only removes path resources and multicast tree in case of finding a better AP and core path. If a better solution could not be found, nothing happens and the user continues receiving in the same AP and in the same network path.

3.3. Access Network Selection

The access network selection process implemented absorbs the main concepts of the solution proposed by V. Jesus et al.[53] and studied by N. Coutinho et al. [61]. This section will briefly describe this scheme, the main guidelines considered in the development of the solution, and the modelling of several characteristics of each element in the network, providing an easier manipulation of the information.

The main objective of the network selection scheme proposed is to produce a ranked list of candidates APs that the terminal may then connect. The ranked list is composed by flow maps [9], each containing a possible distribution of the user's flow through the available APs.

Although the ranked list should be formed based on QoE values, the main elements of the network are modelled according to their characteristics, due to the subjectivity of this metrics and the difficulty of associating it with the flow maps rank.

Points of Attachment (PoA) characteristics usually are divided into two obvious groups: static and dynamic characteristics. The static features considered in each PoA are monetary cost and user's preference. The resources of the PoA cannot be only related with bandwidth, but also with the capacity to provide different services to the user that wants to connect to it. So, considering the fact that our architecture supports QoS and multicast, it is relevant to add them in the process of AP selection. Since multicast is used, it is important to choose the same AP to users that want to receive the same flows. Regarding QoS, it is helpful to concentrate the same CoS in

the same AP. However, aggregating CoS or FIDs in the same AP should affect the QoE perceived by the user.

User's features can also be divided into static and dynamic. The static features of a user are related with all the context information that can be relevant in the AP selection. An important guideline, besides ranked list, is that the resource management is totally independent of the ranked lists process. This means that only PoA with resources available (bandwidth, delay, loss) are allowed to enter in the flow map calculation, thereby reducing processing efforts.

In order to be able to model any criteria to be used in the algorithm, it was decided to format it into a matrix presentation form. This is a friendly and legible way of organizing the different types of information of each entity. It is important to start with the definitions:

- W is the number of characteristics of a PoA that will enter in the ranking list

- M is the number of PoA that belongs to the ranking list

- k is the index of a terminal belonging to the set of the K terminals able to be selected, k Є K and #k = K

- Flow map allows mapping each of the Nk flows of a terminal to one PoA out of the Mk possible, $FM^{(k)}: F^{(k)} -> M^{(k)}$.

To model the three basic and independent entities in the architecture scheme (PoAs, users and flow maps), a specific matrix was defined for each. The PoA profiles cover all the features and context information about each PoA specifically. User profile relies on user/terminal preferences and with non real-time activity of the user, being totally independent of the PoAs properties. Flow maps are related with user's flows and with the resources available, being a kind of bridge between the information of the PoA and the user's personal preferences and status.

PoA Profiles:

Regarding PoA profiles, they are defined as follows: $AP = (AP_{ij})_{M \times W}$ .This matrix keeps the PoA properties and can be easily changed according to different criteria or preferences relevant in the mobility management decision. In order to map numerical values into properties, it is used a simple analysis of each property setting, an empirical numerical value to the criteria or being this value the result of a cost function [55].

The AP matrix is built based on all the specific properties of each PoA, being constituted by three types of properties:

$$AP = \left(AP^{(user)} \middle| AP^{(static)} \middle| AP^{(dynamic)}\right)_{M \times W}$$

The first substructure is set by information proceeding from the user, such as its preferences for the PoA. The static part refers to the features of the PoA that, first of all, are static and independent of context, users, or time. The last part is built regarding the information that comes from the network, like the current resources status of the PoA.

Access Technology	User Preferences (static)	Monetary Cost (static)	Subgrouping (dynamic)	CoS (dynamic)	Bandwidth Allocation (dynamic)
WiMAX 1	100	30	90	90	50
UMTS 1	70	50	60	50	100
Wi-Fi 1	80	80	0	0	90
WiMAX 2	100	30	30	70	10
Wi-Fi 2	80	80	0	0	30

Table 1 - Possible PoA properties

An example of PoA properties and their empirical values is presented in Table 1. In this matrix, the values closer to 100 are the best ones in the specific criteria and 0 values are the worst. Bandwidth allocation can be a good example of a dynamic property of a PoA, since it is adjustable and a result of a simple cost function, the more occupied is a PoA lower will be this value. Besides Subgrouping and CoS Used are dynamics, they have not a cost function, only levels according to their characteristics.

User Profile:

The user profile is based on properties and information independent of the context and real-time activity of the network. In order to have the proper interaction between the PoAs and the users, the user profile matrix must be modelled concerning to the PoA properties:

$$UP^{(k)} = (UP_{ij})^{(k)}_{W\times W}, (UP_{ij})^{(k)} = 0 \; if \; i \neq j.$$

The UP is a diagonal matrix whose elements are weights that measure the importance given by the user k to the respective PoA criterion. It is possible to shape qualitatively and quantitatively users using various combinations of different weights for each of the properties of the PoAs. Making a simple example by following this logic, different user may coexist, such as business man, gamer and groupie. As it is understandable and common sense, different users

have different needs, and these requirements may be quantitatively weighted by the values in the UP matrix. So, a weight distribution like the one presented in Table 2 can model the type of users and their requirements.

User Profile	User Preferences	Monetary Cost	Subgrouping	CoS	Bandwidth Allocation
Business man	0.5	1.0	1.5	1.0	1.0
Gamer	1.5	0.5	1.0	1.5	1.0
Groupie	0.5	1.5	0.5	0.5	0.5

Table 2 - Possible weight distribution according to user profiles

As it is really apparent, all these properties and values are easily configured and modified according to the criteria followed by the architecture designer, as planned in the design guidelines and requirements for the network selection scheme.

Flow Maps:

The flow maps indicate the distribution of the different flows that belong to the same user through the available and allowed PoAs. It is mathematically defined as:

$$FM^{(k,l)} = (FM_{ij})^{(k,l)}_{N\times M},\ FM^{(k,l)}_{ij} \in \{0,1\},\ \forall\, i,j$$

The l index defines a specific flow map for a given terminal *k*. Since flow is defined as the minimum indivisible unit of resources, $\sum_{j=1}^{M} FM^{(k,l)}_{i,j} = 1,\ i = 1,\dots,N$.

Flow Maps Calculation:

Flow maps calculation [61] is the final stage to choose an AP to forwarding data to a User based on previous information. This stage consists in algebraic manipulation of the matrices, previously described and includes 7 steps.

1. Obtain a normalized version of *AP* to generate *APN*.

2. Find user profile group, retrieve the group profile preferences and generate *APNU*.

3. Generate CAP using $(CAP_i)_{M\times 1} = \sum_{i=1}^{W} APNU_{ij}$, overall cost of each PoA, already normalized and personalized.

4. Through updated network's database resources, find the best S flow maps as described previously, according to the service mix deployed in the network.

5. Generate matrix APA for each flow map, $(APA_{ij})_{S\times M} = \sum_{m=1}^{N}(FM_{mj})^{(i)}$. This matrix determines how much a certain PoA is used for each flow map.

6. Determine the ranking of each flow map by generating the matrix WFM (weights of flow maps) using $(WFM_i)_{S\times 1} = (APA_{ij})_{S\times M} \times (CAP_i)_{M\times 1}$.

7. Find in WFM the best ranked flow maps. The quality value of a flow map is defined by $Q_i = \frac{WFM_i}{\max(WFM_i)}$.

3.4. Summary

In this chapter the entire architecture evaluated in this Thesis was detailed, regarding its main ideas, components and architecture. All interactions were explained to a better understanding of the entire architecture. NUM is the central decision component and it is responsible for the network selection; CB is database of the entire network providing context information from different sources; IPT works in the reservation path and builds multicast trees and MTO works as an overlay to ensure the function independent of the underlying technology in core and access network. Also TNCP is an important component not only to provide mobility, but also to measure QoE and provide user context information.

An access network selection algorithm is presented, based on the context information from users, network and environment. These solutions, taking into account, both network operation and users preferences, never forget the QoS pretended for each CoS. The algorithm presented is supported by matrices operation in order to produce a ranked list of the best PoA to the user.

4. Architecture Implementation

After explaining the architecture, it is necessary to develop and evaluate the ideas. So, it was used the network simulator NS 2.31 to implement the architecture components, taking into account the architecture ideas explained in chapter 3.

Section 4.1 begins with an overview of the simulator and their main principles. The same section also includes the limitations of the simulator and background work needed to start the development of the architecture. Section 4.2 explains all modules created to support the architecture idea. This section is divided according to the functional blocks, permitting a better comprehension of entire simulator implementation. Finally, Section 4.3 resumes the entire chapter.

4.1. Network Simulator (NS 2.31)

The Network Simulator (NS) was developed by UC Berkeley and allows the simulation of technologies and network protocols. NS is a discrete event simulator oriented for networking research. NS2 was first developed in 1989 as a variant of the real network simulator. Currently, NS2 has also included several contributions from worldwide researchers.

4.1.1. Overview

NS2 is an open-source network simulator which has as main purpose the research in computer communication networks, providing a fundamental tool for students researching in this area.

NS2 uses an open source code, being under constant investigation and enhancement for years. It contains modules for many network components, like routing, transport layer protocols, QoS methods and applications. However, most research needs simulation modules which are beyond the scope of the built-in NS2 modules. To incorporate theses modules into NS2, a deep understanding of the simulator internal architecture is required.

The NS2 simulator is supported by object oriented languages, C++ and Otcl, and its code structure is divided according to the processing level. C++ programme language is used to functions, procedures and classes that need many processing cycles and, in opposite, Otcl is used in works that need few computational processing and constant changes.

The simulation results are written in trace files. Each line of the trace file is produced for an event of each packet, covering all directions from the sender node to the listener node. Additionally, NS2 can also generate files for Network Animator (NAM), a visual interface bundled together with NS2, which enables users view the recording of a simulation.

4.1.2. Limitations and Incompatibilities

The wireless feature introduced into NS is done using C++ language. However, this approach was not followed in multicast module development, since it is practically all written in Otcl language. This difference is responsible for a set of problems related with the good connection between the two languages.

The information regarding the number of hops between the nodes is fed to the central object *god*. The number of mobile nodes is passed as argument which is used by *god* to create a matrix to store connectivity information of the topology.

After several days of research, no answers appear to solve this issue. The reply from the NS2 community was clear. It is not possible to have in the same scenario multicast and mobility, unless the whole multicast code is translated to C++ language due to the problem of the connection with the god object. So, another solution had to be found. The solution followed the idea of the MIP example that comes with NS2. In this MIP example, a mobile node (not a wireless mobile node) has several links, one to its Home Agent and many to its several Foreign Agents. Since these links are dynamic, the mobile node is connected to one of the access routers and when it aims to move, the current link goes down and the link that is connected to its new access router goes up. Thanks to MIP, packets are forwarded to and from the new mobile node location. This example shows a good way to simulate nodes movement without the need of wireless. However, when talking about mobility we always associate it to wireless scenario. In order to emulate wireless characteristics, particularly packet losses and delays due to collisions, Error Models had to be added. The Error Model allows some configurations that force packet dropping as well as increase the delay on a particular link.

Later in this chapter (4.2.4), wireless simulations are studied in order to construct a solid error model, which presents the wireless domain behavior with the increase of the MTs number.

4.1.3. Understand Support Implementations

Before creating new agents and functions in NS2, it was important not only to understand the simple agents of transport, applications and routing, but specially MIRA and multicast NS2 implementations. MIRA implements two ways of work, one mode is per flow and another mode is per class with over provisioning. They were studied in detail, understanding the code and tested them with several scenarios. Besides of the better result of the over provision model, it presents a serious failure, since the ingress nodes do not communicate between them, in order to inform the bandwidth consumption of a shared link. Modifying all code to permit ingress nodes communication is a hard task and cannot bring so good benefits to entire architecture. Besides, the over provision mode requires reservations between ingress and egress nodes, disabling the possibility of construct sub-AMTs trough ONs in the core. The per-flow model has been adopted by IPT architecture element. Since MIRA uses the RIB table to construct the QoS path and multicast tree, it is necessary to modify them to allow the choice of the entire path between ONs.

4.2. Extension of Simulator

In order to evaluate the architecture explained before, this section will describe the NS2 implementation of some components of the architecture, since the entire architecture is the integration of this thesis with another one. These parts are focused on mobility and user's context, allocations of sub-AMTs and also related with AP context-aware selection.

4.2.1. MTO

MTOs are an important part in implementation of the sub-AMTs concept, since they have as main function the traffic forwarding between sub-AMTs of the same AMT. Therefore, ONs can be compared to proxies, as they change the IP destination and source according to the next multicast group and multicast source respectively (Figure 10). ONs can be configured in every node of the network according to network operator preferences. ONs also have the purpose of creating packet copies in case of existing different destinations to the same flow ID. One good example of copy utilization is when an AP has two users, one that can support multicast and another that cannot, allowing the users, to receive data independently of the multicast support or even IP version. One copy of the original multicast data content is created and then ON sends this unicast data packet to the unicast user.

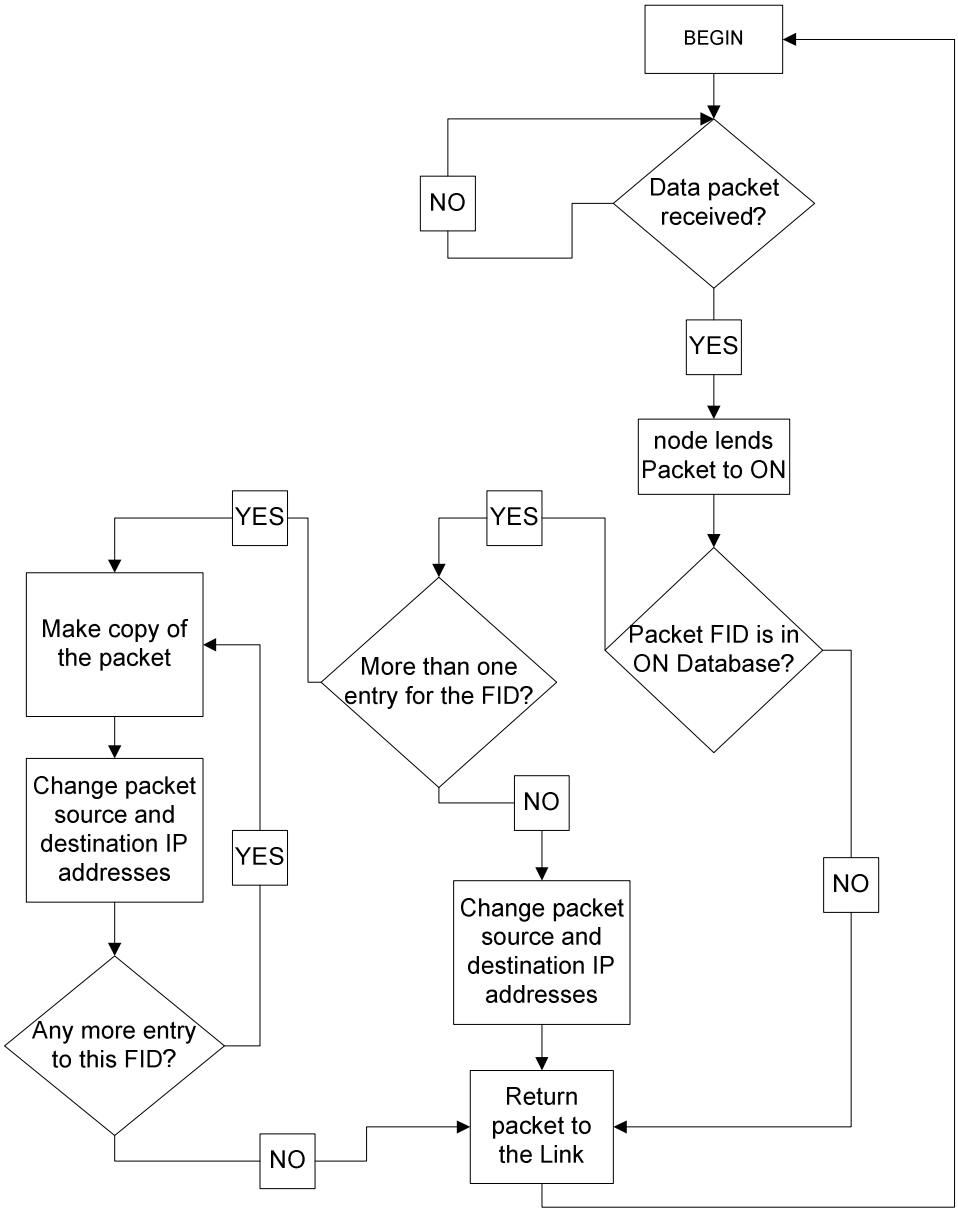

Figure 10 - Proxy block ON diagram

Figure 10 illustrates the entire process of proxy role, played by each ON in the network. First, only in data packets it is necessary to modify the IP address and IP destination, so only data packets begin the analysis process to determine proxy settings. After analysis of packet type, receiver node delivers the packet to the ON of the same node. Then ON looks to the FID field of IPv6 header to compare with its FID database, deciding if there is any database information to this FID. Subsequently, the IP source and IP destination are changed according to ON database; when

there is more than one IP source/destination to the same flows, packet copies are created and sent to the respective IP destinations.

As explained before, the ONs need a database, because they have to analyse all data packets and compare their FIDs with ON proxy database (Table 3).

FLOW ID	
IP source address	IP destination address
IP source address	IP destination address

Table 3 - ON proxy database

ONs also need to interact with a main instance, named MTO&AMT controller to receive requests with respective information and then reporting the success or failure of the operation. This controller sends packets in order to configure remotely the proxy settings. Figure 11 illustrates the distribution of AMT&MTO controller messages after chosen the AP and entire core path.

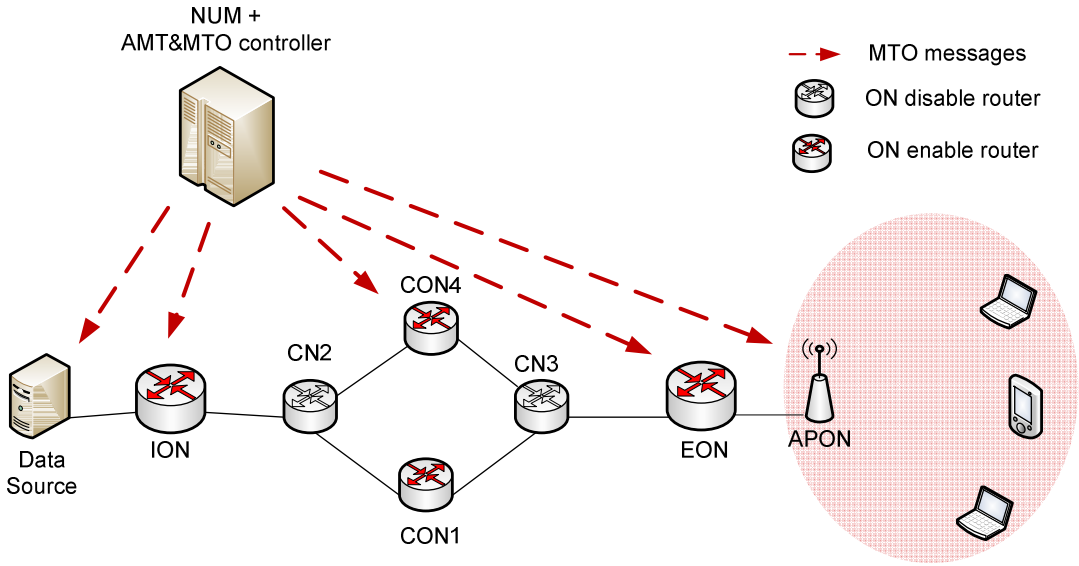

Figure 11 – AMT&MTO delivering messages

ONs also need to interact with MIRA agent of the same node in order to obtain a multicast tree with resources reservation, delivering the entire information needed to allocate resources in the pretended path. In that case, IPT signals the entire path until the destination with

MIRA message in order to allocate resources, and then a signalling message returns back through the same path to build multicast tree. Figure 12 shows the building process of chosen AMT and sub-AMTs, according to the selected ON to enter in the flow acquisition process. NUM chooses not only the entire core path and the AP, but also the ONs involved in the AMT. Between two selected ONs there is a sub-AMT with a different multicast group responsible to guarantee QoS to multicast data content. In case of Figure 12 the AMT selected is constituted by 4 sub-ATMs. The AMT begins in the data source and ends in the AP (configured as ON). The introduction of sub-AMTs concept improves the network behaviour when a user moves to another AP or when a core link fails, since it is only necessary to change the affected sub-AMT (resources and multicast tree). Sub-AMTs have the advantage of hiding different technologies in access and core network. If CN3 node does not support multicast, CON4 can configure IP destination packets not to a multicast group but to the unicast IP address of the EON, maintaining the other sub-AMTs with multicast trees.

