Internet Research Task Force (IRTF)
Request for Comments: 5757
Category: Informational
ISSN: 2070-1721
February 2010

T. Schmidt
HAW Hamburg
M. Waehlisch
link-lab
G. Fairhurst
University of Aberdeen

Multicast Mobility in Mobile IP Version 6 (MIPv6): Problem Statement and Brief Survey

Abstract

This document discusses current mobility extensions to IP-layer multicast. It describes problems arising from mobile group communication in general, the case of multicast listener mobility, and problems for mobile senders using Any Source Multicast and Source-Specific Multicast. Characteristic aspects of multicast routing and deployment issues for fixed IPv6 networks are summarized. Specific properties and interplays with the underlying network access are surveyed with respect to the relevant technologies in the wireless domain. It outlines the principal approaches to multicast mobility, together with a comprehensive exploration of the mobile multicast problem and solution space. This document concludes with a conceptual road map for initial steps in standardization for use by future mobile multicast protocol designers. This document is a product of the IP Mobility Optimizations (MobOpts) Research Group.

Status of This Memo

Table of Contents

1. Introduction and Motivation

Group communication forms an integral building block of a wide variety of applications, ranging from content broadcasting and streaming, voice and video conferencing, collaborative environments and massive multiplayer gaming, up to the self-organization of distributed systems, services, or autonomous networks. Network-layer multicast support will be needed whenever globally distributed, scalable, serverless, or instantaneous communication is required.

The early idea of Internet multicasting [1] soon led to a wide adoption of Deering's host group model [2]. Broadband media delivery is emerging as a typical mass scenario that demands scalability and bandwidth efficiency from multicast routing. Although multicast mobility has been a concern for about ten years [3] and has led to numerous proposals, there is as yet no generally accepted solution. Multicast network support will be of particular importance to mobile environments, where users commonly share frequency bands of limited capacity. Reception of "infotainment" streams may soon require wide deployment of mobile multicast services.

Mobility in IPv6 [4] is standardized in the Mobile IPv6 RFCs [5][6], and it addresses the scenario of network-layer changes while moving between wireless domains. MIPv6 [5] only roughly defines multicast mobility for Mobile Nodes (MNs) using a remote subscription approach or through bidirectional tunneling via the Home Agent (HA). Remote subscription suffers from slow handovers relying on multicast routing to adapt to handovers. Bidirectional tunneling introduces inefficient overhead and delay due to triangular forwarding, i.e., instead of traveling on shortest paths, packets are routed through the Home Agent. Therefore, these approaches have not been optimized for a large scale deployment. A mobile multicast service for a future Internet should provide "close-to-optimal" routing at predictable and limited cost, offering robustness combined with a service quality compliant to real-time media distribution.

Intricate multicast routing procedures are not easily extensible to satisfy the requirements for mobility. A client subscribed to a group while performing mobility handovers requires the multicast traffic to follow to its new location; a mobile source needs the entire delivery tree to comply with or to adapt to its changing position. Significant effort has already been invested in protocol designs for mobile multicast receivers; only limited work has been dedicated to multicast source mobility, which poses the more delicate problem [65].

In multimedia conference scenarios, games, or collaborative environments, each member commonly operates as a receiver and as a sender for multicast group communication. In addition, real-time communication such as conversational voice or video places severe temporal requirements on mobility protocols: Typical seamless handover scenarios are expected to limit disruptions or delay to less than 100 - 150 ms [7]. Jitter disturbances should not exceed 50 ms. Note that 100 ms is about the duration of a spoken syllable in real-time audio. This problem statement is intended to also be applicable to a range of other scenarios with a range of delivery requirements appropriate to the general Internet.

This document represents the consensus of the MobOpts Research Group. It has been reviewed by the Research Group members active in the specific area of work. In addition, this document has been comprehensively reviewed by multiple active contributors to the IETF MEXT, MBONED, and PIM Working Groups.

1.1. Document Scope

This document defines the problem scope for multicast mobility management, which may be elaborated in future work. It is subdivided to present the various challenges according to their originating aspects, and identifies existing proposals and major bibliographic references.

When considering multicast node mobility, the network layer is complemented by some wireless access technology. Two basic scenarios are of interest: single-hop mobility (shown in Figure 1.a) and multi-hop mobility (shown in Figure 1.b). Single-hop mobility is the focus of this document, which coincides with the perspective of MIPv6 [5]. The key issues of mobile multicast membership control and the interplay of mobile and multicast routing will be illustrated using this simple scenario.

Multi-hop network mobility is a subsidiary scenario. All major aspects are inherited from the single-hop problem, while additional complexity is incurred from traversing a mobile cloud. This may be solved by either encapsulation or flooding ([8] provides a general overview). Specific issues arising from (nested) tunneling or flooding, especially the preservation of address transparency, require treatment analogous to MIPv6.

```
                                       +------+           +------+
                                       |  MN  |  =====>   |  MN  |
                                       +------+           +------+
                                          |                  .
                                          |                  .
                                          |                  .
                                       +-------+          +-------+
                                       | LAR 1 |          | LAR 2 |
                                       +-------+          +-------+
                                                \        /
                                            ***  ***  ***  ***
                                           *   **   **   **   *
   +------+           +------+            *                    *
   |  MN  |  =====>   |  MN  |             *  Mobile Network  *
   +------+           +------+            *                    *
      |                  .                 *   **   **   **   *
      |                  .                  ***  ***  ***  ***
      |                  .                  |                 .
   +-------+          +-------+         +-------+          +-------+
   | AR 1  |          | AR 2  |         | AR 1  |  =====>  | AR 2  |
   +-------+          +-------+         +-------+          +-------+
       |                |                   |                |
       ***  ***  ***  ***                   ***  ***  ***  ***
      *   **   **   **   *                 *   **   **   **   *
     *                    *               *                    *
      *  Fixed Internet  *                 *  Fixed Internet  *
     *                    *               *                    *
      *   **   **   **   *                 *   **   **   **   *
       ***  ***  ***  ***                   ***  ***  ***  ***

     a) Single-Hop Mobility                  b) Multi-Hop Mobility
```

Figure 1: Mobility Scenarios - A Mobile Node (MN) Directly Attaching to Fixed Access Routers (ARs) or Attached via Local Access Routers (LARs)

2. Problem Description

2.1. General Issues

Multicast mobility is a generic term, which subsumes a collection of distinct functions. First, the multicast communication is divided into Any Source Multicast (ASM) [2] and Source-Specific Multicast (SSM) [9][10]. Second, the roles of senders and receivers are distinct and asymmetric. Both may individually be mobile. Their interaction is facilitated by a multicast routing protocol such as the Distance Vector Multicast Routing Protocol (DVMRP) [11], the

Protocol Independent Multicast - Sparse Mode / Source-Specific Multicast (PIM-SM/SSM) [12][13], the Bidirectional PIM [14], or the inter-domain multicast prefix advertisements via Multiprotocol Extensions for BGP-4 (MBGP) [15]. IPv6 clients interact using the multicast listener discovery protocol (MLD and MLDv2) [16][17].

