Efficient and Scalable Protocols to Support Source Specific Multicast (SSM) Over Mobile IPv6 Networks

Gopakumar Kurup

B.Eng in Electronics and Electrical Engineering
MSc. in Microwaves and Optoelectronics

A Thesis submitted to
The Department of Electrical and Computer Systems Engineering
Monash University, Australia
for the degree of Doctor of Philosophy

July 2006

Contents

List of Figures

List of Tables

Abstract

The research presented in this thesis offers novel methods developed to improve IPv6 multicast performance for mobile users in wireless networks.

Data delivery through multicasting is becoming increasingly important in parallel with the accelerating trend towards all-IP-wireless-network designs. The existing protocol standards for multicasting called Any Source Multicast (ASM) are burdened with a myriad of interlaced components and found to be too complex for successful large scale deployments. The recently proposed Source Specific Multicast (SSM) method simplifies the multicast (or group communications) architecture on the Internet. The SSM model is seen as the most promising and realistic group communication solution to date. But, to ensure a wider adoption, it still requires design improvements, especially for mobile devices. A core component to support the SSM model is a protocol capable of specifying the multicast source address, similar to IPv4 group management (Internet Group Management Protocol Version 3 – IGMPv3). In IPv6 networks, Multicast Listener Discovery Version 2 (MLDv2) has been proposed to provide the ability to specify the multicast source address to enable SSM.

Since SSM and MLDv2 have been proposed recently, their behaviour and dynamics are not known. In addition to this, protocols and mechanisms designed for traditional wired networks do not always transfer efficiently to mobile or wireless systems. This research seeks answers to these issues, and focuses on the challenges and trade-offs for distributing multicast traffic efficiently in a mobile IPv6 network. The analysis study performed in the first part of this thesis, through a theoretical framework and subsequent simulation experiments, reveals the MLDv2 performance shortcomings previously unknown to the research community. To rectify this, a new method called Adaptive Listener Tracing (ALT) is proposed in this thesis. The experiments conducted with the ALT algorithm show better link bandwidth utilisation and significant MLDv2 performance improvements. Also, the optimal protocol settings are deduced through an extensive study of bandwidth utilisation efficiency and tuning effects of the MLDv2 protocol variables.

The second part of this thesis identifies the current problems related to preserving multicast sessions during movement and offers solutions to achieve a seamless service. The increasing need for mobile Internet devices to maintain communications during movement has led to the trend of relying on the network (or Internet Protocol – IP) layer for mobility management. One such protocol to provide session mobility

is Mobile IPv6 (MIPv6), which is in the process of development and standardisation. Although the primary concern in MIPv6 design is to maintain unicast sessions, it recommends the use of remote subscription or bi-directional tunneling methods for multicast data delivery. When multicast listeners move and subsequently reattach to another part of the network, MLDv2 cannot be relied upon to update the multicast group management in a timely manner to ensure a seamless multicast data delivery. In order to reduce the multicast latencies caused by node movements, an extension of the Layer-2 triggered handover mechanism is implemented and evaluated in this thesis. With mandatory MLDv2 support (and per-host tracking capability) for all IPv6 hosts, which caters for better authentication, authorization and accounting, the results in this thesis show that a Layer-2 triggered mechanism offers an efficient and elegant MIPv6 SSM solution.

Past experience of Internet usage shows that, a protocol (regardless of capability) without an integrated security solution will not be widely adopted. Due to the one-to-many (and generally, high data rate) nature of multicast applications, securing multicast networks and minimising potential abuse is important for a successful deployment. Since MLDv2 is a new protocol and an important component of SSM, a security and threat analysis for MLDv2 is essential as a part of this research. The security considerations are deduced in this thesis by identifying various trust models for the MLDv2 protocol, their functionality and interactions with link-layer and multicast proxy devices. The findings and results from the MLDv2 security and threat analysis are presented in the third and final part of the thesis.

Declaration

I declare that this thesis does not contain any material previously accepted for the award of any other degree or diploma at any university or institution; and that to the best of my knowledge, this thesis contains no material previously published or written by any other person, except where due reference is made in the text.

Gopakumar Kurup
Melbourne
July 2006

Acknowledgments

My utmost gratitude to my supervisors Dr. Ahmet Şekercioğlu and Dr. Nallasamy Mani for their continuous encouragement and guidance throughout the candidature and completion of this thesis. The funding from MIMOS Berhad and the Australian Telecommunications CRC made the research possible. To the CTIE researchers, thank you for all the discussions, banter and coffee. To Mahizzan Mohd Fadzil, Dr. Mohamed Awang Lah and Dr. Richard Nelson for encouraging me to start this journey. To Amma, Acha and Shoba, thank you for the all the love and strength, without which none of this would have been possible nor have any significance.

para mis padres

Glossary

bid-down	the switching of MLDv2 backward compatibility to MLDv1
granularity	mode a qualitative indicator of the MLDv2 discriminating ability for multicast group management
handoff	the Layer-2 host re-attachment (between APs) due to movement
handover	the host Layer-3 information reconfiguration due to movement
host-suppression	multicast hosts on the same subnet do not need to respond when MLDv1 report messages with similar listening states are detected
join latency	the MLDv2 group management updating latency due to host movement
leave latency	the time elapsed between the last multicast host leaving a network attachment and the continued delivery of multicast data to that link
Layer-2	the Data Link Layer in the OSI model.
Layer-3	the Network Layer in the OSI model.
link	an IPv6 defined common communication medium below the IP-Layer
link-up	a deterministic event associated with a Layer-2 connection between a host and a AP

MLDv2 proxy	a device which forwards MLDv2 query and report messages on behalf of hosts and multicast routers which are not directly connected
multicast handover latency	the time elapsed between a multicast host re-joining a network attachment and continue receiving multicast data through movement
snooping switch	a Layer-2 switch which uses a forwarding algorithm based on the network (Layer-3) information

List of Acronyms

AAA	Authentication, Authorization and Accounting
AH	Authentication Header
ALT	Adaptive Listener Tracing
API	Application Protocol Interface
AP	Access Point
AS	Autonomous System
ASM	Any Source Multicast
BGP	Border Gateway Protocol
BSD	Berkeley Software Development
BSSID	Basic Service Set Identification
BT	Bi-directional Tunneling
BU	Binding Update
CBT	Core Based Tree
CGA	Cryptographically Generated Address
CoA	Care of Address
CSR	Current State Report
CTP	Context Transfer Protocol
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuration Protocol
DMA	Dynamic Multicast Agent
DMSP	Designated Multicast Service Provider
DR	Designated Router
DVMRP	Distance Vector Multicast Routing Protocol
ESP	Encapsulating Security Payload
EXPRESS	Explicit Request Single Source
FA	Foreign Agent
FN	Foreign Network
GQ	General Query
GSAKMP	Group Secure Association Key Mgmt. Protocol
HA	Home Agent
HN	Home Network
IANA	Internet Assigned and Numbers Authority
ICMP	Internet Control Management Protocol
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol

IRTF	Internet Research Task Force
IP	Internet Protocol
IPSec	Internet Protocol Security
LAN	Local Area Network
LLQC	Last Listener Query Count
LLQI	Last Listener Query Interval
LLQT	Last Listener Query Time
MA	Multicast Agent
MAGMA	Multicast and Anycast Group Management
MAR	Multicast Address Record
MASSQ	Multicast Address Source Specific Query
MALI	Multicast Address Listener Interval
MBGP	Multicast Extensions to BGP version 4
MBone	Multicast Backbone
MHA	Multicast Home Agent
M-HBH	Multicast Hop By Hop
MIP	Mobile Internet Protocol
MLDv2	Multicast Listener Discovery Version 2
MN	Mobile Node
MoM	Mobile Multicast Protocol
MOSPF	Multicast Open Shortest Path First
MR	Multicast Router
MRD	Maximum Response Delay
MSA	Multicast Support Agent
MSDP	Multicast Source Discovery Protocol
MSEC	Multicast Security
MSLR	Modified Source List Record
MSF	Multicast Source Filter
MSNIP	Multicast Source Notification of Interest Protocol
NAT	Network Address Translator
ND	IPv6 Neighbour Discovery
OSPF	Open Shortest Path First
P2P	Peer to Peer
PIM	Protocol Independent Multicast
PIM(sm/dm)	PIM routing in (sparse mode/dense mode)
QI	Query Interval
QQIC	Querier Query Interval Code
QR	Querier Router
QRI	Query Response Interval
QRV	Querier Robustness Variable
RBMoM	Range Based Mobile Multicast Protocol
RGMP	Receiver-initiated Group Membership Protocol
RIP	Routing Information Protocol
RA	Route Advertisement
RFC	Request For Comment
RP	Rendezvous Point

RPF	Reverse Path Forwarding
RS	Remote Subscription
RTCP	Real Time Control Portocol
RTP	Real Time Transport Portocol
RV	Robustness Variable
SDP	Session Directory Protocol
SEND	Securing Neighbour Discovery
SCR	State Change Report
(S,G)	(Source, Group) multicast channel
SSID	Service Set Identifier
SSM	Source Specific Multicast
TRPF	Truncated Reverse Path Forwarding
UDP	User Datagram Protocol
WG	(IETF Standards) Work Group

List of Symbols

η	MLDv2 signaling traffic overhead efficiency
N_{CSR}	Number of Current State Report messages
N_{G}	Number of multicast groups
N_{ll}	Number of last listener
N_{MN}	Number of Mobile Nodes per link
N_{SCR}	Number of State Change Report messages
N_{S_i}	Number of multicast sources per mode
R_{ACC}	Access network bandwidth
R_{MLD}	MLDv2 traffic data rate during QI
$R_{\mathrm{MLD}_{\mathrm{LLQI}}}$	MLDv2 traffic data during LLQI
R_{APP}	Application data rate
T_{Assoc}	Layer-2 Re-association Latency
T_{Auth}	Layer-2 Re-authorisation Latency
T_{JL}	Join Latency
T_{L2}	Layer-2 Latency
T_{LLQI}	Last Listener Query Interval
T_{LL}	Leave Latency
T_{MALI}	Multicast Address Listener Interval
T_{MH}	Multicast Handover Latency
T_{MSF}	Multicast Source Filter Latency
T_{MRD}	Multicast Response Delay
T_{Probe}	Layer-2 Probe Latency
T_{QI}	Query Interval
T_{QRI}	Query Response Interval
T_{RE}	Router Re-election Interval
T_{S_i}	Source Timer in `include` Mode

Chapter 1

Multicasting in a Mobile Environment

1.1 Background and Motivation

Multicasting aims to support one-to-many or *group* communications in an efficient and scalable manner using a set of Internet based protocols. The advantage of multicasting is that a source only generates and sends a single data packet to reach a group of hosts (identified by a common Internet Protocol multicast address). The multicast routing protocol used by intermediate routers allows them to replicate data packets as required and forward the copies when interested hosts exist on their downstream interfaces. Multicasting ensures only a single data packet is transmitted on any given link regardless of the number of hosts it serves. The resultant potential bandwidth saving is immense, especially for the delivery of high bandwidth applications to a large audience. The efficiency of multicasting enables the provisioning of multimedia broadcasts[1] and delay-sensitive applications to bandwidth limited access technologies, in particular wireless networks, which was not possible before.

Multicasting is designed to support *broadcast-like* applications on the Internet where the same data set is of interest to multiple listeners (i.e., hosts that wish to receive the same data packets). Without multicasting, the unicast alternative requires the source to send multiple data packets (containing the same information) to all listeners simultaneously. In most circumstances, a unicast mechanism will not scale efficiently, especially if there is a large listener base. Multicasting allows

---

[1] An IPv6 multicast television service was demonstrated in Japan recently as part of the 4th MEDIA broadcasting and Video On Demand service. http://www.ipv6style.jp/en/action/20040902/index.shtml

the senders' *distribution cost*[2] to remain at *one unit* irrespective of the number of listeners present because the source does not need prior knowledge of who, where or how many listeners there are. The (small) initial setup cost of the source is almost independent of current or future number of listeners, making multicasting a highly scalable service.

The pervasive availability of multicasting protocols across the Internet will enable cheap, efficient and easy to set up broadcasting technologies. Current terrestrial broadcast systems are encumbered by the physical location (and limitations) of transmitters and receivers, government licensing, legislations and censorship. The expensive start up costs and a tightly regulated industry have inhibited a highly participatory and vibrant broadcasting environment. On the other hand, a multicast source can be easily set up using only a personal computer and Internet access bandwidth of a single application data stream it serves. Multicasting will drastically lower the cost and barrier of entry to provide Internet broadcast applications to potentially all Internet Protocol (IP) enabled devices anywhere in the world.

The need for a diverse and thriving broadcast community is becoming increasingly important. Large and concentrated broadcast networks lead to only profit driven and homogeneous content made available for the mass market. A number of factors have led to the consolidation of a small number of big media companies around the world[3]. Firstly, the deregulation of the communications market has allowed (the previously restricted) cross ownership of companies which create content and those which distribute it. Secondly, in tandem with most other trade and commercial activities, media distribution and broadcasting channels have become borderless and global in reach and coverage. A complementary and alternative distribution technology will ensure that fringe, cultural or less commercially attractive content will have a means to reach an audience.

New Internet technologies and applications present unprecedented opportunities to change the way we communicate. For example, the popularity of Internet based publishing (web logs or blogs) points to a latent demand for different information sources other than commercial ones available in the current marketplace. Similarly, peer-to-peer[4] (P2P) [ATS04] file sharing networks gained much popularity in distributing pre-recorded material especially music. However, P2P services have

---

[2] This includes Internet access bandwidth, multicast source processing power and other distribution associated equipment and infrastructure cost.

[3] In the U.S. alone, during the 2003 Federal Communication Commissions media ownership review, the data showed that 85 percent of media sources were owned by only 5 companies.

[4] A P2P network relies on the computing power and bandwidth of the participants within the network rather than concentrating it in a relatively few servers.

been taken to task[5] for the presence of copyrighted material on the distribution network. The P2P technologies were not designed to assist copyright infringements but to facilitate efficient sharing of digital content files and real-time data, such as telephony traffic. In effect, the legal action taken by the recording industry is trying to eliminate a technology which does not discriminate the distributed material on its networks according to copyright terms.

The constant lobbying and increase of copyright terms[6] are also perceived to have long term negative consequences to society as a whole. Traditionally (upon copyright expiry), this freely available material and knowledge were used extensively and built upon for future works. A leading thinker of copyright issues, Lessig [Les04] points out that with current copyright trends, concentrated control over content creation and distribution will lead to the diminishing of works in the public domain. New technologies will encourage the design of alternative commercial content distribution models and adoption of new copyright[7] schemes. Multicasting and complementary P2P networks will be an integral part in supporting and shaping future content creation and distribution [TSKK03].

Internet based broadcast-like data delivery schemes will only succeed if there is a viable and complementary mechanism for the end devices to receive the distributed content. The trend is for most networks and end devices to rely on the network (IP) layer for connectivity and mobility functions. The fourth generation cellular telephony networks will be entirely packet-switched and use many of the protocols evolved from today's Internet. The All-IP-wireless-network designs are further encouraged by the acceptance of Mobile IP and IEEE 802.11x access technologies. The use of license free (or public) frequency spectra in IEEE 802.11x based access schemes is also very attractive from cost and performance perspectives. With pervasive Internet availability, broadcast-like and delay-sensitive content delivery to mobile devices (anywhere and any time) using multicasting becomes a distinct possibility.

---

[5] The legal action initiated by the recording industry against Napster and Kazaa in the U.S. and Australia respectively are recent examples.

[6] The Sonny Bono Copyright Term Extension Act passed by the U.S Congress in 1998 increased the existing term for an additional duration of 20 years.

[7] The Creative Commons is one such example which presents multiple and varied rights for the content creator to choose from. http://www.creativecommons.org

1.2 Basic Concepts

Data packets are sent towards and reach a particular host in the Internet identified by a unique address, in a similar fashion to the current postal service. In the Internet, an IP address serves as a unique endpoint identifier for the destination host and the address is used by other hosts to initiate and maintain communications. In the case of multicasting, the communication entails a data source sending (the same) information destined to a group of hosts. The early motivation for multicasting was to devise an efficient and scalable data delivery mechanism to a group of receivers (i.e., multicast listeners). The original IP multicast design had to fulfill the following three requirements:

- a source can transmit User Datagram Protocol[8] (UDP) traffic to a certain multicast address without registering or scheduling transmission,
- (any number of) sources can transmit to the same multicast address without group membership knowledge, and
- multicast listeners can join and leave the group at will.

The initial multicast model was proposed to the Internet Engineering Task Force (IETF) community by Deering and Cheriton [DC85]. The idea was to extend the existing IP identifiers for a group or class of addresses, reserved for multicasting. Any number of hosts interested in a multicast session would have to know the particular address in use, and adopt that multicast address to start listening. When a host wants to stop listening, it can discard the multicast address to stop receiving the data packets. Multicast routers and other network devices conspire to deliver the data packets, in spite of the multicast source not having any knowledge of the listeners and vice versa. Subsequent revisions and refinement finally culminated in the RFC 1112 [Dee89] specification which is the definitive reference and commonly termed as the Any Source Multicast (ASM) model. In the ASM model, any source can send data packets destined to any multicast address. Thus, ASM supports both the one-to-many and many-to-many group communication models.

IP mobility is the network layer protocol support for continuous communications as hosts move around in the Internet. The basic challenges for devices depending on the IP layer for mobility functions are:

---

[8] UDP is a lightweight, simple and efficient datagram transport protocol. UDP is widely used for streaming audio and video because there is no time to retransmit erroneous or dropped packets.

- to maintain the application session connectivity even though the host's IP address changes whenever it moves and reattaches to a different point of the network, and
- to achieve reachability in spite of host movement in a scalable manner without the need for host-specific routes to be propagated throughout the Internet routing infrastructure.

The Mobile IP protocol is designed to support transparency above the IP layer, including maintenance of active applications, during host movements. Mobile IP [Per96], is the standard pursued by the IETF with the initial Mobile IPv4 (MIPv4) standard [Per02][9] supporting IPv4 hosts. Similarly, Mobile IPv6 (MIPv6) [JPA04] is the standard to manage mobility for IPv6 systems.

The initial motivation for designing the next generation IP (Internet Protocol version 6 – IPv6) was the impending IPv4 address exhaustion due to the exponential growth of the Internet. The introduction of Network Address Translators (NATs) [SH99, SE01] provided a possible solution but hid several nodes using private[10] addresses behind a common global[11] address. Transparent routing between hosts in the private network and the external Internet is facilitated by a NAT router. The usage of NATs however, hinders P2P applications and communications initiated from outside the private NAT configured network domain.

IPv6 is designed with the success and prior experience of IPv4 and will potentially reach into larger spheres of communication devices and networks. Some of the IPv6 [DH98] advantages over IPv4 include:

- a larger address space of 2^{128} (compared to 2^{32} for IPv4) [HD98],
- an auto-configuration mechanism allowing hosts to generate their own addresses [TN98],
- built-in authentication header [KA98b] and encryption [KA98c] for security provision at the IP layer,
- destination options in headers which gives it inherent mobility support [DH98, Section 4.6], and
- mandatory multicast support for all hosts [Lou04] and easier multicast address management with well defined administrative regions.

---

[9] The current standard is being discussed and in the process of revision at the IETF at present [Per05].

[10] Address realm independent of external network addresses.

[11] Addresses in the public realm with unique assignment by IANA or equivalent address registry.

With a large public address space, integrated security and efficient routing, IPv6 will encourage more applications to be designed for the Internet platform. The simple protocol extensions for mobility and plug-and-play features of IPv6 augurs well for supporting mobile devices using wireless access on the Internet.

1.3 Challenges and Solutions

Early attempts at multicast protocol designs were done without a clear understanding of commercial requirements or robust implementation strategies. Many of the multicasting architecture complexities arise from including mechanisms to address too many issues too broadly. Often, these issues have conflicting requirements, like the considerations for one-to-many and many-to-many information delivery models. In the ASM model, any source can send multicast data packets destined to any multicast address. Applications such as online gaming and video-conferencing, in which some or all of the participants become data sources, are examples of the many-to-many model.

In the ASM model, the multicast host does not know the IP address of the data sources associated with the multicast groups it listens to. An additional network device is required to discover the source IP address for each multicast group. When a host expresses interest in listening to a multicast group, all of the data sources of that group must be determined for data to be delivered to the interested host. The ASM model relies on a Rendezvous Point (RP) for the source discovery mechanism. The RP is shared by all multicast sources to distribute data within a configured network domain. All multicast data distribution in a network is anchored at the RP and commonly termed as a shared multicast tree model. Hence, the RP is potentially a hot spot for multicast traffic and a single point of failure. The RP and other additional protocols required to provide interdomain source address discovery for ASM cause major complexities as discussed in more detail in Section 2.2.1.

Applications that are believed to possess the greatest potential for commercial viability on the Internet use the one-to-many, or broadcast-like model [CMK$^+$02]. The newly proposed Source-Specific Multicast (SSM) supports multicast data delivery from one specified source for a multicast group. The key distinguishing SSM property is that, hosts subscribe to a multicast 'channel' identified by the combination of an unicast source address and a multicast group address. The SSM model sacrifices the many-to-many functionality and shifts the source discovery responsibility to the hosts. SSM eliminates the need of many intermediate protocols and devices required for ASM, thus radically simplifying the multicast data delivery mechanism.

A core component of the SSM model is a protocol capable of specifying the multicast source address, similar to IPv4 group management (Internet Group Management Protocol Version 3 – IGMPv3). In IPv6 networks, Multicast Listener Discovery version 2 (MLDv2) has been proposed to provide the multicast listener host with the ability to specify the source address for each multicast group. MLDv2 is also used by IPv6 multicast routers to discover the presence of SSM listeners on directly attached links, and which multicast channels are of interest to those neighboring hosts.

Multicast routing protocols build data delivery trees which are shaped by multicast group management updates. Multicast group management reflects the joining and leaving of multicast listener hosts. In mobile networks, multicast group management has an added complexity of host movements leading to changes in their network point of attachment. The network (i.e. routing protocol) needs to be updated with this movement if the host is to continue receiving multicast data. Ideally, upon movement to a new link, a host should also leave multicast groups on the previous link as quickly as possible. Current multicast group management protocols do not take possible host movement into consideration and hence, their updating latencies and resultant performance in mobile environments are not well understood.

In Mobile IP systems, a Home Agent[12] (HA) in the Home Network (HN) provides the mobility management functionality when a host moves to a Foreign Network (FN). The host acquires a new IP address, called the Care-of-Address (CoA), from a Foreign Agent (FA) server when it moves to a FN and updates the HA with its new address. While in the FN, the data packets destined for the mobile host are intercepted at the HA and encapsulated within another IP packet and sent to the FA. The FA decapsulates the data packets and forwards it to the mobile host. The encapsulation and decapsulation process of packets between the HA and FA is also known as tunneling. Data packets from the mobile host can be sent directly from the FA and routed towards the corresponding host because its destination IP address in known.

Although conceptually simpler than unicast since multicast addresses are not tied to any one individual link, subnet or network topology, mobile multicast has its own set of unique constraints and challenges. Problems still exist for the various protocols which have been proposed to support a mobile multicasting architecture. The resultant research topics can be broadly categorised into several issues as il-

---

[12] Usually in the form of a software module running in a router.

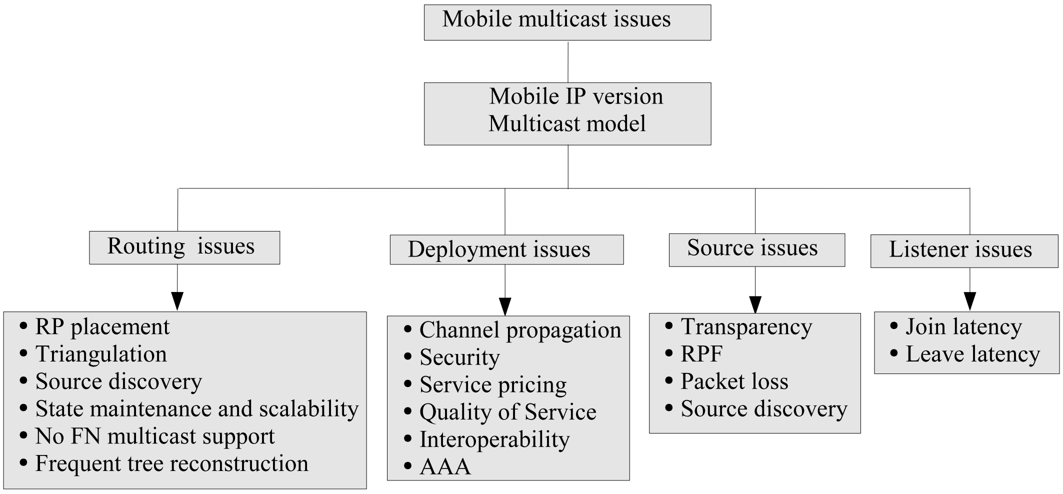


Figure 1.1: A general overview of mobile multicast issues and challenges [RKL+04].

lustrated [13] in Figure 1.1. The first challenge is to determine whether to use the (many-to-many) ASM or (one-to-many) SSM model. The next issue is to evaluate the multicast data handling mechanisms proposed by the different MIP versions. The rest of this section provides an overview of general problems affecting mobile multicasting, starting with the routing issues.

In the ASM model, the RP needs to be pre-configured and placed within the network prior to the construction of a multicast data delivery tree. Without a mechanism to predict host distribution or movements in a mobile network, the RP might not be ideally nor optimally located. When multicast traffic has to go through the RP, it does not necessarily use the shortest data delivery path between the source and multicast listeners. This phenomenon is commonly termed as 'routing triangulation'. The further away the RP is located from the hosts it caters for, the worse the delay and packet processing effects of the routing triangulation. The RP placement considerations and the ideal location are ASM routing issues which need to be addressed.

In the Internet, individual network boundaries are defined by Autonomous System (AS) numbers. Unicast routing information is peered between different AS networks through border routers running Border Gateway Protocol (BGP) sessions. Multiprotocol BGP (MBGP) is an enhanced BGP feature that carries IP multicast addresses and routes. The multiprotocol feature adds the capability to exchange multicast routing information throughout the Internet and to connect multicast

---

[13] The figure was first illustrated by Romdhani et al. [RKL+04]. For the purpose of this research, MIPv6, SSM and access network based challenges have been included.

topologies between different networks. In the ASM model however, inter-domain multicast scalability is almost impossible as there is no specific mechanism for multicast source addresses to transverse network domain boundaries. The Multicast Source Discovery Protocol (MSDP) [FM03] was proposed as a stop gap measure but it was not widely adopted to exchange multicast source address information between network domains. As a result of these routing complexities, multicast services are virtually non-existent in today's commercial networks providing Internet services.

MIP systems provide session continuity for multicast communications in a similar tunneled fashion as unicast packets. Multicast data reception however, does not have the same unicast issues regarding IP address changes when network boundaries are crossed as discussed in Section 1.2. The MIP specified Bi-directional Tunneling (BT) [JPA04, Section 10.4.3] method ensures the availability of multicast services (similar to the HN) when the host is roaming in a FN. BT means that while multicast sessions are continuously available, additional propagation and processing latencies are induced by the packets' path via the HN. The indirect path taken by the data packets causes routing inefficiency. Additional routing states need to be maintained for every tunnel and once the upper of states held is breached, the multicast scalability properties are affected. The workings of BT are discussed in detail in Section 2.4 and illustrated in Figure 2.6a.

MIPv6 also specifies an alternative mechanism to support multicast hosts which relies on the FN multicast services. This mechanism is known as Remote Subscription (RS). The use of RS eliminates multicast tunneling and maintains the optimal shortest path routing between the multicast source and the mobile hosts. The RS method ensures multicast scalability with no requirement to maintain tunneling states. However, RS might not be suitable for high mobility scenarios with the need for frequent routing tree re-constructions. The unavailability of multicast routing support in the FN is also a concern for the RS method.

Mobile multicast sources pose an even more complex problem where its IP address changes, by moving to a FN. In the ASM model, unless the source receives an explicit notification from one of its listeners after it moves, it will not forward any data from the new network. In the SSM model, the effects of source IP address changes is even more pronounced since multicast channels are identified by the combination of multicast source and group addresses. Multicast listeners of an existing channel have no means of knowing about the source movement and the subsequent address changes. Maintaining a transparent multicast service with source movement is therefore important. Due to the security concerns and routing policies of the FN, a source may not be able to forward multicast data. There is also a possibility of data packet loss while the host moves and reattaches to another network.

There also exists an array of mobile multicast deployment issues which have not been addressed. There are no established mechanisms for SSM channel information (i.e. source and group address) propagation. The pervasive availability of the SSM channel information throughout the network is essential but especially difficult to ensure in mobile environments. Unlike ASM, SSM allows for each multicast listener to be tracked but Authentication, Authorisation and Accounting (AAA) mechanisms are yet to be implemented and tested rigorously. To ensure commercial viability of multicast services, Quality of Service (QoS) provisioning, service pricing and interoperability between Internet Service Providers (ISP) have to be addressed as well.

1.4 Critical Issues and Research Aims

Mobile IP and multicasting are important technologies to support multimedia content distribution over the Internet but are not widely deployed to date and remain largely in the realm of research. The major challenges thus far, include efficiency, scalability and security problems affecting the underlying proposed protocols. The newly proposed SSM and MIPv6 protocols have potentially better designs, features and functionalities to overcome the problems of the older protocols. Both of the protocols provide a promising way forward and have been proposed as future IETF standards. However, an in depth analysis of the inter-working and interaction of both protocols are lacking to date. The preliminary research results of the protocols warrant and encourage further research to overcome the problems encountered in previous mobile multicast architecture attempts.

As discussed in the previous section, mobile multicast data delivery on the Internet can be achieved by a combination of three basic mechanisms, namely by,

- local multicast group management; which enables routers to learn the presence of multicast listeners on their directly attached networks,
- global multicast routing; which enables routers to exchange information, build multicast delivery trees and forward data across the Internet, and
- mobility management support; which enables hosts to reattach to a network after movement and to continue communications.

Multicast group management is conducted through a series of message exchanges between listener hosts and multicast routers, triggered by a set of timers.

Ideally, group management should be robust and updated as quickly as possible when any multicast listener state changes (i.e. hosts start or stop listening to one or more multicast groups) occur on any network link. The speed and robustness in which IPv6 SSM group management are achieved by MLDv2 is termed 'granularity'. Achieving higher granularity ensures minimal multicast set up time, bandwidth wastage, a seamless service and enhanced user experience. Granularity is a qualitative indicator of the MLDv2 discriminating ability in group management. Nevertheless, higher granularity means more MLDv2 messages are exchanged more frequently. Higher granularity results in higher MLDv2 (or signaling) traffic, which is to be avoided especially in bandwidth constrained access networks. The maximum granularity setting is often limited by the link bandwidth before it starts to affect multicast and other data delivery.

The MLDv2 protocol has been primarily designed for fixed hosts and networks so the default protocol settings (in the proposed specification) might not be suitable for mobile networks. Wireless access schemes for mobile networks are affected by ambient factors making them generally less reliable that wired networks. For example, in lossy wireless networks, there is a possible need for multiple MLDv2 packet retransmissions, set by the Robustness Variable (RV) parameter in the protocol. The MLDv2 robustness, the resulting granularity and the subsequent delivery of multicast data in wireless networks are important issues, and the dynamics of which are not well understood. Devising an analysis framework to enable the study of MLDv2 granularity especially in limited bandwidth networks is the first aim of this research.

Measuring and analyzing MLDv2 characteristics and MLDv2 traffic for various multicast listener behaviors are beneficial in understanding and improving group management protocols. Using the MLDv2 analysis framework, the dissertation aims to obtain results which will assist in characterizing MLDv2 behaviour. The second aim of this research is to determine the optimised MLDv2 granularity for various multicast listener densities, types of multicast applications and access network bandwidths. The results will also be useful for developing and testing more efficient multicast routing, resource reservation algorithms and AAA protocols for future multicasting technologies.

The use of MIP protocols solves the network or IP layer problems caused by host movement, commonly termed as the 'macro' mobility management. However, host movement in mobile networks also involves handoffs between wireless transceivers (or access points), each of which covers only a very small geographic area. Access point handoffs are commonly termed 'micro' mobility management and the use of

MIP protocols are less suited for such applications. Micro and macro mobility management for mobile multicast hosts are made complicated by several factors due the different types of possible host movements. For example, host movements between wireless cells may or may not change IP subnets, and therefore multicast group membership. The uncertainty caused by such host movements makes it necessary to determine if a transition across IP subnet boundaries has occurred, using movement detection techniques[14]. This study aims to investigate possible techniques that may offer faster convergence and far less overhead than MIP solutions.

Multicasting is usually associated with the delivery of large bandwidth data streams. Hence, malicious modification of multicast group information on any IP subnet is a significant cause for concern on network resources. Additionally, the limited feedback mechanisms available for UDP multicast data streams mean that service theft and network denial-of-service are potentially easier than in bi-directional communication streams. Although MLDv2 is only specified for and operates within a single IP link, any form of security abuse of the existing (and implicit) trust employed in the MLDv2 protocol may change routing states significantly and affect data delivery on multiple hops in the Internet.

The proposed MLDv2 protocol has many new features and functionalities which need a comprehensive security analysis. Potential security attacks need to be identified and their affects made known for security considerations. One of the MLDv2 attack protection techniques from hosts on external networks is achieved through the prevention of forwarding packets without link-local IP source addresses. Identifying the source of an attacker is of interest and certainly possible, but does not mitigate the potential for attacks. It also does not prevent the negative impact to the network and the consequences of the abuse. The research in this thesis aims to analyse and consider the various MLDv2 trust models, security threats and possible abuse mechanisms.

Mobile hosts in an IP network wishing to continuously receive multicast data has its own set of unique problems. In summary, the aim of this research is to find solutions that ensure that:

- the join and leave latencies during a handover process are minimal; to support delay-sensitive applications,
- the overhead signaling traffic is kept as low as possible; so that efficient data delivery can be achieved in bandwidth constrained access networks,

---

[14] The Detecting Network Attachment (DNA) IETF WG was recently established to recommend possible solutions and establish a standardisation track.

- minimal tunneling and routing states are held within the network; to achieve a scalable architecture regardless of the network size or number of mobile hosts,
- maximise the available network resources in the visited network; to minimise propagation and processing delays caused by traffic transversing the HN,
- secure communications, and
- compatibility with other Internet protocols; in order not to adversely impact source discover mechanisms and other protocols like QoS and AAA.

1.5 Thesis Structure and Contributions

The rest of this thesis is organised and structured in the following manner. Chapter 2 contains the literature review of the progress in research and the current state of standardisation within the IETF for mobile multicast architectures and the underlying protocols. In order to gain a better understanding of the current protocol versions, a brief evolution of the IPv6, multicast and mobility protocols since its early inception is presented. The historical perspective frames a context for the current design rationale based on the research progress and deployment experiences throughout the years.

Having defined the sphere of research, Chapter 2 continues with a comprehensive review and evaluation of prior work conducted by other academic groups in this area, their results and the achieved progress to date. The cumulative progress made thus far in the three areas of IPv6, SSM and MIPv6 protocols has resulted in distinct advantages over previous versions. Some of the fundamental changes in the newer protocol designs have enabled novel approaches to be formulated and experimented in solving many of the existing mobile multicast research problems. Chapter 2 concludes with a summary of the current problems which still remain and those addressed in this thesis to help ensure the success of SSM and MIPv6 protocols to support wide scale mobile multicast deployment.

The SSM paradigm and the protocols required to support it are at their initial stage of research and so no prior performance studies have been conducted. In Chapter 3, a performance evaluation of MLDv2, the newly proposed IPv6 group management protocol, is conducted. This study aims to contribute towards design improvements by providing feedback. The two critical performance parameters to be measured are identified as the signaling traffic overhead contribution and the MLDv2 updating latencies in mobile multicast networks. The MLDv2 specified timers, messages and interaction for SSM group management are used to formulate the MLDv2 link traffic and latency equations during various multicast events. The initial MLDv2 performance evaluation is conducted for the default timer settings specified in the proposed draft standard. The analysis is extended by obtaining MLDv2 traffic and latency results for the proposed operating range of the protocol settings. For a comprehensive set of performance results, the MLDv2 traffic measurements were required from networks with a large number of nodes. Hence, simulation experiments were conducted to obtain more comprehensive results from large networks. Chapter 3 concludes with a discussion of the results presented and reiterates the protocols' shortcomings identified by the analysis, namely handover latencies concerns and signaling overhead which reduces MLDv2 efficiency.

Chapter 4 begins with reviewing the current proposed techniques for improving MLDv2 group management efficiency. The prescribed methods improve various important characteristics but not the MLDv2 signaling traffic overhead, which was found to be particularly disruptive at certain multicast events in our study in Chapter 3. In Chapter 4, a proposed algorithm to improve the signaling overhead of MLDv2 using the idea of adaptive tracing, which is called Adaptive Listener Tracing (ALT) is introduced. The detailed design of ALT is presented. ALT uses a simple, easy to implement design and does not disrupt the current MLDv2 protocol workings in any manner. The ALT algorithm is used as a complementary component to the existing MLDv2 protocol with significant signaling overhead advantages.

The ALT algorithm is incorporated into our existing MLDv2 simulation modules and further experiments are carried out to verify the reduction in MLDv2 signaling traffic. The results measured using the ALT algorithm are compared to the original MLDv2 protocol. The improved results make the ALT algorithm useful for designing and developing future multicast routing and possibly resource reservation protocols for mobile networks.

In Chapter 5, movement and handover associated multicast latency problems for mobile hosts are addressed. The various delay components which contribute to the overall multicast handover latencies are identified. The present research proposals and available techniques for reducing these latencies are described and evaluated. The most promising method to date is by using Layer-2[15] triggering mechanisms implemented for MIPv6 unicast systems. The Layer-2 triggering mechanism is extended and implemented for multicast group management updating.

The experimental results obtained using the Layer-2 triggering mechanism are

---

[15] The Data Link Layer in the OSI model.

compared to the original MLDv2 results from Chapter 3 and the improvements are outlined. The study on multicast latencies is further expanded to include routing latency components which is caused by the multicast tree reconfiguration when hosts move between IP subnets. Simulation experiments were conducted to obtain results and verify the improvements using the Layer-2 triggering mechanism. To verify that the ALT algorithm and the Layer-2 triggering mechanism work from a deployment point of view, experiments were also conducted on a test network. The testbed experiments are conducted using systems to deploy an SSM MIPv6 network which are currently available. The testbed was also used to evaluate a possible channel discovery mechanism and outline other outstanding issues to be addressed for a successful SSM MIPv6 deployment.

In Chapter 6, the security considerations and trust models for MLDv2 are investigated. The security analysis includes MLDv2 working and interactions with Layer-2 and multicast proxy devices. A security and threat analysis for each model is conducted. Possible attacks ascribed to particular roles within the network are evaluated with respect to the various initiatives and proposals within the IETF to secure local IPv6 packet delivery.

The conclusion in Chapter 7 outlines the contributions of this thesis and the alternative approaches adopted by various other academic groups since the start of this research and their respective progress. Possible future research directions and areas of work are identified. Other outstanding issues for a successful Internet-wide SSM MIPv6 deployment are also discussed.

The derivation of all the equations used in Chapter 3 is given in Appendix A. The simulation modules used to replicate the MLDv2 functionalities, the network topologies used and various protocol settings employed in the experiments are shown in Appendix B. The equipment, operating systems and configurations used to conduct the experiments for SSM and MIPv6 protocol improvements are presented in Appendix C.

Chapter 2

Current State of Research and Standardisation

2.1 Introduction

This chapter offers a review of the current research activities and state of the art in the standardisation of IPv6 based multicasting and mobility protocols. A considerable amount of effort has either gone into devising better IP multicasting or IP mobility (primarily for unicast communications) designs separately. A small proportion of prior IP mobility research has considered multicasting issues but none of the proposed methods neither has been extensively tested or widely adopted. The recently proposed SSM [HC04] and MIPv6 [JPA04] protocols however, seem to be the most promising way forward in solving many of the existing mobile multicast research problems.

The rest of this chapter is structured in the following manner. In order to gain a better understanding of the motivation and design considerations of multicasting protocols, the evolution from the initial ASM model to the newly proposed SSM model is provided in the following section. The changes to the multicast addressing scheme, the routing and group management protocols required to support the new SSM model are presented. Then, an explanation of how multicasting is achieved in IPv6 and the components required to specifically support SSM are given. Mobility in the IP layer is explained with emphasis on the workings and advantages of the new MIPv6 system. The proposed multicast handling mechanism in MIPv6 systems is explained and illustrated. A comprehensive review and evaluation of prior work conducted in the area of mobile multicasting, their results and progress to date are given. The chapter concludes with a summary and discussion of the problems which still remain for MIPv6 SSM mobile multicasting and the specific issues addressed in this thesis.

2.2 Multicast: Past, Present and Future

2.2.1 Any Source Multicast

Evolution and Operation

The initial multicast model with the basic design requirements listed in Section 1.2 was proposed to the IETF community by Deering and Cheriton [DC85]. A number of the ideas for the original multicast model specified by the IETF was from Deering's thesis [Dee91]. The concept was to extend the existing IP by enabling identifiers for a class of addresses or multicast groups. A Class D[1] range of IPv4 addresses from `224.0.0.0` to `239.255.255.255` were reserved for IP multicasting [Dee89]. The initial IP multicasting model required two new protocols; the Internet Group Management Protocol (IGMP) and the Distance Vector Multicast Routing Protocol (DVMRP).

The IGMP uses a simple message exchange mechanism for multicast hosts and routers to convey information on the local network. The Internet Group Management Protocol version 1 (IGMPv1) [Dee89, Appendix 1] was based on two primary IP messages; a query message sent by the multicast router and a report message sent by the host. As shown in Figure 2.1, a host, H_1 uses the IGMPv1 report to communicate multicast group membership requests to its local multicast router, MR. The router MR places the multicast information from the received report as an entry in its multicast table, which is called a multicast join. The router periodically sends out query messages to determine if multicast groups remain of interest to any of the hosts H_1, H_2 or H_3 on the local network. If the router does not receive a report message back form any host after a query is sent, the router removes the corresponding multicast group entry from its table which is called a multicast leave. Using IGMPv1, a host wishing to leave a multicast group cannot explicitly notify the router. Multicast data is forwarded till the next query message is sent and there are no reply reports. The local network bandwidth is wasted during this period.

The updated Internet Group Management Protocol version 2 (IGMPv2) spec-

---

[1] The IPv4 address space can be subdivided into five classes – Class A, B, C, D and E. Each class consists of a contiguous subset of the overall IPv4 address range.

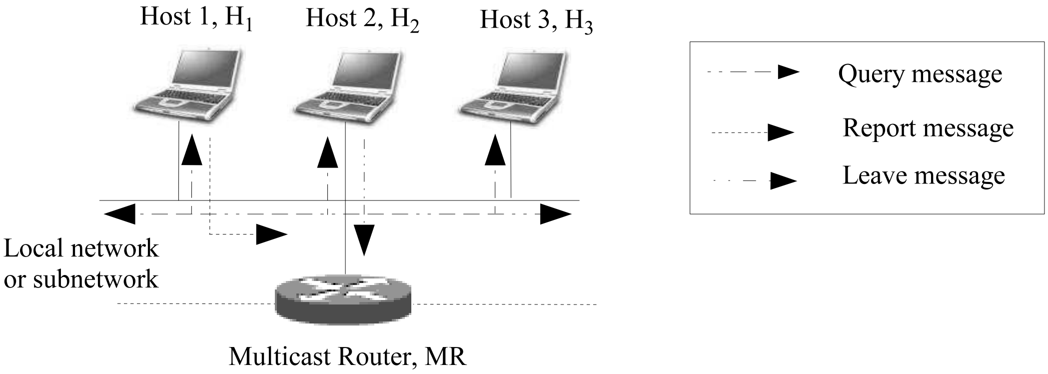
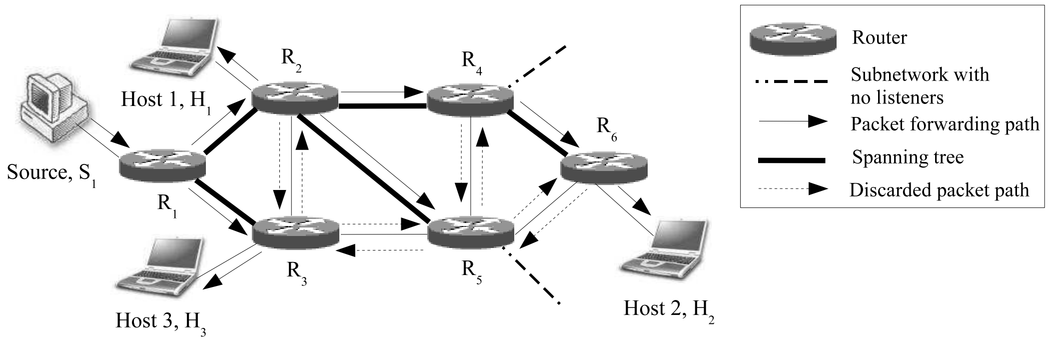


Figure 2.1: Internet Group Management Protocol messages.

