Multicast Service Delivery in Next Generation Wireless Networks

Alexander Daniel Gluhak

Submitted for the Degree of Doctor of Philosophy from the University of Surrey

UniS

Centre for Communication Systems Research
School of Electronics and Physical Sciences
University of Surrey
Guildford, Surrey GU2 7XH, U.K.

August 2006

© Alexander Daniel Gluhak 2006
Summary

Mobile network operators have recently started looking into ways to increase their own network scalability, in order to support a large number of customers with new bandwidth consuming multimedia services. The two most promising solutions identified are to extend the existing networks with multicast capabilities and to cooperate with network operators of different wireless access technologies. As a consequence of these trends, a next generation network environment will allow mobile users to receive multimedia service data from a variety of multicast capable access networks.

Although considerable progress has been made with the standardisation of multicast mechanisms such as Multimedia Broadcast and Multicast Services (MBMS) for UMTS networks, shortcomings still exist in emerging multicast technologies and their interworking with each other.

One of the critical realisations leading to this research was the observation that the establishment and release of multicast bearers, particularly in UMTS networks, requires signalling intensive procedures, as compared to the simple mechanisms of IP multicast on the Internet. Especially for services such as location based multicast services, where a user is expected to change multicast groups more frequently, a considerable signalling burden may be added to a network. This is hardly acceptable for mobile networks, where wireless resources are valuable and scarce. One contribution made in this thesis extends the currently defined mechanisms in MBMS to allow the concurrent delivery of different versions of location based content using the same multicast bearer service. It is shown by simulation study that the proposed mechanism achieves significant signalling savings, especially over the air interface, compared to the case where separate multicast bearer services are utilised for the delivery of different location specific flows.

Another significant observation was that the current receiver driven service model of IP multicast is not suitable to allow efficient multicast delivery in a wireless network environment with multiple access networks. This thesis argues that efficient multicast delivery requires mechanisms for delivery coordination, in order to avoid the same multicast traffic being delivered via multiple access networks to the same location. Based on a detailed analysis of the shortcomings of current IP multicast group management mechanism, two incremental solutions to achieve multicast delivery coordination in next generation networks are developed and their advantages and disadvantages thoroughly studied. The first approach achieves delivery coordination by introducing a group management support as a session layer solution, leaving the operation of current existing IP multicast mechanisms completely unchanged. The second approach provides a solution on the network layer to achieve multicast delivery coordination, and requires the modification of the current IP multicast group management mechanisms. Proof-of-concept prototypes are built to demonstrate the feasibility of both solutions. An evaluation of their performance is achieved by analytical and simulation study and is complemented by a testbed study of the prototypes.
Key words: Multicast Delivery Coordination, Heterogeneous Wireless Networks, Multicast Group Management, MBMS
Acknowledgements

Many people deserve my gratitude and are in one or the other way responsible for my achievements in the past few years that have culminated into this dissertation.

I would like to thank both my supervisors Rabim and Klaus for their continuous support and guidance during my research and giving me various opportunities for developing myself, not only in terms of the technical knowledge I acquired in my field of research, but also in terms of growing my character as a human being. Among the most memorable experience was the research visit in Japan and I would like to thank them both for their confidence and trust they put into me. I would also like to thank Kar Ann, who has been a great help for me at the beginning of my studies to demystify the mysteries of simulations.

I would like to thank all my friends and colleagues in the centre, which often made me forget the hard times during my study and gave me extra motivation to overcome the many doubts and struggles with the reasons of my doings that I encountered during the past few years.

I am also grateful to my parents, who made me aware of the significance of education and put me into a situation that I could always chose my ways without restrictions. They gave me the believe and exemplified to me that hard work and determination can make you go a long way.

My biggest thanks goes to my great wife Monica for her encouraging support and her selfless forbearance right from the beginning of our marriage and the trust and believe she put into me. I deeply appreciate her countless sacrifices, the many nights and weekends I spent working in the office, instead of being with her, as well as the time of absence during my research visit in Japan.
Contents

1 Introduction .......................... 1
   1.1 The Challenges ....................... 2
      1.1.1 Mechanisms for multicast bearer service management 3
      1.1.2 Coordinating multicast delivery in heterogeneous wireless networks 4
   1.2 Contributions ......................... 7
   1.3 Organisation ......................... 8

2 Background and Related Work .... 10
   2.1 An overview of IP multicast on the Internet ....... 10
   2.2 Multicast technologies in wireless networks .......... 12
      2.2.1 Multicast in UMTS networks ............ 12
      2.2.2 Multicast in DVB networks ................ 18
   2.3 Multicast flow filtering ................. 22
   2.4 Multicast delivery coordination ................. 23
      2.4.1 Multicast group management ............ 24
      2.4.2 Multicast access control at the router ....... 26
      2.4.3 Multicast delivery in heterogeneous network ....... 27
      2.4.4 Session layer approaches ............ 29

3 MBMS Protocol Extensions .......... 31
   3.1 Current provisioning of location based service in UMTS ....... 32
   3.2 Proposed service provisioning principles ............ 32
   3.3 Protocol extensions .................... 35
      3.3.1 Flow forwarding mechanism ............ 35
      3.3.2 Update mechanism for flow forwarding entries ....... 36
   3.4 Evaluation .................................. 39
   3.5 Summary .................................. 43
4 Group Management Support

4.1 Overview of the group management support................................................ 45
4.2 Service provisioning phases ......................................................................... 47
4.3 Context-aware group manager....................................................................... 49
  4.3.1 Group membership management function ...................................... 50
  4.3.2 Session control function ..................................................................... 51
  4.3.3 Network management function ........................................................ 53
4.4 Multicast signalling channel ............................................................................ 53
  4.4.1 Context information based receiver subset addressing ................ 55
  4.4.2 Message format on the multicast signalling channel .................. 57
4.5 Multicast middleware..................................................................................... 60
  4.5.1 Multicast middleware principles ........................................................ 61
  4.5.2 Design overview ................................................................................. 62
  4.5.3 Operational example ........................................................................... 65
4.6 Service example of a multicast session ......................................................... 67
4.7 Summary........................................................................................................... 69

5 IGMP Extensions

5.1 Introduction to IGMP ..................................................................................... 72
5.2 Overview of protocol extensions ..................................................................... 74
5.3 Design principles .......................................................................................... 76
5.4 Router extensions.......................................................................................... 76
  5.4.1 Multicast group filters ........................................................................ 77
  5.4.2 REDIRECT message type ................................................................... 78
  5.4.3 IGMP protocol modifications ........................................................... 78
5.5 Host extensions .............................................................................................. 80
  5.5.1 IGMP protocol modifications ........................................................... 80
  5.5.2 Socket API ........................................................................................... 81
5.6 An operational example ................................................................................. 84
5.7 Summary........................................................................................................... 85
6 Implementation 87

6.1 Group manager ................................................................. 88
6.1.1 Multicast user service configuration ................................. 88
6.1.2 Group entity ................................................................. 89
6.1.3 Service announcement and user registrations ................... 90
6.1.4 Resource management functionality ................................. 90
6.1.5 Session control function ................................................ 91
6.2 Multicast middleware ....................................................... 92
6.2.1 Introducing TESLA ....................................................... 93
6.2.2 Realisation ................................................................. 94
6.3 Implementation of the IGMP router side extensions ............... 96
6.3.1 Multicast router support on a Linux system ....................... 97
6.3.2 Protocol modifications .................................................. 98
6.4 Implementation of the IGMP host side extensions ................. 100
6.4.1 Overview of the Linux networking stack ......................... 101
6.4.2 Data structures relevant to IP multicast ............................ 102
6.4.3 Protocol modifications .................................................. 103
6.5 Summary ................................................................. 105

7 Evaluation 107

7.1 Evaluation of the MSCH .................................................... 107
7.1.1 Modelling parameters .................................................. 108
7.1.2 Distribution of multicast receivers ................................. 111
7.1.3 Delivery cost ............................................................. 112
7.1.4 Assumptions ............................................................. 114
7.1.5 Signalling load analysis for single message delivery .......... 116
7.1.6 Signalling load considering impact of MSCH management .... 124
7.1.7 Summary of observations ............................................. 129
7.2 Testbed evaluation of the group management support ........... 130
7.2.1 Testbed setup ........................................................... 131
7.2.2 Experimental prototype evaluation ................................. 132
7.3 Simulation study of IGMP extension .................................... 139
## Contents

7.3.1 Protocol overhead for continuous operation ...................................... 139  
7.3.2 Protocol overhead considering a load balancing example .................. 142  
7.3.3 Protocol overhead considering three access networks ...................... 144  
7.4 Testbed evaluation of the IGMP extensions ........................................ 147  
7.4.1 Testbed setup .................................................................................. 147  
7.4.2 Testbed results ................................................................................ 148  
7.5 Qualitative comparison of approaches .............................................. 150  

8 Conclusions ......................................................................................... 154  
8.1 Future work .................................................................................... 155  

A Additions to Evaluations .................................................................. 157  
A.1 Costs considering multicast bearer management in UMTS network .... 157  
A.2 Costs considering multicast bearer management in DVB network ...... 161  

Publications ......................................................................................... 163  

Bibliography ......................................................................................... 164
# Glossary of Terms

## Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3G</td>
<td>3rd Generation</td>
</tr>
<tr>
<td>3GPP</td>
<td>3rd Generation Partnership Project</td>
</tr>
<tr>
<td>ACK</td>
<td>Acknowledgement</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>APN</td>
<td>Access Point Name</td>
</tr>
<tr>
<td>AR</td>
<td>Access Router</td>
</tr>
<tr>
<td>ATM</td>
<td>Asynchronous Transfer Mode</td>
</tr>
<tr>
<td>BSA</td>
<td>Bearer Selection Algorithm</td>
</tr>
<tr>
<td>BSD</td>
<td>Berkeley Software Distribution</td>
</tr>
<tr>
<td>BMS</td>
<td>Broadcast Multicast Service Centre</td>
</tr>
<tr>
<td>CN</td>
<td>Core Network</td>
</tr>
<tr>
<td>DMB</td>
<td>Digital Multimedia Broadcast</td>
</tr>
<tr>
<td>DSM-CC</td>
<td>Digital Storage Media Command and Control</td>
</tr>
<tr>
<td>DVB</td>
<td>Digital Video Broadcast</td>
</tr>
<tr>
<td>DVB-CBMS</td>
<td>Digital Video Broadcast - Convergence of Broadcast and Mobile Services</td>
</tr>
<tr>
<td>DVB-G</td>
<td>Digital Video Broadcast Gateway</td>
</tr>
<tr>
<td>DVB-H</td>
<td>Digital Video Broadcast - Handheld</td>
</tr>
<tr>
<td>DVB-T</td>
<td>Digital Video Broadcast - Terrestrial</td>
</tr>
<tr>
<td>DVB-TS</td>
<td>Digital Video Broadcast Transmission System</td>
</tr>
<tr>
<td>EPG</td>
<td>Electronic Program Guide</td>
</tr>
<tr>
<td>FFE</td>
<td>Flow Forwarding Entry</td>
</tr>
<tr>
<td>GA</td>
<td>Group Address</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>GM</td>
<td>Group Manager</td>
</tr>
<tr>
<td>GMMF</td>
<td>Group Membership Management Function</td>
</tr>
<tr>
<td>GGSN</td>
<td>Gateway GPRS Support Node</td>
</tr>
<tr>
<td>GMS</td>
<td>Group Management Support</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GTP</td>
<td>GPRS Tunnelling Protocol</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>HIP</td>
<td>Host Identity Payload</td>
</tr>
<tr>
<td>HTTP</td>
<td>HyperText Transfer Protocol</td>
</tr>
<tr>
<td>HQ</td>
<td>High Quality</td>
</tr>
<tr>
<td>ICR</td>
<td>Internal Contributional Report</td>
</tr>
<tr>
<td>IGMP</td>
<td>Internet Group Management Protocol</td>
</tr>
<tr>
<td>IGMPv2</td>
<td>Internet Group Management Protocol Version 2</td>
</tr>
<tr>
<td>IGW</td>
<td>Interworking Gateway</td>
</tr>
<tr>
<td>IMS</td>
<td>IP Multimedia Subsystem</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPv4</td>
<td>Internet Protocol Version 4</td>
</tr>
<tr>
<td>IPv6</td>
<td>Internet Protocol Version 6</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>INT</td>
<td>IP MAC Notification Table</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LQ</td>
<td>Low Quality</td>
</tr>
<tr>
<td>LSA</td>
<td>Local Service Area</td>
</tr>
<tr>
<td>MAC</td>
<td>Medium Access Control</td>
</tr>
<tr>
<td>MacOS</td>
<td>Macintosh Operating System</td>
</tr>
<tr>
<td>MBMS</td>
<td>Multimedia Broadcast and Multicast Services</td>
</tr>
<tr>
<td>MBS</td>
<td>Multimedia Bearer Service</td>
</tr>
<tr>
<td>MGA</td>
<td>Multicast Group Address</td>
</tr>
<tr>
<td>MIME</td>
<td>Multipurpose Internet Mail Extensions</td>
</tr>
<tr>
<td>MLD</td>
<td>Multicast Listener Discovery</td>
</tr>
<tr>
<td>MM</td>
<td>Multicast Middleware</td>
</tr>
<tr>
<td>MPE</td>
<td>Multi-Protocol Encapsulation</td>
</tr>
<tr>
<td>MSCH</td>
<td>Multicast Signalling Channel</td>
</tr>
<tr>
<td>MSISDN</td>
<td>Mobile Station Integrated Service Digital Network</td>
</tr>
<tr>
<td>NAI</td>
<td>Network Access Interface</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>NMF</td>
<td>Network Management Function</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnection</td>
</tr>
<tr>
<td>PDP</td>
<td>Packet Data Protocol</td>
</tr>
<tr>
<td>PDU</td>
<td>Protocol Data Unit</td>
</tr>
<tr>
<td>PIM</td>
<td>Protocol Independent Multicast</td>
</tr>
<tr>
<td>PLMN</td>
<td>Public Land Mobile Network</td>
</tr>
<tr>
<td>PSI</td>
<td>Program Specific Information</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RA</td>
<td>Routing Area</td>
</tr>
<tr>
<td>RAB</td>
<td>Radio Access Bearer</td>
</tr>
<tr>
<td>RANAP</td>
<td>Radio Access Network Application Part</td>
</tr>
<tr>
<td>RLF</td>
<td>Router Level Filtering</td>
</tr>
<tr>
<td>RGMP</td>
<td>Receiver-Initiated Group Management Protocol</td>
</tr>
<tr>
<td>RM</td>
<td>Resource Management</td>
</tr>
<tr>
<td>RNC</td>
<td>Radio Network Controller</td>
</tr>
<tr>
<td>RTP</td>
<td>Realtime Transport Protocol</td>
</tr>
<tr>
<td>SAP</td>
<td>Session Announcement Protocol</td>
</tr>
<tr>
<td>SCF</td>
<td>Session Control Function</td>
</tr>
<tr>
<td>SDR</td>
<td>Session Directory</td>
</tr>
<tr>
<td>SI</td>
<td>Service Information</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>SGSN</td>
<td>Serving GPRS Support Node</td>
</tr>
<tr>
<td>SRNC</td>
<td>Serving Radio Network Controller</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TV</td>
<td>Television</td>
</tr>
<tr>
<td>UDLR</td>
<td>Unidirectional Link Routing Protocol</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UE</td>
<td>User Equipment</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunications System</td>
</tr>
<tr>
<td>VLC</td>
<td>Video LAN Client</td>
</tr>
<tr>
<td>WiMax</td>
<td>World Interoperability for Microwave Access</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>XCast</td>
<td>Explicit Multicast</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

The demand for ubiquitous wireless data services has significantly increased in recent years and this trend is expected to even further increase in the future. Services that are able to target large user audiences are expected to become a major source of revenue for both network operators and 3rd party service providers. Examples of such services include push delivery of multimedia content, video and audio streaming, multimedia conferencing and multiplayer games. In order to support a large number of customers with new bandwidth consuming services, mobile operators have started looking into ways to increase the scalability of their own network. The two most promising solutions identified in a beyond 3G environment are 1) to extend the existing networks with multicast capabilities [1, 2] and 2) co-operation between network operators of different wireless access technologies [3, 4, 5].

Although IP multicast delivery [6] has been around for more than a decade and its concept is well understood by the research community, current mobile data networks do not support multicast. Only recently, 3GPP [7] has addressed the issue with the introduction of Multimedia Broadcast and Multicast Services (MBMS) [8, 9] in UMTS Release 6. MBMS will offer unidirectional multicast and broadcast bearer services, which can be utilised by multicast user services to transport data resource efficiently to a group of users. Resource savings are achieved by constructing a shared delivery path throughout the core network and by utilising shared channels over the radio link, where and whenever appropriate. The first multicast capable UMTS terminals are expected to appear end of 2008, with roughly a third of the terminals and networks supporting MBMS by 2010 [1].

On the other hand, by interworking between different access network technologies, mobile operators are able to enhance their coverage and capacity for service delivery, without the need of acquiring licenses for additional spectrum or purchasing new costly
1.1. The Challenges

access network infrastructure. IEEE 802.11x technologies (WLAN) have been recently deployed in major cities all over the globe in order to cover hotspots areas such as airports, hotels, etc. Therefore current standardisation efforts of 3GPP focus on WLAN interworking [10], however, mainly focus on point-to-point communication. In contrast the emerging digital broadcasting networks have relatively large coverage areas, which makes them very suitable for point-to-multipoint delivery of content to a potentially large group of receivers. The introduction of DVB-H [11] and the standards for data broadcast [12] will also allow the delivery of IP data services via DVB to small mobile devices. Alternative broadcasting standards are emerging all over the world such as Digital Multimedia Broadcast (DMB) [13] in Korea and Europe or Qualcomms MediapLO [14] in the US. Looking at these scenarios, a mobile user will most likely possess a terminal with multiple network interfaces and will be able to receive multicast traffic from a variety of available access networks at its location.

This thesis acknowledges the importance of multicast delivery in a future wireless network scenario and argues that the existing receiver driven multicast mechanisms are unable to provide efficient multicast delivery in such an environment. The presented work recognises the need for additional network control mechanisms and advertises a shift in the paradigm from a purely receiver driven to a network controlled provision of multicast services. A novel multicast mechanism for UMTS networks that allows more scalable delivery for a variety of multicast services is introduced. Furthermore, mechanisms are presented that allow cooperating network operators with different access network technologies to coordinate multicast delivery efficiently in an heterogeneous wireless network environment.

The remainder of this chapter is structured as follows. The first section motivates the work by presenting shortcomings and challenges of multicast delivery in heterogeneous wireless networks and describes the approach taken to overcome these issues. In the second section a summary of the contributions of this thesis is briefly provided. Finally the chapter concludes by outlining the structure of this thesis.

1.1 The Challenges

The introduction of multicast capabilities in wireless networks will alleviate some of the scalability problems that network operators will be facing in future. Although considerable progress has been made with the standardisation of multicast mechanisms such as MBMS and the standards are slowly reaching maturity, some shortcomings still remain. One of the critical realisations leading to this thesis was the observation that the establishment and release of multicast bearers, particularly in UMTS networks, requires signalling intensive procedures, as compared to the simple mechanisms of IP multicast.
1.1. The Challenges

on the Internet. Especially for services where a user is expected to change multicast groups more frequently, a considerable signalling burden may be added to a network. This is hardly acceptable for mobile networks, where wireless resources are valuable and scarce. Another significant observation was that the current receiver driven service model of IP multicast is not suitable to allow efficient multicast delivery in a multi-access wireless network environment. Efficient multicast delivery requires mechanisms for delivery coordination, in order to avoid the same multicast traffic being delivered via multiple access networks to the same location. The following sections briefly describe the challenges addressed by this thesis and introduces the taken approaches followed.

1.1.1 Mechanisms for multicast bearer service management

In the current multicast service model, multicast delivery is achieved by an interworking of local and global mechanisms. The local mechanism is often referred to as multicast group management, while global mechanisms are summarised as 'multicast routing'. Using a multicast group management protocol, receivers are required to notify a multicast enabled router within their subnet about their interest in receiving data from a particular multicast group. This process is also often referred to as joining. Multicast routing protocols executed in routers in the networks then use this information to establish appropriate multicast delivery paths to interested receivers. Data sent by sources to the multicast groups is forwarded along the path in a resource efficient manner. Likewise in some group management protocol implementations, receivers notify a router if they are not interested in receiving data of a particular multicast group, thus leaving the multicast group.

Joining and leaving of multicast groups is achieved by sending simple unacknowledged messages in an Internet environment, introducing little signalling overhead to the network. The same mechanisms are also used in MBMS to initiate the establishment or release of appropriate delivery paths within UMTS networks. However, in addition to these messages a sequence of signalling intensive procedures is triggered for every interested receiver. These signalling procedures are referred to as multicast bearer service activation and deactivation respectively within the MBMS standard and carry out tasks such as access control and context configuration in the network nodes and receivers. Especially for services in which a user is expected to change multicast groups more frequently in order to change a received service flow, e.g. location based user services, these signalling procedures may add a considerably high signalling burden to the network.

While these procedures have been already carefully designed, it is very difficult to modify them without losing functionality, in order to reduce the signalling load. An al-
1.1. The Challenges

The alternative approach addressed in this thesis, avoids frequent changes of multicast groups. Receivers stay connected to the same multicast bearer service for the whole duration of a session. Mechanisms in the network ensure that the correct service flow is delivered to the receivers. Using this method frequent establishments and releases of multicast bearers services can be avoided, thus significantly reducing the signalling load in the network.

Multicast service delivery faces not only challenges within particular access networks introduced by novel multicast technologies, but also when several access networks have to interwork efficiently with each other. The following subsection presents the issues that arise in an heterogeneous wireless network scenario and an overview of the solution.

1.1.2 Coordinating multicast delivery in heterogeneous wireless networks

The availability of multiple access networks together with the existence of multiple network interfaces within user terminals provides new opportunities as well as challenges for both multicast receivers and network operators. One of the major challenges for network operators in such a heterogeneous network environment is to coordinate the delivery of IP multicast data. Unfortunately this cannot be easily accomplished with the current group management model [6], which is purely receiver-initiated. In order to establish a multicast session, a mobile receiver enables the reception of data from a particular multicast group via one of its interfaces and sends a request to join the attached access network. Multicast enabled routers at the network edge determine the requested multicast groups of their receivers on the local subnets and trigger multicast routing protocols and other access network specific mechanisms to forward the respective multicast traffic. This leaves the selection of the network interface and hence choice of delivery network up to the receivers.

Figure 1.1 illustrates the problem using a simple example. All receivers have different network access interfaces available, however, are assumed to be at the same location and are expected to receive the same flow of session data. While the 1st and 2nd receiver join the service via the UMTS network, receivers 3 and 4 choose to initiate the session via WLAN, and the 5th receiver requests the multicast service via DVB. Consequently the same service content is delivered via three different data paths to the same location. Knowing that all receivers have a UMTS network access interface, the receivers could be directed to join the UMTS network for receiving the traffic. Respective resources in the other access networks could be preserved and used for alternative services.

In order to coordinate data delivery more efficiently in an interworking network environment, operators would prefer to direct users to establish multicast bearers in suitable
1.1. The Challenges

delivery networks, or even balance the network load by moving groups of receivers to a different access network. Such coordination however cannot be accomplished with the current receiver-initiated multicast service model.

A further problem is the inherent heterogeneity of mobile receiver capabilities. The heterogeneity is due to differences in available network interfaces, user location and hence availability of access networks, service preferences, hardware features such as I/O capabilities, processing power and memory storage and software features such as supported applications and media codecs. This demands multiple service flows within a multicast session to satisfy receiver heterogeneity, despite joint efforts by industry [15] to confine heterogeneity by developing common guidelines and specifications. A major requirement for efficient multicast service delivery is the knowledge of the existing heterogeneity of the receiver population.

Recognising the need for more network control in the current multicast service model, two distinct solutions for multicast delivery coordination are proposed: one within the session layer and one within the network layer, each with different advantages and disadvantages.

As a session layer solution, a context aware group management support has been de-
1.1. The Challenges

veloped, which is especially suitable for an interworking mobile and broadcast network environment. Like in the current multicast service model, receivers still have the freedom to select the service they want. However, using group management support, network operators now have the freedom to dynamically determine appropriate service flows and suitable delivery paths, while considering user preferences. The underlying principle of the group management support is a decoupling of a multicast service and its service flows from multicast groups or multicast bearer services, over which they are provisioned to the users. A multicast service is no more a representation of a network layer identifier but is elevated to an entity, to which interested receivers can directly refer.

Group management support requires the deployment of an additional group manager entity in the operators network, and of a multicast middleware library in the terminal. Instead of joining a multicast group that provides a particular service flow of a multicast service, receivers subscribe to an interested multicast service with the group manager in the network. The group manager aggregates useful context information of the subscribed receivers from context information databases in the network and provides this information to resource management functionality in the network. Based on resource conditions and context information of the heterogeneous receivers, intelligent resource management algorithms [16, 17] select appropriate service flows and optimise the use of the delivery networks. The group manager further provides the required session management mechanisms to implement the resource management decisions by supporting network initiated multicast bearer establishment and release as well as vertical handoff for groups of heterogeneous receivers. Using a control signalling plane, the group manager communicates with the multicast middleware in the receiver terminal and initiates the establishment, migration or release of appropriate multicast bearers transparently to applications.

Delivery of such session control signalling from coordinating network entities such as the group manager to a group of receivers of a multicast user service presents a particular challenge. The separate delivery of control signalling to every receiver, as it is currently done in most of the networks, may cause significant signalling overhead. Therefore, the control signalling added by the group management support has to be delivered in a scalable manner, especially for multicast service where the number of expected users can be very large. Group management support addresses this issue by specification of a novel multicast signalling channel, which allows scalable delivery of control signalling to large receiver groups.

The network layer approach proposes modifications to the current existing multicast group management model to achieve delivery coordination. Delivery coordination is realised by providing means to operators to restrict the access of particular multicast
1.2. Contributions

groups for selected subnets within an access network and provide mechanisms to control hosts to establish a session in a subnet of an alternative network.

In order to accomplish these goals, receiver and router side extensions to the current Internet group management protocol (IGMP) have been proposed. While group membership management has been previously performed for all multicast groups, the router side extensions now allow group membership collection to be disabled for selected multicast groups. An operator can specify a list of multicast groups for each router interface, for which group membership operations are not performed. That way the provision of multicast services can be restricted only to desired subnets. As a consequence, receivers that try joining a multicast group on a subnet on which that multicast group has been disabled, will not be able to receive any traffic destined to the group. In such cases the receiver is notified by a feedback mechanism and is redirected to join an alternative access network. If the network topology is known, receivers can be redirected to specific access networks. On the receiver side, IGMP has been extended to perform group management operations across multiple access networks. If joining a multicast group is unsuccessful for a particular network interface, a new interface is selected for rejoining the multicast group using a different subnet. The mechanisms introduced here not only allow operators to coordinate multicast service delivery in a multi-access environment, but also increase the robustness for multicast service delivery for receivers with multiple access interfaces.

1.2 Contributions

This thesis examines multicast service delivery in a heterogeneous wireless network environment and postulates that current multicast mechanisms in wireless networks require extensions for efficient provision of multicast services. It asserts that signalling procedures for establishment and release of multicast bearer services in MBMS are signalling intensive, especially when used for services with multiple flows. It is shown that by adaption of existing mechanisms a significantly lower signalling load can be achieved. Further this thesis explores the hypothesis that appropriate mechanisms at session and network layer can provide delivery coordination, which is required for resource efficient delivery of multicast services in an environment with multiple access networks. This thesis makes the following contributions:

- The development of novel extensions to existing MBMS mechanisms to allow a significant reduction of signalling overhead in UMTS networks for provision of location based multicast services.
• A performance evaluation and verification of the extensions by a developed layer 3 MBMS simulation model. Compared to the current approach, significant signalling saving can be achieved over the wireless link. It has been found that the savings are higher the more likely users are expected to change service flows during a session.

• The development of a session layer solution in the form of a group management support, that enables interworking operators to coordinate multicast delivery in an heterogeneous wireless network environment. The group management support increases overall network scalability by allowing operators to efficiently make use of their network resources.

• The design and implementation of a proof-of-concept prototype of group management support and its evaluation in a testbed. The implemented prototype is easily deployable and supports legacy applications, since no modifications to the current terminal APIs are required.

• An analytical evaluation of the multicast signalling channel that has been proposed as part of the group management support to carry efficient downlink signalling from coordinating network entities to a group of receivers.

• The development of a network layer solution to achieve multicast delivery coordination in heterogeneous networks. The solution is realised through router side and host side extension to the Internet Group Management Protocol (IGMP).

• The verifcation of functionality and a performance analysis of the added overhead by network layer solution using simulations.

• A prototype implementation of the IGMP extensions in a software based router and terminal. The performance of the prototype has been further evaluated in a testbed.

• A qualitative comparison of the session layer approach and the network layer approach for multicast delivery coordination.

1.3 Organisation

The subsequent chapters of this thesis present the aforementioned contributions in detail and are structured as follows:

Chapter 2 introduces relevant background on existing multicast mechanisms in wireless networks to understand the contributions made by this thesis. By surveying related
work in the areas of MBMS, multicast group management, flow filtering and multicast delivery coordination, the herein presented work is motivated.

Chapter 3 presents the proposed MBMS extensions that allow the provision of different location-based service flows via a single multicast bearer service. Then the developed layer 3 MBMS simulation model is described. The simulation model is used to evaluate the performance of the proposed extensions by comparing them to the current approach using separate multicast bearer services.

In chapter 4 group management support as a session layer solution for multicast delivery coordination is presented. First, fundamental concepts and design decisions of the group management support are introduced. Furthermore, the individual components are described, illustrating how these components interwork to achieve multicast delivery coordination. The chapter concludes with a service example.

Chapter 5 describes a network layer solution to achieve multicast delivery coordination in form of IGMP extensions. Initially the basic principles are presented, clarifying how the delivery coordination mechanism is achieved. The required extensions at the router and the host instance of the IGMP protocol are described.

In order to demonstrate the viability of the proposed concepts, proof-of-concept prototypes have been developed. The implementation of both solutions, the group management support and the IGMP extensions is described in section 6.

An evaluation of both approaches is then provided in chapter 7. The evaluation consists of two complementary parts. First, the introduced signalling overhead is evaluated analytically and through simulation. Then through testbed experiments of the implemented prototypes, further performance characteristics are obtained and the validity of the developed concept is verified. The chapter concludes with a qualitative comparison of both approaches.

Finally, chapter 8 presents a summary of the thesis and concludes it with a discussion of the specific contributions. In addition, open questions and challenges and future work are identified and briefly discussed.
Chapter 2

Background and Related Work

Multicast has been a fertile research area for many years. This chapter provides an introduction to existing multicast mechanisms, focusing on the wireless domain, and discusses the issues raised in a next generation wireless network environment. By explaining the issues and surveying previous approaches in related areas, the need for mechanisms to achieve multicast delivery coordination in heterogeneous wireless networks is motivated.

Section 2.1 gives a brief overview of the basic IP multicast mechanisms used in the Internet. Section 2.2 then presents technologies to achieve IP multicast delivery in wireless networks. Section 2.3 surveys work addressing the filtering of flows within multicast groups. Furthermore alternative approaches of multicast delivery coordination are presented in section 2.4.

2.1 An overview of IP multicast on the Internet

Facing the growing demand in bandwidth consuming multi-media services and applications in the recent years, mechanisms that allow resource efficient IP data delivery to a larger receiver audience are gaining greater importance. Traditional unicast communication is not well suited to provide scalable data delivery to many receivers. A source sending service data to multiple users using unicast delivery has to send a copy of it to each user. As a result network resources can be wasted, since routers and links on common paths towards the destination, will have to process and forward redundant packets.

IP multicast transmission, in contrast, provides a resource efficient way of point-to-multipoint communication. The source needs only to send a single copy of service
2.1. An overview of IP multicast on the Internet

data addressed to an IP multicast group address. Routers on the delivery paths towards the receivers duplicate packets only when really necessary, in the cases where the routes towards the receivers diverge. IP multicast utilises the User Datagram Protocol (UDP) \[18\] for the transport of service data. For reliable delivery, additional higher layer mechanisms have to be implemented. While IP multicast provides its services on the network layer, it is also important to note that interaction with link layer mechanisms is supported. If operated over a broadcast medium like Ethernet, IP multicast addresses are mapped to a medium access control (MAC) layer multicast addresses. Thus network interface cards at routers and receivers are able to filter incoming MAC frames based on the multicast address rather than solely relying on the IP layer to perform the filtering. By default, IP multicast traffic, once send to a subnet by a router, will propagate to all segments of the subnet. In order to have traffic of a multicast group only reach the segments of a subnet with interested receivers, additional link mechanisms are able to perform adequate filtering with layer 2 switches \[19, 20\].

Since its introduction in the late 80s by Deering \[6\], IP multicast mechanisms as well as its service model have constantly evolved. IP multicast is facilitated through a combination of functions and protocols. A brief overview of the most important functions is provided:

- **Multicast Group Management** deals with the collection and maintenance of the multicast group membership, the set of receivers which are interested in receiving data sent to the same multicast group. Multicast group management protocols operate between hosts and the first hop multicast router on a subnet. Using a group management protocol receivers notify multicast routers about the IP multicast groups they are interested in. Routers collect and maintain this membership information for each of their interfaces.