Any solution for multicast mobility needs to take all of these functional blocks into account. It should enable seamless continuity of multicast sessions when moving from one IPv6 subnet to another. It is desired to preserve the multicast nature of packet distribution and approximate optimal routing. It should support per-flow handover for multicast traffic because the properties and designations of flows can be distinct. Such distinctions may result from differing Quality-of-Service (QoS) / real-time requirements, but may also be caused by network conditions that may differ for different groups.

The host group model extends the capability of the network-layer unicast service. In common with the architecture of fixed networks, multicast mobility management should transparently utilize or smoothly extend the unicast functions of MIPv6 [5], its security extensions [6][18], its expediting schemes FMIPv6 [19] and Hierarchical Mobile IPv6 Environment (HMIPv6) [20], its context transfer protocols [21], its multihoming capabilities [22][23], emerging protocols like PMIPv6 [62], or future developments. From the perspective of an integrated mobility architecture, it is desirable to avoid multicast-specific as well as unicast-restricted solutions, whenever general approaches can be derived that can jointly support unicast and multicast.

Multicast routing dynamically adapts to the network topology at the locations of the sender(s) and receiver(s) participating in a multicast session, which then may change under mobility. However, depending on the topology and the protocol in use, current multicast routing protocols may require a time close to seconds to converge following a change in receiver or sender location. This is far too slow to support seamless handovers for interactive or real-time media sessions. The actual temporal behavior strongly depends on the multicast routing protocol in use, the configuration of routers, and on the geometry of the current distribution tree. A mobility scheme that readjusts routing, i.e., partially changes or fully reconstructs a multicast tree, is forced to comply with the time scale for protocol convergence. Specifically, it needs to consider a possible rapid movement of the mobile node, as this may occur at much higher rates than common protocol state updates.

The mobility of hosts using IP multicast can impact the service presented to the higher-layer protocols. IP-layer multicast packet distribution is an unreliable service that is bound to a connectionless transport service. Where applications are sensitive to packet loss or jitter, countermeasures need to be performed (loss recovery, content recoding, concealment, etc.) by the multicast transport or application. Mobile multicast handovers should not introduce significant additional packet drops. Due to statelessness, the bi-casting of multicast flows does not cause degradations at the transport layer, and applications should implement mechanisms to detect and correctly respond to duplicate datagrams. Nevertheless, individual application programs may not be robust with respect to repeated reception of duplicate streams.

IP multicast applications can be designed to adapt the multicast stream to prevailing network conditions (adapting the sending rate to the level of congestion, adaptive tuning of clients in response to measured delay, dynamic suppression of feedback messages, etc.). An adaptive application may also use more than one multicast group (e.g., layered multicast in which a client selects a set of multicast groups based on perceived available network capacity). A mobility handover may temporarily disrupt the operation of these higher-layer functions. The handover can invalidate assumptions about the forwarding path (e.g., acceptable delivery rate, round-trip delay), which could impact an application and level of network traffic. Such effects need to be considered in the design of multicast applications and in the design of network-layer mobility. Specifically, mobility mechanisms need to be robust to transient packet loss that may result from invalid path expectations following a handover of an MN to a different network.

Group addresses, in general, are location transparent, even though they may be scoped and methods can embed unicast prefixes or Rendezvous Point addresses [24]. The addresses of sources contributing to a multicast session are interpreted by the routing infrastructure and by receiver applications, which frequently are aware of source addresses. Multicast therefore inherits the mobility address duality problem of MIPv6 for source addresses: addresses being a logical node identifier, i.e., the home address (HoA) on the one hand, and a topological locator, the care-of address (CoA), on the other. At the network layer, the elements that comprise the delivery tree, i.e., multicast senders, forwarders, and receivers, need to carefully account for address duality issues, e.g., by using binding caches, extended multicast states, or signaling.

Multicast sources, in general, operate decoupled from their receivers in the following sense: a multicast source sends packets to a group of receivers that are unknown at the network layer and thus operates without a feedback channel. It neither has means to inquire about the properties of its delivery trees, nor the ability to learn about the network-layer state of its receivers. In the event of an inter-tree handover, a mobile multicast source therefore is vulnerable to losing connectivity to receivers without noticing. (Appendix A describes implicit source notification approaches). Applying a MIPv6 mobility binding update or return routability procedure will similarly break the semantic of a receiver group remaining unidentified by the source and thus cannot be applied in unicast analogy.

Despite the complexity of the requirements, multicast mobility management should seek lightweight solutions with easy deployment. Realistic, sample deployment scenarios and architectures should be provided in future solution documents.

2.2. Multicast Listener Mobility

2.2.1. Node and Application Perspective

A mobile multicast listener entering a new IP subnet requires multicast reception following a handover in real-time. This needs to transfer the multicast membership context from its old to its new point of attachment. This can either be achieved by (re-)establishing a tunnel or by transferring the MLD Listening State information of the MN’s moving interface(s) to the new upstream router(s). In the latter case, it may encounter any one of the following conditions:

- o In the simplest scenario, packets of some, or all, of the subscribed groups of the mobile node are already received by one or several other group members in the new network, and thus multicast streams natively flow after the MN arrives at the new network.

- o The requested multicast service may be supported and enabled in the visited network, but the multicast groups under subscription may not be forwarded to it, e.g., groups may be scoped or administratively prohibited. This means that current distribution trees for the desired groups may only be re-joined at a (possibly large) routing distance.