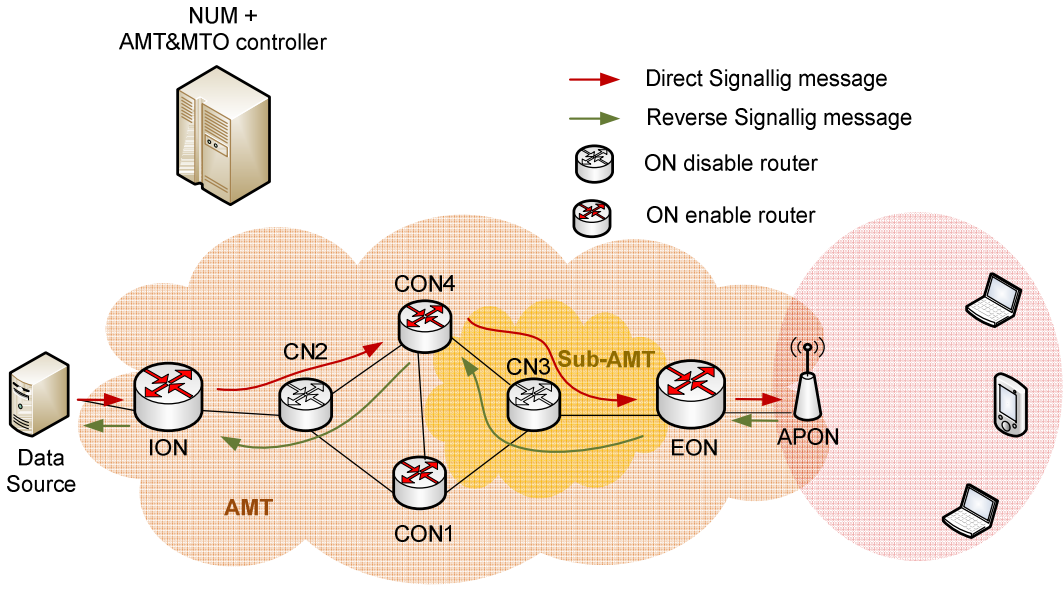

Figure 12 - Signalling to build multicast AMTs and sub-AMTS

When the ON receives the OK response from IPT, it introduces information on its database, filling the IP source and IP destination to the respective FID. To report a successful or a failed process, ON only fills the status flag with one or zero respectively, in the message that it receives from the AMT&MTO controller and forwards it back. This operation mode of recording only after receiving the response, allows the correct working of all network, independently of the loss of control messages (MIRA messages), maintaining a correct proxy database in each ON.

4.2.2. MTO&AMT Controller

MTO&AMT controller is a central unit designed to interact with MTO in the network and it is in the same machine than NUM. AMT&MTO controller can be defined as a bridge between NUM (higher layer) and the ONs/IPT (lower layers). While NUM is the brain that makes all decisions based in entire network information, the MTO&AMT controller enforces the decisions. This is a way of dividing the work in decision and execution. So the MTO&AMT controller needs to exchange messages with ONs, in order to maintain the correct function of all pieces. Most often, messages do not need only proxy settings, but also information for the ONs to interact with IPT, in order to allocate resources and construct multicast trees. AMT&MTO controller also provides several functions in order to facilitate the interaction with NUM, sending different information to NUM according to simple requests of it. Since AMT&MTO controller also works as an interface it simplifies the interaction with connected entities.

The following messages, reserve, release and proxy (presented in Table 4 and Table 5) are used by MTO&AMT controller to trade information with ONs.

Header Field	Function
Message type	Indicates the type of the message (Request reserve, Response reserve, Request release , Response release)
Reserve source	Indicates the first node of the reserve (MTO)
Reserve destination	Indicates the last node of the reserve (MTO)
Flow ID	Indicates the Flow ID of the reserve (1, 2, 3...)
Bandwidth	Indicates the bandwidth needed for the reserve
CoS	Indicates the CoS needed to be reserved to the flow (0,1,2,3,4,5)
Flag Multicast	Indicates if the Path supports multicast or not (1/0)
Flag IPv6	Indicates if the Path supports IPv6 or not (1/0)
Multicast Group	Indicates the multicast group
Reserve Path	Is a vector with all nodes between Reserve source and Reserve destination
Proxy source	Indicates the value of source IP address for data packets
Proxy destination	Indicates the value of destination IP address for data packets

Flag Status	Indicates status of the response message, OK or Not OK (1/0)

Table 4 - Fields of the reserve and release messages header

The message of Table 4 is used in four different types, as it can be seen in the Message Type (Request reserve, Response reserve, Request release and Response release). Request release message needs the same parameters of the Request reserve message, since all information about pretended reserve/release need to be delivered for both cases. To reserve a path between ONs, it is necessary to know characteristics of the data flow that will cross the path, such as Flow ID, Bandwidth, CoS, Flag Multicast, Flag IPv6, Multicast Group and Reserve Path. When these parameters are delivered to the IPT, it not only tries to reserve a path for the data flow, but it also uses join messages to construct the multicast tree across the reserved path.

Some fields of mentioned message headers are only used to configure proxy settings as it can be seen in the proxy message header (Table 5). Besides the Flow ID, used for both processes, resources allocation and proxy configuration, it is necessary to fulfil the Proxy source and the Proxy destination, since they can be different from the Reserve source and Reserve destination respectively.

Header Field	Function
Message type	Indicates the type of the Proxy message (proxy add or proxy remove)
Flow ID	Indicates the Flow ID (1, 2, 3...)
Proxy source	Indicates the value of source IP address for data packets
Proxy destination	Indicates the value of destiny IP address for data packets
Flag Status	Indicates status of the response message, OK or Not OK (1/0)

Table 5 - Fields of the proxy message header

The Proxy message is usually sent to APs, since the links from AP to Users do not have reserved paths for data flow (QoS wireless classes are not used). It is only necessary to change source and destination IP address of the data packet, so that all process is transparent to users, and they receive data traffic with originals IP addresses of the source.

AMT&MTO controller only records reservation (Table 6) or proxy (Table 7) information in its database when it receives back from ON a message with OK Flag Status.

This operation mode of record only after receive the response of the MTO, allows the correct function of all network, independently of the loss of control messages, maintaining the synchronization of the entire network resources information, as the proxy information saved in each ON .

This record information is useful when NUM needs to release or even change the sub-AMTs. In this case, NUM request information about a path or even a user, and AMT&MTO controller collect the information pretended and delivery it to NUM.

Field	Function
Reserve source	Indicates the first node of the reserve (MTO)
Reserve destination	Indicates the last node of the reserve (MTO)
Flow ID	Indicates the Flow ID of the reserve (1, 2, 3...)
Bandwidth	Indicates the bandwidth needed for the reserve
CoS	Indicates the CoS needed to be reserved to the flow (0,1,2,3,4,5)
Flag Multicast	Indicates if the Path supports multicast or not (1/0)
Flag IPv6	Indicates if the Path supports IPv6 or not (1/0)
Multicast Group	Indicates the multicast group
Reserve Path	Is a vector with all nodes between Reserve source and Reserve destiny
Proxy source	Indicates the value of source IP address for data packets
Proxy destination	Indicates the value of destiny IP address for data packets

Table 6 - Reserves database

Field	Function
Flow ID	Indicates the Flow ID (1, 2, 3...)
Proxy source	Indicates the value of source IP address for data packets
Proxy destiny	Indicates the value of destiny IP address for data packets

Table 7 - Proxy database

Information of Table 6 and Table 7 is similar to the header messages of Table 4 and Table 5, since database keeps the information contained in the fields of the control messages, so it is not necessary a detailed explanation about the fields of the AMT&MTO controller databases.

4.2.3. IPT Changes

IPT is the key to transport data flow over the internet. In order to have an implemented and tested solution to IPT, MIRA was used with some significant modifications. The main change to integrate MIRA in this architecture is the introduction of the source routing in MIRA messages. This is a fundamental change to allow NUM to choose the entire path between traffic sources and user terminals. To implement source routing it is necessary to add a vector with pretended path to MIRA message. This vector is delivered to IPT together with other variables, being necessary at the end of each link to withdraw the first position of the vector and include them in the destination IP address of MIRA message. This is a practice solution to control the entire path of the MIRA messages and respectively to fulfil the MRIB with intended path.

Beside changes referred before, some functions were also introduced to interact with MTO. IPT receives requests from ON and it has to inform the result of the processes back, in order for the ON to report this information to its control unit. It was necessary to fulfil all parameters of MIRA command with values received in the AMT&MTO controller message.

4.2.4. Wireless Emulation

As it was referred previously (4.1.2), multicast is incompatible with wireless scenarios in NS-2. Therefore, to solve this limitation, it was implemented an error model to increase delay and to force wireless loss packets rate. The loss rate and delay model used by an AP is related with number of received users and the assumption of any interference between APs. So, when a user starts or ends to receive data packets from one AP, it is necessary to recalculate the delay and loss rate of the AP, in order to change rate model error lost and delay of the links connected to this AP. First, it was created a pure wireless scenario and the values of delay and loss rate with the increase of the number of Mobile Terminals (MT) were analysed (Table 8). It is used an average rate of 100kps in order to allow 10 users to be connected at the same AP receiving a moderate rate of multimedia content. Since the wireless bandwidth is 1 Mbps (NS-2 default), considering a higher rate of data content will limit the number of users connected to each AP.

MTs receiving	APs	Average Data Rate	Data packet size	Types of data traffic	Wireless Bandwidth
1-10	1	100 kbps	1000 Bytes	CBR and EXP	1 Mb

Table 8 - Wireless Scenario Characteristics

The number of MTs was increased from 1 to 10, and consequently, the network performance is affected. The presented average values are the result of twenty simulations for each situation with confidence values of 90%. Several confidence intervals are so small that it is impossible to see them in the graphics (Figure 13 and Figure 14).

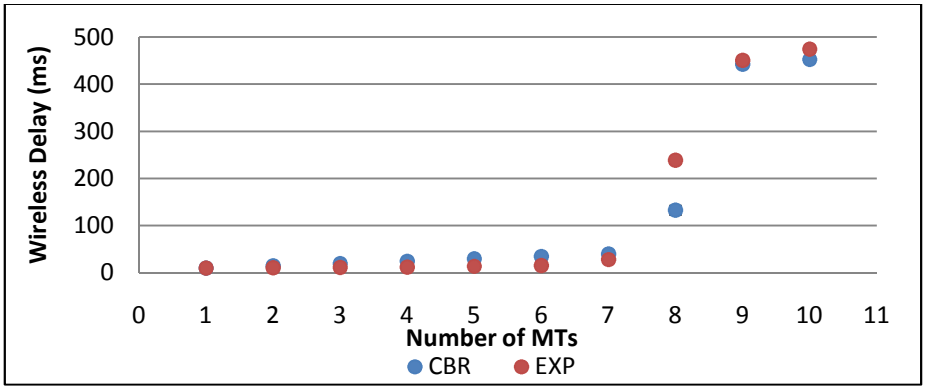

Figure 13 - Delay in Wireless Scenario

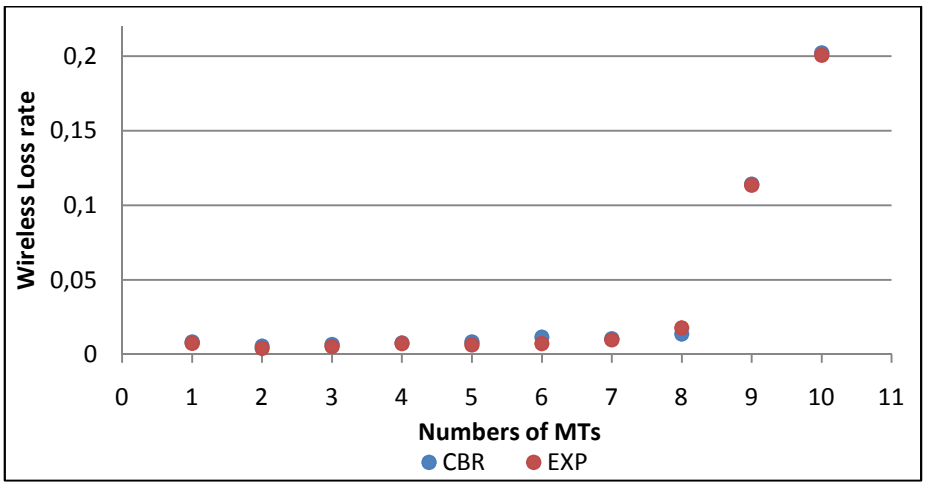

Figure 14 - Packet Loss in Wireless Scenario

As we can see, the values presented by EXP and CBR traffic are similar, so it will be used a mean of both (Table 9), as the pretended scenarios also have EXP and CBR traffic applications

running at the same time. As it is used a wireless bandwidth of 1 Mb and a traffic rate of 100 kbps with 10 MTs, all AP bandwidth were consumed and this AP will no more be selected until it releases some bandwidth. Table 9 resumes the delay and loss rate introduced in the error model according to the number of users connected to the same AP.

MTs	Wireless Delay (ms)	Wireless Loss
1	9,691	0,0079
2	12,476	0,0049
3	15,366	0,0060
4	18,319	0,0075
5	21,516	0,0075
6	24,911	0,0094
7	33,772	0,0101
8	185,660	0,0158
9	446,176	0,1139
10	463,176	0,2015

Table 9 - Parameters of the Error Model

The delay and loss values of the Table 9 are introduced at real-time in scenario variables, in order to a reality emulation of the wireless medium access. It is necessary to control the number of users that receive data flows in the same AP and recalculate the respective delay and loss values when this number change.

4.2.5. TNCP

This section is divided into three main important parts with different functions, such as, user context, user mobility and users QoS feedback experience. These parts will be explained independently, but the database (Table 10) for them is common, since it is easier to aggregate all information by interface.

Field	Function	
User ID	Number to identify each User	
Type	Identifies a profile to each User (Business, Gamer, Groupie)	
Interfaces	**Sub Field**	**Function**
	AP	Identifies the IP address of AP that interface is connected

	Flag Active	Indicates if interface is active or inactive (1/0)
	IP	Indicates the IP address of the Interface
	Flag BW	Indicates if interface is being used (1/0)
	Flag IPv6	Indicates if the interface supports IPv6 or not (1/0)
	Flag Multicast	Indicates if the interface supports multicast or not (1/0)
	Last Time	Indicates the time of the last packet received
	N Recv	Indicates the number of received packets
	N Drop	Indicates the number of dropped packets
	Flag Send	Indicates if Bad Receive packet was sent

Table 10 - User database

Each user sends his context to CB in the beginning of the scenario, and each time he changes something in any interface, it is necessary to re-send users context information. Each user has a fixed User ID to identify them even when his IP interfaces addresses change. Besides, he is associated with a profile Type (business, gamer, groupie) with different needs and preferences. As users can have many interfaces, such WiFi, WiMAX and UMTS, and also several interfaces by each technology, every interface has it own context information. Each interface has an IP address, IP address of connected AP, and Flag BW to inform if an interface is already receiving a data flow. An interface also has Flags to inform if it supports multicast (Flag Multicast) and IPv6 (Flag IPv6). TNCP keeps this context information in its context database, in order to send packets with this context in Users Context message header (Table 11), when it is necessary.

Header Field	**Function**	
Message type	Identifies packet as User context Message (User Context)	
User ID	Number to identify each User	
Type	Identifies a profile to each User (Business, Gamer, Groupie)	
Interface	**Sub Field**	**Function**
	AP	Identifies the IP address of AP, connected to Interface
	Flag Active	Indicates if interface is active or inactive (1/0)
	IP	Indicates the IP address of the Interface
	Flag BW	Indicates if Interface is being used (1/0)
	Flag IPv6	Indicates if the Interface supports IPv6 or not (1/0)

	Flag Multicast	Indicates if the Interface supports multicast or not (1/0)

Table 11 - Fields of the User Context message header

In order to emulate wireless in mobile terminals as explained before (4.2.4), besides error models and links ups and downs, it is necessary to have a flag (Flag Active) for each interface to know if the interface is up or down. When an interface goes down/up, it is important to update CB with the new user context (User context message header). Specifically, if the interface goes down while receiving data packets, a Warn Move message (Table 12) is triggered in order to inform the event to NUM. Then, NUM reacts according to this information in order to forward data traffic to another user's interface, allowing user to continue receiving the data content. The Warn Move header only contains the IP address of the AP connected to the interface (AP address) and the Flow ID that is being received by that interface.

Header Field	Function
Message type	Indicates if a receiving interface downs or receives under QoS requirements (Warn Move or Bad Recv)
AP address	Indicates the IP address of the AP connected
Flow ID	Indentify the Flow ID received in interface

Table 12 - Fields of the warning messages header

Other important function implemented in these TNCP agents is the measure of QoS parameters of the received data flows. User records in its interfaces structures the number of data packets received and dropped, and also the time of last data packet received. With this information, TNCP can measure QoS of each interface, comparing the loss rate and delay, about a Flow ID of certain CoS, with a table with maximum delay and maximum loss rate per CoS (Table 13). This table is manual defined by each user according to the expected behaviour of each CoS. When the QoS decreases under the minimum to ensure a good service, TNCP sends a Bad Recv message (Table 12) to NUM with Flow ID and AP address where it is receiving badly. Then, NUM tries to find a better path to forward data packets of the bad received Flow ID.

Field	Function
CoS Number	Indicates the number of CoS (0,1,2,3,4,5)

Max Delay	Indicates maximum delay for each CoS
Max Loss rate	Indicates maximum loss rate for each CoS

Table 13 – Database of the minimum QoS values per CoS

Next diagram (Figure 15) resumes all operation of the TNCP agent in order to a better understanding of the entire process. In the left side it is explained the down interface related to mobility, and in the right side it is explained the users QoS experience and their feedback. In the centre, it contains a simple process using a timer to know when an interface stops receiving data packets, assuming a trigger time of one second.

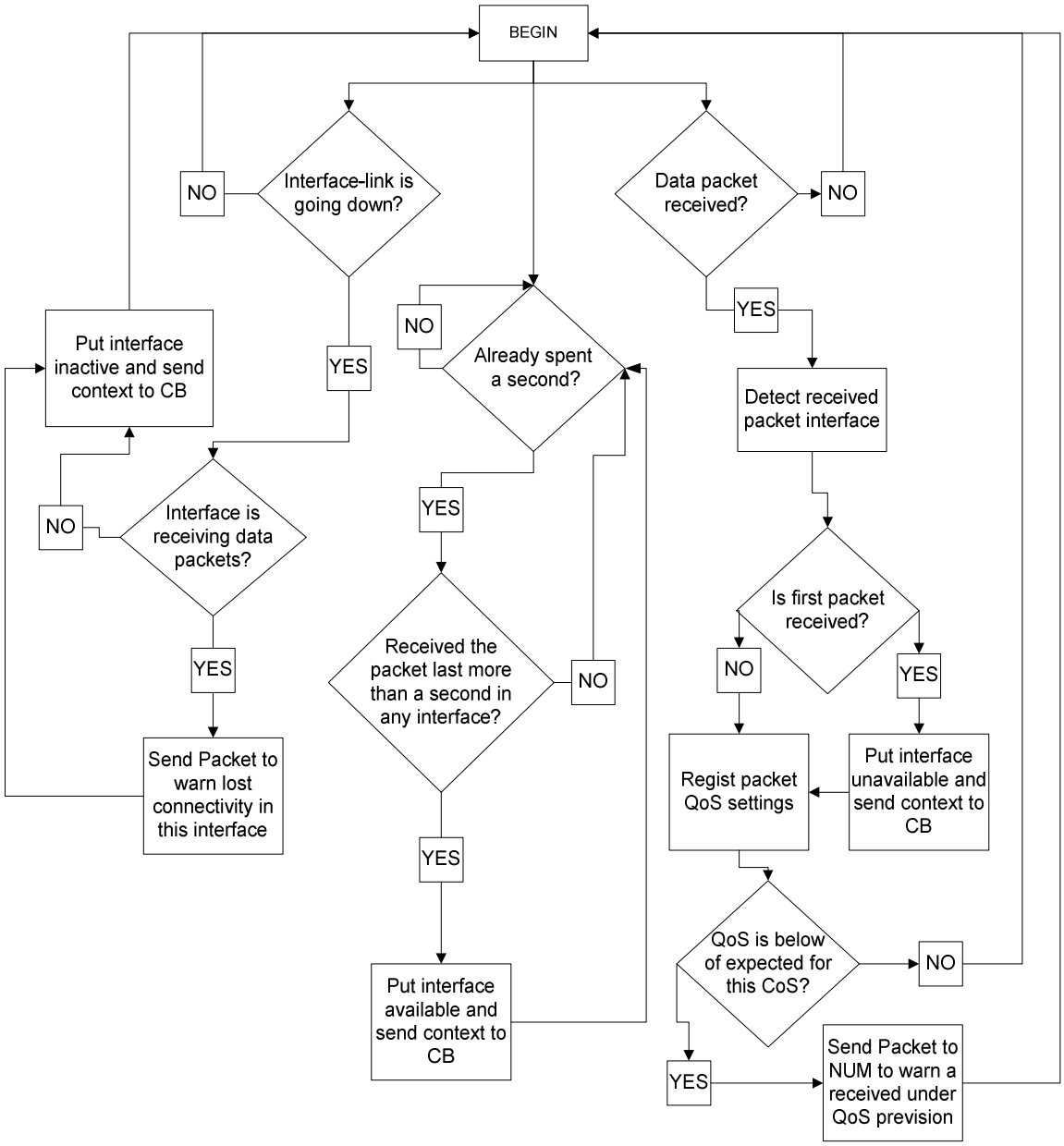

Figure 15 - Block User diagram

In the left side, the emulation of mobility is illustrated. Since mobility emulation is used, mobility means loss or acquisition of connectivity in one of the links between a user and an AP. In the scenario, only the number of interfaces down/up is chosen and they automatically interact with TNCP to emulate wireless mobility. In the centre of Figure 15 it is showed the process to detect when an interface stops to receive the data content in each interface. It is configured a timer, scheduled for each second, that observes if the interface recently received data packets, viewing the time of the last packet received by the interface. In the right side, it is illustrated the

process to control the QoS received by each interface. This process is supported by the loss monitor agent (4.2.7) and it saves the relevant information of the received packets (last time, dropped packet and received packets) in order to compare them with the expected values.