- **Multicast Routing** protocols ensure that efficient delivery paths from sources sending to a multicast group to all interested receivers are established. The collection of paths over which a multicast packet is sent is called a multicast delivery tree. Multicast routing protocols have the following tasks: The construction and maintenance of multicast delivery trees to connect the multicast group members within the network and the forwarding of multicast packets on those delivery trees. For their operation, multicast routing protocols utilise the group membership information collected by the group management protocols.

- **Multicast Address Management** deals with the assignment and the scope of multicast addresses. The initial multicast service model allowed senders to send data addressed to any valid multicast address. If two sources sending in the same scope use the same multicast address, unintentional address collisions may
2.2 Multicast technologies in wireless networks

Multicast technologies in wireless networks occur. By coordinating address assignment, multicast address management aims to avoid address conflicts within a domain or between different domains.

- **Multicast Security** protocols make sure that only intended receivers can receive or make use of data sent to a multicast group and that receivers only obtain data of intended sources. This includes issues such as authentication and authorisation of group members that want to receive data of a particular group as well as the source(s), sending data to this group. Other aspects include the encryption of IP multicast data and scalable mechanisms for encryption key distribution.

- **Multicast Service Announcement and Discovery** handles the ways, how non members of a multicast group can be informed about an ongoing multicast session, or discover an ongoing session. It also handles how a source can notify its willingness to send data to a specific multicast group.

To date a large number of mechanisms and protocols have been proposed within the research community to achieve the required functionality. With regard to the presented multicast functions, this thesis mainly focuses on mechanisms concerned with multicast group management; nevertheless contributions related to the area of multicast routing in mobile networks are made.

2.2 Multicast technologies in wireless networks

The basic principles of IP multicast delivery are also applicable to wireless networks. Some wireless networks can be seen as mere extensions to the wired Internet. For example wireless networks based on IEEE 802.11 technologies employ the same IP based infrastructure as wired local area networks, only replacing the Ethernet medium by a wireless medium for access on the last hop. Thus current IP multicast protocols operate the same way as over a wired Ethernet link. Other wireless networks however employ more sophisticated architectures and transmission technologies and may not natively support the existing Internet IP multicast mechanisms. Examples of such networks are mobile networks and digital broadcasting networks. In the following an overview of relevant mechanisms to achieve IP multicast transmission in UMTS and DVB networks is provided.

2.2.1 Multicast in UMTS networks

UMTS networks offer a highly sophisticated network bearer architecture for data delivery to mobile users in a cellular environment. Within the UMTS architecture, the
General Packet Radio Service (GPRS) is utilised for bidirectional transport of packet-based data. A common packet domain Core Network (CN) is used to interface to different Radio Access Networks (RAN). On top of this IP based infrastructure, GPRS implements an overlay architecture providing authentication and charging, mobility management, quality of service routing and packet forwarding.

As traditional mobile networks were used to support mobile communication between two parties, GPRS was initially designed for point-to-point communication. The current UMTS Release 5 allows the reception of multicast data as an option in the GPRS specification. From the Internet point of view, IP multicast terminates at the Gateway GPRS Support Node (GGSN). Multicast applications running on the UMTS mobile terminal can use a group management protocol to join a multicast group on the Internet via the GGSN. The GGSN acts as a multicast leave router and delivers incoming multicast traffic via point-to-point connection through the UMTS networks, to the interested receivers. While the reception of multicast traffic from the Internet is supported, no bandwidth savings are achieved within the UMTS network. Data is delivered via individual connections to each receiver, instead of using shared resources in CN and the RAN.

In order to support resource efficient delivery of IP multicast traffic in UMTS networks, Multimedia Broadcast and Multicast Services (MBMS) [8, 9] have been recently standardised and included in the new UMTS release 6. MBMS provides point-to-multipoint bearer services, which can be used by multicast or broadcast applications to transfer data efficiently from one source to multiple mobile receivers. MBMS supports the delivery of both IPv4 and IPv6 multicast data and tries to make use of existing IETF mechanisms wherever appropriate. In the following subsections, an overview of the functional MBMS architecture is provided. Furthermore, important procedures that are required for the management of the MBMS multicast bearer plane in the CN are explained.

**MBMS architectural overview**

As mentioned above, MBMS provides resource efficient multicast bearer services that can be used by multicast user services or applications to deliver service content to a potentially large number of receivers. MBMS bearer services use shared delivery paths in the core network up to the radio access network and shared downlink channels over the radio link. Two different modes are defined for the MBMS bearer service, a broadcast mode and a multicast mode.

The broadcast mode is intended for sending service data from a single source to all receivers in a defined broadcast area. A broadcast area can be pre-configured and
2.2. Multicast technologies in wireless networks

Multicast technologies in wireless networks may consist of one or several UMTS cells. In the multicast mode service data can be delivered from a source to a multicast group in a multicast service area. Similar to the broadcast mode the multicast service area can also be pre-configured, but data is only delivered to those cells in the service area, where users have expressed interest in receiving the service. Both modes intend to make efficient use of radio and network resources. Broadcast and multicast services can consist either of a single on-going session or several intermittent sessions. Unlike in broadcast mode where every user is able to receive the MBMS data, the multicast mode requires a subscription to the multicast group and the users joining before the start of the session. In the multicast mode the network is able to create charging data per user for a particular session.

Figure 2.1 shows the UMTS reference architecture, including the functional entities required by MBMS. Besides a new network entity called Broadcast Multicast Service Centre (BMSC), MBMS extends existing Gateway GPRS Support Node (GGSN), Serving GPRS Support Node (SGSN) and Radio Network Controller (RNC) with MBMS specific functionality. The BMSC is the entry point for a content provider in order to utilise the MBMS services inside a Public Land Mobile Network (PLMN).

The BMSC authenticates and authorises content providers and verifies the integrity of the content. It can determine the QoS parameters of the MBMS service, allows the definition of the service area and generates charging data for the content provider. It also provides functions to announce the service and to schedule the MBMS data for transmission. The $G_{mb}$ reference point has been added to provide an interface for control plane signalling between BMSC and GGSN. IP multicast data is delivered to the MBMS bearer services via the already existing Gi reference point, which is used to interface the GGSN to public data networks.
2.2. Multicast technologies in wireless networks

MBMS context

For each multicast service two types of MBMS context are maintained in BMSC, GGSN, SGSN and RNC. The first one is the MBMS bearer context, which stores bearer specific parameters. Such parameters include the associated IP multicast address, a list of downstream nodes, service area and QoS specific parameters. There is at most one MBMS bearer context per multicast bearer service in a particular network node. MBMS bearer context is used for forwarding multicast data on the bearer service and therefore only exists in network nodes, that are part of a shared delivery tree for a particular multicast service. Each node stores the addresses of its downstream nodes in the delivery tree in the list of downstream nodes attribute of the respective MBMS bearer context. Each data packet that arrives at the multicast bearer service from an upstream node is replicated and forwarded to each downstream node of the list.

The second type of context, maintained only for MBMS bearer services in multicast mode, is the MBMS UE context. There is one MBMS UE context per network node per multicast group for each interested user. MBMS UE context is stored in the corresponding MBMS bearer context along the nodes of the delivery tree. MBMS UE context stores user specific information, which is used for mobility management, billing purposes and other uses.

Unlike in the IP multicast group management model on the Internet, group membership information is maintained for every user, not only for a particular group. Furthermore, group membership information is maintained for a UE in every node that is part of its routing path along the delivery tree within the UMTS network.

MBMS procedures

Figure 2.2 shows the MBMS service activation procedure for multicast bearer services. The purpose of the activation procedure is to register the user with the network to enable the reception of a specific multicast bearer service. The service activation procedure establishes MBMS UE context in the network nodes. It also may trigger the establishment of MBMS bearer context, which is required for the establishment of multicast delivery trees with appropriate quality of service to respective cells within the service areas. The establishment of the appropriate delivery trees is done through the registration procedure.

2. Recognising the UE through the PDP context, the GGSN extracts the IP multicast address from the join request and requests an authorisation for the user at the BMSC for the identified multicast service. The BMSC verifies if a valid subscription to the multicast user service exists for the UE indicating success or failure in its authorisation response.

3. The GGSN then notifies the SGSN currently serving the UE about the intended multicast service activation.

4. A SGSN supporting MBMS then requests the MBMS context activation by the UE.

5. UE creates the corresponding context and proceeds with the activation of the multicast service, providing the SGSN with its own QoS capability.

6. Knowing that the terminal is able to support the bearer service, the SGSN creates a user-specific MBMS context for the UE and requests the GGSN to also create a corresponding context.
7. The GGSN, which may be different from the initial one, verifies if the user is entitled to receive the multicast service.

8. After successful authentication, GGSN creates the corresponding user specific context and notifies the SGSN.

9. The SGSN then notifies the UE of the required bearer capabilities and that the activation procedure has been completed successfully.

10. For Packet Mobility Management (PMM) connected UEs, user specific MBMS context is provided to the RNC via MBMS UE linking signalling. Registration is performed by a downlink node e.g. SGSN to its uplink node e.g. GGSN, whenever the first user specific context for multicast bearer service was created and no service specific context exists. Through the registration procedure the downlink node becomes part of the delivery tree in the network.

Analogous to the activation procedure the deactivation procedure is used to deregister a UE from a multicast bearer service. As a result of the procedure, which is shown in figure 2.3, all user specific context for a multicast bearer service are removed from the network nodes. In addition, if a network node notices, that it does not serve users for a multicast bearer service, it deregisters from the uplink node, removing itself from the multicast delivery tree. This is done through the deregistration procedure.

1. The deactivation procedure is initiated by sending an explicit leave IGMP/MLD message to the GGSN over the preestablished PDP context.

2. The GGSN notifies the BMSC that a UE wants to stop receiving data from the indicated multicast bearer service.

3. The BMSC verifies if the user has established the respective multicast bearer service and requests the removal of a user specific context from the GGSN.

4. The GGSN notifies the SGSN that the UE wishes to deactivate the indicated multicast bearer service.

5. The SGSN then request the deactivation of the context for the multicast bearer service, which the UE confirms after freeing up the context resources for the bearer service.

6. If user specific context has been previously linked with the RAN for a UE, it is released through the delinking procedure.

7. The SGSN then requests the GGSN to release user specific resources for the multicast bearer service.
8. The GGSN frees the resources and indicates successful deactivation to the BMSC.

9. Finally GGSN informs the SGSN of the successful deactivation and the SGSN also frees up any user related context for the multicast bearer service.

Both procedures, the service activation and deactivation, are signalling intensive procedures, which are executed for every UE that wishes to start or stop receiving data from a multicast service. Registration and deregistration procedures are responsible for maintaining the MBMS delivery tree in the network. Unlike the service activation or deactivation, they are triggered by network nodes only when a first user enters or a last user leaves the service area covered. However, with increasing number of users, these procedures can add a significant signalling burden to the network.

2.2.2 Multicast in DVB networks

Originally designed to carry broadcasting content for digital television, the Digital Video Broadcasting (DVB) standard has become an attractive alternative to deliver IP data services [23]. The DVB project and ETSI have recently standardised the IP
2.2. Multicast technologies in wireless networks

datacast standard [12, 24], which facilitates the delivery of IP data over DVB, alongside audio and video content. Likewise the IETF has created the DVB-IP group [25] to look into the issues of IP data transport over DVB.

The IP datacast standard over DVB networks will allow the delivery of high bandwidth IP data flows to mobile terminals. In particular, the terrestrial versions of DVB, namely DVB Terrestrial (DVB-T) and DVB Handheld (DVB-H) are suitable for mobile reception. DVB-T was initially designed for stationary receiver set-top boxes in a home environment. Data rates up to 25 Mbit/s can be typically provided using a single 8MHz channel in the Ultra High Frequency (UHF) band. DVB-T was further optimised and developed into DVB-H, in order to allow mobile reception DVB-T and to suit the requirements for small handheld devices. DVB-H significantly reduces power consumption at the receiver and introduces features for better mobility support. DVB-H supports data rates of typically up to 10Mbit/s per 8MHz channel.

In the following an overview of IP multicast service provision in DVB networks is provided. Furthermore, problems for multicast service delivery due the unidirectional nature of DVB are briefly discussed, while presenting an existing solutions addressing this problem.

MPEG-2 layer in DVB

For DVB systems, MPEG-2 has been chosen as the standard for compression of the high quality digital video stream. MPEG-2 also defines a transport mechanism to multiplex various video, audio and data streams together to one common Transport Stream (TS), which also allows the synchronised play-out of all this components at the receiver. Compressed media and data components are packetised into fixed sized MPEG-2 TS packets of 188 bytes, which are combined to several logical channels into one common TS. The logical channels are identified by 13-bit packet identifiers (PID) which are part of the header MPEG-2 TS packets. Theoretically 8192 channels can be transmitted inside one TS, however a small number of PID channels are reserved for service specific signalling. This additional signalling information is generated in the form of service information (SI) tables, in order to allow the receiver later to tune to a specific channel within the transport stream and to reassemble and decode the original video, audio or data stream.

IP over DVB

The DVB project has specified a Data Broadcasting Standard [26], which allows insertion of various user data types including IP data packets in the MPEG-2 TS. Figure 2.4
2.2. Multicast technologies in wireless networks

shows an overview of the protocol stack used for IP data delivery over DVB. Multi Protocol Encapsulation (MPE) has been recommended for encapsulating IP data packets. MPE is based on the section formats of DSM-CC (Digital Storage Media Command and Control), which was defined in the MPEG-2 standard as a toolkit for developing control channels associated with MPEG-2 streams. Incoming IP data packets are first encapsulated in MPE packets, and then segmented to fit into the MPEG-2 TS packets and multiplexed onto a logical channel of the TS. Every MPE packet includes the next hop destination MAC address in its header.

Figure 2.5 shows the encapsulation process. Each logical channel is identified by a PID value. The receiver will be able to identify the channel carrying IP data by consulting the SI tables that are generated during IP data encapsulation. The encapsulation is usually carried out by an IP/MPE encapsulator, which is often referred to as IP/DVB gateway. Since the number of logical channels in one TS is quite limited, IP data packets from IP data connections (source receiver pairs) can be multiplexed into one channel. Packets belonging to the same data stream are uniquely identified by the PID value, the source address and the destination address and are referred to as IP stream.

In order for a receiver to locate an interested IP stream in the TS sent by the DVB transmitter in a network, additional service information needs to be generated during encapsulation. For this purpose an IP MAC notification (INT) table is used to signal the availability and location of an IP stream in a TS.

**IP multicast over DVB**

In order to receive data sent to a multicast group, users usually locally configure their network interface to extract incoming packets for the multicast group to pass it to the IP layer. At the same time a group membership message is sent to the access router to notify the interest in receiving multicast traffic. In a DVB-T/H network, no direct return channel is available. Although reception of IP multicast data is possible, once
2.2. Multicast technologies in wireless networks

Figure 2.5: Encapsulation of IP data into the MPEG2 transport stream.

In such circumstances, IP multicast services sent via the DVB network need to be determined by the network operator in advance. Using an Electronic Program Guide (EPG) or well known multicast channels for service announcements, receivers are able to learn about service available on the DVB network. If interested in a service the DVB receiver in the user terminal will tune in the appropriate TS and consult the INT table to locate the IP stream within the TS. The IP datagrams belonging to the IP stream are decapsulated from the MPE packets and passed to the IP layer for further processing. Optional filtering can also be performed using the MAC address within the MPE packets.

Dynamic initiation of multicast service by the receiver is only possible via an alternative return link. A multicast router, however, assumes multicast traffic to be forwarded to an interface, over which a group membership message has been received. A user that attempts sending a group membership message to advertise its interest in a multicast group over the return link, e.g. a UMTS network, would thus receive the multicast traffic via the return link. In order to ensure correct operation of IP multicast, the group membership message should arrive at respective subnet of the multicast router that 'feeds' the IP/DVB gateway for transmission over DVB.

In order to assure proper operation of IP multicast group management and other routing mechanisms assuming a bidirectional link, the Unidirectional Link Routing Protocol (UDLR) [27] has been proposed. UDLR emulates bi-directional connectivity for the unidirectional broadcast link. UDLR does the emulation by establishing a layer-2 tunnel and this requires a bi-directional return channel. In order to work, UDLR requires a server running on the network side and a client module in the receiver, which both represent the endpoints of the layer-2 tunnel. Both client and server encapsulate the packets coming from the upper layers using generic router encapsulation (GRE) [28]
2.3 Multicast flow filtering

The overhead of IGMP signalling for joining and leaving a multicast group has been already a subject for study by the Internet research community. The signalling overhead may not be negligible for multicast applications, which may require a frequent change of multicast groups during runtime, e.g., large distributed simulations. Furthermore the associated join and leave delay may become critical to their operation.

In [29], Levine et al. have analysed different mechanisms that are used to scope content delivery to particular receivers for large scale applications using IP multicast. In particular two common techniques namely addressing and filtering have been examined. Addressing assumes multicast flows to be delivered in separate multicast groups to the receivers. Despite the resource efficiency of the addressing approach, applications may suffer from join/leave delays when changing flows and the networks face additional signalling overhead introduced by the group management signalling. Filtering assumes multiple application flows to be broadcast to all receivers via a common multicast group. Receivers then filter the content which they do not require. While the approach does not suffer from delay and signalling overhead, it does waste network resources, since flows may be delivered to network segments without interested receivers.

These observations have motivated other researchers to propose an approach based on router level filtering (RLF) [30]. RLF extends common IP multicast mechanisms by introducing capabilities in routers to filter flows within a multicast group. The semantics of filters are identified by the applications. Applications label the subflows with flow identifiers and receivers express their interest in flows by composing filters. These filters are then pushed upwards towards the routers of the multicast delivery tree. As a result, routers only forward the required flows on the links towards the receivers. Thus, unlike in the traditional filtering approach at the receivers, no additional network resources are wasted in terms of bandwidth. RLF mainly targets the signalling overhead and the join/leave latencies when communication flows and hence multicast groups need to be changed frequently during an application session.

Content based multicast [31] is another proposal for applying content based filtering by
nodes that a part of an IP multicast tree. The work proposes the use of mobile filters to achieve a higher personalisation of multicast content. However most of the work is based on determining optimal placement of mobile filters within the multicast delivery tree, according to receiver interest.

The required signalling for multicast bearer service activation/deactivation in UMTS networks is by a magnitude larger than required IGMP/MLD group management signalling to notify leaf routers on the Internet. Therefore efficient filtering mechanisms for MBMS are required, in particular for multicast services in which service flows for receivers are expected to change more frequently. Location based services are suitable examples for where such mechanisms can be used.

2.4 Multicast delivery coordination

When hosts are interested in receiving IP traffic from a particular multicast group, they advertise their interest to the neighbouring multicast router by using a multicast group management protocol. Since in the current group management model, a multicast group membership is always tied to a particular interface, the host implicitly selects the delivery network, to which the network interface is attached.

The purely receiver driven multicast group management model is based on the principle, that a receiver is free to decide which multicast group to join and what network interface to use for the delivery. In fact, when the initial multicast model was developed in the late 80s, most of the hosts were merely attached to a single network. Assuming the host decided which interface to use for the delivery, most of the research in optimising multicast delivery has therefore focused on multicast routing protocols. The main challenge addressed has been to deliver IP multicast data most efficiently from a source to a particular subnet. In the presence of multiple interfaces at the hosts attached to different access networks, another more fundamental question becomes more apparent: Besides delivering IP multicast data most efficiently from a source to a particular subnet, on which subnet shall the IP multicast data actually be delivered?

Paradoxically, the receivers, which currently decide this question, do not care about the delivery network, unless the delivery quality, availability or delivery price are affected. In contrast network operators have a higher interest in the management of traffic to assure appropriate resource utilisation. Particularly in the wireless domain, effective resource utilisation is a major concern, where the availability of network resources is usually more restricted. An operator who owns multiple access networks, or cooperates with other operators for service delivery, would like to select an appropriate network for the service delivery, or balance the network load during a session. While the current
multicast service model does not provide the desired features, additional mechanisms for such multicast delivery coordination are required. There are many feasible approaches to realise such mechanisms for multicast delivery coordination. Replacing the existing, purely receiver driven, multicast mechanisms with mechanisms that allow network operators to control multicast delivery more tightly, is considered as too radical, since it causes significant deployment problems. Therefore incremental solutions are preferred, which require little changes to implement the desired functionality, while reusing existing mechanisms as much as possible. Two possible ways to achieve such an incremental approach are:

- adapting existing multicast mechanisms and protocols to implement the desired features
- adding new mechanisms to implement the desired features, leaving existing mechanisms unchanged.

While each of those approaches offers certain advantages over the other, they also expose distinct weaknesses. A discussion of those is provided in chapter 7. The group management support, proposed as an solution for multicast delivery coordination in this thesis, falls in the first of the two categories: It provides a session layer solution on top of the existing network layer multicast mechanisms. Related research and mechanisms can be found in work on multicast access control, heterogeneous wireless networks, and in the area of session layer support for applications. The second approach proposed in this thesis, provides a solution for multicast delivery coordination on the network layer by extending IGMP; it can be classified as belonging to the latter category. A survey of the evolution of the group management protocol and previous attempts of its modification is provided. However the approaches tackled only some of the related problems.

2.4.1 Multicast group management

Since its introduction in the late 80s by Deering, the Internet group management protocol (IGMP) underwent several revisions. The initial version, IGMPv1 [6] provided a simple query/response mechanism for routers to learn about multicast group membership of hosts attached to a routers interface. Routers periodically send host membership queries, while hosts reply with host membership reports containing the addresses of groups which they are subscribed to. In order to inform the router of a requested membership more quickly, hosts send unsolicited membership reports immediately after they join. When leaving a multicast group, hosts stop replying with membership
2.4. Multicast delivery coordination

reports for that group. If no membership reports are received after a membership query by a router, the router assumes no interested members are present and stops forwarding incoming multicast traffic on that interface. This timeout based mechanism has proved to be inefficient, since traffic may be unnecessarily forwarded on a link until the current query interval expires. In order to improve the leave latency, IGMPv2 [21] allowed hosts to send a leave request, when stopping to listen to a multicast group. The router still uses general queries to learn about the overall membership of the attached hosts on each link. However after receiving a leave request, a router issues a group specific query to determine if other hosts are still members of that group. If this query remains unanswered, the router assumes no interested members are present and stops forwarding traffic on the queried interface. Both versions provide the so called any source multicast model or (*,G), where any source (*) could send to a multicast group G, and all subscribed receivers had to receive traffic from all sources. Due to access control considerations, lack of address space and inter-domain routing problems, support for source filtering has been introduced in the latest revision IGMPv3 [32]. Hosts now have the ability to specify (S,G) a list of sources S, in the form of a source filter and a filter mode, besides the multicast group G. Thus in source specific multicast, routers only forward traffic of sources sending to a multicast group, to which receivers have explicitly subscribed. An equivalent group management protocol implementation for IPv6 also exists, named Multicast Listener Discovery (MLD) protocol, where MLDv1 [22] and MLDv2 [33] reflect the functionality of IGMPv2 and IGMPv3, respectively.

Despite the revisions in the group management protocol, IP multicast deployment is still far behind expectations. The most prominent analysis of the problems behind the multicast service model has been made in [34]. Diot et al. identified the lack of access control due to the open group management model as one of the main problems of the multicast service model. While some of the issues have been later addressed within IGMPv3, considerable protocol overhead is introduced due to the removal of the report suppression mechanism in IGMPv1/v2.

Liao and Yang [35] therefore proposed a new receiver-initiated group management protocol (RGMP). RGMP completely removes the query mechanisms from the router and replaces it with soft-state, which needs to be frequently updated by the receivers. Receivers need to maintain timers for each subscribed multicast group and source, and report joining or leaving, state changes and periodic updates to the router. Lower protocol overhead is achieved by not using query messages and applying suppression mechanisms based on timer management in the hosts.

Mazumder, Almeroth and Sarac discuss in [36] the inability of a host to determine a failure during multicast service provisioning. Possible sources for failure have been identified starting from the local host up to the multicast sender and a tool has been
presented called the multicast detective, which aids troubleshooting at the receiving host. The authors have outlined the lack of network feedback as a major drawback in the current multicast model and propose improvements in the form of a join acknowledge (IGMP/MLD ACK message) sent by the router on receipt of a membership report back to the host, or an IGMP/MLD status query message sent by the host to the router to learn if its membership status has been reflected by the router. While outlining these ideas in detail, the reference fails to provide any implementation details, simulation or testbed results.

Also group management modifications for IP multicast delivery in wireless networks have been proposed. Kaur, Madan and Ganesan aim to reduce the protocol overhead of IGMP when handing over to a new access router [37]. Instead of sending separate membership reports and leave messages for every multicast group a mobile host has subscribed to, an aggregation mechanism is proposed. The aggregation mechanism allows several multicast group addresses to be included in a single message. Furthermore new IGMP message formats are introduced. As a result fewer messages need to be sent when leaving a previous access router or subscribing to a new one, thus reducing the IGMP signalling overhead and join latency. The proposed mechanism is however only useful if a host has been subscribed to multiple multicast groups.

Xylomenos [38] investigates the use of IGMPv2 and IGMPv3 for MBMS multicast bearer management and compares their performance in terms of signalling overhead. He outlines that the current query response model of IGMP is not suitable for MBMS, since membership queries and reports are not sent on a broadcast medium and therefore heard by others, but rather on individual point-to-point connections to the GGSN. He outlines how reliable IGMP message delivery can be improved in MBMS. IGMP message retransmission can be suppressed by cross-layer notification, where the MBMS layer notifies IGMP to cancel retransmissions when the bearer is successfully established.

While each of the approaches addresses different deficiencies of IP multicast group management, none of them has addressed issues that may arise on hosts with multiple network interfaces. Like the surveyed approaches, the network layer approach presented in this thesis also modifies the existing multicast group management mechanism. Its aim, however is to extend the multicast group management model currently limited to a single interface to operate across multiple interfaces available at a receiver.

2.4.2 Multicast access control at the router

A passive form of delivery coordination can be achieved by restricting the network access of receivers for a particular multicast service. By introducing mechanisms for
access control, the delivery of traffic to particular multicast group can be disabled for selected subnets.

Lehtonen and Harju have studied issues of multicast access control for receivers and senders and proposed a controlled multicast framework [39]. The work provides access control of multicast receivers joining specific multicast groups (G) or (S,G) and multicast senders at the edge routers. A central Multicast Control Agent (MCA) holds a database of all controlled multicast groups describing authorised sources and receivers. Each edge router runs a filtering layer between IP and IGMP protocols, which intercepts incoming IGMP messages of receivers and multicast data packets from sources. A protocol called Multicast Control Protocol (MCOP) [40] is introduced for configurations and queries between the 2 entities. Initially MCA configures each edge router with access restricted IP multicast addresses. Then, for each new receiver/source, where no authorisation state exists, routers query MCAs for validation. The results of the validation are stored locally at the router for further messages and packets, and can be updated/deleted by the MCA. Membership request from unauthorised receivers and data packets of unauthorised sources are discarded by the filtering layer. IGMP protocols and routing protocols remain unmodified. While the framework prevents membership reports of undesired receivers to reach the router, it cannot prevent undesired receivers receiving the traffic of groups that an authorised receiver on the same subnet has joined. Furthermore the filtering process remains unacknowledged, leaving the receivers unaware of the reasons for failure to receive multicast traffic. Feedback mechanisms could ensure that appropriate failure handling mechanisms can be executed at the receiver.

2.4.3 Multicast delivery in heterogeneous network

A more active approach of delivery coordination targeting hybrid mobile networks has been proposed by Lohmar et al. [41]. The work, which has been carried out as part of the IST OverDRIVE project [42], identified that current group management functionality of IP multicast and MBMS are not efficient for the requirements in a multi-access system and that new tasks and functions are required. Assuming a common core network connecting multiple access networks, a new group management model is proposed, in order to optimise multicast delivery to a heterogeneous group of receivers with different mobility patterns. The overall task of the group management model is to ensure the optimal usage of links and system resources. Four basic tasks for group management are identified: group membership handling, group partitioning, media selection and group mobility management. For group membership management a registration process is identified, similar to the MBMS model, where a user first registers with a
2.4. Multicast delivery coordination

group membership server to be able to join a multicast session. The group partitioning function is the main function of the group management model. It is responsible for deciding the optimal transmission and to trigger respective functions to implement these decisions. Optimisation is achieved by dividing members of the multicast group into smaller subgroups or merging them into a larger subgroup. Two main criteria for determining the optimal transmission are proposed for the group partitioning process, namely network efficiency and user satisfaction. Finally the group mobility function is responsible for executing grouping decisions made by implementing seamless mobility of multicast receivers through appropriate protocols. The support of seamless session continuity when moving between hierarchical access networks as well as the support for per-flow handover for multicast traffic have been identified as main requirements. This paper [41] underlines that dedicated mobility and session management protocols are required to implement the interface between group partitioning and group mobility functions. The contributions that have been made with respect to delivery coordination are mainly of theoretical nature. It fails however to provide any details or implementation of such protocols.

Another approach targeting multicast delivery in mobile and broadcast networks has been proposed by Berg [43] et al. The work has been carried out in the IST CISMUNDUS [44] research project. The project developed a delivery subsystem and corresponding interfaces that allow multicast services to be delivered, in a converged mobile and broadcast network environment. The system provides a standardised framework for discovery of such services. The delivery network is dependant on the service characteristics and pre-configured by the network operator. Service announcements are sent to each network, with appropriate service descriptions. The receiver is able to join a service on the network, on which the service announcement has been received. Thus delivery coordination is statically achieved. Receivers can only join multicast services that are advertised and offered within the system. Furthermore no dynamic changes to a different access network are possible during a session.

The DVB-CBMS technical module of the DVB project, looking at Convergence of Broadcast and Mobile Services (CBMS), has recently released an IP datacast specification over DVB-H networks [24]. A general technical framework for IP datacast systems has been specified. Although both mobile and broadcast networks are included in the architecture, data service are delivered via multicast only over the broadcasting network. The mobile network solely serves the purpose of requesting premium content, accessing interactive service content via unicast or digital rights management transactions.
2.4. Multicast delivery coordination

2.4.4 Session layer approaches

Most network applications and operating systems currently available use the Berkley socket API, which exports a connection abstraction for communication. A connection can be seen as a communication channel that is used by applications on two remote end points to transfer data packets between them. In TCP/IP a connection is defined by two communication end points, each identified by a network layer identifier, the IP address, and a transport layer identifier, the port number, and the transport protocol being used. Once specified, applications use these end points for communication for the duration of a session. The dependence on a network layer identifier as part of a communication association between application entities has a major disadvantage. If one of the network layer identifiers changes, e.g., due to mobility, during a communication session, the communication end point becomes unusable to the application.

A session layer can provide the application with consistent communication abstraction, which conceals any change of network layer identifiers to the application. In [45], Snoeren proposes an end-to-end approach for Internet mobility, based on a session layer. The session layer manages underlying TCP or UDP connections seamlessly to applications, while users may change network layer identifiers when moving to different networks. Besides connection management, the session layer provides session management functionality to manage session states in times of longer disconnections. His work concentrates solely on unicast communication between two end systems.

The session initiation protocol [46] is a control signaling control to establish, modify or terminate sessions between two or more applications. Although the name suggests SIP to be located in the session layer, it is actually an application layer protocol. SIP is integrated as part of the application, thus only SIP aware applications can use the provided functionality. Instead of using communication end points based on network layer identifiers, SIP uses e-mail like addresses, the so-called SIP URIs (e.g., sip:alex@surrey.ac.uk). Although SIP may be used to control and renegotiate sessions between multiple communication participants, it is not scalable for large numbers of receivers, since the signaling is delivered via unicast between parties.

In [47] Swan and Row have recently motivated the case for a multicast session layer. The authors argue that the appearance of new multicast service models, such as any source multicast, source specific multicast or application layer multicast leave application developers with a dilemma to know the features and the API of each of the protocols in order to chose the right one for a particular application environment. A multicast session layer can provide a higher level abstraction to a collection of different multicast services, which will simplify application development and satisfy heterogeneous deployment of multicast services. With appropriate network feedback, the session layer
could automatically select appropriate multicast services to improve the multicast applications. New services can be integrated within the multicast session layer, while still providing the same interfaces to the application programmers.
Chapter 3

MBMS Protocol Extensions

The dissemination of user data according to the user location is considered an important multicast service to be offered in the future by mobile network operators and service providers. Examples of such location based multicast services are delivery of traffic or weather information, news or radio feeds, electronic newspapers with regional scope, or electronic advertisements of shops, restaurants or entertainment facilities around the users current location. A location based multicast user service thus provides multiple versions of content or flows customised to localised service areas.

The current mechanisms proposed in [9] allow a multicast user service to use different local service areas for the same bearer service for different sessions, which are the same or a subset of the overall multicast service area as defined in [8] for multicast bearer service. Using the same multicast bearer service a multicast user service is able to provide localised versions of content in consecutive sessions. For each session the local service area is adjusted at session start and the respective local content sent via the same multicast bearer service.