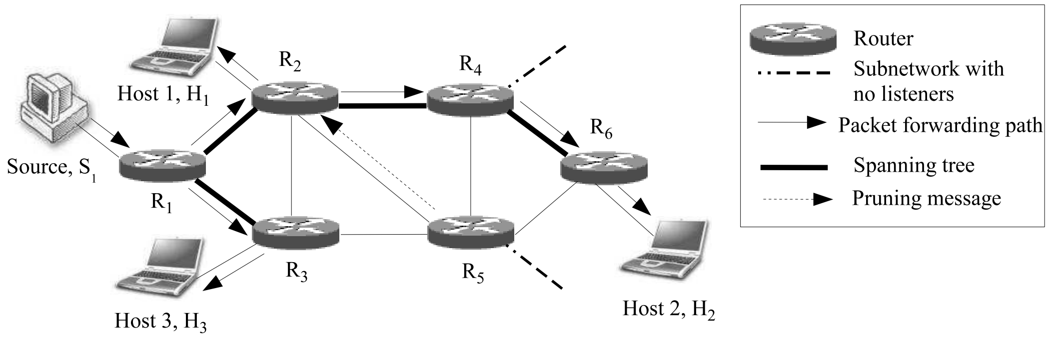
ification [Fen97] adds a third IGMP leave message. When host H_2 wants to stop receiving multicast data, it can send a leave message to the router MR. It is possible to have more than one multicast router present to ensure redundancy or for other network deployment considerations. To avoid the phenomenon where all of the routers forward the same multicast traffic, one router has to be elected to serve the subnetwork. IGMPv2 includes a method of electing the router by way of IP address comparison; the one with the lowest IP address is elected.

While IGMP is used by hosts to register interest, multicast traffic still needs to find a path from the data source to the host. Hence, there is a need to use multicast routing protocols. The initial multicast routing protocol was based on the Reverse Path Forwarding (RPF) technique as shown in Figure 2.2a. When router R_1 receives a multicast packet from source S_1, it replicates and routes (or floods) the packet to all its interfaces except the one it originated from. All the other routers in the network repeat the same procedure with the assumption that the original interface they receive the packet from leads back to source S_1. In doing so, the routers ensure data packets reach all parts of the network.

The first multicast model used the Distance Vector Routing Multicast Protocol (DVMRP) [WPD88] to route and deliver multicast packets. The DVMRP is based on the Truncated Reverse Path Forwarding (TRPF) [Dee88] algorithm which compares the data delivery path of all of the packets it receives and only forwards the one taking the shortest path from the source. In Figure 2.2a, although R_3 receives similar packets from R_1 and R_2, using the TRPF algorithm, it only forwards packets from R_1 to the multicast host H_3. The multicast data delivery paths within a network often project a tree shape, rooted at the source and having multiple branches extending towards the multicast hosts. The router R_5 does not have any interested



(a) Spanning Tree



(b) Truncated Reverse Path Forwarding

Figure 2.2: Multicast forwarding algorithms.

multicast hosts on its downstream[2] link, it then sends control (or prune) messages back to the upstream router R_2 to prune its branch from the multicast tree. The DVMRP will periodically re-broadcast multicast traffic in order to reach any hosts that may have newly joined the network. The DVMRP can be characterized as a broadcast and prune routing protocol. The use of DVMRP results in a simple data distribution model and has distinct advantages. The multicast group join is quick as data from new sources is automatically sent to all hosts initially. Also, using TRPF, DVMRP has its own multicast network topology discovery mechanism allowing for both faster adaptation to change and a more stable multicast delivery tree.

The DVMRP was not widely supported in the commercial Internet initially. Instead, a multicast network was created by using mrouted[3] by building virtual

---

[2] The downstream direction in multicasting is defined as the direction of data flow from the source towards the listeners.

[3] A software process enabling DVMRP routing which forwards multicast packets.

point-to-point links or tunnels between DVMRP-capable machines. It was termed Multicast Backbone (MBone) [Cas93] and served as the first experimental and semi-permanent IP multicast testbed to develop and test multicast protocols by the research community. The MBone was also used to carry IETF meeting audio transmissions [CD92] on the Internet. The DVMRP nature to broadcast packets frequently made it unsuitable for low speed network connections. Also, the need to a maintain large number of routing states for DVMRP did not scale across Internet domains. Further revisions and refinement to the multicast design phase finally culminated in RFC 1112 [Dee89] which is the reference for the multicasting model commonly termed Any Source Multicast (ASM).

The next multicast routing protocol iteration was based on the Open Shortest Path First (OSPF) [Moy89] unicast routing protocol. The OSPF was designed to distribute the routing topology within a network rapidly based on link-state algorithms. A link-state routing algorithm is based on every router receiving a map of the network connectivity (of all other routers) in the form of a graph. Each router then independently calculates the best route for every possible destination in the network. Unlike DVMRP which shares the routing information with all the routers, in OSPF, only the information required to construct connectivity maps is passed between routers. The improved Open Shortest Path First version 2 (OSPFv2) [Moy94a] introduced additional features of hierarchical routing information exchange, traffic load balancing between the various links and importing of external routing information from other networks. Multicast extensions to Open Shortest Path First (MOSPF) [Moy94b] was proposed to support multicast routing.

MOSPF builds a multicast delivery tree by using IGMP information in routers and the OSPF link-state database. The MOSPF routers can be used in conjunction with non-multicast OSPF routers which allows the gradual deployment of multicasting capability within a network. However, a MOSPF router eliminates all non-multicast OSPF router paths when it creates a source rooted shortest path multicast tree. The omission of non-multicast routers can create a number of potential problems. Packets may be forwarded along suboptimal routes since the shortest path between two points maybe through non-multicast routers. Unicast connectivity to a destination may not reflect multicast connectivity within a network. The forwarding of multicast and unicast packets between two points may follow entirely different paths through the network making it difficult to debug routing problems. MOSPF also requires OSPF as an accompanying routing component and can sometimes cause heavy router processing loads.

Protocol Independent Multicast (PIM) is a relatively new set of multicast routing protocols. The PIM protocols are able to establish multicast routes for hosts which span a wide-area and interdomain networks. Although PIM functions with an existing unicast routing table, it is independent of any one specific unicast routing protocol. PIM makes a clear distinction between the usage of routing protocols for dense and sparse environments. Dense-mode refers to the protocol operating in an environment where multicast hosts are packed densely and bandwidth is plentiful. Like DVMRP, Protocol Independent Multicast dense-mode (PIMdm) [DEF$^+$96] first floods multicast traffic across the internetwork and then prunes the subnets that do not have multicast hosts. Sparse-mode refers to the protocol optimized for environments where multicast hosts are distributed across many regions of the network and bandwidth is not necessarily abundant. Sparse-mode does not imply there are less multicast hosts but just that they are widely dispersed across the Internet. This distinction and hence the two different protocols is justified because when multicast hosts and senders are sparsely distributed across a wide area, both DVMRP and MOSPF as dense-mode protocols are not efficient. DVMRP periodically sends multicast packets over links that do not have multicast hosts while MOSPF can send group membership information over links that do not lead to senders or hosts.

The various attempts at dense mode routing protocols over the years were still not able to achieve an efficient multicast model which could scale across multiple networks. This led to the development of sparse mode[4] routing protocols. In sparse mode, routers serving downstream multicast hosts wishing to receive multicast traffic must send explicit join messages towards (the predefined) designated routers within the network domain, termed Core Routers or Rendezvous Points (RP). A multicast data delivery tree is created from a predefined center or Core Based Tree (CBT). The CBT concept was first discussed in the research community by Ballardie [BFC95] and eventually standardised by the IETF [Bal98].

The Protocol Independent Multicast sparse-mode (PIMsm) was specified to support the CBT delivery model [EFHT98]. The PIMsm protocols use a bootstrap feature to discover the presence of RPs within a network and which multicast groups they represent. As shown in Figure 2.3, RP$_1$ is shared by sources S_1 and S_2 to serve a CBT multicast domain. Any number of sources can send data to a multicast group, identified by a class D IP multicast group address, G_1. The multicast host, H_3 sends an IGMPv2 join message without specifying a particular IP source address for the multicast group (*, G_1), towards the router R_4. The router R_4 sends a PIMsm join message towards the router RP$_1$. The router RP$_1$ starts forwarding multicast

---

[4] Uses a pull model to deliver multicast traffic. Only routers that have active multicast listeners downstream, explicitly requested for and are forwarded multicast data.

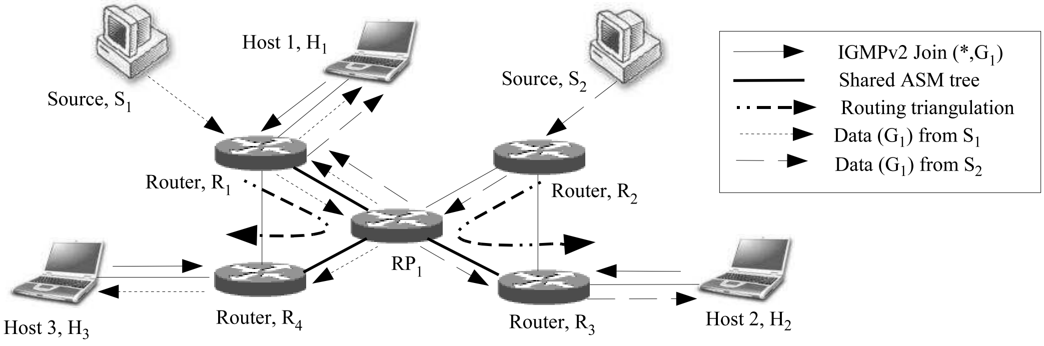


Figure 2.3: ASM data delivery with a shared tree (showing routing triangulation).

packets towards the router R_4. Initially, all multicast data to listeners has to go through the RP_1, but in instances when the path to a source crossed a multicast tree branch, PIMsm has a route optimisation feature. This feature allows source, S_1 to access towards the host H_3 through router R_1 and R_4 directly instead of using RP_1. The sparse mode model achieved significant advantages over dense mode by providing better routing state scalability and eliminating inefficient packet flooding.

Complexities

One of the early requirements for the multicasting design was not to impose any restrictions on the sender, i.e. any source can transmit using any multicast group destination IP address. As shown in Figure 2.3, both sources, S_1 and S_2 can send multicast data to the group address, G_1. Also, there was no access control requirements for the multicast hosts, i.e. a host only needed to specify the multicast group address and the network had to determine the source for that group and conspire to deliver the data. A complex set of protocols were required to support the ASM model that had inherent drawbacks. For example, in Figure 2.3 the data from source S_1 has to transverse RP_1 when host H_1 listens to the group G_1 initially, although there is shorter and direct path. With the multicast tree rooted at RP_1, there is no guarantee that the data is traveling through the shortest path between the source and the multicast hosts, a phenomenon commonly termed routing triangulation. Also, RP can potentially become a hot spot (or a single point of failure) along the multicast data delivery path.

RP acts as a central point of control and needs to keep a full list of routing entries. It creates a flat routing structure requiring full routing entry exchanges and inhibits routing aggregation[5]. The number of routing table entries grows with the

---

[5] Routing aggregation enables the exchange of information between routers only using a summary

number of multicast services, which limits the scalability of the CBT model. Also, inter-domain scalability is impossible as in the current specification multicast addresses cannot transverse domain boundaries defined by Autonomous System (AS) numbers (and peered through Border Gateway Protocol – BGP sessions). The near term solution was to extend BGP to carry multicast routes using Multiprotocol Extensions to BGP (MBGP) [BCKR98]. The use of MBGP enabled the exchange of multicast routing information based on each AS's multicast topology or source information. The final missing component of sparse mode source information distribution within networks led to the near term solution of Multicast Source Discovery Protocol (MSDP) [FM03]. The MSDP provides a peering service between each RP in PIM domains for source IP addresses and the corresponding multicast groups it serves. The progress over the years in the ASM model has made multicasting less complex but it is still affected by inter-network protocol and deployment problems.

2.2.2 Source Specific Multicast

Architecture and Design

Due to the complexities in designing and implementing the ASM model [KRT$^+$98], the next phase of research considered a simpler service model; aiming ultimately at achieving an Internet wide and commercially viable multicast solution. Holbrook and Cheriton [HC99] proposed the EXPlicit REquest Single Source (EXPRESS) design, which was a shift from the many-to-many to a one-to-many multicast model. The EXPRESS method (which was pursued for standardisation and renamed as SSM at the IETF), defined logical 'channels' instead of only relying on multicast group IP addresses. An IP unicast source address (S_i), and the multicast group address (G_j), are used in tandem to create a unique multicast channel with the identity ($S_\mathrm{i}, G_\mathrm{j}$). SSM hosts subscribe (or start listening) to this channel whereas in ASM, hosts relied upon multicast group IP addresses. When a multicast host subscribes to a SSM channel, it receives data from the source S_i, to a destination multicast group address G_j. SSM gained momentum within the IETF. An overview of SSM is provided by Bhattacharyya et al. [Bha03] and standardisation efforts are described by Holbrook [HC04].

The SSM model is designed to support broadcast or one-to-many type applications. To enable many-to-many applications using SSM, one channel for each source will need to be mapped for multicast hosts. The potential drawbacks include the necessity to know and respond to every join and leave of each and every one-to-many

---

(or partial) addresses which is more efficient.

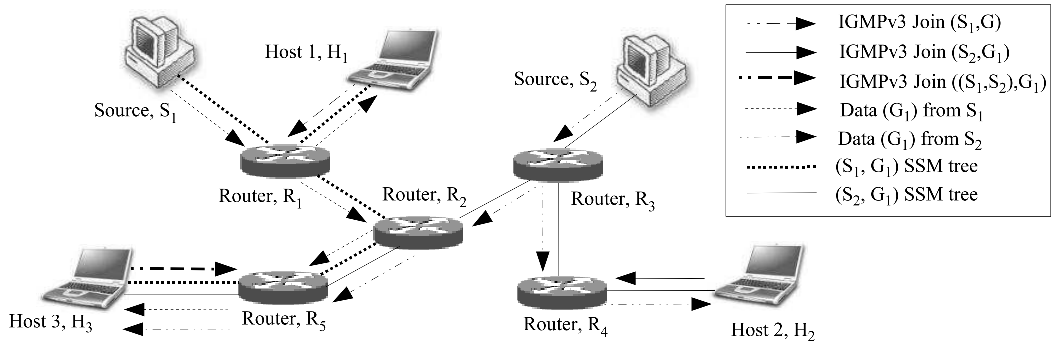


Figure 2.4: SSM data delivery with a source rooted tree.

host. The corresponding multicast trees need to be readjusted for every join and leave. Frequent multicast join and leave increases the states held by routers thus limiting the service scalability.

Components and Workings

The central coordinating agency for IP address allocations, the Internet Assigned Numbering Agency (IANA), has reserved the IPv4 address range 232.0.0.0 to 232.255.255.255 for the exclusive usage of SSM [HC04]. These addresses fall within the earlier allocated multicast address range in the hope that SSM can co-exist without much changes required in the ASM capable networks. The existing ASM applications have to be modified to contain the extra source address information associated with each multicast group. When a SSM capable application discovers a channel of interest, the associated addresses have to be passed onto the network layer module to start the subscription process. SSM aware applications use specific Application Programming Interfaces (APIs) to conduct the notification process [TFQ04].

At the network layer, a new Internet Group Management Protocol version 3 (IGMPv3) [Cai02] was introduced with the ability to specify both the source and group addresses for an SSM channel. IGMPv3 also supports source filtering, or the ability of a host to express interest in receiving data packets sent only by specific sources, or from all but some specific sources. For example in Figure 2.4, H_1 and H_2 send IGMPv3 join messages with the fields (S_1, G_1) and (S_2, G_1) to routers R_1 and R_3 respectively. Data from S_1 takes the shortest path to host H_1. Unlike in ASM, the SSM delivery tree is rooted at the source and not at a RP. There is no need for the traffic to transverse a central point in the network like in ASM.

The new Protocol Independent Multicast sparse mode version 2 (PIMsmv2) [FHHK04] specification includes source specific host reports as required by the SSM

	ASM	SSM
Routing tree type	Shared bi-directional only	Per-source uni-directional only
Address allocation	(core, class D) model	(source, group) model
Sender authentication and authorisation	Not available	Multiple senders not allowed for same group
Receiver authentication and authorisation	Not supported	Per-host tracking provided
Interdomain and Core (RP) protocols	Required (PIM, MSDP & BGP4)	No cores used
Group controls	Yes, at core	Yes, at source
Modifications	Yes	No, but requires IGMPv3

Table 2.1: A comparison of the ASM and SSM model.

model. When a leaf router (which has been renamed as the Designated Router (DR) in SSM) running PIMsmv2 receives an IGMPv3 join message in the SSM address range, it must ensure that the request contains a group associated source address. The primary concern of PIMsmv2 is to prevent ASM model behaviour within the SSM address range in networks with dual capability. The same rules apply for any RPs existing within a network. Table 2.1[6] gives a summary of the ASM and SSM multicast model differences.

Advantages

SSM also lends itself to an elegant solution to the ASM access control problem. Any SSM source can transmit to any group destination address. The SSM source is independently responsible for resolving address collisions for the various channels that it creates. SSM averts the problem of needing a global multicast address allocation scheme because every channel is unique. When a source transmits to a group address, it is automatically ensured that the channel identity is unique because of its own individual IP address (except in the case of malicious acts such as address spoofing). No other sender's data (even with the same multicast group address) will have the same channel identity. This added security feature makes it much harder to spam[7] a SSM channel than an ASM multicast group.

The SSM model relies on source based forwarding trees, thus eliminating the RP based shared trees, as shown in Figure 2.4. By virtue of a source based tree, neither

---

[6] A more generic comparison for the current multicast protocols and models is presented by Diot et al. [DLL$^+$00].

[7] The malicious sending of unsolicited data or messages.

the RP nor the MSDP protocol is required for the SSM model. The complexity of the SSM multicast routing infrastructure is low, making it viable for immediate deployment. There is no difference in how MBGP is used for ASM and SSM to exchange multicast group information between domains.

2.3 Internet Protocol version 6

2.3.1 SSM Components

Unlike IPv4, IPv6 has been designed to support multicasting from the beginning. Multicast addresses are part of the IPv6 addressing schema with well defined administrative regions that are easier to manage. Prefix-based multicast addresses required for IPv6 SSM have been defined in RFC 3306 and allocated by the IANA with the format `FF3x::/96` [HT02]. Application Protocol Interface (API) requirements for SSM are identified in the Multicast Source Filtering API [TFQ04] as an extension to the basic IPv6 socket definitions in RFC 2553 [GTBS99]. The standard specifies new programming socket options and ioctl[8] commands to manage source filters for group memberships.

The IPv6 Multicast Listener Discovery (MLD) protocol provides similar multicast group management functionalities as IPv4 IGMP. IPv6 multicasting is easier to deploy as MLD support [Lou04] is mandatory for all IPv6 hosts. The initial Multicast Listener Discovery version 1 (MLDv1) specification RFC 2710 [DFH99] was designed based on IGMPv2 to support ASM. The IETF Multicast and Anycast Group Management (MAGMA) WG has proposed the Multicast Listener Discovery version 2 (MLDv2) specifications [VC04] to enable SSM. MLDv2 is an asymmetrical protocol which specifies separate behaviours for routers and hosts. A detailed discussion of the use of MLDv2 in the SSM destination address range is provided by Holbrook [HCH03]. The MLDv2 protocol is discussed in more detail in Section 2.4.1.

The PIMsm protocol requirements to support SSM routing have been documented by Holbrook [HC04]. The PIMsmv2 [FHHK04] protocol specifies SSM forwarding semantics and has been proposed for standardisation. It is capable of supporting thousands of groups, different types of multicast applications, and all major underlying Layer-2 subnetwork technologies.

---

[8] A programming language function which manipulates the underlying device parameters of special files.

2.3.2 Mobile IP

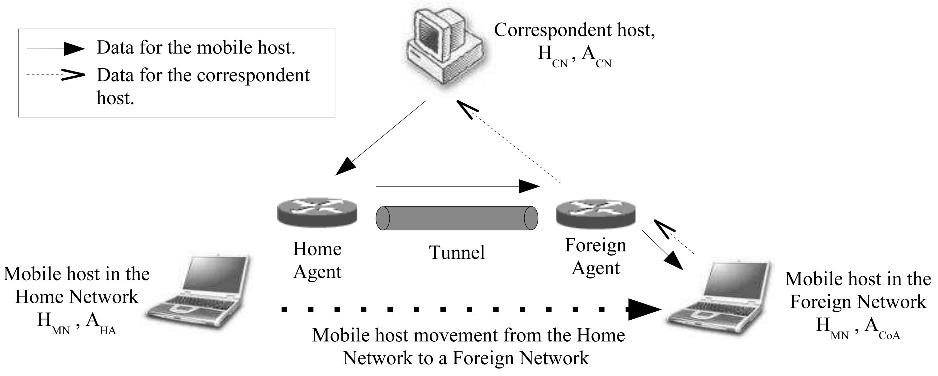
Mobile IP networks enable host mobility support on the IP infrastructure without requiring any modifications to the applications, corresponding hosts or routers as stated in Section 1.2. In early MIP designs, a Home Agent (HA) server in the Home Network (HN) provided the mobility management functionality when a mobile host moved to a Foreign Network (FN). The basic workings of MIPv4 are shown in Figure 2.5a. When a mobile host, H_{MN} with a home IP address A_{HN} moves to a FN, it is required[9] to acquire a new Care-of-Address (CoA) from the Foreign Agent (FA). The host H_{MN} with the new IP address, A_{CoA} has to update its HA. While in the FN, all of the data packets destined for the mobile host, H_{MN} to the address A_{HN} are intercepted at the HA and forwarded through a tunnel to the FA. The FA decapsulates the packets and sends it to mobile host H_{MN} with the address, A_{CoA}. Data packets from the mobile host H_{MN} are sent directly from the FA and routed towards the corresponding host, H_{CN} because its destination IP address, A_{CN} in known from the received packets.

The Mobile IPv6 (MIP6) WG is developing IPv6 host and router support to permit hosts to seamlessly roam specifically in IPv6 networks. The current MIPv6 standard [JPA04] supports transparency above the IP layer, including the maintenance of active TCP connections and UDP port bindings. IPv6 mobility support is potentially simpler to implement than in IPv4 because MIPv6 does not need a dedicated (FA) router for IP address assignments in the FN. In MIPv6 systems, as shown in Figure 2.5b, when a mobile host, H_{MN} moves from its HN to a FN, it can employ a 'stateless' or 'stateful' mechanism to obtain a CoA. Stateless addresses are obtained with an auto-configuration mechanism [TN98] which uses a router advertised network prefix to create a complete IPv6 address. Stateful addresses are leased from the network using Dynamic Host Configuration Protocol version 6 (DHCPv6) [DBV+03]. Unlike in IPv4, auto-configuration and router discovery protocol support are mandatory prerequisites specified for *all* IPv6 hosts, making them MIPv6 ready without any additional requirements.

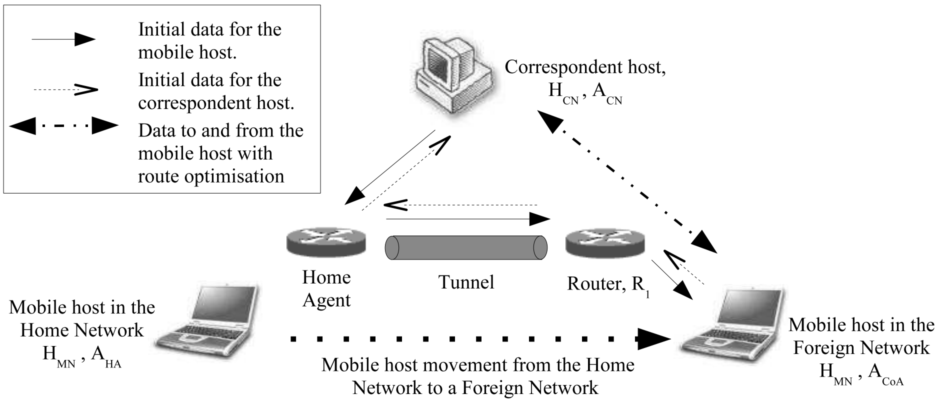
Also, MIPv6 is more efficient with hosts able to communicate directly with each other (without the v4 tunneling) using a route optimisation technique. As shown in Figure 2.5b, the host H_{MN} has to update the HA with its new address A_{CoA}. When it receives a data packet from the corresponding host H_{CN}, it sends a reply directly back using its new CoA. In MIPv6, the corresponding host is able to send a packet directly back to the mobile host without going through the HN, thus avoiding

---

[9] IP addresses are network dependent. A HN IP address is not portable to the FN due to security and scalability concerns.



(a) MIPv4



(b) MIPv6

Figure 2.5: Mobile IP.

routing triangulation.

Mobile Multicast Hosts

Although primarily designed for unicast connections, MIPv6 introduces two possible mechanisms to maintain multicast sessions in spite of host movements and network re-attachments, i.e. Bi-directional Tunneling (BT) and Remote Subscription (RS) [JPA04, Section 10.4.3]. As illustrated in Figure 2.6a, the BT method forwards multicast data from the source S_1 to the mobile host H_{MN} through the HA. The advantage of BT is that roaming hosts can rely on the availability of similar multicast services to its HN regardless of movement. The HA has to create forward tunnels to the visited network for every single multicast host. The HA must be capable of receiving MLD reports through a reverse tunnel from the mobile host, H_{MN}, in order to determine which groups have been subscribed to. To avoid ambiguity on the HA due to mobile hosts which may choose identical source addresses for their MLD function, it is necessary for the HA to identify the issuer of a particular MLD message. This requires the HA to note which tunnel the MLD message arrived from. The MIPv6 specification does not require full IPv6 multicast router functions on the HA and multicasting may be possible to achieve through a proxy MLD device, as shown in Figure 4.1. To refresh the mobile host's current multicast group membership information, the HA must also periodically transmit MLD query messages through the tunnel to the mobile host.

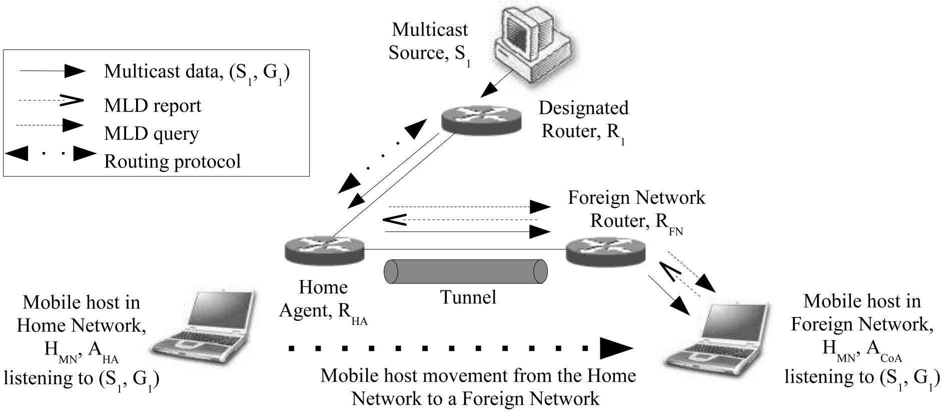
In the RS method, a mobile host can join a multicast group via a (local) multicast router on the foreign network being visited. As shown in Figure 2.6b, the mobile host, H_{MN} must use its CoA, A_{CoA} and not the Home Address, A_{HA} destination option when sending MLD messages to the local multicast router MR_1 in the FN. The router MR_1 forwards multicast data directly from the source S_1 to the mobile host H_{MN}. The direct sending of data from the router MR_1 is only applicable while the mobile host is at that foreign link. The host H_{MN} has to notify the multicast router in the new network it moves to of its multicast subscription state.

2.4 MIPv6 SSM Research

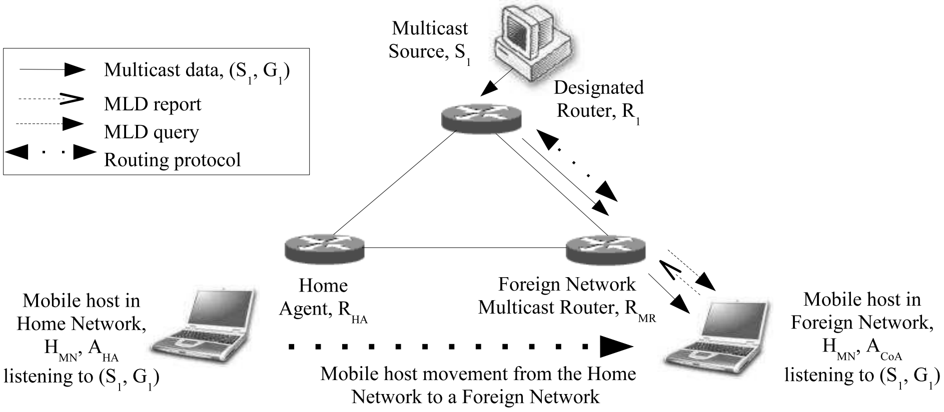
2.4.1 Multicast Group Management Efficiency

Multicast Backbone

The MBone [Cas93] was the first experimental network available to the research community for developing and testing multicast protocols. The MBone was created primarily due to the lack of multicast routing support in the wider commercial Internet during that period. Large scale multicast data and group management measurements could be conducted on the MBone. The initial multicast group research and measurements were conducted and reported by Almeroth [AA97]. The study was to assist in scheduling of worldwide MBone events which are typically announced ahead of time in a global multicast session directory. The research conducted by Almeroth was to determine the temporal and spatial statistics of multicast sessions using hosts' listening durations and their distances from the source. The results showed how the general multicast listener behaviour on the MBone was. However they were not able to specifically distinguish any group management characteris-



(a) Bi-directional Tunneling



(b) Remote Subscription

Figure 2.6: Multicast in Mobile IPv6.

tics nor provide specific signaling efficiency measurements. The measurements were based on the IPv4 dense mode ASM model and they were limited by the closed tunneled nature of the MBone network. In the early days of multicast research, the design of routing protocols and group management mechanisms were of high priority while the IGMP signaling efficiency was not sufficiently explored.

Receiver-initiated Group Management Protocol

The first IGMP traffic measurement and performance results available in the current literature are conducted by Liao [LY99]. Liao's study identifies the IGMPv2 and

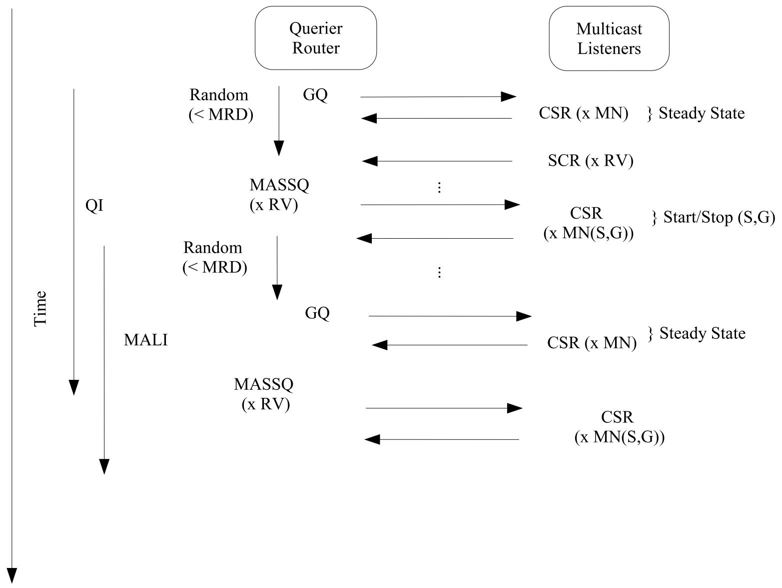
IGMPv3 signaling performance penalties due to their query and response mechanism. Liao proposed an alternative group management protocol called the Receiver-initiated Group Management Protocol (RGMP) which combines the advantages of IGMPv2 and IGMPv3 without any apparent performance degradation. The RGMP messages and timers are illustrated in Figure 2.7b. In the steady state, the multicast host, H_1 sends a Current State Record (CSR) message to refresh the multicast router, MR_1 of its current listening state and sets a timer T_1 for that record.

When other multicast hosts with the same listening state on the link receive the same CSR, they also reset their own timer for that record. If the listening states of the host H_1 do not change within the time T_1, the host sends out a similar CSR again, to notify MR_1 to keep forwarding multicast data. As illustrated in Figure 2.7a, IGMPv3 causes an implosion of reply messages ($\mathrm{CSR} \times N_{\mathrm{MN}}$) without the host suppression mechanism. Unlike IGMPv3, the number of RGMP messages does not increase linearly with the number of multicast hosts N_{MN} as illustrated in Figure 2.7b. RGMP also introduces a self-synchronised refresh timer based on each multicast group. If there are other hosts on the link listening to different multicast channels, the self-synchronised timers T_1 and T_2 ensure that CSR messages are sent with an even distribution over time.

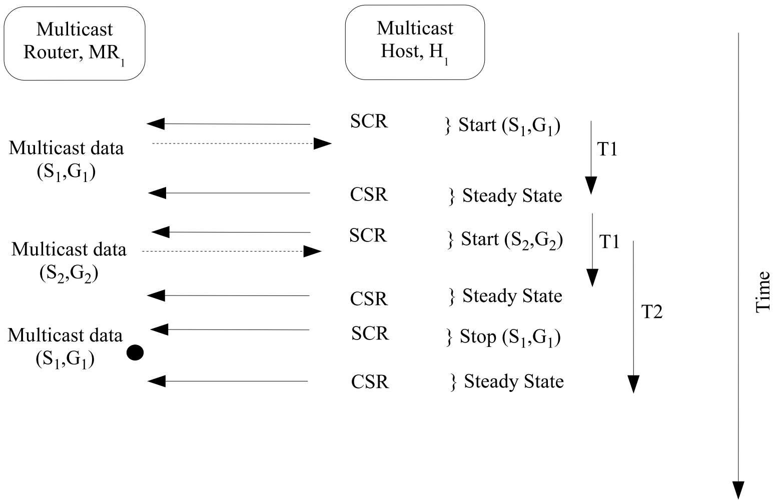
RGMP is very simple in comparison to IGMPv2 and IGMPv3. There is no need for a specific querier and hence no timers or messages are required as shown in Figure 2.7a. The RGMP signaling efficiency improvements over IGMPv2 and IGMPv3 are discussed in Section 4.2.4. The use of RGMP is, however, not suitable for mobile multicast hosts which are not aware of impending movements and hence cannot update the routers. The RGMP mechanism also increases the computational complexity of the end hosts due to the need to keep state and timers for all the listening states, making it unsuitable for simple and cheap devices.

Real Time Transport Protocol

The Real Time Transport Protocol (RTP) [SCFJ96] has been proposed to overcome the packet loss and delay disadvantages of best effort real-time data delivery through the Internet. RTP provides information for a listener to reconstruct the data stream, or detect the gaps through packet loss within the stream. RTP also identifies the data payload type and session members and timestamps the data so receivers can reconstruct a sender's data stream in time as well as in space. The RTP Control Protocol (RTCP) [SCFJ96, Section 6.0] is used in conjunction with RTP. RTCP is based on the periodic transmission of control packets to all participants in the



(a) IGMPv3 for IPv4 and MLDv2 for IPv6



(b) Receiver-initiated Group Membership Protocol (RGMP)

Figure 2.7: Comparison of IGMPv3 and MLDv2 to RGMP messages and timers.

session, using the same distribution mechanism as the data packets. RTP, however, does not specify any specific underlying network or transport protocols but can be used for data transfer to multiple destinations using multicasting.

The known problems of RTP originate from the RTCP part [RS98]. Each new

RTP member behaves initially like it is the only member of the group. All RTCP members send packets in their fair share of RTCP bandwidth. A new member however, not knowing of any other members, believes all of the bandwidth belongs to it. This causes congestion as many RTP sessions exhibit a rapid increase in group membership at certain points in time. The congestion is due to inaccuracies in the group size estimates obtained by listening to the group. To estimate group sizes, hosts must determine the number of distinct members which send RTCP packets. A unique identifier for each host must be stored for counting purposes. For large groups, keeping such a state does not scale. Demirci's [DB03] study on the comparable performance between IGMPv3 and RTP concludes that the former has better latency performance. There are no known comparable studies but with the extra control packets required RTP systems, RTP will be less efficient for group management signaling than IGMP. Further studies need to be carried out to determine signaling overhead performance advantages. No studies have been conducted on the use of RTP for IPv6 systems.

Multicast Listener Discovery

The current available research literature does not provide any performance studies for MLDv1 [DFH99]. As discussed in Section 2.3.1, in order to support SSM, MLDv1 had to be updated to include the SSM address range, the multicast source filtering capabilities and the per-socket listening states. The new functionalities introduced in MLDv2 resulted in more messages required to achieve group management. The MLDv2 protocol new functionalities and features will affect its performance (for example, the signaling link traffic contribution and granularity) but such a comparison has not been performed.

One of the first MLDv2 studies was conducted in INRIA[10]. The INRIA research measured MLDv2 implementation specific interaction and response time parameters within an operating system [AS03]. This study was conducted at the early stage of the MLDv2 specification and helped researchers understand and improve the MLDv2 module within operating systems and make available this functionality to the application layer for SSM usage. The work in INRIA by Asaeda [AS03] mainly expands on the complex Multicast Source Filtering (MSF) procedure, applied to a 4.4BSD[11] kernel. After presenting the implementation concept and design, Asaeda provides measurements to evaluate the implementation behaviour under various operating

---

[10] Institut National De Recherche En Informatique Et En Automatique, http://www.inria.fr/

[11] Berkeley Software Development operating system remains a popular experimentation and testing platform for many Internet related technologies and protocols.

conditions. The work does, however, point out that the MLDv2 implementation has to be supported for all the end devices for SSM to work, it is complex and burdensome. The study does not include measured results for signaling efficiency nor an analysis for an end-to-end MLDv2 performance primarily due to the lack of available wide-scale experimental implementations.

The RENATER[12] research group is experimenting with IPv6 multicast deployment issues for fixed networks [M6B]. Currently, their network is setup with an RP which tunnels IPv6 multicast packets in IPv4 unicast packets for global participants. They have not experimented with SSM but they provide information on the general multicast protocol, configuration and application issues based on their experience. In Section 4.2, the more specific solutions proposed to increase overall link bandwidth efficiency are presented. These proposed solutions don't directly address the multicast group management efficiency but looks at some other aspects of improving the general link bandwidth usage. The solutions primarily extend the link bandwidth reach and efficiency through the introduction of external network devices.

2.4.2 Group Management Security Issues

Previous work to secure multicast groups has primarily focused on access and abuse of multicast data [HW04] but not on the signaling messages. The protection of MLD signaling (nor having relied upon group signaling keys) has not been addressed. Security considerations for IGMPv3 in IPv4 [Cai02, Section 9] proposes a security mechanism for multicast group management based on IPSec Authentication Headers (AH) [KA98a, KA98b]. Here, the provision of signaling and message integrity is based on shared keys where any possessor of the shared key can undertake the transmission of 'authenticated' messages.

Similarly, the specification also proposes the application of future key exchange procedures to ensure that IGMPv2 query and leave messages be authenticated. However, no such key exchange mechanisms have been deployed for IPv4 to date. In either scenario (key exchange or shared key), the host multicast group management reporting remains unsecured. At the time of the MLD proposal, IPSec AH security associations were not capable of binding to arbitrary multicast destinations.

A comparable protocol to MLD is IPv6 Neighbour Discovery (ND) [NNS98], which resolves last hop link-layer address mappings and routing between hosts and

---

[12] Le Reseau National de Telecommunications pour la Technologie Enseignement et la Recherche, http://www.renater.fr/

routers. It is worth noting that at this time, the IETF is in the midst of proposing similar systems for authentication of ND message exchanges [Ark05]. Both MLD and ND are involved in the automatic configuration and pose serious chicken-and-egg problems for IPv6 systems to use IPSec based key exchanges [Lou04, Nik04]. Additional considerations for MLD in different access network environments are provided in other IETF documentation [HM05, FHHS04, CKS05].

2.4.3 Mobile Multicast Issues

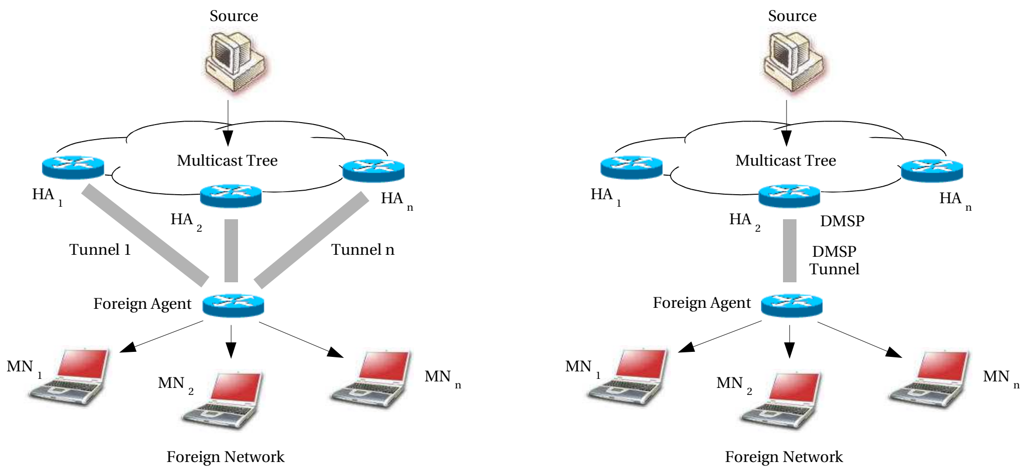
Tunneling

The current challenges in the provisioning of multicast services for mobile IP hosts are explored by the network research team at Laboratory, Louis Pasteur University (LSIIT) and their survey looks at specific issues related to the IETF proposed protocols for IPv4 mobile multicasting [JN03]. The research though, was conducted prior to the design of MIPv6 SSM protocols and does not address the specific problems.

The advantage of BT is that roaming hosts can rely on the availability of similar multicast services to its HN regardless of movement. Using BT, the HA needs to build an equal number (to the roaming hosts) of tunnels to the visited network. As shown in Figure 2.8(a), when MN_1, roams in the FN, the Home Agent, HA_1 has to build a tunnel to forward the multicast data. Similarly, tunnels have to be built for MN_2 till MN_n from their respective HAs. This technique is similar to that of handling unicast data and discards all the multicasting scaling advantages. Employing bi-directional tunneling to sustain mobile multicasting results in a ‘tunnel convergence’. A tunnel convergence happens when several mobile hosts (with or without similar listening states) roam in the same visited network. The disadvantages of BT are that all multicast bandwidth saving advantages are lost whenever more than a single host is in the visited network. The multicast data path is also not optimal due to the routing triangulation through the HA.