4.2.6. Context-Aware Access Network Selection

This section is related with the Algorithm of AP selection and the information used in the decision computation. This algorithm code itself is the centre of network access decision, since it uses the APs and Users Context collected by other functions. Basically, this algorithm could be described as a function that receives user context, APs context and QoS requirements, and returns the best AP to the FID desired. This algorithm is included in the NUM, allowing an intelligent choice of AP, before the core path is selected to a certain FID of a certain user. The algorithm constructed can be divided into four generic parts (3.3). First, it is necessary to build a list of candidates AP, based on connectivity and QoS parameters of each AP (delay, loss rate and bandwidth). Next, APN matrix can be constructed based on the type of each candidate AP. Then, UP matrix is also created from user profile (business, gamer, groupie). After this, only matrix operation will be executed in order to obtain a normalized ranked list of APs.

To select an AP, it is necessary to analyse the characteristics of all APs in the network, so AP database (Table 14) is in NUM, where the AP selection function is used. Aiming that an AP becomes a part of the candidates list, it is necessary to analyse its Max Bandwidth, Current Bandwidth, average Delay and Loss rate. If these QoS requirements are above the minimum requested, AP Type, FIDs and CoS information is used to rank the AP in a normalized list (3.3).

The algorithm returns the best AP to user receiving the required flow, determining the end of the AMT and the last sub-AMT. Then, it is chosen the entire path between data source and selected AP considering the bandwidth available and delay of each path. This path core selection is not implemented in this work, being made in a complementary Thesis. Both works were integrated with each other, forming a complete architecture, capable of efficiently select the best multiparty delivery, in a dynamic way.

Field	Function
IP address	Indicates the IP address of the AP
Max Bandwidth	Indicates the maximum bandwidth
Current Bandwidth	Indicates the current bandwidth available

Delay	Indicates Current AP delay
Loss rate	Indicates Current AP lost rate
Type	Indicates the profile of the AP (WLAN, WiMAX, UMTS)
FIDs	Indicates the Flow Ids used by the AP
CoS	Indicates the Class of Service for each FID

Table 14- APs database

Since the wireless mobility and wireless error model are emulated, the scenario interacts with Table 14 and TNCP to construct and keep the APs information (eg delay, loss, and bandwidth). In AP database is saved all FID that across the AP and their respective CoS, in order to exist more information to decide the best AP to each FID.

4.2.7. Others Relevant Changes

In order to collect the information about the traffic application requirements, a command on the UDP Agent was created to send a message to CB with this information. Since each CBR or EXP application is attached to an UPD agent, it was chosen to implement this command, due to its simplicity comparing to the same implemented solutions in traffic applications. This modification is important not only to start the scenario, registering traffic application settings, but also when new traffic application appears in the internet.

For registering traffic application requirements, the following message header (Table 15) was created. This header contains Flow ID and Multicast group used by the application, as QoS parameters (rate and CoS).

Header Field	Function
Message type	Indicates the type as a Traffic Registration message (Traff Reg)
Flow ID	Indicates the Flow ID (1, 2, 3...)
CoS	Indicates the number of CoS (0,1,2,3,4,5)
Rate	Indicates the bandwidth of traffic application (kbps)
Multicast group	Indicates destiny IP multicast address of the traffic application

Table 15 - Fields of the Traffic Application Context message header

Another important change regarding architecture efficiency was the modification of the loss monitor agent. This agent can be attached to all nodes and it is responsible for receiving the data packets that arrive to the destination, before dropping them. As only terminals are the end of data packets, we configure loss monitor agents to each one in order to monitor QoS. This agent uses RTP header to verify sequence numbers of the received data packets and detect how many packets were lost, through the difference between expected sequence number and number received. Loss monitor does not keep information, but each time it receives a packet, it sends information to TNCP. Then TCNP, with saved information, analyses the QoS of the received flow, calculating the rate of drop and the delay between each two sequential received packets.

Besides these new functionalities, two problems intrinsic to NS2 were resolved. It was necessary few modifications in the code, but a harder work of debug, in order to find the problems and fix them. First problem is related with classifier, which did not mark some packets with correct CoS. The second problem is related with data packets to change between sub-AMTs. The multicast classifier needed to be changed to permit forward data traffic, of an unknown interface, to another multicast tree. When ON change IP destination, the data packet has to enter in a new multicast tree, which is not expected for this packet.

4.3. Summary

This chapter described the NS2 implementation of the architecture. The limitation of the NS2 was addressed, specially the integration of multicast mobility in wireless environments, which is a huge disadvantage and required turn-around solutions. All agents, databases and messages were exposed in detail to a better comprehension of the interaction between components of the architecture. Besides the descriptions about the components and wireless emulation model, other relevant changes not directly connected to the principal components were exposed.

5. Architecture Evaluation

This chapter presents the evaluation of the proposed architecture based on the results of the simulation through different scenarios. These scenarios were chosen in order to give a better analysis of the architecture, specially focused on the implementation extensions performed (4.2).

This section focuses on the most relevant results in architecture evaluation, since it is possible to obtain a large collection of them.

Section 5.1 describes the main scenario configuration as a condition to achieve the main results obtained along the entire chapter. Section 5.2 analyses the impact of MTs number in the architecture results. Section 5.3 presents the results in several scenarios, with a variation in the number of APs. Section 5.4 tests the influence of non multicast support nodes in a network scenario with core nodes that do not support multicast. Section 5.5 performs the evaluation of the core ONs' influence in terms of overhead and time of receiving back after a movement. Section 5.6 focuses on the effect of groups of users according to resources or network conditions. Section 5.7 provides an assessment of different methods to select an AP based on context information. Finally, section 5.8 resumes the most relevant results.

5.1. General Considerations

In order to obtain results in different situations more easily, it was created a generic scenario with input parameters such as number of ingress, egress and core nodes, core ON, APs, MTs, data sources, data flows, and sessions. NS and scenario seeds are also important inputs, since the results are the same for each seed allowing the repeatability of simulations. NS seed is changed to obtain different results for the same scenario in order to treat them statistically (average values and confidence intervals). Scenario seed is used to change almost all values of it, such as links between nodes, but also to change traffic conditions and users' profile. However, the topology code implemented automatically generates a scenario based on input parameters and configuration rules, easing the evaluation of different situations. In order to understand why those scenarios were used, an example of the topology used along the entire section, with some changes, need to be considered.

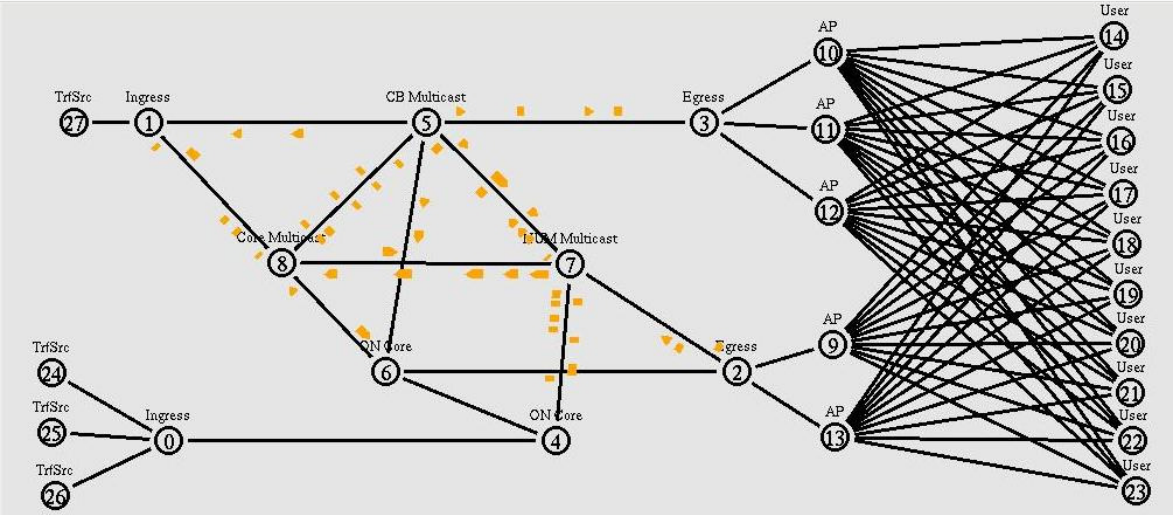

Figure 16 - Example of an evaluated scenario

As presented in the image, the scenario has 4 data sources connected with 2 ingress nodes. Between 2 ingress nodes and 2 egress nodes, 5 core nodes are used, of which 2 are ONs. Then, 5 APs interconnect the 10 MTs (multihomed) with the egress nodes. The orange packets in the figure are only a simple example, and it is caused by the flooding process to discover paths between Traffic Sources and APs.

Excluding wired links with error model to emulate wireless, the other links are configured with a random delay between 1 and 2 seconds and a bandwidth between 5 and 7 Mb. In wireless emulation part, all links are configured as the model presented before (4.2.4), changing dynamically depending on the number of data receivers for each AP.

In what concerns to the data traffic, all flows have a packet size of 1000 bytes and an average rate of 100 Kbps. The EXP is an exponential traffic, configured to have 80% of the time with a rate of 125 Kbps and 20% with 0 Kbps. Since CBR is a constant bit rate, it always presents the rate of 100 Kbps. The CoS of each flow is randomly chosen, but it is guaranteed that more than an half of the traffic is BE to simulate a real network. It was used the six CoS integrated on MIRA, defining the maximum of LB to each CoS: signaling, routing, EF, BE, AF1 and AF2. Signaling and routing classes were configured with 1.25 % of link LB each. BE class has 65% of link LB, and AF1 and AF2 have 13% for each one.

NUM and CB are located in the core network, randomly distributed, as the core ONs. All ingress and egress nodes, APs and data sources need to have the ON function configured.

Session setup is automatically initiated in NUM with no request from the users; in the future it will be triggered by the SM. After the first second to stabilize the system (discovery paths

and flows/users registration), session setup is generated in NUM with 2 flows to 20% of the users, randomly chosen at each new second. The simulations have a total time of 20 seconds, previously configured, due to the computational effort for higher times. The results for the same number of sessions improve as the simulation time increase. The scenarios are constituted by some elements of each parameter, in order to decrease the charge of computational effort and the time to obtain results from the scenarios.

Some measurements with their respective graphics (overhead, delay, loss) are presented along the entire section, so a brief explanation is described next.

Overhead is presented in percentage $\left(\frac{\text{control bytes}}{\text{total bytes}}\right)$ along with the number of control bytes in some cases to allow a better understanding, because a better overhead percentage does not necessarily mean less control bytes.

The average delay in the entire network and per CoS is measured, in seconds, according to the number of sessions established.

Loss is another important measure to evaluate the network and the architecture proposed. Like delay, the entire network and each CoS will be used to get the measures. Loss is showed in percentage $\left(\frac{\text{bytes}}{\text{bytes}}\right)$, according to the number of session setups.

Other important results, which may improve the analysis of the implemented architecture, are the percentage of sessions blocked, because they allow us to evaluate the capability of each scenario according to network entities.

5.2. Influence of MTs Numbers

The behaviour of the network considering the number of MTs in the scenario is one of the most important aspects to bring into account in the evaluation, since the number of users per session (20%) is related with the total number of users. It is relevant to analyse the QoS experienced by the users with different number of MTs, in order to receive data flows.

Ingress	Egress	Core	Core ON	APs	Data Sources	Data Flows
2	2	5	2	6	4	20

Table 16 - Fixed parameters to evaluate the influence the Number of MTs

The fluctuation between the number of sessions for each MTs number (5, 10, 15) in the network allows us to analyse changes in several parameters, like overhead, delay, loss and CoS treatment. Table 16 shows the fixed parameters, considering a favourable scenario to test the MTs influence.

Overhead parameter, caused by control packets, is important to evaluate the proposed architecture, considering that implemented control messages do not charge the network significantly. Figure 17 allows the comparison between 3 different number of users (5, 10, 15), while the Figure 18 illustrates the percentage of control message, in terms of all packets in the network. The Figure 19 presents the percentage of blocked flows, which helps to understand the results achieved, that show the capability of serving sessions, according to the number of users.

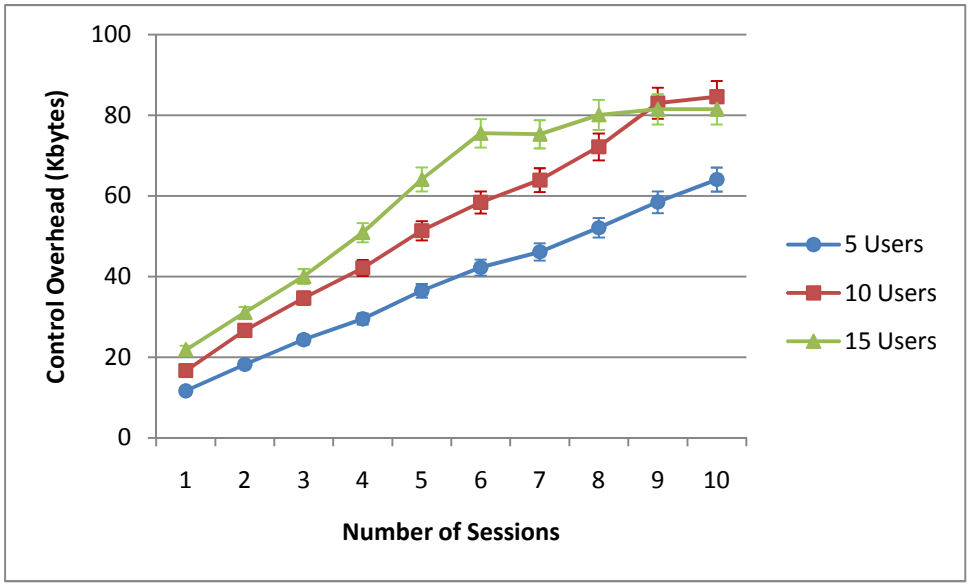

Figure 17 – Control Overhead (Kbytes) per number of sessions, with several number of users

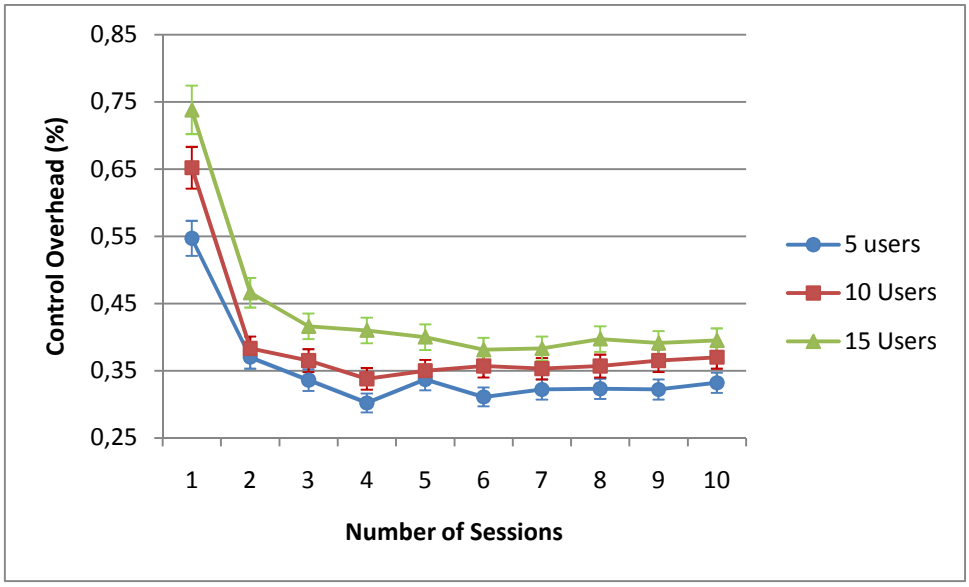

Figure 18 – Control Overhead (%) per number of sessions, with several number of users

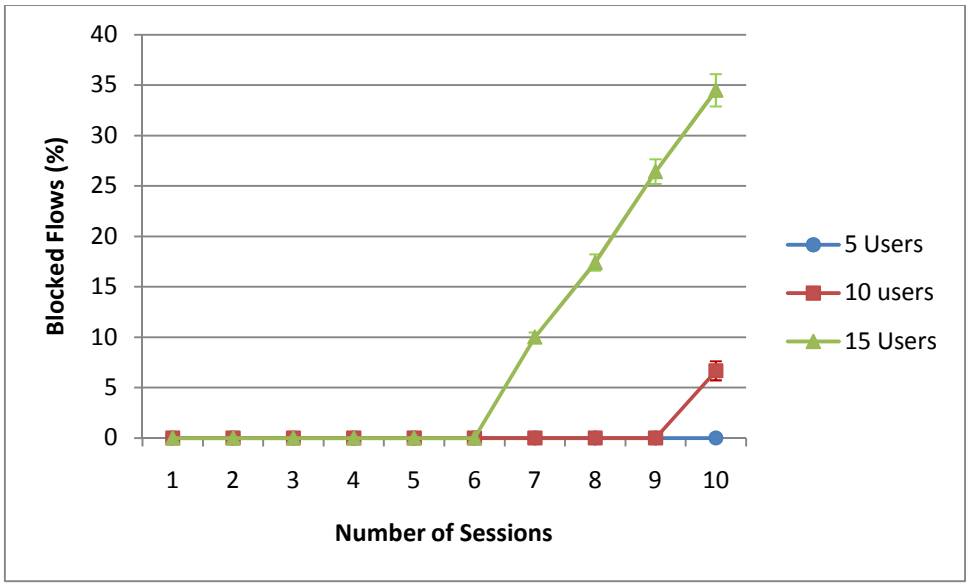

Figure 19 - Blocked Flows per number of sessions, with several number of users

The results presented in Figure 17 shows that the overhead increase in accordance with the raise of the number of users. However, when there are 15 users, the growth is not linear: from 6 sessions, the served sessions stabilize and any session requested is blocked. The case of 10 users also presents stabilization from 9 sessions. These specific results can be confirmed in Figure 19, where it is showed a linear increase of blocked flows. One flow is blocked when network resources are enough to satisfy flow requirements, such as APs overload. According to Figure 18 there is a low level of overhead as the number of sessions and users increase. The value of

overhead percentage tends to stabilize around 0.35 %, independently of sessions and number of users, which is not critical considering the amount of control information exchanged and the number of users. The higher value for 1 session is based in the generation of few data flows comparing to control messages, since initial users and sources context messages are the same independently of the number of sessions.

Network delay and losses between data source and MT are presented in Figure 20 and Figure 21 respectively.