- o The new network may not be multicast-enabled or the specific multicast service may be unavailable, e.g., unsupported or prohibited. This means that current distribution trees for the desired groups need to be re-joined at a large routing distance by (re-)establishing a tunnel to a multicast-enabled network node.

The problem of achieving seamless multicast listener handovers is thus threefold:

- o Ensure multicast reception, even in visited networks, without appropriate multicast support.

- o Minimize multicast forwarding delay to provide seamless and fast handovers for real-time services. Dependent on Layer 2 (L2) and Layer 3 (L3) handover performance, the time available for multicast mobility operations is typically bound by the total handover time left after IPv6 connectivity is regained. In real-time scenarios, this may be significantly less than 100 ms.

- o Minimize packet loss and reordering that result from multicast handover management.

Moreover, in many wireless regimes, it is also desirable to minimize multicast-related signaling to preserve the limited resources of battery-powered mobile devices and the constrained transmission capacities of the networks. This may lead to a desire to restrict MLD queries towards the MN. Multihomed MNs may ensure smooth handoffs by using a "make-before-break" approach, which requires a per-interface subscription, facilitated by an MLD JOIN operating on a pre-selected IPv6 interface.

Encapsulation on the path between the upstream router and the receiver may result in MTU size conflicts, since path-MTU discovery is often not supported for multicast and can reduce scalability in networks with many different MTU sizes or introduce potential denial-of-service vulnerabilities (since the originating addresses of ICMPv6 messages cannot be verified for multicast). In the absence of fragmentation at tunnel entry points, this may prevent the group from being forwarded to the destination.

2.2.2. Network Perspective

The infrastructure providing multicast services is required to keep traffic following the MN without compromising network functionality. Mobility solutions thus have to face some immediate problems:

- o Realize native multicast forwarding, and where applicable, conserve network resources and utilize link-layer multipoint distribution to avoid data redundancy.

- o Activate link-multipoint services, even if the MN performs only a L2/vertical handover.

- o Ensure routing convergence, even when the MN moves rapidly and performs handovers at a high frequency.

- o Avoid avalanche problems and stream multiplication (n-casting), which potentially result from replicated tunnel initiation or redundant forwarding at network nodes.

There are additional implications for the infrastructure: In changing its point of attachment, an exclusive mobile receiver may initiate forwarding of a group in the new network and termination of a group distribution service in the previous network. Mobility management may impact multicast routing by, e.g., erroneous subscriptions following predictive handover operations, or slow traffic termination at leaf nodes resulting from MLD query timeouts, or by departure of the MN from a previous network without leaving the subscribed groups. Finally, packet duplication and reordering may follow a change of topology.

2.3. Multicast Source Mobility

2.3.1. Any Source Multicast Mobility

A node submitting data to an ASM group either forms the root of a source-specific shortest path tree (SPT), distributing data towards a rendezvous point (RP) or receivers, or it forwards data directly down a shared tree, e.g., via encapsulated PIM Register messages, or using bidirectional PIM routing. Native forwarding along source-specific delivery trees will be bound to the source’s topological network address, due to reverse path forwarding (RPF) checks. A mobile multicast source moving to a new subnetwork is only able to either inject data into a previously established delivery tree, which may be a rendezvous-point-based shared tree, or to (re-)initiate the construction of a multicast distribution tree for its new network location. In the latter case, the mobile sender will have to proceed without knowing whether the new tree has regained ability to forward traffic to the group, due to the decoupling of sender and receivers.

A mobile multicast source must therefore provide address transparency at two layers: To comply with RPF checks, it has to use an address within the source field of the IPv6 basic header, which is in topological agreement with the employed multicast distribution tree. For application transparency, the logical node identifier, commonly the HoA, must be presented as the packet source address to the transport layer at the receiver side.

The address transparency and temporal handover constraints pose major problems for route-optimizing mobility solutions. Additional issues arise from possible packet loss and from multicast scoping. A mobile source away from home must respect scoping restrictions that arise from its home and its visited location [5].

Intra-domain multicast routing may allow the use of shared trees that can reduce mobility-related complexity. A static rendezvous point may allow a mobile source to continuously send data to the group by encapsulating packets to the RP with its previous topologically correct or home source address. Intra-domain mobility is transparently provided by bidirectional shared domain-spanning trees, when using bidirectional PIM, eliminating the need for tunneling to the corresponding RP (in contrast to IPv4, IPv6 ASM multicast groups are associated with a specific RP/RPs).

Issues arise in inter-domain multicast, whenever notification of source addresses is required between distributed instances of shared trees. A new CoA acquired after a mobility handover will necessarily be subject to inter-domain record exchange. In the presence of an embedded rendezvous point address [24], e.g., the primary rendezvous point for inter-domain PIM-SM will be globally appointed, and a newly attached mobile source can contact the RP without prior signaling (like a new source) and transmit data in the PIM register tunnel. Multicast route optimization (e.g., PIM "shortcuts") will require multicast routing protocol operations equivalent to serving a new source.

2.3.2. Source-Specific Multicast Mobility

Source-Specific Multicast has been designed for multicast senders with static source addresses. The source addresses in a client subscription to an SSM group is directly used to route identification. Any SSM subscriber is thus forced to know the topological address of the contributor to the group it wishes to join. The SSM source identification becomes invalid when the topological source address changes under mobility. Hence, client implementations of SSM source filtering must be MIPv6 aware in the sense that a logical source identifier (HoA) is correctly mapped to its current topological correspondent (CoA).

As a consequence, source mobility for SSM requires a conceptual treatment beyond the problem scope of mobile ASM. A listener subscribes to an (S,G) channel membership and routers establish an (S,G)-state shortest path tree rooted at source S; therefore, any change of source addresses under mobility requires state updates at all routers on the upstream path and at all receivers in the group. On source handover, a new SPT needs to be established that will share paths with the previous SPT, e.g., at the receiver side. As the principle of multicast decoupling of a sender from its receivers holds for SSM, the client updates needed for switching trees become a severe burden.