In order to provide different localised version of content simultaneously, a multicast service would need to utilize a separate multicast bearer service for each local area. A user moving from one local service area to another, however, would have to change to a new bearer service in order to continue receiving the location specific content of the same multicast user service. Moreover, the frequent establishment and release of bearer services may lead to significant signalling overhead, especially for popular location based multicast services.

This chapter presents a novel efficient delivery mechanism, which allows a multicast user service to provide different versions of location based service content concurrently using the same MBMS bearer service. Section 3.1 introduces briefly the current approach using separate multicast bearer services for each service flow. Then the principles of the
3.1 Current provisioning of location based service in UMTS

In the following the current approach is presented, which is required to provide location based multicast user services with concurrent flows to local service areas.

Figure 3.1 shows an example of an MBMS enabled UMTS network. A location based multicast user service provides different versions of location specific content to five local service areas (LSA), enumerated LSA1-LSA5.

For each of the local service areas the multicast user service uses a separate multicast bearer service (MBS), since data is sent simultaneously to all local service areas. The sources of the multicast user service are not explicitly depicted, but they feed the five different service flows to the BMSC on separate bearer services (one location specific service flow per bearer service). The different delivery trees for the multicast bearer services MBS1-MBS5 are indicated by lines of different style. It is assumed that interested receivers are present in each of the LSAs.

It is not difficult to see that a user who moves from one service area to another would need to change the bearer service to continue receiving location specific content of the same multicast user service. Changing the MBS, however, requires the release of the previous MBS and the establishment of a new MBS for the user. In other words additional signalling is required for the deactivation of the old MBS and the activation of the new MBS.

As shown in section 2.2.1, signalling procedures for service activation and deactivation contribute significantly to the signalling load in the UMTS network. However in the described case of location based multicast user service activation/deactivation procedures are executed more frequently, not only once when starting/terminating to receive the multicast service, but also whenever changing a local service area. This holds true especially for larger number of receivers, smaller LSAs and increasing user mobility.

3.2 Proposed service provisioning principles

In addition to the IP multicast address, which identifies a multicast bearer service, a location area identifier is used in the network nodes to separate the flows of the different
locations. Each location specific flow, sent by a multicast user service, is labelled with the location area identifier. Network elements along the multicast distribution tree within the UMTS network forward only flows to downstream nodes serving the respective service areas.

Figure 3.2 shows the principle of the proposed mechanism. As in the previous example the existence of five local service areas (LSA) LSA1-5 is assumed. The multicast user service provides relevant location specific content as service flows F1-5 to the BMSC, e.g., F1 for LSA1, F2 for LSA2 etc. using a single MBS for all service flows. Further the example assumes that interested receivers for the location based multicast service have joined the service in all five local service areas and the respective multicast delivery tree has been established within the UMTS network. The BMSC forwards all five flows to the GGSN, as its downstream nodes service all five service areas. SGSN1 covers LSA1, LSA2 and LSA 3, while the downlink nodes of SGSN2 service LSA4 and LSA5. Therefore the GGSN only forwards flows F1, F2 and F3 over the core network (CN) bearer to SGSN1 and flows F4 and F5 to SGSN2, respectively. Likewise SGSN1 forwards only flows F1 and F2 over the In bearer to RNC1 and F3 to RNC2, while SGSN2 provides flows F4 and F5 to RNC3 and only F5 to RNC4, respectively. The RNCs then relay appropriate flows over radio bearers to the respective cells of the
3.2. Proposed service provisioning principles

Figure 3.2: Delivery of multiple flows within a single multicast bearer service.

It is important to note that the receivers are left unaware of the flow labels and do not need to do any additional filtering. Their only association is to the multicast group and hence the multicast bearer service of the multicast user service. The network nodes are aware of the flow labels and ensure, that only an appropriate flow is transmitted over the radio bearer of the multicast bearer service within the cells of a respective LSA. Thus the proposed extensions only require modification to the forwarding and bearer management mechanisms within the network infrastructure.

As a consequence of the proposed mechanism, it can be seen that the required bandwidth, hence the required quality of service, varies at the different links between the network nodes and is not homogeneous for the whole MBMS bearer. However the bandwidth requirements of the radio bearers correspond to only those of a single flow and are thus homogeneous across all cells of the different LSAs. At any part of the delivery tree only necessary flows are forwarded downwards to the downlink nodes traversing the same network nodes and links as in the case shown in Figure 3.1 where separate multicast bearer services are utilised. The total aggregate bandwidth requirements for a multicast user service are the same for both cases, resulting in the same network load at each network node and intermediate links. Therefore the overall relative delay is not expected to increase. Moreover, only one multicast bearer context needs to be created.
in the network nodes of the delivery tree. This reduces the memory space needed for storing the multicast bearer context in network nodes and improves the scalability of the network. The savings, however, may be partly neutralised by required additions to multicast bearer context as described later in this section.

3.3 Protocol extensions

In order to implement this approach, some extensions are required to the currently specified MBMS mechanisms. The required extensions can be summarised as follows:

- Packet forwarding in the network nodes should not only be based on IP multicast address, but also on flow labels of the IP packets. For this reason the list of downlink nodes in an MBMS bearer context is enhanced by a flow forwarding entry for each node in the list.

- The registration procedure is enhanced to carry an additional attribute containing static local service area information; this information is propagated to each network node in the delivery tree.

- A flow registration procedure is introduced that is responsible for updating and maintaining the flow forwarding entries in the network nodes.

In the following subsection details of the implementation of these mechanisms are described.

3.3.1 Flow forwarding mechanism

It is assumed that the cells of each local service area (LSA) are exactly known for a multicast user service, and do not change for the lifetime of a multicast session. For each LSA a multicast user service generates a flow with the same QoS characteristics but with localised service content. Since all packets are sent using the same multicast bearer service (i.e., using the same IP multicast address), other means such as a flow labels can be used to distinguish between packets belonging to a flow. In other words, the source generating a flow for a multicast user service labels the packets with a unique flow identifier. Network elements in the delivery tree can use this identifier to identify packets belonging to the same flow within a multicast bearer.

Each LSA is defined by one or more cells, in which the same local content or flow is provided. LSAs are statically defined for a multicast user service and pre-configured in
3.3. Protocol extensions

Throughout this chapter the identifier for a LSA or its respective flow are used interchangeably.

The static LSA information is part of the multicast bearer context, and is propagated to each network node at the creation of the bearer context. As described in section 2.2.1, the creation of a MBMS bearer context is done by the registration procedure. It can be realised as a simple extension of the already existing MBMS service area attribute. No modification to the existing procedures are required.

Knowing its underlying LSAs and hence the flows identifiers, a network node in the delivery tree is able to associate the flow identifiers with its downlink nodes.\(^1\)

It should be noted that the static LSA information only tells what flows should be forwarded to a downlink node. However, there may be the case that not all flows are required to be sent to a downlink node. The example described in figure 3.2 is based on the assumption that there are interested receivers present in all local service areas. For instance, assuming the case that no interested receivers are present in LSA2, SGSN1, GGSN and BMSC would still unnecessarily forward flow F2 down the delivery tree, when only relying on static LSA information. Therefore additional flow forwarding entries (FFEs) are required, which reflect the actual state of flows needed in the network.

The multicast bearer context of each node is enhanced by FFEs for each downlink node element in the list of downlink nodes attribute. Figure 3.3 shows the FFEs for the network elements in the example. The flow labels of arriving packets on the multicast bearer are evaluated against the FFEs and then further replicated to the respective downlink nodes. For reasons of simplicity it is assumed that a downlink node connects only to one uplink node.

### 3.3.2 Update mechanism for flow forwarding entries

In this subsection the required mechanism to update and maintain FFEs is described. This is achieved by a modification of the MBMS registration procedure.

As in the current standard, the registration procedure is used to construct the delivery tree for the multicast bearer service and propagate relevant bearer context information to the respective network nodes. However besides the registration procedure, a procedure to register or deregister flows is added to maintain the FFEs in the network elements.

After service activation, MBMS UE context is created in SGSN and GGSN for a UE. In case no multicast bearer context is yet existing, GGSN and SGSN perform a regis-

\(^1\)It is assumed that a network node is able to associate a service area with its downlink nodes. Otherwise this information has to be added to the static LSA information.
3.3. Protocol extensions

Figure 3.3: Flow forwarding entries in the network nodes of the example shown in figure 3.2.

tration procedure. After the bearer context has been created, static LSA information is available in the network nodes. The FFEs for the downlink nodes however remain blank, since only the RNCs are aware of the exact location of a connected UE.

Likewise, when the first MBMS UE context is provisioned to an RNC for multicast bearer service, the RNC executes the registration procedure. After the registration the RNC obtains relevant bearer context information, including the static LSA information. In addition the RNC updates its FFE if required and may initiate the flow registration procedure as shown in figure 3.4. The required signalling and respective actions in the network nodes are described in the following in more detail:

1. Every time an MBMS UE context is provisioned to the RNC and if no entry exists, it updates the FFE for the NodeB serving the UE. MBMS UE context may be either provisioned via the MBMS UE linking procedure, or during a Serving RNC (SRNC) relocation. An update may also occur within the RNC when an connected UE moves to a cell of a different LSA, e.g., initiated by a cell update. The RNC then checks if the corresponding flow had been already registered with the SGSN. If not it sends a modified registration message, a so-called flow registration request (FRReq) message (IP multicast address, flow id), notifying the SGSN to start forwarding the indicated flow over the Iu bearer for the multicast bearer service. The SGSN updates the FFE of the respective RNC in its list of downlink nodes and sends a flow registration response (FRRes) back to the RNC.

2. The SGSN in turn checks if the flow has been already registered with the GGSN, e.g. on behalf of a previous request of another RNC. If not it sends an FRReq
3.3. Protocol extensions

message (IP multicast address, flow id) to the GGSN. The GGSN updates the FFE in the respective SGSN in the list of DL nodes in the bearer context and returns a FRRes message to the SGSN.

3. Finally the GGSN checks if the flow had been registered with the BMSC for a previous registration by an SGSN. If not the GGSN registers the flow with the BMSC by sending an FRReq message (IP multicast address, flow ID) to the BMSC. The BMSC updates the FFE entry of the respective GGSN and returns an FRRes message to the GGSN.

At the beginning of a session, QoS attributes are usually provided by the session start procedure for the different flows. Based on FFE information, each network node is able to compute the bandwidth parameters for the required flows. Appropriate core network (CN) bearer, In bearer and radio bearers (RB) can thus be established or modified as required during a session. Figure 3.5 shows the same flow for the deregistration process. The details of the procedures are described as follows:

1. As soon as the RNC detects that no UEs are present for a MBS under a NodeB it removes the appropriate flow entry from the FFE. When the last entry of a specific flow is removed from all DL node contexts (here NodeB context) the RNC sends a flow deregistration request message (FDReq) to the SGSN (IP multicast address, flow ID). The SGSN removes the flow id from the FFE of the respective RNC and then sends a deregistration response message (FDRes) to the RNC.

2. If no FFE in the list of DL nodes contains an entry of the flow, the SGSN sends a FDReq message (IP multicast address, flow ID) to the GGSN. The GGSN removes the flow from the list of DL nodes and then sends an FDRes message in return to the SGSN.
3.4 Evaluation

A layer 3 MBMS simulation model has been developed based on the simulation environment provided by OPNET Modeler [48]. The signalling procedures have been modelled according to the current MBMS specification [9] and considering the individual protocol specifications for RANAP [49], GTP [50], and Session Management (SM) [51] signalling. In addition the proposed extensions have been implemented. The flow registration and deregistration messages over the different interfaces have been defined the same format as the respective messages used for the regular MBMS registration and deregistration procedures, solely extended by an attribute to carry the flow identifier.

The simulation model included BM-SC, GGSN, two SGSNs, three RNCs per SGSN and 7 NodeBs per RNC. Each NodeB served exactly one cell. 1000 UEs have been uniformly distributed within the network.

For each multicast session 100 receivers have been selected according to a uniform distribution. The typical length of a session for the multicast user service was assumed to be 10 minutes. The values over 1000 consecutive sessions have been averaged for each run, and the mean over 10 independent runs with different seeds has been found to provide results with sufficiently small confidence interval for a confidence level of 95%.

The simulations have been performed for varying sizes of local service areas and mobility of receivers. To avoid unnecessary simulation complexity a simplified mobility model
was used, based on the random way-point model. Each UE stayed for a certain period in a cell, before it randomly selected an adjacent cell with equal probability for each cell. The sojourn time in a cell was determined by a uniform distribution, ranging for fast UEs between 50-75 seconds (Case A) and between 150-200 seconds for slow UEs (Case B). The required signalling load for the current approach, using separate MBS for each LSA (labelled MBMS) and the approach with the proposed extension, which allows the delivery of multiple flows via a single multicast bearer (labelled MBMS+) are compared in the following for the above described simulation scenarios. The signalling load analysis is limited to MBMS specific signalling, including the proposed extensions.

Figure 3.6(a) shows the MBMS related RANAP signalling load over the Lu interface between RNC and SGSN for both schemes as a function of LSA size. As expected the signalling load for mobility case A is higher, since the UEs change service areas more frequently. It can be observed that the proposed MBMS+ scheme reduces the required signalling load significantly for either mobility case. The more frequent receivers cross the boundaries between service areas, the larger are the signalling savings. The implications of higher flow registration signalling due to frequent changes of service area are more obvious for small LSA. With increasing LSA size, RNCs may service multiple cells of the same LSA. Registration or deregistration does not occur that frequently when an UE changes the LSA, since the RNC may still require the flow for another UE that has subscribed in one of those cells.

Figure 3.6(b) presents the MBMS related GTP signalling in the core network between the SGSN and GGSN. Also here the signalling savings of the proposed MBMS+ scheme are high for both mobility cases. Difference in signalling load among the two mobility cases for the proposed approach are only observed for very small LSA sizes. Flow registration signalling happens less frequently between GGSN and SGSN, since SGSNs cover multiple RNCs with the possibility of overlapping LSAs. Even if a RNC deregisters for a flow, another serving a cell within the LSA may still host UEs interested in the multicast service.

SM signalling takes place between SM entities in the SGSN and UE. Unlike GTP and RANAP signalling, which solely takes place within the network, SM signalling is carried over the air interface and is thus more crucial. Signalling for bearer establishment and release takes only place once in the proposed approach, since the UEs stay connected to same MBS for whole duration of the session. In contrast when using separate MBS, the signalling load increases significantly when LSAs are changed more frequently during a session, as shown in figure 3.6(c).

Finally the overall signalling load is shown figure 3.6(d). Noticeable in all curves shown is a slight variation of the signalling load for the current MBMS approach, especially visible at a LSA size of 8 and 10. This is due to unmatched alignment of LSA size and
3.4. Evaluation

Figure 3.6: MBMS related signalling for different sublayer protocols for services with higher popularity.

The flow registration and deregistration procedures are executed only if a user is the first user to enter a LSA for RNC/SGSN or a user is the last user to leave a RNC/SGSN. In a simulation with 100 receivers the chances are relatively high even for small LSA sizes, that there is continuously a receiver within a LSA. Therefore a second set of simulations have been performed with only 50 receivers interested in the multicast session. In such a scenario chances are higher that receivers enter a LSA with no previous receivers present or being the only receiver when leaving the LSA. Hence more signalling due to flow registration and deregistration is to be expected. Similar things apply to the registration and deregistration procedure in the conventional MBMS approach.

Figure 3.7(a) shows the RANAP signalling load. For large LSA sizes, registration and deregistration signalling for the current MBMS scheme do not happen so frequently.
3.4. Evaluation

Hence the overall signalling load is significantly lower for 50 receivers than for 100 receivers. However with decreasing LSA size, registration and deregistration procedures will be executed much more frequently. The increase in signalling load is clearly observable in the figure. Same applies for the proposed MBMS+ approach, where the signalling increase is to be attributed to the frequent execution of flow registration and deregistration procedures. However as expected the proposed MBMS+ approach still outperforms the current MBMS approach in both mobility cases.

The GTP signalling load increase is not as obvious for GTP signalling, due to the hierarchically higher positions of SGSN and GGSN. As shown in figure 3.7(b) a notable increase is observable only for very small LSA sizes.

The SM signalling load in contrast is not influenced by the presence of the number of UE in a LSA. As expected SM signalling load is just 50% for both approaches, as shown in figure 3.7(c), for half the number of UEs. For completeness figure 3.7(d) shows the

Figure 3.7: MBMS related signalling for different sublayer protocols for less popular services.
total signalling load for the scenario with 50 UEs.

\section*{3.5 Summary}

The proposed work extends the currently defined mechanisms in MBMS to allow the concurrent delivery of different versions of location based content using the same multicast bearer service. Forwarding of packets on the multicast bearer is not only based on the IP multicast address, but also on different flow labels which have been uniquely assigned to each location specific flow. For this reason the list of downlink nodes attribute in an MBMS bearer context has been enhanced by a flow forwarding entry for each node in the list. A flow registration procedure is introduced, which is responsible for updating and maintaining the flow forwarding entries in the network nodes. Furthermore static local service area information is carried as an additional attribute in the registration procedure.

The benefits of the approach are significant signalling savings, especially over the air interface, compared to the case where separate bearer services are utilised for the delivery of different location specific flows. Simulation results are presented to support the proposed extensions. Signalling savings increase with smaller size of local service areas and higher user mobility, since local service areas are more likely to be changed by users during a session. It has been also found that the overall signalling load is proportionally higher for services with low receiver popularity. This is due to more frequent flow registration and deregistrations. Flow registration and deregistration procedures are executed when a receiver is first one to enter or subscribe within a local service area. With popular services the chances of other users already being in a local service area are higher, hence the flow registrations and deregistration are rarely executed.
Chapter 4

Group Management Support

This chapter presents group management support (GMS), as a session layer approach to provide mechanisms for efficient multicast delivery coordination in a heterogeneous wireless network environment. Within the current IP multicast group management model, a multicast group is defined as a set of receivers with a common network layer association. A user initiates the reception of a flow of a multicast user service by subscribing to a specific IP multicast address in the network layer. The user not only selects the desired multicast user service, but also implicitly the multicast bearer service and the network for the delivery. Furthermore, an application for the multicast user service at the receiver, will maintain this association for the whole duration of a session.

In order to overcome the intrinsic lack of flexibility, a decoupling of multicast user service and its service flows from multicast bearer services in the networks is required. That way a session of a multicast user service can be dynamically instantiated in different service flows and network connections to reflect the heterogeneity of receivers and available access networks at their location. The proposed GMS therefore raises the abstraction of a multicast group above the network layer. Instead of directly subscribing to a multicast group on the network layer, receivers notify their interest in receiving a multicast user service by subscribing for the multicast user service to a network layer independent group. Mechanisms in the network can then select appropriate service flows for all users of that group and initiate the establishment of multicast bearer services in suitable networks. Furthermore, delivery networks and service flows may be changed even during a session.

The first section of this chapter gives an overview of the components of the multicast GMS and places it into the context of a network architecture. Then phases of a multicast service with the GMS are briefly described. In the subsequent sections, each component of GMS is described in detail. The chapter concludes with a demonstration.
4.1 Overview of the group management support

As discussed in section 1.1, knowledge of existing receiver and network heterogeneity is required, in order to effectively coordinate multicast service delivery in such a multi-access network environment. A decentralised approach for coordination, in which this information is kept local at the receivers, however, is very difficult to implement for several reasons. In order to implement an autonomous decision at each receiver, a receiver would require the knowledge of context information of all other receivers that are interested in the same multicast user service. Even if such a decision could be based on partial knowledge, e.g. a localised subset of the receivers, a substantial amount of signalling would be required to exchange such information on a peer-to-peer basis. Also the capability of storing such information at the receiver for popular multicast user services with large receiver groups is another concern, since memory availability is usually limited in mobile terminals. A further issue is privacy, since receivers would be forced to share their own context information, required for decision making, with other receivers of the same multicast user service. On the other hand decisions such as network selection have also to consider resource information of the networks. Often such information is not available at the receiver terminals. Furthermore, operators are reluctant to disclose to or share such information with the user.

As a consequence a network-centric approach seems to be a more natural choice, especially from the viewpoint of an operator, who owns the access network(s). A coordinating network entity in the network could easily access required network resource information for any decision making process. In addition it would allow operators to completely retain the control of the management of their own network resources and resource information. Advantages also exist for the access of user related context information. Some of the required user related context information is already existing in databases in the network. For example the UMTS network provides context information storage and update mechanisms regarding terminal information, location or user profiles. This user related context information can be easily accessed by the coordinating network entities, without the need to share information with other receivers. Since receiver and network knowledge are concentrated in the network, decision making can be centralised and thus is simpler to implement. Furthermore dedicated network entities do not undergo the same restrictions as a mobile terminal with respect to computational power, energy and memory availability.

The work presented therefore takes a network-centric approach and proposes a session
4.1. Overview of the group management support

layer GMS to achieve the multicast delivery coordination. Figure 4.1 depicts the GMS as part of an interworking architecture [52, 53] for next generation wireless networks.

The GMS is a functional part of so called interworking gateways (IGW), which each co-operating network operator deploys in its network. Besides the GMS, an IGW implements other essential interworking functions such as resource management (RM) [54], security or device presence system and defines a logical interface, which enables signalling message exchange for interworking purposes. The IGW ensures, that operators may interwork efficiently for service delivery, without the need to give up the own network autonomy or disclose any sensitive network related information. Besides functional components within the networks, the architectural framework also defines extensions for user terminals and interfaces between the IGW and these functions.

An overview of functional components of the GMS are given in figure 4.2. As depicted in the figure, GMS can be decomposed into three distinct components: a group manager (GM) at the network side, a multicast middleware (MM) in the user terminal and a multicast signalling channel (MSCH) for efficient communication between the GM and the MM in the terminal.

As mentioned above, the GM is part of the IGW, located in the network of each co-operating operator. It interacts with other gateway internal functional components components, e.g. the RM. Besides gateway internal interactions, a GM may also inter-
act with network entities located in its own network, or via a peer GM in the network of an interworking operator, in order to configure required bearer plane resources. Further a GM has access to user related context information and provides an interface for the content and service provider to configure service-related parameters. For each multicast user service a corresponding group entity exists at the GM. A group entity stores a list of interested receivers and service related parameters, such as information about offered service flows, parameters for data and control plane management and service specific policies.

At the terminal side, a MM is introduced in order to handle seamlessly changes of flows and multicast bearers during a multicast session. The MM is situated in the session layer of the OSI [55] model, below the application and above transport and network layers. No changes to the existing transport and network protocols or to the applications are required. The MM is responsible for managing required multicast bearer services at the user terminal transparently to the application, implementing the delivery coordination as indicated by the group manager. For this purpose a control plane has been introduced between the GM in the network and the MM in the terminal. The control plane is realised by a MSCH, in order to support scalable delivery of required control signalling from the GM to a potentially large group of receivers.

4.2 Service provisioning phases

Before going into detail about each functional component of GMS in the following sections, it is important to have an understanding of the different stages and the roles of the components during multicast service provisioning. Figure 4.3 therefore shows the different phases of service provisioning and the life cycle of a group in GMS. Some
of these phases take place before, others during or after a session of a multicast user service. The various phases are listed below and described in more detail:

**Group Creation** Before a service provider is able to provide a multicast user service, it has to create a group at the GM for that particular service. During this process a unique group identifier is created and assigned to the group. The service provider then configures service related parameters, such as service descriptions, offered service flows, utilised multicast address and port numbers etc. Part of this information is used for the configuration of service announcements.

**Service Announcement** During service announcement, users are able to learn about upcoming sessions of multicast user services. Service announcements provide the user with information required for subscription to a multicast user service and the establishment of the required control plane.

**Group Registration** Users that are interested in receiving a multicast user service register with GM, providing a unique user identifier, e.g. IMSI (International Mobile Subscriber Identity) and group identifier obtained from the service announcement. At the same time, the control signalling plane for that multicast user service is established. The GM adds the user to the group associated with the multicast user service.

**Session Establishment** The GM is triggered as soon as the service is scheduled to start and supported service flows and delivery networks have been selected for the receiver. Using the MSCH the GM initiates the establishment of required multicast bearers by notifying the MM at the registered receivers.

**Session Maintenance** This phase takes place during a multicast session. Based on context information change, e.g. users' location or resource conditions in network cells, GM may initiate vertical network handoff to a different access network for a subgroup of receivers.

**Session Termination** The multicast user service provider will usually indicate the termination of a session to the GM, when all the session data has been transferred. As a consequence GM will initiate the release of all multicast bearer services by triggering the MM at the subscribed receivers.

**Group Deregistration** Each receiver that has registered to the group for a multicast user service, can reverse this process by deregistering at any time of a session. This process is implicitly done, when the session terminates or when the group is deleted.
Group Deletion A service provider, who does not any more wish to provide a multicast user service, can delete the associated group on the GM. By this process all user and service related context for this group is released.

4.3 Context-aware group manager

The heart of the GMS is the context-aware GM, located in the IGW. The GM plays two significant roles in the provision of multicast services. Firstly, it accumulates and maintains knowledge of currently interested multicast receivers for a multicast service and assists the RM in its decisions making by providing relevant context information of users for a multicast service and other service related information. Secondly, it provides necessary session management functionality for delivery coordination by executing the resource management decisions. This includes mechanisms for network-initiated bearer establishment and release for groups of receivers, independent of the selected access networks. Other session management tasks include the execution of vertical network handoff and flow handoff for groups of receivers whenever required during a multicast session.

The GM has been logically separated into three functional blocks. As shown in figure 4.2, the GM consists of a Group Membership Management Function (GMMF), a Session Control Function (SCF) and a Network Management Function (NMF). The
following subsections describe each functional component in more detail.

4.3.1 Group membership management function

The GMMF is concerned with the collection and maintenance of the group membership for a multicast user service. It provides a set of functional primitives that allows the creation and management of groups and specification of service related parameters. The functional primitives can be separated into primitives used by service providers to configure a multicast user service at the GM and primitives used by the mobile users to register their interest for a particular service. Main primitives offered to provider of a multicast user service are:

- Create Group
- Delete Group
- Configure Service Parameters.

Furthermore the basic set of primitives provided to mobile users are:

- Subscribe to Group
- Unsubscribe from Group.

Before a multicast user service can be provisioned, an initial service setup at the GM is required. This includes the creation of a group entity for the multicast user service in a group management database and the configuration of service related parameters. A group entity holds information for a multicast user service. Besides a unique group identifier, it stores a list of interested receivers, which is initially empty. For each service flow communication parameters need to be specified. The parameters include at least the multicast group address and the port number, on which the respective flow will be sent. Furthermore the multicast group address and port number of the MSCH need to be configured. After a successful service configuration, the service is announced to the mobile users. Announcements can be realised in various ways, e.g. on a service portal website, electronic program guide, or via service announcement channels using the Session Announcement Protocol (SAP) [56].

After learning about an upcoming session of an interesting multicast user service, users can subscribe for that service with the GMMF. The subscription process can take place via a service portal website, or via dedicated signalling between user and GMMF. The GMMF identifies the group entity for the multicast user service and adds the user to
the list of interested receivers. In addition, relevant context information of the new subscriber is retrieved from respective context information databases in the network and stored for later use. For on demand services, the GMMF also notifies the RM to trigger batching algorithms, in order to determine the optimum service scheduling time. The GMMF also informs the RM of any user context information change. Users are also able to deregister from a group at any time. Deregistration happens implicitly after a service session has terminated.

The physical realisation of the group management database depends on the scalability requirements applicable. In MBMS for example, the Broadcast Multicast Service Centre (BMSC) stores context for every group member using the UMTS network for MBMS services [9]. While a centralised database may be sufficient for services with low or medium popularity, a distributed architecture may be required to handle the demand for highly popular services. Furthermore, several GMs can be deployed in an operator’s network, each of them hosting a different subset of offered multicast user services.

4.3.2 Session control function

The SCF provides the session management functionality required for the multicast delivery coordination. It realises the control plane mechanisms between the GM and MM of the receivers subscribed to a multicast user service. The SCF thus allows the management of multicast bearer services, regardless of the underlying access network technologies. It achieves this by providing session layer mechanisms, which trigger the required network layer services of the respective access networks.

Different scenarios that involve the delivery of multicast user services to receiver groups in an heterogeneous wireless network environment have been investigated in [57]. The scenarios have been analysed to identify required group management functionality and control signalling necessary for the coordination of multicast delivery. In most of the cases signalling information has to be provided to a group of receivers simultaneously. Some of the scenarios revealed similar functional requirements, this led to the identification of mechanisms for three main signalling purposes. The required signalling mechanisms are summarised and their purpose briefly explained as follows:

Network-initiated establishment of multicast bearers: In order to allow advanced interworking functionality such as dynamic access network and bearer selection, network operators need a way to initiate the establishment of suitable multicast bearers. Resource management algorithms [58] select suitable bearer paths, e.g. according to receiver preference, the availability of current network resources or
terminal capabilities and then trigger the establishment of those for the interested receivers.

**Vertical network handoff for groups of receivers:** During a multicast session conditions may arise where a change of current access network may be required. An example of a network initiated vertical handoff would be a load balancing situation: In order to save own network resources, resource management functionality may decide to handover a group of receivers in several cells of an access network to an alternative network of an interworking operator with different access network technology. Thus signalling has to be delivered to the respective receivers in order to initiate a change of the delivery network.

**Flow handoff for groups of receivers:** Often a change of an access network may lead to a change of the delivery characteristics e.g. bandwidth availability. In such cases the flow within a multicast session may change, e.g., the change to a different QoS \(^1\) of a media flow or the addition/removal of media flows. Furthermore, to increase the delivery flexibility, e.g. in an emergency situation, receivers may be temporarily downgraded to a lower rate flow in order to free up network resources, or may be upgraded if sufficient network resources are available.

Three elementary messages have been defined for the control plane to implement the identified session management functionality, namely **ESTABLISH**, **RELEASE** and **MIGRATE**. These control messages represent instructions that are sent by the SCF to affected receivers of a multicast user service. The purpose of the messages is described below. Details of message formats are given in the description of the MSCS in section 4.4.

- **ESTABLISH**: This message initiates the establishment of multicast bearer services. With the **ESTABLISH** message, the SCF instructs the MM in the terminal to start receiving one or more flows on the indicated multicast bearer on particular access networks.

- **RELEASE**: This message initiates the release of one or more multicast bearer services. The **RELEASE** message is used by the SCF to indicate the MM to stop listening to one or more service flows and release the identified multicast bearers.

- **MIGRATE**: The **MIGRATE** message is used for implementing a vertical network handoff and/or flow handoff. The SCF instructs the MM in the receiver terminal to migrate from a currently established multicast bearer service to another multicast bearer services on the same or an alternative access network.

\(^1\)With QoS we refer to the required bandwidth of a flow
4.4 Multicast signalling channel

Actions of the SCF are triggered by the RM [58]. Once the scheduling function in
the RM determines a time for the session start for a multicast user, algorithms in the
RM select appropriate service flows and delivery networks for the group of registered
receivers. The RM notifies the SCF in the GM about its decisions and initiates the
establishment of appropriate multicast bearers in the selected networks. Likewise, once
a session terminates, the RM triggers the SCF to initiate the release of the established
bearer plane resources. Furthermore during a session, optimisation algorithms in the
RM may decide to move a subset of receivers to an alternative access network by
triggering the SCF to initiate a vertical network handoff for the receiver subset.

4.3.3 Network management function

While the SCF is concerned with the implementation of the required control plane
towards the receivers, the NMF deals with the network-side configurations, which may
be required for multicast bearer management on the network side. MBMS for instance
requires the configuration of multicast bearer service parameters at the BMSC, before
multicast bearer services can be established. The NMF provides the required parameters
to the BMSC, before the SCF triggers the establishment of the respective services
at the receiver. Likewise, DVB-T/H networks may require configuration, when the
UDLR [27] protocol is not utilised. The NMF could configure IP/DVB gateways or
gateway managers in cells with receivers including supporting functionality such as
IGMP proxies to establish multicast bearer services for selected service flows. Final
details of NMF signalling cannot be provided at this stage, since the interfaces of rele­
vant standards are still under development. On the other hand technologies belonging
to the 802.x such as Ethernet, WLAN or WiMax do not require such configuration, if
the access routers are IP multicast enabled. The mechanisms initiated by the SCF at
the receiver are sufficient for required multicast bearer management.

4.4 Multicast signalling channel

The introduction of a control plane for coordination of multicast data delivery will
require signalling message transport between the GM and the MM in the terminals of
interested receivers. Two major issues arise from the provision of such control signalling.
Firstly, the control signalling targets a potentially large group of receivers. Therefore
delivery of such signalling has to be scalable, in order to keep the signalling load of the
additional control plane as low as possible. Secondly, the signalling should be carried
independently of underlying access networks in order to satisfy a vastly heterogeneous
set of receivers.
Scenario based analysis has revealed that control signalling will often target a larger subset of receivers [59]. As a consequence the use of a MSCH for efficient communication between the GM and MM in the receiver terminals has been investigated. Instead of delivering a signalling message via unicast, individually to all affected receivers, a single message is sent to a specific multicast group address, identifying the MSCH. Receivers, which need to receive the signalling message subscribe to the multicast group address of the MSCH over which the message is sent. Using the multicast capabilities of underlying IP layer, the MSCH is independent of the access network technology used for its provision.