Mobile Multicast Protocol

To solve the tunnel convergence problem of BT, the Mobile Multicast Protocol (MoM) was proposed by Harrison [Har97]. In the MoM scheme, a Designated Multicast Service Provider (DMSP) is elected for each network from the numerous HAs corresponding to the listeners in the visited network. A simple illustration of this mechanism in Figure 2.8(b) shows the designation of HA_2 as the DMSP. The DMSP also acts as the tunneling point to the visited network for all multicast data delivery.



(a) Tunnel convergence.

(b) Mobile Multicast Protocol.

Figure 2.8: Mobile multicast protocol eliminates tunnel convergence.

The MoM method as it has been proposed for IPv4 systems cannot be extended directly onto MIPv6 due to the unavailability of a FA. The complex MoM protocol is due to the inability of the FN to pick the closest DMSP and the re-designation when (in the illustrated case) MN_2 either leaves the multicast group or the visited network. In mobile environments with dynamic and quick host movements, this scheme becomes quite cumbersome with multiple state changes and the need for the re-election of DMSPs. Although the DMSP method provides a marginal gain, it has not been pursued within the IETF.

RBMoM

The Range-Based Mobile Multicast (RBMoM) method was designed to reduce the (possibly) long tunnel distance using MoM. Lin's updated proposal [Lin02] uses a combination of BT and RS and provides simulated results for various network scenarios. The RBMoM [LW00] protocol uses Multicast Home Agents (MHA) in designated points in the network to serve a predetermined area as shown in Figure 2.9. RBMoM is similar to MoM but it has multiple MHAs with predefined service areas. In the FN, each host subscribes to and receives traffic from the assigned MHA in that coverage area. In the case of MH_1 currently being served by MHA_1 moving to the service range of MHA_2, a handover has to take place for it to continue receiving multicast data. This scheme is a compromise between the need for multicast tree reconfiguration and the possible shortest path delivery. Like MoM, the need for

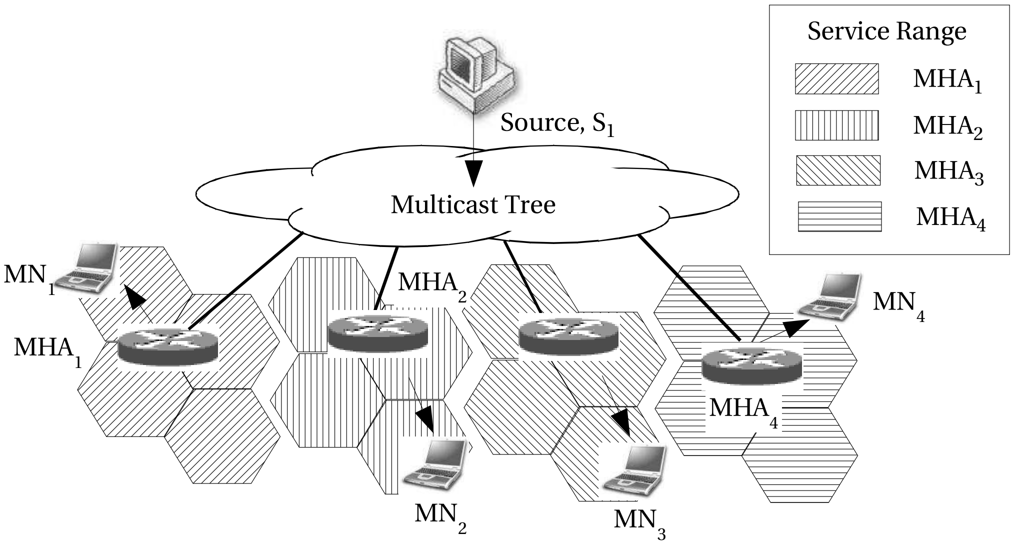


Figure 2.9: Service ranges in RBMoM protocol.

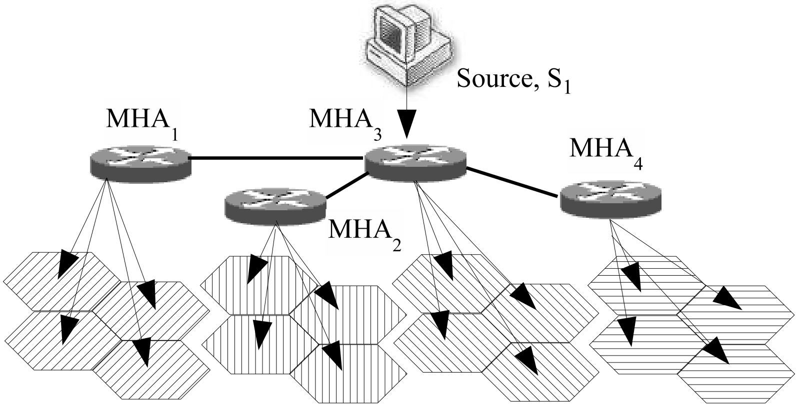


Figure 2.10: A hierarchical multicast architecture.

dedicated FAs for this scheme makes it difficult to implement in MIPv6 systems.

Hierarchical Multicast Agents

Several techniques have been proposed that uses the advantages of RS and BT [CCH99, MBM+99]. A hierarchical multicast architecture based on Multicast Agents (MAs) [WC01] was proposed by Wang. The proposed MAs serve multiple FNs as shown in Figure 2.10. The agent MHA_1 would join the multicast session and serve the host MN_1 These methods tackled with various degrees of success the problem of maintaining mobile multicast sessions by trying to reduce either tunnel convergence, multicast tree reconfiguration and optimised tunneling.

Dynamic Multicast Agent

The Dynamic Multicast Agent (DMA) is also designed to address the problem of delivering IPv6 multicast data to mobile hosts. The DMA method proposed by Zhang [ZSZ05] uses both the BT and RS methods. In the DMA proposal, a hybrid solution of Movement Based Method and Distance Based Method allows hosts to optimize multicast routes. The DMA method also reduces the number of handoffs by selecting new multicast agents dynamically. It aims to minimise routing triangulation and multicast handoff latency.

Remote Subscription

The BT associated disadvantages do not exist in the RS method since it delivers multicast traffic through the shortest available path from the source. The common perceived disadvantage of RS is that signaling has to be frequently updated and for fast moving nodes, it is less than optimal. We aim to show that the impact described above is minute (and it can be further reduced with minimal protocol enhancements) in comparison to the advantages gained. Table 2.2 shows the relative merits of both the RS and BT schemes.

While the use of bidirectional tunneling can ensure that multicast trees are independent of the mobile nodes movement, in some cases such tunneling can have adverse affects. The latency of specific types of multicast applications (such as multicast based discovery protocols) will be affected when the round-trip time between the foreign subnet and the home agent is significant compared to that of the topology to be discovered. In addition, the delivery tree from the home agent in such circumstances relies on unicast encapsulation from the agent to the mobile node. Therefore, bandwidth usage is inefficient compared to the native multicast forwarding in the foreign multicast system. At the time of this research, there were no known published performance analysis or results comparing the BT versus RS method of mobile multicasting.

Although all of the current proposals elegantly solve many of the current mobile multicast problems, they still remain largely in the realm of research. It is not clear whether any of the tunneling or agent-based systems could be deployed in large scale networks. We will argue that with the current advances in AAA and PIM-SSM support, it is worth exploring the RS method and examine its performance and advantages over the BT method.

	ADVANTAGES	DISADVANTAGES
Bidirectional Tunneling	Similar services available to that of the HN. Source-rooted trees for mobile sources. Possibly faster joins after handoffs.	Causes triangular routing. Service scalability limitations. Increases HA processing overhead. Increases traffic latency.
Remote Subscription	Optimal data path between source and mobile host. Inherits multicast bandwidth efficiency. Scalable architecture.	FN must be multicast capable. Requires native multicast support.

Table 2.2: A comparison of MIPv6 BT and RS advantages and drawbacks.

2.5 Conclusion

2.5.1 Discussion

A general survey and taxonomy of the current multicast research and the associated proposed solutions are provided by Mir [Mir01] and Ramalho [Ram03]. The MIPv6 SSM solution seems like the most promising way forward in mobile multicasting. To a large extent, SSM eliminates the protocol and deployment complexities of prior multicast architectures but at the expense of source mobility (in effect, change of source IP address) in highly mobile environments. However, we believe the trade-off is viable and practical for a significant number of applications and worthy of further research. However, there are many issues concerning the deployment and implementation, and to a lesser degree, specification of multicasting protocols in IPv6 to solve. With the current set of protocols, global IPv6 inter-domain multicast is impossible except using SSM. One of the known problems is that there is no viable mechanisms to convey information about multicast sources between PIM-SM RPs. The survey by Savola [Sav04] describes known problems, and raises issues to be addressed.

The IGMPv1 achieved dynamic group management and introduced unsolicited host reports to reduce the multicast join latency. IGMPv2 was able to reduce the leave latency by incorporating a leave message and distinguishing two types of query messages, i.e. a general query as in IGMPv1 and a group specific query. The group specific query has a short interval and is used to determine if there are any other remaining listeners on a subnetwork. IGMPv3 adds the ability to specify multicast sources and removes the host suppression functionality. There are circumstances when link-local multicast-blocking Ethernet switches which are important for wireless networks exist, but MLDv2 will not work [Sav04].

Under most circumstances, there is no prior knowledge of the number or demographics of multicast subscribers for any given group. The proposed mechanisms to secure multicast signaling are not extensible to any arbitrary group of users, and require manual configuration. Such manual configurations contradict the goals of achieving and maintaining IPv6 plug-and-play capabilities, and may not be possible to implement in MLDv2.

The IETF MIPv6 WG is moving forward to focus on deployment issues in MIPv6 and provide appropriate protocol solutions to address known deficiencies and shortcomings. The general challenges to achieve multicasting in mobile environments are documented by Jelger [JN02]. Among the various proposed solutions, one can observe that while all of them provide innovative mechanisms for optimised multicast data delivery, most of them have deployment problems. In particular, it is easy to deduce that most of the tunneling solutions do not scale with the size of the Internet. The proposed protocols also to some extent require pre-arranged collaboration between routers which belong to different entities. In the current form, the RS method does not provide mechanisms to enable local multicast sessions to survive handoffs and to seamlessly continue from a new CoA on each new foreign link. Any such mechanism developed as an extension to the current RS specification needs to take into account the impact of fast moving mobile hosts on the Internet. Host movement effects the multicast routing protocols and the proposed mechanism must have the ability to maintain the integrity of source specific multicast trees and branches.

The years of research and experimentation of multicasting has begun to show signs of architecture maturity. Multicasting is moving a step closer to commercial deployment. This Chapter has examined briefly the evolution of the multicasting protocols and limiting factors which have shaped them. The lessons learned from the initial many-to-many data delivery design and the ensuing complexity has motivated the pursuit of the simpler one-to-many model, and hence SSM.

The next stage of multicast research must include and consider the practical requirements of the source, the listeners and the network service providers. The service and protocol architecture must be easily deployable. The control and management should be able to scale with the growing Internet. Listeners expect to obtain multicast channels information everywhere, a secure service and more importantly a seamless service while mobile and roaming.

2.5.2 Research Scope

The potential adoption of MIPv6 SSM is rooted in the continued development, evaluation and standardisation of new protocols. The current group management signaling inefficiency, mobile latency and service scalability issues are gaps which need to be addressed in IPv6 mobile networks. The research for this thesis determines the effects of varying listener density distributions on the sparse mode multicast spanning trees and methods to minimise delays in initiating and maintaining multimedia applications in a mobile networks. With a host of new protocols being standardised for SSM and MIPv6, studies need to be conducted to evaluate their inter-working and performances. The impending growth of multicast applications will be likely in wireless networks using mobile devices as receivers. With inherently less bandwidth available in comparison to fixed networks, MLDv2 performance needs to be determined and where possible, enhanced.

One of the important areas yet to be addressed are group management issues in a mobile environment. There are no existing mechanisms to update access links and multicast routers, when a SSM host leaves. Neither is there a mechanism to trigger the new link to continue receiving multicast data when a host arrives. Both these issues are important ones to address and solve for delay-sensitive applications to work seamlessly with host movements in mobile networks.

The common negative perception of using RS to make multicasting available in visited networks has been the need to reconstruct the multicast tree with movement. The scaling property of such a mechanism needs to be investigated and determined. Our analysis determines the delay and processing cost of this process and argues that it is negligible in comparison to BT and other alternative proposals.

Chapter 3

MLDv2 Performance Evaluation

3.1 Introduction

The support of the Multicast Listener Discovery (MLD) protocol is a mandatory requirement for *all* IPv6 nodes [Lou04], making multicasting easier to adopt in IPv6 than in IPv4 systems. The IPv6 based MLD protocols provide equivalent capabilities to that of the IPv4 Internet Group Management Protocol (IGMP) to manage multicast groups. The MLDv2 protocol is based on the IGMPv3 as described in Sections 2.2.2 and 2.3.1. The MLDv2 is a core and critical protocol that provides multicast group management to support IPv6 SSM.

The current multicasting architectures and underlying protocols described in Section 2.2 were primarily designed for wired hosts, prior to the concept and design of mobility protocols, such as MIPv6. Hence, the dynamics and the performance of multicasting protocols for mobile hosts and networks have not been studied. As stated in our literature review in Section 2.4.1, we have not found any prior studies of MLDv2 signaling traffic efficiency for MIPv6 SSM networks. Although protocol efficiency is a valid concern within the IETF standardisation track, it is neither measured nor strict criteria have been agreed upon for standards approval and adoption [Bra96]. A proof of concept, inter-working with other existing protocols and security considerations drive the IETF protocol standardisation process.

The multicast signaling traffic and the resultant bandwidth consumption are important aspects to consider for multicasting support in wireless networks [Var02]. The total amount of bandwidth used by the application and the MLDv2 traffic are essential information for network planning and service provisioning purposes. Efficient multicasting is increasingly important due to the growing number of mobile hosts relying on the Internet for communications. The two key focus areas of the following research are to: 1) minimise multicast group management signaling traffic in order to preserve sufficient transmission capacity for bandwidth-limited access networks and 2) reduce movement induced multicast latencies to ensure seamless connections for mobile hosts. The literature review in Section 2.4.1 shows, both these issues above have not been addressed.

In this chapter, we first formulate an analysis framework to determine the MLDv2 traffic performance. In Section 3.4.4, the multicast join and leave latencies when a MN moves between subnets are determined. From the latency equations, we determine the potential maximum and minimum delays. In the interest of determining the MLDv2 protocol performance, the following MLDv2 study primarily concerns:

- the formulation of a framework and subsequent equations for measuring the signaling traffic,
- the characterisation of signaling traffic for multicast steady state, join and leave instances,
- the analysis of signaling traffic efficiency with various number of hosts and applications, and
- the determination of multicast latencies by relying only on group management updates.

The remainder of this chapter is organised in the following manner. The next section outlines the MLDv2 design rationale, features and functionalities incorporated in the protocol. The formalisation of the MLDv2 message exchanges into equations, the simulation experimental setup and analysis parameters used for the following analysis are described in Section 3.2. The MLDv2 protocol traffic and latency analysis is initially conducted with the recommended default timer settings and the associated results are presented in Section 3.4. The MLDv2 traffic analysis is further expanded by conducting experiments and obtaining results for various timer settings within the specified operating range. The chapter is concluded with an in depth analysis and discussion of the results obtained from the various equations and experiments.

3.2 Features and Functionalities

Unlike in MLDv1, the MLDv2 report messages contain the source IP (address) information for each subscribed multicast group, which is a basic requirement for the SSM model to work. The source address specifying capability means that hosts can choose or filter the multicast data from both desired and undesired source IP addresses for each multicast group. In order to support SSM, a host's IP service interface[1] must support the following operation:

IPv6MulticastListen (socket, interface, IPv6 multicast address, filter mode, source list) where,

- *socket* specifies the requesting entity; for example a unique identifier within a software program or process,
- *interface* specifies the identity of the local network attachment,
- *IPv6 multicast address* specifies the multicast group IP address,
- *filter mode* specifies the desired and/or undesired source IP address, and
- *source list* is used when multiple source records are held in the filter mode.

The IPv6 addressing schemes allow for a host's MLDv2 report message to be addressed only to the MRs. In MLDv1, report messages are broadcast to all hosts. With MLDv1 host suppression capability, multicast hosts do not need to respond when similar reports are received from other hosts on the network. The removal of host suppression from the MLDv2 specification means that all multicast hosts are required to respond to MR query messages. The multicast hosts' report message responses allow the MR to conduct per-host tracking. Per-host tracking is a requirement for Authentication, Authorisation and Accounting (AAA) in MIP systems which have been identified and summarised [ACG00] for various access schemes. Based on the AAA criteria, the various proposed mechanisms are being evaluated by the IETF with a view of recommending appropriate schemes [MB01].

The important new features of MLDv2 include,

- the IPv6 source address filtering,
- the reports sent to the 'all MLDv2-capable multicast routers' using the address `ff02::16` and

---

[1] A process or system call within a software implementation

- the removal of host-suppression.

A summary of all the MLDv2 changes and enhancements to the original MLDv1 protocol is provided in the specification [VC04, Appendix B].

3.3 Experimental Method

The MLDv2 protocol achieves multicast group management through a series of query and report message exchanges between the multicast router and the hosts. The following study starts with the relevant MLDv2 messages and timers which trigger the message sending for MIPv6 SSM hosts and routers. The type of messages, the occurrence sequence and the triggering timers are categorised according to multicast steady state, join and leave instances[2]. The messages and timers identified for the MLDv2 traffic are described and illustrated in Section A.1 and Figure A.1 of Appendix A respectively. The MLDv2 messages, the query/reply interaction and the resultant traffic on the link is formulated in Section A.4 of Appendix A. The derived MLDv2 signaling traffic equations are used for the analysis in the following sections.

The MLDv2 traffic calculations using all the equations derived in Appendix A represent an average data rate over the query and response message intervals. In order to obtain more representative results, where large enough deployments are not available for measurements, simulation experiments are necessary. The simulation experiment results represent the theoretical peak MLDv2 traffic data rates. The simulation models, network topology and protocol settings used for the experiments conducted in this chapter are given in Appendix B.

3.3.1 Parameters

Theoretically, there are no MLDv2 protocol specified limits imposed on the number of multicast channels a host could listen to simultaneously. However, multicasting is generally associated with high data rate and time-sensitive applications. The number of simultaneous multicast applications supported is commonly bound by other constraints like network resources, bandwidth, end host processing and display capabilities. In the case of mobile devices, they tend to have smaller user interfaces than those available to larger fixed hosts to process and display the application data.

---

[2] These multicasting terms are described and illustrated in Section 2.2.1 and Figure 2.7a respectively.

It is difficult to imagine and that there will be rare instances where users subscribe to multiple music, video or other real-time applications at the same time.

For the purpose of this research, the upper limit of simultaneous channels[3], $N_{\mathrm{G}} = 10$ is used[4]. Also, in wireless access networks even with the multicasting bandwidth efficiency advantage, there is a finite limit of applications which can be supported simultaneously due to finite bandwidth availability. The MLDv2 source filtering capability allows for source IP addresses to be in the include or exclude mode for each of the multicast group records. There are no empirical results or guidelines to base the setting on, but for the purpose of this research, one address in each mode is thought to be adequate.

The MLDv2 signaling traffic analysis is conducted for a varying number of multicast hosts. With the current multicast protocols, neither the source nor the routers know the number of multicast hosts they serves. Although there have been previous studies to predict the number of multicast hosts, these techniques have not been deployed to provide any empirical results [AABN03, FT99, LN00]. The only previous empirical multicasting measurements and studies available from the MBone audiocast sessions conducted by Almeroth et al. [AA97], do not provide any indication of the number of potential applications.

The results presented in the following sections assume that the access network and IP header overheads are common to both the multicast data and MLDv2 data packets. The results presented ignore the header lengths for both messages, rendering the results relative and not absolute values. The advantage of this approach is that the MLDv2 traffic calculations and analysis are valid across multiple (and independent of) underlying network access schemes. The MLDv2 signaling efficiency presented in the following sections are valid for both wireline and wireless networks. The MLDv2 signaling data rate is also analysed and compared to the multicast application data rate.

---

[3] The symbol G is used to denote *group* in previous multicast research and this thesis keeps to that convention.

[4] The only other IGMP analysis available in the literature review is for the RGMP proposal by Liao [LY04] which uses 15 channels as the upper limit. The reasoning behind this limit is similar to this research which assumes a practical multicast user limit.

3.4 Results with Default Protocol Settings

3.4.1 Query Response Interval Traffic

The MR periodically checks and refreshes the multicast host subscription states by sending a General Query (GQ) message, every Query Interval (QI), T_{QI}. Multicast hosts must reply with a Current State Record (CSR) message within the Query Response Interval (QRI), T_{QRI}, specified within the GQ message. As illustrated in Figure A.1 of Appendix A, the message exchange during the QRI represents the multicast steady state. The total number of MLDv2 messages during a QI, T_{QI} is given in Equation A.2. The resultant MLDv2 data rate, R_{MLD} in bps (Equation A.4) is given by,

$$R_{\mathrm{MLD}} = \frac{8(28 + N_{\mathrm{MN}}(8 + \sum_{i=1}^{N_G}(20 + 16N_{S_i}))}{T_{\mathrm{QRI}}}, \tag{3.1}$$

where T_{QRI} is the Query Response Interval, N_{G} is the number of multicast groups, N_{MN} is the number of multicast hosts and N_{S_i} is the number of data sources associated with the multicast group (in both the include and exclude modes).

The MLDv2 data rate in Equation 3.1 is dependent on the number of multicast groups, N_{G} but not the actual application data rate for any of the groups. The MLDv2 protocol's minimum, default and maximum timer settings [VC04] are shown in Table 3.1. With the default QI setting $T_{\mathrm{QI}} = 125$s and QRI setting $T_{\mathrm{QRI}} = 10$s, Table 3.2 shows the MLDv2 traffic data rate R_{MLD} for varying number of multicast hosts N_{MN}, groups N_{G} and number of data sources N_{S_i}. The results presented in Table 3.2 from Equation 3.1 show the *average* MLDv2 traffic data rate R_{MLD} within the QRI time, T_{QRI}. For example, for a network with $N_{\mathrm{MN}} = 100$, $N_{\mathrm{G}} = 5$ and $N_{S_i} = 10$, the average $R_{\mathrm{MLD}} = 72.66$ kbps. In practise, the MLDv2 data rate R_{MLD} might be higher due to the random reply time of CSR messages. The QRI specified within the GQ dictates the random duration within which each host has to reply with CSR messages. In order to get a better approximation of the actual peak MLDv2 data rate due to the randomness of report replies, simulation experiments are necessary.

The experiments are conducted in the simulated network which consist of multiple hosts connected to a MR using hubs on links as illustrated in Figure 3.1. The models created for the simulation experiments and the parameters used for the following study are given in Section B.1 of Appendix B. The MLDv2 messages exchanged between the MR and the hosts are captured and illustrated in Figure 3.2a. When a host sends a multicast join SCR message at t = 5s, neither the MR nor

PARAMETER	DEFAULT VALUE	MIN / MAX VALUE	NOTES
Robustness Variable (RV)	2	0 / 7	Number of message retransmissions
Last Listener Query Interval (LLQI)	1s	0 / 65.5s	Leave latency of last listener
Query Interval (QI)	125s	1s / 248s	Time between GQs
Query Response Interval (QRI)	10s	0s / 65.5s	$T_{\text{QRI}} < T_{\text{QI}}$

Table 3.1: MLDv2 parameters and their settings.

N_{MN}	N_G	N_{S_i}	R_{MLD} (KBPS) AVERAGE	R_{MLD} (KBPS) PEAK
1	1	1	0.06	0.67
5	1	1	0.20	1.34
10	1	1	0.37	1.82
10	1	2	0.50	2.67
10	2	2	0.92	3.65
10	5	2	2.17	7.39
10	5	5	4.09	8.77
10	10	5	8.09	25.15
100	5	5	40.66	57.00
100	5	10	72.66	106.18

Table 3.2: Average and peak MLDv2 steady state link traffic.

any other multicast host needs to respond with MLDv2 messages. When the MR sends a GQ message at t = 10s, all the existing multicast hosts respond with CSR messages within the specified default QRI, T_{QRI} = 10s between t = 10s to t = 20s.

The MLDv2 messages of Figure 3.2a are plotted against time and shown as the MLDv2 data rate R_{MLD} in Figure 3.2b. The *peak* R_{MLD} results from the simulation experiments shown in the fifth column of Table 3.2 are higher than the *average* R_{MLD} calculated from Equation 3.1. In the steady state without any multicast host joins or leaves, the MLDv2 traffic R_{MLD} pattern will repeat for during the QRI duration T_{QRI} every QI duration T_{QI}. As shown in Figure 3.3, the first MR query message is sent at t = 10s, followed by t = 135s and t = 260s for a QRI default setting, T_{QRI} = 125s.

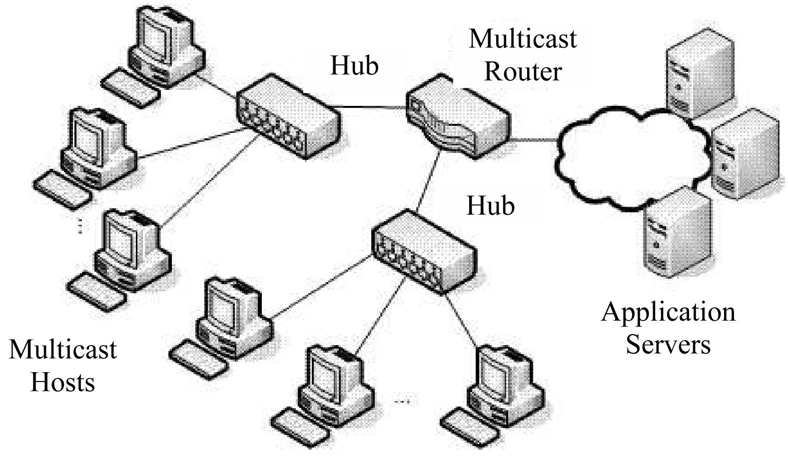
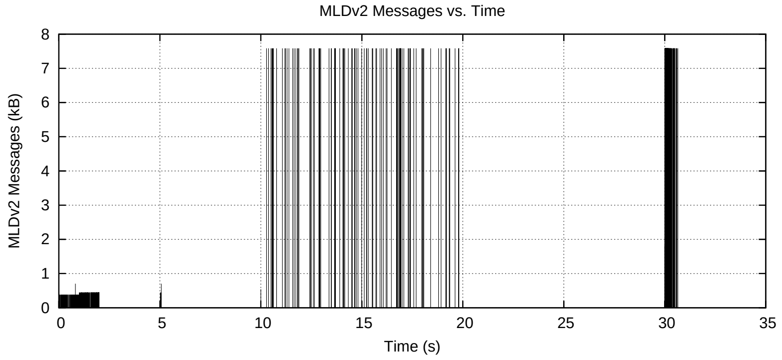
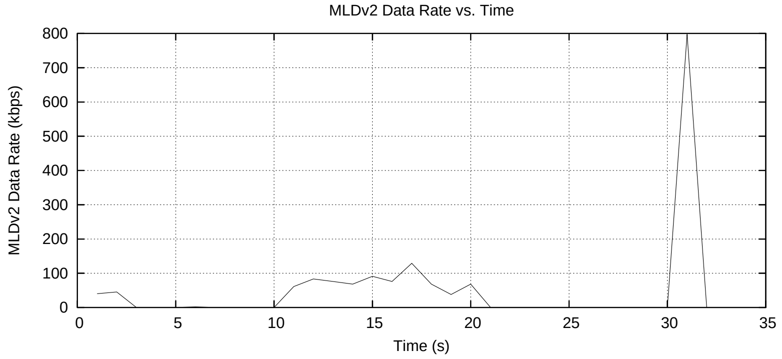


Figure 3.1: Network diagram of simulation experiment.



(a) Messages



(b) Data rate

Figure 3.2: The MLDv2 traffic during a GQ, multicast join and leave.

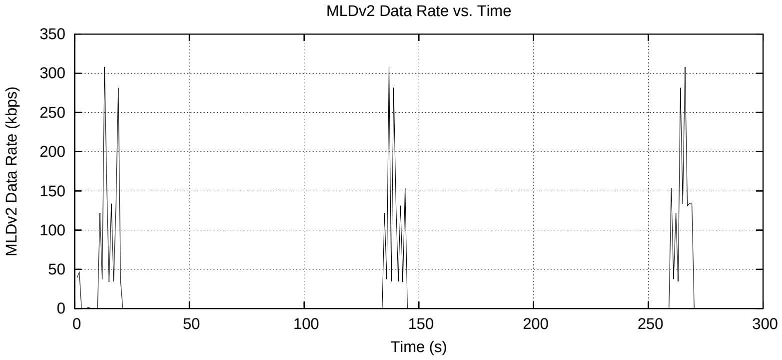


Figure 3.3: The MLDv2 traffic in the steady state over multiple QI and QRI.

3.4.2 Efficiency: Signaling Overhead Factor (η)

The MLDv2 traffic contribution for achieving group management is considered the signaling overhead associated with each multicast channel. For the purpose of this research, we define the MLDv2 signaling overhead factor, η for each multicast channel and associated application data rate as,

$$\eta = (1 + \frac{R_{\mathrm{MLD}}}{R_{\mathrm{APP}}}), \tag{3.2}$$

where R_{MLD} is the MLDv2 signaling data rate and R_{APP} is application data rate. The MLDv2 signaling overhead factor η in Equation 3.2 simplifies the necessary calculations for bandwidth provisioning in multicast networks. For multicast network bandwidth planning, each multicast channel (bandwidth) provided must be multiplied by the factor η to ensure no data nor signaling packets are lost through network congestion.

The results in Table 3.3 show the corresponding MLDv2 overhead factor η values for the average MLDv2 signaling traffic R_{MLD} using Equation 3.2. The results in Table 3.3 also show the corresponding peak η values from the R_{MLD} obtained through the simulation experiments. For the purpose of this analysis, the signaling factor η is calculated with $R_{\mathrm{APP}} = 20$ kbps. There is a net increase in MLDv2 signaling traffic R_{MLD} with the number of channels MLDv2 manages but it is not linear relationship. The increase of R_{MLD} is minimal in comparison to N_{G} because multiple multicast records of the same host are packed into a single CSR message. The MLDv2 signaling overhead efficiency is tied with the number of multicast channels it manages. The precise method of calculating MLDv2 signaling efficiency also considers the application data rates of the channels managed. The application data rate R_{APP} is indicative of the type of access network and bandwidth available.

N_{MN}	N_G	N_{S_i}	η Average (Theory)	η Peak (Simulations)
1	1	1	1.00	1.03
5	1	1	1.01	1.07
10	1	1	1.02	1.09
10	1	2	1.03	1.01
10	2	2	1.02	1.09
10	5	2	1.02	1.04
10	5	5	1.02	1.09
10	10	5	1.04	1.13
100	5	5	1.41	1.57
100	5	10	1.73	2.06

Table 3.3: The average and peak MLDv2 signaling overhead factor (η) with R_{MLD} = 20 kbps for various N_{MN}, N_{G} and $N_{\mathrm{S_i}}$.

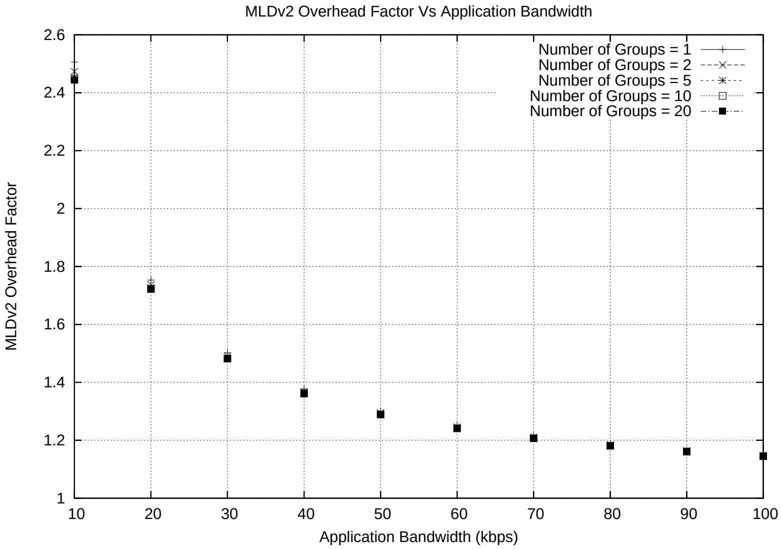


Figure 3.4: The MLDv2 signaling overhead factor, η versus multicast application data rates.

In Figure 3.4 the factor η is plotted for various numbers of groups N_{G} with filtering mode N_{S_i} = 10 and number of hosts, N_{MN} = 100. The MLDv2 signaling overhead factor η remains almost constant for various number of groups, N_{G} with a constant application data rate R_{APP} for all multicast groups. For simple location based services like weather and traffic updates which use only text transmissions, the application data rate being less than 10kbps, the signaling overhead η is a large value. The resulting MLDv2 signaling efficiency for small data rate applications is low.

3.4.3 Last Listener Query Interval Traffic

The multicast steady state changes when a join or leave message is sent by a host. Both occurrences cause different types of MLDv2 message exchanges and the resultant MLDv2 signaling traffic as shown in Figure A.1 of Appendix A. The join SCR message received at t = 5s in Figure 3.2a, shows no impact on R_{MLD} and explained in Section 3.4.1. If the join SCR is for a channel with existing listeners on the link and contains the same associated include and exclude modes, there is no link traffic impact. The join SCR message received by the MR could be for a completely new channel i.e. without existing hosts listening on the link. The MR updates the PIM-SSM routing protocol with the new SCR and the multicast data is forwarded to the link. When the join SCR for a channel with existing multicast hosts is received, but with different include and exclude modes, a MASSQ message has to be sent. All the existing multicast hosts have to respond with a CSR message.

As shown in Figure A.1 of Appendix A, when the MR receives a leave SCR message, it sends a Multicast Address Source Specific Query (MASSQ) message. All the existing multicast hosts on the network listening to the same channel have to send corresponding CSRs within the Last Listener Query Interval (LLQI). The LLQI period, T_{LLQI} is specified within the MASSQ message. Both the leave SCR and MASSQ messages are RV dependent and they are retransmitted according to the RV setting. The number of MLDv2 messages and the respective message lengths during a multicast leave are given in Equation A.5 in Appendix A. During an LLQI, the MLDv2 signaling traffic, $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ in bps is given by (Equation A.6),

$$R_{\mathrm{MLD}_{\mathrm{LLQI}}} = \frac{(RV + 1 + N_{\mathrm{MN}}) \times (8 + \sum_{i=1}^{N_G}(20 + 16N_{S_i}))}{T_{\mathrm{LLQI}}}, \tag{3.3}$$

where T_{LLQI} is the Last Listener Query Interval period and RV is the Robustness Variable. The average MLDv2 traffic $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ for various number of multicast hosts N_{MN}, groups N_{G} and sources in both include and exclude modes N_{S_i} calculated from Equation 3.3 are given in Table 3.4. The default LLQI duration T_{LLQI} = 1s and with the number of hosts N_{MN} = 100 from Equation 3.3 the average MLDv2 traffic during LLQI, $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ = 93.52 kbps.

The peak $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ results obtained from the simulation experiments are illustrated in Figure 3.2a. When a leave SCR message is received at t = 30s, all the existing multicast hosts have to respond with CSR messages within the LLQI duration, T_{LLQI} = 1s. The resultant MLDv2 signaling traffic $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ is shown between t = 30s and t = 31s. The MLDv2 signaling traffic is significant in a large

N_{MN}	N_G	N_{S_i}	$R_{\text{MLD}_{\text{LLQI}}}$ (KBPS) AVERAGE	$R_{\text{MLD}_{\text{LLQI}}}$ (KBPS) PEAK
1	1	1	0.18	0.59
5	1	1	0.35	0.96
10	1	1	0.57	2.33
10	1	2	0.78	5.32
10	2	2	1.46	12.57
10	5	2	3.48	22.70
10	5	5	6.60	48.31
10	10	5	13.10	77.62
100	5	5	52.32	252.41
100	5	10	93.52	796.62

Table 3.4: Average and peak MLDv2 signaling traffic during a multicast leave.

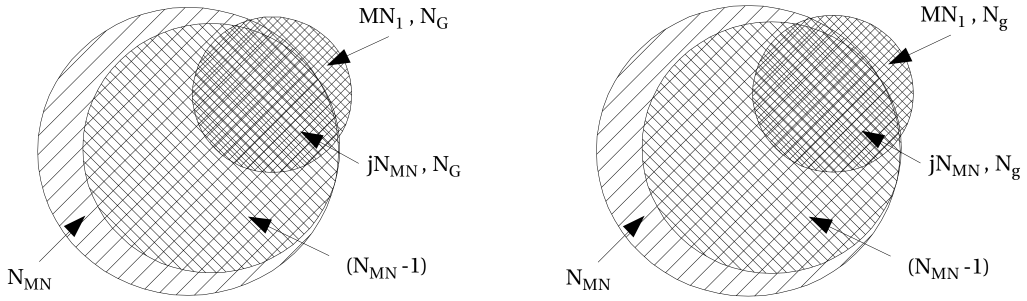
homogeneous multicast listener base with the leaving of even a single multicast host.

When a host unsubscribes to one or more multicast channels, there might be other existing listener hosts for the same channels on the link. However, it is possible that not all of the other multicast hosts on the link are listening to all of the same unsubscribed channels. In this case, unlike the consideration for Equation 3.3, a completely homogeneous host listening state on the link does not exist. In Figure 3.5(a), the area N_{MN} represents the total number of hosts on the link. A leaving multicast host MN_1 can unsubscribe to all of its channels N_{G} which are commonly shared by a fraction of hosts, jN_{MN} $(0 \leqslant j \leqslant 1)$ of the total multicast hosts N_{MN} on the link. The hosts jN_{MN} which respond with CSR messages during the multicast leave of host MN_1 are represented by $(jN_{\text{MN}}, N_{\text{G}})$. In this instance, the resulting MLDv2 signaling traffic, ${R^j}_{\text{MLD}_{\text{LLQI}}}$ in bps, is given by,

$$ {R^j}_{\text{MLD}_{\text{LLQI}}} = \frac{(RV + 1 + jN_{\text{MN}}) \times (8 + \sum_{i=1}^{N_G}(20 + 16N_{S_i}))}{T_{\text{LLQI}}}, \tag{3.4} $$

where T_{LLQI} is the Last Listener Query Interval, RV is the Robustness Variable, jN_{MN} is number of proportional multicast hosts, N_{G} the number of channels and N_{S_i} the number of sources in both include and exclude modes.

As shown in Figure 3.5(b), it is also possible to receive a leave SCR message from the host MN_1 with a number of channels, N_{g}. The number of unsubscribed channels, N_{g} could be less than the total number of multicast channels N_{G} on the link. The number of channels N_{g} is common but not completely equal to the total number of channels N_{G}, i.e. $(0 \leqslant N_{\text{g}} \leqslant N_{\text{G}})$. The number of unsubscribed channels N_{g} might not be subscribed by all the hosts, N_{MN}. If the proportion of hosts jN_{MN}



(a) Proportional Hosts.

(b) Proportional Groups.

Figure 3.5: Multicast host leaves in non-homogeneous listener networks.

have also subscribed to the same number of common channels N_{g}, then the resultant MLDv2 traffic ${R^{jg}}_{\mathrm{MLD}_{\mathrm{LLQI}}}$ is given by,

$$ {R^{jg}}_{\mathrm{MLD}_{\mathrm{LLQI}}} = \frac{(RV + 1 + jN_{\mathrm{MN}}) \times (8 + \sum_{i=1}^{N_g}(20 + 16N_{S_i}))}{T_{\mathrm{LLQI}}}, \tag{3.5} $$

where T_{LLQI} is the Last Listener Query Interval, RV is the Robustness Variable, jN_{MN} is number of proportional multicast hosts, N_{G} the number of common channels and N_{S_i} the number of sources in both include and exclude modes.

The resultant MLDv2 signaling traffic ${R^{jg}}_{\mathrm{MLD}_{\mathrm{LLQI}}}$ is similar to that of Equation 3.3, but ${R^{jg}}_{\mathrm{MLD}_{\mathrm{LLQI}}}$ changes with a *spread* factor, $(\frac{N_g}{N_G} \times jN_{\mathrm{MN}})$, and the proportional number of hosts, jN_{MN}. The MLDv2 link traffic ${R^{jg}}_{\mathrm{MLD}_{\mathrm{LLQI}}}$ results for a random *spread* factor are plotted in Figure 4.6a.

3.4.4 Join and Leave Latency

A handoff occurs when a multicast host moves from one point of attachment on the access network and subsequently re-attaches to another. The IP layer and multicast group management effects due to the handoff depends on the connection of both the previous and new access points in the mobile network topology. Mobile multicast host movements can be classified into three different types:

- *Between APs only*; host movement from one AP to another, connected to the same multicast router interface,
- *Intra-router*; host movement from one AP to another connected to different interfaces of the same router and

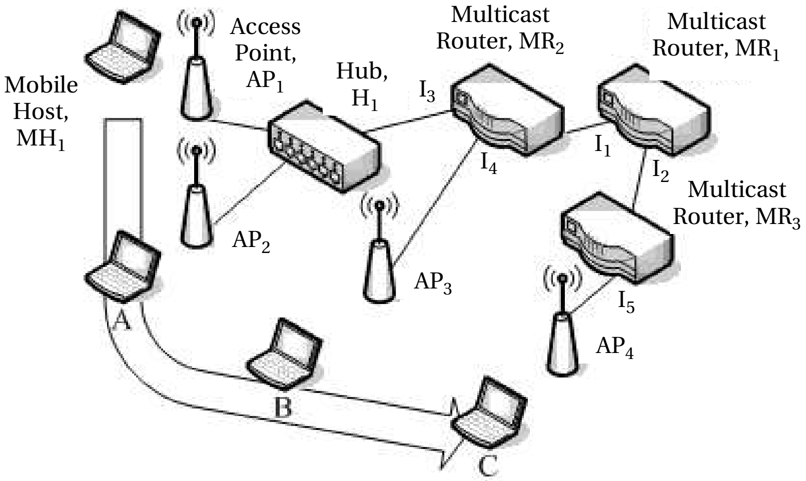


Figure 3.6: Mobile multicast host movements.

- *Inter-router*; host movement from one AP to another connected to different routers.

The possible types of host movement described above are illustrated in Figure 3.6. For the MLDV2 latency studies in this chapter, only the types of handoff which require group management updates are considered. In order to continue receiving multicast data, host movement for handoff types B and C in Figure 3.6 need MLDv2 updates.