An SSM listener may subscribe to or exclude any specific multicast source and thereby wants to rely on the topological correctness of network operations. The SSM design permits trust in equivalence to the correctness of unicast routing tables. Any SSM mobility solution should preserve this degree of confidence. Binding updates for SSM sources thus should have to prove address correctness in the unicast routing sense, which is equivalent to binding update security with a correspondent node in MIPv6 [5].

The above methods could add significant complexity to a solution for robust SSM mobility, which needs to converge to optimal routes and, for efficiency, is desired to avoid data encapsulation. Like ASM, handover management is a time-critical operation. The routing distance between subsequent points of attachment, the "step size" of the mobile from previous to next designated router, may serve as an appropriate measure of complexity [25][26].

Finally, Source-Specific Multicast has been designed as a lightweight approach to group communication. In adding mobility management, it is desirable to preserve the leanness of SSM by minimizing additional signaling overhead.

2.4. Deployment Issues

IP multicast deployment, in general, has been slow over the past 15 years, even though all major router vendors and operating systems offer implementations that support multicast [27]. While many (walled) domains or enterprise networks operate point-to-multipoint services, IP multicast roll-out is currently limited in public inter-domain scenarios [28]. A dispute arose on the appropriate layer, where group communication service should reside, and the focus of the research community turned towards application-layer multicast. This debate on "efficiency versus deployment complexity" now overlaps the mobile multicast domain [29]. Garyfalos and Almeroth [30] derived from fairly generic principles that when mobility is introduced, the performance gap between IP- and application-layer multicast widens in different metrics up to a factor of four.

Facing deployment complexity, it is desirable that any solution for mobile multicast does not change the routing protocols. Mobility management in such a deployment-friendly scheme should preferably be handled at edge nodes, preserving a mobility-agnostic routing infrastructure. Future research needs to search for such simple, infrastructure-transparent solutions, even though there are reasonable doubts as to whether this can be achieved in all cases.

Nevertheless, multicast services in mobile environments may soon become indispensable, when multimedia distribution services such as Digital Video Broadcasting for Handhelds (DVB-H) [31][32] or IPTV develop a strong business case for portable IP-based devices. As IP mobility becomes an important service and as efficient link utilization is of a larger impact in costly radio environments, the evolution of multicast protocols will naturally follow mobility constraints.

3. Characteristics of Multicast Routing Trees under Mobility

Multicast distribution trees have been studied from a focus of network efficiency. Grounded on empirical observations, Chuang and Sirbu [33] proposed a scaling power-law for the total number of links in a multicast shortest path tree with m receivers (proportional to m^k). The authors consistently identified the scale factor to attain the independent constant k = 0.8. The validity of such universal, heavy-tailed distribution suggests that multicast shortest path trees are of self-similar nature with many nodes of small, but few of higher degrees. Trees consequently would be shaped tall rather than wide.

Subsequent empirical and analytical work [34][35] debated the applicability of the Chuang and Sirbu scaling law. Van Mieghem et al. [34] proved that the proposed power law cannot hold for an increasing Internet or very large multicast groups, but is indeed applicable for moderate receiver numbers and the current Internet size of N = 10^5 core nodes. Investigating self-similarity, Janic and Van Mieghem [36] semi-empirically substantiated that multicast shortest path trees in the Internet can be modeled with reasonable accuracy by uniform recursive trees (URTs) [37], provided m remains small compared to N.

The mobility perspective on shortest path trees focuses on their alteration, i.e., the degree of topological changes induced by movement. For receivers, and more interestingly for sources, this may serve as a characteristic measure of the routing complexity. Mobile listeners moving to neighboring networks will only alter tree branches extending over a few hops. Source-specific multicast trees subsequently generated from source handover steps are not independent, but highly correlated. They most likely branch to identical receivers at one or several intersection points. By the self-similar nature, the persistent sub-trees (of previous and next distribution tree), rooted at any such intersection point, exhibit again the scaling law behavior, are tall-shaped with nodes of mainly low degree and thus likely to coincide. Tree alterations under mobility have been studied in [26], both analytically and by simulations. It was found that even in large networks and for moderate receiver numbers more than 80% of the multicast router states remain invariant under a source handover.

4. Link-Layer Aspects

4.1. General Background

Scalable group data distribution has the highest potential in edge networks, where large numbers of end systems reside. Consequently, it is not surprising that most LAN network access technologies natively support point-to-multipoint or multicast services. Wireless access technologies inherently support broadcast/multicast at L2 and operate on a shared medium with limited frequency and bandwidth.

Several aspects need consideration: First, dissimilar network access radio technologies cause distinct group traffic transmissions. There are:

- o connection-less link services of a broadcast type, which mostly are bound to limited reliability;
- o connection-oriented link services of a point-to-multipoint type, which require more complex control and frequently exhibit reduced efficiency;
- o connection-oriented link services of a broadcast type, which are restricted to unidirectional data transmission.

In addition, multicast may be distributed via multiple point-to-point unicast links without the use of a dedicated multipoint radio channel. A fundamental difference between unicast and group transmission arises from power management. Some radio technologies adjust transmit power to be as small as possible based on link-layer feedback from the receiver, which is not done in multipoint mode. They consequently incur a "multicast tax", making multicast less efficient than unicast unless the number of receivers is larger than some threshold.

Second, point-to-multipoint service activation at the network access layer requires a mapping mechanism from network-layer requests. This function is commonly achieved by L3 awareness, i.e., IGMP/MLD snooping [70] or proxy [38], which occasionally is complemented by Multicast VLAN Registration (MVR). MVR allows sharing of a single multicast IEEE 802.1Q Virtual LAN in the network, while subscribers remain in separate VLANs. This L2 separation of multicast and unicast traffic can be employed as a workaround for point-to-point link models to establish a common multicast link.

Third, an address mapping between the layers is needed for common group identification. Address resolution schemes depend on framing details for the technologies in use, but commonly cause a significant address overlap at the lower layer (i.e., more than one IP multicast group address is sent using the same L2 address).