Ideally only receivers, for which a control signalling message is intended, should be subscribed to the MSCH at the time the signalling message is sent. While this concept may work perfectly in theory, it exhibits some practical problems. In most cases a control message will not be intended for all receivers of a multicast user service. Rather a signalling message, such as a request for vertical handoff would target a subset of receivers, e.g. only those receivers capable of using a multicast bearer in the new access network. This would require a way to inform the receivers to subscribe or unsubscribe from the MSCH, whenever a new message needs to be sent. While such notification will add to the required signalling load, frequent 'join' and 'leave' of receivers will further increase the signalling load, thus reducing the foreseen benefits of the MSCH.

It is therefore more realistic to assume that receivers of a particular multicast service are subscribed to the MSCH for the lifetime of the session. Within the MSCH an addressing expression is used in addition to the signalling message as shown in figure 4.4. The addressing expression allows identifying of the subset of receivers, for which the signalling message is actually intended. The MM in the receiver terminals evaluates the addressing expression, and based on the outcome of the assessment, accepts or silently discards the signalling message.

In order to minimise the required addressing expression and hence the signalling load on the MSCH, a receiver aggregation mechanism has been proposed that is based on common receiver context information. Details of this mechanism are presented in subsection 4.4.1. The structure of a message on the MSCH is described in subsection 4.4.2. An analytical evaluation of the MSCH is later given in chapter 7.
4.4. Multicast signalling channel

4.4.1 Context information based receiver subset addressing

A natural way of addressing the receivers is by explicitly encoding a list of identifiers within the message. Every receiver can then check if its own identifier is part of the message and based on this decide to further process or discard the message. Similar to Xcast [60], the unicast address of receivers can be used. The use of explicit encoding of the receivers unicast address has two main problems.

Firstly, in a heterogeneous network environment, hosts may have multiple network interfaces accessing different access networks of different domains. Thus such a multi-homed terminal may have several IP unicast addresses, which need to be known by the GM. Then the identifier of the network on which the user has established the MSCH should be used. Furthermore, the utilised address should be statically configured or at least known before and consistent during the multicast session. Another option would be the use of a unique personal identifier, such as host identity [61] for the user instead. This identifier should be consistent and independent of any network address.

The second and by far more critical problem is the scalability of the approach. As long as the subset of receivers is small, it may not be very expensive to explicitly list each IP unicast address. Taking a IPv4 unicast address with the size if 32 bit as an example, a message targeted at a subgroup of 10 receivers will require 320 bytes of addressing information. However if 10,000 receivers need to be addressed, the required addressing information for a single message would take up 320 kByte, which by far exceeds any reasonable limit. For the 128 bit long IPv6 addresses this problem becomes even more severe.

Analysing the signalling application scenarios, the following important observation has been made: In many cases the control signalling targets a group of users with common context e.g. all receivers in a certain area/cells of a network or all receivers currently receiving a flow with the same quality of service. This has motivated the proposition of a receiver aggregation mechanism for the MSCH that is based on receiver context information. A subset of receivers on the MSCH is described by context information that those receivers have in common. The requirement for such a mechanism to work is that the network entity, sending the control messages via the MSCH has access to the context information of these receivers. Moreover, receivers need to evaluate the specification of the context information provided in the addressing expression and be able to infer whether or not the specification applies to them. Useful context information, which can be used for such address aggregation has been identified and is described as follows:

**Receiver location:** Often control signalling will target a set of receivers at a geographical location. Geographical locations can be described logically by specify-
4.4. Multicast signalling channel

Multicast signalling channel and cells or by GPS information. For example, load balancing will try to free up resources in a cell or cell cluster of a network by switching the multicast bearer to another access network with more available resources. Users in a cell cluster could be easily aggregated by an expression such as 'all receivers in cells 4,5,6,7 of a UMTS network'.

**Terminal capabilities**: Terminal capabilities are attributes that can be useful to express commonness among users. Terminal capabilities include available network access interfaces (NAI), maximum supported QoS for a connection on a NAI, available memory, software and codecs, etc. A control message initiating a vertical handoff could move all receivers with an appropriate NAI to a different access network. An expression such as 'all receivers with NAI type UMTS' represents a short but powerful aggregation for such a use case.

**Receiver preference**: As with terminal capabilities, receiver preferences are attributes, which can be used to identify a subset of receivers. Preferences can be expressed in 'delivery network' or the 'QoS' for the service flows. A control message using preferred access network as a receiver aggregation could initiate the establishment of a multicast bearer service on the respective access network for all receivers, which have their preferences in common.

**Communication context**: Communication context describes the multicast bearers and flows of a receiver that are currently associated with the reception of a multicast service. Communication context can be described by delivery network, multicast group address, source address, QoS of received flows and source and destination ports. Receivers are aware of their communication context and the information can be used to efficiently aggregate receivers, e.g., receivers subscribed to a common multicast bearer or receiving the same service flow. Note that unlike the previously mentioned context information, communication context does not exist before a communication is established. Therefore, communication context can only be used for addressing expressions of control messages, which are sent during a session.

**Network operator**: Commonness among receivers can be also expressed by identifying the network operator to which they belong. A network operator may want to return a set of customers to its own network after temporarily load balancing them to an cooperating network operator. A subset of receivers can thus be easily specified as 'all receivers belonging to network operator Vodafone'.

This list of context information can be easily extended as new useful context information for aggregation becomes available. Within the addressing expression, context
information is expressed as a key-value pair, with the type of context being the key, and a context attribute representing the value. Context attributes can be further decomposed into attribute-types and associated attribute-values. For example the context type 'location' can be expressed by attribute types 'network' and 'cell', with 'UMTS' and '7,8,9' being examples of the respective attribute-values. Two or more context type expressions can be combined by logical operators to characterise a receiver subset more specifically. Higher flexibility can be further achieved by nesting of such expressions. An example of a nested expression is given as follows:

{ ['Location':(['Network':'UMTS'] & ['Cells':'6,7,8'])] & ['Interface':'DVB'] }.

The expression describes all receivers with a DVB network interface present in cells 6, 7 and 8 of a UMTS network. In a load balancing scenario a control message with this addressing expression could thus initiate a vertical handoff to a DVB network to free up resources in cells 7,8,9 of the UMTS network. As demonstrated in the example, a receiver subset can be accurately identified with a relatively short expression, instead of using hundreds or more explicit addresses.

In some cases a receiver subset cannot be unambiguously described by a combination of the above described context attributes. In such cases explicit addressing can be used complementary, in order to achieve the required granularity. An example of such an hybrid addressing expression using a combination of context information based and explicit addressing is given as follows, describing all receivers with a WLAN network interface, except receivers A and B:

{ ['Interface':'WLAN'] \ ['Explicit':['IPAddress':'A,B']] }.

4.4.2 Message format on the multicast signalling channel

A common way to exchange context information between applications is by serialising the context information into a presentation based on markup languages such as the Extensible Markup Language (XML) [62]. XML allows the presentation even of complex context information expressions by providing a hierarchical data structure consisting of markup tags with attributes and contents. Context types attributes and values are defined an XML schema, which specifies utilised name spaces and data type definitions. According to this schema, applications can encode relevant context information into an XML instance before sending it to another application. Following the XML schema, the application on the other end is able to decode the received XML instance into an appropriate context representation, regardless of the platform. Besides platform independence, XML is easily extensible. New context information types and attributes can be added at a later stage by simply modifying the XML schema. Furthermore the
### 4.4. Multicast signalling channel

<table>
<thead>
<tr>
<th>Context Information Type</th>
<th>Attribute Type</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Network</td>
<td>DVB</td>
</tr>
<tr>
<td>Cell</td>
<td></td>
<td>1,2,5</td>
</tr>
<tr>
<td>GPS</td>
<td></td>
<td>N49° 00' 32&quot; ...</td>
</tr>
<tr>
<td>Terminal Capabilities</td>
<td>Network Interface</td>
<td>UMTS,DVB</td>
</tr>
<tr>
<td></td>
<td>Supported QoS</td>
<td>256k</td>
</tr>
<tr>
<td>Service Preferences</td>
<td>Delivery Network</td>
<td>WLAN</td>
</tr>
<tr>
<td></td>
<td>Desired QoS</td>
<td>384k</td>
</tr>
<tr>
<td>Communication Context</td>
<td>Delivery Network</td>
<td>WLAN</td>
</tr>
<tr>
<td></td>
<td>Current QoS</td>
<td>384k</td>
</tr>
<tr>
<td></td>
<td>Multicast Addr</td>
<td>239.27.0.8</td>
</tr>
<tr>
<td></td>
<td>Source Addr</td>
<td>123.44.32.2</td>
</tr>
<tr>
<td></td>
<td>Port</td>
<td>1500</td>
</tr>
<tr>
<td>Explicit Addressing</td>
<td>IP Address</td>
<td>89.112.11.10</td>
</tr>
<tr>
<td></td>
<td>Host Identity</td>
<td>128 bit hash</td>
</tr>
<tr>
<td></td>
<td>User Identity</td>
<td>IMSI</td>
</tr>
<tr>
<td>Network Operator</td>
<td>Operator Name</td>
<td>Vodafone</td>
</tr>
</tbody>
</table>

Table 4.1: Context information types, associated attribute types and example values.

A human readable format of XML simplifies the development process and initial demonstrations.

Although proposals have been made [63] to introduce a common description language for context information, no such implementation yet exists. Rather each application framework uses its own description tailored to its specific needs [64, 65, 66, 67, 68]. Likewise a suitable XML schema for the context information identified in the previous subsection has been made for the MSCH. Table 4.4.2 shows an overview of the specified context types, associated attribute-types and examples typical attribute values.

An addressing expression can either consist of attributes of one of the defined context types terminal capabilities, namely communication context, location, user preference or explicit addressing type. Furthermore an addressing expression can also be a nested expression or a combination of any expression, including the defined context types or further nested expressions, with logical operators. The corresponding XML schema is shown in figure 4.5.

In order to keep a consistent format on the MSCH, the XML schema was extended to also include the message body of the signalling payload. Figure 4.6 shows the XML schema of the message on the MSCH. Any message transmitted on the MSCH, has to
4.4. Multicast signalling channel

Figure 4.5: XML schema for addressing expression on MSCH.
4.5 Multicast middleware

The GMS on the user terminal is realised by a MM, which resides directly underneath the application layer. The purpose of the MM is to reveal changes to the underlying multicast bearer services throughout the lifetime of a multicast session. Subsequent sections present the principles of the MM, then details of the internal design are conform to the depicted format.

As shown in figure 4.7, the message body itself consists of a message type, which is represented by string enumerators ESTABLISH, RELEASE and MIGRATE. The first two message types consist of one further information element. The information elements contain as parameters the IP multicast address, port number and signalling network of the multicast bearer to be established/released. For the MIGRATE message, two information elements need to be specified. The first one identifies the old and the second one the new parameters of the multicast bearer to be utilised.

4.5 Multicast middleware

The GMS on the user terminal is realised by a MM, which resides directly underneath the application layer. The purpose of the MM is to reveal changes to the underlying multicast bearer services throughout the lifetime of a multicast session. Subsequent sections present the principles of the MM, then details of the internal design are
4.5. Multicast middleware

Applications usually initiate the establishment and release of multicast bearers by creation or deletion of transport protocol end points, named sockets. The concept of sockets have been initially introduced in BSD-4.1c standard of Unix to enable inter-process communication between two applications that can be located on separate systems interconnected via a computer network. A socket corresponds to a transport protocol end point, usually identified by 3-tuple \(<\text{protocol}, \text{local-address}, \text{local-port}>\) or \(<\text{protocol}, \text{remote-address}, \text{remote-port}>\). BSD provides a socket application program interface (API), offering a basic set of function calls for sending and receiving data. Today sockets have been included into most modern operating systems such as Microsoft Windows, almost all Unix and Linux derivations or Apple's MacOS. In the following, a socket that is directly used for communication across a computer network will also be referred to as a network socket.

As a transport protocol, IP multicast applications usually utilise UDP \(^2\). In order to receive IP multicast data, an application is required to perform the following steps [69]:

1. Create a socket for the UDP transport protocol.
2. Bind to the socket by specifying a local address and local port.
3. Join a multicast group on a network interface.

Likewise in order to stop receiving IP multicast data, an application requires to:

1. Leave the multicast group on the network interface.
2. Close the socket.

The MM presents the application with a virtual socket, which is dynamically mapped to a transient network socket. The virtual socket remains the same for the application for the whole duration of a session. The MM creates and destroys network sockets in order to establish or release required multicast bearer services as directed by the GM. Changes of underlying multicast bearer services are executed seamlessly and thus remain transparent to the application for the whole duration of a session. The advantage

\(^2\)Some applications also use reliable multicast protocols, which in turn are implemented on top of UDP
of using a middleware at the session layer of the OSI model is that all necessary extensions can be implemented at the user-level, thus leaving the Internet protocol stack in the kernel space unchanged. The disadvantage is an increased processing overhead by the additional middleware layer.

The basic concepts are depicted in figure 4.8. An application that attempts to receive multicast data usually creates a network socket and associates the socket to multicast group and a particular interface. Any changes of underlying multicast bearers, e.g. change of interface or multicast group, would also require the application to directly modify the respective socket associations. Thus each application would need to be specifically written to implement the required handling. An application using the MM in contrast does not directly associate a socket to a particular network interface and multicast group. Instead the MM creates a socket pair and connects one end to the application. It then creates a network socket associated with the multicast group and interface as directed by the GM. Data received on the network socket is then delivered to the application via the socket pair.

4.5.2 Design overview

The behaviour of the MM at the user terminal is best described by a state transition diagram, as depicted in figure 4.9. With regard to a particular multicast service, the MM can be in four different states:

**IDLE:** Within this state the MM has no association with a particular multicast service. It is the initial state of the MM. No MSCH as well as multicast bearers for the data plane exist at this state. The MM is not reachable for any control messages sent by the GM to a particular multicast service.
4.5. Multicast middleware

**MSCH IDLE:** The MM is in this state when a user has registered with a multicast service and a multicast bearer for the MSCH has been established. No multicast bearers for the data plane are existing. The only association the MM has with the multicast service is via the established MSCH. The MM is ready to receive control messages from the GM, sent to the registered multicast service receivers.

**MSCH ESTABLISHED:** As in the MSCH idle state the MSCH is subscribed to the multicast bearer of the MSCH. The MM is able to receive and act on control messages, sent by the GM. In addition a multicast bearer for the data plane has been established. Incoming service data is forwarded to the application for the multicast service. The MM will spend most of the time in this state during an active multicast service session.

**MSCH MIGRATING:** The MM is in this state during an ongoing vertical network handoff or flow handoff. Multicast bearer for the MSCH as well as for the data plane have been established. In addition a new bearer has been created on a new access network in case of a vertical network handoff or for a new flow in case of a flow handoff. Compared to the MSCH ESTABLISHED state, only little time is usually spent in this state during an active multicast service session.

A transition from one state to another is triggered by several significant events. Events will only cause transitions and associated actions if they occur in the correct states as depicted in the state transition diagram. Default action for events received in an unexpected state is to silently ignore those. In the following a list of events is provided with details of their cause:

**Join MSCH:** This event occurs, if the user application triggers the establishment of the MSCH for a multicast service by joining the multicast group of the MSCH obtained from the service announcement. During transition action A1 is executed.

**Leave MSCH/Close socket:** This event occurs, if a user triggers the release of the MSCH by either leaving the multicast group of the MSCH on the application socket, or by closing the application. Depending on the starting state, either Action A2 or A8 are executed on transition.

**ESTABLISH:** The event is triggered by the reception of a correct ESTABLISH message from the GM over the MSCH and the successful evaluation of the addressing expression of the message. The MM executes action A3 on transition.

**RELEASE:** The event is triggered by the correct reception of a RELEASE message from the GM over the MSCH and the successful evaluation of the addressing expression.
expression of the message. Depending on the starting state either action A4 or A7 are executed.

**MIGRATE:** The event is triggered by the correct reception of a MIGRATE message from the GM over the MSCH and the successful evaluation of the addressing expression of the message. Action A5 is executed on transition.

**Data arrival on new bearer:** This event occurs as soon as the first packet arrives on the new bearer during a migration process. The MM executes action A6 on transition.

Finally the executed action during state transitions are briefly described as follows:

**A1:** Establish multicast bearer service for MSCH.

**A2:** Release multicast bearer service for MSCH.
A3: Establish multicast bearer service for data plane.
A4: Release multicast bearer service for data plane.
A5: Establish additional multicast bearer service for new data plane.
A6: Tear down multicast bearer service of old data plane.
A7: Tear down all multicast bearer services of the data plane.
A8: Tear down all multicast bearer services for data plane including the one for the MSCH.

4.5.3 Operational example

Figure 4.10 explains the operation of multicast service delivery for applications using the MM on an session example. The application initially learns the multicast group address of an interested multicast user service via some form of service announcement. It then creates a socket and associates the socket with an interface and multicast group address. As shown in figure 4.10(a), the MM intercepts the socket calls and returns a virtual socket to the application. At the same time the MM establishes a network socket with the parameters provided by initial API call. This network socket establishes the multicast bearer service for the MSCH. Thus the information provided by the service announcement identifies the parameters required for the MSCH. Data arriving at this socket is interpreted as control messages by the MM and are never passed to the application.

After an establishment request has been received from the GM on the MSCH, the MM creates a new network socket, this time for the data plane, with the parameters indicated by the ESTABLISH message. Data arriving on this socket is assumed to be multicast service data and is passed to the application as shown in figure 4.10(b).

Figure 4.10(c) shows the case during a vertical network handoff. After receiving a MIGRATE message from the MSCH, the MM creates a new network socket associated with the new network interface, initiating the establishment of a multicast bearer service on the new access network. As soon as service data is received from the new network socket, the MM starts passing data from the new network socket to the application. At the same time, the previous socket is closed and old bearer service released, as shown in figure 4.10(d). This way a vertical network handoff can be executed seamlessly to the application.

The MM processes all control messages received on the MSCH. Before acting on a control message, the MM first evaluates the context information based addressing expression. The context expression is compared to the current context information, while
4.5. Multicast middleware

Figure 4.10: Example of a session setup and vertical handoff using the MM.
applying the specified logical operators. If the evaluation is successful, the message body of the control message is further processed and appropriate actions are taken. If the evaluation fails, the addressing control signalling message is silently discarded.

It should be noted that the current implementation only allows a change of interface for the data plane. The MSCH, once established on an interface, stays on the same interface for the whole duration of a session.

4.6 Service example of a multicast session

This section briefly presents a service example, showing how the functional components of the QMS interact to achieve multicast delivery coordination.

A provider of a multicast user service, e.g. network operator, uses the service primitives provided by the GMMF to configure the service at the GM. This step involves the creation of a group for the multicast user service and configuration of parameters for the MSCH and offered service flows. After the multicast user service has been configured, service announcements are created with relevant service information and parameters required for initiation to advertise the service to the users, e.g. announcement on a website.

Figure 4.11 shows a signalling flow example for session setup. Users learn about a service session, e.g. by visiting a portal website, and if interested register for a multicast user service with the GMMF by providing the group ID for the service and a user identifier. The GMMF adds the user to the group membership database of the service and obtains relevant context information of the user. In case of an on-demand service, batching and scheduling algorithms in the RM [58] are informed of the new user registration. The user also obtains the Multicast Group Address (MGA) of the MSCH for the service and possible signalling networks from the service announcement and provides this to the MM. The MM initiates the establishment of the multicast bearer service for the MSCH by sending an IGMP join message to the access router (AR) of the signalling network. An AR can be either a multicast enabled router behind a WLAN access point or a GGSN in case of UMTS network. In some cases IGMP signalling itself may not be sufficient for multicast bearer establishment. An UMTS network for example executes in an addition to IGMP signalling an MBMS multicast service activation procedure in order to establish a multicast bearer.

Once the service session is scheduled to start, the RM selects suitable service flows and delivery networks for the interested group of receivers and triggers the SCF to initiated the establishment of the required multicast bearers for the data plane. The SCF determines the receiver subsets for the selected flows and delivery networks. It then
4.6. Service example of a multicast session

Figure 4.11: Signalling diagram of a typical session setup for a multicast user service using the GMS.

sends an appropriate ESTABLISH request for the identified receiver subsets, providing MGA and other parameters required to establish the data plane for the session. The MM in the user terminals then joins the multicast group on identified networks, to establish required bearer services and begins forwarding incoming service data to the application.

Figure 4.12 depicts an example of a vertical network handoff for a receiver group, which can happen for, e.g., load balancing reasons. The RM reacts on resource conditions in the network and triggers the SCF to perform a vertical network handoff, balancing a subgroup of receivers in parts of the network to an alternative access network. The SCF identifies the target receiver subset and sends a MIGRATE message on the MSCH. The message identifies the MGA of the multicast bearer service, the old access network from which and the new access network to which the bearer is migrated. The MM at the identified receiver terminals executes the command by sending IGMP join request to the new access network to establish a multicast bearer service. Once data is received on the new bearer, it sends a IGMP leave request to the old network. As a consequence the previous multicast bearer service is released.
4.7 Summary

This chapter presented a GMS as a session layer solution to achieve multicast delivery coordination in a heterogeneous wireless network environment.

In the current multicast service model, users interested in receiving data of a multicast service, subscribe to a multicast group address on a particular network interface. Thus a user not only selects the desired multicast service, but also implicitly the multicast bearer service and the network for the delivery. Furthermore an application for the multicast service at the receiver will usually maintain this association for the whole duration of a session. In order to overcome this lack of flexibility, a decoupling of the multicast user service and its service flows from multicast bearer services in the networks is required. The GMS provides necessary mechanisms to achieve the required decoupling. Instead of directly subscribing to a multicast group on the network layer, receivers notify their interest in receiving a multicast user service by subscribing to a network layer independent group at the group manager for that multicast user service. Considering resource management decisions, a session of a multicast service can thus be dynamically instantiated in different service flows and network connections to reflect the heterogeneity of receivers and available access networks at their location.

The GMS is realised by a GM as part of an interworking gateway in the network and a MM in the terminal. The GM plays two significant roles in the provision of multicast services. Firstly it accumulates and maintains knowledge of currently interested multicast receivers for a multicast service and assists resource management functionality in its decisions making, by providing relevant context information of users for a multicast
service and other service related information. Secondly, it provides necessary session management functionality for delivery coordination, by executing the resource management decisions. This includes mechanisms for network-initiated bearer establishment and release for groups of receivers, independent of the selected access networks. Other session management tasks include the execution of vertical network handoff and flow handoff for groups of receivers whenever required during a multicast session.

The MM is introduced on the terminal side in order to handle seamlessly changes of flows and multicast bearers during a multicast session. The MM is situated in the session layer of the OSI model, below the application and above transport and network layers. No changes to the existing transport and network protocols or to the applications are required. The MM is responsible for managing required multicast bearer services at the user terminal transparently to the application, implementing the delivery coordination as indicated by the group manager. For this purpose a control plane has been introduced between the GM in the network and the MM in the terminal.

In order to support scalable delivery of required control signalling from the GM to a potentially large group of receivers, a MSCH is proposed. The MSCH is common to all receivers of a particular multicast service. Efficient addressing of a receiver subset on the MSCH are achieved by a novel a receiver aggregation mechanism based on common receiver context information.
Chapter 5

IGMP Extensions

The previous chapter has presented an approach for multicast delivery coordination that does not require any modifications to multicast related mechanisms and protocols. Coordinated multicast delivery is achieved by an additional session layer and network support on top of existing multicast protocols. Instead of adding additional functionality on top of existing ones, this chapter explores how existing multicast mechanisms can be adapted to provide the required delivery coordination in an heterogeneous wireless network environment.

The availability of multiple access networks together with the existence of multiple network interfaces at the host provides new opportunities as well as challenges for both multicast receivers and network operators. Unfortunately the characteristics of such a network environment are not adequately reflected by the current IP multicast group management model. The presented work aims therefore to adapt the group management model to consider multihomed capabilities if available and leverage them to the advantage of both network operators and receiving hosts. In particular extensions to the current Internet group management protocol (IGMP) [6] are presented as a network layer approach to implement the required delivery coordination.

Section 5.1 gives first an overview of the operation of the IGMP protocol. Then section 5.2 motivates the extension of IGMP to consider multihomed capabilities of a host and introduces the main features of the proposed solution. Since multiple versions of IGMP exist, the most commonly used version, IGMPv2 [21], has been chosen as an example throughout this chapter. The proposed principles, however, are also applicable to the other versions and are easily transferable with minor adjustments to the respective features of the version. The presented solution requires modifications on both router and host side implementations of IGMP and section 5.3 describes the design principles they are based on. Then the router side extensions are specified in
section 5.4. A description of the host side extension is given in section 5.5. An example demonstrates the new protocol features in section 5.6, while section 5.7 summarises this chapter.

5.1 Introduction to IGMP

IGMP is an integral part of IP and is required to be implemented by every host that wishes to receive IP multicast traffic. A host uses IGMP to inform a multicast enabled router, located on its local subnet, of its interest in receiving IP traffic sent to particular multicast groups. Routers provide this group membership information to multicast routing protocols for the establishment of multicast delivery paths, used to forward the IP traffic efficiently to the interested receivers.

IGMPv2 messages are 8 octets long and are directly encapsulated in IP datagrams, with an IP protocol number of 2. Since IGMP messages should only reach routers directly attached to the local subnet, the IP datagrams are sent with a Time To Live (TTL) value set to 1. Furthermore, the router alert option is set in the IP header.

IGMP is based on a query-reply mechanism, where routers periodically query hosts for interested group membership using group membership queries, and hosts reply with the interested group membership using group membership reports. The interval between two periodic queries can be configured but is typically 125 seconds. Besides periodic queries, which are also referred to as general queries, so-called group specific queries exist. While general queries can invoke membership reports for any multicast group, group specific queries only aim to obtain group membership information for a particular multicast group.

The router maintains a separate list of multicast group memberships on the subnet attached to each enabled interface, which is updated by the incoming membership reports. Multicast routing protocol deliver traffic for interested multicast groups to the router and the router forwards the traffic via interfaces where respective group memberships have been collected. If after a group membership query no membership report for an initially listed multicast group is received, the group membership is considered obsolete and removed from the list and respective multicast traffic is not further forwarded on the interface. In order to minimise the state required at the router, only interested multicast groups at an interface need to be maintained within the router. Thus routers are usually unaware of which host or how many hosts on a subnet are interested in receiving multicast traffic. Explicit membership traffic is however optional.

The length of the periodic query interval may lead to delays detecting the appearance or ceasing of interest for group memberships at hosts in a particular subnet. As a
5.1. Introduction to IGMP

Figure 5.1: Example of IGMPv2 operations.

consequence, hosts may have to wait to receive traffic for a desired multicast group or traffic may be unnecessarily forwarded in a subnet for a period of time. In order to speed up the join process, users can send unsolicited membership reports to inform the router immediately of a multicast group membership. Likewise hosts that end their interest in multicast groups can send a leave message for that group to their multicast router. Routers then send a group specific query to determine if any other host is still interested in that multicast group, before removing the entry from the membership list of an interface.

Within a host multicast group membership is specific to a particular network interface. Applications on the host side use the socket interface to advertise their interest or cease of interest for a particular multicast group to the IP networking stack. Using respective socket options, applications specify which group membership to add or to drop on a particular network interface. If no interface is provided the default network interface is assumed. Group membership reports are only sent by IGMP when a new multicast group membership is added to a particular interface. No reports are sent for successive joins for the same multicast group on the same interface. Likewise a leave message is only send for a multicast group, when the last application drops the group membership
5.2 Overview of protocol extensions

The current group management mechanisms can result in inefficient data delivery in the presence of multiple access networks, as users are free to join any multicast group/multicast source using any network interface they like. In particular this may lead often to a situation, where the same data is being delivered unnecessarily via multiple networks to the same location, as described in the introductory example in section 1.1.

Operators controlling both networks however, or operators cooperating with their networks would like to avoid such a situation and, instead, select one common delivery network in order to utilise network resources more efficiently. Delivery coordination also includes the possibility of balancing the load between access networks. This implies handing off receivers of multicast groups from particular links of an access network to another, in best case seamlessly to the multicast application even during sessions. In summary, there is a clear need for operators to direct hosts to join a specific access network or at least prevent a host from joining a specific multicast group on a link.

The presented approach in this chapter achieves this by adding the capability to the current group management model 1) to (temporarily) disable group membership collec-
5.2. Overview of protocol extensions

tion of multicast groups on particular router interfaces and 2) to redirect multihomed hosts to alternative access network.

A further observation motivating the work presented is that the availability of multiple interfaces is not adequately reflected by the current group management mechanisms at the receiver side. Current IGMP implementations are only concerned with the group membership management on a particular interface. To make thing worse, most multicast applications do not consider the availability of multiple network interface at a host. While the socket interface provides support to specify a specific network interface to establish a multicast group, most multicast applications lack the support of providing this option to the user. For example commonly used media playback applications such as Helix player by Real Networks or Windows Media Player by Microsoft provide an opportunity to specify an IP multicast address and port number to join a multicast group on the Internet. The user however has no opportunity to specify a desired network interface, instead the application will establish a session on the current default interface of the host. Writing network aware application considering multiple host interfaces or providing the application user with a possibility to specify a network interface is a first step to leverage from the advantages of a multi access network scenario.

A group management model that considers multiple available interfaces at the host could handle such issues even transparently to the application. Upon a network notification of an unsuccessful join attempt, a multihomed host could automatically retry joining on a different interface by selecting any other available interface. Such a fallback mechanism could improve the robustness of multicast delivery significantly. In case none of the attached access networks would support the forwarding for the desired multicast group, the application could be notified about the failure (e.g. via the socket interface). That way alternative measures can be taken by the application, or at least the user could be notified about the cause of the failure.

In the presented approach receivers benefit from an increase in robustness of multicast service delivery by taking advantage of multiple available access networks. This is achieved by extending the current multicast group management with mechanisms for 1) automatic fail-over or seamless change to an alternative interface considering user preferences and 2) provision of feedback to application in case of group management failure.

In order to consider receiver preference and restrictions when joining a multicast group, an ordered list of network interfaces can be optionally provided through the API call. The group management instance on the host side only considers the interfaces provided in the list and will probe for possible networks in the specified order.

At the same time, the group management mechanism also considers the operator re-
requirements on multicast service coordination. Starting from simply redirecting the host to try rejoining using an alternative interface, coordination could go as far as the operator proposing, which access network and hence interface to chose for a multicast service delivery.

5.3 Design principles

When making the proposed changes to the IGMP protocol, there are a number of important design considerations, which affect both protocol entities and the socket API.

The envisioned functionality should be achieved with a minimum of modifications required for the IGMP protocol entities on the host side and router side. Changes should be incremental in such a way that currently existing multicast mechanisms still remain supported. Furthermore, the solution has to be scalable, not adding unnecessary high signalling burden to the network.

A special challenge represents the required changes to the socket API. A large set of applications already exists today, which should continue to be supported even with the proposed modifications of IGMP. Thus changes to the API should provide both source and binary compatibility with programs written with the original API. In other words, program binaries which already exist on the system should continue to operate as expected without the need of recompilation or modification of sources. Also the changes to the API should be as small as possible to allow application programmers to easily write application with the new API. In addition, applications written using the new API should detect when the new functionality is not available at the system and react gracefully to such a condition.

5.4 Router extensions

The router side extensions are realised by the introduction of 1) multicast group filters, to describe supported and unsupported multicast groups, 2) an additional state in the IGMP protocol state machine to reflect proper protocol handling for unsupported groups and 3) a new IGMP message as receiver feedback mechanism. Details on the purpose of these extensions, their implementation and how they interwork are provided in the following subsections.
5.4. Router extensions

5.4.1 Multicast group filters

The current IGMPv2 implementation performs group management operations such as group membership collection and querying irrespective of the multicast group address. However, it is also desirable to temporarily suspend such operations for particular multicast groups. This way, it can be guaranteed that only multicast traffic of desired groups may be forwarded in particular subnets. A network operator needs thus the flexibility to specify a set of supported or unsupported multicast groups \(^\dagger\) for each interface.

The specification of supported or unsupported hosts is performed by filters, which apply to a specific interface. Each filter consists of a list of IP multicast addresses or optionally a list of (IP multicast address, network prefix) tuples and a filter mode, which can be either include or exclude. A list of IP multicast addresses in include mode specifies the list of supported IP multicast addresses; all others are assumed to be unsupported. In exclude mode, the list of IP multicast addresses specifies the unsupported multicast addresses, hence all other IP multicast addresses are assumed to be supported. Figure 5.2 shows an example of a possible filter specification for the filtering at the router.

Each incoming membership report sent by a host should be examined on a router's interface. In case the multicast group is found to be supported, IGMP performs operation as normal e.g., collecting group membership, triggering routing protocols when required. For unsupported multicast groups however, a new message, called REDIRECT message, is sent back to the host. A REDIRECT message contains at least the IP multicast address of the unsupported group and optionally a network prefix of a neighboring access network, which serves as an indication for the host. Using this network prefix, the network operator may direct/assist a host to select a suitable interface to rejoin a group.

The configuration of these filters is outside the scope of this work. However, existing mechanisms can be utilized to achieve this configuration, e.g., adding this capability to current network management tools for router configurations or by using alternative management protocols such as Multicast Control Protocol (MCOP) \([40]\).