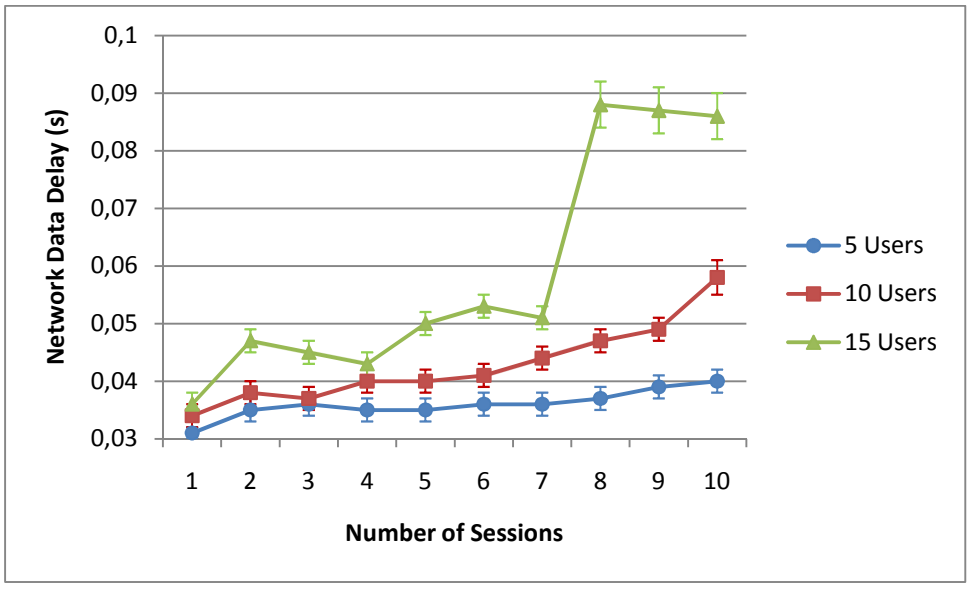

Figure 20 - Network Data Delay per number of sessions, with several number of users

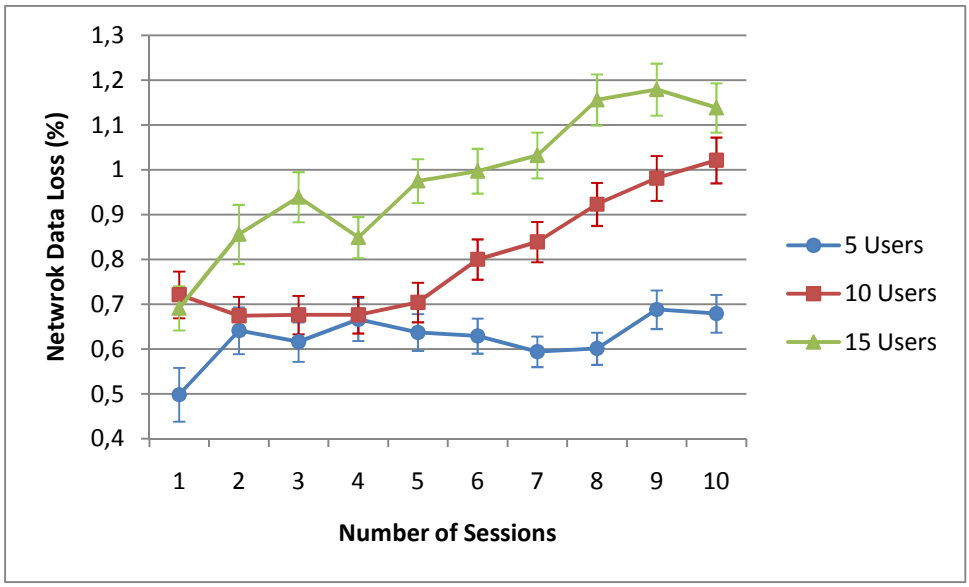

Figure 21 – Network Data Loss per number of sessions, with several number of users

From the results obtained, it can be stated that the delay of delivered data packets and the losses observed behave according to the expected (Figure 20 and Figure 21). Figure 21 results are not as linear as delay, because the loss rate is statistic and its results become more linear in a longer period of time. However, the graphic lines with different number of users show the expected trend: a decreasing performance in a scenario with higher number of users. Scenario with 15 users evidences a delay and loss stabilization from 8 sessions, when the limit sessions, established to the network resources, is reached. With 8 sessions to 15 users, especially in the delay graphic (Figure 20), there is an abrupt growth that can be explained through the high quantity of BE data, allocated in some APs, increasing the number of collisions.

Since more than an half of the data traffic is BE, this CoS data traffic has a huge impact in network data delay. However, it is relevant to analyse the delay and loss of each used CoS, since it was used a QoS based in DiffServ classes previously configured. In order to give a better explanation and optimization of the process, it is showed the EF and BE class only. It was chosen EF and BE CoS because they have a distinct treatment, representing elite QoS and non QoS treatment, respectively. First, the delay for both classes will be compared and analysed, in order to evaluate the QoS treatment. Figure 22 represents EF class delay, while Figure 23 represents the delay of BE class. The graphic only starts from 3 sessions, since the 2 first sessions do not contain EF class traffic.

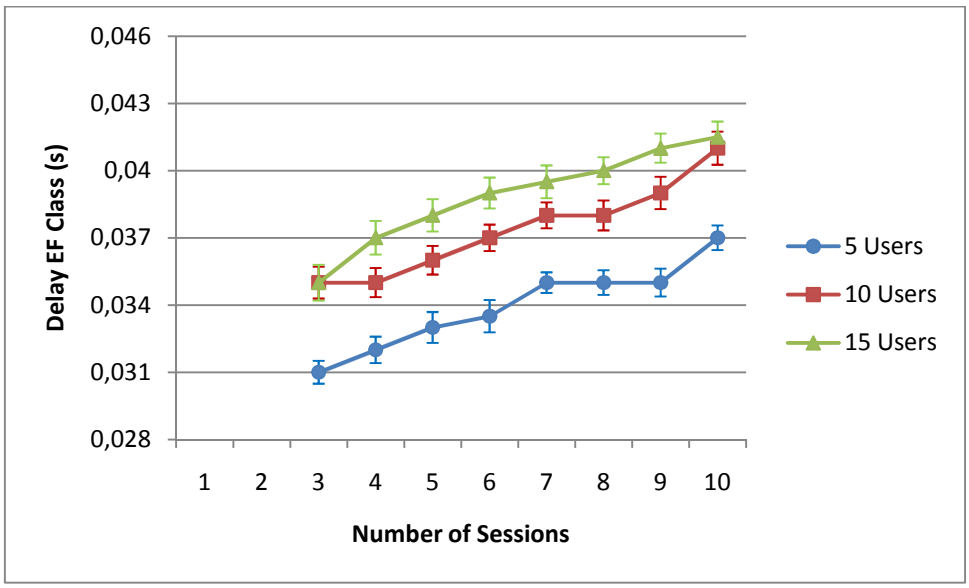

Figure 22 - EF Class Delay per number of sessions, with several number of users

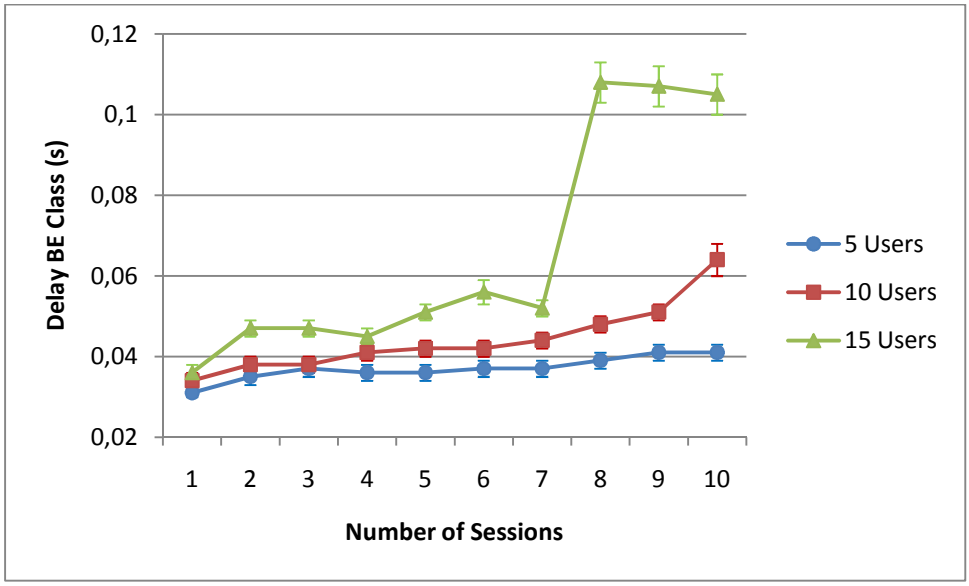

Figure 23 - BE Class Delay per number of sessions, with several number of users

As expected in both classes, delay increases, not only with the number of users but also with the number of sessions. However, in EF class, the delay of several users tends to be similar with high number of sessions, reaching the maximum delay allowed by this CoS (around 0.042 s). The delay of BE class is similar to the network data delay (Figure 20), as explained before. As intended, the EF class shows a better delay performance than BE one. BE class delay is limited by the network resources available, while EF class delay is configured, in order to have a maximum delay, independent of the number of sessions.

Regarding the loss per classes, Figure 24 and Figure 25 present the EF and BE class loss, respectively.

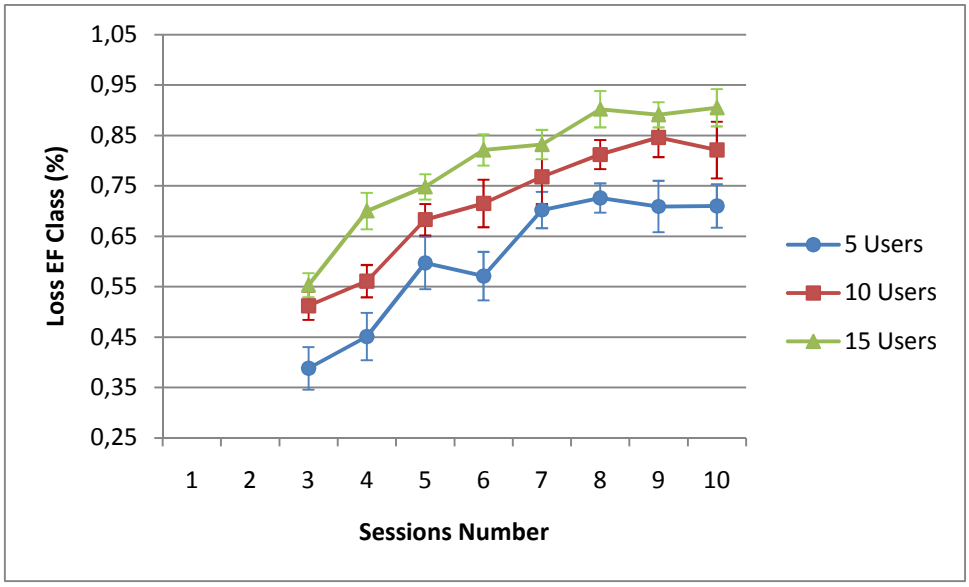

Figure 24 - EF Class Loss per number of sessions, with several number of users

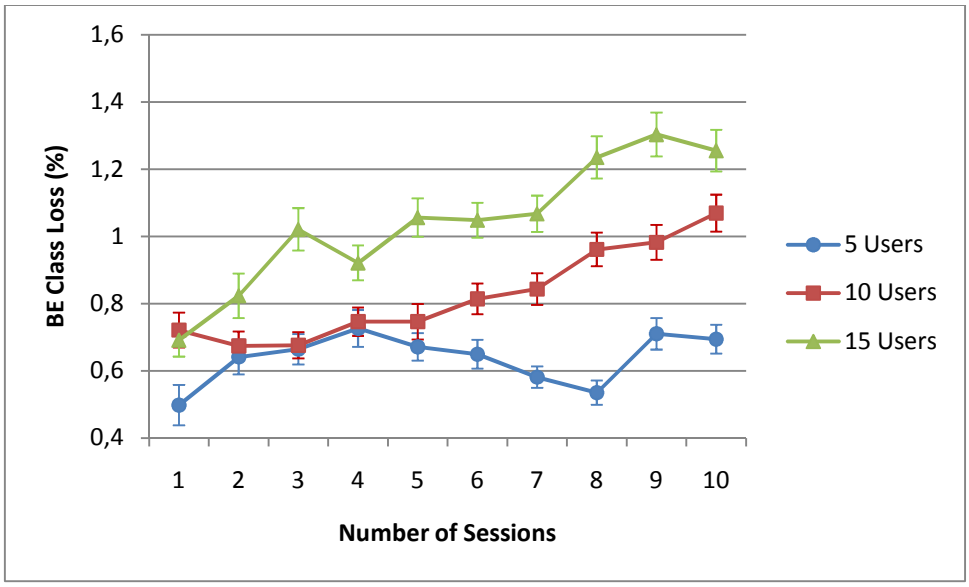

Figure 25 - BE Class Loss per number of sessions, with several number of users

The behaviour of the losses in EF and BE classes is similar to delay. The loss increases with number of users and sessions. The class EF tends approximately to 0.8 %, presenting a better performance than class BE, since its losses are limited only by network available resources.

5.3. Influence of APs Numbers

The APs number is a significant test to observe the behaviour of the data treatment in different situations: sometimes the User has only few APs available to receive the data flows. Cases of 4, 6 and 8 APs are tested with fixed number of 10 users and other parameters according to Table 17. The number of users per session is maintained in 20% of total users, so each session with two flows contain two users.

Ingress	Egress	Core	Core ON	MTs	Data Sources	Data Flows
2	2	5	2	10	4	20

Table 17 - Fixed parameters to evaluate influence of APs Numbers

It is important for each user to receive the data with QoS according to the expected one, independently of the accessible APs, since each CoS has their own requirements regarding to delay, bandwidth and losses. This test is also useful to observe the percentage of rejected flows with different number of APs, in order to evaluate the available and wasted resources, and also to plan an efficient network.

The control overhead is presented in Figure 26 and analysed together with the blocked flows (Figure 27).

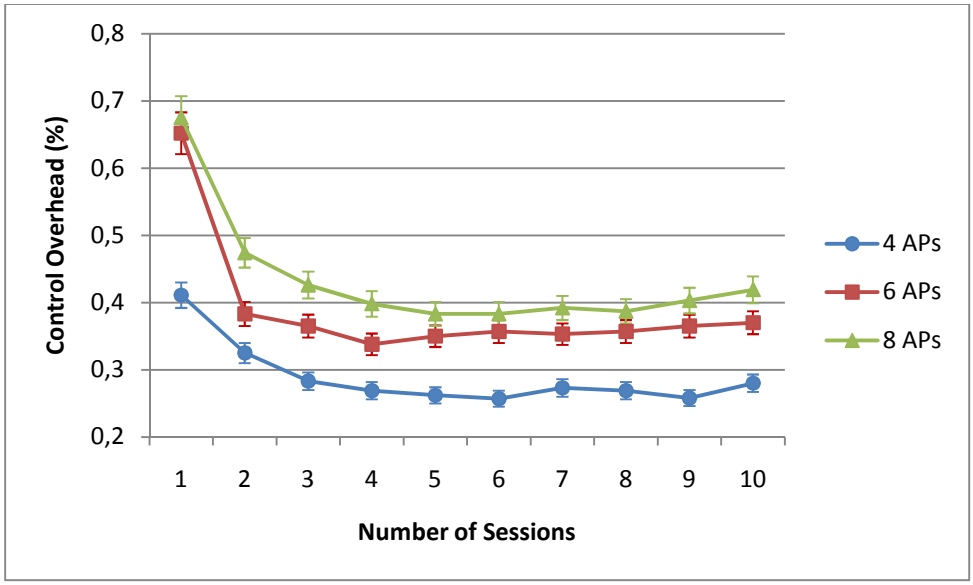

Figure 26 – Control Overhead (%) per number of sessions, with several numbers of users

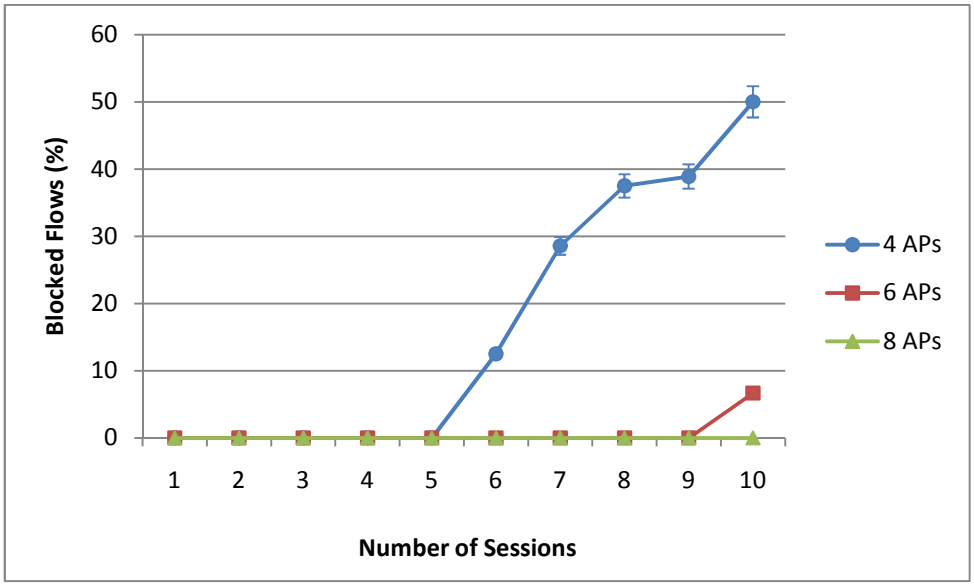

Figure 27 – Blocked Flows per number of sessions, with several numbers of users

As it can be observed in the Figure 26, the overhead has a low value that quickly establishes around 0.35 %. As expected, more APs mean more resources in access network and consequently more overhead of control. Besides this increment in the overhead, it does not have a significantly weight and control overhead can be viewed as independent of the number of APs. This is also true, since the number of served sessions is limited and takes into account network available resources. Figure 27 illustrates the blocked flows decreasing with the number of APs. For 4 APs it is evident a high number of blocked flows, showing that from 5 sessions, almost every sessions requested are blocked, which means it is impossible to serve 10 users in 4 APs.

Figure 28 and Figure 29 show the network data delay and loss, respectively. These QoS parameters are important to evaluate the general network behaviour.

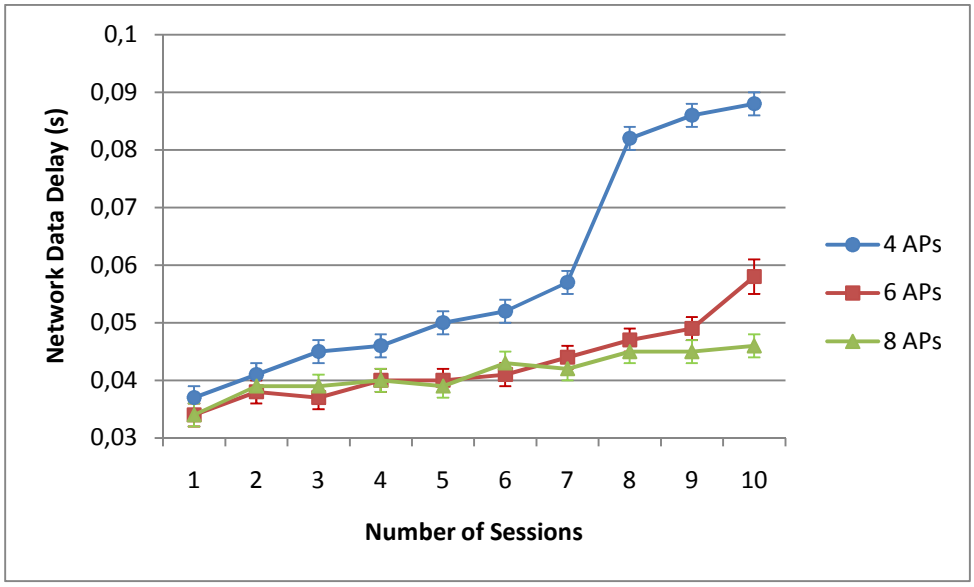

Figure 28 - Network Data Delay per number of sessions, with several numbers of users

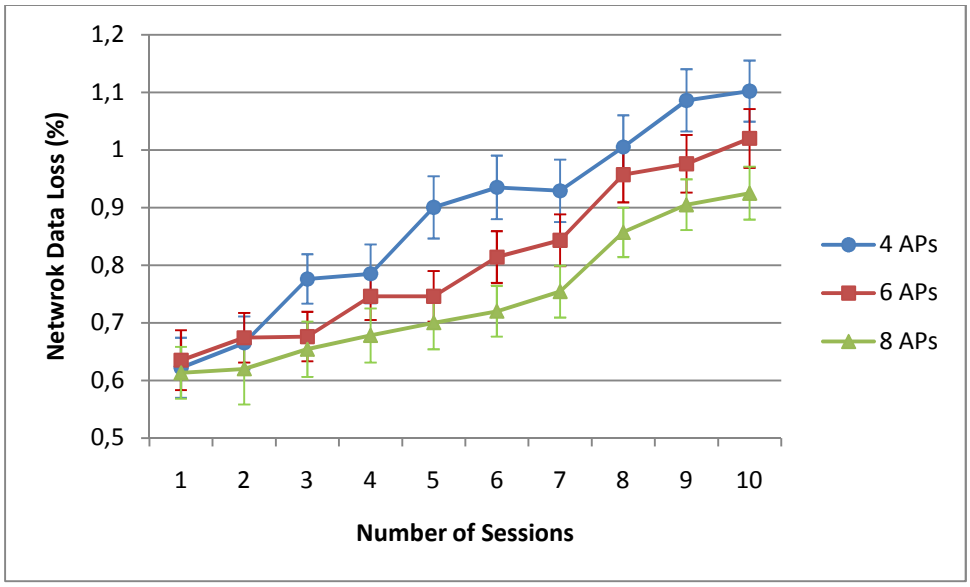

Figure 29 - Network Data Loss per number of sessions, with several numbers of users

As predicted, the data delay (Figure 28) has better results with higher number of APs, since more APs mean more available resources to distribute data flows sessions. The 4 APs curve has an exponentially growth for 8 sessions, due to the fact that all available APs resources are close to be totally occupied, having more collisions caused by a large number of users connected to the same AP. Analysing the graphic of the Figure 29, we can attend to the loss increase with the number of APs decreasing. Loss has a similar behaviour to delay (Figure 28), with a maximum percentage of 1.1 %.