4.2. Multicast for Specific Technologies

4.2.1. 802.11 WLAN

IEEE 802.11 Wireless Local Area Network (WLAN) is a broadcast network of Ethernet type. This inherits multicast address mapping concepts from 802.3. In infrastructure mode, an access point operates as a repeater, only bridging data between the Base (BSS) and the Extended Service Set (ESS). A mobile node submits multicast data to an access point in point-to-point acknowledged unicast mode (when the ToDS bit is set). An access point receiving multicast data from an MN simply repeats multicast frames to the BSS and propagates them to the ESS as unacknowledged broadcast. Multicast frames received from the ESS receive similar treatment.

Multicast frame delivery has the following characteristics:

- o As an unacknowledged service, it offers limited reliability. The loss of frames (and hence packets) arises from interference, collision, or time-varying channel properties.

- o Data distribution may be delayed, as unicast power saving synchronization via Traffic Indication Messages (TIM) does not operate in multicast mode. Access points buffer multicast packets while waiting for a larger Delivery TIM (DTIM) interval, whenever stations use the power saving mode.

- o Multipoint data may cause congestion, because the distribution system floods multicast, without further control. All access points of the same subnet replicate multicast frames.

To limit or prevent the latter, many vendors have implemented a configurable rate limit for forwarding multicast packets. Additionally, an IGMP/MLD snooping or proxy may be active at the bridging layer between the BSS and the ESS or at switches interconnecting access points.

4.2.2. 802.16 WIMAX

IEEE 802.16 Worldwide Interoperability for Microwave Access (WIMAX) combines a family of connection-oriented radio transmission services that can operate in single-hop point-to-multipoint (PMP) or in mesh mode. The latter does not support multipoint transmission and currently has no deployment. PMP operates between Base and Subscriber Stations in distinguished, unidirectional channels. The channel assignment is controlled by the Base Station, which assigns channel IDs (CIDs) within service flows to the Subscriber Stations. Service flows may provide an optional Automatic Repeat Request (ARQ) to improve reliability and may operate in point-to-point or point-to-multipoint (restricted to downlink and without ARQ) mode.

A WIMAX Base Station operates as a full-duplex L2 switch, with switching based on CIDs. Two IPv6 link models for mobile access scenarios exist: A shared IPv6 prefix for IP over Ethernet Circuit Switched (CS) [39] provides Media Access Control (MAC) separation within a shared prefix. A second, point-to-point link model [40] is recommended in the IPv6 Convergence Sublayer [41], which treats each connection to a mobile node as a single link. The point-to-point link model conflicts with a consistent group distribution at the IP layer when using a shared medium (cf. Section 4.1 for MVR as a workaround).

To invoke a multipoint data channel, the base station assigns a common CID to all Subscriber Stations in the group. An IPv6 multicast address mapping to these 16-bit IDs is proposed by copying either the 4 lowest bits, while sustaining the scope field, or by utilizing the 8 lowest bits derived from Multicast on Ethernet CS [42]. For selecting group members, a Base Station may implement IGMP/MLD snooping or proxy as foreseen in 802.16e-2005 [43].

A Subscriber Station multicasts IP packets to a Base Station as a point-to-point unicast stream. When the IPv6 CS is used, these are forwarded to the upstream access router. The access router (or the Base Station for IP over Ethernet CS) may send downstream multicast packets by feeding them to the multicast service channel. On reception, a Subscriber Station cannot distinguish multicast from unicast streams at the link layer.

Multicast services have the following characteristics:

- Multicast CIDs are unidirectional and available only in the downlink direction. Thus, a native broadcast-type forwarding model is not available.

- The mapping of multicast addresses to CIDs needs standardization, since different entities (Access Router, Base Station) may have to perform the mapping.

- CID collisions for different multicast groups may occur due to the short ID space. This can result in several point-to-multipoint groups sharing the same CID, reducing the ability of a receiver to filter unwanted L2 traffic.

- The point-to-point link model for mobile access contradicts a consistent mapping of IP-layer multicast onto 802.16 point-to-multipoint services.

- Multipoint channels cannot operate ARQ service and thus experience a reduced reliability.

4.2.3. 3GPP/3GPP2

The 3rd Generation Partnership Project (3GPP) System architecture spans a circuit switched (CS) and a packet-switched (PS) domain, the latter General Packet Radio Services (GPRS) incorporates the IP Multimedia Subsystem (IMS) [44]. The 3GPP PS is connection-oriented and based on the concept of Packet Data Protocol (PDP) contexts. PDPs define point-to-point links between the Mobile Terminal and the Gateway GPRS Support Node (GGSN). Internet service types are PPP, IPv4, and IPv6, where the recommendation for IPv6 address assignment associates a prefix to each (primary) PDP context [45].

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

The 3GPP MBMS has the following characteristics:

- There is no immediate Layer 2 source-to-destination transition, resulting in transit of all multicast traffic at the GGSN.

- As GGSNs commonly are regional, distant entities, triangular routing and encapsulation may cause a significant degradation of efficiency.

In 3GPP2, the MBMS has been extended to the Broadcast and Multicast Service (BCMCS) [46], which on the routing layer operates very similar to MBMS. In both 3GPP and 3GPP2, multicast can be sent using either point-to-point (PTP) or point-to-multipoint (PTM) tunnels, and there is support for switching between PTP and PTM. PTM uses a unidirectional common channel, operating in unacknowledged mode without adjustment of power levels and no reporting on lost packets.

4.2.4. DVB-H / DVB-IPDC

Digital Video Broadcasting for Handhelds (DVB-H) is a unidirectional physical layer broadcasting specification for the efficient delivery of broadband and IP-encapsulated data streams, and is published as an ETSI standard [47] (see http://www.dvb-h.org). This uses multiprotocol encapsulation (MPE) to transport IP packets over an MPEG-2 Transport Stream (TS) with link forward error correction (FEC). Each stream is identified by a 13-bit TS ID (PID), which together with a multiplex service ID, is associated with IPv4 or IPv6 addresses [48] and used for selective traffic filtering at receivers. Upstream channels may complement DVB-H using other transmission technologies. The IP Datacast Service, DVB-IPDC [31], specifies a set of applications that can use the DVB-H transmission network.