In Figure 3.6, when host MN_1 moves from AP_1 to AP_3, it will have to wait for the next scheduled MLDv2 GQ message sent by MR_2 on interface I_4. Upon receiving the GQ message, the host MN_1 will have to respond with a CSR message to continue receiving multicast data. The timing intervals and the handover point during the MN movement is shown in Figure 3.7. The Join Latency T_{JL}, is the MLDv2 message exchange caused by the host movement and is given by,

$$T_{\mathrm{JL}} = T_{\mathrm{QI}} + t_r - \tau, \tag{3.6}$$

where τ is the MN handover time which has lapsed since the last GQ on the new link, T_{QI} is the Query Interval of the newly joined link and t_r is the random CSR message reply time within T_{QRI}. The default settings for $T_{\mathrm{QI}} = 125\mathrm{s}$ and $T_{\mathrm{QRI}} = 10\mathrm{s}$. In the worst case scenario, with $t_{\mathrm{r}} = 10\mathrm{s}$ (default T_{QRI}) and $\tau = 0\mathrm{s}$, the maximum potential Join Latency from Equation 3.6 is $T_{\mathrm{JL}} = 135\mathrm{s}$. Simulation experiments are conducted to determine the average Join Latency T_{JL} with various T_{QI} settings. The Join Latency T_{JL} for 50 random host movements with default $T_{\mathrm{QI}} = 125\mathrm{s}$ are illustrated in Figure 3.8a. The summary of the T_{JL} results from the experiments

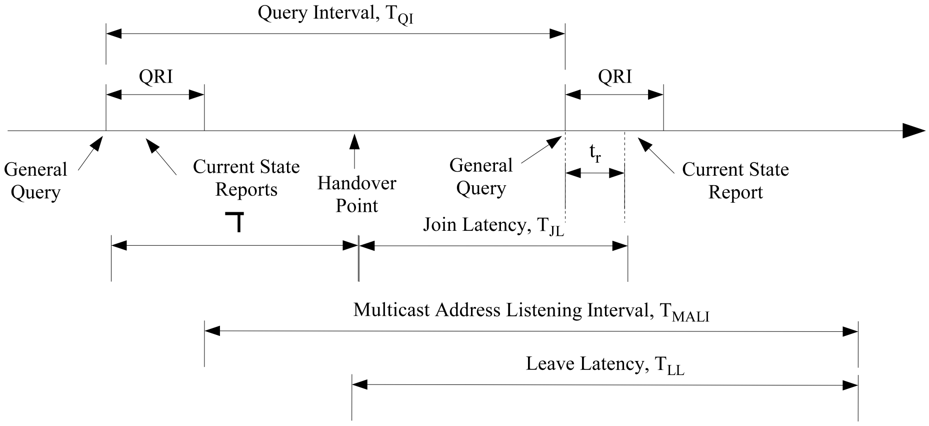


Figure 3.7: Multicast join and leave latency time intervals and time lines.

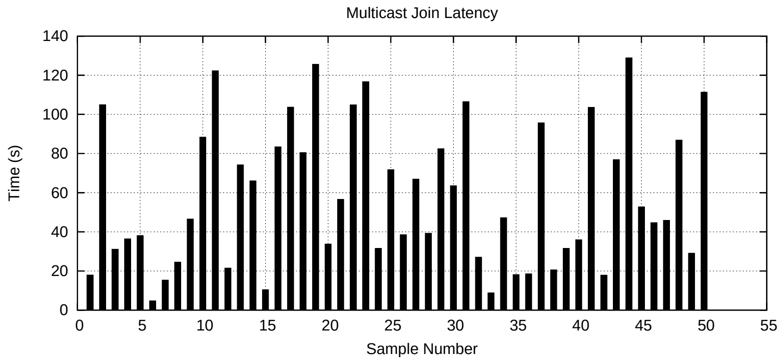
with a range of T_{QI} settings are presented in Table 3.5.

Referring to Figure 3.6, it is possible that the moving host MH_1 is the only listener of one or more channels on the interface I_3 served by access points AP_1 and AP_2. When the host MH_1 moves to a new access point, AP_3 or AP_4, it leaves behind a trailing multicast record in the previous interface I_3. The time it takes for the MLDv2 protocol to update and remove the trailing MAR on interface I_3 is called the Leave Latency, T_{LL}, and it is given by,

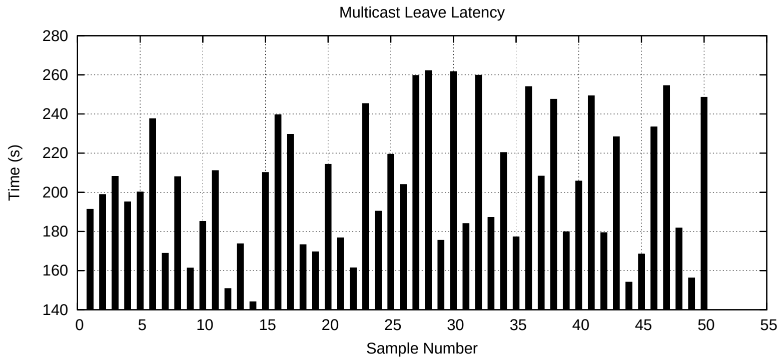
$$\begin{aligned} T_{\mathrm{LL}} &= (T_{\mathrm{MALI}} + T_{\mathrm{LLQI}}) - \tau, \\ &= ((\mathrm{RV} \times T_{\mathrm{QI}}) + T_{\mathrm{QRI}}) + T_{\mathrm{LLQI}} - \tau, \end{aligned} \tag{3.7}$$

where, RV is the Robustness Variable, T_{QI} is the Query Interval, T_{MALI} is Multicast Address Listener Interval, T_{LLQI} is Last Listener Query Interval, T_{QRI} is the Query Response Interval and $\mathrm{t} = \tau$ is the MN handover time. The Leave Latency T_{LL} represents the duration in which the network resources are wasted by the multicast trailing states left in the previous link.

With default MLDv2 timer settings, from Equation 3.7 the maximum Leave latency, $T_{\mathrm{LL}} = 261\mathrm{s}$. Simulation experiments are conducted to determine the average Leave Latency T_{LL} with various protocol timer settings. The Leave Latency T_{LL} results from the simulation experiments for 50 random host movements with default protocol timer settings are presented in Figure 3.8b. A summary of the latency results from the rest of the experiments are given in Table 3.5.



(a) Join latency



(b) Leave latency

Figure 3.8: The MLDv2 handover latency results.

3.5 Results from Protocol Tuning

3.5.1 Robustness Variable

The MLDv2 standard [VC04, Section 9] equates the number of message retransmissions to the protocol robustness. The RV setting of the MLDv2 protocol determines the number of message retransmissions. The MLDv2 protocol is robust to a factor of (RV – 1). The RV can be set between a minimum of zero and a maximum of seven as shown in Table 3.1 [VC04, Section 9]. The MLDv2 GQ and CSR messages (which are only used to refresh the current multicast listening state record on the MR) are independent of the RV setting. The GQ and CSR messages are sent only once per instance to avoid overloading the network with MLDv2 signaling traffic. Hence, the RV setting does not affect the multicast steady state MLDv2 signaling

	T_{QI} (s)	MIN (s)	MAX (s)	AVERAGE (s)
T_{JL}	125	4.77	122.31	58.21
	60	5.18	59.89	35.17
	30	5.18	28.44	17.84
T_{LL}		137.38	280.01	194.99

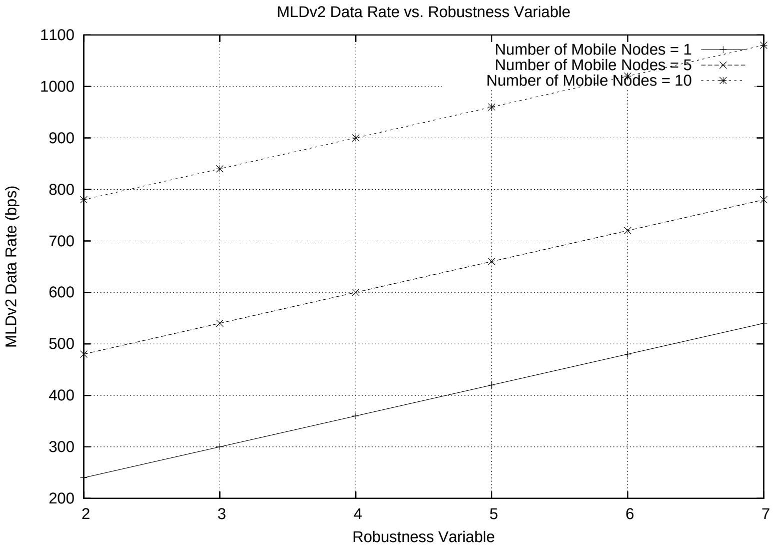
Table 3.5: A summary of the join and leave latency results.

traffic R_{MLD} as given by Equation 3.1. Similarly, the RV setting has no bearing on the MLDv2 signaling overhead factor, η, in Equation 3.2.

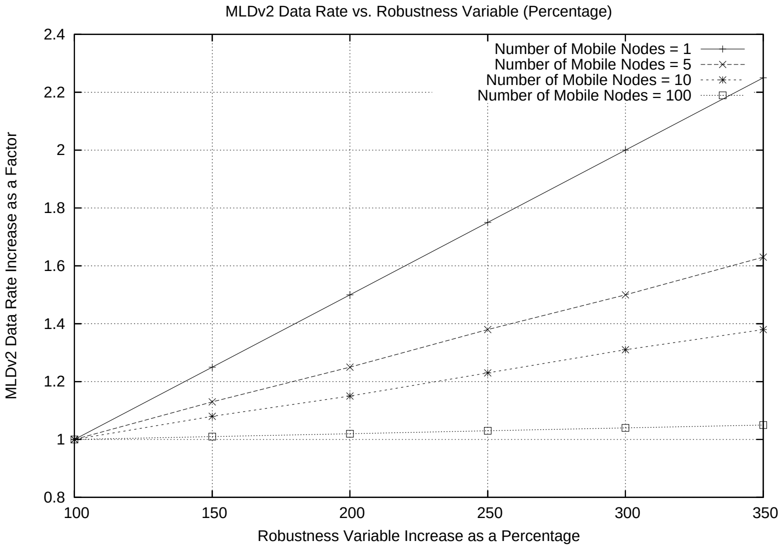
The MLDv2 state change MASSQ and SCR messages are RV dependent to ensure robustness. The multicast leave MLDv2 traffic $R_{\text{MLD}_{\text{LLQI}}}$ in Equation 3.3, increases with RV. The MLDv2 signaling data rate, $R_{\text{MLD}_{\text{LLQI}}}$ increases linearly with RV when the number of hosts N_{MN} is relatively small (i.e. RV $\simeq N_{\text{MN}}$) as shown in Figure 3.9a for $N_{\text{MN}} = 1, 5, 10$. For a large number of multicast hosts, ($N_{\text{MN}} \gg$ RV), RV has minimal effects on $R_{\text{MLD}_{\text{LLQI}}}$.

In a network with $N_{\text{MN}} = 1$, increasing the default RV $= 2$ setting to a maximum of RV $= 7$, increases the MLDv2 data rate $R_{\text{MLD}_{\text{LLQI}}}$ by a factor of 2.25. In a network with $N_{\text{MN}} = 100$, increasing the default RV $= 2$ setting to a maximum of RV $= 7$, increases the MLDv2 data rate $R_{\text{MLD}_{\text{LLQI}}}$ by a factor of 1.05. As shown in Figure 3.9b, the relative increase of MLDv2 signaling traffic $R_{\text{MLD}_{\text{LLQI}}}$ is higher for a smaller number of hosts ($N_{\text{MN}} = 1, 5, 10$). The phenomena observed in Figure 3.9b is explained in the following text. As shown in Figure A.1 of Appendix A, during a multicast leave, the number of SCR messages N_{SCR} is relatively small in comparison to the number of CSR messages N_{CSR}, ($N_{\text{SCR}} \lll N_{\text{CSR}}$). Since N_{CSR} is RV independent, the increase of the RV dependent N_{SCR} contribution to $R_{\text{MLD}_{\text{LLQI}}}$ in Equation 3.3 is negligible.

The RV setting does not control the QI, which is used to send GQ messages and refresh the multicast state in the MR. Hence, the RV setting does not affect the multicast Join Latency, T_{JL} in Equation 3.6. The RV setting does however affect the multicast Leave Latency T_{LL}, which is a multicast state change event. The Leave Latency T_{LL} as given by Equation 3.7, increases (almost) in proportion to RV (with $T_{\text{QRI}} \leqslant T_{\text{QI}}$ and $T_{\text{LLQI}} \lll T_{\text{QI}}$). With all the MLDv2 timer and RV settings at default values, the Leave Latency $T_{\text{LL}} = 261$s. If all MLDv2 protocol timers have default settings, the maximum setting of RV $= 7$, increases the Leave Latency to $T_{\text{LL}} = 886$s. If RV $= 7$ and all MLDv2 protocol timer settings are at maximum, the Leave Latency, has a theoretical maximum of $T_{\text{LL}} = 238983.2$s.



(a) The increase in actual $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$.



(b) The increase in $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ as a percentage.

Figure 3.9: The multicast leave MLDv2 data rate with various RV settings.

3.5.2 Query Interval

The MR sends out a GQ message to the subnets it serves every QI, T_{QI}. The QI setting does not affect the multicast steady state and multicast leave MLDv2 signal-

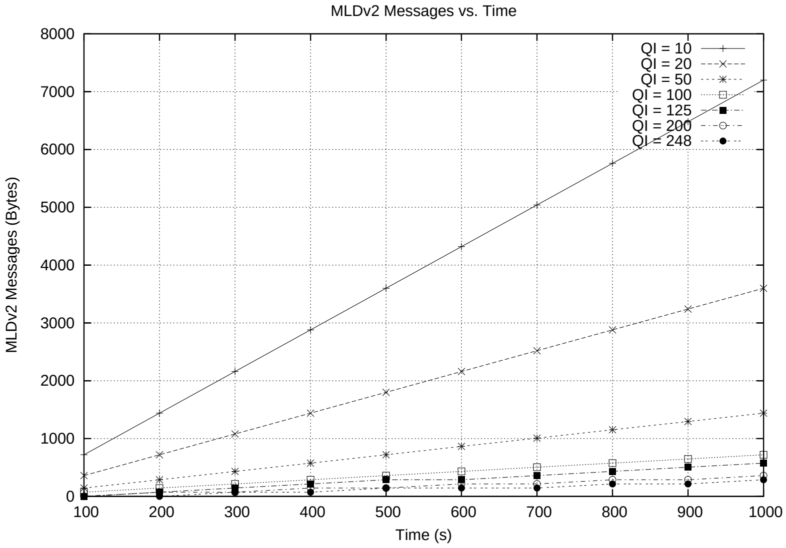


Figure 3.10: The MLDv2 messages for various QI.

ing data rate (R_{MLD} and $R_{\text{MLD}_{\text{LLQI}}}$) as given in Equation 3.1 and 3.3 respectively. The QI setting does however, affect the total amount of MLDv2 messages which are sent over the Multicast Address Listening Interval, T_{MALI} duration. The T_{MALI} interval associated with each MAR in the MR might be over several T_{QI} intervals ($T_{\text{MALI}} \gg T_{\text{QI}}$). Decreasing the T_{QI} setting, increases the frequency of GQ messages sent by the MR and ultimately the number of reply CSR messages. The total number of MLDv2 messages for various QI settings is shown in Figure 3.10. With the default QRI setting T_{QRI} = 10s, the minimum QI should not be lower than QRI ($T_{\text{QRI}} \geq$ 10s). All the reply CSR messages cannot be expected by the router before t = T_{QRI}. The MLDv2 signaling overhead factor, η from Equation 3.2, is QRI dependent and not affected by the QI setting.

From Equation A.11, the Join Latency T_{JL} is dependent on the QI setting, T_{QI}. A smaller T_{QI} setting lowers the Join Latency T_{JL}. A smaller T_{QI} setting also lowers the Leave Latency T_{LL} as given in Equation 3.7. With all other MLDv2 timers at default setting, the Leave Latency can vary from T_{LL} = 11s (with (($T_{\text{QI}} = T_{\text{QRI}}$ = 10s) + (T_{LLQI} = 1s)) to T_{LL} = 63559s for the maximum QI setting, T_{QI} = 248s.

3.5.3 Query Response Interval

The QRI is the given duration for multicast hosts to reply with CSR messages after receiving a GQ message. As shown in Figure 3.7, the multicast hosts reply after a random interval, t_r, within the duration T_{QRI}. The random reply scheme ensures that not all hosts reply with CSR messages at once. If all the multicast hosts send CSR messages at the same time, a MLDv2 signaling traffic R_{MLD} spike will be caused every T_{QI}. The steady state MLDv2 signaling traffic R_{MLD} from Equation 3.1 is T_{QRI} dependent. The R_{MLD} on the link is inversely proportional to the T_{QRI} setting.

As given in Table 3.1, the QRI has a setting range between T_{QRI} = 0s to T_{QRI} = 65.5s. For example, reducing QRI from the default value of T_{QRI} = 10s to T_{QRI} = 1s, increases the *average* R_{MLD} = 726.6 kbps and the *peak* R_{MLD} = 1.062 Mbps with the same experimental parameters as given in Table 3.2.

The QRI setting affects the MLDv2 signaling overhead factor, η, as given in Equation 3.2. The factor η increases inversely to T_{QRI}. The QRI setting does not affect the Join Latency, T_{JL}. The QRI does however, impact the Leave Latency T_{LL} as given in Equation 3.7. With all other MLDv2 protocol timers at default settings, tuning QRI between the minimum and maximum settings causes the Leave Latency T_{LL} = 251.0s and T_{LL} = 361.5s.

3.6 Discussion

The analysis framework and equations derived in this chapter have been used to determine the MLDv2 protocol efficiency and latency performances. One of the MLDv2 performance indicators is the group management granularity[5]. The MLDv2 performance is measured by the ability to learn about and act upon listening to state changes of multicast hosts quickly. The QRI has to be at the lowest possible setting ($T_{QRI} \longrightarrow 0$) to ensure timely CSR message updates. The QRI setting impacts the the MLDv2 signaling traffic R_{MLD} and $R_{\mathrm{MLD_{LLQI}}}$ for both the multicast steady state and state change occurrences. Hence, a lower T_{QRI} setting adversely impacts the MLDv2 signaling overhead factor, η. A higher MLDv2 overhead factor η decreases the MLDv2 signaling efficiency. The MLDv2 signaling efficiency is an important consideration where available network bandwidth is constrained or at a premium, which happens in most wireless access networks.

The MLDv2 signaling overhead factor η has to be taken into consideration for access network bandwidth provisioning purposes. If the QRI setting is lowered without considering η, both the MLDv2 messages and multicast data packets will be lost every QI (for the duration of QRI) when the access network bandwidth limit is breached. Decreasing the QRI also increases the multicast leave MLDv2 signaling

---

[5] The concept and description of MLDv2 granularity is introduced in Section 1.4.

traffic $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$. If the total MLDv2 signaling traffic $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ and application bandwidth R_{APP} data rate is larger than the access network band width, R_{ACC}, then packets will be lost. The multicast data packets and MLDv2 signaling messages will be lost for the duration T_{LLQI} during the access network bandwidth breach.

The results in Section 3.4.2 show that in order to support small bandwidth applications the MLDv2 signaling overhead factor η is higher. In bandwidth constrained access networks, contrary to what is ideal, the MLDv2 signaling traffic R_{MLD} utilises a higher proportion of the bandwidth. For example, from Figure 3.4, the η for a digital radio[6] application of 128kbps, is negligible. However, location based services like weather forecasts, traffic reports and public transport schedules are primarily text based applications with, R_{APP} = 5 - 10 kbps and the associated MLDv2 signaling overhead η is large.

The MLDv2 signaling overhead factor η is independent of the number of multicast groups N_{G} subscribed. The MLDv2 protocol design improves signaling efficiency by cascading[7] all the host's scheduled reports into a single MLDv2 CSR message. This improves MLDv2 signaling efficiency over IGMPv2 as shown in results presented by Liao [LY99].

In high mobility perceived networks (i.e. with rapid and frequent multicast host handoffs), a higher MLDv2 group management granularity is required. Faster MLDv2 updates ensure that minimal wastage of the limited bandwidth available in wireless access networks. The Join Latency, T_{JL}, is the delay or disruptive period for the multicast service during a host handoff. To minimise the Join Latency T_{JL}, the QI, T_{QI} needs to be set at a low value. The network bandwidth wastage during the Leave Latency T_{LL} is dependent on the number of multicast groups N_{G} and associated application data rate R_{APP} subscribed by the last listener. The bandwidth wastage during T_{LL} is significantly higher than a proper multicast host leave SCR message sequence. The leave SCR message decreases the MAR trailing state to T_{LLQI} with default $T_{\mathrm{LLQI}} = 1\mathrm{s}$.

The MLDv2 RV setting determines the protocol robustness. The MLDv2 robustness is an important consideration in wireless access networks where data packets are more likely to be lost or dropped. The packet loss can be frequent and severe with estimates varying between 1% to 30% [Var02].

The MLDv1 protocol signaling overhead increases with number of groups N_{G}

---

[6] The provisional Australian proposal for digital radio services has allocated 128kbps and 256kbps data rates.

[7] This is however subject to the MAR and MLDv2 packet size is less than the Maximum Transmission Unit (MTU). The Ethernet MTU is 1550 KB.

but not the number of hosts N_{MN} because of the host suppression feature. The MLDv1 signaling traffic makes if suitable for networks with a small number of multicast groups but capable of supporting large number of multicast hosts. The MLDv2 protocol is capable of of per-host tracking by removing the host suppression feature. The per-host tracking function is important for supporting AAA systems. However without the MLDv1 host suppression functionality, the MLDv2 signaling traffic R_{MLD} increases linearly with the number of multicast hosts N_{MN}, as shown in Table 3.2. The MLDv2 signaling traffic R_{MLD} is more suited to a large number of groups N_{G} subscribed by a small number of multicast hosts N_{MN}. However, without host suppression, MLDv2 has also enabled the use of snooping switches in access networks. The workings and bandwidth efficiency advantages of snooping switches are given in Section 4.2.3.

3.7 Conclusion

In this chapter, a MLDv2 performance evaluation framework and the required equations are derived and presented. Using the framework, a MLDv2 performance evaluation is conducted for the default timer settings and the corresponding results are presented. The analysis is further extended for the entire operating range of the MLDv2 protocol settings.

The MLDv2 performance analysis in this chapter shows that a uniform MLDv2 protocol timer and RV setting are suitable for different access network or application bandwidths. The multicast leave MLDv2 signaling traffic $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ and overhead factor η is not practical for any multicast network deployment. For the successful deployment of SSM in MIPv6 networks, the MLDv2 signaling traffic efficiency has to be improved.

A multitude of applications from broadcast-like Internet radio to P2P gaming sessions to location based services will rely on SSM for a scalable and efficient data delivery mechanism. The latency tolerance for a voice or music broadcast application will be different from a text-based weather report. Working within the latency limits is critical from the user's acceptance and quality perception perspective. The mobile multicast latency caused by host movements and subsequent network handoffs measured in this chapter are too high for practical applications and have to be reduced.

Chapter 4

Improving MLDv2 Efficiency Using The Adaptive Listener Tracing Method

4.1 Introduction

The multicasting protocols which exist today as described in Section 2.2, were initially designed for the use of fixed hosts. Ideally, using the same set of protocols, multicasting should also be supported for mobile hosts.

Multicasting is particularly suited for mobile hosts using wireless access networks, where a limited amount of bandwidth is generally shared among the mobile hosts. However, mobile multicasting is challenging due to various factors. Unlike most wired networks, wireless access schemes typically differ with the following characteristics,

- asymmetrical bandwidth; the available link bandwidth to and from the mobile host might not be the same,
- lower bandwidth; the available bandwidth is often small and in some instances shared among the mobile hosts present,
- lower link quality; various environmental and host movement factors cause higher packet loss and
- the presence of snooping switches[1]; often used to extend and maximise the

---

[1] Layer-2 switches which also consider upper-layer information in IP packet forwarding decisions.

access network bandwidth.

The wireless access network characteristics make it difficult for multicast data delivery and group management to work efficiently (in a similar fashion for that of fixed hosts). A comprehensive qualitative comparison of multicast issues for fixed and wireless networks have been identified by Varshney [Var02].

Wireless networks present unique challenges for the MLDv2 protocol to function in an optimal manner. On one hand, the MLDv2 signalling messages should be ideally kept to a minimum due to the access network bandwidth constraints. On the other hand, in a lossy wireless network, the MLDv2 protocol should retransmit messages to remain robust. The MLDv2 message retransmissions are controlled by the value of the Robustness Variable (RV). The MLDv2 signalling traffic data rate R_{MLD} increases with the RV value as analysed in Section 3.5.1 and illustrated in Figure 3.9. A uniform MLDv2 protocol RV setting for all access network schemes might not be suitable. Achieving an optimum MLDv2 protocol performance is a compromise between minimising MLDv2 signalling traffic and maximising robustness.

The removal of the MLDv1 specified [DFH99] host-suppression functionality enables MRs running MLDv2 to track the per-host multicast listener status. The per-host tracking capability is essential for supporting AAA systems [ACG00]. However, without host-suppression, the MLDv2 signalling efficiency is low as shown by the results in Chapter 3. The results from Section 3.4.3 show that the multicast leave MLDv2 signaling traffic $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ severely limits the MIPv6 SSM service scalability (as discussed in detail in Section 3.6). The MIPv6 SSM scalability limits with respect to the number of multicast hosts and application data rates which can be supported in a given access network bandwidth are further analysed in Section 4.5.

The research in this chapter aims to,

- deduce an efficient method to improve the MLDv2 signalling traffic efficiency,
- measure the improved MLDv2 signalling traffic efficiency using the new method and
- compare the improved results to that of the current MLDv2 signalling traffic presented in Chapter 3.

The rest of this chapter is organised in the following manner. The current proposed methods to improve the MLDv2 protocol performance and link bandwidth utilisa-

---

Snooping switches are discussed in detail in Section 4.2.3.

tion is presented and evaluated. The negative effects of MLDv1 host-suppression in the presence of snooping switches are illustrated. The link bandwidth capacity and utilisation equations derived in Section A.4 of Appendix A are used to demonstrate the current MLDv2 protocol signalling scalability problems. The Adaptive Listener Tracing (ALT) method is proposed to improve the MLDv2 signalling traffic efficiency. The simulation experiment results for MLDv2 signalling traffic using the ALT method are presented. The results obtained are compared to the MLDv2 signalling traffic results in Chapter 3 to determine the improvements achieved.

4.2 Current Proposed Methods

4.2.1 Multicast Source Notification of Interest Protocol

Several mechanisms have been proposed to improve the existing MLDv2 protocol performance. The Multicast Source Notification of Interest Protocol (MSNIP) [HHK04] is a proposed MLDv2 protocol extension that operates between the multicast data source and its first-hop[2] router. The MSNIP protocol provides information on the presence of multicast hosts to the source. When there are no hosts currently listening, the first-hop router sends a MLDv2 message to stop the source transmitting data for the multicast channels. When there are interested multicast hosts for the channels downstream, the first-hop router sends a MLDv2 message for the source to start forwarding data.

The use of MSNIP is advantageous when a data source is serving a large number of multicast channels simultaneously but only a small subset of the channels have active listeners. The potential bandwidth savings using MSNIP is at the link connecting the data source and first-hop router. In bandwidth limited wireless access networks, MSNIP is particularly efficient when the multicast source is a mobile node. The use of MSNIP, however, does not increase the MLDv2 signalling efficiency in a multicast hosts access network. There are no known MSNIP implementations nor experimental results yet. The IETF MAGMA WG has reached a consensus to adopt in its charter[3], the MSNIP proposal as an extension to the MLDv2 protocol.

---

[2] The first-hop router is the network router designated to serve the multicast source in forwarding data to hosts in different subnets.

[3] http://www.ietf.org/html.charters/magma-charter.html.

4.2.2 MLDv2 Proxy

The MLDv2 proxy [FHHS04] is designed to extend the multicast capability without running multicast routing protocols in the entire network. In certain network topologies, it might neither be possible nor necessary to run multicast routing protocols on all routers or network devices. In such networks, an edge device can learn multicast group membership information and forward it to routers further upstream in the network. The MLDv2 based forwarding on edge devices can greatly simplify the design and implementation of those devices. Without the need to support the more complicated multicast routing protocols like PIM-SSM, the cost and complexity of the MLDv2 proxy device can be reduced and easily deployed in any network.

As illustrated in Figure 4.1, the MLDv2 proxy has a single upstream interface I_1 and multiple downstream interfaces, I_2 and I_3. The MLDv2 proxy acts like a MR by learning and keeping a record of all the multicast groups of interest on its downstream interfaces I_2 and I_3. On the upstream interface I_1, the MLDv2 proxy acts like a multicast host and forwards MLDv2 report messages towards the designated MR. The proxy device also forwards MLDv2 query messages from the interface I_1 to its downstream interfaces I_2 and I_3. The MLDv2 report messages from host H_1, H_2 and H_3 are combined and sent to the designated MR as a CSR message $(G, \texttt{include}(S_1, S_2))$ by the proxy. The CSR messages used to refresh the multicast router records ensure that channels $(G, \texttt{include}(S_1))$ and $(G, \texttt{include}(S_2))$ are forwarded towards the proxy device and multicast hosts H_1, H_2 and H_3.

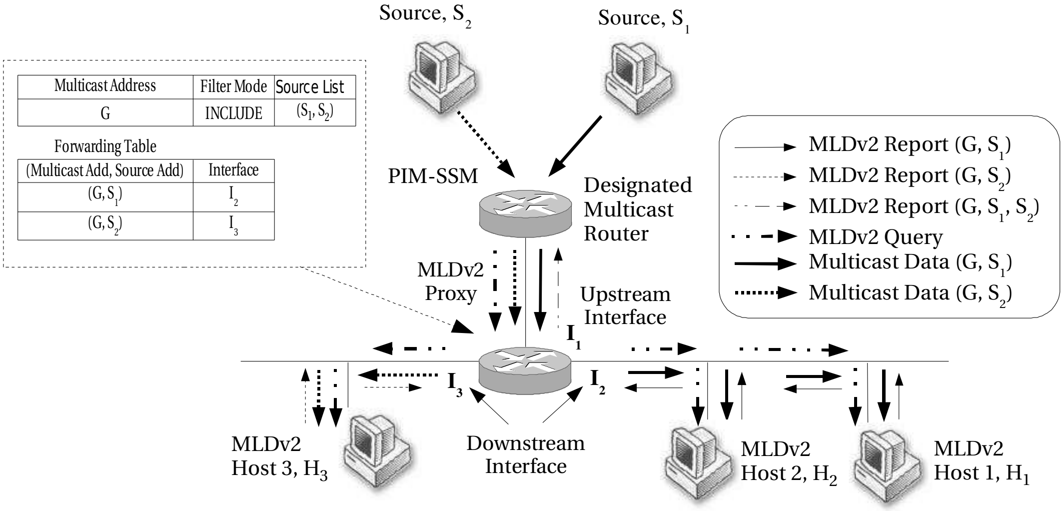
The MLDv2 proxy concept has been adopted in the IETF MAGMA WG charter and pursued as a potential standard [FHHS04]. Hence, MLDv2 proxies will potentially be an important and integral technology for successful MIPv6 SSM deployments. However, the MLDv2 proxy concept and workings are still at the initial research stage. There are no known implementations nor experimental results for MLDv2 proxy efficiency to date.

4.2.3 Snooping Switch

All multicast data and MLDv2 packets are encapsulated by Layer-2 headers and use the multicast or broadcast Layer-2 destination addresses, hexadecimal `3333` for the first 2 octets[4] [Cra98]. When a Layer-2 switch receives packets starting with the Layer-2 address `3333`, it traditionally forwards a copy to all of the remaining interfaces except the one it receives the packet from. This forwarding method ensures

---

[4] An IPv6 packet with a multicast address G_j, consists of 16 octets (or 128 bits). The last 4 octets of the multicast address make up the 48 bit Ethernet address.



Multicast Address	Filter Mode	Source List
G	INCLUDE	(S_1, S_2)

Forwarding Table

(Multicast Add, Source Add)	Interface
(G, S_1)	I_2
(G, S_2)	I_3

Figure 4.1: A MLDv2 proxy device.

that multicast packets reach all hosts connected to all of the switch's interfaces. Unlike broadcast packets though, forwarding the multicast packets to all of the switch's interfaces is not a strict requirement. All the switch interfaces (or segments) might not have multicast hosts connected and thus, the forwarding of multicast packets to all switch interfaces might be a waste of bandwidth.

The snooping switch advantage is achieved by using a forwarding algorithm based on the upper (network) layer information of the multicast packets. In a snooping switch (unlike a conventional switch), the Layer-3 (network or IP) information influences the Layer-2 forwarding rules. Hence, a MLDv2 snooping switch [CKS05] does not strictly adhere to the ISO specified 7 layer model[5].

The snooping behaviour is also present in some routers which use upper (transport) layer information to act as a firewall[6]. The workings of a snooping switch is illustrated in Figure 4.2. A snooping switch creates an internal table of the devices attached directly to its ports and the respective multicast listening states. The snooping switch algorithm often uses a variety of methods to discover the interfaces with routers attached. The MRs in the network are discovered through either the Neighbour Discovery protocol [NNS98], Router Solicitation protocol [TN98, Section 5.5] or snooping the messages sent to the switch interfaces. The MLDv2 report messages (G, S_1) and (G, S_2) are only sent to the MR port, P_1.

---

[5] The ISO specified OSI model specifies separate functionality for the data link and network layers. Snooping switches breach that distinction.

[6] An Internet firewall is an IP-packet filtering device used primarily as security measure. Packets are allowed to pass through the firewall by matching a set of predetermined rules.

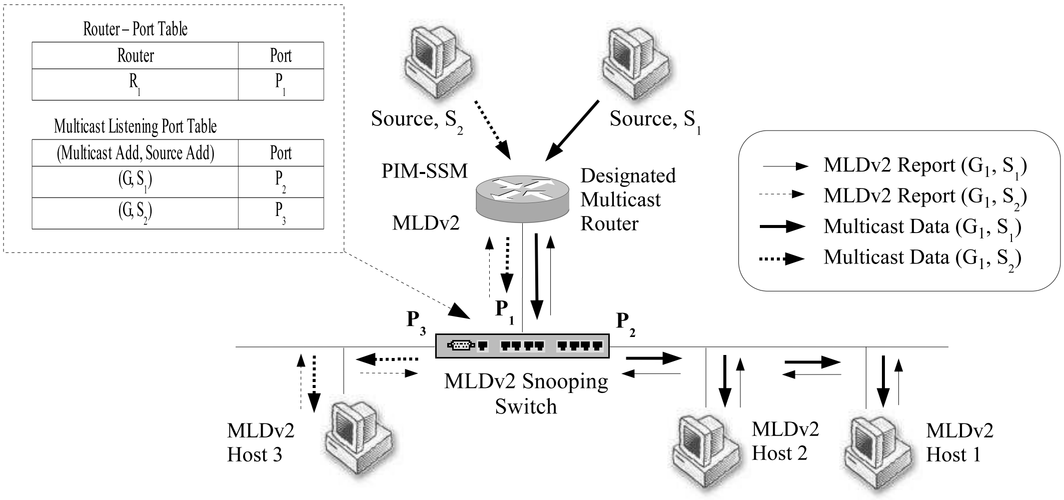


Figure 4.2: A Layer-2 snooping switch with the MLDv2 state mapping.

The snooping mechanism can distinguish between multicast data and MLDv2 packets. A snooping switch only forwards MLDv2 report packets to interfaces with MRs attached. The multicast hosts H_1 and H_2 listen to the channel (G_1, S_1) on port P_2 and host H_3 to channel (G_1, S_2) on port P_3. The snooping switch keeps this information in a table with port and multicast channel mapping. Hence, multicast packets from data source S_1 and S_2 are not forwarded to port P_2 and P_3 respectively.

With the MLDv1 host-suppression feature, hosts on the same subnet (for e.g. hosts H_1 and H_2) do not respond when MLDv1 report messages with similar listening states to that of the host are detected. Snooping switches assume that the suppressed hosts do not exist and might prevent MLDv1 query and report messages reaching all multicast hosts on the subnet. Hence, to increase robustness, the MLDv2 specification does not support the host-suppression functionality. Snooping switches have only recently been proposed as a mechanism to improve multicasting efficiency. From the literature review, snooping switches are still at the research stage and no theoretical nor experimental results are available to date.

4.2.4 Receiver-initiated Group Management Protocol

The Receiver-initiated Group Management Protocol (RGMP) proposed by Liao et al. [LY99] combines the advantages of IGMPv2 and IGMPv3 without any apparent group management signalling performance degradation. The RGMP message exchange mechanism is described in Section 2.4.1 and illustrated in Figure 2.7b. The work by Liao is based on IPv4 IGMPv3 with source filtered SSM hosts and does not consider IPv6 MLDv2 specifically. Hence, the results cannot be directly compared to the ones obtained in Chapter 3. The network topology used for the experiments are similar to that of Figure 3.1 in Chapter 3. Experimental results show an increase of over 60% in RGMP signaling traffic efficiency in comparison to IGMPv3 with the number of hosts, $N_{\mathrm{MN}} = 30$ [LY04, Section 3]. The experiments are repeated for a number of multicast hosts ($1 \leqslant N_{\mathrm{MN}} \leqslant 50$) and a number of mulitcast groups ($0 \leqslant N_{\mathrm{G}} \leqslant 30$). Using RGMP, the signalling traffic efficiency improves from approximately 10% ($1 \leqslant N_{\mathrm{MN}} \leqslant 10$) to 85% ($40 \leqslant N_{\mathrm{MN}} \leqslant 50$) over IGMPv3.

Although RGMP exhibits better signalling efficiency than IGMPv3, it is not suitable for the use of mobile multicast hosts. Unlike MLDv2, RGMP does not use any MR query messages. The RGMP relies on the multicast hosts being completely responsible to group management updates as illustrated in Figure 2.7b. Without any movement prediction mechanisms, the mobile host cannot be relied upon for providing the RGMP update messages. The RGMP protocol has not been pursued in the IETF standardisation track to date. The RGMP has not been considered for MIPv6 host multicast group management [JPA04]. Also, the lack of multicast states held in the MR using RGMP makes AAA systems difficult to implement.

4.3 Design Criteria for Improvements

The design of IGMP and MLD protocols are described in Section 2.2.1. The specific features, functionalities and advantages of the MLDv2 protocol are provided in Section 3.2. The proposed approach to reduce the MLDv2 protocol's signalling traffic $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ should broadly adhere to the following criteria:

1. As minimal changes as possible to the existing MLDv2 protocol design;
    - the MLD protocol has gone through many iterative design stages and uses well established IPv6 Internet Control Message Protocol (ICMP) message structures to construct CSR, SCR and Query messages [VC04, Section 5],
    - the MLD protocol is also used for other additional IPv6 functions (for e.g. to obtain a solicited multicast host address[7]) and
    - major changes to the protocol will further delay the IETF standardisation process for MIPv6 SSM protocols.

---

[7] The solicited multicast host address is an important an integral component of Duplicate Address Detection (DAD) mechanisms [Moo05].

2. No additional security concerns;
    - the proposed method should not cause any additional security concerns or threats (and at the very least maintain the current level of MLDv2 security[8]).
3. No inter-protocol issues;
    - The current suite of IPv6 protocols interact and rely on each other for various network functionalities. The proposed mechanism should not cause any protocol inter-operating complexity.

4.4 The ALT Mechanism

The MLDv2 protocol's signalling traffic performance calculated in Section 3.4 inhibits MIPv6 SSM network scalability. The multicast leave MLDv2 signalling traffic $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$, calculated in Section 3.4.3, is large in comparison to the multicast data traffic, R_{APP}. In the MLDv2 protocol query/reply mechanism, the MR is required to send out a MASSQ (S_i, G_j) message every time it receives a leave SCR (S_i, G_j) message as illustrated in Figure 2.7a. All remaining hosts for the multicast channel (S_i, G_j) need to reply with CSR messages resulting in the MLDv2 signalling traffic.

The MLDv2 signalling traffic $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ (Equation 3.3) is caused by two basic assumptions by the MR:

- that every leave SCR message is treated as been received from the last multicast listener host on the network and
- the LLQI duration T_{LLQI} should be set low enough to increase the MLDv2 granularity[9] (and ensure a timely updating of the routing protocol).

Using the MLDv2 protocol, the MR creates a multicast record for each join SCR message with the format below,

1. **Multicast Address Record**. The multicast listening state which is a set of records with the format: $\mathrm{MAR}_{\mathrm{n}}[G_j, T_{M_{\mathrm{sf}}}, M_{\mathrm{sf}}, N_{S_i}]$, where,
    - G_j is the IPv6 multicast address to which the MLDv2 SCR message request pertains to,

---

[8] A comprehensive study of the MLDv2 protocol security and threat analysis is conducted and presented in Chapter 6.

[9] MLDv2 granularity is a qualitative indicator of the MLDv2 discriminating ability in group management and described in Section 1.4.

  - $T_{M_{\mathrm{sf}}}$ is the source filter timer (but only used when the source is in the exclude mode, $M = \texttt{exclude}^{10}$),
  - M_{sf} is the source filter mode which may either be in the $M = \texttt{include}$ or $M = \texttt{exclude}$ mode and
  - N_{S_i} is the source list which contains the number of multicast data sources (with IPv6 addresses S_i) in SSM mode[11].

2. **Source List Record**. Each record $\mathrm{MAR_n}$ describes a specific multicast listening state, which consists of two independent source lists for M = `include` and M = `exclude` modes. Each source list is also built as a record entry with a linked list in the format: $N_{S_i}[S_i, T_{S_i}]$ where,
  - S_i is the IPv6 source address for the multicast group G_j and
  - T_{S_i} is the source timer before the entry is removed from the listening multicast record $\mathrm{MAR_n}$.

In the current format, the information captured in the record $\mathrm{MAR_n}$ is not enough to deduce if the MLDv2 leave SCR (S_i, G_j) message received by the MR is from the last multicast listener in the network. If additional information regarding the number of hosts N_{MN} is made available to the MR, it can make a more informed decision when to send out an appropriate MASSQ (S_i, G_j) message.

The ALT mechanism assists the MR in knowing whether the leave SCR message received *is* from the last listener in the network (while being able to maintain a low T_{LLQI}). The ALT method enables the MR to make a more informed decision based on a set of rules. The ALT mechanism gives the MR an added 'tracing' capability when maintaining a host entry in the MAR. The original MLDv2 source record $\mathrm{MAR}_n[G_j, T_{M_{\mathrm{sf}}}, M_{\mathrm{sf}}, N_{S_i}]$ with the Source List Record N_{S_i} is extended to be in the following format,

1. **Modified Source List Record** (MSLR). The record is of similar functionality as above but has an additional field: ${N'}_{S_i}[S_i, T_{S_i}, N_{ll}]$, where,
  - S_i is the IPv6 source address for the multicast group G_j,
  - T_{S_i} is the source timer before the entry is removed from the listening records $\mathrm{MAR_n}$ and

---

[10] When the filter timer $T_{M_{\mathrm{sf}}}$ expires, the source filter switches back to include mode, $M_{\mathrm{sf}} = \texttt{include}$.

[11] The IP address is a list of zeros when in the ASM mode.

- N_{ll} is the last listener list which records the number[12] of recent listener reports to an MR for the record $\mathrm{MAR_n}[G_j, T_{M_{\mathrm{sf}}}, M_{\mathrm{sf}}, N_{S_i}]$.

The MR starts to populate the additional last listener list N_{ll} with a simple counting mechanism $(N_{ll} + 1)$ every time it receives a MLDv2 SCR message with the record $\mathrm{MAR_n}$. The ALT mechanism works in conjunction with the MLDv2 protocol as an added adaptive tracing capability. It is not necessary to memorize every listener of a specific source. In practical implementation, it could be an array with a fixed record length. If there are no more SCR messages from a specific host, the last listener entry can be replaced or ignored. The ALT method adjusts according to the number of entries required in last listener list N_{ll} for the anticipated number of multicast hosts N_{MN}.

In ALT implementations, the last listener list field can be a simple array with a fixed record length, k. If the number of hosts N_{MN} is greater than the array size k, the entries can be rewritten with the new join SCR information or ignored. When source records N_{S_i} are processed from the MLDv2 CSR message, the last listener list N_{ll} and the entries can be easily maintained simultaneously. The last listener list size N_{ll} is theoretically only curtailed by implementation specific limitations. The only way to ensure that the MLDv2 signalling traffic $R_{\mathrm{MLD_{LLQI}}} \rightarrow 0$ is to trace all listeners N_{MN} on the link. Also, the current listening states of all the listeners will have to be tracked frequently. The last listener N_{ll} array size is a trade-off between the router's processing load versus the MLDv2 signalling efficiency gained. The compromise of limiting the last listener list to an upper limit, k, for a proportion of hosts is, that both router processing is not burdened and an acceptable level of MLDv2 signalling traffic efficiency is achieved.

The perceived listener density and available link bandwidth will lead to the optimum number of listener records to be maintained. For e.g., we are not able to calculate precisely the optimal theoretical k value. The simulation experiments in the following sections with various number of hosts N_{MN}, proportional hosts jMN and groups N_g help us deduce the k value empirically.