Figure 30 and Figure 31 show the delay values referred to EF and BE classes respectively. It is necessary to observe the behaviour of a higher CoS and a non QoS class varying the number of APs.

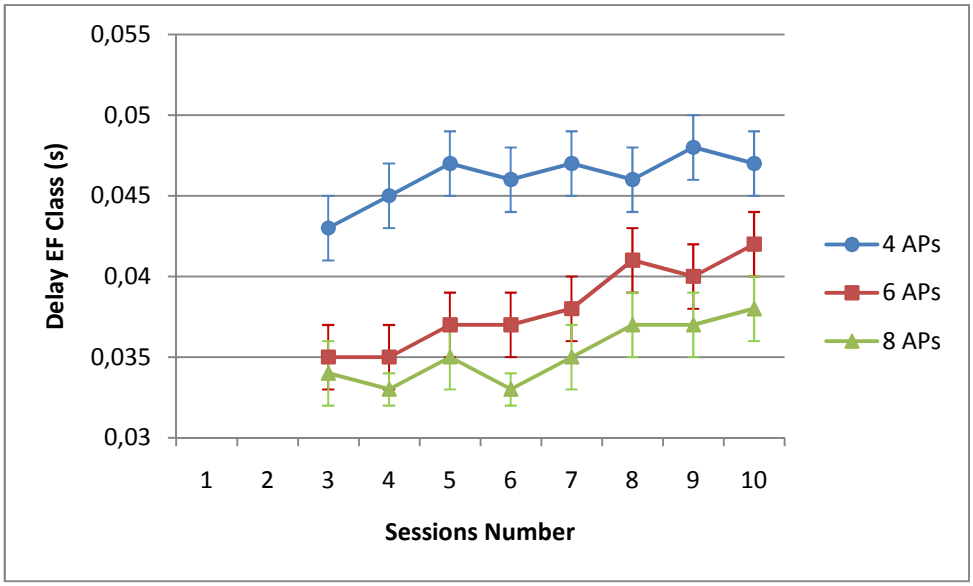

Figure 30 – EF Class Delay per number of sessions, with several numbers of users

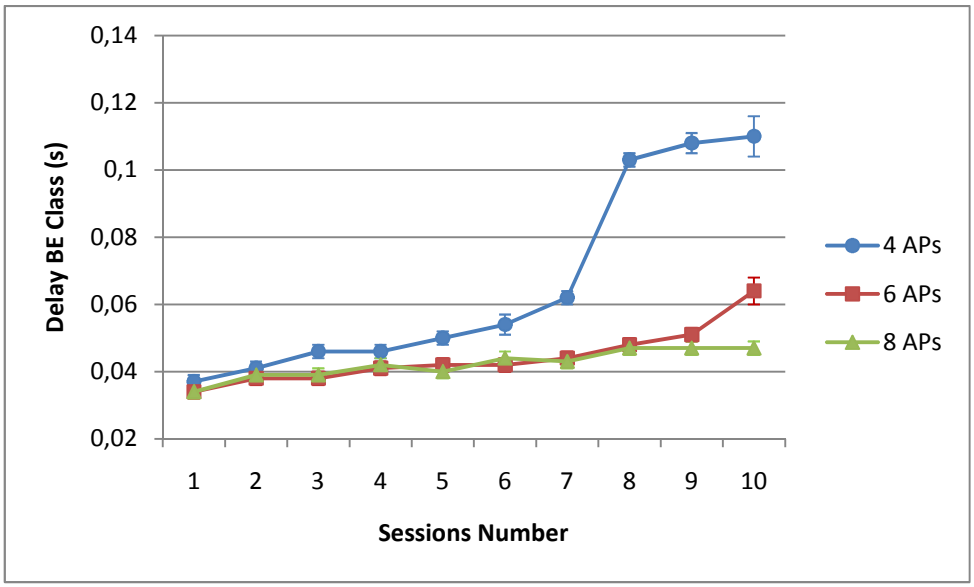

Figure 31 - BE Class Delay per number of sessions, with several numbers of users

The analysis of delay per CoS shows a higher value to less number of APs. The number of sessions increasing also gives a higher delay to both CoS. However, the growth of EF delay is smaller and possibly devalued. The delay for the 4 APs tends to stabilize from 5 sessions with a

maximum defined of 0.048 seconds. As noticed, the delay growth in the Figure 28 and Figure 31 are similar, because more than an half of the data traffic of the network is BE.

In order to complement the analysis of the CoS treatment, it is relevant to view the growth of the Loss in EF and BE classes, Figure 32 and Figure 33 respectively.

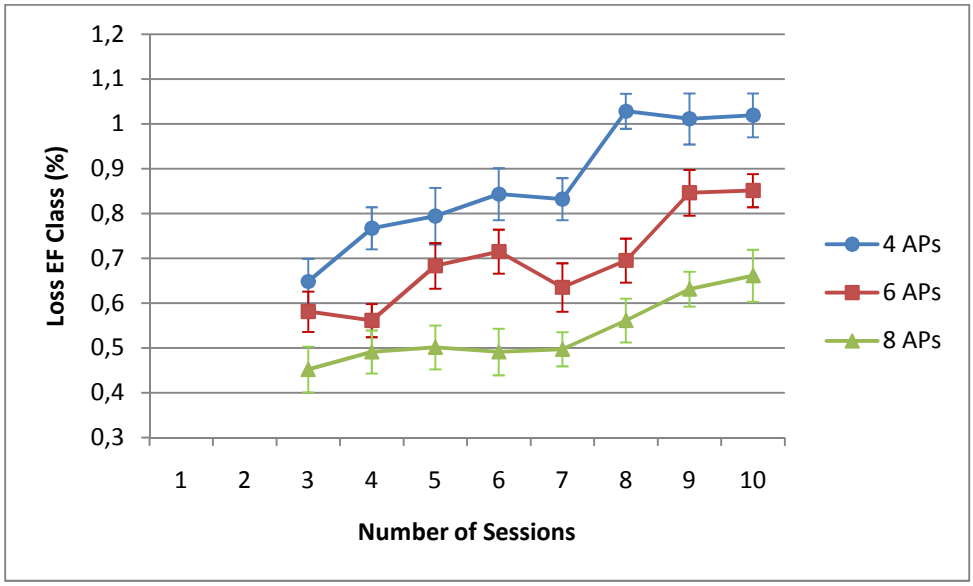

Figure 32 - EF Class Loss per number of sessions, varying the number of APs

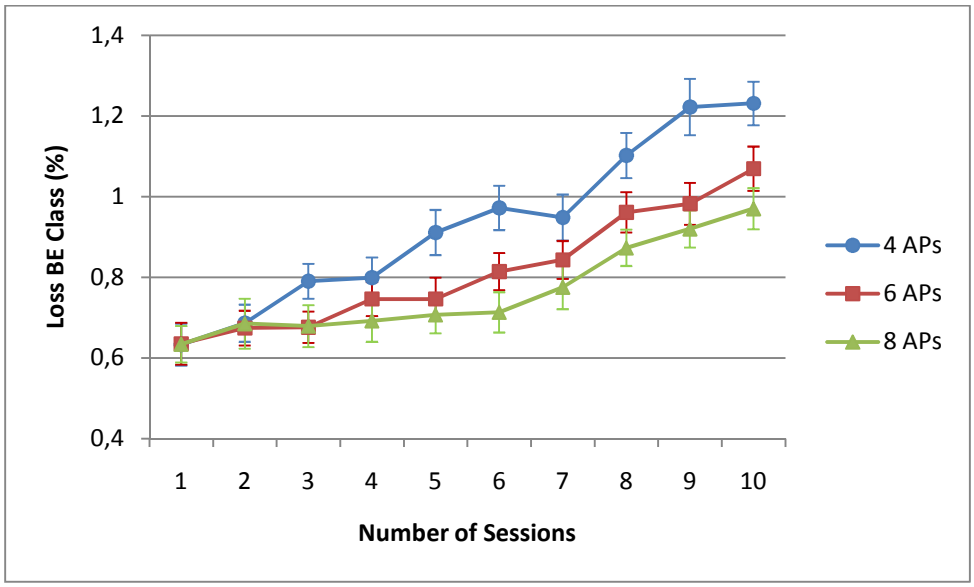

Figure 33 - BE Class Loss per number of sessions, varying the number of APs

The graphics of the Figure 32 and Figure 33 reveals an increase of loss with the number of sessions and with the number of APs decreasing. The growth of EF is less marked than BE, hitting

a maximum value around 0.9 %, lower than BE maximum loss, which is assigned by network available resources.

5.4. Influence of Unicast Core Nodes

As explained in section 3.2, the architecture supports different IP versions and a mixer of multicast and only unicast nodes through the ONs abstraction layer. It is important to evaluate the impact in control overhead, data delay and loss, with the configuration of nodes that do not support multicast. It is important to measure the percentage of unicast packets all over the network, in order to understand the impact of each unicast node in it. They are randomly distributed in the core and they have different impacts according to the chosen position.

Ingress	Egress	Core	Core ON	APS	MTs	Data Sources	Data Flows
2	2	5	2	7	10	4	20

Table 18 - Fixed parameters to evaluate influence of non-multicast core nodes

It was created a scenario with 5 core nodes, in which 2 of them were always ON because they are needed to support multicast to be the bridge between two different technology areas. The scenarios with 0, 1, 2 and 3 unicast nodes were tested. To a better focus analysis of unicast influence, the other parameters were fixed according to the Table 18.

The control overhead is presented in the Figure 34, varying the number of unicast nodes and number of sessions. Figure 35 allows us to understand the impact of each unicast core node in data packets.

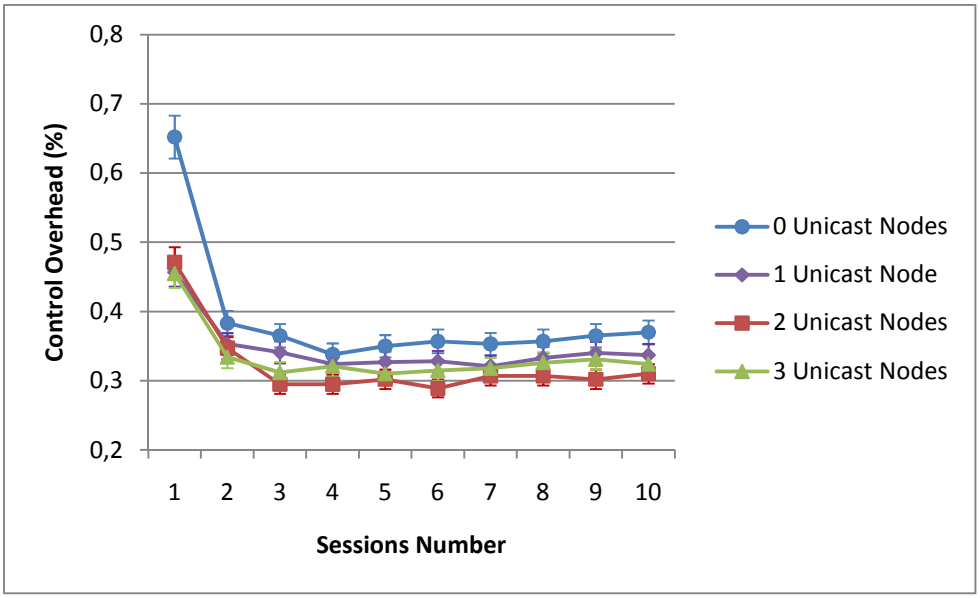

Figure 34 – Control Overhead (%) per number of sessions, varying the number of unicast nodes

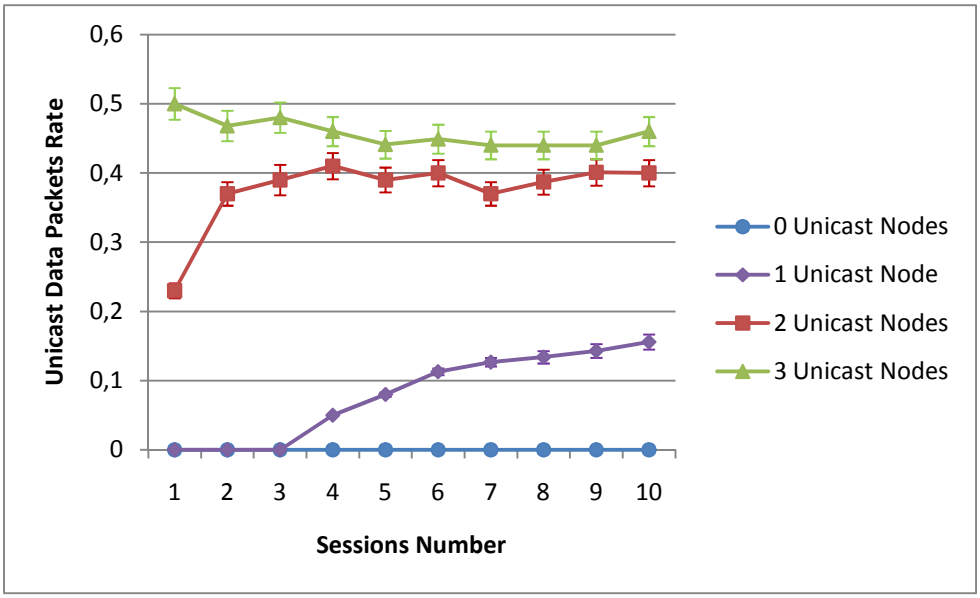

Figure 35 - Rate of unicast data packets per number of sessions, varying the number of unicast nodes

According to the graphic of the Figure 34, the behaviour of overhead control is similar in the different situations that vary with the number of unicast nodes. When all nodes support multicast (0 unicast nodes), the overhead of control is slightly higher than the other cases, but this difference might be neglected. In this approach it is irrelevant the technology used in the core network, since it presents an insignificant impact in the final network performance. The percentage of overhead of control tends to be about 0.35%. The Figure 35 reveals that the rate of

unicast data packets increases with the increase of the unicast nodes in the core network. It is important to highlight that the rate of unicast data packets for 2 unicast nodes is close to 3 unicast nodes, and distant from the 1 unicast node. Since unicast nodes are randomly distributed in the core network, the second unicast node is disposed in a path where large data traffic exists.

The delay and loss of the data network are presented in Figure 36 and Figure 37, varying with the number of unicast nodes along the sessions.

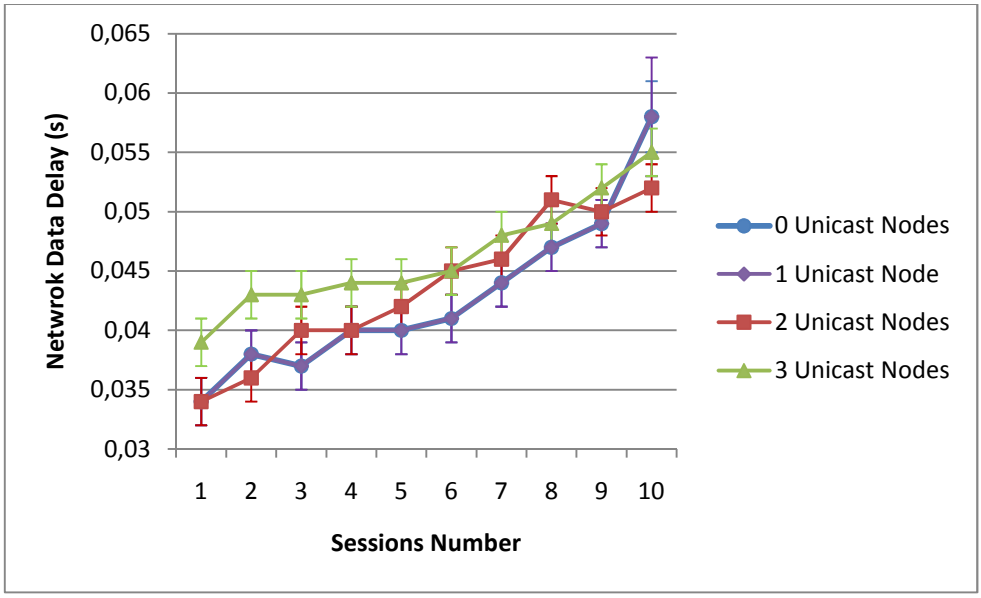

Figure 36 - Network Data Delay per number of sessions, varying with the number of unicast nodes

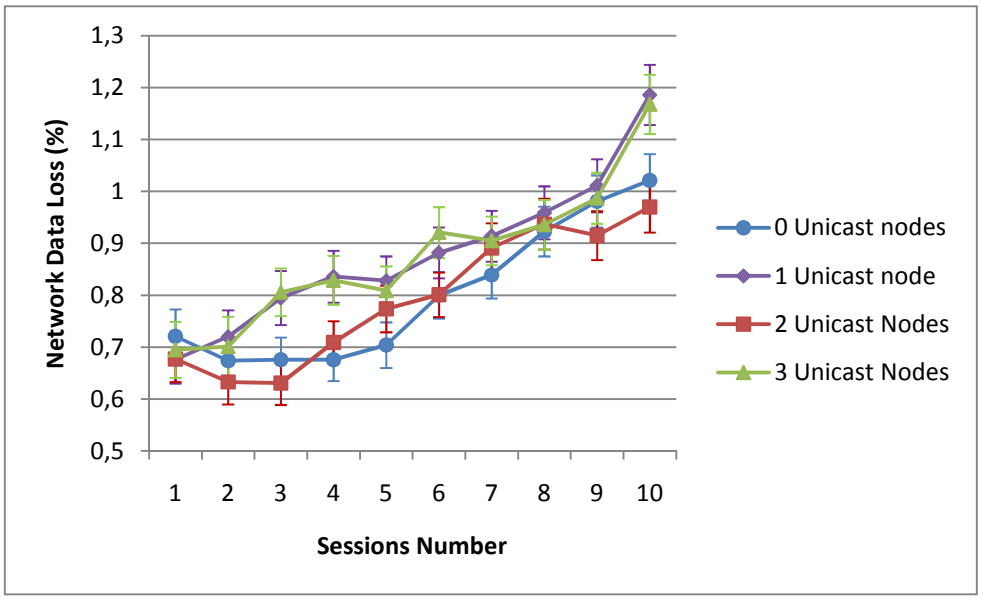

Figure 37 - Network Data Loss per number of sessions, varying with the number of unicast nodes

The results exhibit a similar behavior in terms of delay (Figure 36) and loss (Figure 37) as expected. The growth of the number of unicast nodes has little differences, although the error associated is significant, as it can be confirmed by the error bars. Delay and loss increase with the number of sessions. The presence of unicast nodes in the core network does not affect the performance of the network, maintaining similar delay and loss to data packets.