Multicast distribution services are defined by a mapping of groups onto appropriate PIDs, which is managed at the IP Encapsulator [49]. To increase flexibility and avoid collisions, this address resolution is facilitated by dynamic tables, provided within the self-contained MPEG-2 TS. Mobility is supported in the sense that changes of cell ID, network ID, or Transport Stream ID are foreseen [50]. A multicast receiver thus needs to relocate the multicast services to which it is subscribed during the synchronization phase, and update its service filters. Its handover decision may depend on service availability. An active service subscription (multicast join) requires initiation at the IP Encapsulator / DVB-H Gateway, which cannot be signaled in a pure DVB-H network.

4.2.5. TV Broadcast and Satellite Networks

IP multicast may be enabled in TV broadcast networks, including those specified by DVB, the Advanced Television Systems Committee (ATSC), and related standards [49]. These standards are also used for one- and two-way satellite IP services. Networks based on the MPEG-2 Transport Stream may support either the multiprotocol encapsulation (MPE) or the unidirectional lightweight encapsulation (ULE) [51]. The second generation DVB standards allow the Transport Stream to be replaced with a Generic Stream, using the Generic Stream Encapsulation (GSE) [52]. These encapsulation formats all support multicast operation.

In MPEG-2 transmission networks, multicast distribution services are defined by a mapping of groups onto appropriate PIDs, which is managed at the IP Encapsulator [49]. The addressing issues resemble those for DVB-H (Section 4.2.4) [48]. The issues for using GSE resemble those for ULE (except the PID is not available as a mechanism for filtering traffic). Networks that provide bidirectional connectivity may allow active service subscription (multicast join) to initiate forwarding from the upstream IP Encapsulator / gateway. Some kind of filtering can be achieved using the Input Stream Identifier (ISI) field.

4.3. Vertical Multicast Handovers

A mobile multicast node may change its point of Layer 2 attachment within homogeneous access technologies (horizontal handover) or between heterogeneous links (vertical handover). In either case, a Layer 3 network change may or may not take place, but multicast-aware links always need information about group traffic demands. Consequently, a dedicated context transfer of multicast subscriptions is required at the network access. Such Media Independent Handover (MIH) is addressed in IEEE 802.21 [53], but is relevant also beyond IEEE protocols. Mobility services transport for MIH are required as an abstraction for Layer 2 multicast service transfer in an Internet context [54] and are specified in [55].

MIH needs to assist in more than service discovery: There is a need for complex, media-dependent multicast adaptation, a possible absence of MLD signaling in L2-only transfers, and requirements originating from predictive handovers. A multicast mobility services transport needs to be sufficiently comprehensive and abstract to initiate a seamless multicast handoff at network access.

Functions required for MIH include:

- Service discovery.
- Service context transformation.
- Service context transfer.
- Service invocation.

5. Solutions

5.1. General Approaches

Three approaches to mobile multicast are common [56]:

- Bidirectional Tunneling, in which the mobile node tunnels all multicast data via its home agent. This fundamental multicast solution hides all movement and results in static multicast trees. It may be employed transparently by mobile multicast listeners and sources, at the cost of triangular routing and possibly significant performance degradation from widely spanned data tunnels.

- o Remote Subscription forces the mobile node to re-initiate multicast distribution following handover, e.g., by submitting an MLD listener report to the subnet where a receiver attaches. This approach of tree discontinuation relies on multicast dynamics to adapt to network changes. It not only results in significant service disruption but leads to mobility-driven changes of source addresses, and thus cannot support session persistence under multicast source mobility.

- o Agent-based solutions attempt to balance between the previous two mechanisms. Static agents typically act as local tunneling proxies, allowing for some inter-agent handover when the mobile node moves. A decelerated inter-tree handover, i.e., "tree walking", will be the outcome of agent-based multicast mobility, where some extra effort is needed to sustain session persistence through address transparency of mobile sources.

MIPv6 [5] introduces bidirectional tunneling as well as remote subscription as minimal standard solutions. Various publications suggest utilizing remote subscription for listener mobility only, while advising bidirectional tunneling as the solution for source mobility. Such an approach avoids the "tunnel convergence" or "avalanche" problem [56], which refers to the responsibility of the home agent to multiply and encapsulate packets for many receivers of the same group, even if they are located within the same subnetwork. However, this suffers from the drawback that multicast communication roles are not explicitly known at the network layer and may change unexpectedly.

None of the above approaches address SSM source mobility, except the use of bidirectional tunneling.

5.2. Solutions for Multicast Listener Mobility

5.2.1. Agent Assistance

There are proposals for agent-assisted handover for host-based mobility, which complement the unicast real-time mobility infrastructure of Fast MIPv6 (FMIPv6) [19], the M-FMIPv6 [57][58], and of Hierarchical MIPv6 (HMIPv6) [20], the M-HMIPv6 [59], and to context transfer [60], which have been thoroughly analyzed in [25][61].

All these solutions presume the context state was stored within a network node that is reachable before and after a move. But there could be cases were the MN is no longer in contact with the previous network, when at the new location. In this case, the network itself cannot assist in the context transfer. Such scenarios may occur when moving from one (walled) operator to another and will require a backwards compatible way to recover from loss of connectivity and context based on the node alone.

Network-based mobility management, Proxy MIPv6 (PMIPv6) [62], is multicast transparent in the sense that the MN experiences a point-to-point home link fixed at its (static) Local Mobility Anchor (LMA). This virtual home link is composed of a unicast tunnel between the LMA and the current Mobile Access Gateway (MAG), and a point-to-point link connecting the current MAG to the MN. A PMIPv6 domain thereby inherits MTU-size problems from spanning tunnels at the receiver site. Furthermore, two avalanche problem points can be identified: the LMA may be required to tunnel data to a large number of MAGs, while an MAG may be required to forward the same multicast stream to many MNs via individual point-to-point links [63]. Future optimizations and extensions to shared links preferably adapt native multicast distribution towards the edge network, possibly using a local routing option, including context transfer between access gateways to assist IP-mobility-agnostic MNs.

An approach based on dynamically negotiated inter-agent handovers is presented in [64]. Aside from IETF work, numerous publications present proposals for seamless multicast listener mobility, e.g., [65] provides a comprehensive overview of the work prior to 2004.

5.2.2. Multicast Encapsulation

Encapsulation of multicast data packets is an established method to shield mobility and to enable access to remotely located data services, e.g., streams from the home network. Applying generic packet tunneling in IPv6 [66] using a unicast point-to-point method will also allow multicast-agnostic domains to be transited, but does inherit the tunnel convergence problem and may result in traffic multiplication.