The ALT mechanism is designed in the following manner. As the ALT flowchart in Figure 4.3 shows, when the MR receives a MLDv2 SCR (S_i, G_j) message, the message type has to be determined first. When a join SCR (S_i, G_j) message is received if an existing record, $\mathrm{MAR_n}[G_j, T_{M_{\mathrm{sf}}}, M_{\mathrm{sf}}, N_{S_i}]$ does not exist, then one is created. A corresponding MSLR $N_{S_i}[S_i, T_{S_i}, N_{ll}]$ is created and the last listener list is set, $N_{ll} = 1$. If the join SCR message is for an existing record MAR_n, the

---

[12] The number of records held in the last listener list N_{ll} is adaptive and will always satisfy the condition $(0 \leqslant N_{ll} \leqslant N_{\mathrm{MN}})$ where N_{MN} is the total number of multicast hosts.

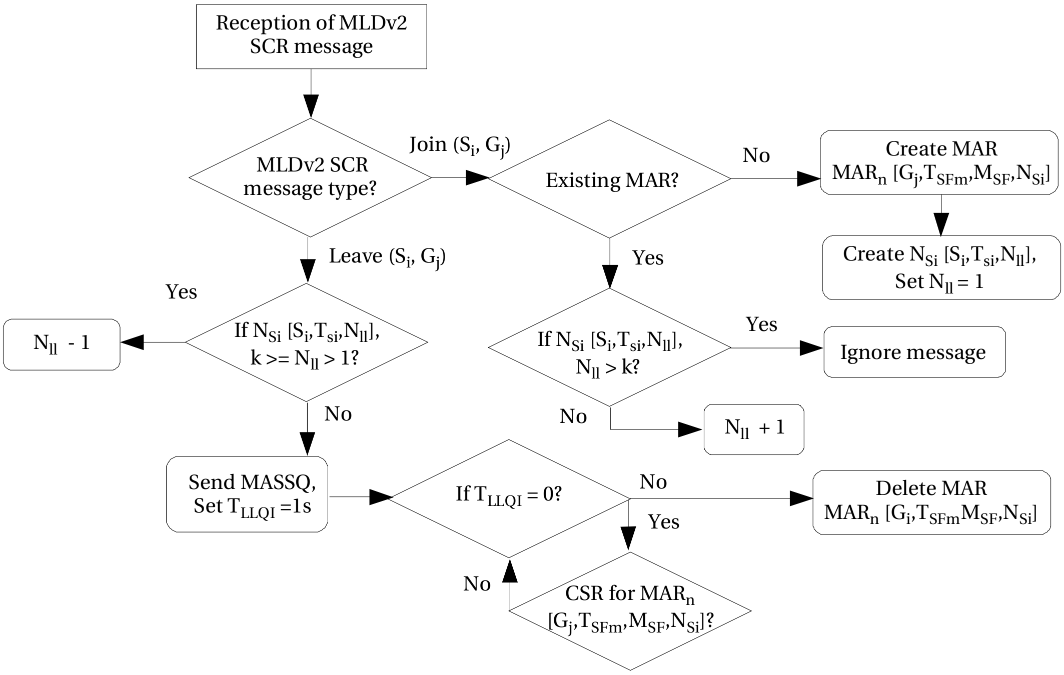


Figure 4.3: The ALT algorithm flowchart.

listener count N_{ll} has to be compared against a preset tracing limit, k. For conditions where, $(1 \leqslant N_{ll} < k)$, the last listener counter is increased to $(N_{ll} + 1)$. For cases where $(N_{ll} \geqslant k)$, no action is required and the SCR message is ignored.

If the MLDv2 SCR message received indicates a multicast leave (S_i, G_j), and $(N_{ll} \geqslant k)$ the message is ignored. For a leave message with $(1 \geqslant N_{ll} \geqslant k)$, then $(N_{ll} - 1)$ for the record MAR_n. Else, the ALT sends out a MASSQ message for the record MAR_n and sets $T_{\text{LLQI}} = 1\text{s}$. During T_{LLQI} if any CSR MAR_n message is received, the last listener list $(N_{ll} + 1)$ and the record is processed by MLDv2 functions (like any other MLDv2 CSR message during the QRI, T_{QRI}). If $T_{\text{LLQI}} = 0$, and no other MLDv2 messages (S_i, G_j) are received, the record MAR_n is deleted from the MR. Although it is not a strict requirement, but we find to our advantage, only the MR needs to run this algorithm. The ALT method requires no changes to the host, making it much easier to implement from a practical perspective. The ALT algorithm can also be incorporated into MLDv2 proxy devices.

4.5 Link Bandwidth Capacity

Ideally, when a multicast host's listening state changes, the MLDv2 update messages have to be sent as quickly as possible. A timely update means higher MLDv2 granularity and minimal access network bandwidth wastage. The time it takes for a MR to learn and stop forwarding multicast data is known as the MLDv2 leave latency T_{LL} as derived in Section 3.4.4. Unlike MLDv1, the MLDv2 protocol takes an active role in minimising the Leave Latency T_{LL} by sending out a MASSQ message as shown in Figure A.1 of Appendix A. If no CSR messages are received within the Last Listener Query Interval, T_{LLQI}, the MR stops forwarding the multicast channel to that interface.

As shown in Equation 3.7, the multicast Leave Latency, T_{LL}, is dependent on the value of the the Robustness Variable, Query Interval, T_{QI}, Query Response Interval, T_{QRI} and Last Listener Query Interval, T_{LLQI}. In lossy access networks, RV needs to have a high setting to ensure MLDv2 protocol robustness. Reducing the timers T_{QI}, T_{QRI} and T_{LLQI} to make the MLDv2 protocol updating faster also causes the MLDv2 signalling traffic R_{MLD} and $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ to increase as shown in Equation 3.1 and 3.3 respectively. As derived in Equation A.9 of Appendix A, in an access network with link bandwidth R_{ACC}, the maximum number of multicast hosts N_{MN} that can be supported before packets are lost is given by,

$$N_{\mathrm{MN}} \leqslant \left(\frac{(R_{\mathrm{ACC}} - R_{\mathrm{APP}}) \times T_{\mathrm{LLQI}}}{(8 + \sum_{i=1}^{N_G}(20 + 16N_{S_i}))}\right) - RV - 1, \tag{4.1}$$

where RV is Robustness Variable, N_{S_i} is the number of data sources, N_{G} is the number of multicast groups and T_{LLQI} is the Last Listener Query Interval and R_{APP} is the application data rate.

Apart from Equation 4.1, another useful tool for network planning and provisioning is the ability to determined the number of multicast hosts N_{MN} which can be supported in a given access network with link bandwidth R_{ACC}. For such a measurement, the possible maximum application data rate R_{APP} should satisfy the equation,

$$R_{\mathrm{APP}} \leqslant R_{\mathrm{ACC}} - \frac{(RV + 1 + N_{\mathrm{MN}}) \times (8 + \sum_{i=1}^{N_G}(20 + 16N_{S_i}))}{T_{\mathrm{LLQI}}}, \tag{4.2}$$

where the symbols are the same as Equation 4.1.

	MIN (kbps)		MAX (kbps)		AVERAGE (kbps)	
	R_{MLD}	$R_{\mathrm{MLD}_{\mathrm{LLQI}}}$	R_{MLD}	$R_{\mathrm{MLD}_{\mathrm{LLQI}}}$	R_{MLD}	$R_{\mathrm{MLD}_{\mathrm{LLQI}}}$
Without ALT	13.79	238.41	37.89	241.22	23.40	240.13
With ALT	6.21	5.54	29.06	7.58	22.29	7.04
Improvement	54.97%	97.67%	23.30%	96.85%	4.74%	97.07%

Table 4.1: A summary of the MLDv2 and ALT simulation experiment results.

4.6 MLDv2 Signalling Traffic Results

4.6.1 Without ALT

Simulation experiments are conducted to obtain the multicast leave signalling traffic $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ using the ALT method. The simulated network topology is illustrated in Figure B.2, and the MLDv2 protocol settings are given in Table B.1 of Appendix B. To reflect a non-homogeneous listener network, the following experiments uses a random proportional host[13], $j\mathrm{MN} = 0.5$. The MLDv2 messages exchanged between the MR and hosts are illustrated in Figure 4.4a. The messages observed between t = 0s and t = 2s are sent to initialize the multicast host listening states. At t = 5s, a multicast join SCR message is sent by a host towards the MR and no subsequent messages are observed. The MR sends a GQ message after t = 10s and the multicast hosts respond within QRI, (default T_{QRI} = 10s) between t = 20s and t = 30s with CSR messages. The MLDv2 message length[14], L_{MLD}, is not uniform from all the hosts due to the non-homogeneous listening state.

At t = 30s, the MR receives a leave SCR message and sends out a corresponding MASSQ message to determine if the SCR message was from the last listener. The remaining hosts on the network respond within the LLQI, (T_{LLQI} = 1s), between t = 30s and t = 31s. The MLDv2 signalling data rates R_{MLD} and $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ corresponding to the MLDv2 message exchanges are shown Figure 4.4b. The results in Table 4.1 show that the maximum MLDv2 signalling traffic without ALT during the QI, R_{MLD} = 29.06 kbps and during the LLQI $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ = 241.22 kbps.

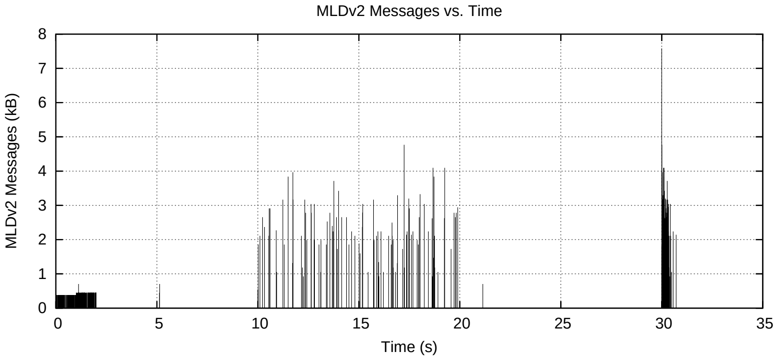
4.6.2 With ALT

Using the ALT method, the MR will not send a MASSQ message following the leave SCR message unless the last listener list is empty $N_{\mathrm{ll}} = 0$. Figure 4.5a shows the MLDv2 messages exchanged using ALT for experiments with similar parameters to

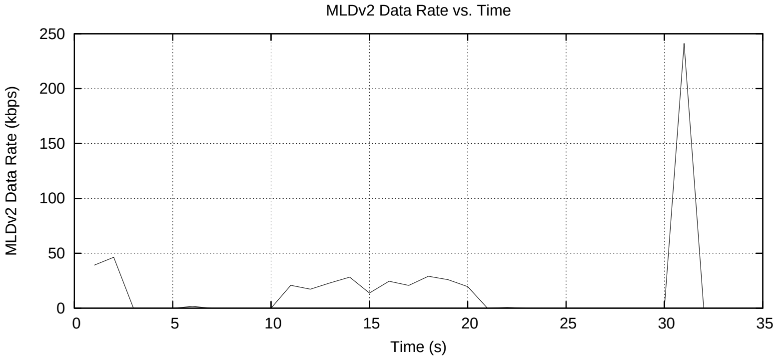
---

[13] The concept of proportional hosts and channels is described in Section 3.4.3.

[14] The MLDv2 message length is derived in Section A.4 and given by Equation A.2 of Appendix A.



(a) Messages



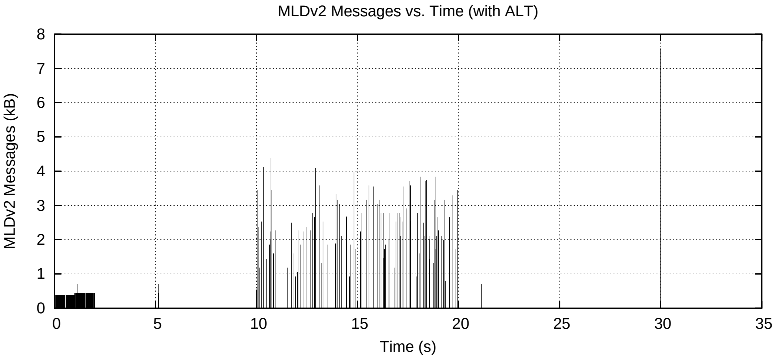
(b) Data rate

Figure 4.4: MLDv2 signalling traffic for random multicast listening states.

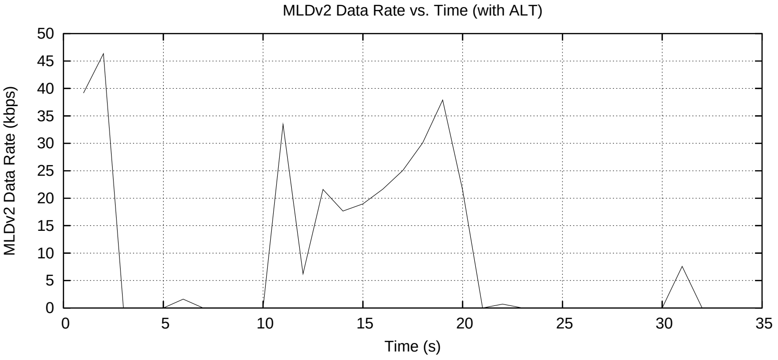
the ones used in Section 4.6.1. The MLDv2 messages exchanged between t = 0 to t = 2s, are to set up the initial listening states of the hosts. At t = 5s, a MLDv2 join SCR is sent by a host and no other messages are observed. At t = 10s, the MR sends a GQ message and hosts respond with the CSR messages within the QRI, (T_{QRI} = 10s) from t = 20s to t = 30s. The MLDv2 message length, L_{CSR}, is not uniform from all the hosts due to the non-homogeneous listening state. The corresponding MLDv2 signalling traffic data rate is plotted in Figure 4.5b. The MLDv2 signalling traffic data rate results in Table 4.1 show a maximum of R_{MLD} = 37.89kbps.

At t = 22s, a leave SCR message is sent for (S_i, G_j) but the MR MAR$_n$ $N_{\mathrm{ll}} \geqslant$ = 0. The MR does not send out a MASSQ and the resultant $R_{\mathrm{MLD_{LLQI}}}$ = 0.70kbps. At t = 30s, a host sends a multicast leave SCR message containing the entire host listening states for the network. The MR sends out a MASSQ message for and sets

$T_{\mathrm{LLQI}} = 1\mathrm{s}$ for the entire record MAR_n. The messages exchanged would reveal the worst case scenario as all multicast hosts N_{MN} have to respond with CSR messages for their respective multicast states. Figure 4.5b shows the corresponding MLDv2 signalling data rate R_{MLD} and $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ for the message exchange of Figure 4.5a. Table 4.1 shows the maximum $R_{\mathrm{MLD}_{\mathrm{LLQI}}} = 7.58\mathrm{kbps}$.



(a) Messages



(b) Data rate

Figure 4.5: The MLDv2 messages and data rate using the ALT method.

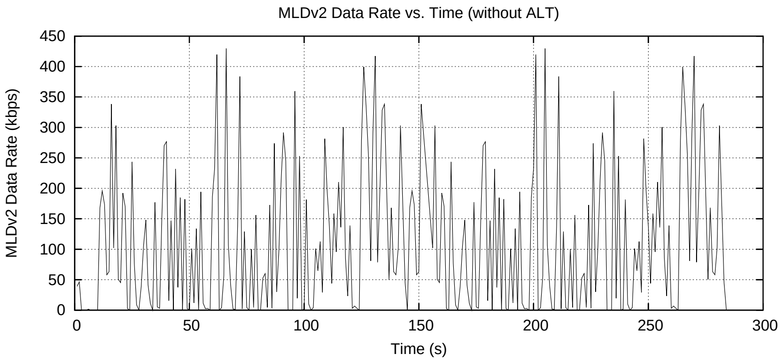
4.6.3 Dynamic Multicast Network

The results in Figure 4.5 show the MLDv2 signalling improvement over the current protocol specification with explicit join and leave messages sent by the multicast hosts at predetermined intervals. In order to obtain more accurate MLDv2 signalling traffic conditions, the simulation experiments are conducted to emulate deployed multicast networks where the join and leave events are expected to be random. For the following experiment, the join and leave messages are randomly generated over a period of time. The multicast listening states of all the multicast hosts present on the network overlap $jN_{\mathrm{MN}} = 5$, but are not completely homogeneous $Ng = 0.5$. The host listening states are generated randomly as the experiments in Section 4.6.1 and 4.6.2.

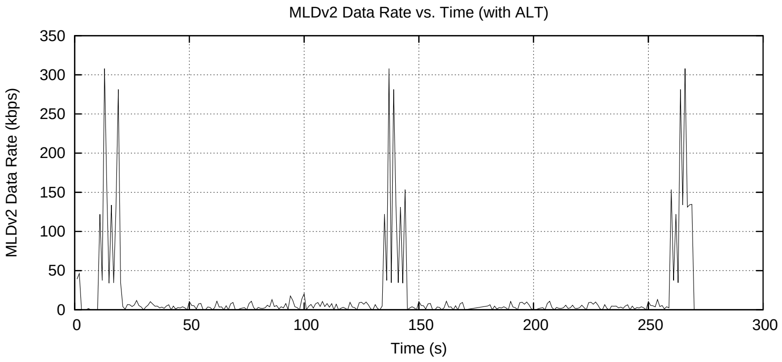
Instead of only sending a SCR message to leave the entire multicast group, N_{G}, every host sends multicast join or leave messages randomly. The host can only however, send a leave SCR message for the channels in their current listening state. To observe a clearer picture of the MLDv2 message exchange, the random is adjusted to occur frequently. Further simulations (again with random generated listening states) over several QIs gives us a better insight into the ALT link traffic improvements. Figure 4.6a shows the resulting MLDv2 data rate R_{MLD} and $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ on the multicast network. Without ALT, in Figure 4.6a, the MLDv2 signalling traffic caused by a multicast leave message maybe higher than the peak R_{MLD} caused by a GQ message.

As plotted in Figure 4.6b, at time t = 10s to t = 20s, the multicast hosts respond to a GQ message within the QRI, T_{QRI} = 10s. The GQ messages repeat every QI, T_{QI} = 125s. By not tracing the entire multicast hosts on the network $k \leqslant N_{\mathrm{MN}}$ information in the last listener list, N_{ll}, it is possible that there remains MLDv2 message exchanges even when the leave SCR message received is not from the last listener. The resultant R_{MLD} is seen between the QRI, t = 20s and t = 135s. The MLDv2 signalling traffic during this period is caused by the random join and leave messages on the network. The MLDv2 signalling traffic R_{MLD} decreases with the increasing number of traces k held in the last listener record N_{ll} held by the MR.

Table 4.2 gives a summary of the MLDv2 signalling traffic results from the dynamic multicast network experiments. In both experiments with and without ALT, the Query Interval, T_{QI} = 125s and the Query Response Interval (default T_{QRI} = 10s) occurs at t = 10s to 20s, t = 135s to 145s and t = 270s to 280s. The resulting average MLDv2 signalling traffic with and without ALT, R_{MLD} = 133.62kbps and R_{MLD} = 193.40kbps respectively. In a dynamic multicast join and leave network, the are possibly periods without any multicast activity and hence, no MLDv2 signalling traffic at all. The MLDv2 signalling traffic observed (apart from T_{QRI}) represents the join and leave occurrences. The average MLDv2 signalling traffic during LLQI with and without the ALT mechanism are, $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ = 4.17kbps and $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ = 104.08kbps respectively.



(a) MLDv2 traffic data rate without ALT



(b) MLDv2 traffic data rate with ALT

Figure 4.6: The MLDv2 traffic data rate comparison with and without the Adaptive Listener Tracing method.

4.7 Conclusion

With the current set of multicast protocols, the number of multicast hosts in a network and the channels they listen to are not known. Hence, the MR cannot determine if MLDv2 messages are from the last listener. There have been prior attempts at estimating multicast hosts and the proposed methods use probing techniques and analytical models [AABN03, FT99, LN00]. The estimation proposals use their own tuning parameters whose optimal values are dictated by the type of network and multicast host listening state. The problem with the estimation techniques however, is that additional signalling messages are required for periodic updates (even when there are no changes to the listening states of the multicast hosts). These proposed

	MIN (kbps)		MAX (kbps)		AVERAGE (kbps)	
	R_{MLD}	$R_{\text{MLD}_{\text{LLQI}}}$	R_{MLD}	$R_{\text{MLD}_{\text{LLQI}}}$	R_{MLD}	$R_{\text{MLD}_{\text{LLQI}}}$
Without ALT	45.18	0.00	417.22	429.73	193.40	104.08
With ALT	33.98	0.00	307.99	20.48	133.62	4.17
Improvement	24.79%	0.00%	26.18%	95.23%	30.91%	95.99%

Table 4.2: A summary of the MLDv2 traffic data rate showing the improvements achieved with the ALT method.

techniques are not suitable for increasing the MLDv2 signalling traffic efficiency, η.

Although the ALT mechanism itself does not need to trace all the hosts, per-host tracking is possible through the existing MLDv2 functionality. The ALT algorithm is applied to SCR messages to determine when MASSQ messages need to be sent by the MR. Using ALT in conjunction with the MLDv2 protocol results in the multicast group management protocol being:

- Robust; retaining the query/reply MLDv2 design makes the protocol robust. The ALT soft state tracing mechanism an adaptive array is suited for best-effort IP networks,
- Efficient; the ALT algorithm reduces the MLDv2 signalling traffic by 95.99% in a dynamic multicast network, making it more efficient. The available access network bandwidth capacity can be better utilised to support more hosts and higher application data rates.
- Scalable; the ALT algorithm does not need to be supported in any multicast host making it easier to support and implement. Hosts only need to support the current MLDv2 protocol.
- Source filtering; the ALT mechanism retains the MLDv2 source filtering capability by tracing multicast listeners.
- Self-synchronised; the MLDv2 query mechanism and messages remain the same but is synchronised according the listener tracing mechanism. A more informed decision can be made to determine the actual last listener on the multicast network.

The ALT mechanism satisfies all the design considerations identified in Section 4.3. The ALT algorithm processing overheads in the MR can be reliably expected to remain below the access network bandwidth wastage without it. The ALT algorithm used in conjunction with the existing MLDv2 protocol design retains all the robustness and advantages of the latter without the associated signalling traffic inefficiencies identified in Chapter 3. The use of ALT decreases the MLDv2 protocol signalling traffic $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ irrespective of the number of multicast hosts N_{MN}, multicast groups N_{G} and number of data sources N_{S_i}.

Chapter 5

Minimising Multicast Handover Latency: Using Layer-2 Triggering

5.1 Introduction

When a mobile Internet host moves, it has to re-attach to different access points in a wireless network to maintain communications. For seamless mobile Internet multicasting, a host requires fast, transparent and smooth handovers between the different access points in the network. Hence, mobility and multicasting Internet Protocols have to inter-operate to ensure continuous data delivery in spite of host movement and subsequent re-attachment in the wireless network. When a mobile host re-attaches to a different point in the wireless network, the host needs to re-join its existing multicast channels. The multicast Handover Latency T_{MH}, is the time it takes to re-join the multicast channels and continue receiving data on the new link and should be kept to a minimum. Ideally, when possible, the host should also leave the same multicast channels on the previous link. The multicast Leave Latency, T_{LL}, which represents the trailing states[1] left behind in the previous link should also be minimised.

The MIPv6 standard supports multicast host mobility by Remote Subscription (RS) or through Bi-directional Tunneling (BT) via the Home Network (HN) as described in Sect ion 2.3.2. The BT method causes inefficient routing and mul-

---

[1] The network bandwidth and processing resources are wasted during period T_{LL} in the previous link.

ticast delays due to the routing triangulation[2] forwarding effects. Therefore, the BT method has scaling limitations and cannot be considered as a solution for large scale MIPv6 SSM deployments. The RS method is more efficient and scalable than BT but thought to suffer from slow handover latencies, as the multicast routing protocol has to adapt to mobile host movements. When a host moves, the multicast routing and data delivery tree should pursue it to the new point of attachment on the network. A mobile multicast service should strive to achieve *optimal* routing at predictable and limited cost, low handover latency and robustness to support a service quality compliant to real-time media distribution.

The IPv6 MLDv2 protocol assumes that all multicast hosts are constantly attached to the same point in the network for the duration of the multicast session. The MLDv2 protocol does not take possible mobile multicast host movement into consideration. The host and the MR which it is connected to, expect the MLDv2 message query/reply transactions to be completed according to the specified sequence [VC04], as shown in Figure 2.7a. Without any multicast handover solution, the host does not initiate MLDv2 procedures when it re-attaches to a new link. Also, without any movement prediction schemes, a mobile host is not aware of impending movement and cannot send the necessary MLDv2 messages before leaving the current network attachment. Hence, the current MLDv2 Join Latency T_{JL}, and Leave Latency T_{LL} (as the results in Section 3.4.4 show), do not meet the requirements for most real-time applications during a multicast handover process.

At the time of MIPv6 research and standards writing, movement detection mechanisms were not understood well enough to be included in the specification [JPA04, Section 11.5]. Optimized movement detection techniques that allow faster host IPv6 layer reconfiguration upon network re-attachment were lacking. The IETF however, has recognised that host movement detection is a critical component in ensuring a seamless host handover procedure. The current research progress has prompted the IETF to create the Detecting Network Attachment (DNA) WG for standardisation work [Int]. The DNA WG is working on standards that allow a host to detect its movement, IP layer configuration and connectivity status quickly. The research results presented in this chapter aims to contribute towards the IETF DNA WG mobile multicast host movement detection standardisation considerations. It is expected that future versions of the MIPv6 specification or other IETF documents may contain movement detection algorithms that provide a better multicast handover latency performance.

In this chapter, the Layer-2 triggering mechanism is used to reduce the multicast

---

[2] Multicast data packets have to transverse the HN, as shown in Figure 2.6.

Handover Latency, T_{MH}. While the proposed Layer-2 triggering mechanism itself is not dependent on the routing protocol, in order to provide a more comprehensive latency study, the following analysis makes use of the PIM-SSM intra-domain routing protocol. The PIM-SSM multicast routing protocol is anticipated to be the most widely used for MIPv6 SSM services [Bha03].

The rest of this chapter is organised in the following manner. The MIPv6 handover concepts and relevant messages for unicast and multicast connections are described and illustrated. The various types of multicast host movement and the associated delay components are identified. The multicast join and leave latencies from Chapter 3 are extended to include the Layer-2 and routing protocol delay components. The Layer-2 based triggering mechanism design and experimental implementation are given. A Layer-2 triggered ICMPv6 notification mechanism is also proposed to decrease the multicast Leave Latency, T_{LL}. The results from both simulation and testbed network experiments are measured and compared to the original multicast Join Latency, T_{JL} obtained in Chapter 3.

5.2 Mobile IPv6 Handovers

5.2.1 Unicast

In unicast communications, the IPv6 address in use is usually based on a network prefix [TN98]. The IPv6 network prefix is commonly distributed hierarchically[3] and likely to change at different parts of a mobile network. When a mobile host moves and re-attaches to another part of the network, the change of address affects its reachability (as described in Section 1.2). The MIPv6 standard supports transparent host mobility when it moves from one point of attachment on the network to another [JPA04]. The use of MIPv6 allows hosts to be constantly reachable while keeping application sessions alive. The MIPv6 specification describes the generic use of IPv6 Neighbor Discovery (ND) [NNS98] and Neighbor Unreachability Detection (NUD)[4] to signify Layer-3 host movement.

Once movement is established, the host needs to start the primary Care of Address (CoA) selection process again by performing Duplicate Address Detection (DAD) [TN98, Section 5.4] as shown in Figure 5.1. The DAD protocol uses Neighbor Solicitation and Advertisement messages to ensure that the host's link-local address

---

[3] The network prefix address is often assigned to and advertised by the local router.

[4] Using NUD, when a host detects that the default router is no longer reachable, it is a possibility that the host has moved to another part of the network.

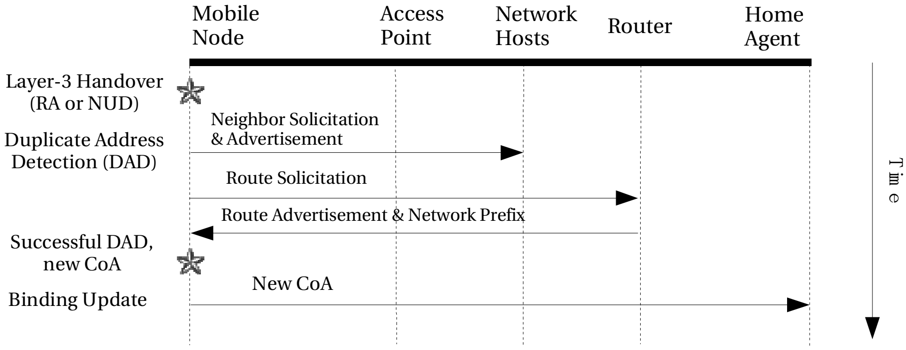


Figure 5.1: The MIPv6 specified unicast handover message sequence.

is unique on the new link. The host also needs to immediately send a Router Solicitation message in an attempt to acquire fresh routing and network prefix information from the new default router. The solicited Router Advertisement (RA) message from the router provides the new network IPv6 address prefix. Once DAD is complete, the host can form a new Care-of-Address (CoA) with the new prefix and its link-local address[5]. The host is required to send a Binding Update (BU) message to register the new IPv6 CoA with its Home Agent (HA).

5.2.2 Multicast

Unlike unicast, multicast group addresses in general are not network location dependent. In SSM, source addresses are interpreted and used by the routing infrastructure and by host applications. When a host moves and re-attaches to a new part of the network, a MLDv2 SCR join message should be sent for its existing channels $(S_\mathrm{i}, G_\mathrm{j})$ towards the new router, nMR, as illustrated in Figure 5.2. The router nMR sends PIM-SSM routing update messages in the upstream direction towards the router sMR serving the multicast source, S_i.

In the worst case scenario, without an existing multicast tree, the PIM-SSM updating has to reach the source router, sMR. The multicast data delivery tree for the channel $(S_\mathrm{i}, G_\mathrm{j})$ is constructed and the data is forwarded towards the host, H_1. Ideally, where possible the host, H_1 should also send a MLDv2 leave SCR message to its previous multicast router pMR to notify the router of its movement. The router pMR has to send out a corresponding MASSQ message for $(S_\mathrm{i}, G_\mathrm{j})$. If the previous router, pMR, determines that host H_1 is the last listener, it sends its own PIM-SSM update message to prune the multicast tree.

---

[5] This is an example of obtaining CoA through stateless address auto-configuration. It is also possible to use a stateful mechanism like DHCPv6 [DBV+03].

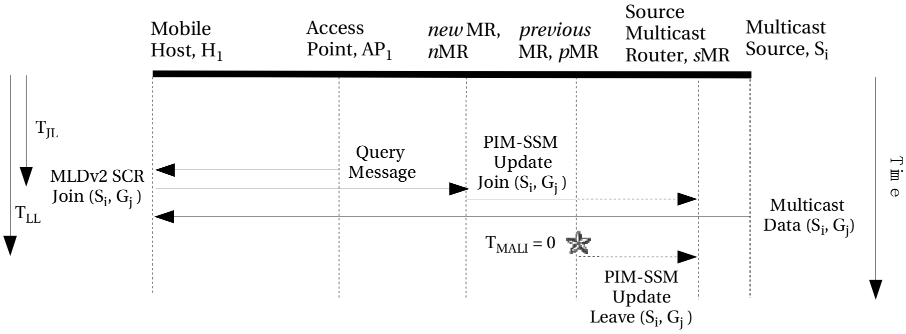


Figure 5.2: The MIPv6 RS multicast handover messages and sequence.

5.2.3 Multicast Support Agent

There are prior proposals using handover prediction mechanisms such as the Multicast Support Agent (MSA) to minimise the handover delays [Jia00]. One of the principal motivations for the MSA was a hosts limitation in not knowing of the arrival at a new link and the need to rejoin multicast groups again. The resulting delay was having to wait for a MLDv2 query message from the new MR. If a host understands that the link has changed, an unsolicited group-join report can be sent immediately, effectively eliminating the query and response back off times.

Jiang [Jia00] proposes an accelerated group join MSA which resides on the new access network and uses handover prediction mechanisms. The MSA initiates the sending of multicast traffic onto the new link by the time the mobile host joins. Predicting the hosts next link is challenging in most networks and would not be suitable, for example with Fast Handover mechanisms [Koo05]. Additionally, handover prediction mechanisms are not available in most access network schemes and the MSA will not work.

5.2.4 Router Advertisement Flag

A MIPv6 host determines IP subnet movement based on the RA prefix information and decides whether to initiate an inter-subnet handover. Our initial mobile multicast proposal [KD§04] was for routers to include an ‘option’ or ‘flag’ in the IPv6 RAs to provide hosts with multicast routing information from the network. The RA message flag information indicates the presence of a new MR and the need to initiate MLDv2 updating. Similar to the RA message reception which initiates a CoA process as shown in Figure 5.1, it could also be used to trigger MLDv2 updates. However, the default RA interval in MIPv6, $T_{\mathrm{RA}} = 1$s, incurring a multicast Handover Latency, T_{MH} of up to three seconds, which is less than T_{JL} calculated in

Section 3.4.4 but still not suitable for real-time applications.

5.2.5 Multicast Context Transfer

The experimental Context Transfer Protocol (CTP) [LNPK05] is designed to minimise disruption mobile host applications during movement. The key CTP design objectives are to reduce handover latency, packet loss and to avoid the re-initiation of signaling to and from the mobile host upon movement. The CTP introduces a mechanism for the secure transfer of context data between routers. The CTP scheme uses the listeners current context in the previous router to quickly re-establish multicast trees in the next router. The primary CTP motivation is to quickly re-establish context transfer candidate services without requiring the mobile host to explicitly perform all protocol flows for those services from the start.

Context transfer mechanisms for fast IPv6 mobile multicast have been proposed to the IETF by Miloucheva [MV05]. Optimal multicast context transfer block and operational considerations are based on Fast Handovers for MIPv6 [Koo05] and Candidate Access Router Discovery. The requirements for MLDv2 context extension and transfer operation at access routers to support multicast are according to the MIPv6 specification. The possible interactions of MLDv2 and PIM-SSM for multicast routing state updates based on context transfers are also discussed. However, the proposed CTP schemes are still at the conceptual stage and have no published handover latency results to date.

5.3 Multicast Host Movement

5.3.1 Movement Types

Multicast mobile host movement and subsequent AP handoffs[6] cause different effects on the IP layer and hence, multicast data delivery. Mobile multicast host movements can be classified into three different types:

- *Between APs only*; host movement from one AP to another, connected to the same multicast router interface,
- *Intra-router*; host movement from one AP to another connected to different interfaces of the same router and

---

[6] In the current literature, the terms handover and handoff are generally interchangeable. For the purpose of this thesis, handover is used to describe Layer-3 and handoff for Layer-2 movement respectively.

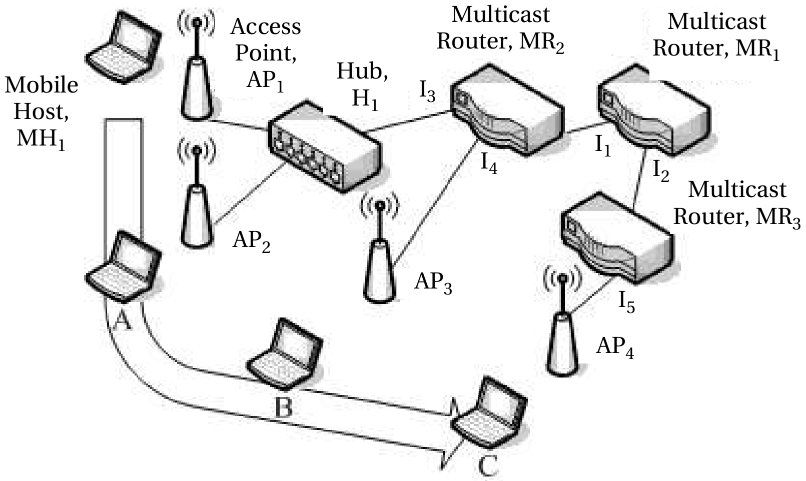


Figure 5.3: Mobile multicast host movements.

- *Inter-router*; host movement from one AP to another connected to different routers.

As illustrated in Figure 5.3, in the case of AP movement only, host H_1 moves from AP_1 and re-attaches to AP_2 at Point A. Both AP_1 and AP_2 are connected to the same interface I_3 of the multicast router, MR_2. There is no MLDv2 group management updates required as the host H_1 listening states $(S_{\mathrm{i}}, G_{\mathrm{j}})$ already exist and the multicast data forwarded on the interface, I_3. Intra-router movement occurs when host H_1 moves from AP_1 and re-attaches to AP_3 at Point B. The access point AP_3 is connected to a different interface, I_4 of the same router MR_2, to that of AP_1. The host H_1 will need to update the multicast group management and send a MLDv2 CSR message to continue receiving multicast data $(S_{\mathrm{i}}, G_{\mathrm{j}})$ from interface I_4. The router MR_2 is an existing member of the multicast data delivery tree but needs to update its MLDv2 MAR to include the interface, I_4 for the channel $(S_{\mathrm{i}}, G_{\mathrm{j}})$.

For inter-router host movement, the host moves from AP_1 and re-attaches to AP_4 at Point C. The access point AP_4 is attached to a different router MR_3 through the interface I_5. The interface I_5 of the router MR_3 might not be currently forwarding multicast data for the channel $(S_{\mathrm{i}}, G_{\mathrm{j}})$. The new router MR_3 might or might not be part of the existing multicast data delivery tree. Hence, apart from updating the MLDv2 MAR, the router MR_3 might have to send PIM-SSM update messages to upstream routers in order for the host H_1 to continue receiving multicast data $(S_{\mathrm{i}}, G_{\mathrm{j}})$.

5.3.2 Handover Latency

When a mobile host detects or suspects that its underlying Layer-2 connectivity has changed, it needs to check whether its IP (Layer-3) addressing and routing configurations are still valid. Changes to a Layer-2 connection do not also, necessarily mean changes in the Layer-3 connectivity as described in Section 5.3.1. In the case that the Layer-3 connectivity has changed, the host requires to initiate the unicast and multicast mobility procedures as illustrated in Figures 5.1 and 5.2 respectively.

In the case of AP movement only, the MLDv2 group management is not affected by the host H_1 re-attachment to AP_2 at Point A. The host H_1 does not need to send any MLDv2 messages and will continue receiving multicast data once the Layer-2 re-attachment to AP_2 is complete. For AP movements, the multicast Handover Latency T_{MH} is caused by the Layer-2 AP re-attachment process delays only.

For intra-router host movement the multicast routing tree exists on MR_2 but the MLDv2 MAR needs to be updated to include the interface, I_4. The existing multicast routing tree and data delivery path is not affected by the host movement. The multicast Handover Latency T_{MH} for intra-router host movement is caused by the Layer-2 AP re-attachment, MLDv2 message exchange and processing delays. For inter-router movement, the host H_1 will re-attach to a completely new router MR_3 at Point C. It is possible that the router MR_3 is not part of the existing multicast data delivery tree. The multicast Handover Latency, T_{MH} PIM-SSM routing message exchange and processing delays between routers in addition to the Layer-2 AP and MLDv2 delays identified above. A multitude of factors attribute to and influence the PIM-SSM propagation delay including the source router distance, multicast tree and router's processor loading.

Hence, the general multicast Handover Latency T_{MH} encompassing all movement types is defined as,

$$T_{\mathrm{MH}} = T_{\mathrm{MLD}} + T_{\mathrm{L2}} + T_{\mathrm{PIM}}, \tag{5.1}$$

where T_{MLD} is the MLDv2 message exchange delay, T_{L2} is the Layer-2 movement detection and re-attachment delay and T_{PIM} is the PIM routing tree reconfiguration delay. The MLDv2 message exchange delay, T_{MLD} is defined in Equation 3.6 and the multicast Handover Latency T_{MH} can be re-written as,

$$T_{\mathrm{MH}} = T_{\mathrm{QI}} + t_r + T_{\mathrm{L2}} + T_{\mathrm{PIM}} - \tau, \tag{5.2}$$

where τ is the host handover[7] time which has lapsed since the last GQ message on the new link, T_{QI} is the Query Interval of the newly joined link, t_r is the random CSR message reply time within T_{QRI}. The focus of this research is primarily on the Layer-2, MLDv2 and MIPv6 protocol interactions and latencies. The hardware specific processing delays, link quality and external ambient factors are excluded in the following experiments and analysis.

5.3.3 Leave Latency

In Figure 5.3, when the host H_1 re-attaches to AP_4 at Point C, it leaves behind a trailing multicast record in the previous router MR_2. The time taken by the MLDv2 protocol to remove the trailing record on interface I_3 of MR_2 is called the multicast Leave Latency, T_{LL}. The Leave Latency[8], T_{LL} is given by,

$$\begin{aligned} T_{\mathrm{LL}} &= (T_{\mathrm{MALI}} + T_{\mathrm{LLQI}}) - \tau, \\ &= ((\mathrm{RV} \times T_{\mathrm{QI}}) + T_{\mathrm{QRI}}) + T_{\mathrm{LLQI}} - \tau, \end{aligned} \tag{5.3}$$

where, RV is the Robustness Variable, T_{QI} is the Query Interval, T_{MALI} is Multicast Address Listener Interval, T_{LLQI} is Last Listener Query Interval, T_{QRI} is the Query Response Interval and $\mathrm{t} = \tau$ is the host handover time. A summary of the results from the simulation experiments in Section 3.4.4 are given in Table 3.5. With default MLDv2 timer settings, the maximum Leave Latency, $T_{\mathrm{LL}} = 261\mathrm{s}$.

Employing movement prediction technologies [FR04, PA02, WCB04], it is possible to send a SCR message before the host leaves the existing part of the network. However, host prediction mechanisms are difficult to implement, costly and not common in most access network technologies. Apart from predicting the Layer-2 handoff time in advanced and being able to send an Unsolicited Report (default value is 1 second), the other problem is preventing all other existing hosts responding to the subsequent MASSQ messages sent by the router pMR. The resultant MLDv2 signaling data rate, $R_{\mathrm{MLD_{LLQI}}}$ when all the other hosts respond with CSR messages, reduces the MLDv2 signaling efficiency[9].

---

[7] The timing intervals and the handover point during the host movement is shown in Figure 3.7.

[8] The multicast Leave Latency is described in Section 3.4.4 and illustrated in Figure 3.7.

[9] The MLDv2 signaling traffic $R_{\mathrm{MLD_{LLQI}}}$ analysis is presented in Section 3.4.3.

5.4 Layer-2 Triggering Mechanism

5.4.1 Design Criteria

Since a Layer-3 multicast Handover Latency T_{MH}, of several seconds (relying on the MLDv2 mechanism) is unacceptable for most delay-sensitive applications, other complementary mechanisms are required. Inter-layer communications using the additional information available from the newly attached network AP is a possibility. The Layer-2 handoff information available upon AP re-attachment can be used for decreasing Layer-3 multicast handover delays. Since a Layer-3 handover always starts with the re-establishment of a Layer-2 connection, an ongoing Layer-2 handoff is a good indication of a potential Layer-3 handover. By using the Layer-2 re-attachment indication, a host can initiate a Layer-3 multicast handover much earlier than waiting for the MLDv2 or MIPv6 RA updates [KDŞ04], because the Layer-2 handoff latency is relatively shorter.

The Layer-2 information is typically an indication that a new attachment link is up or based on the radio signal strength [IEE] received by the host from the new AP. Link-up[10] triggers correspond to the establishment of a new Layer-2 link, which allows IP (Layer-3) communication over it [IEE]. The Layer-2 link-up event is deterministic and the Layer-2 link change notification can be provided to the IP-layer when it concludes. The Layer-2 link-up event could be used to trigger the sending of MLDv2 messages for quick multicast group management updates.