5.5. Influence of Core ONs

As described in section 3.2, the ONs must be in ingress, egress, APs and data sources. However, the number of ONs in the core can be chosen according to operator decision, from none to all. Due to this possible variation, it is important to study the influence in control overhead. Besides, the time that the user needs to received back data packets, after a movement, is a very important measure, since ONs facilitates the user movement with a fast reconstruction of QoS data path and multicast tree.

Ingress	Egress	Core	APS	MTs	Data Sources	Data Flows
2	2	5	7	10	4	20

Table 19 - Fixed parameters to evaluate influence of core ONs number

In order to make a detailed analysis of core ONs' influence, it is relevant to maintain the other scenario's parameters fixed (Table 19), in spite of the changes occurred in the number of core ONs. The users' mobility definitions, such as APs connections and disconnections, are maintained in all scenarios with different number of ONs. Considering a core network defined with 5 nodes, the cases 0 and 2 core ONs will be studied.

In order to evaluate the influence of the number of ONs in the core network, results concerning the control overhead (Figure 38) and time to a MT receive data back in new AP, after a movement (Figure 39) were obtained.

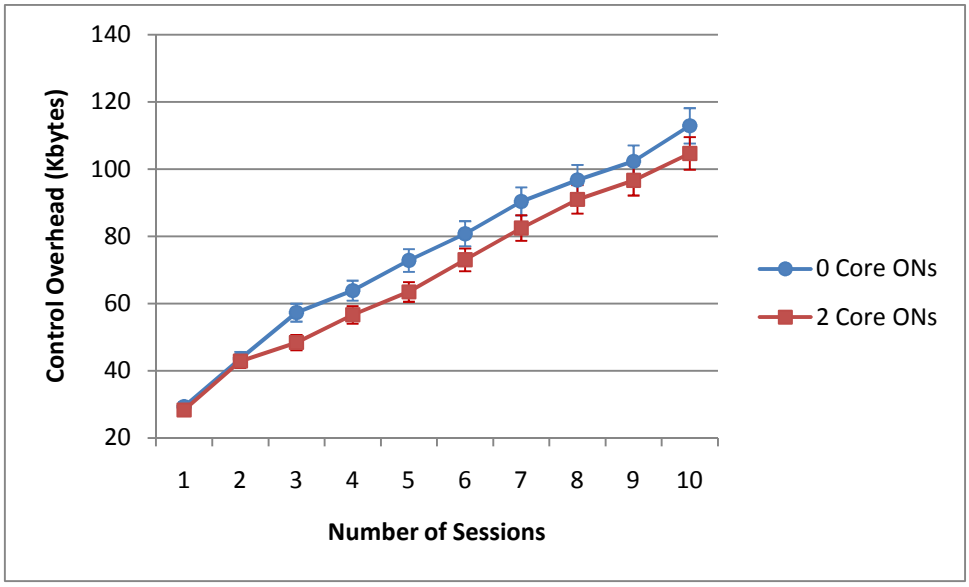

Figure 38 – Control Overhead (Kbytes) per number of sessions, varying the number of core ONs

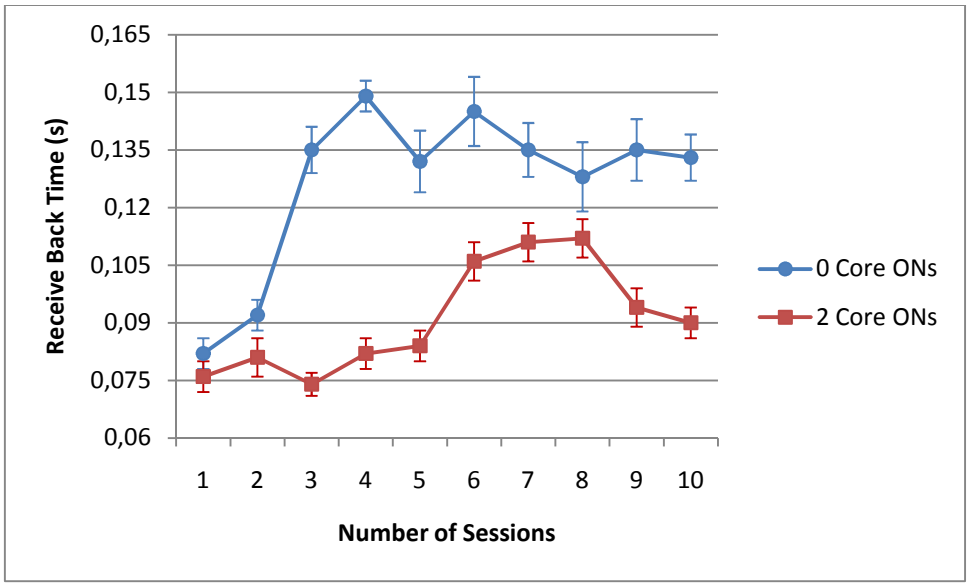

Figure 39 – Receive Back Time per number of sessions, varying the number of core ONs

As showed in Figure 38, the overhead of control for 2 Core ONs is lower than the result for 0 Core ONs. Initially, when the sessions are established, the overhead for 0 Core ONs is lower than for 2 Core ONs. However with MT's movements the situation turns over: when a MT changes to an AP, it is connected to another egress node; core ONs facilitate the handover not only in time but also in control packets to reserve a new path and build another multicast tree/branch. As previously described, Figure 39 confirms a better level of receiving back time with 2 core ONs, considering all number of sessions. However, the studied scenario is an uncharged one, especially

concerning to APs, which means that the time of receiving back depends mostly on the load of the used AP. When Warn Move message is sent through an overload AP or when MT receives back in an overload AP, the time of receiving back increases significantly, as we can see with several number of sessions (Figure 39). In scenarios where the number of core nodes is huge, the time of travelling across the core becomes relevant for the time to receive back after a MTs movement.

5.6. Study of Subgrouping

The Subgrouping concept was already described in section 2.4 being it associated with session context, allowing two users to receive the same content but with different codecs. From the multicast traditional perspective, the users are in the same group but in different subgroups. Subgrouping is also applied when a user that receives the same multicast group is divided into several APs, in order to maintain QoS for each CoS. This last aspect of Subgrouping has a special relevance in this study, due to its simple analysis through simulation results.

Ingress	Egress	Core	Core ON	APs	Users	Data Sources	Data Flows
2	2	6	3	7	15	2	12

Figure 40 - Fixed parameters to evaluate influence of subgrouping

The results refer to the behavior of the network when five users receive two flows for each session. The users have different profiles, so they attribute different preferences to subgrouping parameter. The performance of the network was evaluated varying the weight of subgrouping and maintaining the weights of the other parameters equals.

The subgrouping weight parameter influences the number of users that will receive the same multicast group in the same AP. A higher subgrouping weight means more users receiving same multicast group in the same AP.

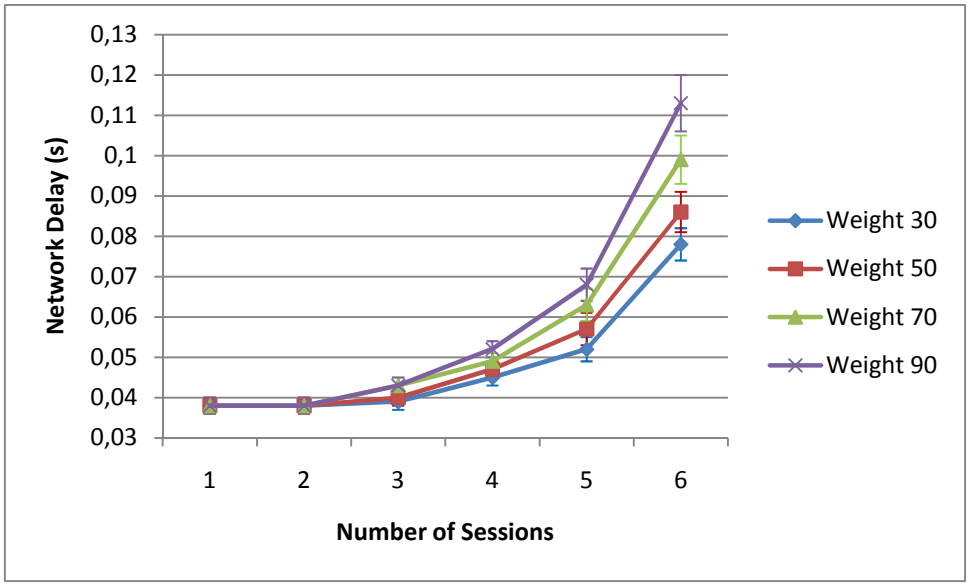

Figure 41 - Network Data Delay per number of sessions, varying with the weight of Subgrouping

Analyzing the Figure 41, it is noticed that, with the increase of the subgrouping weight and the number of sessions, the delay increases. Remember that it was used wired links to connect users to APs, configuring respective error models, so it is necessary to create copies of packets to the users that want to receive the same flow.

In order to have less control overhead and, consequently more subgrouping weight (Figure 42), network performance decreases, since it will be allocated the same AP to several users that want to receive the same multicast group. The losses are not presented, since they have a similar behaviour as the delay.

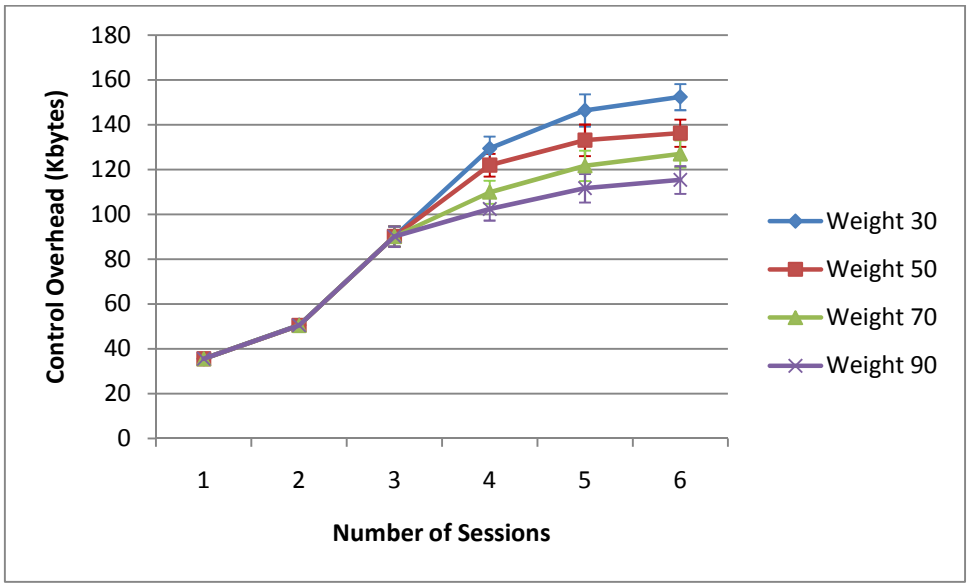

Figure 42 - Control Overhead (Kbytes) per number of sessions, varying the weight of Subgrouping

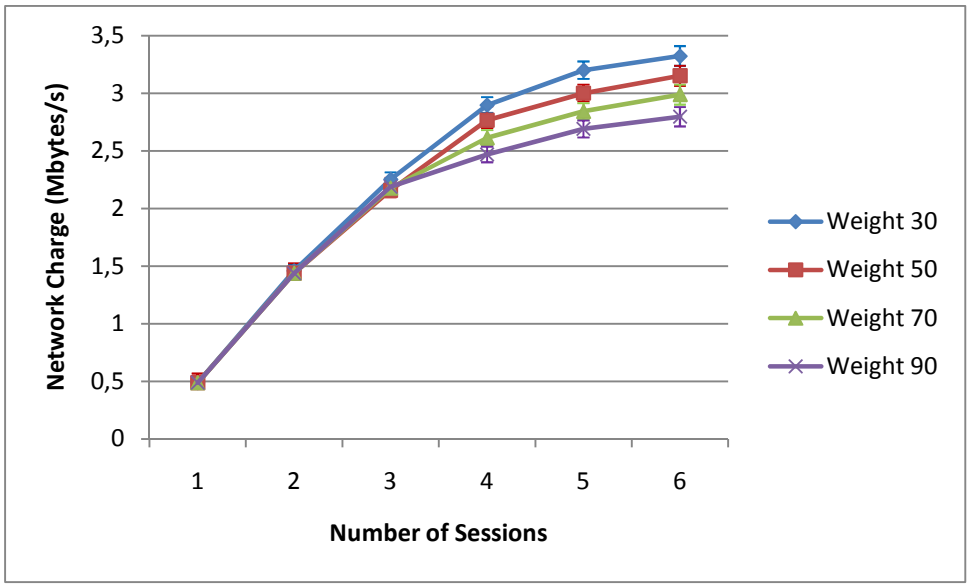

Figure 43 - Network load (Mbits/s) per number of sessions, varying with the weight of Subgrouping

At the other hand, the overhead and the network load reduce with the increase of the subgrouping weight. If it admits a higher weight on the subgrouping, the same AP and core path will be chosen more times, for the same multicast group, which means that it will not be necessary so many control messages to configure the network. This means also that the data traffic is lesser to serve the same number of users with the same sessions, preventing unnecessary copies. The best solution could be the equilibrium of these parameters, maintaining delay and loss values acceptable as lower charge and control overhead in the network.

5.7. Access Network Selection Methods (Random, Without CoS, CoS)

This test shows the advantages and disadvantages of each access network selection methods. The random method represents today the AP selection, based in the signal strength, so in a mobile environment it depends on user's locations, and in wireless emulated scenarios it corresponds to a random selection. The second method, Without CoS, treats all traffic with the same preference, being considered as BE. In this case, it is used a load balancing distribution only considering bandwidth as unique QoS requirement. The Users' profiles and Subgrouping weight

also become part of the algorithm in all approaches. Last method considers the entire algorithm adding the method before, not only weight to CoS, being the trend to attend the same CoS even in the same AP, but also the measure to avoid the priority class of each AP to be impaired, preventing the users to have a bad QoS of higher CoS.

Ingress	Egress	Core	Core ON	APS	MTs	Data Sources	Data Flows
2	2	5	2	7	10	4	20

Table 20 - Fixed parameters to evaluate influence of Access Network Selection Methods

Table 1 shows the fixed values used in order to compare the three methods results. The number of APs and MTs was chosen to guarantee that all flows of all sessions are served and a fair comparison is realized.

First it is important to evaluate the impact of control messages in the network through the Control Overhead (Figure 44 and Figure 45).

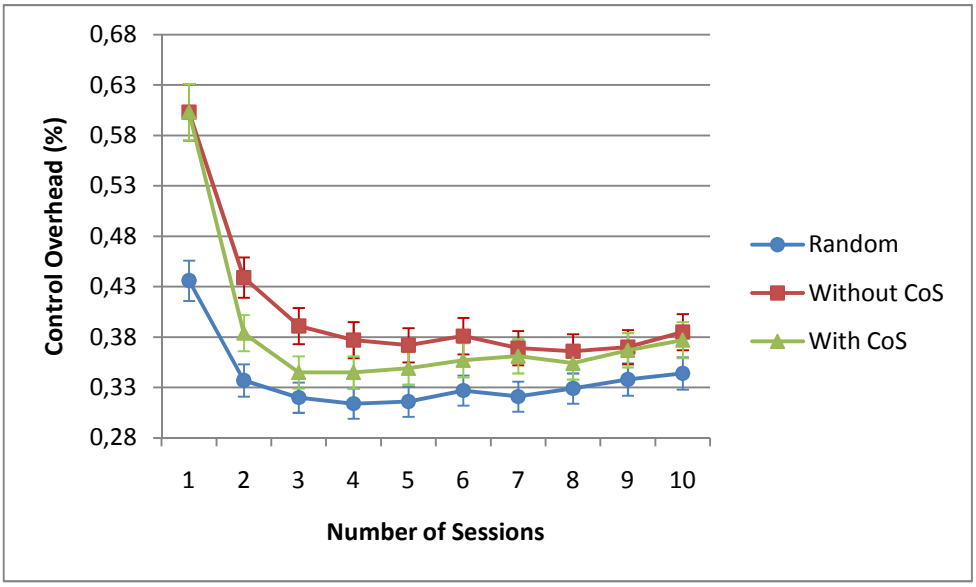

Figure 44 – Control Overhead (%) per number of sessions, varying Network Access Selection

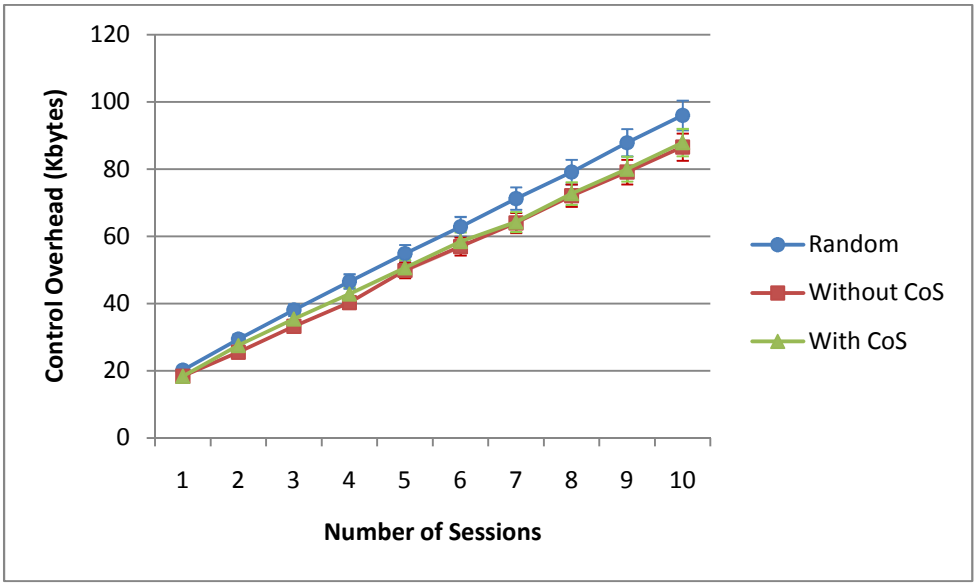

Figure 45 – Control Overhead (Kbytes) per number of sessions, varying Network Access Selection

As observed in the graphic of the Figure 44, Random selection has a fewer percentage of overhead, while selection without classes has the higher percentage. This result does not seem to be correct, since a random selection probably chooses different APs for users that want to receive the same flow, leading to the use of more control messages to configure multicast QoS path and multicast trees. The Figure 45 revolves all doubts, since it measures the number of control bytes used in each different selection, where the random selection values are higher than with and without CoS. The percentage overhead of random distribution presents a low value due to the increase of data packets in the network, generated by the increasing of multicast branches to several APs chosen to the same flow.

Figure 46 and Figure 47 presents the results of network delay and loss respectively. Before evaluated the CoS treatment, it is important to observe the entire network behavior, with several number of sessions, from 1 to 10.