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

The tunnel entry point performing encapsulation should provide fragmentation of data packets to avoid issues resulting from MTU-size constraints within the network(s) supporting the tunnel(s).

5.2.3. Hybrid Architectures

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

An early hybrid architecture using reactively operating proxy-gateways located at the Internet edges was introduced by Garyfalos and Almeroth [30]. The authors presented an Intelligent Gateway Multicast as a bridge between mobility-aware native multicast management in access networks and mobility group distribution services in the Internet core, which may be operated on the network or application layer. The Hybrid Shared Tree approach [67] introduced a mobility-agnostic multicast backbone on the overlay.

Current work in the SAM RG is developing general architectural approaches for hybrid multicast solutions [68] and a common multicast API for a transparent access of hybrid multicast [69] that will require a detailed design in future work.

5.2.4. MLD Extensions

The default timer values and Robustness Variable specified in MLD [17] were not designed for the mobility context. This results in a slow reaction of the multicast-routing infrastructure (including L3-aware access devices [70]) following a client leave. This may be a disadvantage for wireless links, where performance may be improved by carefully tuning the Query Interval and other variables. Some vendors have optimized performance by implementing a listener node table at the access router that can eliminate the need for query timeouts when receiving leave messages (explicit receiver tracking).

An MN operating predictive handover, e.g., using FMIPv6, may accelerate multicast service termination when leaving the previous network by submitting an early Done message before handoff. MLD router querying will allow the multicast forwarding state to be restored in the case of an erroneous prediction (i.e., an anticipated move to a network that has not taken place). Backward context transfer may otherwise ensure a leave is signaled. A further optimization was introduced by Jelger and Noel [71] for the special case when the HA is a multicast router. A Done message received through a tunnel from the mobile end node (through a point-to-point link directly connecting the MN, in general), should not initiate standard MLD membership queries (with a subsequent timeout). Such explicit treatment of point-to-point links will reduce traffic and accelerate the control protocol. Explicit tracking will cause identical protocol behavior.

While away from home, an MN may wish to rely on a proxy or "standby" multicast membership service, optionally provided by an HA or proxy router. Such functions rely on the ability to restart fast packet forwarding; it may be desirable for the proxy router to remain part of the multicast delivery tree, even when transmission of group data is paused. To enable such proxy control, the authors in [71] propose an extension to MLD, introducing a Listener Hold message that is exchanged between the MN and the HA. This idea was developed in [59] to propose multicast router attendance control, allowing for a general deployment of group membership proxies. Some currently deployed IPTV solutions use such a mechanism in combination with a recent (video) frame buffer, to enable fast channel switching between several IPTV multicast flows (zapping).

5.3. Solutions for Multicast Source Mobility

5.3.1. Any Source Multicast Mobility Approaches

Solutions for multicast source mobility can be divided into three categories:

- o Statically Rooted Distribution Trees. These methods follow a shared tree approach. Romdhani et al. [72] proposed employing the Rendezvous Points of PIM-SM as mobility anchors. Mobile senders tunnel their data to these "Mobility-aware Rendezvous Points" (MRPs). When restricted to a single domain, this scheme is equivalent to bidirectional tunneling. Focusing on inter-domain mobile multicast, the authors designed a tunnel- or SSM-based backbone distribution of packets between MRPs.

- o Reconstruction of Distribution Trees. Several authors have proposed the construction of a completely new distribution tree after the movement of a mobile source and therefore have to compensate for the additional routing (tree-building) delay. M-HMIPv6 [59] tunnels data into a previously established tree rooted at mobility anchor points to compensate for the routing delay until a protocol-dependent timer expires. The Range-Based Mobile Multicast (RBMoM) protocol [73] introduces an additional Multicast Agent (MA) that advertises its service range. A mobile source registers with the closest MA and tunnels data through it. When moving out of the previous service range, it will perform MA discovery, a re-registration and continue data tunneling with a newly established Multicast Agent in its new current vicinity.

- o Tree Modification Schemes. In the case of DVMRP routing, Chang and Yen [74] propose an algorithm to extend the root of a given delivery tree for incorporating a new source location in ASM. The authors rely on a complex additional signaling protocol to fix DVMRP forwarding states and heal failures in the reverse path forwarding (RPF) checks.

5.3.2. Source-Specific Multicast Mobility Approaches

The shared tree approach of [72] has been extended to support SSM mobility by introducing the HoA address record to the Mobility-aware Rendezvous Points. The MRPs operate using extended multicast routing tables that simultaneously hold the HoA and CoA and thus can logically identify the appropriate distribution tree. Mobility thus may reintroduce the concept of rendezvous points to SSM routing.

Approaches for reconstructing SPTs in SSM rely on a client notification to establish new router state. They also need to preserve address transparency for the client. Thaler [75] proposed introducing a binding cache and providing source address transparency analogous to MIPv6 unicast communication. Initial session announcements and changes of source addresses are distributed periodically to clients via an additional multicast control tree rooted at the home agent. Source tree handovers are then activated on listener requests.

Jelger and Noel [76] suggest handover improvements employing anchor points within the source network, supporting continuous data reception during client-initiated handovers. Client updates are triggered out of band, e.g., by Source Demand Routing (SDR) / Session Announcement Protocol (SAP) [77]. Receiver-oriented tree construction in SSM thus remains unsynchronized with source handovers.