\(^\dagger\)which ever requires less router state
5.4. Router extensions

5.4.1 Redirect Message Type

As previously explained, a **REDIRECT** message is sent by a router as a response to a membership report received by a host for an unsupported multicast address. An unsolicited **REDIRECT** message is also sent by the router after a filter change for each multicast group, which state from supported to unsupported. That way, currently subscribed receivers on a router link can be notified.

Figure 5.3 shows the format of the **REDIRECT** message. In its simplest form the format of the redirect message corresponds to IGMPv2 message format with message type **REDIRECT**, represented by the value of 0x18 and a Max Response Time field set to zero. The group address corresponds to the unsupported multicast group address, for which a membership report has been received.

If a network prefix is provided in the filter entry for the particular multicast address, the IGMP protocol instance at the router will specify the network prefix in an optional field to assist the host with the interface selection. In that case the length of the message is 12 instead of 8 bytes.

5.4.3 IGMP protocol modifications

The router behaviour in presence of multiple routers on the link (querier/non-querier) remains unchanged. However an additional state is required, called Idle state, in which a router can reside with respect to any single unsupported multicast group on any single attached network. Figure 5.4 shows the resulting IGMP+ state diagram at the router side for a querying router. For reasons of overview IGMP specific events and actions have been omitted at the transitions of the state diagram. Also the state introduced for IGMPv1 downwards compatibility has not been considered. Please refer to [21] for full information.

Two new events are introduced, which cause state transitions from and to Idle state:
5.4. Router extensions

The initial state depends on the filter settings and can be either No Members Present for supported multicast groups or Idle for unsupported ones. Furthermore a new action is introduced, namely 'send redirect request'. As a result of the action a REDIRECT message is sent to the group being reported. The action is performed in response to a membership query in idle state or in the other states in case of a disable event except the No Members Present state.

Likewise the same Idle state has been defined for routers in the role of a non-querrier, as shown in figure 5.5. State transitions occur from Idle to No Members Present state in the case of an enable event, while a disable event causes a transition from all other states to Idle state. In contrast, no send redirect request action is executed at non-querrier.
5.5 Host extensions

The host side extensions require modifications on the host side to IGMP protocol implementation as well as the multicast socket API. In the following the required changes are described.

5.5.1 IGMP protocol modifications

IGMP protocol operations for each multicast group are currently handled independently on each interface. A host can be in three different states with respect to a single multicast group on a single network interface. These 3 states are depicted in figure 5.6.

In order to handle the introduced REDIRECT router message, a new event is introduced, namely redirect received. This event may only occur if the host is in Delaying Member or Idle Member state and forces a state transmission to Non-member state. Furthermore a new action named reselect is introduced, which is taken in response to the redirect receive event. The action is used to notify upper layer that a subscribed multicast group on a particular interface is not supported any more.
5.5. Host extensions

While IGMP operations are limited to a single interface an IGMP interface manager (IIM) is introduced, in order to handle (automatic) interface reselection for a particular socket. The IIM coordinates IGMP operations and multicast group over various interfaces of the host. For each socket, the IIM maintains a list of preferred interfaces and the index for currently successfully selected interface. The options for reselection of an interface during operation are restricted to the interfaces maintained in this list.

In default mode, an interface in this list can only be used once during operation. In case all interfaces have been used within the list, e.g. if a REDIRECT message has been received on all attached subnets, the multicast group is considered unsupported and an error EGPNOTSUPP is set. If the support for multicast group on these subnets, however, is disabled at different times, a reuse of a previously used interface may become sensible. In order to cover this case an interface reuse option can be specified. Adequate timers should then prevent the reuse of an interface for a certain guard period, in order to avoid a ping pong effect between interfaces.

5.5.2 Socket API

Figure 5.7 shows the state transition diagram of the of the IIM with respect for a multicast group on a particular socket. Before a multicast group is joined on a socket, the IIM is in the Non-member state. After a multicast group is added via the socket interface, the IIM transfers to Interface to Select state. The IIM selects the first interface in the list of interfaces and adds the membership on the respective interface. Successful information is assumed as long as no reselect notification is received from the IGMP protocol instance. As aforementioned, such a notification is triggered by the IGMP protocol entity for the interface when a REDIRECT message is received.
In case of a notification the IIM assumes the group membership to be dropped on the current interface and performs two possible actions:

1. A redirect message was received without optional network prefix. The IIM chooses the next interface in the list to rejoin the multicast group. If the end of the interface list has been already reached and the interface reuse option is not enabled, the error EGRPNOTSUPP is set and the IIM moves to the No Interface to Select state. In case of an enabled reuse option the first interface in list which is not within a guard period is selected again. If all interfaces are in a guard period the error EGRPNOTSUPP is set and a transition to the No Interface to Select state occurs.

2. A redirect message was received with a network prefix proposed by the router. The IIM tries to find a matching network interface in its list with the network prefix. In case of a match the IIM uses this interface to rejoin the multicast group. Otherwise the next interface in the list is selected. As for the first case when all interface have been initially used and the interface reuse option is not enabled, the error EGRPNOTSUPP is set and the IIM moves to the No Interface to Select state. In case of an enabled reuse option the first interface in list which is not within a guard period is selected again. If all interfaces are in a guard period the error EGRPNOTSUPP is set and a transition to the No Interface to Select state occurs.

A transfer to the Non-member state takes place from both the Interface to Select
5.5. Host extensions

Table 5.1: Newly introduced socket options.

<table>
<thead>
<tr>
<th>Socket Option</th>
<th>System Call</th>
<th>Argument</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP_MIF_ADD_MEMBERSHIP</td>
<td>setsockopt()</td>
<td>struct ip_mif_mreq</td>
</tr>
<tr>
<td>IP_MIF_DROP_MEMBERSHIP</td>
<td>setsockopt()</td>
<td>struct ip_mif_mreq</td>
</tr>
<tr>
<td>IP_MULTICAST_MIF</td>
<td>getsockopt()</td>
<td>struct ip_mif_mreq</td>
</tr>
<tr>
<td>IP_MULTICAST_MIF_ERROR</td>
<td>getsockopt()</td>
<td>int</td>
</tr>
</tbody>
</table>

As mentioned in section 5.3, compatibility is a crucial design issue for the extension to the socket API. Drawing on experiences of previous attempts to modify the socket API, e.g. the introduction of source filters [70] in the socket API, the proposed modifications are described in the following.

The main difference to the original API comes from the need of the user to specify a list of network interfaces, instead of a single interface to join the multicast service. One could easily extend the current API call to provide a list of alternative interfaces instead passing a new data structure. This would however render old source code and binaries incompatible. Therefore new socket options are specified, which can be used by new applications to exploit the multi-interface feature, while keeping the behaviour of the original socket options unchanged. Alternatively, instead of defining new socket options, new system calls could be implemented. However extending a well known programming abstraction such as the socket interface by new options is considered more likely to be accepted by OS developer such as for Linux than the introduction of new system calls.

Table 5.1 provides an overview and brief description of the introduced socket options. The first two socket options are exclusively used for the `setsockopt()` system call. IP_MIF_ADD_MEMBERSHIP allows adding a multicast, while specifying multiple network interfaces. A consecutive call of `setsockopt()` with this option replaces the current interface list by a new interface list. IP_MIF_DROP_MEMBERSHIP removes the membership for a particular multicast group on the socket. The latter two options are used with the `getsockopt()` system call. IP_MULTICAST_MIF returns the current list of specified interfaces. Using the IP_MULTICAST_MIF_ERROR option an error for the multicast group can be queried on the socket.

In order to provide a list of interfaces and the interface reuse mode to the IIM via the socket interface, a new data structure needs to be defined. Figure 5.8 shows the structure `ip_mif_mreq`, which is passed to the socket call for the first three options, and
#include <netinet.h>

struct ip_mif_mreq {
    struct in_addr imr_multiaddr; // multicast group address
    uint32_t imr_ifrmode; // interface mode
    uint32_t imr_jnumif; // number of interface in list
    struct in_addr imr_iflist[0]; // list of interface addresses
};

Figure 5.8: Data structure for providing arguments to new socket options.

5.6 An operational example

In order to demonstrate the new protocol features, a brief operational example is given in this section. In figure 5.9, hosts with two network interfaces are considered. Both hosts, Host 1 and Host 2, are connected to subnet A with interface A and subnet B with interface B respectively, with Router A and Router B acting as querying multicast routers on the respective subnets.

Initially no multicast groups are disabled in the subnets. Host 1 joins multicast group 239.0.10.10 with interfaces A being the first interface in the argument list. Therefore a group membership report is send on subnet A. The router picks up the group membership report on the interface attached on the subnet and starts forwarding the multicast traffic. For reasons of brevity, the periodic general membership queries are omitted in this example. After some time the network operator decides to balance the load to alternative subnet for the particular multicast group and disable the multicast group on the interface attached to subnet A. As a result a redirect message is sent on the respective interface, which is heard by all other hosts subscribed to that multicast group. In the example Host 1 drops the group membership on subnet A and rejoins the multicast on the second interface on subnet B. Host 1 now receives the multicast traffic from router B.

At a later time Host 2 also subscribes to the multicast group 239.0.10.10, with interface A being the preferred interface. Since the multicast group is not provided on subnet...
5.7 Summary

A network layer solution to achieve multicast delivery coordination in a heterogeneous network environment has been presented in this chapter. As part of the solution, extensions to the current Internet group management protocol are proposed that consider multi-homed capabilities of a host, in order to reflect the characteristics in such an network environment more adequately.

In order to manage network resources in such an environment more efficiently, operators
require the capabilities for each individual multicast group 1) to control the delivery of multicast traffic on each subnet of an access network, and to 2) perform load balancing between access network. The presented approach achieves this by adding the capability to the current group management model 1) to (temporarily) disable group membership collection of multicast groups on particular router interfaces and 2) to redirect multihomed hosts to alternative access network.

Receivers benefit from an increase in robustness of multicast service delivery by taking advantage of multiple available access networks. This is achieved by extending the current multicast group management with mechanisms for 1) automatic fall-over or seamless change to alternative interface considering user preferences and 2) provision of feedback to application in case of group management failure.

The proposed extensions require the modification of IGMP protocol on host side as well as on the router side. Router side extension are realised by the introduction of

- multicast group filters for each router interface, to describe supported and unsupported multicast groups
- an additional state in the IGMP protocol state machine to reflect proper protocol handling for unsupported groups
- a new IGMP message, called redirect request, as receiver feedback mechanism.

The host side extensions comprise modifications to IGMP host side protocol entity as well as the multicast socket API. In particular the following additions have been made:

- Adaption of the IGMP protocol state machine for an interface on the host side to process the newly introduced redirect message.
- Introduction of an IGMP interface manager to manage multicast group memberships across multiple available interfaces with respect to a network socket.
- Introduction of new socket options and data structures for the multicast socket API. The socket options allow the specification of an ordered list interfaces when adding/dropping multicast group memberships on a socket and offer an interface to determine errors, which may have occurred.
Chapter 6

Implementation

While many developed concepts may work on paper and maybe even in a simulation environment, they often fail to do so once deployed in a real networking environment. The reasons for such failure are often a lack of understanding of implementation details or misconceptions of the characteristics of the target application environment. The importance of prototypes for verification is also stressed by many standardisation bodies such as the IETF or 3GPP. The IETF for example requires several independent implementations of a new mechanism or protocol before a solution can be accepted as an Internet standard [71]. Likewise 3GPP performs feasibility studies based on prototypes within their working groups before recommendations for a standards are made.

This chapter describes proof-of-concept implementations of the presented solutions for multicast delivery coordination, the GMS and the IGMP extensions. The proof-of-concept implementation demonstrate the feasibility and applicability of the developed solutions in real world applications. Furthermore they form the basis of the testbed evaluations, which are described in chapter 7.

The implementation of the GMS is realised by two parts: a GM on the network side and a multicast middleware (MM) on the terminal side. Section 6.1 describes the implemented components of the GM, which include the GMMF and the SCF. The network-side functionality of the MSCH has been integrated into the SCF. The MM implementation is described in section 6.2 and reflects the complete functionality as specified in the chapter 4. The proposed IGMP modifications as specified in section in chapter 5 affect the IGMP protocol entities on the router side as well as on the hosts. Section 6.3 covers the router side implementation, while section 6.4 is concerned with the host side implementation. The chapter is then concluded with a summary in section 6.5.
6.1 Group manager

The GM is responsible to implement the delivery coordination of multicast user services in an interworking wireless network environment. Normally the GM will be part of an interworking gateway functionality, running on network servers within the core network of the operator. To avoid unnecessary complexity the gateway has been implemented as single application called the IGW manager. Besides the GM, only essential functionality has been implemented required to demonstrate the GM operations. This includes a simplified RM and a hard-coded user context information database.

The IGW manager has been implemented as application with graphical user interface (GUI) support. A GUI is a desired feature, since it allows comfortable configuration of multicast user services. Further tools have been added to manually perform experimental evaluations, e.g. a message editor to create signalling messages on the MSCH and visualisation tools to monitor the operation for verification. The open source version of the QT [72] application development framework has been used for the implementation. QT provides useful C++ class-libraries suitable for cross-platform development, which are easily portable to most of popular operating systems. Required libraries include GUI, XML, event processing and networking support.

6.1.1 Multicast user service configuration

When starting the IGW manager the group membership management database is usually empty, since no groups for multicast user services have yet been created. A service provider needs to use the service primitives provided by GMMF to configure a multicast user service. There is a single GMMF entity with the group manager responsible for the management of multiple groups. The service provider related primitives of the GMMF are accessed by a GUI frontend, as shown in figure 6.1.

In order to configure a new multicast user service, a group entity for that service needs to be created. A unique identifier is automatically assigned to the group entity, shown in the listbox on the left. Then subsequently service related parameters need to be configured. This includes a descriptive service name for the user, and the IP multicast address and port number for each service flow. Each service flow has an additional QoS parameter, e.g. data rate, required by the RM function. Further configurations include parameters for the MSCH, namely multicast group, port number and utilised signalling network. Also additional RM related service parameters such as scheduling policies can be set. Details on the implemented RM functionality will be given at a later point in this chapter.
Once the configuration steps are finalised, the multicast user service can be provided to the users by the GMS. Relevant service announcement are configured, so users are able to learn about a multicast user service and obtain relevant parameters for service registration. Moreover, configuration of the user service can be modified at a later stage or a user service removed from the GMS by deleting the corresponding group entity.

6.1.2 Group entity

For each multicast user service a separate group entity exists in the GM. Besides service related parameters, a group entity also maintains a list of interested receivers. The GMMF receives incoming user registration for multicast user services and adds the users to the respective group entity. Likewise the GMMF acts on incoming user deregistration by removing the user from the appropriate group entity.

While adding an interested user, the group entity obtains relevant user related context information from context databases in the network. In the current implementation this is achieved by accessing a hard-coded context information database. The pointers to the context information are stored as part of a user data structure in the user list of a group and can be accessed by RM or SCF functionality whenever required.

Each group entity has been implemented as a separate thread, in order to support concurrent delivery coordination for multiple multicast user services. Each group entity
6.1. Group manager

also implements its own instance of RM and SCF for independent operation. Differential treatment of multicast user services can be achieved by specifying, e.g. different resource management policies.

6.1.3 Service announcement and user registrations

A typical way of discovering and accessing services on the Internet is by visiting a website of a service provider. Many mobile operators also enable access to their services via a portal website. Users can browse in a categorised database presented by linked websites for interesting services and request to register for it within an HTTP session. An alternative way of realising a service announcement is by using the session announcement protocol [56] over well known multicast IP addresses, so called session announcement channels. The session directory tool (SDR) [73] on the Internet is an example. Subscription could be also received by dedicated signalling between the users and the GM. Although existing mechanism such as SIP event subscription framework [74] or IMS group management [75] could be utilised, the implementation complexity at receiver side would significantly increase. The required extension would have to be integrated in the application or as part of the MM.

For reasons of implementation simplicity, the service portal approach has been adopted in the prototype of the GMS. An HTML frontend has been created for a service portal web site offering streaming video content. An Apache web server has been used to host the service. A user logs onto the service portal by providing a user identifier and credentials for authentication in form of a password. This authentication may not be required in a real mobile network, where the user could be identified by the connection used to access the portal. Once the user selects a service, e.g. by clicking on a link associated with the service, a script on the web server is triggered to perform registration of the user with the group for the service. A python script has been used as a server backend, to interact with the GMMF in the GM. The script generates a group registration message carrying the identifier of the user and the group ID for the service of interest. At the same time the user would download a small browser configuration file. The browser then launches an appropriate application for receiving the service at the receiver, e.g. a media player. Details on this are provided in section 6.2.

6.1.4 Resource management functionality

The group entity invokes the RM function, every time a user is added to its list. For on demand services a simple size based or time based batching algorithm is executed to determine the scheduled time of the service. The scheduling policy as well as the
parameters are configured for each multicast user service individually at creation of the respective group entity. For size based batching, a service session is initiated when a certain threshold number of users is reached. Time based batching schedules a session after a predefined time-out, independent of the number of group members. The timeout is usually started when the first user registers for a group. Once the service initiation has been determined, RM executes a service flow and network selection algorithm, which considers each receiver in the group and its context information, as well as resource availability in the networks. Useful context information currently includes terminal capabilities and user location. As a result, each user in the group is assigned a certain service flow and delivery network, and the results are stored in the corresponding user structure. Details on the resource management algorithms can be found in [58].

The RM obtains resource information from a database that has been implemented within the IGW manager. For each network, resource availability can be configured individually per cell, in order to evaluate algorithms under different conditions. After network selection has been performed for a user service, the resource information database is updated to reflect the decisions. In a real network environment such information would be available from distributed resource monitors within the operators own network or from peer RM in cooperating networks [76].

6.1.5 Session control function

The SCF is invoked, once the RM has performed service flow and network selection for each user in the group. A matching algorithm in the SCF first identifies the subgroups of receivers according to selected service flow and delivery network. Then common user context information is analysed and suitable addressing expressions are created for the signalling messages MSCH, which uniquely identify each of the subgroups. Finally messages are sent on the MSCH to establish the required multicast bearers for service delivery. Figure 6.2 shows a textual representation of a generated message used for the establishment of multicast bearer services in a network.

After the messages for establishment have been sent, the SCF notifies the sources of a multicast user service to start sending the selected service flows on the established multicast bearers.

During a session, RM may decide to balance the load in parts of one access network to another. The SCF is informed about the intended change and identifies the affected receiver subset. As for the establishment suitable messages on the MSCH are created and sent in order to implement the required vertical handoff. Since such dynamic resource management algorithms are yet to be implemented, a message editor has been integrated in the IGW manager to manually generate any possible messages for a
6.2 Multicast middleware

An application on the user terminal uses the services provided by the MM to receive IP multicast data instead of directly invoking services provided by the standard network protocol stack. The MM therefore needs to export stub routines in form of some API to the application. A customised API, created from scratch, could most intuitively present the service offered by the MM. Application programmers would use this interface API to write MM aware applications. A major disadvantage of the approach, however, is that a large set of legacy applications would remain unsupported, since they were written using the API provided by the standard socket interface. In order for this application to work with the MM, the actual sources of the application would require modification.

Usage of the MM without the need to modify existing applications would greatly simplify the deployment of the GMS. Therefore a major requirement for the implementation of the MM was to allow applications to use its functionality with the standard socket interface for IP multicast, without changing the sources or binaries. In order to achieve the goals the implementation made use of a transparent and extensible session layer.

Figure 6.2: XML representation of an ESTABLISH message.

particular MSCH. This allowed verification of the correct behaviour of the MM in the terminal for different scenarios. Figure 6.3 shows an example of a created message to handover a subset of receivers in a particular area from one access network to another.

Furthermore the SCF is also triggered at the end of a session, to release the previously established bearers. All receivers that have been serviced during the session are removed from the user list in the group entity. In some cases unsupported receivers may remain, e.g. receivers which could not be supported due to lack of available network resource at their location. These receivers can remain in the group in order to be considered for the next scheduled session.
6.2. Multicast middleware

Figure 6.3: XML representation of an MIGRATE message with expression for receiver subset addressing.

tool kit, named TESLA [77].

In the following the main concepts of TESLA will be briefly introduced. Then the implementation of the MM using TESLA will be described. Finally an example demonstrating the use of the MM for a video streaming application will be given.

6.2.1 Introducing TESLA

TESLA is an interposition agent toolkit that allows the integration of session layer services, without the need of modifying network layer services in the kernel or the applications using them. TESLA makes use of a known principle called dynamic library interposition [78]. Using dynamic linker in the system, TESLA can insert itself between any dynamically linked application and the standard C library, like, which also implements the socket API. All network related system calls are intercepted and routed to service handlers, which can implement the required session layer functionality. The MM functionality has thus been implemented as such a service handler. Figure 6.4 illustrates the principles in more detail. The left side shows a multicast application
using a conventional network protocol stack. On the right, the case with an interposed TESLA library is depicted, which is dynamically loaded at application start. By providing the same interface as libc, the multicast application has the illusion to directly interact with the network protocol stack.

Figure 6.5 shows part of the socket interface that have been redefined by TESLA and are used by the MM in order to implement the desired functionality. Upgrading the terminal with the MM only requires the installation of a library, which consists of the TESLA interposition functionality and the service handler for the MM.

6.2.2 Realisation

The MM service handler intercepts and handles all IP multicast related socket calls made by the application. The multicast application assumes that the multicast group address and port number provided by a service announcement are used for establishment of multicast bearers for service data delivery. The MM however uses those parameters, which are provided by calls to the socket API, to establish the MSCH. The application is left unaware of the operation and expects delivery of data once the service session is started.

Control messages that are sent via the MSCH are received by the MM service handler. The service handler first calls functions to evaluate the addressing expression part of the control message. If the addressing expression has been found to match the own context, the message body is further processed, otherwise the message is silently discarded. Receiver context information is currently hard-coded into configuration files.
6.2. Multicast middleware

int accept(int sd, struct sockaddr *addr, socklen_t *addrlen);
int bind(int sd, const struct sockaddr *addr, socklen_t addrlen);
int close(int sd);
int socket(int domain, int type, int protocol);

int getsockopt(int sd, int level, int optname, void *optval, socklen_t optlen);
int setsockopt(int sd, int level, int optname, const void *optval,
               socklen_t optlen);

int read(int sd, void *msg, size_t len);
int write(int sd, const void *msg, size_t len);

int send(int sd, void *msg, size_t len, int flags);
int recv(int sd, const void *msg, size_t len, int flags);

int sendto(int sd, const void *msg, size_t len, int flags,
           const struct sockaddr *to, socklen_t tolen);
int recvfrom(int sd, void *msg, size_t count, int flags,
             const struct sockaddr *from, socklen_t *fromlen);

Figure 6.5: Socket interface used by IP multicast applications that has been redefined by TESLA.

and accessed by the MM service handler, whenever required. However it is expected, that in a future implementation, receiver context information is dynamically managed by a daemon running as a background process on the user terminal. The MM service handler will thus obtain relevant context information by requesting them directly from the daemon.

A message body that has been accepted is further processed by the MM service handler. Three possible actions are taken, based on the message type. In case of an ESTABLISH message, the MM service handler first identifies the interface for the selected network, creates a new socket using the socket API of the standard C library, binds the socket to the identified multicast group and port number for the data bearer and joins the respective multicast address on the interface. Incoming data, on this socket, is passed to the applications. In case of a MIGRATE message, the same steps are repeated for

\(^1\)In Unix terms a daemon is a process running in the background, which performs a specified operation at predefined times or in response to certain events.
the new multicast bearer. The old socket is closed as soon as data on the socket for the new multicast bearer arrives. A RELEASE message closes the socket currently used for the data plane.

As soon as the user terminates the multicast application, all open sockets are closed by the MM service handler. With the application also the MM service handler terminates.

In the following an example of a launch of a multicast multimedia streaming application is given. The selected application is Video LAN Client (vlc) [79], a popular open-source media player client available on many system platforms, e.g. Windows, Linux, Macintosh. If a user wishes to start receiving an RTP based video stream from multicast address 239.12.0.5 and received on the application port 1234, it would usually need to type the following command line:

```
% vlc rtp:0239.12.0.5:1234
```

Using the MM handler support, simply two arguments would need to be prepended as follows:

```
% tesla +mm_handler vlc rtp:0239.10.10.1:5000
```

A wrapper script named 'tesla' launches the application named vlc with application parameters, by pre-loading the TESLA interposition library, with the service handler for the MM named 'mm_handler'. As before, the application parameters that follow the application name specify the transport protocol ('RTP'), multicast address and port number. This time the IP multicast address and port number, however, refer to the MSCH.

Launching of the application has been simplified within the browser. A new MIME type has been defined and associated with an file ending '.ion'. When clicking at the link to subscribe for a service at the web site of the service portal, a configuration file with that MIME type is download, which specifies the required application parameters. A script, installed at the receiver, is automatically invoked by the web browser, launching the vlc player as described above, without any requiring any user interaction.

### 6.3 Implementation of the IGMP router side extensions

In a dedicated hardware router, the IGMP protocol is part of a specialised operating system, e.g. Cisco IOS. The modification of such proprietary operating systems, however, requires significant expertise, access to source code and suitable development tools. Fortunately router functionality does not necessarily have to be implemented by dedicated hardware routers. While not providing the performance and high availability
6.3. Implementation of the IGMP router side extensions

of a dedicated hardware router, a PC with multiple network interfaces and suitable software support can provide router capabilities, sufficient for most experimental purposes. The Linux operating system for example, provides essential routing functionality and protocols in its network stack. Thus a PC with Linux operating system has been configured to act as a router. In fact many researchers within the Internet community, tend to implement and test network protocols and algorithms on Linux based routers, before hardware vendors implement them in their dedicated routing hardware.

In the following a brief overview of the multicast related router functionality on a Linux based router is provided. Then the required modifications to the IGMP protocol implementation on a Linux based multicast router are presented.

6.3.1 Multicast router support on a Linux system

Although available in most Linux implementations, multicast support is an optional feature, which requires explicit configuration within the Linux kernel [80]. Once enabled, multicast support comprises host side functionality of the IGMP protocol as well as forwarding support for multicast packets.

The Linux implementation of the IP protocol layer maintains routing information independent of address format such as IPv4, IPv6 or other network layer protocols within a Routing Policy Database (RPDB) [81]. The RPDB consists of two major components: a Forwarding Information Base (FIB) and the FIB rules. The FIB stores routing information while the rules are used to select a particular routing table, when multiple tables are configured. For increased system performance, known routes are stored in a route cache, which is consulted instead of the routing tables when possible, to allow fast forwarding decisions. The population of the FIB is either achieved statically via a application configuration program such as route or dynamically via a routing protocol.

Multicast routing protocols are realised by an external user mode process, also referred to as routing daemons, interacting with the kernel [82]. While routing of packets still takes place in the kernel space for increased performance, a routing daemon, such as mrouted or PIMd is required to update the forwarding entries in the FIB. Communication between the routing daemon and the kernel forwarding modules takes place via so called netlink sockets [83], which provide a special means of interprocess communications between user space and kernel space via the standard socket interface. Routing daemons, such as PIMd also exchange information with their peers via a routing protocol. The protocols are implemented on top of raw sockets, which provide a direct interface to the IP layer, thus bypassing the transport layer protocols such as UDP. The router side implementation of IGMP is usually also part of the routing daemon.
6.3. Implementation of the IGMP router side extensions

<table>
<thead>
<tr>
<th>File Name</th>
<th>Type of Modifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>defs.h</td>
<td>Added new function declarations</td>
</tr>
<tr>
<td>igmpv2.h</td>
<td>Redirect message type definitions</td>
</tr>
<tr>
<td>igmp.c</td>
<td>Sockets and message handling routine for pimdctl messages</td>
</tr>
<tr>
<td></td>
<td>Access list storing disabled multicast groups for each interface</td>
</tr>
<tr>
<td></td>
<td>Functions for access list management</td>
</tr>
<tr>
<td></td>
<td>Message handling of disabled multicast groups in IGMP state machine</td>
</tr>
<tr>
<td>igmp_proto.c</td>
<td>Generation of REDIRECT message</td>
</tr>
</tbody>
</table>

Table 6.1: Modified files of the pimd source tree.

As with the routing protocols, raw sockets are used for the IGMP message exchange with hosts on a subnet.

6.3.2 Protocol modifications

In the following the implementation of the router side extension to IGMP, as proposed in chapter 5, are described. The described enhancements are based on an open source implementation of PIMd [84] for Linux systems. PIMd implements as routing protocol the Protocol Independent Multicast Sparse Mode (PIM-SM) [85] version 2 and as group management protocol the router side protocol entity of IGMPv2.

Since PIMd runs in user space, modifications to the IGMPv2 modifications are straightforward. PIMd source code is written in the C programming language and organises code specific to IGMP operations mainly in two source files, namely igmp.c and igmp_proto.c. The igmp.c file provides functions for generic protocol initialisation, protocol state machine for received message processing and a generic function to send IGMP messages. The igmp_proto.c file provides function to manipulate internal protocol state e.g. membership state for interface and timers, and functions for the generation of required protocol messages. Table 6.3.2 shows an overview of modified files in the PIMd source tree directory for the proposed router side enhancements.

An access list is introduced for each interface, storing the IP multicast group addresses, which are temporarily not supported. In the current implementation, access lists can be configured by a simple configuration tool named pimdctl, which has been specifically developed for this purpose. The configuration tool interacts with the daemon via a UDP session, generating messages that disable or enable multicast groups on particular
6.3. Implementation of the IGMP router side extensions

router interfaces. The configuration can take place locally on the host running PIMd or even remotely from a different host. In order to disable the multicast group 239.0.10.10 on the router interface 192.168.24.1, the tool is invoked with the following command line parameters:

```
% pimdctl 192.168.24.1 disable 239.0.10.10
```

Likewise, to enable the multicast group again, the following command line parameters need to be specified:

```
% pimdctl 192.168.24.1 enable 239.0.10.10
```

In order to receive the control messages from pimdctl, PIMd needs to listen on a specific port on each interface via a UDP socket. For this the initialisation function in the igmp.c file has been enhanced, to create and register a new UDP socket for each interface at start time. Furthermore functions are implemented to handle incoming control messages from the pimdctl configuration tool and which allow the manipulation of the access list. On reception of a `disable` command for a particular multicast group on an interface, a corresponding REDIRECT message needs to be generated. As mentioned in chapter 5, this message is used to redirect receivers that are currently interested in the disabled multicast group to an alternative subnet. For this purposes a new function has been added to the igmp_proto.c file.

While the realisation with the `pimdctl` configuration tool is sufficient to demonstrate the mechanisms of the proposed protocol modification, a more advanced version could be based on configuration management tools such as provided by the Internet Standard Management Framework [86, 87]. Such an implementation, however, has been left for future work.

Additional modifications have been made to the protocol state machine for message processing in the igmp.c file. After extracting the group address on receipt of a membership report, it is verified if the group is currently disabled on the incoming interface. This is achieved by a match of the group address with the configured access list and the filter mode of the access list. If the multicast group is enabled normal protocol operation is assumed. The reception of a membership request for a disabled group also invokes a generation of a newly defined REDIRECT message. Verification of the multicast group address also takes place on receipt of an IGMP leave message. In case of an enabled multicast group, normal protocol operation is assumed, while in the case of a disabled multicast group the leave message is silently ignored. An overview of added functions and brief description of their purpose is provided below.

`accept_igmp` - igmp.c: Modification to existing functionality to handle incoming IGMP messages. After receiving a membership report for an disabled multicast group
on an interface a redirect message is generated. A leave request for a disabled multicast group is silently ignored.

**access_list_add - igmp.c:** Add a multicast group to the list of disabled multicast groups for a particular interface.

**access_list_remove - igmp.c:** Remove a multicast group from the list of disabled multicast groups for a particular interface.

**access_list_lookup - igmp.c:** Verify if a multicast group has been disabled multicast groups for particular interface.

**igmp_ctrl_read - igmp.c:** Read and process incoming control message from pimdctl utility.

**init_igmp - igmp.c:** Initialise for each interface an access list and sockets for interactions with the pimdctl utility. Register igmp_read_ctrl as respective message handler.

**reject_membership_report - igmp.proto.c:** Generate appropriate REDIRECT message and send on the respective interface.

### 6.4 Implementation of the IGMP host side extensions

The implementation complexity of the host side extensions of IGMP is comparably higher than the router side extensions. This is due to the fact that the IGMP protocol entity for the host side in Linux is implemented as part of the TCP/IP networking stack of the kernel. Modifications to code running in kernel space should be done with special care, since small mistakes can lead to a failure of the complete operating system. Therefore before making any modifications, the implementation of IGMP and its interactions with other parts of the TCP/IP network protocol stack and network device drivers need to be thoroughly understood. Unfortunately little and mainly outdated information has been available on the implementation details of multicast features within the Linux network protocol stack. Thus most of the understanding had to be derived by studying the actual kernel sources and the comments contained within. In addition, the debugging process for code running in kernel space is much more complex than code executed in the user space.

In the following a brief overview of the multicast related parts of the Linux protocol stack is provided, introducing the data structures and mechanisms relevant to the IGMP modifications. Then implementation details of the modifications are described.
6.4. Implementation of the IGMP host side extensions

6.4.1 Overview of the Linux networking stack

Networking capabilities are a fundamental part of the Unix operating systems and its derivations, such as BSD or Linux, and have played a significant role in their world wide acceptance and success. First implementations of the TCP/IP protocol stack for Unix like systems date back to the late 1970s and have been since enhanced and further developed by engineers and researchers from different organisations all over the world. Although many other protocol families have found their way into the networking stack of todays Linux implementation, most of them appear insignificant to the widespread deployment of TCP/IP and the Internet.