5.4.2 Access Network Handoffs

Most wireless devices are designed with a hardware control functionality which allows for firmware to probe for the AP identity. To facilitate the handover process, beacons or RAs are implemented in a variety of wireless networks. For example, in an IEEE 802.11 wireless access network, the APs periodically broadcast beacon frames as an indication of whether hosts should initiate a handoff [IEE]. As part of the link establishment, Basic Service Set Identification (BSSID) and Service Set Identifier (SSID) associated with the AP is learned by the mobile host.

The BSSID identifier is unique and set to the hardware address of the wireless interface of the AP. The SSID information carries the identifier of the Extended Service Set[11]. To discover movement, the host could periodically probe the AP Layer-2 BSSID address from the beacon frames and compare it to the held record.

---

[10] A Layer-2 event signifying the interface being capable of communicating data packets again.

[11] A set of APs and associated hosts that share a common distribution system.

The host will scan each Layer-2 wireless channel, send a Probe Request packet and wait for the Probe Response packet from the AP. After a number of Authorization messages, the host will re-associate with the new AP and start using it for network connectivity. A mismatch of IDs could point to a AP handoff, and the need to initiate Layer-3 updating. In an IEEE 802.11 wireless network, the beacon frame interval is 100ms, incurring a Layer-2 handoff latency of 100 to 450ms [Por03].

5.4.3 Multicast Handover

The Layer-2 triggered multicast handover mechanism is shown in Figure 5.4. Once Layer-2 movement is detected, the host forges a GQ message and sends it to the Layer-3 loop back interface destination IPv6 address, `::1/128`. The host assumes that it is a genuine GQ message from the router and responds with a MLDv2 CSR message using the destination IPv6 address `ff00::16` towards the new router, nMR.

The QRI (controlled by the value in the MRD field) of the generated false GQ message has to be set at a small value[12] for an immediate host CSR message response[13]. The host sends a MLDv2 CSR message with Filter Mode Change and Source List Change records to indicate a (possible) new listening record on the link. When the router nMR receives the MLDv2 CSR report message, it will initiate the appropriate PIM-SSM router message exchange to start forwarding multicast data. The obvious advantage of the Layer-2 triggered mechanism is using the existing MLDv2 messages with minimum alterations and extending it to reduce the multicast handover latency.

5.4.4 Multicast Leave

An explicit multicast leave notification to the router pMR can be achieved by including a 'previous router' option in the host's MLDv2 report messages to the new router. The host is aware of the specific router interface identity of the attached link from the Router Advertisement by setting the R flag. The previous router knowledge allows new routers to perform a context transfer which removes only those groups associated with the link-local identity of the host making the request. Since the link-local identity is likely to remain the same as the host changes links, this identity can be used to remove state on the previous access network. It enables much faster soft-state removal for old multicast groups, freeing up resources on the

---

[12] The response interval approaches zero ($T_{\mathrm{QRI}} \longrightarrow 0$).

[13] The MLDv2 message exchange and timers are described in Section 2.4.1 and illustrated in Figure 2.7a.

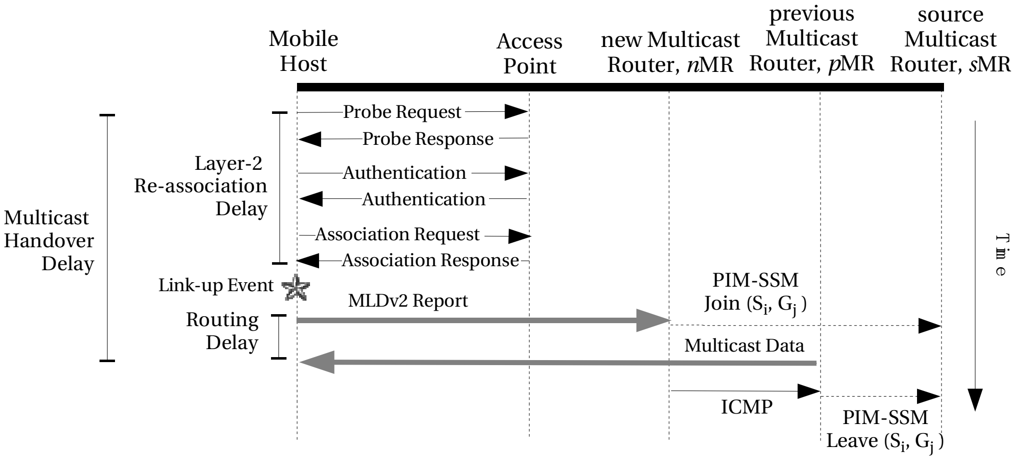


Figure 5.4: The Layer-2 re-association process and subsequent multicast messages.

previous router.

The simplest option would be, for the Layer-2 triggered host to send a normal unicast packet with the leave MLDv2 SCR information to the previous router pMR. However, since the MLDv2 protocol is a link-local only protocol[14], the packets will be dropped and this mechanism will fail. Hence, the direct sending of a MLDV2 leave SCR message will fail with the current MLDv2 specification. It is not an optimal solution as relying on off-link MLDv2 messages creates security threats as described in Section 6.2.

The sending of an ICMPv6 message from the router nMR towards the router pMR is more appropriate. An ICMPv6 message can be sent towards the router pMR after the Layer-2 triggering as shown in Figure 5.4. The leave ICMPv6 message will carry the host's MLDv2 CSR records. When the previous router receives such an ICMPv6 message, it has to query the appropriate multicast channels for other listeners on the link.

The current MLDv2 messages shown in Figure A.2 of Appendix A are in ICMPv6 formats with only the value of the type field[15] as a differentiating factor. The ICMPv6 messages are grouped into error messages and informational message classes. The ICMPv6 error messages are identified by having a zero in the high-order bit of the type field. Hence, the error ICMPv6 messages are from types 0 to 127 and the informational messages from types 128 to 255. A possible solution is to designate a new ICMPv6 type [CD98] for mobile multicast usage and send it to the previous

---

[14] Checks are conducted to ensure packets are from the current link with a destination address of `ff00::16` and hop limit =1 as described in Section A.1 of Appendix A.

[15] MLDv2 query message type = decimal 130, MLDv2 report message type = decimal 143.

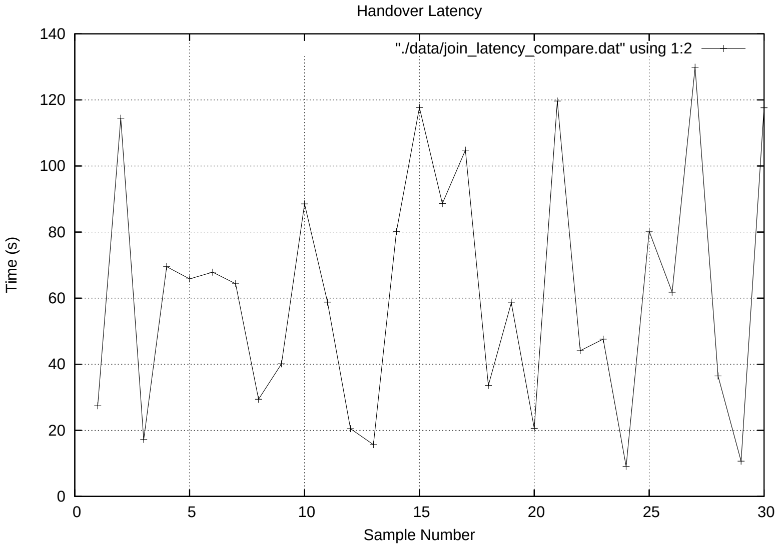


Figure 5.5: The Multicast Handover Latency, T_{MH}, without Layer-2 triggering.

router. Routers will treat these ICMPv6 types as reports from previously attached listeners. With the Layer-2 triggered ICMPv6 method, the MLDv2 protocol works in its current form and not dependent on any handover prediction mechanisms.

5.5 Handover Latency Results

5.5.1 Without Layer-2 Triggering

Without any Layer-2 triggering or movement prediction mechanisms, the host has to rely on the next MLDv2 GQ message from router nMR to re-join its existing multicast channels. The multicast Handover Latency T_{MH} are shown in Figure 5.5. With a default setting of $T_{\mathrm{QI}} = 125$s, the average Handover Latency $T_{\mathrm{MH}} = 71.77$s for random host movements.

The multicast Handover Latency T_{MH} is inversely proportional to the QI setting, T_{QI}. The multicast Handover Latency, T_{MH} results for various QI and T_{QI} are plotted in Figure 5.6. The results is Table 5.1 show that for a $T_{\mathrm{QI}} = 30$s setting, the minimum Handover Latency $T_{\mathrm{MH}} = 5.18$s. The negative effect of reducing T_{QI} is that the average number of MLDv2 messages exchanged increases over time, thus causing poor network utilisation[16].

---

[16] The MLDv2 signaling efficiency study and results are presented in Section 3.4.2.

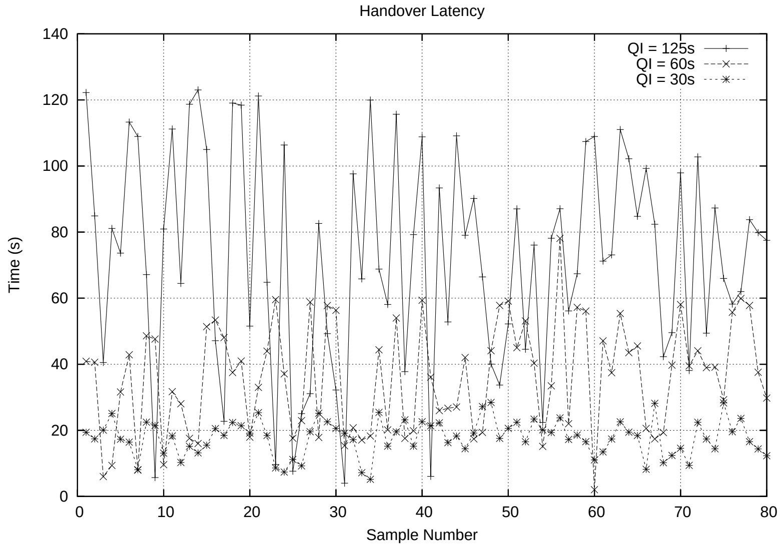


Figure 5.6: Multicast Handover Latency, T_{MH}, with varying Query Interval T_{QI}.

	T_{QI} (s)	MIN (s)	MAX (s)	AVERAGE (s)
T_{JL}	125	4.01	123.04	71.77
	60	5.18	59.89	35.17
	30	5.18	28.44	17.84
T_{LL}		137.38	280.01	194.99

Table 5.1: The multicast Handover Latency, T_{MH}, and Leave Latency, T_{LL}, without Layer-2 triggering.

5.5.2 With Layer-2 Triggering

The simulation experiments (similar to that of Section 5.5.1) are repeated using the proposed Layer-2 triggering mechanism. Once the host establishes a Layer-2 re-attachment, a link-up event triggers the sending of a MLDv2 CSR message. The Layer-2 triggered multicast Handover Latency, T_{MH}, obtained from the experiments are shown in Figure 5.7. The results in Table 5.2 show that with Layer-2 triggering, the average multicast Handover Latency, $T_{\mathrm{MH}} = 444$ ms. The multicast Handover Latency results with and without the Layer-2 triggering mechanism are compared in Table 5.2. The simulation experiments however, cannot distinguish the latency contributions by the individual delay components, as given in Equation 5.2. Without taking into account the MLDv2 message exchange delays, prior studies indicate that the Layer-2 hand-off delays T_{L2} vary between 300 to 500 ms, depending on the channel probing methods employed [GGZZ04]. Hence, it is probable from the results in Figure 5.2, that the MLDv2 delay component, T_{MLD} is only minimal and

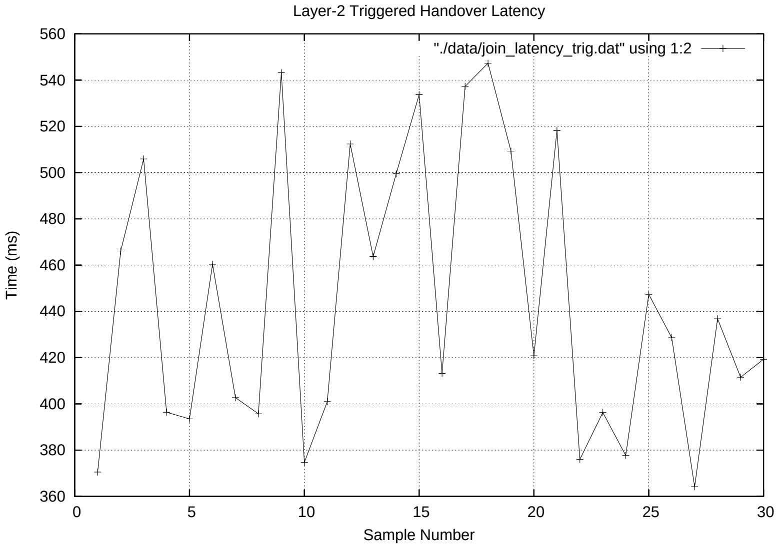


Figure 5.7: The Layer-2 triggered multicast Handover Latency, T_{MH}.

T_{MH}	MIN (s)	MAX (s)	AVERAGE (s)
WITHOUT LAYER-2 TRIGGERING	4.01	123.04	71.77
WITH LAYER-2 TRIGGERING	0.36	0.55	0.44

Table 5.2: A summary of the multicast Handover Latency, T_{MH}, results.

limited by the available router processing power.

5.5.3 With Layer-2 Re-attachment

With a Layer-2 triggering mechanism, the MLDv2 message exchange latency, T_{MLD} is reduced to the same order of magnitude (i.e. milliseconds) as the Layer-2 re-attachment delay components. It is an improvement of several magnitudes in comparison to both the Join Latency T_{JL} of Section 3.4.4 and the RA flag trigger proposed in Section 5.2.4. The Layer-2 re-attachment process and delays are dependent on ambient operating conditions. In order to better understand the latency issues using the Layer-2 triggering mechanism, the simulation experiments in Section 5.5.2 are repeated on a testbed MIPv6 SSM network (as illustrated in Figure C.1 of Appendix C). The hardware, software and respective configurations for the experiments are also detailed in Appendix C.

The Layer-2 re-attachment delay contributions to the multicast Handover Latency T_{MH} are differentiated and determined by our experiments on the testbed network. The Layer-2 movement detection and re-attachment latency T_{L2} of Equa-

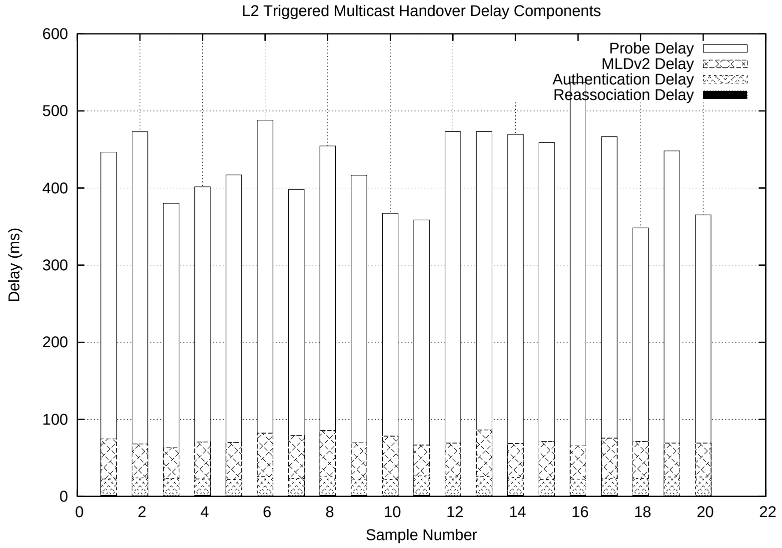


Figure 5.8: The multicast Handover Latency, T_{MH}, results showing the delay components.

tion 5.2 is made up of three delay components,

$$T_{\mathrm{L2}} = T_{\mathrm{Probe}} + T_{\mathrm{Auth}} + T_{\mathrm{Assoc}}, \tag{5.4}$$

where T_{Probe}, T_{Auth} and T_{Assoc} are the probe, authentication and association delays.

The various delay components contributing to the overall multicast Handover Latency, T_{MH} are measured from the testbed network experiments. The multicast Handover Latency T_{MH} is primarily dictated by the Layer-2 hand-off delay component, T_{L2}, as shown in Figure 5.8. The results in Table 5.3 show that on average, the Layer-2 delay, $T_{\mathrm{L2}} = 87.70$ % of the overall multicast Handover Latency, T_{MH}. Also, within the Layer-2 delay, T_{L2}, the probe latency, T_{Probe}, on average contributes to 83.19 % of the overall multicast Handover Latency, T_{MH}. The testbed experiment results concur with previous published results, which shows that the Layer-2 re-attachment delay is primarily influenced by the channel probing techniques employed [GGZZ04].

5.5.4 With Routing Delays

The experiments conducted in Sections 5.5.2 and 5.5.3 measure the Layer-2 re-attachment and the MLDv2 message exchange delays. For a more complete multicast handover latency analysis, the PIM-SSM routing delays T_{PIM}, have to be determined (as shown in Equation 5.2). Once the Layer-2 re-attachment and the

	T_{PROBE} (ms)	T_{AUTH} (ms)	T_{Assoc} (ms)	T_{MLD} (ms)	T_{MH} (ms)
MIN	277.00	20.00	1.00	40.00	348.30
MAX	471.00	25.00	1.50	60.00	536.50
AVE	359.40	22.50	1.30	48.80	432.02
AVE %	83.19 %	5.21 %	0.30 %	11.30 %	100.00 %
AVE %	87.70 %			11.30 %	100.00 %

Table 5.3: A summary of the multicast Handover Latency T_{MH} delay components and values.

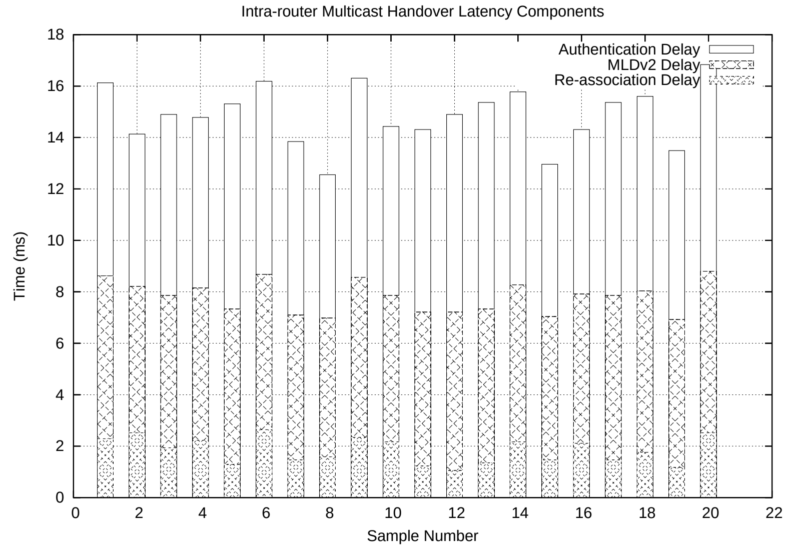


Figure 5.9: The multicast Handover Latency T_{MH} for an intra-router host movement with an existing multicast tree.

MLDv2 message exchange are complete, the PIM-SSM (routing messages) have to be sent from the router nMR as shown in Figure 5.4.

For intra-router host movement to Point B in Figure 5.3, the multicast routing tree already exists on router MR_2 and further PIM-SSM updates are not required. The MLDv2 message exchange on the new interface, I_4 of MR_2 ensures that the multicast channels are forwarded. From the results in Section 5.5.3, the probe delay, T_{Probe} is a few hundred milliseconds. The multicast Handover Latency is plotted in Figure 5.9 without the probe delay, T_{Probe}, to clearly show the MLDv2 message exchange and Layer-2 delays in a intra-router mobile multicast handover. The results in Table 5.4 show that the average multicast Handover Latency, $T_{\text{MH}} = 14.83\text{ms}$.

For inter-router host movement of Type C in Figure 5.3, the multicast delivery tree might already exist on the new router, MR_3. The experimental multicast Handover Latency, T_{MH} for an inter-router host movement with an existing multicast

	MIN (ms)	MAX (ms)	AVE (ms)
T_{MLD}	5.57	8.03	7.08
T_{AUTH}	5.40	6.39	5.95
T_{Assoc}	1.06	2.64	1.78
T_{MH}	12.55	16.83	14.83

Table 5.4: A summary of the multicast Handover Latency T_{MH} results with the multicast tree on nMR.

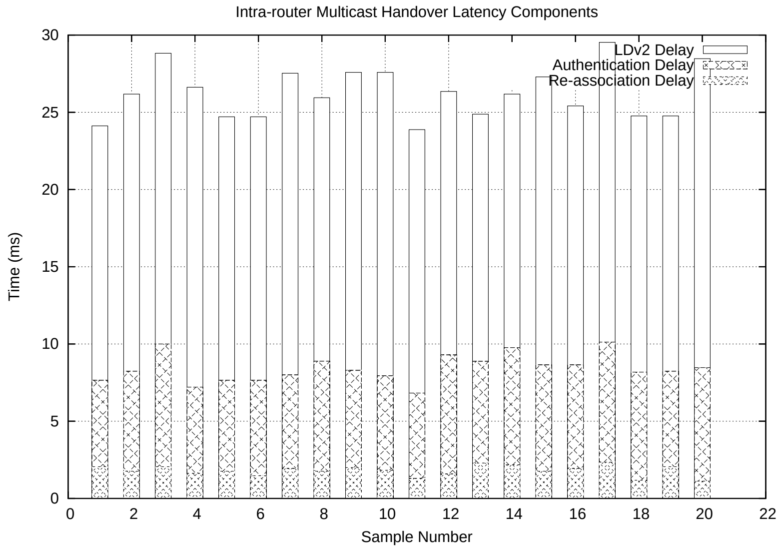


Figure 5.10: The multicast Handover Latency T_{MH} for an intra-router host movement without an existing multicast tree.

tree on the new MR is plotted in Figure 5.10. The average multicast Handover Latency, $T_{\text{MH}} = 26.42$ms as shown in Table 5.5.

For inter-router host movement without an existing multicast tree at the router nMR, the PIM-SSM routing protocol is responsible for constructing the multicast delivery tree. The experiment results to determine the multicast Handover Latency T_{MH} incorporating the PIM message exchange latency, T_{PIM} is shown in Figure 5.11. In the testbed network experiments, the multicast source router sMR is a leaf router and only 1 hop away from the router, nMR as shown in Figure C.1. The PIM-SSM propagation latency, T_{PIM} will increase proportionally with the relative upstream distance of the source router, sMR from the host along the multicast tree. The multicast Handover Latency, T_{MH}, delay components are measured for both with an without and existing multicast tree on the router nMR and given in Table 5.4.

	MIN (ms)	MAX (ms)	AVE (ms)
T_{MLD}	16.00	20.00	17.92
T_{AUTH}	5.53	7.94	6.69
T_{ASSOC}	1.12	2.35	1.78
T_{MH}	23.88	29.26	26.42

Table 5.5: A summary of the multicast Handover Latency T_{MH} results without the multicast tree.

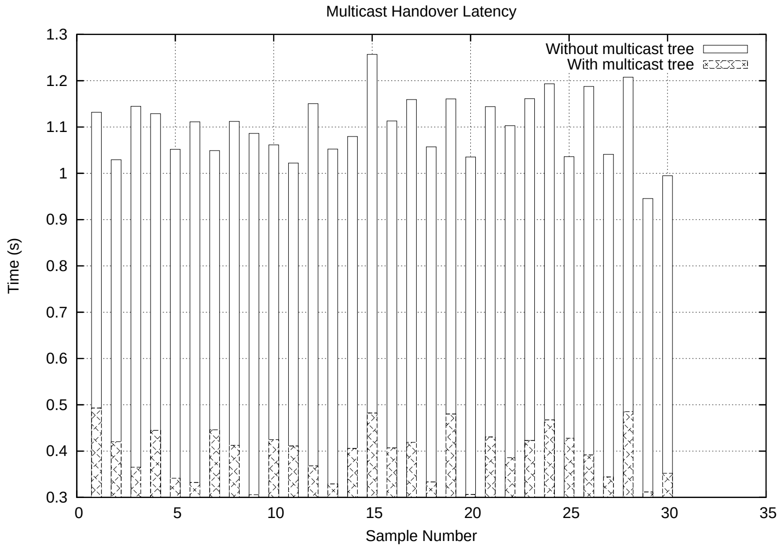


Figure 5.11: The inter-router multicast Handover Latency, T_{MH}, with and without an existing multicast tree on nMR.

5.6 Leave Latency Results

5.6.1 Without ICMPv6 Notification

Without any external notification mechanism, the mobile host relies on MLDv2 messages and the potential multicast Leave Latency T_{LL} is given by Equation 5.3. The experimental results for random host movements and the subsequent multicast Leave Latency T_{LL} is shown in Figure 5.12. The average Leave Latency T_{LL} = 204.13s as shown in Table 5.6.

5.6.2 With ICMPv6 Notification

The Layer-2 triggered ICMPv6 leave message to be sent towards the previous router as described in Section 5.4.4. The trailing MAR is removed after the Last Listener Query Time, T_{LLQI} with a theoretical minimum Leaving Latency, T_{LL} = 2s

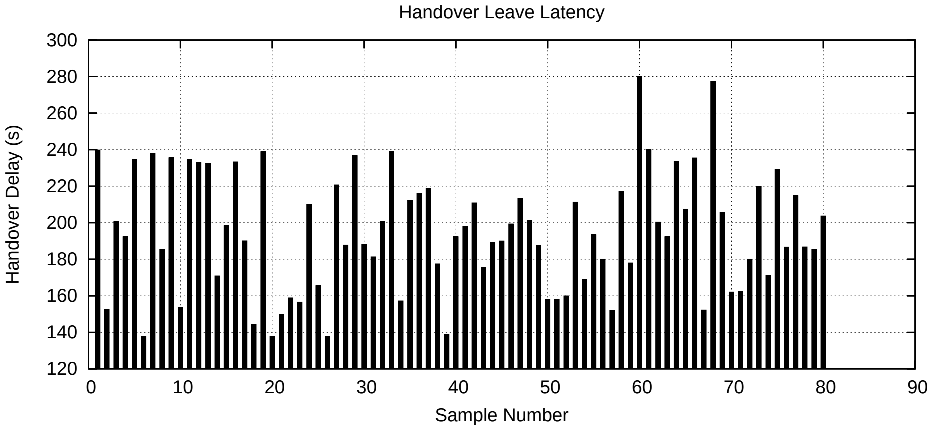


Figure 5.12: The multicast Leave Latency T_{LL} with default MLDv2 timer settings.

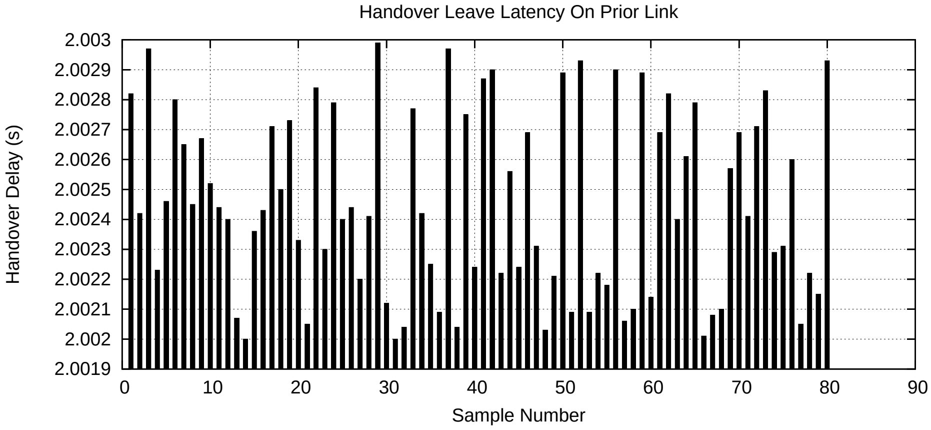


Figure 5.13: The multicast Leave Latency T_{LL} with triggered MLDv2 leave messages.

with default MLDv2 timer settings (ignoring the network propagation and router processing delays). The multicast Leave Latency T_{LL} results with the ICMPv6 notification mechanism is shown in Figure 5.13. The results in Table 5.6 show that the average $T_{\mathrm{LL}} = 2.51$s.

5.7 Conclusion

Real-time communications such as voice or video applications over IP have severe temporal requirements. Seamless handovers are required to limit disruptions or delay to less than 100ms and jitter disturbances should not exceed 50ms. The 100ms delay limitation represents the approximate duration of a spoken syllable in real-time audio. Also, multicasting is usually associated with high bandwidth

T_{LL}	MIN (s)	MAX (s)	AVERAGE (s)
WITHOUT ICMP	144.13	262.23	204.13
WITH ICMP	2.411	2.591	2.509

Table 5.6: The multicast Leave Latency, T_{LL}, with and without the ICMPv6 notification.

applications and trailing states from previous routers need to be removed quickly once the mobile host has successfully re-attached to a new part of the network. The delay-sensitive application requirements above place severe handover latency restrictions to multicast and mobility protocols.

The movement detection time is what it takes for the host to determine that it is on a new link. Our recent work to rationalize access network configuration systems indicates that this issue is common to many IP subsystems, and need not be undertaken for multicast alone [DK03]. The Layer-2 triggered mobile multicast solution proposed and tested in this chapter has the advantage of functioning without any movement prediction mechanisms. The simple Layer-2 triggering mechanism is used to successfully reduce both the multicast Handover Latency, T_{MH} and the Leave Latency, T_{LL}.

The Layer-2 triggering mechanism proposed in this chapter and the results obtained from the experiments indicate that the MLDv2 latency component, T_{MLD} can be reduced to the magnitude of milliseconds. The MLDv2 latency results from both the simulation and testbed network experiments show a vast improvement over results in Section 3.4.4. Accordingly, if the Layer-2 T_{L2} delay can be reduced or circumvented, the only remaining delay is the multicast tree reconfiguration time, T_{PIM}. The effects of mobility on multicast routing algorithm convergence is an area which will require significant future research and is not in the scope of this research.

Chapter 6

MLDv2 Security Considerations

6.1 Introduction

Multicasting is usually associated with the delivery of large bandwidth data streams. Hence, malicious modification of data streams on any subnets is a significant cause for concern on network resources. Additionally, the limited feedback mechanisms available for User Datagram Protocol (UDP) multicast data streams mean that service theft and network Denial-of-Service (DoS) attacks are easier than in bi-directional unicast communications. Securing IP multicast encompasses into three components [HHC01]:

- end-to-end data protection (together with the group key management),
- routing protocol protection (to ensure correct routing behavior) and
- access control (group management) level.

The first two components listed above have been addressed in prior research. The end-to-end multicast data protection together with the group key management protocol using Cryptographically Generated Addresses (CGA) [Aur05] have been proposed by Castellucia [CM03]. The routing protection is specific to each multicast routing protocol and in the case of PIM [EFHT98, Section 2.12], the specification recommends the use of the IPSec protocols [KA98a]. The third security component at the access control level has not been been addressed and is analysed in this chapter.

The ASM model forwards traffic from *any* active data source to all hosts requesting that multicast group data. In Internet broadcast-like applications, the ASM behavior is highly undesirable as unwanted sources can easily disrupt legitimate data delivery by simply sending traffic to the same multicast group address. This disturbance depletes host network bandwidth with unwanted traffic and disrupts the desired multicast data reception. In IPv6 SSM, multicast traffic from each *individual* data source will be forwarded[1] across the network only if it is requested (using MLDv2 join messages) from an interested host. In SSM, the above mentioned type of DoS attack cannot be made by simply sending traffic to an arbitrary multicast group.

The MLDv2 protocol is an important and essential requirement for all IPv6 hosts and networks [Lou04]. The abuse of the existing (and implicit) trust employed in MLDv2 may significantly affect not only the local host network, but possibly multiple hops in the Internet. Although MLDv2 is only specified for and operates within a single IPv6 link, MLDv2 reports may cause routing state changes beyond the current link[2].

MLDv2 protection from off-link attacks is achieved through the prevention of forwarding packets with link-local source addresses [VC04, Section 10]. Identifying the source of an attacker is possible, but does not mitigate potential attacks nor does it prevent the negative impact and consequences of the network abuse. Several MLDv2 characteristics identified lend itself to potential attacks:

- mandatory query response; without any MLDv2 message authentication, all on-link hosts can be forced to respond with report messages,
- Querier Router (QR) election; the election process uses and relies only on query messages,
- MLDv2 bid-down; backward MLD protocol compatibility mechanisms may force changes to the MLDv2 mode,
- influencing off-link routing; a join SCR message for an arbitrary multicast channel causes changes to off-link routing states,
- query message triggers; a leave SCR message causes the QR to send query messages and
- unprivileged Application Programming Interface (API) access; multicast channels can be accessed through the host APIs [TFQ04] and is open to abuse.

---

[1] Using multicast routing protocols.

[2] Likely to occur when MLDv2 reports are multicast groups for non-link-local data sources.

This chapter analyses the various trust models and security threats specific to MLDv2 group management and access control functions. The MLDv2 trust model workings and interactions with Layer-2 and multicast proxy devices are considered. The MLDv2 security and threat issues for each model with the availability and removal of host-suppression capabilities are discussed. The host-suppression feature can pose as a security threat with attackers potentially stopping multicast data delivery within a link. Also in this chapter, a comparison of MLDv2 with other similar signaling protocols and the proposed trust models put forward is conducted. A study of the security methods applied to the comparison protocols and the suitability and applicability to MLDv2 is presented.

6.2 Trust Models in MLDv2

The MLDv2 signaling on a link consists of query/reply exchange of messages generated by routers and hosts respectively [VC04]. A common set of message exchanges on a link with multicast hosts is illustrated in Figure 2.7a. The message exchanges are based on and exhibit an implicit trust in the relationship, which may be the subject of abuse.

The following trust models are of particular interest and explored in detail in the following sections:

- trust between hosts and routers for multicast group management,
- trust between access network devices, especially multicast snooping switches[3] and
- trust in multicast networks with proxy[4] devices.

Routers' Trust of Hosts

The MLDv2 signaling protocol is used by MRs to determine if multicast channels are of interest to any host on a directly attached link. The MR receives MLDv2 SCR report messages when hosts add to, subtract from or modify the listening states of their set of multicast sources (S_i) or groups (G_j). Also, hosts report multicast channel (S_i, G_j) status periodically with CSR messages in response to MR query messages.

---

[3] Snooping switches are introduced in Section 4.2.3 and illustrated in Figure 4.2.

[4] MLDv2 proxy devices are introduced in Section 4.2.2 and illustrated in Figure 4.1.

When a local-link MR receives a single MLDv2 SCR message, routing table changes to off-link routers may occur. The routing changes are likely to happen for SCR messages pertaining groups or sources from non-local subnets. In the case of MLDv2 abuse, attack amplification effects can cause routing changes to cascade through the network and change the multicast routing topology. Additionally, a potential SCR message abuse may affect the quality of service for other hosts since multicast data streams do not undertake end-to-end data rate limiting. New multicast data streams effectively reduce the available bandwidth on all links where the data is forwarded. If the multicast routing infrastructure is not aware of topological network bandwidth constraints, hosts may cause DoS by spuriously (or accidentally) requesting many large data streams.

The reception of MLDv2 SCR and MLDv1 Done Report messages require the QR to send query messages. The reception of a single SCR message may cause the QR to send multiple (up to the value of QR's RV setting[5]) number of query messages. A bogus SCR message is however, not able to end the forwarding of a legitimate channel because the existing group members will reply with their own CSR messages. The indirect result of the bogus CSR message is, increased MLDv2 signaling traffic data rate, $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ and the host's message processing.

Bogus or repeated CSR messages prolong the multicast channel (S_i, G_j) for longer periods than legitimate host requests. Bogus SCR messages may either drain network resources or flood routing state changes when multiple channels are dropped simultaneously upon expiry of the Multicast Address Listening Interval, T_{MALI} as given by $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ in Equation 3.3. As shown in Table 6.1, the value of T_{MALI} may vary between 1s to 113708s.

The MLDv1 backward compatibility mode [VC04, Section 8] means that in MLDv2 environments, a MR is forced to lose source specific information for particular groups upon the reception of MLDv1 reports[6]. The reception of MLDv1 report messages may cause the MR to use ASM routing methods instead of SSM in the short term, a situation known as a *bid-down* action. A MLDv2 bid-down action has critical consequences on two fronts:

- if existing listeners `exclude` specific sources, then a bid-down causes data from these sources to be delivered and
- in a SSM only deployment, a bid-down action will cause disruptions as there might not be a Rendezvous Point (RP) configured.

---

[5] The maximum RV setting is 7 as shown in Table 6.1.

[6] The QR will continue sending MLDv2 query messages though.

In IPv6, there are currently no authentication or authorization mechanisms defined for multicast group management signaling. Most of the attacks defined above may be performed without explicitly impersonating other hosts nor by breaching the current MLDv2 specifications [VC04]. In the current MLDv2 specification, the process to join multicast channels and modifying source filters are defined as part of the user-level APIs and hence, abuse is possible without privileged access to the operating systems [TFQ04].

Hosts' Trust of Routers

The host's response to a query is typically a CSR message containing its listening states[7] as shown in Figure 2.7a. The CSR message is used to update the MR's timer, T_{MALI} for the MAR and ensures the continued forwarding of multicast data. MR controls the host's response delay (or granularity) by specifying the maximum Query Response Interval, T_{QRI} in the query message's Multicast Response Delay code.

Without the host-suppression functionality in MLDv2, a MR specifying a very small QRI[8] in its query messages causes multicast report responses at fine granularity as given by R_{MLD} in Equation 3.1. In some cases, the severe consequences include loss or delay of multicast data or MLDv2 signaling messages. Hosts cannot determine the query message validity since no authentication or authorization of routers is undertaken. Hosts elect a QR (when query messages from more than one router is present) on the link by choosing the router with the lowest source address. The QR election process is not secure since it is trivial for bogus routers to create the lowest router addresses.

Routers' Trust of Routers

Only one MLDv2 QR per link is responsible for eliciting reports from multicast hosts. The QR is elected using an address identifier[9] and modifications can favour a router in the election process. The QR election occurs when a router with an address lower than any seen in a recent message, sends a query message on the link.

While there is no direct influence on the multicast data delivery, if the non-authorized QR continues querying, it can vary the QI, T_{QI} and QRI, T_{QRI} to cause disruptions. The bogus QR may decrease QI and QRI and disrupt multicast data

---

[7] A MLDv2 message format is illustrated in Figure A.2 of Appendix A.

[8] The MRD code field in the query message is used by the host to determine QRI.

[9] The link-local IPv6 addresses are used.

Abbreviation	Description	Default Value (s)	Min/Max (s)
T_{RE}	Router Re-election Interval	50	0 / 225353.2
T_{LL}	Leave Latency	261	2 / 238983.2
T_{MALI}	Multicast Address Listening Interval	260	1 / 113708
RV	Robustness Variable	2	0 / 7

Table 6.1: The MLDv2 protocol timer and values.

delivery with an increased MLDv2 signaling traffic data rate, R_{MLD} on the link. Also, the QR's RV setting is directly proportional to the multicast Leave Latency T_{LL} as given in Equation 3.7. By falsely increasing the value of RV, the QR prolongs the multicast data forwarding for much longer than required. As shown in Table 6.1, the multicast Leave Latency T_{LL} can vary between 2s to 238983.2s. The bandwidth wastage could possibly cause congestion as multicast delivery streams with no more listeners are still forwarded.

If a legitimate QR is downgraded to non-querier status (by the presence of a fake QR), it can remove groups with listeners if CSR messages are absent within its MALI, T_{MALI}. If the unauthorized router sends only a single query message (and no more), the legitimate QR will stop the query process for the duration Other Querier Present Timeout[10], or querier re-election period, T_{RE} period. The QR re-election delay, T_{RE}, is given by,

$$T_{\mathrm{RE}} = (\mathrm{RV} \times T_{\mathrm{QI}}) + (\frac{T_{\mathrm{MRD}}}{2000}) \tag{6.1}$$

where RV is the Robustness Variable, T_{QI} is the Query Interval and T_{MRD} is the Multicast Response Delay. If a bogus QR does not stop the query process in the presence of a legitimate lower address QR, duplicate MLDv2 report messages will flood the link. Hosts will receive both sets of query messages and will respond equally. Therefore, the presence of any legitimate but misbehaving device (using any address) is similarly harmful to the cases when a false router is elected. The maximum value of T_{RE} = 225353.2s as shown in Table 6.1.

---

[10] The period T_{QPT} is based on the QR's RV and QI setting as advertised in the false query message [VC04, Section 9].

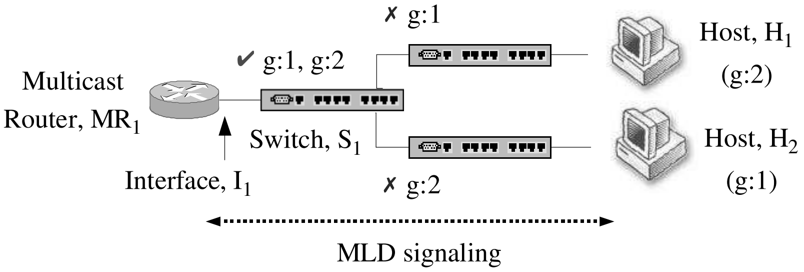


Figure 6.1: Layer-2 snooping switch's forwarding states.

Hosts' Trust of Hosts

Due to the the removal of the host-suppression functionality from the MLDv2 specification, no trust bindings exist between hosts on a link.

6.2.1 Threats Specific to MLDv1

Hosts may avoid transmitting CSR messages in response to query messages if they are configured to use MLDv1. If similar CSR messages (from other hosts on the link) are received within QRI, T_{QRI} a host can suppress its own report messages to reduce MLDv1 signaling traffic. The host-suppression functionality however, has negative consequences to multicast data delivery in networks with snooping switches, as discussed in Section 4.2.3. It is possible to engineer situations where hosts are denied multicast data delivery by being tricked into host-suppression on networks with snooping switches. The MLDv1 host-suppression functionality is discussed further when considering the hosts' trust of switches in Section 6.3.

6.3 Trust Models for Layer-2 Snooping Switches

Multicast snooping [CKS05] and Multicast Router Discovery [HM05] mechanisms can be used to manipulate the local multicast traffic delivery within the last IP hop as illustrated in Figure 6.1. In the example presented in the figure, although hosts H_1 and H_2 are connected to the same interface, I_1 of the multicast router MR_1, they do not receive *all* the MLDv2 messages. The snooping switch S_1, keeps the listening state on all its ports and only forwards relevant MLDv2 messages according to the states held in its record. Although host, H_1 listens to group (g:2), the switch S_1 does not forward the MLDv2 messages with (g:2) information towards the host, H_2. A snooping switch affects not only off-link multicast reception from the router, but also link-local packets such as IPv6 ND messages [NNS98].

Switches' Trust of Routers

A multicast router needs to know of every channel (S_i, G_j) on all its directly attached links. Therefore, snooping switches need to include routers' switch ports as receivers of all channels. The implied trust in switches' monitoring of routers can be abused. The switch's monitoring of router presence ensures that non-local routing occurs for multicast streams originating from sources on the link and allows reception of MLDv2 messages for local hosts.

Snooping switches therefore, need to identify routers and include them in all multicast transmission groups for off-link traffic. Monitoring query messages is an ineffective identification method, since only one router will query at a time. The MRD protocol can be used by all MRs to advertise their presence when solicited by switches [HM05]. The MRD method employed is similar to that of unicast IPv6 Router Discovery and could potentially be achieved using ND options [NNS98]. There are no existing mechanisms to determine if a responding device is a router, and therefore whether all multicast traffic should be sent to that switch port. Also, bogus Multicast Router Terminate messages received on the same switch port as the QR may be used to halt reception of all multicast data.