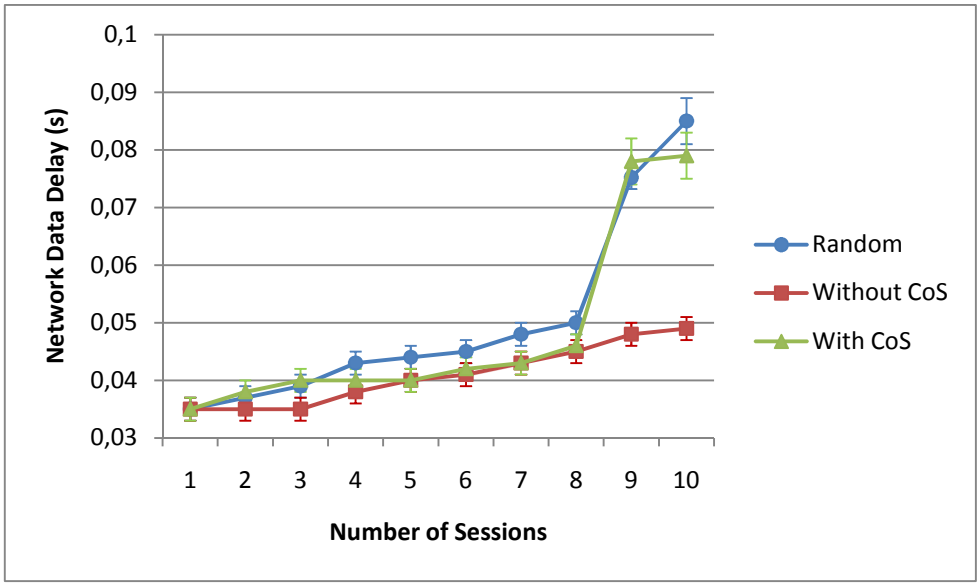

Figure 46 – Network Data Delay per number of sessions, varying Network Access Selection

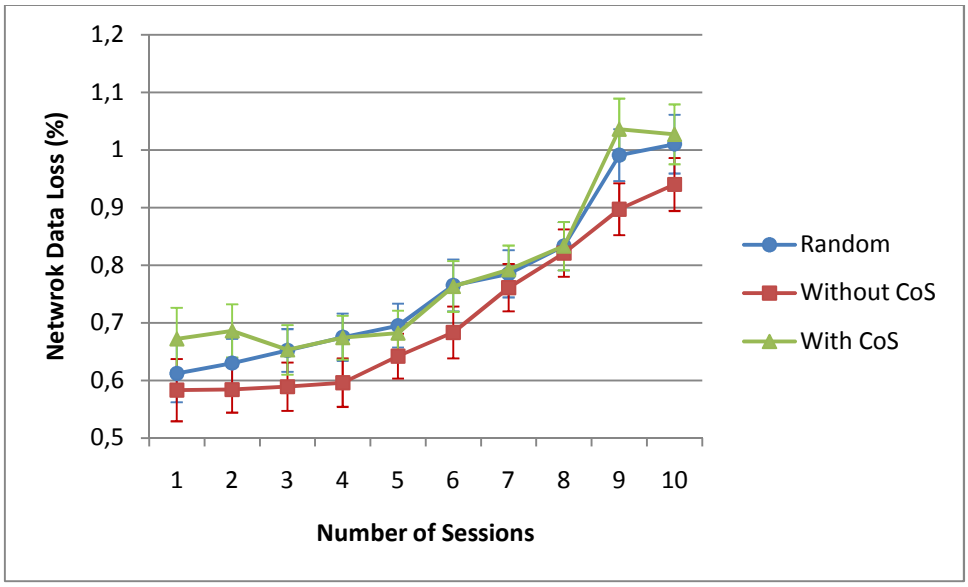

Figure 47 – Network Data Loss per number of sessions, varying Network Access Selection

As expected, with a low number of sessions, the results of delay and loss are similar for all selection methods, since APs and even core network maintain several resources unused. However, beyond 8 sessions, the results are the best to select without CoS, with especial benefit in delay. Since this method treats all traffic as equal QoS, the load balancing becomes more efficient, with an approximate uniform distribution through available APs. The random distribution is even worse than selection with CoS, since it can distribute flows without using some available APs, overloading the others.

After a general analysis of delay and loss in the network, Figure 48 and Figure 49 show the delay obtained in EF class and BE respectively.

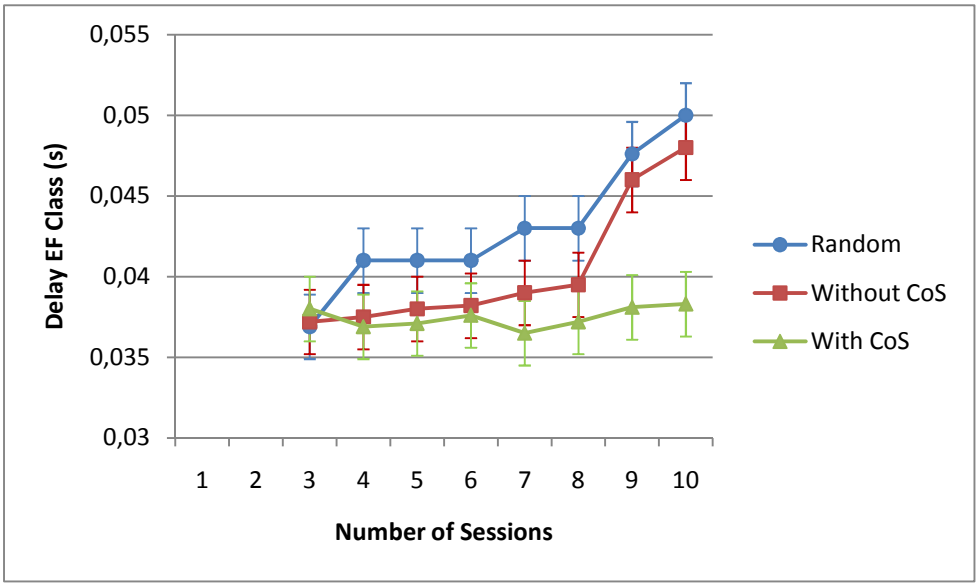

Figure 48 – Delay of EF Class per number of sessions, varying Network Access Selection

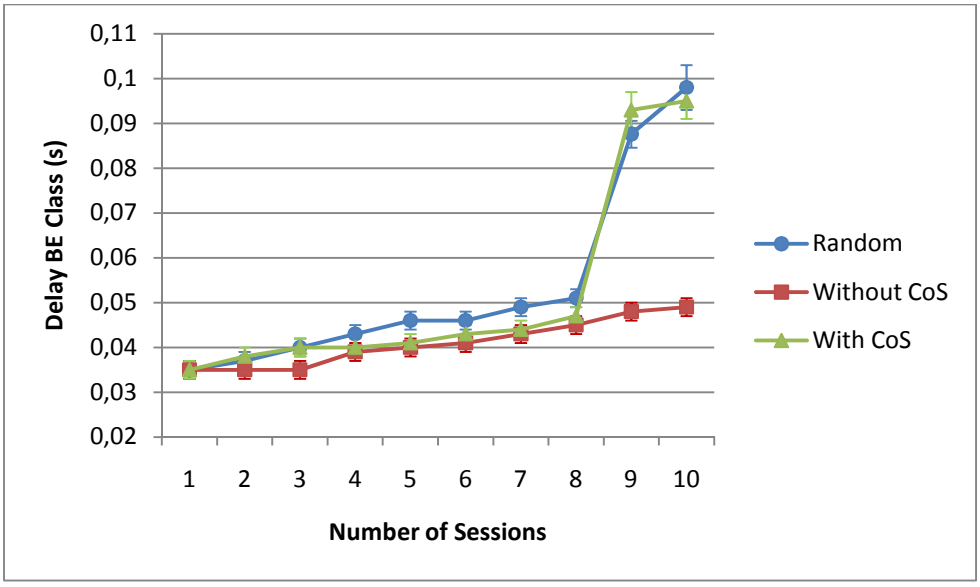

Figure 49 – Delay of BE Class per number of sessions, varying Network Access Selection

The EF class delay (Figure 48) is obviously the better choice to select with CoS, with a maximum value around the 0.038 seconds. Besides, its delay value is equal or higher with few numbers of sessions, it maintains nearly constant and never across the maximum value defined to this class. The selection without CoS begins with better delay times but a quick growth, with the

increase of the number of sessions, and becomes worse with random selection. The Figure 49 has a similar growth as network data delay (Figure 46) and it shows a better result to select without CoS with a higher number of sessions. Both results are similar, since more than an half of the data traffic in the network is BE.

Besides the delay to EF and BE class, the losses for both classes, presented in x and y, complement the analysis and reinforce the CoS treatment.

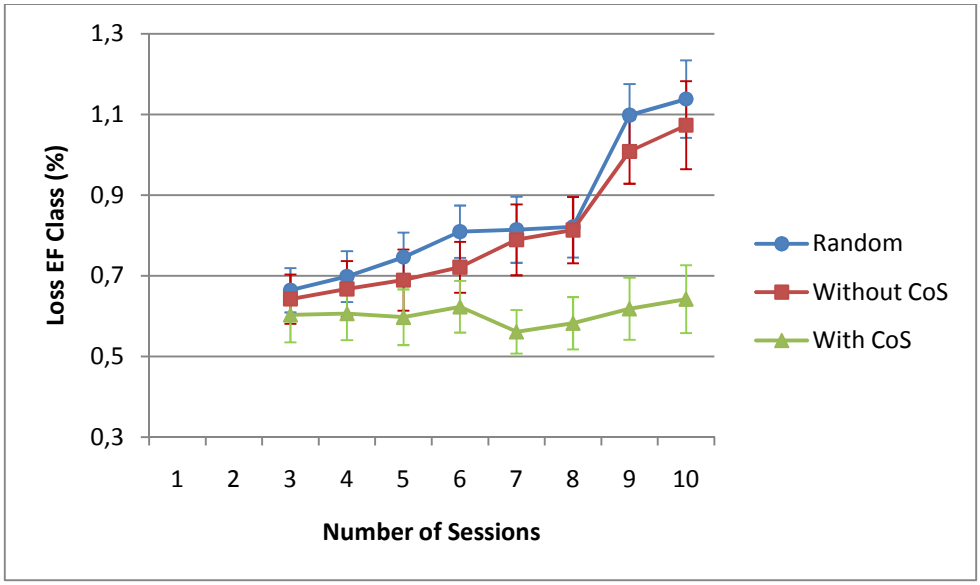

Figure 50 – Loss of EF Class per number of sessions, varying Network Access Selection

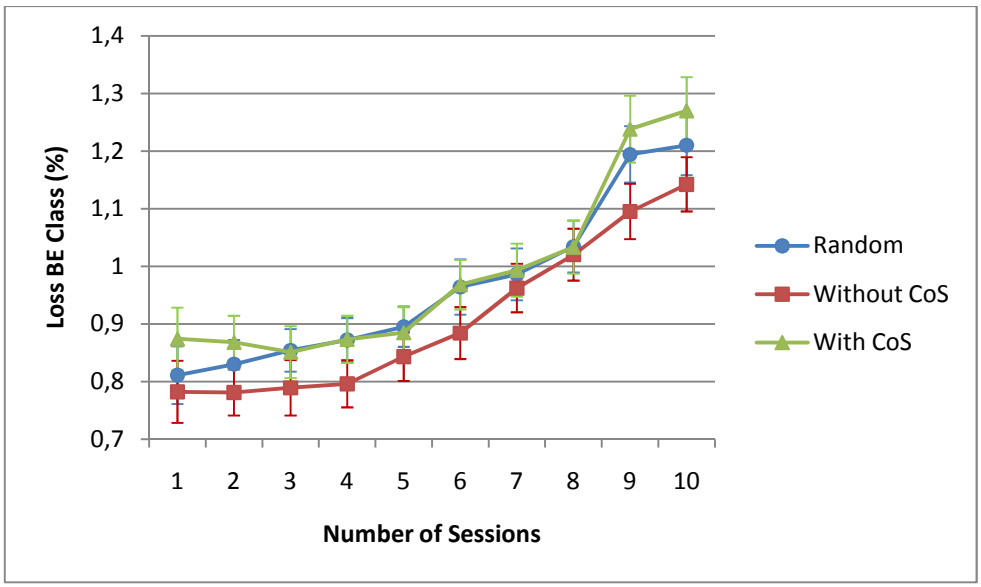

Figure 51 - Loss of BE Class per number of sessions, varying Network Access Selection

Figure 50 presents a loss per CoS similar to the delay explained before, since EF class loss is the lower to select with CoS with large number of sessions. This class has a maximum loss value around 0.7 %, independent of the number of sessions. Besides, selection without CoS contains a lower value: with the increase of the number of sessions it reaches random selection behavior. As for the delay explanation, the BE class loss is similar to the network data loss, and it is more reasonable to select without CoS with elevated number of sessions.

5.8. Bad Receive Feedback

In order to obtain the feedback of the QoE perception by the user when there is a lower QoS then the required one, the Bad Receive process is created as explained in section 3.2. This should not be use as an usual measure but only for a few cases, because the network selection should indicate the best solution for each user. It is important to analyze the impact of this process in data and control overhead. There is only a comparison between the situations with and without Bad Receive, when the same scenario is considered in the process. The fixed parameters created to evaluate the influence of Bad receive feedback, are exposed in the next table.

Ingress	Egress	Core	Core ON	APS	MTs	Data Sources	Data Flows
2	2	5	2	7	10	4	20

Table 21 - Fixed parameters to evaluate the influence of Bad Receive Feedback

The comparison respects only the EF CoS since this process only provides treatment to some flows of the higher CoS, but indifferent to the BE traffic. However, this solution can only have benefits in case of non-congestion networks, since it is impossible to reallocate a new AP or even core path with some rigorous requirement resources. As the EF class is the higher CoS, it provides the delay and loss for this class, considering that it collects the best benefits of the Bad Receive process.

First, it is relevant to observe the impact of bad receive feedback messages in overhead of control and also to contextualize them in the network (Figure 52).

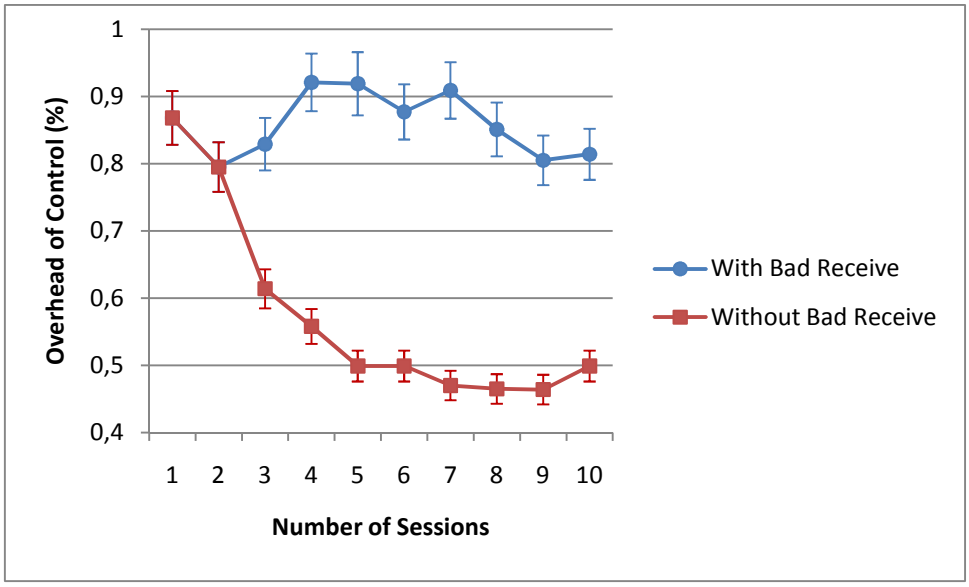

Figure 52 – Overhead of Control per number of sessions, with and without Bad Receive

The Figure 52 presents distinct values for each feature. Overhead with bad receive has high values comparing to the without bad receive, that maintain its value around 0.85 %, varying no more than 0.1 % along the number of sessions. In opposition, the behaviour of overhead without bad receive decreases significantly and tends to 0.5%. After overhead analysis, we can see better results without Bad Receive and it is important to present the delay (Figure 53) and loss (Figure 54) results of the EF class, in order to evaluate if bad receive process enrich our proposal.

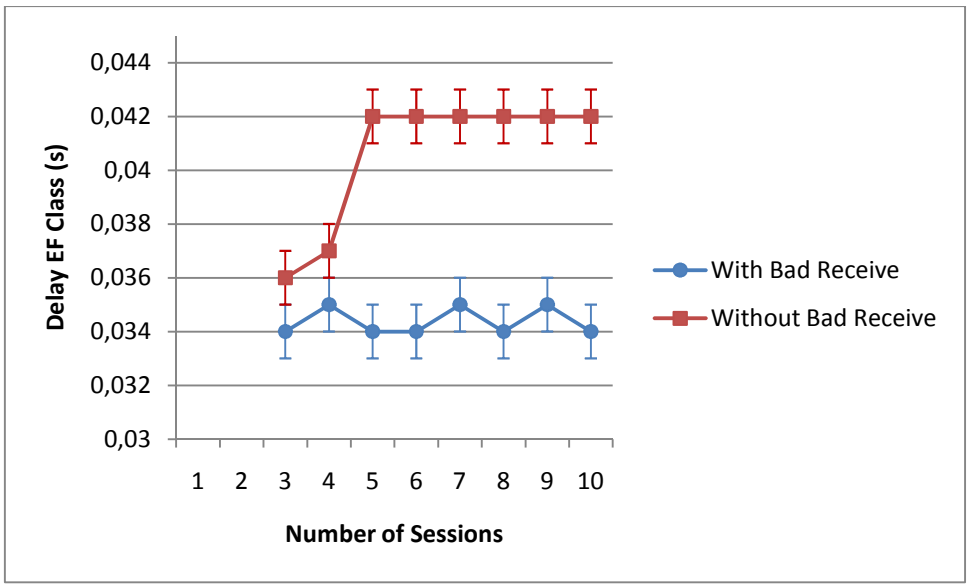

Figure 53 - Delay of EF Class per number of sessions, with and without Bad Receive

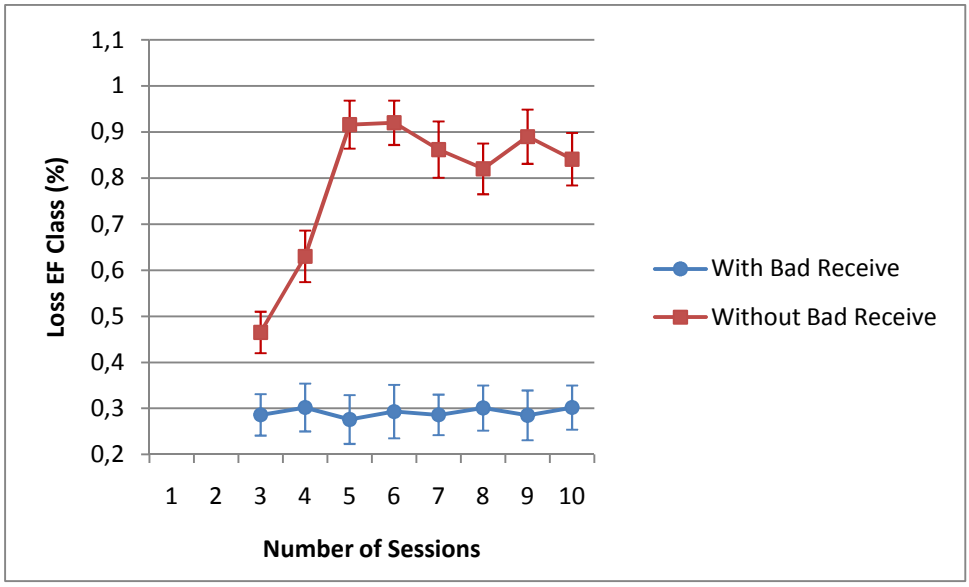

Figure 54 – Loss of EF Class per number of sessions, with and without Bad Receive

The graphics of Figure 53 and Figure 54 show some strong improvements in loss and delay of EF class, with the introduction of bad receive process. However, these results are only possible since the network is not overloaded and has several available resources, especially in APs. In both graphics, with Bad Receive, the delay already has a value around 0.035 seconds and loss around 0.3%. Delay and loss without bad receive grow with number of sessions and stabilize near to 0.042 seconds and 0.9% respectively.

5.9. Comparing with MIRA

This test compares the developed solution with the initial MIRA solution. MIRA is used by each user that has no information on the network and randomly chooses one available AP to receive the pretended data flow. MIRA chooses the core path from data source to AP, based on unicast routing table, and it does not allocate resources in wireless environment. Each session contains 2 flows for 5 users, randomly chosen. Other parameters were chosen according to the Table 22.

Ingress	Egress	Core	Core ON	APS	MTs	Data Sources	Data Flows
2	2	6	3	8	15	3	12

Table 22 - Fixed parameters to compare proposed solution with MIRA

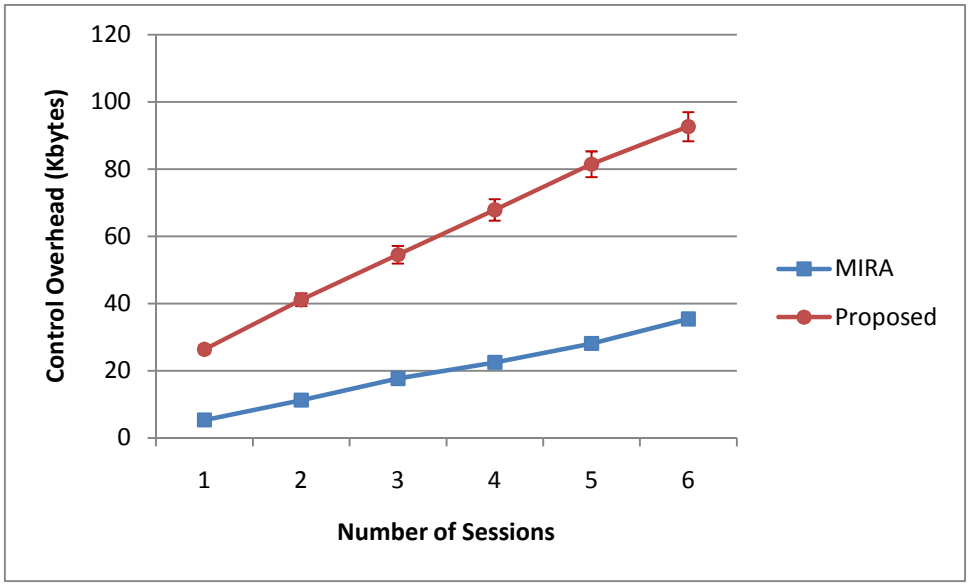

Figure 55 - Control Overhead (Kbytes) per number of sessions, with MIRA and proposed solution

As expected, the proposed solution increases the control overhead (Figure 55), since it not only uses messages to manage resources and AMTs, but also context messages from users and data sources. However, in 20 seconds simulation, the maximum difference is 60 Kbytes that can be considered few relevant in the entire network with increasing of 3Kbytes/s.