Figure 6.6 presents the current networking stack of the latest Linux kernel 2.6, focusing on the TCP/IP protocol family. As can be seen in the figure, most of the network capabilities are part of the kernel space. Applications access transport and network layer services of the operating system via the socket interface. Initially developed for the BSD operating system, sockets provide a standardised protocol-independent interface between application level programs and the networking stack. The socket interface exports its functions to user space as part of the glibc library. The glibc library in turn uses system calls to interface with the socket layer in the kernel space. Each socket entity in the socket layer consists of two parts, a protocol independent part and a part related to a specific protocol family. The protocol dependent part, also referred to as BSD socket entity allows the same interface to be reused for different types of protocols. The protocol dependent part links the socket to the transport and network protocol entities of a of a particular protocol family. The TCP/IP protocols are associated with the Internet protocol family, hence the protocol dependent part is referred to as INET socket. Depending on the type of services requested by the application at socket creation, the INET socket is tied to one of the transport layer protocols UDP or TCP, or directly to the IP layer. For multicast reception, the socket layer provides also an interface to the IGMP protocol entity.

Interaction of the TCP/IP stack with the actual physical network interfaces is achieved via a network device driver. The network device driver provides a common interface abstraction to the network layer, while at the same time implementing hardware dependent functionality for a particular network interface. As part of the Linux network stack a queuing layer is implemented between the IP protocol entity and the network devices drivers. The primary purpose of the queuing layer is to provide independence of buffering, between the device drivers and the network layer protocols. The queuing layer also allows to perform traffic shaping of in- or outgoing packets. Furthermore for outgoing packets the IP protocol entity uses the Address Resolution Protocol (ARP) [88] or its cache to determine the link layer address of the destination.
6.4.2 Data structures relevant to IP multicast

Each protocol layer within the Linux networking stack stores internal state information and information related to communication activities in one or several data structures. In particular, two data structures are of interest for IP multicast reception, they are maintained at socket level and on the interface level. Figure 6.7 shows those data structures and how they are embedded in the main network related data structures of the kernel.

Each socket, which is created with the Internet protocol family, keeps track of joined multicast group, by maintaining a list of `ip_mc_socklist` structures, each of which is associated with a multicast address. On interface level, another data structure named `ip_mc_list` is used for each multicast group membership that has been added to a network interface. The interface uses this list to determine, which multicast packets to filter and to pass to the higher layers. This packets are then forwarded to the respective sockets, at which the multicast groups have been joined. While multiple `ip_mc_socklist` structures may exist for the same multicast in different sockets for the
6.4. Implementation of the IGMP host side extensions

same multicast group, only one ip_mc_list exists at a particular network interface.

6.4.3 Protocol modifications

In order to implement the proposed protocol extensions, a number of additions and modification of functions as well as modification of data structures were required. Table 6.4.3 provides an overview change track of the affected files of within the Linux kernel source tree. The implementation followed the specification in section 5.5. Only the implementation of the reuse option for a provided socket list has not been considered at this stage and has been left for further work. The current implementation, however, was found sufficient to demonstrate the feasibility of the proposed concepts.

In order to implemented the IGMP interface management functionality, the ip_mc_socklist structure has been enhanced. One more data element has been added, namely a pointer to the ip_mreq_if data structure. The structure ip_mreq_if stores a list of interface addresses, that has been provided through the socket interface by the new socket options. This list is then used as a basis for further interface re-selection, which may occur during the operation, e.g. on receipt of a redirect message. The ip_mreq_if data structure is shown in figure 6.8.

In the following the modifications to the existing functions that are required to implement the protocol extensions are briefly summarised:
6.4. Implementation of the IGMP host side extensions

<table>
<thead>
<tr>
<th>File Name</th>
<th>Type of Modifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>include/linux/in.h</td>
<td>Added new socket options</td>
</tr>
<tr>
<td></td>
<td>defined ip.mif.mreq structure</td>
</tr>
<tr>
<td></td>
<td>definedIP.MIF.MREQ_SIZE macro to determine structure size</td>
</tr>
<tr>
<td>include/linux/igmp.h</td>
<td>added new function declarations</td>
</tr>
<tr>
<td></td>
<td>enhanced ip.mc.socklist structure</td>
</tr>
<tr>
<td></td>
<td>defined ip.mreq.iflist structure</td>
</tr>
<tr>
<td>usr/include/netinet/in.h</td>
<td>added ip.mif.mreq structure for user space</td>
</tr>
<tr>
<td>usr/include/bits/in.h</td>
<td>added new socket options for user space</td>
</tr>
<tr>
<td>net/ipv4/ip_sockglue.c</td>
<td>modified the ip_mc_sockopt function to handle</td>
</tr>
<tr>
<td></td>
<td>the newly introduced socket options</td>
</tr>
<tr>
<td>net/ipv4/igmp.c</td>
<td>modified the following functions: ip.mc_join_group</td>
</tr>
<tr>
<td></td>
<td>ip.mc.drop_socket, igmp.rcv</td>
</tr>
<tr>
<td></td>
<td>added the following functions: ip.mc_join_group.mif</td>
</tr>
<tr>
<td></td>
<td>ip.mc.leave_group.mif, ip.if_addr allow</td>
</tr>
<tr>
<td></td>
<td>igmp.heard.redirect.request, igmp_reselect_interface</td>
</tr>
</tbody>
</table>

Table 6.2: Modifications to the Linux kernel source tree.

- **ip_set_sockopt** - net/ipv4/ip_sockglue.c: Updated to handle newly defined socket options.
- **ip.mc_join_group** - net/ipv4/igmp.c: Adapted the initialisation of the modified ip.mc.socklist structure.
- **ip.mc.drop_socket** - net/ipv4/igmp.c: Freeing up memory in interface list has been previously allocated.
- **igmp.rcv** - net/ipv4/igmp.c: Enhancements of protocol state machine for received messages to accept REDIRECT messages.

Furthermore the functions that have been newly added are briefly described as follows:

- **ip.mc_join_group.mif** - net/ipv4/igmp.c: Adds or replaces interface provided by socket call and choses first interface in list to join the multicast group.
- **ip.mc.leave_group.mif** - net/ipv4/igmp.c: Handles the the drop of multicast group on a socket, where multiple interfaces have been specified.
6.5 Summary

This chapter has presented the proof-of-concept implementation of the two previously presented solutions to enable multicast delivery coordination in heterogeneous wireless networks.

The implementation of the GMS has been realised in two parts: a GM on the network side and a MM on the terminal side. The GM is part of an IGW application and has been implemented in the C++ programming language, based on portable libraries of the QT application development framework [72]. Code complexity was approximately 8000 lines of code. The IGW application can be deployed on a Linux based network server and features a multi-threaded group management server and a service manager for service creation. Each service group is managed by a separate thread and provides up to two different service flows. Also batching and network selection is performed independently for each service. In order to allow the configuration of different scenarios, resource settings can be modified by a resource editor. Current resource utilisation in
the cell can be observed by a resource display. Furthermore an internal user context
information database is maintained. Signalling message generation over the MSCH is
either provided automatically triggered by the RM, or manually using a message editing
tool. A webserver provided an interface for service discovery and group subscriptions.
The MM in the terminal has been implemented based on the TESLA session layer
toolkit [77]. The code complexity of own MM specific code included approximately
2000 lines of code. The MM can be easily deployed on a terminal by simply installing an
additional shared library. As a consequence applications do not require modifications,
thus guaranteeing the support of legacy applications.

The implementation of the proposed IGMP extension included modification of the
IGMP on the router side as well as on the host. The router side extensions have been
implemented on a Linux based multicast router. An open source implementation of the
PIMd [84] routing daemon, served as basis for the required modifications. The host side
extensions have been implemented on a Linux host, based on the Linux kernel version
2.6. The implementation complexity on the host side proved to be higher, as compared
to the modification on the router side, since it required modification of kernel code.
The overhead introduced to the kernel size and memory requirement at runtime has
been found insignificantly small.
Chapter 7

Evaluation

This chapter provides an evaluation of both the presented session and network layer solutions to achieve coordinated multicast service delivery in a multi-access network environment. The evaluation approach taken for the proposed solutions is twofold. Firstly, an analytical/simulation study is performed to evaluate the scalability of the solutions with regard to introduced protocol overhead. Secondly, viability of the developed concepts is demonstrated through proof-of-concept prototypes in a real network testbed environment. Furthermore delay measurements during testbed experiments with the prototypes are performed to evaluate their impact on delivery latency.

For the group management support an analytical analysis of the signalling overhead on the MSCH is provided in section 7.1. Furthermore a performance evaluation of the developed prototype has been performed in the testbed environment, which is presented in section 7.2. Likewise a performance evaluation of the introduced signalling overhead by the IGMP extensions has been performed in section 7.3, in form of a simulation study. Furthermore the implemented IGMP extensions have been evaluated in a testbed environment and results are presented in section 7.4. Finally section 7.5 provides a qualitative comparison of both approaches.

7.1 Evaluation of the MSCH

The introduction of a control signalling plane for multicast delivery between group manager and the middleware at the multicast receivers puts additional signalling burden onto the networks. In order to minimise the impact of signalling message delivery, a multicast signalling channel (MSCH) has been proposed in the previous chapter. While the concept of the MSCH suggests a scalable and resource efficient message delivery, it may first require verification considering various application scenarios. In order to allow
7.1. Evaluation of the MSCH

Firstly, an analytical model is developed that allows an evaluation of the signalling message delivery via the MSCH. The model allows a comparison to the conventional case of signalling message delivery, in which a separate control plane is utilised for each receiver. Then the assumptions used for the evaluations are described. Furthermore the obtained analytical results are presented and in detail discussed. The section concludes with a summary of observations made during this analysis.

7.1.1 Modelling parameters

The analytical model should reflect the context in which the group management support is used as realistic as possible. We therefore evaluate the costs for message delivery within an interworking mobile and broadcast network architecture, represented by multicast enabled UMTS and DVB networks.

Figure 7.1 shows a schematic view of the network elements and interconnecting links. Interworking functionality is provided by interworking gateways, located at the edge of the respective networks. Interworking signalling is sent from the group manager,
7.1. Evaluation of the MSCH

which is part of the interworking gateway, to receivers subscribed to a multicast service. Starting from the group manager, the signalling messages travel along the links through the network nodes to the respective receivers.

To simplify notation, each network node is labelled with a lowercase character, which is added to qualify performance metrics and modelling parameters used throughout the analytical model. Furthermore qualifiers specifying link parameters and metrics use both characters of the nodes they interconnect.

Similar to [89] message delivery costs are split into transmission costs over the network links and processing costs within the network nodes. Following the introduced qualifiers the individual cost metrics can be noted as follows:

- \( t_{ig} \): Transmission costs of message delivery between the IGW and GGSN
- \( t_{gs} \): Transmission costs of message delivery between GGSN and SGSN
- \( t_{sr} \): Transmission costs of message delivery between SGSN and RNC
- \( t_{ru} \): Transmission costs of message delivery between RNC and NodeB
- \( t_{mu} \): Transmission costs of message delivery over the UMTS air interface
- \( t_{td} \): Transmission costs of message delivery between IGW and DVB-G
- \( t_{dt} \): Transmission costs of message delivery within the broadcast distribution network
- \( t_{tu} \): Transmission costs of message delivery over the DVB air interface
- \( c_g \): Processing costs of message delivery at GGSN
- \( c_s \): Processing costs of message delivery at SGSN
- \( c_r \): Processing costs of message delivery at RNC
- \( c_n \): Processing costs of message delivery at NodeB
- \( c_d \): Processing costs of message delivery at DVB network gateway
- \( c_t \): Processing costs of message delivery at DVB transmission subsystem

The interconnection of network nodes is usually realised by different networking technologies. The packet switched core network in UMTS release 6 [90] uses an IP backbone network for data plane traffic between GGSN and SGSN, as well as SGSN and RNC nodes. On the other hand RNC and NodeBs in the radio access network connect directly via ATM circuits/trunks. Similarly, broadcast distribution networks are not standardised and can be realised either by ATM [91] [92], IP based backbone networks [93] or even use satellite links to convey data to the transmitter sites. In order to keep the generality of the model, the transmission costs over a network segment can be written as:

\[
t(I) = w_x \times l(I) \times u(I)
\]  

(7.1)

with \( l(I) \) denoting the average distance or number of hops a message travels between two network nodes and \( u(I) \) being the unit transmission costs on a given link between
two network nodes. In addition a factor \( w_t \) is introduced, which allows transmission costs to be weighted differently from processing costs in the analytical model.

Analogously processing costs are weighted with a different factor \( w_p \). Let further \( v(\cdot) \) denote the unit processing cost of a network node. The processing costs can be thus defined as:

\[
c_{(\cdot)} = w_p \times v(\cdot)
\]

As in [89], cost parameters can be interpreted in different ways and are not limited to a particular evaluation metric. Processing costs can be regarded in terms of delay of a particular network element in processing a message or the computational resource required. Likewise transmission costs can express the delay of sending a message on a particular link or the bandwidth requirements for a particular message. It is assumed that the relative cost parameters for network elements and links can be freely defined by the network operators within this analytical framework. Representative values are known from operational experience or can be obtained by suitable measurements. Assuming these values to be known, further elaborations will solely concentrate on providing a methodology to evaluate different ways of delivering the proposed interworking signalling.

Besides parameters for costs, the model also considers parameters defining the network topology. For the UMTS network part a single GGSN is connected to a total number of \( N_s \) SGSNs. Each SGSN manages \( N_{RA/s} \) Routing Areas (RAs). A RA covers a total of \( N_{RA/RA} \) RNC network nodes. Each RNC in turn controls \( N_{n/r} \) NodeBs. It is assumed that a NodeB transmits in a single cell. Similarly it is assumed that one DVB gateway serves as entry point for data to the broadcast distribution network. From there, data is forwarded to DVB transmitter subsystems (DTS) to be broadcast in the respective areas. For sake of simplicity and without loss of generality, it is further assumed that the number of DTS is a multiple of the number of UMTS RA and that \( N_{RA/RA} \) DTS exactly overlap with these RAs. Hence the remaining number of network nodes can be derived as follows:

\[
\begin{align*}
N_{RA} &= N_s \times N_{RA/s} \\
N_r &= N_s \times N_{RA/s} \times N_{RA/RA} \\
N_n &= N_s \times N_{RA/s} \times N_{RA/RA} \times N_{n/r} \\
N_t &= N_s \times N_{RA/s} \times N_{RA/RA}
\end{align*}
\]

with \( N_{RA} \) being the total number of routing areas, \( N_r \) the number of RNCs and \( N_n \) the number of NodeBs, and \( N_t \) the number of DTS in the modelled system.
7.1. Distribution of multicast receivers

While the performance of unicast delivery of interworking messages depends on the number of targeted receivers, the performance in multicast delivery mainly depends on the way these receivers are distributed in the network. Following the approach proposed in [94], the total number of RAs is partitioned into \( r \) different classes. For \( 1 \leq i \leq r \), there are \( N_i^{(RA)} \) RAs of class \( i \), hence \( N_{RA} = \sum_{i=1}^{r} N_i^{(RA)} \).

Let \( \phi_i^{(RA)} \) be the expected number of multicast members in a class \( i \) RA. It is assumed that multicast members enter a class \( i \) RA with rate \( \lambda_i \) and that multicast members reside within an RA for a period \( T_i \), having a general distribution with the mean \( 1/\mu_i \). With the aggregate multicast member arrivals being approximated by a Poisson stream where \( \lambda_i = \phi_i^{(RA)} \times \mu_i \), the expected number of RAs with multicast members present, has been determined in [94] as:

\[
n_{RA} = \sum_{i=1}^{r} (1 - e^{-\phi_i^{(RA)}}) \times N_i^{(RA)}
\]

(7.3)

In the following, the numbers of network nodes serving multicast users are derived. Given that multicast users are located in \( n_{RA} \), the probability of an SGSN not serving at least one of these areas is:

\[
P_S = \begin{cases} \frac{N_{RA} - n_{RA}}{N_{RA}} & \text{if } n_{RA} \leq N_{RA} - N_{RA}/s \\ 0 & \text{otherwise} \end{cases}
\]

(7.4)

Knowing this probability, the total number of SGSNs that are serving multicast users can be calculated as

\[
n_s = N_s \times (1 - P_S).
\]

(7.5)

Furthermore it is assumed that all RNCs that are part of the service area of an RA of class \( i \) have the same multicast population density as the RA and that receivers are uniformly distributed among these RNCs. Therefore the multicast population of an RNC located in a class \( i \) RA is

\[
\phi_i^{(R)} = \frac{\phi_i^{(RA)}}{N_{r/RA}}.
\]

The total number of class \( i \) RNCs is

\[
N_i^{(r)} = N_i^{(RA)} \times N_{r/RA}.
\]

The number of RNC that have multicast users for all \( r \) classes is therefore given by

\[
n_r = \sum_{i=1}^{r} (1 - e^{-\phi_i^{(R)}}) \times N_i^{(r)}.
\]

(7.6)
7.1. Evaluation of the MSCH

The same also applies to the NodeBs within the service area of an RNC. The average multicast user population for a NodeB controlled by a RNC belonging to class $i$ is

$$\phi_{i}^{(n)} = \frac{\phi_{i}^{(r)}}{N_{n/r}}.$$  \hfill (7.1)

The total number of class $i$ NodeBs is therefore

$$N_{i}^{(n)} = N_{i}^{(r)} \times N_{n/r}.$$  \hfill (7.2)

The number of NodeBs that have multicast users for all $r$ classes is then given by

$$n_{n} = \sum_{i=1}^{r} (1 - e^{\phi_{i}^{(n)}}) \times N_{i}^{(n)}.$$  \hfill (7.7)

For the DVB network, the number of DTS serving multicast users can be determined analogously. Since $N_{t/RA}$ DTS cover the area of an RA the average multicast receiver population in a DVB cell is

$$\phi_{i}^{(t)} = \frac{\phi_{i}^{(RA)}}{N_{t/RA}}.$$  \hfill (7.3)

The total number of class $i$ DTS is

$$N_{i}^{(t)} = N_{i}^{(RA)} \times N_{t/RA}.$$  \hfill (7.4)

The number of DTSs that have multicast users for all $r$ classes is therefore given by

$$n_{t} = \sum_{i=1}^{r} (1 - e^{\phi_{i}^{(t)}}) \times N_{i}^{(t)}.$$  \hfill (7.8)

Finally the total receiver population in the network can be computed as

$$N_{total} = \sum_{i=1}^{r} N_{i}^{(RA)} \times \phi_{i}^{(RA)}.$$  \hfill (7.9)

7.1.3 Delivery cost

As aforementioned the group management support requires control messages to be delivered from the group manager to the multicast middleware within the terminals of the user. In the following the costs for signalling message delivery are first derived for the case of using a separate control plane for each user, also referred to as unicast delivery. Then the costs for signalling message delivery via a common control plane on the MSCH are derived, further referred to as multicast delivery.
7.1. Evaluation of the MSCH

In unicast delivery, a copy of the message is transported to each targeted receiver terminal individually. Let \( m \) be the unit size of a control message sent to an affected receiver. Furthermore let \( N_m \) be the average number of messages sent during a session, and \( N_{rx} \) the average number of receivers targeted by a message. The total delivery costs for unicast delivery in the UMTS network can then be expressed as:

\[
S^{(U)}_{\text{uni}} = (t_{tg} + c_g + t_{gs} + c_s + t_{er} + c_r + t_{rn} + c_n + t_{mu}) \times m \times N_m \times N_{rx}.
\]  

Likewise the total delivery cost for the unicast delivery case via DVB network can be calculated as

\[
S^{(D)}_{\text{uni}} = (t_{td} + c_d + t_{dt} + c_l + t_{tu}) \times m \times N_m \times N_{rx}.
\]

Multicast delivery requires all users to subscribe to a multicast bearer service before control messages from the group manager can be received. MBMS bearer services are used to provide the required multicast transport in UMTS networks. When messages are sent on a multicast bearer service, a copy of these messages is transmitted in all those cells of a network, in which user subscribed to the multicast bearer service are present. Within the core network a copy of the message is only forwarded to the downstream network nodes serving the multicast users. Control messages sent over the multicast signalling channel, however, require an additional addressing expression to identify the subset of receivers on the channel for which the control message actually applies. The size of the control message is thus

\[
m_{MSCH} = m + m_{addr}
\]

with \( m_{addr} \) being the size of the required addressing expression.

The total costs for the delivery of control messages via multicast in a UMTS network can be calculated as

\[
S^{(U)}_{\text{multi}} = [t_{tg} + c_g + n_g \times (t_{gs} + c_s) + n_r \times (t_{er} + c_r) + n_n \times (t_{rn} + c_n + t_{mu})] \times N_m \times m_{MSCH}
\]

Likewise DVB bearer services can be used to efficiently transfer IP multicast data. Messages sent on a DVB multicast bearer service are only forwarded to the DTS, where subscribed users are present before being broadcast in the respective cells of the network. The total cost for the delivery of control messages via multicast in a DVB network is therefore

\[
S^{(D)}_{\text{multi}} = [t_{td} + c_d + n_t \times (t_{dt} + c_l + t_{tu})] \times N_m \times m_{MSCH}
\]
Before a message can be sent via the MSCH, a multicast bearer service has to be established for the user group in the respective signalling networks. Likewise, after all control messages related to a multicast session have been sent, the respective multicast bearer services need to be released. The establishment and release will introduce additional signalling load to the network, which has to be considered when evaluating the delivery costs of the MSCH.

Within the UMTS network, multicast bearer services are established by the MBMS service activation procedure, and released by the MBMS service deactivation procedure. Both procedures are executed for every receiver. The procedures are triggered by IGMP messages, which are carried over a general purpose PDP context. Since the reception of unicast message also requires a previous PDP context activation, it is assumed that such a PDP context is already existing for both delivery modes. Therefore only the additional signalling costs for establishment and release of multicast bearer services will be considered.

The total signalling costs for MBMS multicast bearer service activation $S_{act}^{U}$ and deactivation $S_{deact}^{U}$ for a single user have been derived in Appendix A.1. Based on these costs, the total costs for the signalling delivery over the MSCH when provided over a multicast bearer in the UMTS can be summarised as:

$$S_{MSCH}^{U} = \left[ t_{ig} + c_{ig} + n_x \times (t_{gs} + c_{gs}) + n_{tr} \times (t_{tr} + c_{tr}) + n_{tmsc} \times (t_{tn} + c_{tn} + t_{tu}) \right] \times \frac{N_{msc}}{n \times m_{MSCH} + (S_{act}^{U} + S_{deact}^{U})} \times N_{rx} \tag{7.15}$$

Analogously signalling costs for multicast bearer activation $S_{act}^{D}$ and deactivation in DVB networks $S_{deact}^{D}$ have been derived in Appendix A.2. The total costs for the signalling delivery over the MSCH using a multicast bearer in the DVB network can thus be summarised as:

$$S_{MSCH}^{D} = \left[ t_{id} + c_{id} + n_t \times (t_{dt} + c_{dt} + t_{tu}) \right] \times \frac{N_{msc}}{n \times m_{MSCH} + (S_{act}^{D} + S_{deact}^{D})} \times N_{rx} \tag{7.16}$$

7.1.4 Assumptions

In the following it is assumed that the modelling parameters for the transmission and processing costs are available for both networks. In order to examine the topological influence of network nodes on the transmission schemes, two different network configurations are examined. Table 7.1 summarises the parameters of these configurations, which differ in numbers of network nodes. Topology A represents a UMTS network
7.1. Evaluation of the MSCH

Table 7.1: Different configuration of network topology.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>$N_s$</th>
<th>$N_{RA/s}$</th>
<th>$N_{RNC/r}$</th>
<th>$N_{NodeB/RNC}$</th>
<th>$N_{IR/RNC}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topology A-I</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>Topology A-II</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>Topology B-I</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>20</td>
<td>4</td>
</tr>
<tr>
<td>Topology B-II</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>20</td>
<td>8</td>
</tr>
</tbody>
</table>

Table 7.2: Average hop counts for links between network nodes.

<table>
<thead>
<tr>
<th>Link</th>
<th>$l_{gs}$</th>
<th>$l_{sr}$</th>
<th>$l_{rn}$</th>
<th>$l_{ds}$</th>
<th>$l_{lr}$</th>
<th>$l_{ld}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hop count</td>
<td>10</td>
<td>10</td>
<td>1</td>
<td>10</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

with 5 SGSNs, 5 RAs per SGSN, 5 RNCs per RA and 10 NodeBs per RNC. In topology B there are 10 SGSNs, 10 RAs per SGSN, 10 RNCs per RA and 20 NodeBs per RNC. Likewise two configurations for the DVB network topology exist. The configurations are labeled I and II and differ in the ratio of UMTS and DVB network cells $r_{U/D}$, which is assumed 50 and 25 respectively.

Table 7.2 shows the average length of the links between the different network nodes. Based on [95], the average number of hops between hosts within a country on the Internet is approximately 15. It is assumed that the average number of hops between the gateway of a national mobile network and the mobile nodes is not significantly larger. Therefore the links between the nodes GGSN and SGSN as well as SGSN and RNC are set to be $l_{gs} = 10$, $l_{sr} = 10$. Since RNC and NodeBs are generally directly connected via a dedicated connection $l_{rn} = 1$. Links between DVB network gateway and DTS are assumed to have a hop count of $l_{ds} = 10$. The IGWs are assumed to be co-located to the respective network gateways, hence $l_{lr} = 1$ and $l_{ld} = 1$.

The unit costs for processing and transmission of a message are assumed to be higher in the UMTS radio access network (UTRAN) as in the core network (CN). Furthermore it is assumed that the transmission costs over the wireless link are significantly higher than the unit distance transmission costs over the wired network. Table 7.3 shows the parameters for unit processing costs used in the evaluation, which are based on values suggested in [89]. Processing and transmission costs are weighted equally with $w_p = w_t = 1$.

In the modelled topology, DVB network cells cover larger geographic areas than UMTS network cells. Assuming a uniform distribution of receivers, the number of potential users is higher in a larger broadcasting cell. Since the given resource in a cell has
7.1. Evaluation of the MSCH

<table>
<thead>
<tr>
<th>Unit transmission costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u_{lg}$</td>
</tr>
<tr>
<td>0.1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unit processing costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>$v_{g}$</td>
</tr>
<tr>
<td>0.5</td>
</tr>
</tbody>
</table>

Table 7.3: Units cost parameters for transmission and processing of a message.

to be shared by more users, the unit transmission costs over the wireless link is set comparably higher in a DVB network cell.

As in [94], different receiver distributions are considered by modelling two classes of RAs ($r=2$): Class $i = 1$ RAs with a receiver population of $\phi_1 = \lambda_1/\mu_1 = \delta$ and class $i = 2$ RAs, with a receiver population of $\phi_2 = \lambda_2/\mu_2 = 1/\delta$. Each RNC within an RA is considered to serve calls with the same receiver population density. For large values of $\delta$, class 1 RAs are likely to have multicast users present, while in class 2 RAs it is more likely to find no multicast users. Let further $\alpha$ be the proportion of the class $i = 1$ and $1 - \alpha$ the proportion of the $i = 2$ RAs.

Sizes of signalling message of MBMS multicast bearer service activation and deactivation procedures have been obtained from specifications for Session Management (SM) [51], Radio Access Network Application Part (RANAP) [49] and GPRS Tunneling Protocol (GTP) [50] assuming only mandatory message fields. For some of the messages an access point name (APN) was required, which was assumed to be 80 bits. The assumed message sizes for multicast bearer activation and deactivation are summarised in table 7.4. Due to its wide application, IGMPv2 [21] has been assumed as a group management protocol at the receiver. Multicast join and leave messages have the same message size with $m_{join} = m_{leave} = 224$ bits.

7.1.5 Signalling load analysis for single message delivery

In this section the performance of different delivery schemes is analysed, based on the assumptions derived in the previous section.

Figure 7.2 shows the costs for the delivery of a single message for all four topologies as a function of $\alpha$ for three different multicast receiver population cases, with $\delta = 100$ representing low, $\delta = 1000$ medium and $\delta = 10000$ high service popularity. The evaluation has been made on the assumption that the required addressing expression on the MSCH is of the size of a typical signalling payload $m = m_{addr} = 2016$, (e.g.
### 7.1. Evaluation of the MSCH

#### Multicast Bearer Activation Procedure

<table>
<thead>
<tr>
<th>$m_{addr}$</th>
<th>$m_{res}$</th>
<th>$m_{req}$</th>
<th>$m_{res}$</th>
<th>$m_{req}$</th>
<th>$m_{res}$</th>
<th>$m_{req}$</th>
<th>$m_{accept}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>400</td>
<td>80</td>
<td>592</td>
<td>216</td>
<td>64</td>
<td>8</td>
<td>192</td>
<td>80</td>
</tr>
</tbody>
</table>

#### Multicast Bearer Deactivation Procedure

<table>
<thead>
<tr>
<th>$m_{addr}$</th>
<th>$m_{res}$</th>
<th>$m_{req}$</th>
<th>$m_{res}$</th>
<th>$m_{req}$</th>
<th>$m_{res}$</th>
<th>$m_{req}$</th>
<th>$m_{res}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>16</td>
<td>328</td>
<td>80</td>
<td>64</td>
<td>8</td>
<td>344</td>
<td>80</td>
</tr>
</tbody>
</table>

Table 7.4: Size of messages exchanged in the MBMS multicast bearer service activation procedure.

<table>
<thead>
<tr>
<th>Network</th>
<th>Topology A-I</th>
<th>Topology A-II</th>
<th>Topology B-I</th>
<th>Topology B-II</th>
<th>UMTS</th>
<th>DVB</th>
<th>UMTS</th>
<th>DVB</th>
<th>UMTS</th>
<th>DVB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topology A-I</td>
<td>1</td>
<td>50</td>
<td>10</td>
<td>500</td>
<td>100</td>
<td>5000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Topology A-II</td>
<td>1</td>
<td>25</td>
<td>10</td>
<td>250</td>
<td>100</td>
<td>2500</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Topology B-I</td>
<td>0.25</td>
<td>12.5</td>
<td>2.5</td>
<td>125</td>
<td>25</td>
<td>1250</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Topology B-II</td>
<td>0.25</td>
<td>6.25</td>
<td>2.5</td>
<td>62.5</td>
<td>25</td>
<td>625</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 7.5: Average number of receivers per cell for $\alpha = 0.5$.

From section 7.1.4 it is known that $\alpha$ represents the proportion of class 1 RAs with a small receiver population, while $1 - \alpha$ the proportion of class 2 RAs with large receiver population density. For increasing values of $\alpha$, the number of areas with sparse multicast receiver population increases, hence the overall number of multicast users decreases in the network. As a consequence the delivery costs for either delivery modes for both of the networks decreases.

Table 7.5 shows the resulting average number of receivers per cell in the UMTS and DVB network for the different network topologies and receiver densities, considering a proportion $\alpha = 0.5$.

Figures 7.2(a) and 7.2(b) show the costs for a small receiver population with $\delta = 100$ for the different receiver populations for UMTS network and DVB network, respectively. As expected, the unicast delivery costs for topology A-I and A-II are the same within both networks, since the number of RAs and hence the number of receivers within them are identical. The same also applies for topologies B-I and B-II. The signalling costs for
7.1. Evaluation of the MSCH

Figure 7.2: Total costs for a single message delivery against $\alpha$ for different topologies and $m = m_{addr} = 2016$. 

(a) UMTS Network, $\delta = 100$.  
(b) DVB Network, $\delta = 100$.  
(c) UMTS Network, $\delta = 1000$.  
(d) DVB Network, $\delta = 1000$.  
(e) UMTS Network, $\delta = 10000$.  
(f) DVB Network, $\delta = 10000$. 


topologies B are higher due to the larger number of RAs with the same receiver densities and hence higher number of receivers as compared to topologies A. The figures also show that the delivery costs for multicast delivery of a signalling message are always smaller than for the unicast delivery mode regardless of the network for all values of $\alpha$. Furthermore the proportion to unicast delivery stays nearly constant over the whole range of $\alpha$ for each of the topologies. Only for for values of $\alpha \geq 0.9$ does the proportion slightly decrease. The delivery overhead in the UMTS network for multicast delivery in topologies B is only slightly lower than the unicast case, while the difference in topologies A is more than twice as much. This is due to higher number of NodeBs in Topologies B to cover the same multicast receiver population per RA.

While the number of NodeBs per RA in topology A-I and A-II and B-I and B-II are the same respectively, the number of DTSs per RA is different for all four topology cases due to the varying UMTS to DVB cell ratio. As expected the signalling costs in case A-I and A-II are approximately double as high, since twice the number of DTSs are required within a DVB network to cover the same receiver population within a RA. The same can be observed for B-I and B-II, respectively. Furthermore as for the UMTS case, signalling costs for topologies B are proportionally higher than for A, due to larger number of RAs, and hence overall larger number of DTS utilised.