The Secure Neighbour Discovery (SEND) protocol [Ark05] has been proposed to provide authorization for delegated trust of routing for IPv6 Router Discovery. A similar method to SEND has been proposed for MRD authentication even though the message formats differ from ND [HM05]. Without authentication mechanisms, a host may pretend to be a router by sending bogus Multicast Router Advertisements and swamp a network segment with off-link multicast traffic until a snooping switch timeout occurs.

Switches' Trust of Hosts

Snooping switches are required to modify forwarding states to include the ports and network segments with multicast hosts. The reception of report messages are used to change group listening state within the multicast domain. In some cases though, it may be possible to disrupt multicast services from legitimate hosts by moving listener states from one port to another within a link, using impersonation or repeated report messages. For example, it may not be appropriate for the all-routers' or all-snoopers' group messages to be sent across a wireless link. Access control of certain address classes of groups therefore should be considered.

Switches' Trust of Switches

Routers which receive multicast router solicitation messages should respond so that snooping switches can send all multicast packets towards them. Since not all network segments are connected to snooping switches, MRD solicitation response messages may be transmitted across multiple network segments. Therefore, in order to avoid excessive and unnecessary message transmissions, it is essential to ensure that the soliciting host has some authority to send multicast router solicitation messages. In some networks, the snooping switch also acts as MLDv2 signaling proxy, in which case, the trust models defined in Section 6.4 apply.

Hosts' Trust of Switches

When host-suppression is in use, snooping causes difficulties in maintaining proper multicast state [CKS05]. As described in Section 4.2.3, it was one of the factors which led to the removal of the host-suppression feature from MLDv2. Nevertheless, some multicast snooping devices seek to prevent improper states by never forwarding multicast group management reports to ports where there are no multicast routers attached.

Also, a switch may forge group membership query in order to generate multicast snooping states. In this case, the hosts will receive query messages from devices which are not a part of the Layer-3 routing infrastructure, and may not be authorized to send query messages. Switches operating in this mode share many common attributes with MLDv2 proxy devices, as described in Section 6.4.

6.4 Trust Models for MLDv2 Proxies

There are networks which do not have explicit multicast routing protocols running on all the devices in the multicast forwarding path. These networks trust a proxy device to perform the necessary MLDv2 signaling on the local network as shown in Figure 4.1. The working of a MLDv2 proxy device is described in Section 4.2.2. A proxy undertakes MLDv2 signaling on the device interface closer to the multicast infrastructure [FHHS04]. It requests the aggregate of group and source information that hosts on its other interfaces are listening to. Thus, the proxy acts as a host to the multicast router and vice versa.

Proxies' Trust of Routers

The proxy device is connected to a MR on its upstream interface in a manner similar to the current MLDv2 host-to-router interactions [VC04]. The elected QR acts as the forwarding proxy and therefore, assumed to have multicast forwarding capability [FHHS04]. When interacting with a QR, the proxy device makes no further router authorization assumptions except those identified in Section 6.2.

Routers' Trust of Proxies

The proxy device forwards MLDv2 report messages to the MR on behalf of hosts which are not directly connected to the former. The proxy is not the eventual multicast data destination so host access control mechanisms and decisions cannot be undertaken when summarized MLDv2 information is passed to MRs. In instances where the proxy device is able to provide host credentials, communication transparency and access control mechanisms may be restored. Authorisation mechanisms however, have not been considered in the current proposal [FHHS04]. On the proxies' downstream interfaces, it may attempt undertaking query functions in the presence of a real multicast router.

The current research encourages setting a very low proxy address setting to guarantee the proxy to be elected as the QR [FHHS04]. When a MR which is connected to the Internet exists, it should clearly be elected ahead of the proxy. At present, there is no proposed mechanism to determine proxy or router precedence other than through the administrative choice of addresses.

Hosts' Trust of Proxies

In networks where the router is further upstream along the multicast data delivery tree, hosts have to undertake the MLDv2 message exchange with the proxy instead of a router. The message interactions and authorizations are based on the host-to-router model in Section 6.2, even though the MLDv2 proxy may not be part of the authorized Layer-3 routing infrastructure. The proxy device authorization may be assigned by an upstream router or a dedicated device within the network. The trust model however, is complicated if all the multicast devices do not have some form of pre-existing trust established.

A host should always prefer a MR with authorization over the one without (which might be just a proxy device). The proxy device acts as a QR and hosts assume that their responses to query messages mean that MARs are appropriately setup, current and multicast data forwarded. If a proxy device fails to generate and forward appropriate host reports on upstream interfaces, multicast data forwarding may fail.

Proxies' Trust of Hosts

The MLDv2 proxy devices which are QRs have the same trust of end-hosts which exists for the router-to-host model in Section 6.2. In this case though, the host may in itself be a proxy device and the same considerations of Section 6.4 apply.

Proxy's Trust of Topology

Multicast proxy devices rely upon the idea that there are no forwarding loops[11] in the multicast routing topology. Since there are no routing protocols used between proxy devices to detect loops, it is possible for an attacker to set up forwarding loops which will cause damage to packet transmission on multiple links [FHHS04].

6.5 Summary of Threats to MLDv2

The security threats to the MLDv2 protocol can be categorised according to the roles of the attackers. A summary of possible attacks ascribed to particular roles within the network are given below. The types of attacks are valid across and independent of access network topologies.

Bogus Querier

Any device can act as a bogus QR, irrespective of a legitimate router presence. A bogus query message can preempt a QR re-election process. A bogus QR can also cause increased MLDv2 signaling traffic on the network.

Bogus Group Member

An attacker may be able to join many multicast groups and potentially subscribing many fake members to a particular group. In MLDv2, all group hosts are tracked by multicast routers and snooping switches. The existence of multiple bogus membership may exhaust processing power or state within these devices. The manipulation

---

[11] A routing misconfiguration whereby data packets are never forwarded to the destination host.

of bogus group members (even to bogus groups or sources) may cause off-link signaling changes to other multicast routers. The network bandwidth resources may be consumed and quickly exhausted.

Bogus Snooping Switch

With or without snooping switches, the presence of Multicast Router Solicitation messages may make MRs send Multicast Router Advertisements. The falsely solicited advertisements may be used by bogus switches to exhaust network bandwidth.

SSM to ASM Bid-down

Where an attacker sends an MLDv1 SCR message for a group which is currently in SSM mode, the router will immediately switch to ASM mode. The bid-down process can cause multicast streams to originate from multicast data sources which were previously in the SSM `exclude` mode.

6.6 MLDv2 Message Format Security Analysis

In this section, the relevant message construct, definitions and content for MLDv2 [VC04] and MRD [HM05] protocols are identified for security considerations. The potential and possible type of attack strategies mounted by abusing these IPv6 message constructs and exchanges are analysed. Also, the potential message fields which could be utilised for implementing future security mechanisms are reviewed. A summary of the message formats, potential threats and possible utilisation for security mechanisms is given at the end of this section.

MLDv2 Report Messages

The MLDv2 report message consists of an ICMPv6 header[12] and a sequence of MARs, as shown in Figure A.2 of Appendix A. The number of MARs is stated in the fixed MLDv2 Report header field, although the address records themselves can be of variable length. Each record contains two length indicators; indicating the number of 16 octet source addresses and auxiliary data length specification. These values indicate to the host the end of the multicast address record in the

---

[12] ICMPv6 type = 143.

MLDv2 message. The MLDv2 protocol specifies that any data beyond the end of the last record in the message is ignored except for the checksum calculation. The extra fields at the end of MLDv2 report messages can be employed to carry security information.

MLDv2 Query Messages

The query messages of both MLD versions share the same format and ICMPv6 type = 130. The query message versions are distinguished by inspecting its length. If the query message length, $L_{\text{MLD}} \geqslant 22$ octets, it is an MLDv2 query message and therefore does not necessarily have additional information at the end. Any additional information present describes query message semantics and timings, as well as a specified number of multicast source addresses, N_{S_i}. The data beyond the end of the base query fields are ignored, except for the purpose of checksum calculations. The MLDv2 query message fields can be used for security information such as a signatures and authentication.

Multicast Router Solicitation Messages

Multicast Router Solicitation messages are used by Layer-2 switches to request explicit RA messages from multicast routers. There are no configuration parameters in this 4 octet solicitation message, and no explicit delays required by responding routers. The recent IETF discussions seem to agree that data after the end of a message should be ignored (except for ICMPv6 checksums). The implied additional length would be that of the IP datagram minus the fixed message portion and IP headers. The only consideration is for routers to rate limit response advertisements [HM05] and hence minimise the potential for abuse through solicitation message replays.

Multicast Router Advertisement Messages

The IPv4 and IPv6 Multicast Router Advertisement messages share a common format. The IPv6 RA are ICMPv6 messages similar to that of MLD messages and have the same general checksum requirements. The RA messages are 8 octets long and have fixed fields for checksum and the router's multicast advertisement interval. The message also has fields for QI and RV derived from the router's MLDv2 timer settings. There are no correlating fields between solicitation and advertisement messages nor any indication of the message arrival (with no sequence numbers or timestamps). The repetition of previously received messages is therefore trivial if a malicious host exists along the path or link.

Multicast Router Termination Messages

Both the MRD and MLDv1 protocol define terminate messages to update multicast group management explicitly. The MLDv2 protocol in contrast, employs a common report type but with empty record fields to achieve a similar function. The MLDv2 configuration parameters do not affect the zero record MLDv2 4 octet message. Similar to the MLDv2 report messages, the extra fields at the end of the message can be utilised for security information.

Summary of Messages and Formats

Apart from the MLDv1 query message, all other IPv6 messages discussed above provide extra fields at the end of the message which could be utilised. If the fields are used for security information such as a signatures, updating and explicit identification of the host, it can be used for message authenticity and traceability. The existing MLDv2 implementations would be able to read the messages, but not interpret the security information contained in those fields. Due to the inability to add information to the MLDv1 query messages, it may be impossible to provide any security for MLDv1 devices. Multicast snooping devices wishing to support security mechanisms would have to do employing the MLDv2 protocol.

6.7 Conclusion

In this chapter, the analysis presented attempts to expand the current state of multicast security research [CM03, HHC01] and standards [KA98a, Aur05] with the inclusion of MLDv2 signaling considerations. The various trust models presented demonstrate that MLDv2 is susceptible to various forms of abuse, leading to potential of malicious attacks and very substantive damage. Various initiatives to secure local IPv6 unicast packet delivery indicate that it may be worth evaluating whether similar security measures are viable and applicable for multicast group membership management as well.

Although there are no explicit solutions provided as part of this research, the threats and trust models identified will be useful in designing and testing future security mechanisms for multicast group management.

Chapter 7

Conclusions

7.1 Thesis Contribution

7.1.1 MIPv6 SSM

To a large extent, the newly proposed SSM and MIPv6 protocols overcome the complexities of prior attempts at mobile multicasting. However, both protocols have outstanding issues to be addressed before they can be widely deployed. The focus of the research in this thesis is to improve the efficiency and scalability of multicast communications, particularly for mobile hosts and networks. The solutions proposed in this thesis are based on the SSM MIPv6 RS method.

The MIPv6 SSM group management signaling traffic overhead efficiency and handover latencies are critical performance issues addressed in this thesis. The proposed solution retains the efficiency of multicasting data delivery and maintains optimal routing in spite of mobile host movements and subsequent network re-attachments. Also, due to the one-to-many (and generally, high data rate) nature of multicast applications, the multicast security analysis conducted in this research is especially important.

7.1.2 MLDv2 Analysis Framework Formulation

A critical component to support SSM is the newly proposed MLDv2 group management protocol which is capable of multicast data source filtering. The SSM model and the MLDv2 protocol are relatively new and no prior performance studies were available during the course of this project. The MLDv2 protocol requires a vigorous performance study to determine the signaling traffic characteristic and evaluate the possible efficiency penalties.

A MLDv2 performance measurement framework relating the protocol timers, messages and query/reply sequence was formulated. The MLDv2 signaling traffic overhead and multicast handover latency equations were derived for the various multicast join, leave and steady state events. The derived equations relate the MLDv2 signaling traffic overhead efficiency to the multicast robustness, number of hosts and channels. The MLDv2 signaling and latency performance using the default protocol settings and subsequently for the entire operating range were measured and analysed. The analysis results indicate the MLDv2 signaling traffic overhead efficiency and the multicast handover latencies are not suitable for real-time applications and need to be addressed.

7.1.3 Improved MLDv2 Signaling Traffic Performance

The experimental results in Chapter 3 show that the existing MLDv2 signaling traffic overhead performance penalty during a multicast leave is too high. In this research, the Adaptive Listener Tracing (ALT) method is proposed to improve the MLDv2 signaling traffic efficiency. The ALT algorithm only requires multicast router implementation and does not require any modifications for multicast hosts. The ALT algorithm does not disrupt the current MLDv2 protocol workings in any manner. The algorithm's tracing mechanism is adaptive to the number of multicast hosts on the network. The use of ALT decreases the multicast leave MLDv2 protocol signaling traffic, $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ irrespective of the number of multicast hosts N_{MN}, multicast groups N_{G} and number of data sources N_{S_i} present.

The experimental results using the ALT method in Chapter 4 show a significant improvement of 30.91% and 95.99% for the average MLDv2 signaling traffic, R_{MLD} and $R_{\mathrm{MLD}_{\mathrm{LLQI}}}$ respectively. The improved MLDv2 signaling traffic efficiency with the ALT method is useful for designing and developing future multicast routing and possibly resource reservation protocols for mobile networks.

7.1.4 Reduced Mobile Multicast Handover Latencies

In Chapter 5, movement and handover associated multicast latency issues for mobile hosts were identified and addressed. The Layer-2 triggering mechanism is proposed to initiate multicast group management updating in order to reduce the handover join and leave latencies. The Layer-2 triggering mechanism is able to reduce the average multicast Handover Latency, T_{MH}, from 71.77s to 0.44s. The experiments also reveal that approximately 90% of the Layer-2 handoff latency is contributed by the channel probing stage. The formulation of better channel probing techniques will reduce the overall handover latency even further.

7.1.5 MLDv2 Security and Threat Analysis

In this thesis, we have expands the current state of multicast security research with the inclusion of group management signaling considerations. The security considerations and trust models for MLDv2 including the interactions with Layer-2 and multicast proxy devices are identified and investigated. A security and threat analysis for each model is conducted. Possible attacks ascribed to particular roles within the network are evaluated with respect to the various initiatives and proposals within the IETF to secure local IPv6 packet delivery. We have demonstrated through the various trust models that MLDv2 is susceptible to various forms of abuse. The abuse can lead to the potential of malicious attacks and very substantive damage.

7.2 Future Work

The MLDv2 performance results and analysis presented in this thesis do not take into account the Layer-2 overhead packets. For MIPv6 SSM deployment purposes, network engineers would require the access network bandwidth and overhead traffic considerations for multicast service planning and provisioning. The MLDv2 performance framework derived in this research should be extended to include the various wireless access schemes available today.

The ALT method is also self synchronized for the number of last listener list records (N_{ll}) with the traced number of listeners traced (k). The ALT algorithm can be further optimised by finding the ideal tracing number (k) for the various number of multicast hosts. This research can be further improved by conducting an in depth analysis of the trade off between the signaling bandwidth efficiency versus the router processing power and memory requirements of the algorithm.

The IETF standardisation process is long and the MLDv2 protocol specification has taken almost three years to finalise through multiple draft standard iterations. The IETF has recognised the importance of initiating the standardisation process for mobile multicasting and started an initiative under the Mobility Operations (MobOpts) Working Group [SW05a]. Mobility extensions to IPv6 multicast and problems arising from mobile group communication are going to be addressed in the MobOpts WG. The outcome of this research will be channeled through the WG for standardisation considerations.

The multicast tree reconstruction and latency results from this research using Layer-2 triggering show potential for the use of real-time applications. However, the simulation experiments should be extended to include a better Internet-like topology for example *nem* based on map sampling [MP02]. The simulations can also be improved by evaluating host mobility factors and empirical listener densities if known. The simulation models should be extended to determine continuous host movement and effects on multicast tree reconstructions.

The PIM-SSM routing is initiated to deliver data towards hosts from the specified multicast data source. The data source address needs to be made known to the host in advance before it can subscribe to the appropriate channel. There has been some research and progress in providing out-of-band source knowledge for example in Session Initiation Protocol (SIP) [RSC$^+$02] applications. Source information can also be obtained through administrative channels like SAP/SDR [HPW00] schemes or web pages. Promising attempts to develop source address discovery mechanisms are on the way [SW05b].

The PIM-SSM Internet-wide routing scalability is also an unknown quantity. It is an especially acute issue for frequent mobile multicast host movement and data delivery tree reconstructions. The AAA framework [ACG00] has been proposed but no real wide scale deployments exist to understand the implementation difficulties. The multicast tree reconstruction, source information discovery and AAA implementations are all crucial research areas to ensure the wide adoption of MIPv6 SSM systems.

The increasing demand of mobile networks to support Internet hosts has lead to new Internet Research Task Force (IRTF)[1] research and IETF standardisation efforts. Recently, the IRTF has started research efforts for IP mobility optimizations to better understand mobility on the Internet. Similar to the research conducted for this thesis, the IRTF are working towards a successful handover of Internet hosts from one point to another of network attachment. The research efforts include establishing Layer-2 re-authentication, IP connectivity (including network-layer re-authentication) and new route initiation when the handover leads to a subnet change. The IRTF will examine the feasibility of generic mechanisms which integrates the IP and Layer-2 mobile inter-networking for improved handover performances. The IRTF findings will benefit the IETF and IEEE standardization efforts.

---

[1] https://www.irtf.org

Publications Related to the Study Presented in this Thesis

Journal Articles

[with Y. A. Şekercioğlu and W. Chen and N. Mani] Performance of Multicast Listener Discovery (MLDv2) Protocol in Mobile IPv6 Networks: Problems and Possible Solutions *Computer Communications*, (submitted), August 2005.

[with Y. A. Şekercioğlu and L. Chi and N. Mani] Source Specific Multicast (SSM) in Mobile IPv6 Networks: Deployment Experiences and Possible Improvements *TBD*, 2006.

Conference Papers

[with G. Daley and Y. A. Şekercioğlu] Trust Models and Security Considerations in Multicast Listener Discovery Protocol version 2 (MLDv2). In *Proceedings of the IEEE International Region 10 Conference (TENCON 2005)*, Melbourne, Australia, December, 2005.

[with Y. A. Şekercioğlu and N. Mani] Source Specific Multicast (SSM) Group Management Analysis Framework for the Next Generation Mobile Internet. In *Proceedings of the 1st Conference on Next Generation Internet Networks Traffic Engineering (NGI05)*, Rome, Italy, April 2005.

[with G. Daley and Y. A. Şekercioğlu] Improving Multicast Group Management in the Next Generation Mobile Internet. In *Proceedings of the Australian Telecommunication Networks & Applications Conference (ATNAC 2004)*, Sydney, Australia, December 2004.

[with Y. A. Şekercioğlu] Source Specific Multicast (SSM) for MIPv6: A Survey of Current State of Standardisation and Research. In *Proceedings of Australian Telecommunication Networks and Applications Conference (ATNAC 2003)*, Melbourne, Australia, December 2003.

IETF Standardisation Document Submissions

[with G. Daley] Trust Models and Security in Multicast Listener Discovery. draft-daley-magma-smld-prob-00.txt Submitted to IETF Multicast and Anycast Group Management (MAGMA) Work Group, July 2004.

[with G. Daley] Requirements for Mobile Multicast Clients. draft-daley-magma-mobile-00.txt Submitted to IETF Multicast and Anycast Group Management (MAGMA) Work Group, June 2003.

Appendix A

MLDv2 Analysis Framework

A.1 Messages and Timers for SSM

The MLDv2 specification document provides a canonical and comprehensive list of messages and timers used in the protocol [VC04, Section 9]. The relevant MLDv2 report and query messages to join and leave SSM channels (S_i, G_j) are described in the following sections. The application layer[1] protocol uses the appropriate software sockets [TFQ04] to invoke a specific service interface call to enable or disable the reception of multicast data. The software service interface has two functions to enable the reception of multicast data. Firstly, the host adopts the multicast address G_j on its (IP) Layer-3 interface and becomes a member of the multicast group. Secondly, a MLDv2 join message is sent towards the MR to convey the host's multicast channel (S_i, G_j) (or interface address) information to the Multicast Router (MR).

As illustrated in Figure A.1, when a host joins a SSM channel, identified by the source IP address S_i, and multicast group address G_j, it sends State Change Report (SCR) messages towards the MR. The SCR messages contain the multicast record of both the source and group (S_i, G_j) addresses. The host sends multiple SCR messages onto the link with the destination IP address `ff02::16` for the reception of (all) configured MRs. The SCR messages inform the MR of the new multicast host on the network. When multiple MRs exist on the network, the MLDv2 protocol provides a mechanism to elect one of the routers as a Querier Router (QR).

The MR checks every SCR message received to ensure it has a valid link-local address, i.e. the Hop Limit field value is set to 1 and Router Alert option is present. For valid SCR messages, all MRs set the Multicast Address Listener

---

[1] Layer-7 in the OSI specified model.

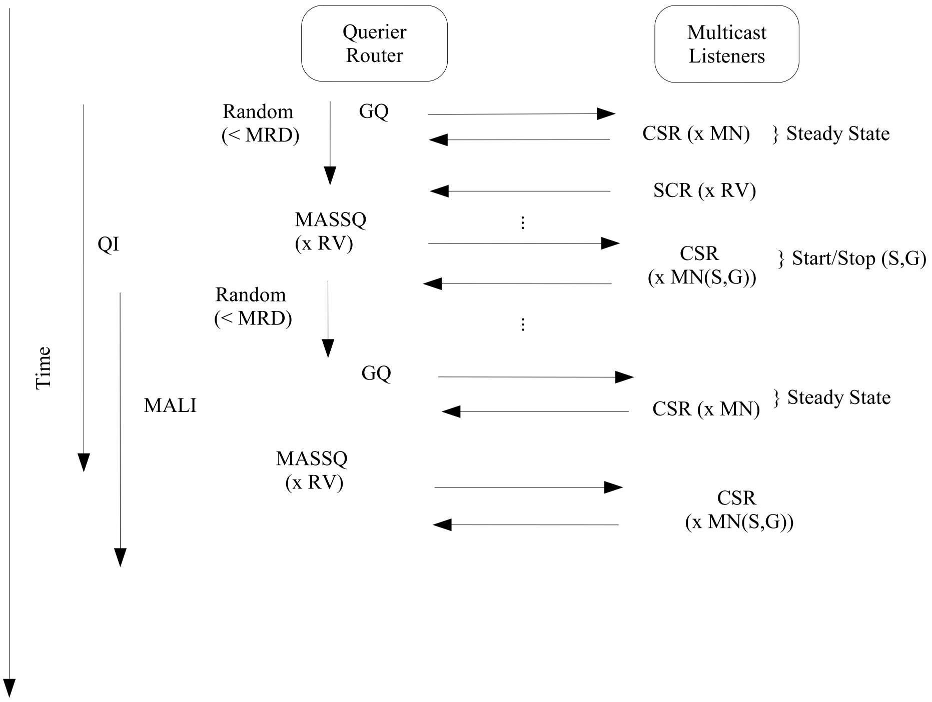


Figure A.1: The MLDv2 protocol query/reply message sequence and associated timers for SSM.

Interval (MALI) value, T_{MALI}[2], for the associated data channel (S_i, G_j) multicast record. The MLDv2 MALI setting, T_{MALI} is the duration before the MR decides there are no more multicast hosts for the channel (S_i, G_j) on a network.

To enhance the MLDv2 protocol robustness and to counter the possible unreliability of message exchanges, packet retransmissions are used. The MLDv2 message retransmissions are dictated by the Robustness Variable (RV) setting. The RV value can be configured. It is represented by a 3-bit Querier's Robustness Variable (QRV) field and has a maximum value of 7 (if not statically pre-configured by network administrators). In the multicast steady state (i.e. without multicast join or leave messages), to avoid MLDv2 signaling overload on the network, the General Query (GQ) and Current State Report (CSR) messages do not apply the RV retransmission rule. The assumption is that the GQ and SCR messages do not generate multicast state changes but they only refresh the current records held by the MR.

Assuming that no associated listening state changes occur for a multicast channel, the next GQ message is sent by the MR after Query Interval (QI) as shown in Figure A.1. Multicast hosts have to respond with a CSR message based on the

---

[2] See Table A.1.

PARAMETER	ABBREV.	DEFAULT VALUE	MIN / MAX VALUE	NOTES
Last Listener Query Interval	LLQI	$T_{\text{LLQI}} = 1\text{s}$	0s / 65.5s	
Query Interval	QI	$T_{\text{QI}} = 125\text{s}$	1s / 248s	Time between successive GQs
Query Response Interval	QRI	$T_{\text{QRI}} = 10\text{s}$	0s / 65.5s	$T_{\text{QRI}} < T_{\text{QI}}$
Robustness Variable	RV	2	0 / 7	Number of message retransmissions
Last Listener Query Count	LLQC	LLQC = RV		
Last Listener Query Time	LLQT	$T_{\text{LLQT}} = T_{\text{LLQI}} \times \text{LLQC}$		
Multicast Address Listening Interval	MALI	$T_{\text{MALI}} = \text{RV} \times (T_{\text{QI}} + T_{\text{QRI}})$		

Table A.1: The MLDv2 protocol timers and their settings.

Query Response Code (QRC) carried by the GQ message. The Maximum Response Delay (MRD) time T_{MRD} used by the host is derived from the QRC field using an exponential algorithm [VC04, Section 5.1.3] to calculate its value. The MRD setting T_{MRD} dictates the duration which is available to the host for responding to the QC message. The actual sending of the CSR message is based on a random delay, t_{r} within the maximum MRD value, T_{MRD}, as shown in Figure A.4.

When a multicast host stops listening and sends leave SCR messages to that effect, the Querier Router (QR)[3] lowers the associated Source Timer value, T_{S_i} (if currently higher) to Last Listener Query Time (LLQT). The LLQT is the duration represented by the value of Last Listener Query Interval (LLQI), T_{LLQI}, multiplied by the Last Listener Query Count (LLQC). LLQT is tunable by changing either the LLQI or LLQC values. As shown in Table A.1, LLQI uses the same value as MRD with the default setting, $T_{\text{LLQI}} = 1\text{s}$. The QR sends out Multicast Address and Source Specific Query (MASSQ) messages to verify the SCR. The LLQC (with a default value of RV), is also the number of MASSQ messages sent before the QR assumes that there are no listeners for a particular channel (S_i, G_j). Non listener hosts do not respond to the MASSQ messages within the time set by T_{LLQI}, the MR updates the PIM-SSM routing protocol and stops forwarding the multicast channel (S_i, G_j). A summary of the MLDv2 protocol timers used in the SSM model is given in Table A.1.

---

[3] The elected MR on a network.

A.2 Signaling Traffic

All MLDv2 messages are made up of an IP header and a Multicast Address Record (MAR). The MLDv2 message length L_{MLD} is given by,

$$L_{\text{MLD}} = L_{\text{IPheader}} + L_{\text{MAR}}, \tag{A.1}$$

where L_{IPheader} is the IPv6 header length and L_{MAR} is the length of the Multicast Address Record (MAR) within the IP message. The MLDv2 message IPv6 header is a fixed length $L_{\text{IPheader}} = 8$ bytes [VC04, Section 5.2] as shown in Figure A.2a. The MAR is made up of the group address information G_j, $L_{\text{MAR}} = 20$ bytes and the source IP addresses N_{S_i} of each group as illustrated in Figure A.2b. The source IP address can be both in the `include` and `exclude` mode. Each IPv6 source address S_i has a length of 16 bytes. Hence, the length of a MLDv2 message from Equation A.1 can be rewritten as,

$$L_{\text{MLD}} = 8 + \sum_{i=1}^{N_G}(20 + 16N_{S_i}), \tag{A.2}$$

where N_G is the number of multicast groups and N_{S_i} is the number of data sources associated with the group i $(i = 1, ..., N_G)$. The GQ message is similar in length to a CSR but without any MAR ($N_G = 0$ and $N_{S_i} = 0$) and hence, $L_{\text{MLD}_{\text{GQ}}} = 28$ bytes. For a single channel (S_i, G_j) record, the SCR, CSR and MASSQ messages are 44 bytes long, given by $L_{\text{MLD}_{\text{SCR}}}$, $L_{\text{MLD}_{\text{CSR}}}$, $L_{\text{MLD}_{\text{MASSQ}}}$ respectively.

In the steady state, without any multicast host join or leave actions, 44 bytes long GQ messages are sent every QI. The existing listener hosts respond with CSR messages within the QRI time. The total number of MLDv2 messages on the network during the QI period (its current value being T_{QI}), is given by,

$$\begin{aligned} L_{\text{MLD}_{\text{QI}}} &= L_{\text{MLD}_{\text{GQ}}} + (N_{\text{MN}} \times L_{\text{MLD}_{\text{CSR}}}) \\ &= 28 + N_{\text{MN}}(8 + \sum_{i=1}^{N_G}(20 + 16N_{S_i})), \end{aligned} \tag{A.3}$$

in bytes, where N_G is the number of multicast groups, N_{S_i} is the number of data sources associated with the group i $(i = 1, ..., N_G)$ and N_{MN} is the number of multicast hosts on the network.

Varying the QI setting T_{QI} on the MR controls the average MLDv2 signaling traffic on the link in the multicast steady state. The higher the T_{QI} values, the longer the duration between successive GQ messages sent by the MR. All the multicast hosts need to respond to GQ messages within the QRI. The resultant length of the MLDv2 messages exchanged within the QRI duration T_{QRI} is given in Equation A.3. The MLDv2 signaling traffic data rate, R_{MLD} during a QRI in bps, is given by,

$$\begin{aligned} R_{\mathrm{MLD}} &= (\frac{L_{\mathrm{MLD_{QI}}}}{T_{\mathrm{QRI}}}) \times 8 \\ &= \frac{8(28 + N_{\mathrm{MN}}(8 + \sum_{i=1}^{N_G}(20 + 16N_{S_i}))}{T_{\mathrm{QRI}}}, \end{aligned} \tag{A.4}$$

where N_G is the number of multicast groups, N_{S_i} is the number of data sources associated with the group i $(i = 1, ..., N_G)$ and T_{QRI} is the current value of QRI duration. The factor 8 in Equation A.4 converts the message lengths in bytes to the data rate in bits per second.

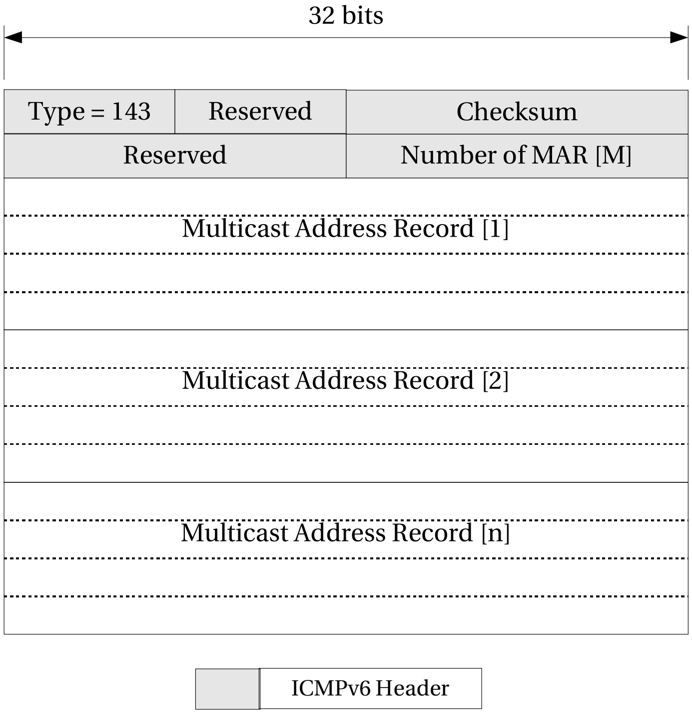
The multicast steady state on the network changes when hosts join or leave new or existing multicast channels. The resulting MLDv2 message exchange and the traffic activity (R_{MLD}) is different for both join and leave instances. During a multicast join, as shown in Figure A.1, there is minimal MLDv2 message exchange and hence, almost no impact on R_{MLD}. The host sends a join SCR message and the router processes the message, creates a MAR and notifies the routing protocol. The multicast routing tree is constructed and data forwarded to the link. When a leave SCR message is received, the MR sends out MASSQ messages. All other existing multicast hosts have to reply with corresponding CSR messages to update the MR. Both the MASSQ and CSR messages are RV dependent and retransmitted. In the event of a multicast leave, the corresponding length of MLDv2 messages $L_{\mathrm{MLD_{LLQI}}}$ in bytes, is given by,

$$L_{\mathrm{MLD_{LLQI}}} = (L_{\mathrm{MLD_{SCR}}} \times RV) + L_{\mathrm{MLD_{MASSQ}}} + (N_{\mathrm{MN}} \times L_{\mathrm{MLD_{CSR}}}), \tag{A.5}$$

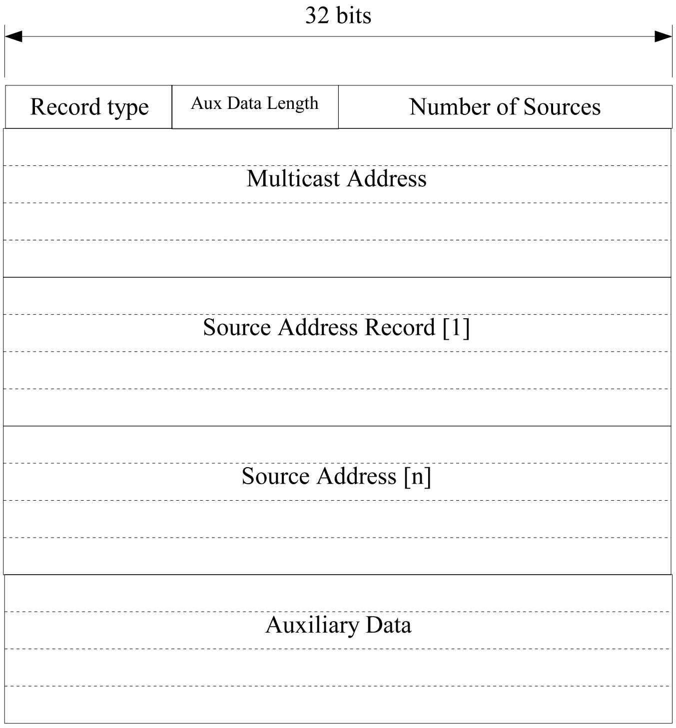
and the resultant MLDv2 signaling traffic $R_{\mathrm{MLD_{LLQI}}}$ in bps during the same period T_{LLQI} is given by,

$$R_{\mathrm{MLD_{LLQI}}} = \frac{(RV + 1 + N_{\mathrm{MN}}) \times (8 + \sum_{i=1}^{N_G}(20 + 16N_{S_i}))}{T_{\mathrm{LLQI}}}, \tag{A.6}$$

where N_G is the number of multicast groups, N_{S_i} is the number of data sources associated with the group i $(i = 1, ..., N_G)$, T_{LLQI} is the Last Listener Query Interval and N_{MN} is the number of multicast hosts.



(a) Message Format



(b) MAR Format

Figure A.2: A MLDv2 message showing the IP header and MAR.

A.3 Signaling Traffic Overhead Factor

In order to provide multicasting services on a particular access network, the MLDv2 signaling data rate has to be considered for bandwidth provisioning purposes. The multicast application data R_{APP} remains constant regardless of the number of multicast hosts N_{MN}. The MLDv2 signaling traffic R_{MLD} is however, dependent on the number of hosts as shown in Equation A.4. The MLDv2 signaling overhead factor, η associated with each multicast channel (or application) is defined as,

$$\eta = (1 + \frac{R_{\mathrm{MLD}}}{R_{\mathrm{APP}}}), \tag{A.7}$$

where R_{MLD} is the MLDv2 signaling traffic and R_{APP} is the application data rate. The MLDv2 signaling traffic is used for multicast bandwidth provisioning in specific access networks.

A.4 Link Bandwidth Capacity

In order to ensure that neither multicast data nor signaling messages are lost, the MLDv2 signaling traffic during a multicast leave event must be taken into consideration. The MLDv2 signaling traffic on the network during a multicast leave event is represented by $R_{\mathrm{MLD_{LLQI}}}$. For the purpose of bandwidth capacity planning in any given access network, the following condition has to be satisfied:

$$R_{\mathrm{ACC}} \geqslant R_{\mathrm{MLD_{LLQI}}} + R_{\mathrm{APP}}, \tag{A.8}$$

where R_{ACC} represents the access network bandwidth, R_{APP} the application data rate and $R_{\mathrm{MLD_{LLQI}}}$ is MLDv2 signaling data rate during a LLQI.

The MLDv2 protocol timers and signaling traffic are illustrated in Figure A.3. The multicast network bandwidth can be approached from two planning considerations. Firstly, given a particular access network having the bandwidth R_{ACC}, and the multicast application data rate R_{APP}, the maximum number of multicast hosts (N_{MN}) must satisfy,

$$N_{\mathrm{MN}} \leqslant (\frac{(R_{\mathrm{ACC}} - R_{\mathrm{APP}}) \times T_{\mathrm{LLQI}}}{(8 + \sum_{i=1}^{N_G}(20 + 16N_{S_i}))}) - RV - 1, \tag{A.9}$$

where N_G is the number of multicast groups, N_{S_i} is the number of data sources associated with the group i ($i = 1, ..., N_G$), T_{LLQI} is the value of the Last Listener Query Interval, R_{ACC} is the access network bandwidth and R_{APP} is the application

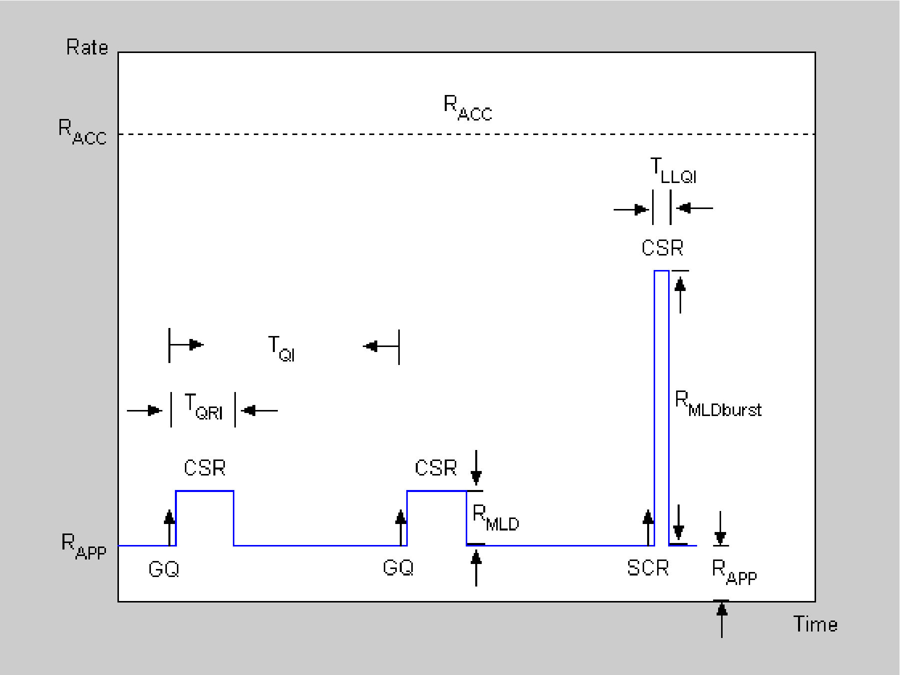


Figure A.3: The MLDv2 protocol data rates and timings.

data rate.

The second multicast network design consideration is, given a particular access network bandwidth and perceived number of multicast hosts, the maximum possible application data should satisfy,

$$R_{\mathrm{APP}} \leqslant R_{\mathrm{ACC}} - \frac{(RV + 1 + N_{\mathrm{MN}}) \times (8 + \sum_{i=1}^{N_G}(20 + 16N_{S_i}))}{T_{\mathrm{LLQI}}}, \qquad (\mathrm{A.10})$$

where N_G is the number of multicast groups, N_{S_i} is the number of data sources associated with the group i $(i = 1, ..., N_G)$, and T_{LLQI} is the value of the Last Listener Query Interval.

A.5 Mobility Considerations

A.5.1 Join Latency

A mobile host which moves between IP subnets requires MLDv2 updating to continue receiving multicast data. For inter-router and intra-router movements, the mobile host has to re-attach to the network at the IP layer. Relying on the MLDv2 mechanism alone for multicast updating, the host will have to wait for the next scheduled GQ message in the new subnet to continue receiving multicast data. The multicast Join Latency T_{JL}, is the delay or disruptive period for the multicast service and is given by,

$$T_{\mathrm{JL}} = T_{\mathrm{QI}} + t_r - \tau, \tag{A.11}$$

where τ is the MN handover time which has lapsed since the last GQ on the new link, T_{QI} is the Query Interval of the newly joined link and t_r is the random CSR message reply time within the T_{QRI}. The timing intervals and the handover point during the MN movement is shown in Figure A.4.

A.5.2 Leave Latency

Without any movement prediction mechanisms, a MN is unlikely to send a multicast leave SCR message before leaving one part of the network. If it is the last host listening to a particular channel, the host movement will leave behind a trailing multicast state on the previous link. The trailing state will only be addressed at the next MASSQ message (after the MALI interval T_{MALI}, which is much greater than the T_{QI}) is sent. The MAR timer will then be set to the LLQI timer, T_{LLQI}. If no other multicast hosts respond within the T_{LLQI} period, the MR updates the PIM-SSM routing protocol and multicast data is no longer forwarded on that link. The time for the trailing states still held in the previous router is called the multicast Leave Latency (T_{LL}) and given by,

$$\begin{aligned} T_{\mathrm{LL}} &= T_{\mathrm{MALI}} + T_{\mathrm{LLQI}} \\ &= ((\mathrm{RV} \times T_{\mathrm{QI}}) + T_{\mathrm{QRI}}) + T_{\mathrm{LLQI}}, \end{aligned} \tag{A.12}$$

where, RV is the Robustness Variable, T_{QI} is the current Query Interval value, T_{QRI} is the Query Response Interval setting and T_{MALI} and T_{LLQI} are the current values of the Multicast Address Listener and the Last Listener Query intervals respectively.

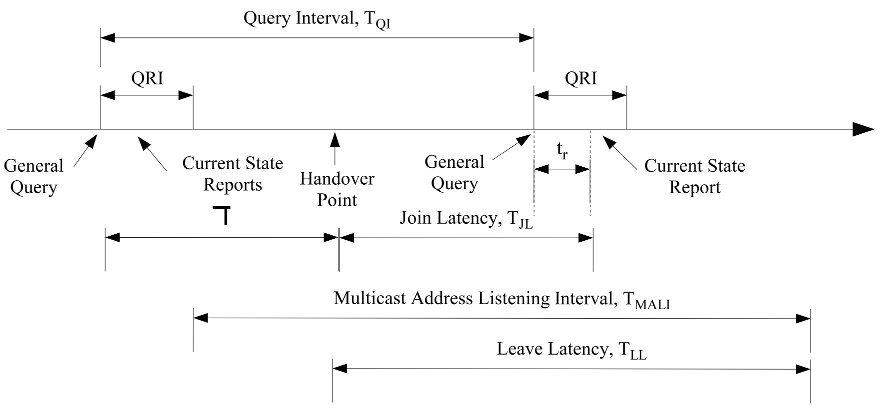


Figure A.4: Time line showing the mobile multicast join and leave latencies.

Appendix B

Simulation

B.1 MLDv2 Implementation

The simulation experiments were conducted on the OMNeT++ simulation platform [OMN96]. As part of the ongoing research program at CTIE[1], on performance analysis of protocols for mobility management in IPv6 networks, a set of OMNeT++ models for accurate simulation of IPv6 protocols was developed [LWV$^+$02]. The IPv6 simulation model suite consists of several functional blocks. The simulation accuracy is ensured because of the fine-grained level of details in the simulation [WWL§05].