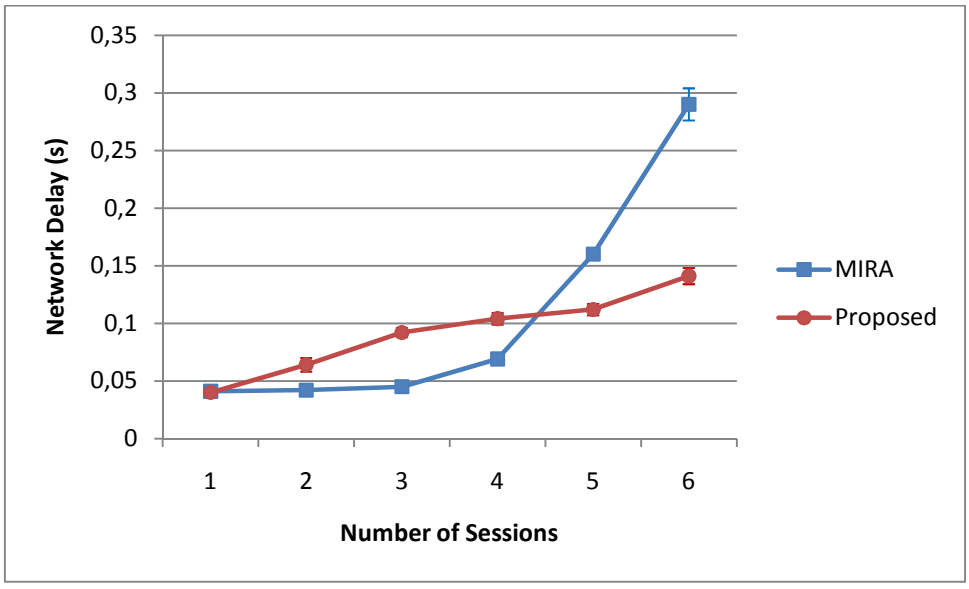

Figure 56 - Network Delay (s) per number of sessions, with MIRA and proposed solution

In Figure 56 it is presented the Network delay for both approaches. With a small number of sessions, MIRA takes a small advantage from proposed solution, since proposed solution uses a

CoS load balancing solution that tends to aggregate the flows from same CoS in the same AP. However, from 5 sessions, MIRA presents a higher delay values comparing to the proposed solution, because proposed solution uses several core paths and APs in a load balancing way to distribute flows according to the network resources. The network loss behaviour is not showed due to its similar behaviour comparing with network delay.

It is also important to analyse the performance of one CoS with higher requirements, such as EF class. Only EF delay is presented, since it is enough to compare both approaches.

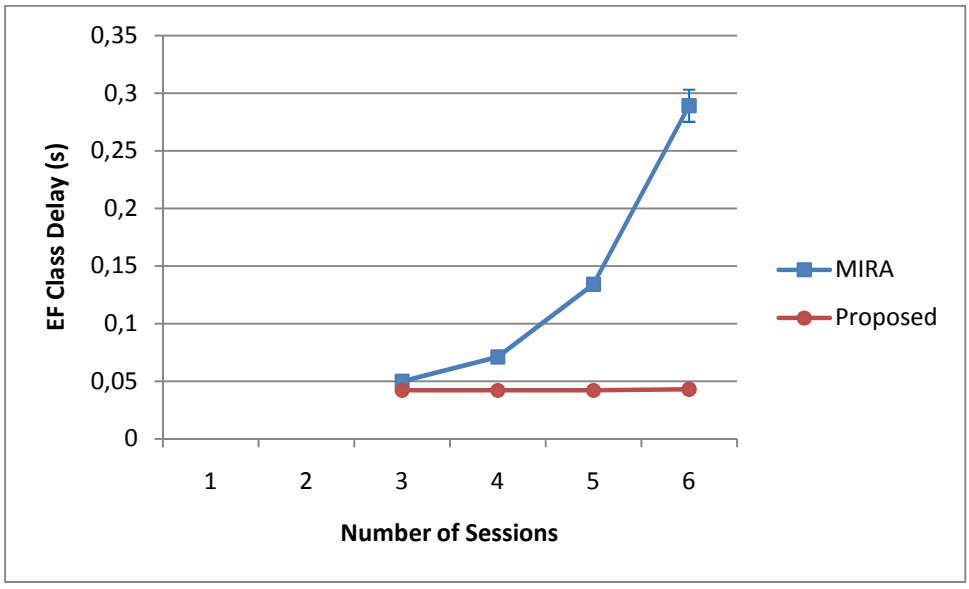

Figure 57 – EF Class Delay (s) per number of sessions, with MIRA and proposed solution

The proposed solution (Figure 57) maintains an equal value for EF delay independently of the number of sessions, satisfying the QoE for the users that receive the data of EF class. Since MIRA only considers QoS until APs, the user needs to randomly choose an AP without knowing which is the best for the pretended flow, and if it prejudices the data neighbour reception.

5.10. Conclusions

The results achieved through the different simulations, in several scenarios, meet, in general, the expectations. In what concerns to the number of users, the increase of MTs and sessions provides a more overhead of control, delay and loss in the network. However, these values keep acceptable, even with large number of sessions and MTs, due to the raise of the number of blocked flows. As expected, the EF class has a better performance than BE: EF has a

maximum delay of 0.042 seconds and a maximum loss of 0.9% influenced by a network operator's decision, while maximum delay and loss for BE class are higher and imposed by the network's resources.

The number of APs influences the number of served flows, since less APs in the network provide more blocked flows, in order to maintain the minimum of QoS required. The resources of a APs network are not totally used to maintain the desired QoS for the higher CoS.

The architecture transparency regarding the core transport technologies is demonstrated by the results. The presence of core nodes devoid of multicast, not only allows the correct function of all multiparty sessions, but also guarantees a similar performance to an entire multicast scenario.

As expected, the configuration of ONs in the core improves the time for users to receive back the data after movement, and also reduces the overhead of control in the network. However, in both situations, the time depends significantly on the wireless time provided by the old and the new AP, which sends warn move messages and receive the data traffic again.

The results of the access network selection methods reveal what was expected: random method is the worst, both in CoS treatment and general network results, with higher delays and more losses. The selection without CoS provides the best general network results with a more efficient load balancing through the available APs. However, the selection with CoS presents the best results for the EF and AFs classes, impairing the BE class. The BE class occupies more than a half of the network, leading to a worst general network performance compared to selection without classes.

The bad receive feedback is revealed as an important auxiliary method to improve the QoS of the higher classes, maintaining low delays and losses. This solution increases the percentage of the overhead of control in 0.4%, but this can be considered insignificant in comparison with the benefits obtained from the process.

The proposed solution shows to be more efficient in giving more QoS and respectively more QoE to users comparing with MIRA solution (start-up QoS no-context-aware solution), specially in the higher CoS, in spite of slightly increasing the control overhead.

6. Conclusion and Future Work

The main purpose of this Thesis was to develop and assess a new architecture for the next generation networks. The multicast approach has been chosen as the main solution to deliver multimedia data, but it is essential to use an efficient solution to support context-aware quality multicast at the same time. In spite of the preference for multicast, the MTO concept allows transparent multiparty sessions regarding used technologies, not only in the core network (multicast/unicast, IPV4/IPv6) but also in access network (such as WiFi, WiMAX, UMTS).

The architecture was developed and tested in a simulation environment using NS2.The agents and protocols were implemented and several scenarios were created to test the behaviour of the architecture, in different situations.

The proposed approach controls the network resources, based on context-aware approach, and blocks some flows to users, in order to maintain the quality that was configured previously, in consequence, each CoS has the expected behaviour. The architecture is transparent concerning multicast and unicast nodes, maintaining a similar performance even with several unicast nodes in the core. The use of ONs in the core network shows a good fulfilment, improving the time that a user needs to receive data back after a movement. The Bad Receive feedback improves the delay and loss for the higher CoS, especially EF class. The random access selection is the worst method to be applied both for CoS and network general results and it should not be used. The access selection with CoS has better results in CoS treatment, EF and AF classes, damaging the BE class and, consequently, the general network results, since the major part of traffic in the network is BE. However, it is the price to pay to ensure QoS to higher CoS.

The presented results demonstrate that the architecture can be used to deliver personalized content with QoS guaranties, without decreasing the performance of the network significantly. This solution also shows a better management of the resources of all CoS, using different paths in the core and choosing different APs for each user and flow ID, throughout context-aware network selection algorithms. This solution functions independently of all technologies used by the entities of the network, making possible its application in NGNs.

However, numerous studies should be done to improve this solution regarding scalability, features and efficiency. First, it is important to improve the decision algorithm, not only in core network but also in the access network. It is imperative to consider different context parameters, especially in environment context, considering parameters such as location and velocity. It is also

important to integrate the new QoE metrics in the decision of the network selection, becoming a good complement to the QoS metrics.

Since it was not possible to implement local link failures in IPT and global link failures in NUM, due to the complexity surrounding, these modifications should be integrated in the proposed NS implementation to test how this problem can affect the network.

To increase the scalability in large networks, it is important to create several NUMs in a hierarchical way to decrease the charge of packets and load of processing of a unique entity in the entire network.

A future improvement is related with a decentralised approach to the network management, in order to achieve better performance, since all decisions are computed in the NUM. It is necessary to distribute the information and the power to some entities in the network.

References

1. Context Casting (C-CAST) project, EU's ICT 7th Framework Programme. [Online] http://www.ict-ccast.eu.

2. **Moy, J.** Multicast Extensions to OSPF. *RFC 1584, Proteon Inc.* 1994.

3. **Waitzman, D., Partridge, C. and Deering, S.** Distance Vector Multicast Routing Protocol. *RFC 1075.* 1988.

4. **Ballardie, A.** Core Based Trees (CBT version 2) Multicast Routing. *RFC 2189.* 1997.

5. **Fenner, B., et al.** Protocol Independent Multicast-Sparse Mode (PIM-SM). *IETF RFC 4601.* 2006.

6. **Fenner, W.** Internet Group Management Protocol, Version 2. *IETF 1112.* 1997.

7. **Deering, S., Fenner, W. and Haberman, B.** Multicast Listener Discovery for IPv6. *IETF RFC 2710.* 1999.

8. **Cain, B., et al.** Internet Group Management Protocol, Version 3. *IETF RFC 2236.* 2002.

9. **Vida, R. and Costa, L.** Multicast Listener Discovery Version 2 for IPv6. *IETF RFC 2710.* 1999.

10. **Bhattacharyya, S.** An Overview of Source-Specific Multicast (SSM). *RFC 3569.* 2003.

11. **Bates, T., et al.** Multiprotocol Extensions for BGP-4. *IETF RFC 2858.* 2000.

12. **Banerjee, S., Bhattacharjee, B. and Kommareddy, C.** Scalable Application Layer Multicast. *In Proc. of ACM Sigcomm.* 2002.

13. **Yeo, C., Lee, B. and Er, M.** Survey of application level multicast techniques. *Transactions of the Elsevier Computer Communications.* 2004, Vols. 27, I.15, pp. 1547-1568.

14. **Cui, Y., et al.** CBroadcast: an Application Layer Multicast. *Transactions of the International Journal of Ad Hoc and Ubiquitous Computing.* 2007, Vol. 2, pp. 232-238.

15. **Lao, L. et al.** A Scalable Overlay Multicast Architecture for Large-Scale Applications. *IEEE Transactions on Parallel and Distributed Systems.* 2007, Vol. 18, pp. 449-459.

16. **Perkins, C. and Ed.** IP Mobility Support for IPv4. *IETF RFC 3220.* 2002.

17. **Perkins, C. and Johnson, D.** Route Optimization in Mobile IP. *IETF.* draft-ietf-mobileip-optim-11.txt, 2001.

18. **Johnson, D.B., Perkins, C. and Arkko, J.** Mobility Support in IPv6. *IETF RFC 3775.* 2004.

19. **Janneteau, C., et al.** Comparison of Three Approaches Towards Mobile Multicast. *IST Mobile Summit, Aveiro.* 2003.

20. **Koodli, R.** Mobile IPv6 Fast Handovers. *RFC 5268.* June 2008.

21. **Soliman, H., et al.** Hierarquical Mobile IPv6 Mobility Management. *RFC 5380.* October 2008.

22. **Suh, K., et al.** Fast Multicast Protocol for Mobile IPv6 in the fast handovers environments. *Internet Draft.* February 2004.

23. **Xia, F. and Sarikaya, B.** FMIPv6 extensions for Multicast Handover. *draft-xia-mipshop-fmip-multicast-01.* March 2007.

24. **Schmidt, T.C. and Waehlisch, M.** Seamless Multicast Handover in a Hierarquical Mobile IPv6 Environment. *draft-schimdt-waehlisch-mhmipv6-04.txt.* December 2005.

25. **Garyfalos, A. and Almeroth, K.** Deployed Complexity Versus Performance Efficiency in Mobile Multicast. *Intern. Workshop on Broadband Wireless Multimedia: Algorithms, Architectures and Applications.* 2004.

26. **Waehlisch, M. and Schmidt, T.** Between Underlay and Overlay: On Deployable, Efficient, Mobility-agnostic Group Communications Services. *Internet Research.* 17, 2007, Vol. 5, pp. 519-534.

27. **Buford, J.** Hybrid Overlay Multicast Framework. *Internet Draft.* 2008.

28. **Chikarmane, V., et al.** Multicast Support for Mobile Hosts Using Mobile IP: Design Issues and Proposed Architecture. *ACM/Baltzer Mobile Networks and Applications.* 1999, Vol. 3(4), pp. 365-379.

29. **Harrison, T., et al.** Mobile Multicast (MoM) Protocol: Multicast Support for Mobile Hosts. *Proceedings ACM MOBIOCOM, Budapest.* 1997.

30. **Lai, J., et al.** Mobile Multicast with Routing Optimization for Recipient Mobility. *Proceedings IEEE ICC.* 2001, pp. 1340-1344.

31. **Chen, K., Huang, N. and Li, B.** CTMS: A novel constrained tree migration scheme for multicast services in generic wireless systems. *IEEE JSAC.* 2001, Vol. 19, pp. 1998-2014.

32. **Tan, CL and Pink, S.** MobiCast: A Multicast Scheme for Wireless Networks. *ACM MONET.* 2000, Vol. 5(4), pp. 259-271.

33. **Zhang, H., et al.** Mobile IPv6 Multicast with Dynamic Multicast Agent. *Internet Draft.* 2007.

34. **Abdala, A. et. al.** An approach to enhance mobile multicast using context transfer. *Industrial Informatics, 2008. INDIN 2008. 6th IEEE International Conference.* 2008.

35. **Kermode, R.** *MADCAP Multicast Scope Nesting State Option.* IETF RFC 2907, 2000.

36. **Moulierac, J., Guitton, A. and Molnár, M.** *Multicast Tree Aggregation in Large Domains.* In Proc. of the 5th IFIP Networking, 2006.

37. **Yang, B. and Mohapatra, P.** *DiffServ-aware multicasting Source.* Transactions of the High Speed Networks Journal, 2004, Vol. 13, pp. 37-57.

38. **Cerqueira, E., et al.** *A Unifying Architecture for Publish-Subscribe Services in the Next Generation IP Networks.* IEEE Globecom Multimedia Communications Symposium, 2006.

39. **Mendes, P.** *OSMAR: Overlay for Source-specific Multicast in Asymmetric Routing environments.* NTT DoCoMo Euro-Labs, 2004.

40. **Pan, P. and Schulzrinne, H.** An Evaluation on RSVP Transport Mechanism. Network Working Group Internet Draft, 2003.

41. **Neto, A., et al.** A resource Reservation Protocol Supporting QoS-aware Multicast Trees for Next Generation Networks. *12th IEEE Symposium on Computers and Communications.* Aveiro, 2007.

42. **Guainella, E. et al.** QoS Managment of Multicast and Broadcast Services in Next Generation Networks. IST Mobile Summit, 2007.

43. **Sargento, S. et al.** Multicast Mobility in Heterogeneous Technologies: Experimental Validation. IEEE Global Telecommunications Conference, acepted in July 2009.

44. **Kewen, L. and Jing, T.** A QoS Mobile Multicast Routing Algorithm Based Ant Colony Algorithm. IEEE computer society, 2008.

45. **802.11e.** Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements. IEEE Standard, 2005.

46. **802.16e-2005, Specifiation.** 802.16e-2005 IEEE Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed Broadband Wireless Access Systems-Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands. Technical Report, 2005.

47. **3rd Generation Partnership Project.** Technical Specification Group Services and System Aspects. *IP Multimedia Subsystem.* Rel. 5 ff, 2002-2007.

48. **Wasserman, M.** Recommendations for IPv6 in Third Generation Partnership Project (3GPP). RFC 3314, 2002.

49. **Chen, J., Rinne, J. and Wiljakka, J.** Problem Statement for MIPv6 Interactions with GPRS/UMTS Packet Filtering. *draft-chen-mip6-gprs-07.txt.* 2007.

50. **3GPP2, www.3gpp2.org.** X.S0022-A, Broadcast and Multicast Service in cdma200 Wireless IP Network. 2007.

51. **Gustaffson, E. and Jonsson, A.** Always Best Connected. *IEEE Wireless Communications.* 2003, Vol. 10, No. 1, pp. 49-55.

52. **Antoniou, J. et al.** Context-Aware Self-Optimization in Multiparty Converged Mobile Environments. Autonomics, 2009.

53. **Jesus, V., Sargento, S. and Aguiar, R.** Any-Constraint Personalized Network Selection. *IEEE Intl Symposium on Personal, Indoor and Mobile Radio Communications.* 2008.

54. **Prehofer, C. et al.** A framework for context-aware handover decisions. *IEE Intl Symposium on Personal, Indoor and Mobile Radio Comm.* Beijing, 2003.

55. **Iera, A., et al.** An Access Network Selection Algorithm Dinamically Adapted to User Needs and Preferences. *IEEE Intl Symposium on Personal, Indoor and Mobile Radio Communications.* 2006.

56. **Ylitalo, J. et. al.** Dynamic network interface selection in multihomed mobile hosts. *Procedings of the 36th Annual Hawaii International Conference.* 2003.

57. **Stevens-Navarro, E. and Wong, V.W.S.** Comparison between Vertical Handoff Decision Algorithm for Heterogeneous Wireless Networks. *Vehicular Technology Conference.* 2006.

58. **Farooq, B. and Victor, C.M.L.** Automated network selection in a heterougeneous wireless network environment. *Network IEEE.* 2007.

59. **Bo, X. and Nalini, V.** Multi-Constraint Dynamic Access Selection in Always Best Connected Networks. *Proceedings of The Second Annual International Conference on Mobile and Ubiquitous System.* IEEE Computer Society, 2005.

60. **Qingyang, S. and Jamalipour, A.** Network selection in an integrated wireless LAN and UMTS environments using mathematical modeling and computing techniques. *Wireless Comunications, IEEE.* 2005.

61. **Coutinho, N. et. al.** Optimizing Network Performance in Multihoming Environments. *International Workshop on Traffic Management and Traffic Engineering for the Future Internet.* 2009.

62. **Simoes, J. et al.** Context-aware Control for Personalized Multiparty Sessions in Mobile Multihomed System. Mobimedia, 2009.

63. **Janneteau, C. et. al.** Context-Aware Multiparty Networking. ICT Mobile and Wireless Communications Summit, 2009.

64. **Neto, A. et al.** Multiparty Session and Network Resource Control in the Context Casting (C-CAST) project. Future Multimedia Networking, 2009.