For larger receiver population with $\delta = 1000$ and $\delta = 10000$, as seen in figures 7.2(c) to 7.2(f), multicast delivery costs stay approximately the same while the unicast delivery costs increase by 10 or 100 respectively. As expected with increasing receiver population, multicast delivery becomes more efficient.

Figure 7.3 observes the signalling costs for the different topologies as a function of $\delta$. Since the ratio of unicast and multicast delivery is nearly constant over the whole range of $\alpha$, a fixed value $\alpha = 0.5$ has been used for the comparison. As in the previous case the addressing expression size was assumed to be equal to the signalling payload with $m_{addr} = 1000$.

Figure 7.3(a) shows the signalling costs in the UMTS network. As in the above case unicast signalling costs topologies A-I and A-II and topologies B-I and B-II are the same over the whole range of delta. Same also applies to multicast signalling costs. Only for very low receiver densities for $\delta \leq 50$ unicast signalling becomes more efficient than multicast delivery in topologies B. For topologies A, the threshold is even lower with $\delta \leq 20$. It can also be observed that multicast signalling costs converge to a constant value for larger values of $\delta$, while unicast delivery costs keep on constantly increasing. While the number of receivers increase for larger values of $\delta$, the costs for unicast delivery are also expected to increase. In case of multicast delivery however, saturation is reached, once all cells of a network occupy at least one multicast receiver. Beyond that point multicast delivery costs stay the same. Figure 7.3(b) shows the
7.1. Evaluation of the MSCH

Figure 7.3: Total costs for a single message delivery as a function of $\Delta t$ for all topologies with $\alpha = 0.5$ and $m = m_{\text{addr}} = 2016$. 
respective signalling costs in the DVB network. The threshold for unicast delivery to become more efficient are $\delta \leq 30$ and $\delta \leq 10$ for topologies B-II and B-I and even lower for A-II with $\delta \leq 5$ and $\delta \leq 2$ for A-I. To conclude the observation, multicast signalling is always more efficient than unicast signalling except for very low receiver population densities. The larger the receiver population density, as well as the receiver population, the higher the benefits of employing a MSCH.

Previous evaluations assumed fixed addressing expression size of $n_{addr} = 2016$. The size of the addressing expression, however, may vary depending on the signalling and receiver scenario. Therefore the impact of the addressing expression size on the signalling costs has to be analysed for the different topologies. Figure 7.4 for shows the signalling costs within a UMTS network as a function of $m_{addr}$, assuming three receiver densities with $\delta = 100, 1000, 10000$ and fixed $\alpha = 0.5$. As expected, the signalling costs for unicast delivery are constant for all topologies, since it is only a feature required for the multicast delivery on the MSCH. In contrast, the multicast signalling costs increase for all topologies as the size of the addressing expression increases. Furthermore, the signalling costs for topologies A-I and A-II as well as B-I and B-II are equal for both unicast and multicast delivery case for all values of $m_{addr}$. In case of low receiver population case as shown in figure 7.4(a), multicast signalling becomes less efficient than unicast signalling for $m_{addr} > 2500$ units in case of topologies B. The break-even point in topologies A lies considerably higher with $m_{addr} > 6500$. The reasons are the same as for the previous cases, since the topologies A cover the same RA with a fewer number of NodeBs. For medium receiver population as shown in figure 7.4(b), the threshold for the topologies B is with $m_{addr} > 17000$ significantly higher, and is met by topologies A only for very large addressing expression sizes beyond 20,000 units. Same applies for all topologies addressing expression sizes for higher receiver population as shown in figure 7.4(c). Even for large addressing expression sizes, multicast delivery always provides a more efficient delivery option in a UMTS network for medium to higher receiver population densities. Only for low receiver population densities and large addressing expression sizes, unicast delivery should be considered.

Figure 7.5 shows the signalling costs as a function of $m_{addr}$ for the DVB network. With increasing number of utilised DTS in the network, the threshold of multicast delivery efficiency decreases. In contrast to the UMTS case, the threshold in the DVB network are well beyond the 20,000 units range for all topologies. Even if an extended range of 50,000 units is considered for $m_{addr}$, multicast delivery is always more efficient than unicast delivery, except for the case of topologies B and a small receiver population density of $delta = 100$, as shown in figure 7.5(a). In this case, multicast delivery becomes less efficient beyond and addressing expression size of approximately 25,000 for topology B-I and 50,000 for topology B-II.
7.1. Evaluation of the MSCH

Figure 7.4: Total costs for a single message delivery as a function of $m_{addr}$ for all topologies within the UMTS network with $\alpha = 0.5$. 
Figure 7.5: Total costs for a single message delivery as a function of $m_{addr}$ for all topologies within the DVB network with $\alpha = 0.5$. 

(a) DVB Network, $\delta = 100$.

(b) DVB Network, $\delta = 1000$.

(c) DVB Network, $\delta = 10000$. 
7.1.6 Signalling load considering impact of MSCH management

The analytical results in the previous subsection have considered the signalling costs for delivery of a single signalling message only. In this section also the impact of establishment and release of the required signalling channels at the receivers will be analysed.

Figure 7.6 shows the costs for the total delivery of a single message including signalling costs for MSCH management for all four topologies as a function of $a$. For a small receiver population with $\delta = 100$ the costs for multicast delivery are higher in a UMTS network than for unicast delivery, due to the high costs for multicast bearer establishment and release. For a larger receiver population, however, as shown in figures 7.6(c) and 7.6(e), multicast delivery becomes more efficient. While the delivery costs for the delivery of a message in multicast mode remain approximately the same even for larger receiver populations as shown in figure 7.2, the total signalling costs increase for higher receiver population densities. This is due to the signalling required for multicast bearer establishment and release, which is proportional to the number of receivers. Similar tendencies can be also observed for the DVB network over the whole range of $a$. In contrast the overhead required for multicast bearer establishment and release in the DVB network is lower. Therefore the delivery over the MSCH remains more efficient than unicast for all topologies, even for smaller receiver population densities.

Figure 7.7 shows the signalling costs as the function of $\delta$ considering the signalling for multicast bearer establishment and release, with $\alpha = 0.5$ and $m = m_{addr} = 2016$. In order for a MSCH to perform more efficiently than unicast signalling, a higher receiver population density is required. In the case of the UMTS network, as depicted in figure 7.7(a), the threshold for multicast delivery being more efficient is $\delta \geq 250$ for topologies A and $\delta \geq 750$ for topologies B, respectively. The threshold for the DVB network are considerably lower as shown in figure 7.7(b), due to the lower signalling overhead for bearer management. The thresholds for the different topologies are $\delta \geq 3$ for A-I, $\delta \geq 6$ for A-II, $\delta \geq 12$ for B-I, and $\delta \geq 25$ for B-II.

As seen in the previous examples, the benefits of utilising a MSCH are partly compensated by high initial costs for establishment and release of an additional multicast bearer. However the previous examples assumed only a single control message to be delivered. With an increasing number of control messages sent during a multicast session, the relative costs of the management signalling can be expected to drop.

In order to gain an understanding of this relationship, the signalling costs are evaluated as a function of the number of control message sent over a channel. Figure 7.8 shows the signalling costs for the UMTS network, considering signalling required for MSCH management. For all topologies and receiver populations it can be observed that unicast
7.1. Evaluation of the MSCH

Figure 7.6: Total costs for a single message delivery against $\alpha$ for different topologies and $m = m_{addr} = 2016$ considering signalling for multicast bearer establishment and release.
Figure 7.7: Total costs for a single message delivery as a function of \( \delta \) for all topologies with \( \alpha = 0.5 \) and \( m = m_{\text{addr}} = 2016 \).
7.1. Evaluation of the MSCH

Figure 7.8: Total signalling costs as a function of number of signalling messages sent during a session with $\alpha = 0.5$ considering signalling for multicast bearer management within the UMTS network.
7.1. Evaluation of the MSCH

Figure 7.9: Total signalling costs as a function of number of signalling messages sent during a session with $\alpha = 0.5$ considering signalling for multicast bearer management within the DVB network.
delivery costs increase much faster than the multicast delivery costs for larger number of messages. The same also applies for the DVB network, which can be observed in figure 7.9. For small receiver populations in the UMTS network several messages may have to be sent to obtain a higher efficiency when using multicast delivery. As shown in figure 7.8(a), multicast delivery pays off already when two or more messages are sent for topologies A, and six or more for topologies B. For medium or high population cases, multicast delivery is always more efficient even if the MSCH would be utilised for a single message. For the DVB network, multicast delivery mode always performs better than unicast, regardless of the receiver population.

7.1.7 Summary of observations

Using an analytical model of an UMTS and DVB network, the performance gains of the proposed MSCH have been evaluated. Signalling costs within the network were modelled as processing costs of messages within the nodes of a network and transmission costs for messages over the links between the network nodes towards the user. The model allows easy customisation to operator specific assumptions and needs, by simply changing the weights of each network node and link for an evaluation. For the performed evaluation suitable weights for the parameters have been obtained from literature or have been derived from reasonable assumptions, considering the characteristics of the network.

Initial analysis concentrated on evaluating the signalling costs for message delivery in both of the networks. The multicast delivery mode, representing message delivery on the MSCH, was compared to unicast message delivery for different receiver distributions and densities within the networks. For the comparisons a typical message delivery case on the MSCH has been assumed. In both of the networks, multicast delivery outperforms unicast delivery, especially for increasing receiver population in the networks. While unicast delivery costs steadily increase with increasing receiver populations, delivery on the MSCH converges to a constant amount, regardless of an further increase of receivers. Looking at the resources of a particular cell, this point is already reached for the first receiver in a cell, when a multicast bearer is established. The employment of an MSCH would bring performance penalties only for very sparse population cases.

Generally it can be observed that topologies with larger cell sizes are more efficient for an MSCH. This is due to the fact that they require fewer cells to cover a particular populated area and hence less aggregate radio resources need to be utilised to reach a particular receiver population. This may however not be valid for interference limited systems, such as UMTS. A larger cell size will require a greater transmission power

\[1\] The use of point-to-multipoint bearers is here assumed
at the transmitter. The resulting increase of interferences within the cell will actually lower radio resource utilisation [96]. Furthermore for sparse receiver populations, the addressing expression on the MSCH can be critical for its performance and should not exceed certain limitations, depending on network and topology. Practical evaluations, however, have shown that the addressing expression size seldomly exceeds the size of the signalling payload, even less likely for small receiver populations.

For a comprehensive analysis not only the cost for message delivery but also the cost for the management of an MSCH have to be considered. In contrast to unicast message delivery, the MSCH requires additional establishment and release of multicast bearers in the utilised signalling network. Unfortunately this involves signalling procedures that are performed for every receiver and have been found to be signalling intensive, especially within the UMTS network. These additional costs reduce the potential savings of the MSCH. Unlike the delivery costs only, the total costs on the MSCH increase for increasing number of receivers, since the signalling load for establishment and release is proportional to the receiver number.

The performance of the MSCH suffers from the management signalling in particular for sparse receiver population densities in the UMTS network. If only a few signalling messages are sent during a session, the employment of an MSCH is not be recommended for the particular case. As the signalling load on the MSCH increases, the saving will increase and may even compensate the management overhead above a certain threshold. For all other evaluated cases the MSCH outperforms unicast even considering management signalling and a low number of messages sent during utilisation. In general it can be observed that the more control signalling messages have to be sent during a session, the lower the relative impact of the management signalling and the higher the overall savings for message delivery of the MSCH.

7.2 Testbed evaluation of the group management support

The implemented prototype of the GMS, as described in section 6.1, has been tested in a real testbed environment. Purpose of the conducted experiments was to ensure the validity of developed functionality and the evaluation of the prototype performance. The first subsection briefly presents the testbed setup used for the evaluation. Then several tests are described with results of the functional validation. A critical parameter is the latency introduced by the GMS, to establish/release multicast bearers or perform vertical network handoffs. Respective delay measurement results are presented to conclude this section.
7.2. Testbed evaluation of the group management support

7.2.1 Testbed setup

For the prototype implementation, a small wireless network testbed was utilised [97]. Unfortunately no DVB or multicast enabled UMTS equipment (supporting MBMS) were available. However since both systems are expected to be conform to current IP multicast protocols, alternative access network technologies that support IP multicast were used as replacement.

Figure 7.10 shows a figure of the prototype setup within the testbed. The setup consists of CISCO hardware routers and switching equipment. As access networks WLAN (802.11b) and Ethernet (802.3) have been utilised. A WLAN access point has been used to represent a DVB network cell. Furthermore three UMTS network cells have been represented by different Ethernet subnets. In order to reflect implications of routing infrastructure, each of the subnets was attached to different router.

Three laptops where used as mobile hosts, powered by a 1.3 GHz Pentium III processor. Each of the laptops was equipped with both a WLAN and Ethernet interface. As operating system Fedora Core 3 Linux has been used. The laptops were assumed to be located in separate UMTS cells, covered by a common DVB umbrella cell. As a consequence each laptop was connected to different Ethernet subnets, while at the same time, having connectivity to the same WLAN access point. An overview of the interface name and associated networks and cells is given for each laptop in table 7.6.

The IGW manager application was setup to run on a desktop server in the network powered by a 2.8 GHz Pentium III. As the for the laptops, the server’s operating system was also Fedora Core 3 Linux. For the content provision video streaming servers
had been setup on a desktop machine in the network with comparable specification. The VLC (Video LAN client) media player [79] has been used as streaming server application.

### 7.2.2 Experimental prototype evaluation

A detailed test plan has been developed to validate the feasibility of the proposed concepts and to measure important performance characteristics of the developed GMS prototype. The testing was carried out in several test sequences, grouped in three main categories based on their test objectives:

- Functional conformance test
- Perception test
- Performance test.

Purpose of the functional conformance test was to ensure that the prototype functionality reflects the required behaviour as described by the specification. The tests were designed to cover the possible cases of protocol behaviour. Both protocol mechanisms in the GM as well as the MM were tested. It should be noted the perception test was executed in parallel with the functional conformance test, however, using only the 'observable' subset of the test sequences.

#### Functional conformance test

Functional conformance test for the MM examined two aspects: the proper handling of control messages received by the GMS, and the correct message filtering based on the
7.2. Testbed evaluation of the group management support

<table>
<thead>
<tr>
<th>Service Component</th>
<th>Multicast Group Address</th>
<th>Selected Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSCH</td>
<td>239.0.10.10</td>
<td>UTMS</td>
</tr>
<tr>
<td>LQ Flow</td>
<td>239.0.0.5</td>
<td>UTMS</td>
</tr>
<tr>
<td>HQ Flow</td>
<td>239.0.0.6</td>
<td>DVB</td>
</tr>
</tbody>
</table>

Table 7.7: Test cases and results for MM protocol conformance test.

evaluation of the addressing expression to describe a receiver subset. For the generation of required test messages, the message editor in the gateway manager has been used. As previously mentioned, the message editor allowed the specification of arbitrary control messages sent over the MSCH. A video streaming service with a high quality (HQ) and low quality (LQ) flow has been utilised for the tests. Table 7.7 shows the sample network configuration for the MSCH and offered flows.

Table 7.8 summarises important test cases used to verify correct protocol message handling by the state machine of the MM and presents the respective test results. In order to determine the correct protocol actions by the MM, `netstat`, a Linux tool, has been used. The `netstat` tool is able to print system information of the Linux networking subsystem. If used with the `netstat -groups` option, `netstat` lists the currently subscribed multicast groups for each network interface on the system. That way it could be examined if the MM has opened required sockets and joined multicast groups on the requested interfaces for MSCH and data delivery. It should be noted that the here presented test cases only represented the results of the MM state machine transitions to states, when receiving the correct control messages. Test have also been performed for each state, sending unexpected protocol messages. Purpose of these tests was to detect undesired state changes. The tests where passed successfully, since undesired state changes did not appear.

The perception test was undertaken at several stages of the functional conformance test. After the 'Multicast Bearer Setup' the high quality flow was displayed by the VLC application at all three user laptops. Likewise, a 'Vertical Network Handoff' resulted in a hardly noticeable disruption of flow. At 'Flow Handoff' and 'Network and Flow Handoff' the quality of flow changed to low and then back to high quality. Finally after a 'Multicast Bearer Release' the VLC stopped displaying service data after the receive buffer has been emptied.

As the second part of the functional conformance test, the correct processing of the addressing expression used for receiver subset addressing in the MM was evaluated. Using the message editor, message expressions covering each context information category as well as combination of them were created and transmitted on the MSCH. Only
7.2. Testbed evaluation of the group management support

<table>
<thead>
<tr>
<th>Tested Feature</th>
<th>Test Action</th>
<th>Expected Result</th>
<th>Observed Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSCH setup</td>
<td>open vlc with parameters obtained by service announcement</td>
<td>eth0: 239.0.10.10 eth1: N/A</td>
<td>eth0: 239.0.10.10 eth1: N/A</td>
</tr>
<tr>
<td>Multicast Bearer</td>
<td>send ESTABLISH message (HQ Flow, DVB)</td>
<td>eth0: 239.0.10.10 eth1: 239.0.0.6</td>
<td>eth0: 239.0.10.10 eth1: 239.0.0.6</td>
</tr>
<tr>
<td>Vertical Network</td>
<td>send MIGRATE message (HQ Flow, UMTS)</td>
<td>eth0: 239.0.10.10 eth1: N/A</td>
<td>eth0: 239.0.10.10 eth1: N/A</td>
</tr>
<tr>
<td>Handoff</td>
<td></td>
<td>eth0: 239.0.10.10 eth1: 239.0.0.5</td>
<td>eth0: 239.0.10.10 eth1: 239.0.0.5</td>
</tr>
<tr>
<td>Flow Handoff</td>
<td></td>
<td>eth0: 239.0.10.10 eth1: 239.0.0.6</td>
<td>eth0: 239.0.10.10 eth1: 239.0.0.6</td>
</tr>
<tr>
<td>Network and Flow</td>
<td></td>
<td>eth0: 239.0.10.10 eth1: N/A</td>
<td>eth0: 239.0.10.10 eth1: N/A</td>
</tr>
<tr>
<td>Handoff</td>
<td></td>
<td>eth0: 239.0.10.10 eth1: 239.0.0.6</td>
<td>eth0: 239.0.10.10 eth1: 239.0.0.6</td>
</tr>
<tr>
<td>Multicast Bearer</td>
<td>send RELEASE message (HQ Flow, DVB)</td>
<td>eth0: 239.0.10.10 eth1: N/A</td>
<td>eth0: 239.0.10.10 eth1: N/A</td>
</tr>
<tr>
<td>MSCH Release</td>
<td></td>
<td>eth0: N/A</td>
<td>eth0: N/A</td>
</tr>
</tbody>
</table>

Table 7.8: Test cases and results for MM protocol conformance test.

receivers with matching context processed the messages, other receivers discarded it. The processing module for addressing expression already underwent extensive testing during implementations with automated module tests. The manual conformance test therefore did not cover all possible combinations. Rather it was only to reassure the correct operation of the processing module for addressing expressions when integrated in the MM within a network environment.

Furthermore the GM and RM functionality was tested in a fully operational mode. In operational mode all signalling messages towards the MM were generated as required by the SCF. This is in contrast to the previous case where signalling messages were generated manually by the message editor. The developed test procedure closely reflected the service provisioning phases. In the following the phases during the operational test procedure are presented:

1. Service provider or operator configures a service at the GM using the service
7.2. Testbed evaluation of the group management support

management interface.

2. Users discover the service via a portal website and subscribe to the GMMF for a service of interest.

3. Each subscription causes an execution of the scheduling and batching function in the RM.

4. Once scheduling function determines the service start, network and flow selection is performed in the RM.

5. The RM annotates its decision in an internal data structure and triggers SCF to establish required multicast bearers at the receivers.

6. The SCF starts the video servers for the selected flows and generates messages in the MSCH to trigger the establishment of the selected multicast bearers.

7. After the session ends the SCF generates required messages for the release of previously established bearers and sends them on the MSCH.

In order verify correct operations of GM and RM functionality, displays as well as message logging functionality have been implemented in the gateway manager. One display allowed to view the internal state of a group within the GM, while another was showing the current resource availability. The tests have been repeated for different resource conditions and receiver heterogeneity cases. In the following the tests that have been performed at each of the stages, are briefly summarised. Vertical handoff functionality could not be evaluated in the operational test, since no dynamic resource management algorithm was available that could make use of this feature. Both vertical network handoff and flow handoff operations, however, have been already verified in the previous tests using the manual mode.

1. Provider Side GM Primitives Test The purpose of this test was to verify the correct operation of the group management primitives provided towards the service provider/operator after service configuration. The creation of the group, uniqueness of user ID, as well as the configured service parameters were examined.

2. User Side GM Primitives Test This test verified the correct operation of the group management primitives towards the user. After a subscription to the group for a service the internal group state was examined, if the user performing the subscription, has been successfully added and relevant context information has been obtained from the data bases.
3. **Batching and Scheduling Test** This test examined the correct operation of the batching and scheduling function. The scheduling time was compared to the expected time defined by the initial configurations.

4. **RM Algorithm Test:** This test examined the correctness of the RM algorithms after network and flow selection have been performed. The resource view as well as user view were utilized for this test. Allocated service flows and networks have been verified, based on the current user context and network resource information.

5. **Session Setup Test:** The purpose of this test was to verify the behaviour of the SCF at session setup. Message generated by SCF to establish multicast bearers were logged into trace files and examined by their correctness. In addition, establishment of the required multicast bearers was verified at the receivers. The launch of the applications providing the data sources of the flows was finally confirmed.

6. **Session Release Test:** The final test aimed to verify the SCF functionality at session release. As in the previous test, the messages generated for message release were logged into a trace file and examined for their correctness. Furthermore, the resulting multicast bearer releases were verified at the receivers.

**Performance test**

Experiments have been performed in order to derive multicast bearer setup and vertical handoff performance of the implemented prototype. The evaluation has focused on the following three performance metrics:

- Session setup delay
- Vertical handoff delay
- Packet loss during handoff

In contrast to the conformance test, all three user terminals were located in the same UMTS cell (Ethernet subnet). Measurements have been performed at each of the users, in order to consider effects of different hardware. The experiments consisted of two parts to evaluate the overhead of the MM on the system performance. In the first part a network initiated bearer setup has been performed and the bearer setup delay was measured. In the second part, a vertical group handoff has been performed from WLAN to Ethernet, and vertical handoff delay as well as packet loss has been
7.2. Testbed evaluation of the group management support

Figure 7.11: Timeline of significant events during session setup and vertical handoff using the GMS.

determined. The experiment was repeated 20 times and measured each user terminal independently.

All measurements have been performed at the receiver terminals, using system time stamps collected within the MM. The time stamps were obtained by the `gettimeofday` system function, which works with microseconds resolution. Figure 7.11 gives an overview of the timeline of important events during a multicast session using the GMS at the receiver and shows how the examined delay metrics have been determined.

Bearer setup delay \( t_{\text{setup}} \) has been calculated as the difference of time between the reception of an ESTABLISH message from the GM, \( t_e \) and the time \( t_{\text{fp}} \) the first data packets arrives on the established bearer path:

\[
    t_{\text{setup}} = t_{\text{fp}} - t_e.
\]

Table 7.9 shows the impact of the MM on the setup delay at the three receivers. Both mean values and standard deviation are presented in the table. In the best case the average setup delay is only 15.9 msec as experienced at receiver C. Considering the processing of outgoing and incoming messages at the network device driver and interface cards, networking stack as well as the IGMP processing at the router, the delay penalties added by the middleware seem arguably small. Average values for other receiver experiences are slightly larger with 22.5 msec at receiver B and 33.0 msec at receiver A, although all receivers have been located within the same subnet. This relates to the fact that different wireless network cards, were used at each of the receivers. As can be seen, the performance is partly dominated by the processing of the wireless network interface card and their respective device drivers at the receivers. In summary, an average setup delay of 23.8 msec was measured during the experiments.
7.2. Testbed evaluation of the group management support

<table>
<thead>
<tr>
<th></th>
<th>μ/ms</th>
<th>σ/ms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver A</td>
<td>33.01</td>
<td>3.53</td>
</tr>
<tr>
<td>Receiver B</td>
<td>22.45</td>
<td>1.18</td>
</tr>
<tr>
<td>Receiver C</td>
<td>15.86</td>
<td>1.45</td>
</tr>
</tbody>
</table>

Table 7.9: Mean (μ) and standard deviation (σ) of session setup delay at receivers.

<table>
<thead>
<tr>
<th></th>
<th>μ/ms</th>
<th>σ/ms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver A</td>
<td>10.70</td>
<td>4.54</td>
</tr>
<tr>
<td>Receiver B</td>
<td>11.01</td>
<td>5.46</td>
</tr>
<tr>
<td>Receiver C</td>
<td>11.34</td>
<td>5.36</td>
</tr>
</tbody>
</table>

Table 7.10: Mean (μ) and standard deviation (σ) of handoff delay at receivers.

Likewise, the vertical handoff delay has been calculated as the difference between the time of receiving a MIGRATE message, \( t_m \), from the GM and the time of receiving the first data packet, \( t_{fph} \), via the newly established bearer path:

\[
    t_{\text{handoff}} = t_{fph} - t_m
\]

Table 7.10 shows the different delays for each receiver measured during the 20 sessions. Differences in delay due to the interface, as with the setup on the wireless network, are hardly observable for the wired interfaces. The average handoff delay for receivers are around 10.7msec and 11.3 msec. The handoff delay is quite low, due to the small scale of the testbed environment. Also it should be noted that an Ethernet or WLAN based environment relies simply on standard IETF IP multicast mechanisms. The signalling procedures for the establishment of a multicast bearer in UMTS network are far more complex and would introduce notable delay. It is therefore important that the latency introduced by mechanisms for multicast bearer management should be kept as low as possible. The MM easily meets these requirements, with an overall system performance of around 11 msec.

Finally the packet loss was examined during the handoff phase. In order to measure the packet loss, the RTP sequence number of incoming data packets was examined shortly before, during and after the handoff phase. Since the MM uses a make before break mechanism, in other words, releases the old bearer only after data on the new multicast bearer has been received, there is virtually no packet loss. However depending on the network scenario and data rate, packets with a slightly lower or higher sequence number could theoretically arrive at the new multicast bearer path, resulting in lost or
duplicate packets. In these cases MM just passes the packets to higher layers, relying on transport protocols such as RTP to take care of error recovery.

### 7.3 Simulation study of IGMP extension

This section presents an evaluation of the IGMP extensions proposed in chapter 5. While the IGMP extensions provide enhanced functionality as compared to the conventional group management model, these newly added mechanisms also introduce additional signalling. A simulation model has been implemented, in order to evaluate the introduced protocol overhead of the IGMP extensions. Purpose of this evaluation is to prove the scalability of our approach for different scenarios. The evaluations show that even for a large number of hosts on a subnet, the introduced overhead is not much greater than of current IGMP. Compared to the bandwidth savings, which can be obtained by the delivery coordination of the IP multicast data traffic, this overhead is negligible.

The simulation study has been performed using the discrete event simulator OPNET Modeler 11 [48]. The standard model for IGMPv2 has been modified to support operation of multiple interfaces on a host and to reflect our proposed extensions.

Three simulation scenarios have been chosen to compare the proposed protocol extensions (IGMP+) with conventional IGMPv2 and to evaluate their scalability. As a performance metric the protocol overhead has been measured while varying the number of participating hosts for a particular multicast group on a subnet. In the first two scenarios, 100 hosts with two network interfaces were considered to be connected to two different subnets. The last scenario considered 100 hosts with three network interfaces, each attached to one of three different subnets. The number of participating hosts for a multicast group was varied between 10 and 100 for each run. Default timer values and protocol parameters for IGMP have been assumed throughout the simulations. Furthermore the IGMP protocol has been assumed to already operate in a steady state, e.g. startup operations to discover initial membership on a link have not been considered.

The remainder of this section describes the simulation scenarios and presents comparing results of the proposed extensions to the conventional group management model.

#### 7.3.1 Protocol overhead for continuous operation

This experiment was conducted to observe the protocol overhead introduced in IGMP+ as a function of the number of participating hosts on a subnet, assuming a multicast
group is disabled on a subnet in the IGMP+ case for the whole duration of a session. Hosts were subscribing to a multicast group providing constant bit rate video service at a data rate of 128 kbit/s. The inter-arrival process used to join and leave the group was assumed to be Poisson (with $\lambda = 1/600$ per sec). 100 cycles (join and leave) per host were performed for each simulation run and the results averaged over the number of cycles. Furthermore an average over 10 independent runs has been found to provide a sufficiently small confidence interval at a confidence level of 95%. Each of the hosts selected a preferred interface for joining the multicast group with one half of hosts preferring the interface attached to subnet 1 and the other half the interface on subnet 2.

Two simulation sets were performed. The first set assumed normal IGMPv2 operation. The second set assumed IGMP+ operation with the multicast group disabled at the router's interface on subnet 1. Signalling load for each IGMP message has been measured separately and included Version 2 Membership Report (Report), Leave Group (Leave), General Query (General), Group Specific Query (GSP Query) and the added Redirect Request (Redirect). The total IGMP related signalling load (Total) corresponded to the sum of all these message on a subnet.

The resulting protocol overhead for the two simulation sets is depicted in figure 7.12, considering the signalling load for each involved protocol message. Figures 7.12(a) and 7.12(c) show the required signalling load for the IGMP case in subnet 1 and subnet 2 respectively. As expected no Redirect messages are sent on either subnet, since they exist only in the proposed protocol modifications. The signalling load on both networks is the same for all messages of the protocol, since an equal number of users have their preferred interface for joining a multicast group on either subnet. Only the signalling load caused by membership reports increases with increasing number of hosts.

Figure 7.12(b) shows the IGMP+ signalling load on subnet 1. The number of membership reports is considerably lower than in conventional IGMP, since hosts with preferred interface on subnet 1, will send a membership report only once, before being redirected to join the multicast group on the other subnet. As expected, the signalling load contributed by the introduced redirect messages corresponds to the number and also overhead of the received membership reports. The signalling load for both the membership reports and redirect request increases with larger number of participating hosts. No leave requests and group specific queries are sent for the disabled multicast group. The amount of general queries is the same for both cases, since IGMP+ keeps operating as IGMP for other enabled groups. The signalling load for the IGMP+ case is depicted in figure 7.12(d). Since all interested hosts subscribe to this subnet, the load due to membership reports is up to 30% higher. For other messages the signalling load for both cases is approximately the same. As expected no redirect message are
7.3. Simulation study of IGMP extension

Figure 7.12: Protocol overhead vs. number of participating hosts in scenario 1.

Figure 7.13: Total protocol overheads.
sent on this subnet.

A direct comparison of the total signalling loads is given figure 7.13(a). The total signalling load on subnet 1 is slightly lower for the IGMP+ case, but matches the IGMP load for large number of participating hosts. In contrast, the total signalling load in subnet 2 is higher for the IGMP+ case, due to the double number of hosts subscribed to it. When comparing the overall load, in all subnets the IGMP+ protocol overhead exceeds the conventional IGMP overhead for a number beyond 15 participating hosts. While an increase of IGMP+ signalling load was expected due to the added redirect message and additional rejoins, the modified protocol still remains scalable even for large number of hosts due to the linear increase.

Figure 7.13(b) shows the IGMP+ to IGMP overhead ratio (IOR) defined as follows:

\[
IOR = \frac{IGMP^+}{IGMP} \times 100\%
\]

where a value below 100 indicates signalling load savings and a value above the required overhead as compared to the unmodified IGMP protocol. The overall added overhead by the proposed extensions is reasonably small and does not exceed 30% even for 100 participating hosts. The overhead due to the protocol operation becomes negligible, with regard to the savings that can be achieved in not being required to forward the session data for a multicast group in both of the subnets.

7.3.2 Protocol overhead considering a load balancing example

The second experiment was undertaken to observe the IGMP+ protocol overhead for a interface redirection during a multicast session. In this scenario all receivers initially joined a multicast session on their preferred interface. Then half way through the session, load balancing was performed from subnet 1 to subnet 2 as part of the scenario. Load balancing was triggered by disabling the multicast group on the router interface attached to subnet 1. This caused all subscribed receivers on subnet 1 to be redirected to subnet 2. As in the previous experiment, a set of experiments with conventional IGMP have been performed as a reference. Users joins/leaves where generated by a Poisson process with \((\lambda = 1/300s)\) at the first half of a session and in the second half respectively. 100 consecutive sessions were performed for each simulation run and the results averaged over the number of sessions. Furthermore an average over 10 independent runs has been found to provide sufficient confidence.

Figures 7.14(a) and 7.14(b) show the required signalling load for the IGMP reference case and the IGMP+ in subnet 1. The load caused by membership reports is lower for the IGMP+ case, since members are redirected to subnet 2 after half of the session.
7.3. Simulation study of IGMP extension

Figure 7.14: Protocol overhead vs. number of participating hosts.
7.3. Simulation study of IGMP extension

- Total signalling load: IGMP v t IGMP+ IGMP* IGMP overheard (lOR]

Figure 7.15: Total protocol overheads.

The signalling load for the redirect message in this experiment is independent of the number of participating hosts and remains very low. Only a single redirect message needs to be send after disabling the multicast group, regardless of the number of receivers in the subnet. That way interface redirection can be performed in a scalable manner even for a large numbers of receivers.