The MLDv2 model was created using the components of the existing ICMPv6 compound module as shown in Figure B.2. The MLDv2 functionalities were designed and created in the ICMPv6 message processor and multicast packet forwarding modules as shown in Figure B.3.

The ICMPv6 message processor module sends out the appropriate MLDv2 query and report messages with the following format:

1. **MLDv2 Record** (IPv6 multicast address, filter timer, filter mode, source list) where,

    - 'IPv6 multicast address' is the multicast address to which the upper layer request pertains to,
    - 'filter timer' is only used when the record is in `exclude` mode and represents the time for the Router Filter Mode to expire and switch to `include`

---

[1] The Centre for Telecommunications and Information Engineering, Monash University, http://www.ctie.monash.edu.au/.

   mode,

   - ‘filter mode’ may either be in `include` or `exclude` mode, and
   - ‘source list’ is either a list of zeros or contains the multicast source (unicast) addresses.

   The memory management is optimised by designing the records as a linked list. Each record describes a specific Multicast Listening State, which consists of two independent source lists (for `include` and `exclude` modes). Each source list is with the format:

2. **Source Record** (IPv6 source address, source timer)

   - ‘IPv6 source address’ is the unicast address associated with the multicast group and
   - ‘source timer’ represents the expiry time for a specific source before being removed from the listening records.

The MLDv2 core module processes and sends the relevant ICMPv6 message according to the new MAR. When a MLDv2 query message is received, the listener responds after a random delay, bound by MRD, a value derived from the message QRI. Before scheduling a response, the listener will check previously scheduled and pending responses and discard duplicates. Upon reception of CSR messages, the router determines whether it pertains a new or existing MAR. If a new MAR adds an entry for the corresponding information. Else, it updates the record filter and source timers. A listener may send either a Source List Change Report or a Filter Mode Change Record for a given MAR. The router must specifically query sources that do not require forwarding. Simultaneously, the router lowers the corresponding source timers to a small interval of LLQT. If no interested report messages are received, the entry is deleted. Multicast traffic forwarding is according to the current maintained listening state which is built from the MLDv2 information base. The listener and router are in the format:

1. **Multicast Listener**

   - Listeners have their own current listening state record. Local changes (join or leave) to the listening state causes an SCR to be sent towards the multicast router immediately.

2. **Multicast Router**

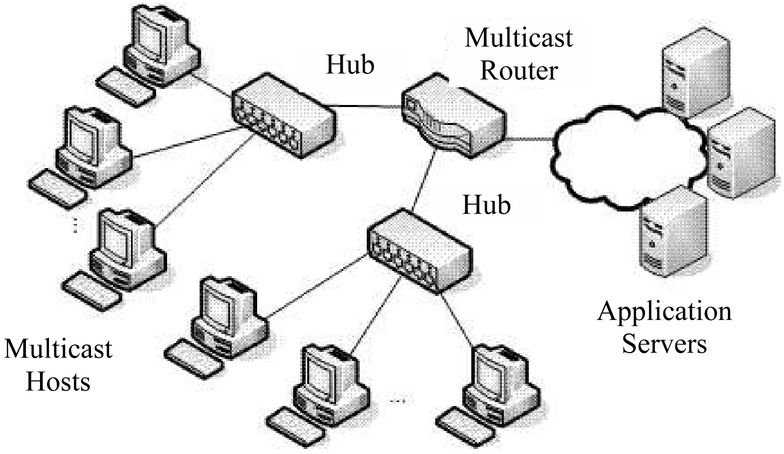


Figure B.1: Topology of the simulated network.

- The routers periodically send GQ messages[2] to learn and update group management on an attached link.

B.2 Network Topology

The simulation experiment test network topology is illustrated in Figure B.1. This topology was also used by Liao et al. for the RGMP evaluation experiments [LY04]. The multicast router has several interfaces connected to different IP subnets. Each hub connects multiple hosts together. Application servers are located in a virtual network cloud and they send multicast data according to the multicast hosts' listening states.

B.3 Simulation Parameters

The simulation experiments were all conducted with the same parameters (and corresponding values) given in Table B.1. At t = 10s, the router sends a GQ message to all of its directly connected interfaces. With the default QRI setting, the listeners uses the Interface Timer to schedule a response after a random delay bound by, $T_{\mathrm{QRI}} = 10$s. At t = 25s, a join SCR message for a new record is sent from a specific listener. The router checks if the received record exists. If it is an existing record, the source timer is reset $T_{S_i} = T_{\mathrm{MALI}}$, else, the router creates a new MAR for the information received.

---

[2] With ICMPv6 MAR = 0.

Simulation Model	Parameter	Value
Multicast Router	Query Interval (QI)	125s
	Query Response Interval (QRI)	10s
	Last Listener Query Interval (LLQI)	1s
	Multicast listening state	Empty
Listeners	Per-Interface state:	
	Number of GroupAddress	5
	Number of Sources per group	10
	Filter mode	`include`
Application Servers	Application bandwidth	20kbs

Table B.1: The MLDv2 protocol parameter settings for the simulation experiments.

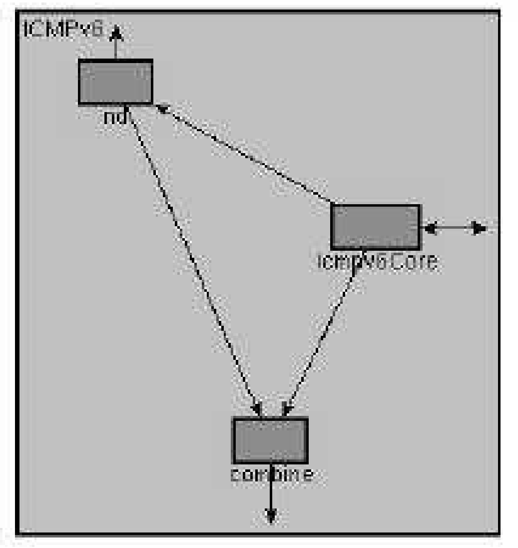


Figure B.2: Components of the ICMP compound module.

At t = 30s, all the records are deleted on a specific listener and the host sends a leave SCR message. The router checks whether the received record exists and if it does (in `include` mode), the router sets the Maximum Response Code = LLQI and sends a MASSQ message for the record.

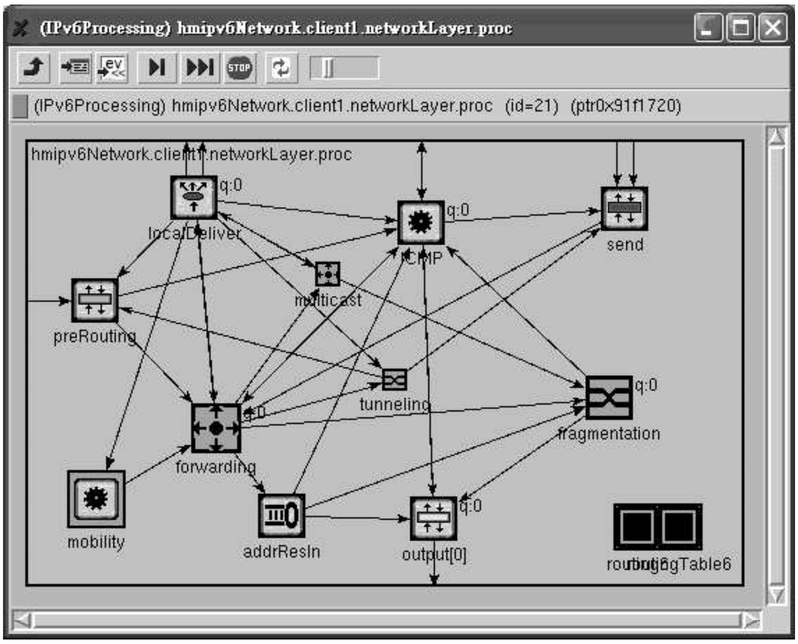


Figure B.3: Simulation models.

Appendix C

MIPv6 SSM Testbed Network

C.1 Network Devices

C.1.1 IPv6 Software

The Widely Integrated Distributed Environment Project (WIDE) [Thee] in Japan, has been the leading research group for IPv6 development. The WIDE group has an extensive IPv6 testbed network and it has been releasing IPv6 implementations on Linux (UniverSAl playGround for IPv6 – USAGI) [Thed] and Berkeley Software Development (BSD) suite (KAME) [Theb]. The WIDE group designed and built the first IPv6 multicast network [Jin00]. We did not have access to the WIDE network and did not use it for our experiments. We did, however, use the WIDE-developed IPv6 implementations on Linux and BSD. The following sections describe how the network elements required for the testbed network were built and configured.

C.1.2 Multicast Routers

The multicast routers for the IPv6 SSM testbed network were built using simple PC machines with multiple physical network interface cards. There are commercial and open-source router platforms at various stages of development and implementation available for building a SSM router. The IPv6 capable FreeBSD OS which supports multicast routing protocol software modules (daemons[1]) were installed on the routers. The forwarding of multicast packets is no different for SSM than for ASM but the routing mechanism is different. The PIM-SSM multicast routing protocol

---

[1] The daemon() function is for programs wishing to detach themselves from the controlling terminal and run in the background as system daemons.

[FHHK04] has been specified for the usage of SSM systems [HC04]. A snap-shot of SSM compatible routers and software (as of the 3rd Quarter of 2004) are listed in the 6NET SSM application testing study [Cho05].

The multicast routers for the testbed network were built using:

- A PC with Pentium II-300 MHz processor and 256MB RAM,
- Three 100Mbps Ethernet Network Interface Cards,
- FreeBSD 4.9–RELEASE Operating System [Thea],
- Mroute6d[2] as the routing protocol with:
    - *route6d* - which provides the IPv6 unicast routing daemon and
    - *pim6sd* - IPv6 PIM sparse mode routing protocol daemon[3].

The original IPv6 PIM software development was from KAME which is available on the FreeBSD OS. The updated *pim6sd*[4] version used on the routers in this experiment was developed at the University of Strasburg (UoS). The UoS multicast routing protocol software has RP-embedded support and *Hello* option number 19 support (Router Option priority [FHHK04, Section 32]). The UoS software version is preferred as it supports fast SSM joins and decrease the join delay for an SSM source.

Wireless Network

The wireless network was built using devices compliant to the IEEE 802.11b specification [IEE]. The IEEE 802.11b wireless access network specifies a high data rate Direct Sequence Spread Spectrum (HR/DSSS) with a maximum data rate of 11 Mbps. The IEEE 802.11b devices operate at the 2.4GHz frequency band with 13 channels which are 5MHz wide. The three APs in the testbed network are located in the same coverage area and set at three different channels as not to cause interference with each other. The theoretical maximum data rate is 11 Mbps, although the actual throughput is likely to be in the 4 to 6 Mbps range depending on ambient conditions.

A snap-shot of usable devices for MIPv6 (as of the 3rd Quarter of 2004) is listed in the 6NET wireless access network study [Dun04, Section 8]. The Wired

---

[2] The software can be invoked from `src/etc/rc.d/mroute6d` on the FreeBSD OS [Thea].

[3] The standalone version for Linux and *BSD systems supports PIMv2 (Protocol Independent Multicast version 2) sparse mode [FHHK04].

[4] CVS version 2004/11/24 from the University of Strasburg (UoS) [Mic].

Equivalent Privacy (WEP) protocol is also enabled on all APs to enhance security in the network and minimise any external affects on the experimental measurements. The wireless device used is:

- Access Point
    - Dlink-DWL-7100 and
    - WEP enabled.

There are APs which support higher layer functionalities such as IPv6 routing, DHCPv6, Home Agent, RADIUS, SNMP etc. In the testbed network design, these protocols were deployed elsewhere in the network, generally in the Access Router and not at the APs.

C.1.3 Multicast Nodes

Listener Hosts

The multicast host uses Fedora Core3 MLDv2 enabled in the kernel[5] as the OS. The network set up is initially tested using the `mpsend`[6] software which is modified to send multicast packets with additional timing and sequence information. The `mcastread`[7] software is also modified to receive, record and display packets according to the sequence number. The multicast packets containing the additional time stamp and sequence number assists in the debugging process. Using both these software packages, the MLDv2 protocol was determined to be working in the network.

Support for SSM in vendor and open source platforms is growing in stature. In our trials we were able to connect eight sites with a variety of such platforms, verifying the basic operation of the protocol, and demonstrating a new reliable file transfer protocol (FLUTE) with an application called Mad, which the project ported so support IPv6 SSM.

The multicast host was built using:

- A PC with Pentium II-300MHz processor with 256MB RAM,
- One 100Mbps Ethernet Network Interface Card,

---

[5] The Linux kernel supports MLDv2 from version 2.4.22 upwards.

[6] The software can be invoked from /kame/freebsd4/usr.sbin/mping/mpsend/ on the FreeBSD OS [Thea].

[7] The software can be invoked from /kame/freebsd4/usr.sbin/mping/mpsend/ on the FreeBSD OS [Thea].

- Fedora Core3 RELEASE Operating System[8],
- MLDv2 function enabled from kernel.
- Application:
  - Robust Audio Tool (RAT)[9] for a IPv6 multicast music reception.
  - `Mad_flute`[10] [Thec] used as an SSM host application.

The mobile multicast host is built using:

- A PC with Pentium II 500MHz with 256MB RAM
- An IEEE 802.11b Cisco Aironet 350 Network Interface Card,
- Fedora Core3 RELEASE Operating System[11],
- MLDv2 function enabled from kernel,
- Application:
  - Robust Audio Tool for a multicast music service.
  - `Mad_flute` [Thec] as the SSM host application.

Data Source

The multicast data source host is built using:

- A PC with Pentium II 300MHz with 256MB RAM,
- A 100Mbps Network Interface Card,
- FreeBSD4.9R+KAME20040726-freebsd49-snap Operating System,
- MLDv2 functionality enabled from KAME kernel.
- Application:
  - Robust Audio Tool

---

[8] http://download.fedora.redhat.com/pub/fedora/linux/core/3/.

[9] RAT is an open source audio conferencing and streaming application developed by University College London http://www-mice.cs.ucl.ac.uk/multimedia/software/rat/.

[10] A new application called Mad using the reliable file transfer protocol (FLUTE) http://www.atm.tut.fi/mad/download.html.

[11] http://download.fedora.redhat.com/pub/fedora/linux/core/3/.

  - `mpsend`: The original mpsend software from KAME is modified to add the sequence number and time stamp on the packet.
  - `mcastread`: The original mcastread software from KAME is modified at also record the additional data information from the SSM data source.

The `mpsend` and `mcastread` software tools are a standard part of FreeBSD and useful for basic multicast testing.

C.2 Device Configuration

The MIPv6 SSM network was set up to conduct the experiments to measure the mobile multicast handover latencies. This network was configured for the measurement of procedures involved and the delay contribution towards the mobile multicast handover latency. The router configuration file specifies *pim6sd* as the multicast routing protocol and *route6d* to provide the underlying IPv6 unicast routing table. If the multicast router is an edge router (providing group management on directly attached links), it also sends Router Advertisement messages to the interfaces with hosts connected with network based IPv6 address prefixes.

The default MLDv2 ICMPv6 Type specified in the Linux kernel (up to version 2.6.5) has been wrongly set. The ICMPv6 Type = 206 should be replaced by the IANA assigned Type = 143. To do this, in the file, /usr/src/linux/include/linux/icmpv6.h we replace the ICMPv6 value of 206 with 143. The host's Linux kernel was recompiled to reflect this new ICMPv6 Type. In the file /etc/rc.conf, the host parameters are set as below,

```
ipv6_enable='YES'
ipv6_gateway\_enable='YES'
ipv6_ifconfig\_rl0='3ffe:3600:1:a::1 prefixlen 64'
ipv6_router\_enable='YES'
ipv6_router='/usr/sbin/route6d'
ipv6_router\_flags= -l
mroute6d_enable='YES'
mroute6d_program='/root/pim6sd/pim6sd'
mroute6d_flags='-d pim'
rtavdv_enable='YES'
rtadvd_interfaces='rl0'
```

In the file /etc/pim6sd.conf,

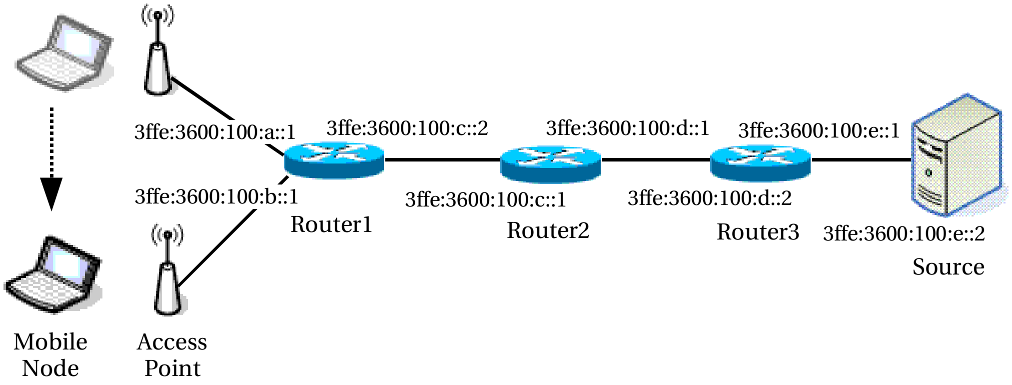


Figure C.1: Testbed Network Topology

```
phyint rl0 enable;
phyint rl0 mld_version 2;
log all;
```

The IP subnetting and address planning are significant parts of designing an IPv6 network. Normally, the number of APs per router influences the addressing plan but for a small testbed network, it is not of concern. Hosts belonging to the same subnet receive the same IPv6 prefix from the router's RA messages. The `/64` prefix is assigned to each router interface and AP.

C.3 Network Topology

The three multicast routers and two wireless APs for the mobile multicast experiments were set up as shown in Figure C.1. The routers are connected together using a 100 Mbps Ethernet connections. The wireless access uses 802.11b and set at 11 Mbps. To ensure an IPv6 only environment, all of the nodes have no IPv4 addresses configured on any of the interfaces. The *pim6sd* daemon for IPv6 sparse mode multicast providing PIM message exchanges between the multicast routers and MLDv2 capability on the router's network interfaces was enabled.

C.4 Measurement Tools

The internal system clocks on all the hosts and routers are synchronised using the Network Time Protocol (NTP) protocol [Mil92]. The Ethereal[12] software version

---

[12] http://www.ethereal.com/

15 was used to capture data packets on all the network interfaces and as the network protocol analyzer. The Ethereal software decodes all the captured packets and displays them with time stamps, characteristics and data contained within. The initial experiments captures and filters the MLDv2 packets to verify that the testbed network implementations comply with the published standards [VC04]. An IEEE802.11b wireless network sniffer[13] was also installed on the mobile hosts to capture and monitor all the Layer-2 interactions on the wireless interfaces. The captured and logged information from the software enabled us to determine the packet interactions and measure the delay component contributions to multicast handover latencies.

---

[13] Wireless Sniffer AiroPeek NX16, http://www.wildpackets.com/products/airopeek/overview.

References

[AA97] K. C. Almeroth and M. H. Ammar. Multicast Group Behavior in the Internet's Multicast Backbone (MBone). *IEEE Communications Magazine*, 35(6):124–129, June 1997.

[AABN03] S. Alouf, E. Altman, C. Barakat, and P. Nain. Optimal Estimation of Multicast Membership. *IEEE Transactions on Signal Processing*, 51(8):2165–2176, August 2003.

[ACG00] B. Aboba, P. Calhoun, and S. Glass. RFC 2989 Criteria for Evaluating AAA Protocols for Network Access, November 2000. URL reference: http://www.ietf.org/rfc/rfc2989.txt.

[Ark05] J. Arkko (Editor). RFC 3971 SEcure Neighbor Discovery (SEND). URL reference: http://www.ietf.org/rfc/rfc3971.txt, March 2005.

[AS03] H. Asaeda and S. Suzuki. MLDv2 Protocol Design, Implementation and Evaluation for Source-Specific Multicast over IPv6. In *Proceedings of the SAINT'03, Symposium on Applications and the Internet Workshops*, pages 244–249, Los Alamitos, USA, January 2003.

[ATS04] S. Androutsellis-Theotokis and D. Spinellis. A Survey of Peer-to-Peer Content Distribution Technologies. *ACM Computing Surveys*, 36(4):335–371, December 2004.

[Aur05] T. Aura. RFC 3972 Cryptographically Generated Addresses (CGA). URL reference: http://www.ietf.org/rfc/rfc3972.txt, March 2005.

[Bal98] A. Ballardie. RFC 2189 Core Based Trees (CBTv2) Multicast Routing, September 1998. URL reference: http://www.ietf.org/rfc/rfc2189.txt.

[BCKR98] T. Bates, R. Chandra, D. Katz, and Y. Rekhter. RFC 2283 Multiprotocol Extensions for BGP-4, February 1998. URL reference: http://www.ietf.org/rfc/rfc2283.txt.

[BFC95] T. Ballardie, P. Francis, and J. Crowcroft. Core Based Tree (CBT): An Architecture for Scalable Multicast Routing. In *Proceedings of the ACM Sigcomm*, pages 88–95, San Francisco, USA, September 1995.

[Bha03] B. Bhattacharyya (Editor). RFC 3569 An Overview of Source-Specific Multicast (SSM), July 2003. URL reference: http://www.ietf.org/rfc/rfc3569.txt.

[Bra96] S. Bradner. RFC 2026 The Internet Standards Process – Revision 3, October 1996. URL reference: http://www.ietf.org/rfc/rfc2026.txt.

[Cai02] B. Cain. RFC 3376 Internet Group Management Protocol, Version 3. URL reference: http:www.ietf.org/rfc/rfc3376.txt, October 2002.

[Cas93] S. Casner. Frequently Asked Questions (FAQ) on the Multicast Backbone. via anonymous ftp from URL reference: http://venera.isi.edu:/mbone/faq.txt, May 1993.

[CCH99] K. H. Chi, C. C. Cheng, and T. L. Huang. A Framework for Mobile Multicast Using Dynamic Route Reconstructions. *The Computer Journal*, 42(6):522–533, 1999.

[CD92] S. Casner and S. Deering. First IETF Internet Audiocast. *ACM SIGCOMM Computer Communication Review*, 22(3):92–97, July 1992.

[CD98] A. Conta and S. Deering. RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, 1998. URL reference: http://www.ietf.org/rfc/rfc2463.txt.

[Cho05] T. Chown (Editor). D5.9: Report Of Testing Application Over PIM-SSM Deployment. Technical report, Information Society Technologies, January 2005. URL reference: http://www.6net.org/publications/deliverables/wp5.

[CKS05] M. Christensen, K. Kimball, and F. Solensky. Considerations for IGMP and MLD Snooping Switches Internet Draft – work in progress, February 2005. URL Reference: http://www.ietf.org/internet-drafts/draft-ietf-magma-snoop-12.txt.

[CM03] C. Castellucia and G. Montenegro. Securing Group Management in IPv6 with Cryptographically Generated Addresses. In *Eighth IEEE International Symposium on Computers and Communication, 2003 (ISCC 2003)*, pages 588–593, Sydney, Australia, June 2003.

[CMK$^+$02] J. H. Cui, D. Maggiorini, J. Kim, K. Boussetta, and M. Gerla. A Protocol to Improve the State Scalability of Source Specific Multicast. In *IEEE Global Telecommunications Conference 2002 (GLOBECOM 02)*, volume 2, pages 1899–1904, Taipei, Taiwan, November 2002.

[Cra98] M. Crawford. RFC 2464 Transmission of IPv6 Packets over Ethernet Networks, 1998. URL reference: http://www.ietf.org/rfc/rfc2464.txt.

[DB03] T. Demirci and S. Bilgen. A Performance Study on Real-time IP Multicasting. In *Eighth IEEE International Symposium on Computers and Communication (ISCC 2003)*, volume 1, pages 441–446, 2003.

[DBV$^+$03] R. Dromsand, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney. RFC 3315 Dynamic Host Configuration Protocol for IPv6, July 2003. URL reference: http://www.ietf.org/rfc/rfc3315.txt.

[DC85] S. Deering and D. Cheriton. RFC 966 Host Groups: A Multicast Extension to the Internet Protocol, December 1985. URL reference: http://www.ietf.org/rfc/rfc966.txt.

[Dee88] S. E. Deering. Multicast routing in internetworks and extended LANs. In *Proceedings of the ACM SIGCOMM'88*, pages 55–64, Vancouver, Canada, August 1988.

[Dee89] S. Deering. RFC 1112 Host Extensions for IP Multicasting, August 1989. URL reference: http://www.ietf.org/rfc/rfc1112.txt.

[Dee91] S. Deering. *Multicast Routing in a Datagram Internetwork*. PhD thesis, Standford University, December 1991.

[DEF$^+$96] S. Deering, D. Estrin, D. Farinacci, V. Jacobson, G. Liu, and L. Wei. PIM Architecture for Wide-area Multicast Routing. IEEE/ACM Transactions on Networking, pg 153-162, April 1996.

[DFH99] S. Deering, W. Fenner, and B. Haberman. RFC 2710 Multicast Listener Discovery (MLD) for IPv6, October 1999. URL reference: http://www.ietf.org/rfc/rfc2710.txt.

[DH98] S. Deering and R. Hinden. RFC 2460 Internet Protocol, Version 6 (IPv6), 1998. URL reference: http://www.ietf.org/rfc/rfc2460.txt.

[DK03] G. Daley and G. Kurup. Requirements for Mobile Multicast Clients Internet Draft – work in progress. URL reference: http://www.ietf.org/internet-drafts/draft-daley-magma-mobile-00.txt, June 2003.

[DLL$^+$00] C. Diot, B. N. Levine, B. Lyles, H. Kassem, and D. Balensiefen. Deployment Issues for the IP Multicast Service and Architecture. *IEEE Network*, 14:78–88, February 2000.

[Dun04] M. Dunmore (Editor). 6NET Framework for the Support of IPv6 Wireless LANs Version 1. Technical Report Deliverable D4.2.2, December 2004. URL reference: http://www.6net.org/publications/deliverables/wp4.

[EFHT98] D. Estrin, D. Farinacci, A. Helmy, and D. Thaler (Editors). Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification, June 1998. URL reference: http://www.ietf.org/rfc/rfc2362.txt.

[Fen97] W. Fenner. Internet Group Management Protocol, Version 2, November 1997. URL reference: http://www.ietf.org/rfc/rfc2236.txt.

[FHHK04] B. Fenner, M. Handley, H. Holbrook, and I. Kouvelas. Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised) Internet Draft – work in progress, October 2004. URL Reference: http://www.ietf.org/internet-drafts/draft-ietf-pim-sm-v2-new-11.txt.

[FHHS04] B. Fenner, H. He, B. Haberman, and H. Sandick. IGMP/MLD-based Multicast Forwarding ("IGMP/MLD Proxying") Internet Draft – work in progress. URL reference: http://www.ietf.org/internet-drafts/draft-ietf-magma-igmp-proxy-06.txt, April 2004.

[FM03] B. Fenner and D. Meyer. Multicast Source Discovery Protocol (MSDP) Internet Draft – work in progress. URL reference: http://www.ietf.org/internet-drafts/draft-ietf-msdp-spec-20.txt, May 2003.

[FR04] F. Feng and D. Reeves. Explicit Proactive Handoff with Motion Prediction for Mobile IP. In *Proceedings IEEE Wireless Communications and Networking Conference*, pages 855–860, Atlanta, USA, March 2004.

[FT99] T. Friedman and D. Towsley. Multicast Session Membership Size Estimation. In *Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOMM'99)*, volume 2, pages 965–972, New York, USA, March 1999.

[GGZZ04] C. Guo, Z. Guo, Q. Zhang, and W. Zhu. A Seamless and Proactive End-to-end Mobility Solution for Roaming Across Heterogeneous Wireless Networks. In *IEEE Selected Areas in Communications*, volume 22 of *5*, pages 838–848, June 2004.

[GTBS99] R. Gilligan, S. Thomson, J. Bound, and W. Stevens. RFC 2553 Basic Socket Interface Extensions for IPv6, March 1999. URL reference: http://www.ietf.org/rfc/rfc2553.txt.

[Har97] T. Harrison. Mobile Multicast (MoM) Protocol: Multicast Support for Mobile Hosts. In *Proceedings of the ACM MOBICOM'97*, pages 151–160, Los Angeles, CA, US, September 1997.

[HC99] H. Holbrook and D. Cheriton. IP Multicast Channels: EXPRESS Support for Large-scale Single-source Applications. In *Proceedings of the ACM SIGCOMM'99*, pages 65–78, Cambridge, MA, USA, September 1999.

[HC04] H. Holbrook and B. Cain. Source-Specific Multicast for IP Internet Draft – work in progress, September 2004. URL Reference: http://www.ietf.org/internet-drafts/draft-ietf-ssm-arch-06.txt.

[HCH03] H. Holbrook, B. Cain, and B. Haberman. Using IGMPv3 and MLDv2 For Source-Specific Multicast. URL reference: http://www.ietf.org/internet-drafts/draft-holbrook-idmr-igmpv3-ssm-04, March 2003.

[HD98] R. Hinden and S. Deering. RFC 2373 IP Version 6 Addressing Architecture, 1998. URL reference: http://www.ietf.org/rfc/rfc2373.txt.

[HHC01] H. He, T. Hardjono, and B. Cain. Simple Multicast Receiver Access Control Internet Draft – work in progress. URL reference: http://www.ietf.org/internet-drafts/draft-ietf-gsec-smarc-00.txt, November 2001.

[HHK04] B. Haberman, H. Holbrook, and I. Kouvelas. Multicast Source Notification of Interest Protocol (MSNIP) Internet Draft – work in progress, 2004. URL Reference: http://www.ietf.org/internet-drafts/draft-ietf-magma-msnip-05.txt.

[HM05] B. Haberman and J. Martin. Multicast Router Discovery Internet Draft – work in progress. URL reference: http://www.ietf.org/internet-drafts/draft-ietf-magma-mrdisc-04.txt, February 2005.

[HPW00] M. Handley, C. Perkins, and E. Whelan. RFC 2974 Session Announcement Protocol, October 2000. URL reference: http://www.ietf.org/rfc/rfc2974.txt.

[HT02] B. Haberman and D. Thaler. RFC 3306 Unicast-Prefix-based IPv6 Multicast Addresses, August 2002. URL reference: http://www.ietf.org/rfc/rfc3306.txt.

[HW04] T. Hardjono and B. Weis. RFC 3740 The Multicast Group Security Architecture, March 2004. URL reference: http://www.ietf.org/rfc/rfc3740.txt.

[IEE] IEEE 802 LAN/MAN Standards Committee. URL Reference: http://www.ieee802.org/.

[Int] Internet Engineering Task Force Detecting Network Attachment Work Group. URL Reference: http://www.ietf.org/html.charters/dna-charter.html.

[Jia00] W. Jiang. *A Mobility Support Agent Architecture for Seamless IP Handover*. PhD thesis, The Department of Teleinformatics, Royal Institute of Technology, Stockholm, June 2000.

[Jin00] T. Jinmei. Implementation and Deployment of IPv6 Multicasting. In *Proceedings of the Internet Society Conference*, pages 277–283, Yokohama, Japan, July 2000.

[JN02] C. Jelger and T. Noel. Multicast for Mobile Hosts in IP Networks: Progress and Challenges. *IEEE Wireless Communications*, 9(5):58–64, October 2002.

[JN03] C. Jelger and T. Noel. An Analysis of Multicast Delivery with Mobile Receivers. In *The 14th IEEE 2003 International Symposium on Personal, Indoor and Mobile Radio Communication Proceedings*, volume 3, pages 2690–2695, Beijing, China, September 2003.

[JPA04] D. Johnson, C. Perkins, and J. Arkko. RFC 3775 Mobility Support in IPv6, June 2004. URL reference: http://www.ietf.org/rfc/rfc3775.txt.

[KA98a] S. Kent and R. Atkinson. RFC 2401 Security Architecture for the Internet Protocol, November 1998. URL reference: http://www.ietf.org/rfc/rfc2401.txt.

[KA98b] S. Kent and R. Atkinson. RFC 2402 IP Authentication Header, November 1998. URL reference: http://www.ietf.org/rfc/rfc2402.txt.

[KA98c] S. Kent and R. Atkinson. RFC 2406 IP Encapsulating Security Payload (ESP), November 1998. URL reference: http://www.ietf.org/rfc/rfc2406.txt.

[KDŞ04] G. Kurup, G. Daley, and Y. A. Şekercioğlu. Improving Multicast Group Management in the Next Generation Mobile Internet. In *Proceedings of Australian Telecommunication Networks and Applications Conference (ATNAC) 2004*, pages 433–436, Sydney, Australia, December 2004.

[Koo05] R. Koodli (Editor). Fast Handovers for Mobile IPv6 Internet Draft – work in progress. URL reference: http://people.nokia.net/~rajeev/draft-ietf-mobileip-fast-mip6-05.txt, June 2005.

[KRT+98] S. Kumar, P. Radoslavov, D. Thaler, C. Alaettinoğlu, D. Estrin, and M. Handley. The MASC/BGMP Architecture for Inter-domain Multicast Routing. In *ACM SIGCOMM 1998 Conference on Applications, Technologies, Architectures and Protocols for Computer Communication*, volume 28, pages 93–104, Vancouver, Canada, October 1998.

[Les04] L. Lessig. *Free culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity.* New York: Penguin Press, 2004.

[Lin02] C. R. Lin. Mobile Multicast Support in IP Networks. In *Proceedings of IEEE GLOBECOM 2002*, pages 1935–1939, Taipei, Taiwan, November 2002.

[LN00] C. Liu and J. Nonnenmacher. Broadcast Audience Estimation. In *Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOMM'00)*, volume 2, pages 952–960, Tel Aviv, Israel, March 2000.

[LNPK05] J. Loughney, M. Nakhjiri, C. Perkins, and R. Koodli. RFC 4067 Context Transfer Protocol (CXTP). URL reference: http://www.ietf.org/rfc/rfc4067.txt, July 2005.

[Lou04] J. Loughney (Editor). IPv6 Node Requirements Internet Draft – work in progress, August 2004. URL Reference: http://www.ietf.org/internet-drafts/draft-ietf-ipv6-node-requirements.

[LW00] C. R. Lin and K. M. Wang. Mobile Multicast Support in IP Networks. In *Proceedings of IEEE INFOCOMM 2000*, pages 1664–1672, Tel Aviv, Israel, 2000.

[LWV+02] J. Lai, E. Wu, A. Varga, Y. A. Şekercioğlu, and G. K. Egan. A Simulation Suite for Accurate Modelling of IPv6 Protocols. In *Proceedings of 2nd International OMNeT++ Workshop*, pages 33–36, Berlin, Germany, January 2002.

[LY99] W. Liao and D. Yang. Receiver-initiated Group Membership Protocol (RGMP): A new Group Management Protocol for IP Multicasting. In *Seventh International Conference on Network Protocols (ICNP '99)*, pages 51–58, Toronto, Canada, October 1999.

[LY04] W. Liao and D. Yang. Receiver-initiated Group Membership Protocol (RGMP): A new Group Management Protocol for IP Multicasting. *IEEE Transactions on Broadcasting*, 50(3):279 – 288, 2004.

[M6B] M6Bone – IPv6 Multicast Network. URL Reference: http://www.m6bone.net/.

[MB01] D. Mitton and M. St. Johns S. Barkley. RFC 3127 Authentication, Authorization, and Accounting: Protocol Evaluation, June 2001. URL reference: http://www.ietf.org/rfc/rfc3127.txt.

[MBM+99] J. McAuley, E. Bommaiah, A. Misra, R. Talpade, S. Thompson, and K. C. Young Jn. Mobile Multicast Proxy. In *IEEE Military Communications Conference (MILCOM'99)*, volume 1, pages 631–635, Atlantic City, USA, October 1999.

[Mic] H. Mickael. Standalone Pim6sd For Linux and *BSD. URL reference: http://clarinet.u-strasbg.fr/~hoerdt/pim6sd_linux/.

[Mil92] D. Mills. RFC 1305 Network Time Protocol (Version 3) Specification, Implementation and Analysis, March 1992. URL reference: http://www.ietf.org/rfc/rfc1305.txt.

[Mir01] N. F. Mir. A Survey of Data Multicast Techniques, Architectures, and Algorithms. *IEEE Communications*, 9:164–170, September 2001.

[Moo05] N. Moore. Optimistic Duplicate Address Detection for IPv6 Internet draft – work in progress. URL Reference: http://www.ietf.org/internet-drafts/draft-ietf-ipv6-optimistic-dad.txt, December 2005.

[Moy89] J. Moy. RFC 1131 Open Shortest Path First, October 1989. URL reference: http://www.ietf.org/rfc/rfc1583.txt.

[Moy94a] J. Moy. RFC 1583 Open Shortest Path First version 2, March 1994. URL reference: http://www.ietf.org/rfc/rfc1583.txt.

[Moy94b] J. Moy. RFC 1584 Multicast Extension to OSPF, March 1994. URL reference: http://www.ietf.org/rfc/rfc1584.txt.

[MP02] D. Magoni and J. J. Pansiot. Internet Topology Modeler based on Map Sampling. In *Proceedings of Seventh International Symposium on Computers and Communications 2002 (ISCC 2002)*, pages 1021–1027, Taormina, Italy, July 2002.

[MV05] I. Miloucheva and K. Venas. Multicast Context Transfer in Mobile IPv6 Internet Draft – work in progress. URL reference: http://www.ietf.org/internet-drafts/rfc-draft-miloucheva-mldv2-mipv6, June 2005.

[Nik04] P. Nikander (Editor). RFC 3756 IPv6 Neighbor Discovery (ND) Trust Models and Threats, May 2004. URL reference: http://www.ietf.org/rfc/rfc3756.txt.

[NNS98] T. Narten, E. Nordmark, and W. Simpson. RFC 2461 Neigbhour Discovery for IP Version 6 (IPv6), December 1998. URL reference: http://www.ietf.org/rfc/rfc2461.txt.

[OMN96] OMNeT++ object-oriented discrete event simulation system. URL reference: http://www.omnetpp.org, 1996.

[PA02] L. Perato and K. Al Agha. Handover Prediction: User Approach Versus Cell Approach. In *IEEE International Workshop On Mobile and Wireless Communications Networks (MWCN'02)*, pages 492–496, Stockholm, Sweden, 2002.

[Per96] C. Perkins (Editor). RFC 2002 IP Mobility Support, October 1996. URL reference: http://www.ietf.org/rfc/rfc2002.txt.

[Per02] C. Perkins (Editor). RFC 3344 Mobility Support in IPv4, August 2002. URL reference: http://www.ietf.org/rfc/rfc3344.txt.

[Per05] C. Perkins (Editor). Mobility Support in IPv4 (revised) Internet Draft – work in progress, October 2005. URL reference: http://www.ietf.org/internet-drafts/draft-ietf-mip4-rfc3344bis-02.txt.

[Por03] M. Portoles. IEEE 802.11 Link-layer Forwarding for Smooth Handoffs. In *Proceedings of 14th International Symposium of Personal, Indoor and Mobile Radio Communications (PIMRC2003)*, Beijing, China, July 2003.

[Ram03] M. Ramalho. Intra- And Inter-Domain Multicast Routing Protocols: A Survey and Taxonomy. *IEEE Communications Survey and Tutorials*, 3(1):2–25, 1st Quarter 2003.

[RKL$^+$04] I. Romdhani, M. Kellil, H-Y. Lach, A. Boubabdallah, and H. Bettahar. IP Mobile Multicast: Challenges and Solutions. *IEEE Communications Surveys and Tutorials*, 6(1):18–41, 2004.

[RS98] J. Rosenberg and H. Schulzrinne. Timer Reconsideration for Enhanced RTP Scalability. In *Proceedings of the Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '98)*, volume 1, pages 233–241, San Francisco, USA, 1998.

[RSC$^+$02] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. RFC 3261 SIP: Session Initiation Protocol, June 2002. URL reference: http://www.ietf.org/rfc/rfc3261.txt.

[Sav04] P. Savola. IPv6 Multicast Deployment Issues Internet Draft – work in progress, February 2004. URL Reference: http://www.m6bone.net/IMG/txt/draft-savola-v6ops-multicast-issues.txt.

[SCFJ96] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. RFC 1889 RTP: A Transport Protocol for Real-Time Applications, January 1996. URL reference: http://www.ietf.org/rfc/rfc1889.txt.

[SE01] P. Srisuresh and K. Egevang. RFC 3022 Traditional IP Network Address Translator (Traditional NAT), January 2001. URL reference: http://www.ietf.org/rfc/rfc3022.txt.

[SH99] P. Srisuresh and M. Holdrege. RFC 2663 IP Network Address Translator (NAT) Terminology and Considerations, August 1999. URL reference: http://www.ietf.org/rfc/rfc2663.txt.

[SW05a] T. Schmidt and M. Waehlisch. Multicast Mobility in MIPv6: Problem Statement Internet Draft – work in progress, October 2005. URL Reference: http://www.ietf.org/internet-drafts/draft-schmidt-mobopts-mmcastv6-ps.

[SW05b] Thomas C. Schmidt and Matthias Wählisch. Extending SSM to MIPv6 — Problems, Solutions and Improvements. *Computational Methods in Science and Technology*, 11, to appear 2005.

[TFQ04] D. Thaler, B. Fenner, and B. Quinn. RFC 3678 Socket Interface Extensions for Multicast Source Filters, January 2004. URL reference: http://www.ietf.org/rfc/rfc3678.txt.

[Thea] The FreeBSD Operating System. URL Reference: http://www.freebsd.org/.

[Theb] The KAME Project. URL Reference: http://www.kame.net/.

[Thec] The MAD Project. URL Reference: http://www.atm.tut.fi/mad/download.html.

[Thed] The USAGI Project – Linux IPv6 Development Project. URL Reference: http://www.linux-ipv6.org/.

[Thee] The WIDE Project – Widely Integrated Distributed Environment Project. URL Reference: http://www.wide.ad.jp/.

[TN98] S. Thomson and T. Narten. RFC 2462 IPv6 Stateless Address Autoconfiguration, 1998. URL reference: http://www.ietf.org/rfc/rfc2462.txt.

[TSKK03] O. Tetsuya, K. Sakai, K. Kikuma, and K. Kurokawa. Study of the Relationship Between Peer-to-peer Systems and IP Multicasting. *IEEE Communications Magazine*, 41(1):80–84, January 2003.

[Var02] U. Varshney. Multicast Over Wireless Networks. *Communications of the ACM*, 45(12):31–37, December 2002.

[VC04] R. Vida and L. Costa (Editors). RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6, June 2004. URL reference: http://www.ietf.org/rfc/rfc3810.txt.

[WC01] Y. Wang and W. Chen. Supporting IP Multicast for Mobile Hosts. *Mobile Networks and Applications*, Volume 6(Number 1):57–66, January 2001.

[WCB04] Y. Wei, S. Chandra, and S. Bhandarkar. A statistical Prediction-based Scheme for Energy-aware Multimedia Data Streaming. In *Proceedings IEEE WCNC*, pages 2053–2057, Atlanta, USA, March 2004.

[WPD88] D. Waitzman, C. Partridge, and S. Deering. RFC 1075 Distance Vector Routing Multicast Protocol (DVMRP), November 1988. URL reference: http://www.ietf.org/rfc/rfc1075.txt.

[WWLŞ05] E. Wu, S. Woon, J. Lai, and Y A. Şekercioğlu. IPv6Suite: A Simulation Tool for Modeling Protocols of the Next Generation Internet. In *Proceedings of the Third International Conference on Information Technology: Research and Education (ITRE 2005)*, pages 434– 438, Taipei, Taiwan, June 2005.

[ZSZ05] H. Zhang, B. Shen, and B. Zhang. Mobile IPv6 Multicast with Dynamic Multicast Agent Internet Draft – work in progress, May 2005. URL Reference: http://www.ietf.org/internet-drafts/draft-zhang-mipshop-multicast-dma.t%xt.