The protocol overhead for membership reports on subnet 2 is larger for IGMP+ case as can be observed from figures 7.14(d). This was expected after a redirection, due to the rejoin of the hosts previously subscribed on subnet 1.

The total signalling load for both cases is depicted in figure 7.15(a). While the total signalling load in the IGMP+ signalling case is lower than the reference case for all number of hosts, it is on the other hand higher on subnet 2. The overall total signalling load is only slightly higher for the IGMP+ case for more than 20 participating hosts. The total IGMP+ to IGMP overhead ratio is less than 20% as shown in figure 7.15(b), even for up to 100 participating hosts in a subnet.

7.3.3 Protocol overhead considering three access networks

The third experiment was conducted in order to evaluate the IGMP+ performance for network assisted interface redirection. With two interfaces available, a host in the previous scenario was only left with the choice to reselect the other available interface after the reception of a redirect request. Hosts with multiple interfaces have more options, if a multicast group is disabled on more than one subnet. On the other hand they may suffer the dilemma, which interface to chose for a rejoin. Most likely they may be probing several interfaces, before a join may be successful.

As mentioned in section 5.4, a network operator can optionally provide a network prefix (NP) to direct a host to join on an interface attached to a specific subnet. That way a
host does not require probing and can directly select the interface where a join would be successful. The additional NP, however, increases the message size of the redirect request. It is therefore important to observe the impact on the protocol overhead for both cases.

Two sets of simulations were performed, one with and one without the use of the optional NP. Each host possessed three network interfaces, each of them attached to a separate subnet. Participating hosts in a simulation run joined a multicast group on one of three subnets. At the time of the subscription, each host specified an ordered interface preference list, which was determined by a uniform distribution out of the 6 possible combinations. The multicast group was disabled on subnet 1 and subnet 2, so hosts could join a multicast group successfully only on subnet 3. As in the Scenario 1, the inter-arrival process used to join and leave the group was assumed to be Poisson (with $\lambda = 1/600$ per sec). 100 cycles (join and leave) per host were performed for each simulation run and the results averaged over the number of cycles. Furthermore an average over 20 independent runs have been found to provide sufficient confidence.

Figure 7.17 shows the overall protocol overhead for the two cases in the three subnets. The left column of figures shows the case with NP. As expected the signalling load on subnet 1 and subnet 2 are the same due to the uniformly distributed interface preference. The same observation can be made for figures 7.16(b) and 7.16(d) in the right column, which depict the case with optional NP in the redirect message. While the signalling load of the redirect request matches the signalling load of membership reports in the case without NP, the signalling load for redirect is higher in the case with NP. This can be explained by the larger message size required to accommodate the NP. The total signalling load, however, for case with NP is lower regardless of the number of participating hosts as compared to the case without NP. The number of join attempts in the case without NP is higher, since hosts with an interface on subnet 2 being 3rd preference need an additional probe on a different subnet. The protocol overhead on subnet 2 is the same for both cases as shown in figures 7.16(e) and 7.16(f), since all hosts will be eventually redirected to that subnet.

Figure 7.17(a) summarises the total protocol overhead in the different subnets and the overall total protocol overhead. The use of a NP reduces required protocol overhead, especially for larger numbers of participating hosts. In order to evaluate the gains of using a NP we defined an efficiency parameter as follows:

$$\text{Efficiency} = (1 - \frac{\text{Overhead with NP}}{\text{Overhead without NP}}) \times 100\%$$

The higher the efficiency the better the performance improvement when using a NP. The efficiency of network prefix use is depicted in figure 7.17(b). While the perfor-
7.3. Simulation study of IGMP extension

(a) IGMP+ signalling load on subnet 1 without network prefix.

(b) IGMP+ signalling load on subnet 1 with network prefix.

(c) IGMP+ signalling load on subnet 2 without network prefix.

(d) IGMP+ signalling load on subnet 2 with network prefix.

(e) IGMP+ signalling load on subnet 3 without network prefix.

(f) IGMP+ signalling load on subnet 3 with network prefix.

Figure 7.16: Protocol overhead vs. number of participating hosts considering the availability of three network interfaces.
7.4. Testbed evaluation of the IGMP extensions

The simulations in the previous sections provided an evaluation of the scalability of the proposed IGMP extensions, by analysing the resulting signalling load for different host numbers on a subnet. In this section, an evaluation of a prototype of the proposed IGMP extensions in a real testbed environment is presented. Besides successfully demonstrating the functionality of the developed protocol extensions, the purpose of the testbed evaluation is to gain additional insights in the delay introduced by the protocol extensions. The first part of this section gives a brief overview of the testbed setup and gives an example for the use of modified API. Then the results obtained from the experiment are presented.

7.4.1 Testbed setup

The proof-of-concept prototype consisted of two Linux based laptop computers, and the required network infrastructure such as routers and switches and a network server, hosting a video server application. Figure 7.18 gives an overview of the testbed setup used for the experiment. Both laptop computers were equipped with an Ethernet and WLAN interface. One laptop computer acted as router and implemented the routing
7.4. Testbed evaluation of the IGMP extensions

daemon as well as the protocol extensions as described in section 6.3. The other router acted as host and implemented the host side extension as described in section 6.4.

The host connected to the Linux based router via a WLAN interface, which acted as WLAN access point for the host. The Linux based router in turn was connected to the network infrastructure with its wired Ethernet interface. As seen in the figure, the Ethernet interface of the host were connected to different subnet of the network infrastructure.

As evaluation scenario for the experiment a multicast based video streaming application has been considered. In order to make use of the features of the IGMP protocol extensions at the host, the application has to be adopted to provide a list of available interfaces through the new API. For this purpose, the network related code in the video streaming client, in this case the VLC media player [79], had to be adopted to use the new socket options instead.

7.4.2 Testbed results

The experiment examined the delay a host experiences, when it is not served by the initially chosen subnet, but instead redirected to join via a different network interface. For this purpose the multicast group 239.0.10.10, offering the video service, has been disabled on the the Linux based router R1. Figure 7.19 shows the message sequence during the redirect process and indicates where the delays were measured at the different stages. The host initially joins the multicast group on the WLAN interface by sending a membership report to R1. Since the multicast group has been disabled, R1 replies with a redirect message. The host receives the redirect message after time $t_{\text{redirect}}$ and passes it to the IIM for the socket for interface reselection. The IIM selects the next
interface in the provided list, which is the Ethernet interface and rejoins the multicast group. When the new membership report leaves the new interface, time \( t_{\text{rejoin}} \) has already elapsed. The router R2 receives the membership report and starts forwarding the multicast traffic on the subnet attached to the host's Ethernet interface. The delay from the initial join, up to the first data packet arriving on the new interface is defined as \( t_{\text{data}} \).

Unlike in the GMS approach, the signalling exchange as well as processing takes place solely in kernel space. Instrumenting the relevant portions of the kernel with mechanisms to generate time stamps for the delay measurement represents a rather difficult task. Therefore \textit{Ethereal} \[98\] one of the most commonly used network protocol analysers, has been utilised for the delay measurements instead. \textit{Ethereal} runs as application with super user privileges on the host and allows to capture a trace of all incoming and outgoing packets on its network interface with time stamps relative to the system clock.

Measurement of 20 independent sessions have been performed for the host. Table 7.11 summarises the mean delay values and their standard deviations obtained during those experiments.

The actual delay penalty as opposed to the case, where a host would join directly on the right interface is expressed by \( t_{\text{rejoin}} \), with an average of approximately 5.2 msec.
## 7.5 Qualitative comparison of approaches

This chapter provided an evaluation of the GMS and the proposed IGMP extensions. Both approaches introduce mechanisms to achieve coordinated multicast delivery in the presence of multiple access networks and given that respective interfaces are available at the receivers. Each of those solution, however, follows a different approach to achieve delivery coordination. The GMS provides a session layer approach by introducing a multicast middleware on top of existing multicast mechanism on the terminal side, and an additional network support in form of group manager in the network. It requires no modification to existing IP multicast mechanisms in the network. The second approach, in contrast, provides a network layer solution by modifying IGMP to achieve the required coordination.

Each of those solutions has its advantages and disadvantages, which need to be understood. Therefore a qualitative comparison of those is provided in this section, while discussing both their advantages and their deficiencies. For the discussion following characteristics are considered:

- Protocol overhead
- Scalability
- Deployment complexity

### Table 7.11: Mean (µ) and standard deviation (σ) of delay measurements performed for IGMP extensions.

<table>
<thead>
<tr>
<th></th>
<th>µ/ms</th>
<th>σ/ms</th>
</tr>
</thead>
<tbody>
<tr>
<td>t_redirect</td>
<td>2.11</td>
<td>0.11</td>
</tr>
<tr>
<td>t_rejoin</td>
<td>5.17</td>
<td>0.41</td>
</tr>
<tr>
<td>t_data</td>
<td>7.50</td>
<td>1.32</td>
</tr>
</tbody>
</table>

This is quite acceptable for any multicast application and not even notable to the user. For increasing network size, the roundtrip time between multicast router and host may increase slightly and hence the delay penalty. A larger increase is however not expected, since IGMP signalling only takes place within the local subnet. The delay until the first multicast data arrives on an interface \( t_{data} \), with an average of 7.5 msec can be also regarded as overall delay for establishment. A vertical handoff initiated by the network by sending a redirect message on an interface would take even shorter, since the time for the initial join to reach the router could be deducted.
7.5. Qualitative comparison of approaches

- Coordination capabilities and features
- Security
- Reliability

Protocol overhead can be expressed in terms of signalling overhead as well as additional delay introduced by the proposed mechanisms, and provides an indication of their performance. The XML based signalling messages used by the GMS are generally larger than the redirect message introduced in the IGMP extensions. For bearer establishment or vertical handoff the signalling load of the session layer solution will be typically larger than the network layer solution, especially if receiver subset addressing is required on the MSCH. This observation however does not include the signalling needed to enable or disable a multicast group on a specific for the case of the IGMP extensions. Also in terms of delay the networks layer solution requires the lower overhead. This is due to the fact that the mechanisms are implemented as part of the TCP/IP networking stack within the operating system kernel. Signalling in the session layer approach traverses the whole networking stack and the required message processing takes place in user space.

Both approaches provide a scalable solution, even for large numbers of receivers as seen in the previous evaluations. The GMS achieves the scalability by using the MSCH to carry control signalling to the receiver group. For very large receiver groups the GM in the network may become a problem. Furthermore the GM represents a single point of failure. A distributed server architecture could be utilised to host the GM to circumvent this problem. Also multiple GM can be utilised to host different multicast services to balance the load for popular multicast services. The network layer approach based on the IGMP extensions, in contrast, does not rely on a central entity such as the group manager. Each router handles decentralised the protocol operations for its users on the subnet.

The deployment complexity differs for both approaches. The network layer approach requires the update of IGMP protocol entities both on router side and at the hosts. Although only minor modifications have been applied to the existing code, the deployment may be considered difficult. While new routers or hosts operating systems may ship the modified version per default, existing systems need to be updated. The update requires the kernel source on the host and routers to be patched and recompiled. Furthermore, existing applications need to be enhanced to support the new functionality by using the provided API. The session layer approach in contrast is easier to deploy, since no modifications to existing multicast mechanisms are needed. The GMS only requires the deployment of a the GM as part of interworking gateway in the network and
the installation of an additional library for the MM on the receiver side. Furthermore legacy applications are supported by the MM without the need of modifications.

The GMS offers a richer set of coordination capabilities as the network layer solution. While the IGMP based solution only allows change of access network for a particular multicast group, the GMS allows the complete change of underlying network layer connection. Hence, not only the access network but also the service flow can be seamlessly changed during a session, by changing the IP multicast and port number of the network layer connection. Furthermore GMS allows the consideration of receiver heterogeneity e.g. terminal capabilities, preferences, context, when access network selection by the resource management is performed. The IGMP based solution only considers receiver preferences locally by specification a prioritised list of interfaces. Thus if the network operators decides to disable the multicast group on a particular subnet, a receiver may remain unsupported if no other interface and/or access network is available at the receiver.

Both approaches may be vulnerable to security threats. A malicious attacker may for example hijack or interfere with the delivery coordination of the GMS by sending wrong control messages to the MSCH of a multicast service. Source specific multicast could be utilised for the MSCH to filter unwanted source sending to the multicast group in the network or at the receivers. Another alternative would be to use security mechanisms on the MSCH to protect from false messages. In case of the IGMP based approach an attacker could send spoofed redirect messages to the receivers to prevent users from accessing a multicast group on a subnet. Since IGMP only operates within a subnet only a local attacker could be successful.

Finally it should be mentioned that both approaches use best effort delivery and thus unreliable multicast mechanisms. Although no problems have been encountered in the testbed environment, packet loss and thus loss of control signalling message may be encountered when operated in larger scale network environments. In order to ensure reliable delivery for the session layer approach, additional reliable multicast protocols could be utilised. Reliable delivery can be also achieved on different layers e.g. by choosing a signalling network for the MSCH with appropriate link layer support. Since IGMP operates directly on IP, no transport layer reliability is available. IGMP however only operates within the subnet. Current reliability is achieved by repeating the signalling message. The number of repetitions is tunable by the so called robustness variable. As IGMP, the session layer approach could use repetition of signalling messages on the MSCH, of course at costs of a higher signalling load.

Table 7.12 summarises the differences of both solutions with respect to the previously discussed characteristics.
### Table 7.12: Test cases and results for MM protocol conformance test.

<table>
<thead>
<tr>
<th></th>
<th>Session Layer (GMS)</th>
<th>Network Layer (IGMP+)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Overhead</td>
<td>Low due to MSCH, dependent on receiver subset addressing expression</td>
<td>Very low, proportional to number of receivers, lower handoff latency</td>
</tr>
<tr>
<td>Scalability</td>
<td>Good, for many receivers distributed GM may be required, single point of failure</td>
<td>Very good since distributed to local subnets</td>
</tr>
<tr>
<td>Deployment Complexity</td>
<td>Easy, only installation of GM in network and MM library on terminal required</td>
<td>More complex, requires code changes to every router and host</td>
</tr>
<tr>
<td>Coordination Capabilities</td>
<td>Advanced, capable of considering receiver heterogeneity</td>
<td>Simple, no receiver heterogeneity can be considered</td>
</tr>
<tr>
<td>Security</td>
<td>Attack possible from anywhere in the network, application of security mechanism on MSCH recommended</td>
<td>Only local attacks possible</td>
</tr>
<tr>
<td>Reliability</td>
<td>Best effort, use of reliable multicast protocols possible, message repetition on MSCH</td>
<td>Best effort, message repetition</td>
</tr>
</tbody>
</table>
Chapter 8

Conclusions

This thesis addresses problems faced for the delivery of multicast services in a next-generation wireless networking environment. The overhead of management signalling for the multicast bearer plane is significantly larger in future wireless systems such as MBMS, as compared to existing mechanisms on the wired Internet. This may result in unnecessary strain on the already scarce wireless network resources, especially for services where users are expected to change bearer services more frequently during a session. In addition, mobile terminals may be equipped with a multitude of network interfaces and provide their users with the capability to access desired services via multiple available access networks. Using the current, purely receiver driven multicast mechanisms, content may be delivered unnecessarily via multiple access networks to the same location. In order to utilise network resources more efficiently, network operators would like to coordinate the delivery of multicast services in such an heterogeneous network environment. Unfortunately, the current multicast service model does not provide the required mechanisms to support such delivery coordination.

In this thesis extensions to existing MBMS mechanisms have been presented that allow a significant reduction in the signalling load for provisioning location based multicast services. Several location based flows can now be delivered concurrently over a single multicast bearer service, thus avoiding the change of bearer service when moving into a new service area. Furthermore two incremental solutions to achieve multicast delivery coordination in a heterogeneous wireless network environment have been proposed. Group management support has been presented as a session layer solution, offering network operators the capability of network initiated multicast bearer establishment and release, vertical network and flow handoff for groups of receivers interested in a multicast service. Group management support is based on existing multicast mechanisms and does not require their modifications or changes to the multicast service application. As a network layer solution, the current Internet group management protocol has
been adapted to consider the availability of multiple interfaces at the receiver. Delivery coordination is achieved by redirecting multicast receivers on particular subnets to establish the session on an alternative subnet. A summary of the specific contributions made in this thesis can be found in section 1.2.

Despite the appearance of novel techniques and advances in wireless communication technologies, the wireless medium will remain a scarce resource and the bottleneck of future wireless communication networks. In contrast, communication bandwidth in wired network infrastructure as well as processing capabilities of network equipment advance at a much faster pace. Therefore, approaches that reduce signalling overhead over the wireless link and instead put the strain on processing within the network infrastructure will contribute to a more scalable future network environment. This concept has been demonstrated as part of the proposed MBMS extensions for location based service delivery.

The availability of multiple access networks together with the existence of multiple network interfaces at the host provides new opportunities as well as challenges for both multicast receivers and network operators in future wireless network environments. Giving each user the choice to select the network for the delivery of a multicast service and blindly delivering the traffic according to its decisions, as is currently done within the multicast service model, will in many cases result in inefficient data delivery. While the choice of the service should unquestionably remain with the user, the choice of the delivery network could be deferred to the network operator with the possibility of considering the preference of users. Intelligent resource management in the operators network can then select appropriate delivery paths and service flows to allow efficient delivery of multicast services to groups of receivers in such a heterogeneous network environment. In order to achieve such delivery coordination across multiple networks, novel mechanisms are required. The two presented approaches within this thesis provide incremental solutions to implement such delivery coordination, based on existing multicast protocols and mechanisms.

All software implementations presented in this thesis can be made available by the author on explicit request.

8.1 Future work

Despite the intention to tackle the most important issues arising in next generation wireless networks for multicast service delivery, many more issues still remain unanswered. A brief discussion of other remaining research issues as well as possible extensions to the contributed solution are given below.
The proposed mechanism for MBMS is based on the assumption that a downlink node, e.g. RNC, is connected to exactly one uplink node, e.g. SGSN, within the delivery tree of the MBMS multicast bearer service. In case an RNC maintains Iu bearers to multiple SGSNs, e.g. if the network operator employs Iu-Flex, modifications need to be made to the proposed mechanisms. The required modifications are left for further study.

Another problem is the alignment of local service areas with the structure of MBMS cell groups, which share a common PDCP and RLC entity in the RNC. Furthermore, a replacement of the flow label by the source unicast address and possibly source port number as an identifier for location-specific flow could be investigated.

The presented solutions for multicast delivery coordination provide necessary mechanisms for directing receivers to multicast bearers on respective access networks. However, additional resource management mechanisms in networks are required to determine suitable delivery networks and service flow according to the conditions in the available networks and heterogeneity of receivers. Novel resource management algorithms and architectures have already started to appear but still remain an extensive area for research.

Group management support as well as such resource algorithms rely on the knowledge of up-to-date receiver context information. Mechanisms for efficient gathering of such information and their accurate update offer a wide exploration space for further investigations.

Also, IGMP extensions implement coordination mechanisms only between routers and the multicast receivers. The proposed solution provides an interface to enable or disable multicast groups at the router via the configuration of access lists. How such access lists are efficiently configured have not been tackled by this thesis. The prototype provides a simple UDP-based protocol for demonstration purposes only. Efficient remote configuration of a potentially large number of router interfaces is still subject for further study. A potential solution would be the integration of such an interface into the internet standard management framework.
Appendix A

Additions to Evaluations

A.1 Costs considering multicast bearer management in UMTS network

In the following layer 3 signalling costs are derived according to the signalling procedures defined in the MBMS specification [9]. A successful completion of those procedures is assumed for the analytical model.

The service activation procedure can be thus decomposed into message exchanges with the following signalling load contributions:

- $s_{\text{igmp}}$: IGMP Join message
- $s_{\text{notif}}$: MBMS Notification Request and Response
- $s_{\text{create}}$: Create MBMS Context Request and Response
- $s_{\text{link}}$: MBMS UE Linking Request and Response
- $s_{\text{act}}$: Request MBMS Context Activation
- $s_{\text{req}}$: Activate MBMS Context Request
- $s_{\text{act}}$: Activate MBMS Context Accept

Summing up the message exchange the total signalling costs for MBMS multicast bearer service activation for a single user can expressed as:

$$ s_{\text{act}}^{(U)} = s_{\text{igmp}} + s_{\text{notif}} + s_{\text{act}} + s_{\text{req}} + s_{\text{create}} + s_{\text{link}} + s_{\text{act}}. \quad (A.1) $$

The IGMP join request is exchanged between UE and GGSN. Since IGMP join request is a higher layer PDU, it is transferred as a RANAP direct transfer message ($m_{rda}$) between RNC and SGSN and GTP-PDU message ($m_{pdu}$) between SGSN and GGSN.
Thus the signalling costs can be defined as, with \( m_{\text{join}} \) being the message size for an IGMP join message:

\[
s_{\text{sigmp}} = m_{\text{join}} \times (c_g + t_{gs} + c_s + t_{sr} + c_r + t_{rn} + c_n + t_{nu}) + m_{\text{pdus}} \times (c_g + t_{gs}) + m_{\text{rdts}} \times (c_r + t_{sr}). \tag{A.2}
\]

The MBMS Notification Request and Response message exchange takes place between GGSN and SGSN. With \( m_{\text{req}} \) being the message size of the notification request and \( m_{\text{res}} \) being the message size of the notification response, the signalling costs are computed as:

\[
s_{\text{notif}} = m_{\text{req}} \times (c_g + t_{gs}) + m_{\text{res}} \times (c_g + t_{gs}). \tag{A.3}
\]

Likewise the Create MBMS Context Request and Response signalling messages are also exchanged between SGSN and GGSN. The signalling costs for the message exchange with \( m_{\text{req}} \) being the size of the Create MBMS Context Request message and \( m_{\text{res}} \) the message size of the Create MBMS Context Response is thus:

\[
s_{\text{create}} = m_{\text{req}} \times (c_g + t_{gs}) + m_{\text{res}} \times (c_g + t_{gs}). \tag{A.4}
\]

MBMS UE Linking Request and Response signalling takes place between SGSN and RNC. The signalling costs for the message exchange with \( m_{\text{req}} \) being the size of the MBMS UE Linking Request message and \( m_{\text{res}} \) the message size of the MBMS UE Linking Response is thus:

\[
s_{\text{link}} = m_{\text{req}} \times (c_r + t_{sr}) + m_{\text{res}} \times (c_r + t_{sr}). \tag{A.5}
\]

The three SM messages Request MBMS Context Activation, Activate MBMS Context Request and Activate MBMS Context Accept are exchanged between UE and the SGSN, with \( m_{\text{req}}, m_{\text{res}} \) and \( m_{\text{accept}} \) being their respective message sizes. SM message are also carried as higher layer PDU across the RANAP interface. The signalling cost for sending the three messages can be thus derived as:

\[
s_{\text{act}} = m_{\text{req}} \times (t_{sr} + c_r + t_{rn} + c_n + t_{nu}) + m_{\text{rdts}} \times (c_r + t_{sr}) \tag{A.6}
\]
\[
s_{\text{req}} = m_{\text{req}} \times (c_a + t_{sr} + c_r + t_{rn} + c_n + t_{nu}) + m_{\text{rdts}} \times (c_a + t_{sr}) \tag{A.7}
\]
\[
s_{\text{accept}} = m_{\text{accept}} \times (t_{sr} + c_r + t_{rn} + c_n + t_{nu}) + m_{\text{rdts}} \times (c_r + t_{sr}). \tag{A.8}
\]

Inserting equations A.2 - A.8 into equation A.1, the total signalling costs for bearer
service activation can thus be rewritten to:

\[
S_{\text{act}}^{(U)} = c_g \times (m_{\text{join}} + m_{\text{pdu}} + m_{\text{mreq}} + m_{\text{mres}} + m_{\text{mreq}} + m_{\text{mres}}) + \\
\left[ c_g \times (m_{\text{join}} + m_{\text{pdu}} + m_{\text{mreq}} + m_{\text{mres}} + m_{\text{mreq}} + m_{\text{mres}} + 2 \times m_{\text{rdt}}) + \\
(\tau_m + c_a + \tau_u) \times (m_{\text{join}} + m_{\text{mreq}} + m_{\text{mres}} + m_{\text{mreq}} + m_{\text{mres}} + 2 \times m_{\text{rdt}}) \right]
\]

Furthermore, the multicast service deactivation procedure can be also decomposed into message exchanges with the following signalling load contributions:

- \( s_{\text{leave}} \): IGMP Join message
- \( s_{\text{udeact}} \): MBMS UE Context Deactivation Request and Response
- \( s_{\text{del}} \): Delete MBMS Context Request and Response
- \( s_{\text{delink}} \): MBMS UE De-Linking Request and Response
- \( s_{\text{dreq}} \): Deactivate MBMS Context Request
- \( s_{\text{dres}} \): Deactivate MBMS Context Response

The sum of the individual signalling load contributions is the total signalling cost for MBMS multicast bearer service deactivation for a single user:

\[
S_{\text{deact}}^{(U)} = s_{\text{leave}} + s_{\text{udeact}} + s_{\text{dreq}} + s_{\text{dres}} + s_{\text{delink}} + s_{\text{del}}.
\]  

The IGMP leave message is sent by the UE to the GGSN. Analogously to the join request, the signalling costs can be defined as follows, with \( m_{\text{leave}} \) being the message size for an IGMP leave message:

\[
s_{\text{igmp}} = m_{\text{leave}} \times (c_g + \tau_g + c_a + \tau_m + c_m + \tau_u + m_{\text{pdu}} \times (c_g + \tau_g) + m_{\text{rdt}} \times (c_g + \tau_g)).
\]

The MBMS UE Context Deactivation Request and Response message exchange takes place between GGSN and SGSN. With \( m_{\text{dreq}} \) being the message size of the notification request and \( m_{\text{dres}} \) being the message size of the notification response, the signalling costs are computed as:

\[
s_{\text{notify}} = m_{\text{dreq}} \times (c_g + \tau_g) + m_{\text{dres}} \times (c_g + \tau_g).
\]
MBMS UE Linking Request message and \( m_{\text{dir}} \) the message size of the MBMS UE Linking Response is thus:

\[
s_{\text{delink}} = m_{\text{dir}} \times (c_r + t_{sr}) + m_{\text{dir}} \times (c_s + t_{sr}). \tag{A.13}
\]

Create MBMS Context Request and Response messages are exchanged between SGSN and GGSN. The signalling costs for the message exchange with \( m_{\text{req}} \) being the size of the Create MBMS Context Request message and \( m_{\text{res}} \) the message size of the Create MBMS Context Response is thus:

\[
s_{\text{det}} = m_{\text{req}} \times (c_g + t_{gs}) + m_{\text{res}} \times (c_s + t_{gs}). \tag{A.14}
\]

Finally the SM messages Deactivate MBMS Context Request, Deactivate MBMS Context Response are exchanged between UE and the SGSN, with \( m_{\text{req}} \), \( m_{\text{res}} \) being their respective message sizes. The signalling cost for sending the two messages can be thus derived as:

\[
s_{\text{der}} = m_{\text{req}} \times (t_{sr} + c_r + t_{rn} + c_n + t_{nu}) + m_{\text{dir}} \times (c_r + t_{sr}) \tag{A.15}
\]

\[
s_{\text{des}} = m_{\text{res}} \times (c_s + t_{sr} + c_r + t_{rn} + c_n + t_{nu}) + m_{\text{dir}} \times (c_s + t_{sr}). \tag{A.16}
\]

Using the derived equations A.11 - A.16, the total signalling costs for bearer service deactivation in equation A.10 can be expressed as:

\[
S_{\text{deact}}^{(U)} = c_g \times (m_{\text{meane}} + m_{\text{pd}u} + m_{\text{ud}res} + m_{\text{dir}req}) + t_{gs} \times (m_{\text{meane}} + m_{\text{pd}u} + m_{\text{ud}res} + m_{\text{dir}req} + m_{\text{dir}res}) + c_s \times (m_{\text{meane}} + m_{\text{ud}res} + m_{\text{dir}req} + m_{\text{dir}res} + 2 \times m_{\text{dir}}) + t_{sr} \times (m_{\text{meane}} + m_{\text{dir}req} + m_{\text{dir}res} + m_{\text{dir}req} + m_{\text{dir}res} + 3 \times m_{\text{dir}}) + c_r \times (m_{\text{meane}} + m_{\text{dir}req} + m_{\text{dir}res} + m_{\text{dir}res} + m_{\text{dir}}) + (t_{rn} + c_n + t_{nu}) \times (m_{\text{meane}} + m_{\text{dir}req} + m_{\text{dir}res}) \tag{A.17}
\]

Considering the costs for multicast bearer establishment and release for every receiver, the total costs for the signalling delivery over the MSCH when provided over a multicast bearer in the UMTS can be summarised as:

\[
S_{\text{MSCH}}^{(U)} = [t_{gs} + c_s + n_s \times (t_{gs} + c_s) + n_r \times (t_{sr} + c_r) + n_n \times (t_{rn} + c_n + t_{nu})] \times N_m \times m^* + (S_{\text{act}}^{(U)} + S_{\text{deact}}^{(U)}) \times N_{rx} \tag{A.18}
\]
A.2  Costs considering multicast bearer management in DVB network

Unlike in UMTS, DVB standards do not (yet) specify any network architecture or procedures to establish IP multicast bearers. Furthermore the current concepts of IP service provision over DVB-H/T assume bearer establishment to be network initiated, e.g. for mobile TV services to cater for DVB only receivers. Users receive a service announcement of upcoming multicast sessions via an EPG and can tune their receiver to an interested session by locally enabling the reception of a multicast group. No interaction with the network is therefore required. Network initiated bearer establishment, however has the disadvantage that a multicast bearer would have to be established in all cells of the network, regardless if interested receivers are present or not. In order to selectively establish multicast bearers in cells with only interested receivers within a DVB network, knowledge of interested receivers for an IP multicast group is required. As a consequence an alternative access network interface as return channel, e.g. UMTS, is needed at the receiver.

Dynamic establishment of multicast bearers in the DVB network can be achieved by mechanisms such as UDLR [27]. In the presence of an alternative return link, UDLR allows normal IP operations over a unidirectional link by a layer 2 tunneling mechanism. That way standard IETF mechanisms such as IGMP can be utilised to perform the necessary IP group management operation. Assuming the employment of UDLR, IGMP join and leave requests can then be tunneled directly to the respective DVB/IP gateway via an alternative access network.

On the other IGMP signalling from every user could be avoided by using the network management functionality of the group manager. The NMF could trigger the DVB/IP gateways for the location, where users are present, to establish the required multicast bearers. This would however bypass existing IETF mechanisms.

For the signalling load evaluation, the employment of UDLR over a UMTS return link and normal IGMP operation are assumed. Each user establishes a multicast bearer on the DVB network, by sending an IGMP join message via the UMTS network path to the IP/DVB gateway located at the DTS of the user cell. It is assumed that the message is tunneled between the two IoN gateways to the DVB distribution network via the interworking link.

With $m_{join}$ being the size of the IGMP message, the resulting signalling costs for a single user for bearer establishment can be computed as:
A.2. Costs considering multicast bearer management in DVB network

Analogously, the signalling costs for the release of a multicast bearer for a single user can be written as:

\[ S_{\text{act}}^{(D)} = m_{\text{join}} \times \left( t_{\text{tg}} + c_g + t_{\text{gs}} + c_s + t_{\text{er}} + c_r + t_{\text{rn}} + c_n + t_{\text{nu}} + \ight. \\
\left. t_{\text{id}} + c_d + t_{\text{dt}} + c_t + t_{\text{tu}} \right) \]  \hspace{1cm} (A.19)

Considering the costs for multicast bearer establishment and release for every receiver, the total costs for the signalling delivery over the MSCH using a multicast bearer in the DVB network can be summarised as:

\[ S_{\text{MSCH}}^{(D)} = \left[ t_{\text{id}} + c_d + n_t \times \left( t_{\text{dt}} + c_t + t_{\text{tu}} \right) \right] \times N_m \times m^* + \left( S_{\text{act}}^{(D)} + S_{\text{deact}}^{(D)} \right) \times N_m \]  \hspace{1cm} (A.21)
Publications

This thesis is based in part of work included in the following publications:

Conferences:
A. Gluhak, K. Moessner and R. Tafazolli, *Controlled Multicast User Service Delivery in Heterogeneous Wireless Networks*, IEICE General Conference, Osaka, Japan, March 2005


Journals:
A. Gluhak, M. Inoue, K. Moessner and R. Tafazolli, *Signalling Channel for Coordinated Multicast Service Delivery in Heterogeneous Wireless Networks*, IEICE Transactions on Communications (Accepted)


Bibliography


[7] “3rd Generation Partnership Project (3GPP), www.3gpp.org, last access on the 17.05.2006.”


[15] “Open Mobile Alliance (OMA), www.openmobilealliance.org, last visit on the 17.05.2006,”.


[44] “IST FP5 Convergence of IP-based Services for Mobile Users and Networks in DVB-T and UMTS Systems (CISMUNDUS) project website: www.iist,”.


[48] “OPNET Technologies Inc., www.opnet.com, last access on the 17.05.2006,”.


[62] "Extensible Markup Language, www.w3.org/xml, last access on the 17.05.2006,”.


[84] "PIMd - A PIM-2 sparse mode multicast router for Linux, homepage: netweb.usc.edu/pim, source download: freshmeat.net/projects/pimd, last access on the 17.05.2006," .