To address the synchronization problem at the routing layer, several proposals have focused on direct modification of the distribution trees. A recursive scheme may use loose unicast source routes with branch points, based on a multicast Hop-by-Hop protocol. Vida et al. [78] optimized SPT for a moving source on the path between the source and first branching point. O'Neill [79] suggested a scheme to overcome RPF check failures that originate from multicast source address changes with a rendezvous point scenario by introducing extended routing information, which accompanies data in a Hop-by-Hop option "RPF redirect" header. The Tree Morphing approach of Schmidt and Waehlisch [80] used source routing to extend the root of a previously established SPT, thereby injecting router state updates in a Hop-by-Hop option header. Using extended RPF checks, the elongated tree autonomously initiates shortcuts and smoothly reduces to a new SPT rooted at the relocated source. An enhanced version of this protocol abandoned the initial source routing and could be proved to comply with rapid source movement [81]. Lee et al. [82] introduced a state-update mechanism for reusing major parts of established multicast trees. The authors start from an initially established distribution state, centered at the mobile source’s home agent. A mobile source leaving its home network will signal a multicast forwarding state update on the path to its home agent and, subsequently, distribution states according to the mobile source’s new CoA along the previous distribution tree. Multicast data is then intended to flow natively using triangular routes via the elongation and an updated tree centered on the home agent. Based on Host Identity Protocol identifiers, Kovacshazi and Vida [83] introduce multicast routing states that remain independent of IP addresses. Drawing upon a similar scaling law argument, parts of these states may then be reused after source address changes.

6. Security Considerations

This document discusses multicast extensions to mobility. It does not define new methods or procedures. Security issues arise from source address binding updates, specifically in the case of source-specific multicast. Threats of hijacking unicast sessions will result from any solution jointly operating binding updates for unicast and multicast sessions.

Multicast protocols exhibit a risk of network-based traffic amplification. For example, an attacker may abuse mobility signaling to inject unwanted traffic into a previously established multicast distribution infrastructure. These threats are partially mitigated by reverse path forwarding checks by multicast routers. However, a multicast or mobility agent that explicitly replicates multicast streams, e.g., Home Agent that n-casts data, may be vulnerable to denial-of-service attacks. In addition to source authentication, a rate control of the replicator may be required to protect the agent and the downstream network.

Mobility protocols need to consider the implications and requirements for Authentication, Authorization, and Accounting (AAA). An MN may have been authorized to receive a specific multicast group when using one mobile network, but this may not be valid when attaching to a different network. In general, the AAA association for an MN may change between attachments, or may be individually chosen prior to network (re-)association. The most appropriate network path may be one that satisfies user preferences, e.g., to use/avoid a specific network, minimize monetary cost, etc., rather than one that only minimizes the routing cost. Consequently, AAA bindings may need to be considered when performing context transfer.

Admission control issues may arise when new CoA source addresses are introduced to SSM channels [84]. Due to lack of feedback, the admission [85] and binding updates [86] of mobile multicast sources require autonomously verifiable authentication. This can be achieved by, for instance, Cryptographically Generated Addresses (CGAs).

Modification to IETF protocols (e.g., routing, membership, session announcement, and control) as well as the introduction of new entities, e.g., multicast mobility agents, can introduce security vulnerabilities and require consideration of issues such as authentication of network entities, methods to mitigate denial of service (in terms of unwanted network traffic, unnecessary consumption of router/host resources and router/host state/buffers). Future solutions must therefore analyze and address the security implications of supporting mobile multicast.

7. Summary and Future Steps

This document is intended to provide a basis for the future design of mobile IPv6 multicast methods and protocols by:

- providing a structured overview of the problem space that multicast and mobility jointly generate at the IPv6 layer;

- referencing the implications and constraints arising from lower and upper layers and from deployment;

- briefly surveying conceptual ideas of currently available solutions;

- including a comprehensive bibliographic reference base.

It is recommended that future steps towards extending mobility services to multicast proceed to first solve the following problems:

1. Ensure seamless multicast reception during handovers, meeting the requirements of mobile IPv6 nodes and networks. Thereby addressing the problems of home subscription without n-tunnels, as well as native multicast reception in those visited networks, which offer a group communication service.

2. Integrate multicast listener support into unicast mobility management schemes and architectural entities to define a consistent mobility service architecture, providing equal support for unicast and multicast communication.

3. Provide basic multicast source mobility by designing address duality management at end nodes.

Appendix A. Implicit Source Notification Options

An IP multicast source transmits data to a group of receivers without requiring any explicit feedback from the group. Sources therefore are unaware at the network layer of whether any receivers have subscribed to the group, and unconditionally send multicast packets that propagate in the network to the first-hop router (often known in PIM as the designated router). There have been attempts to implicitly obtain information about the listening group members, e.g., extending an IGMP/MLD querier to inform the source of the existence of subscribed receivers. Multicast Source Notification of Interest Protocol (MSNIP) [87] was such a suggested method that allowed a multicast source to query the upstream designated router. However, this work did not progress within the IETF mboned working group and was terminated by the IETF.

Multicast sources may also be controlled at the session or transport layer using end-to-end control protocols. A majority of real-time applications employ the Real-time Transport Protocol (RTP) [88]. The accompanying control protocol, RTP Control Protocol (RTCP), allows receivers to report information about multicast group membership and associated performance data. In multicast, the RTCP reports are submitted to the same group and thus may be monitored by the source to monitor, manage and control multicast group operations. RFC 2326, the Real Time Streaming Protocol (RTSP), provides session layer control that may be used to control a multicast source. However, RTCP and RTSP information is intended for end-to-end control and is not necessarily visible at the network layer. Application designers may chose to implement any appropriate control plane for their multicast applications (e.g., reliable multicast transport protocols), and therefore a network-layer mobility mechanism must not assume the presence of a specific transport or session protocol.

Informative References

[1] Aguilar, L. "Datagram Routing for Internet Multicasting", In ACM SIGCOMM ’84 Communications Architectures and Protocols, pp. 58-63, ACM Press, June, 1984.

[2] Deering, S., "Host extensions for IP multicasting", STD 5, RFC 1112, August 1989.

[3] G. Xylomenos and G.C. Plyzos, "IP Multicast for Mobile Hosts", IEEE Communications Magazine, 35(1), pp. 54-58, January 1997.

[4] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[5] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[6] Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", RFC 4877, April 2007.

[7] ITU-T Recommendation, "G.114 - One-way transmission time", Telecommunication Union Standardization Sector, 05/2003.

[8] Akyildiz, I and Wang, X., "A Survey on Wireless Mesh Networks", IEEE Communications Magazine, 43(9), pp. 23-30, September 2005.

[9] Bhattacharyya, S., Ed., "An Overview of Source-Specific Multicast (SSM)", RFC 3569, July 2003.

[10] Holbrook, H. and B. Cain, "Source-Specific Multicast for IP", RFC 4607, August 2006.

[11] Waitzman, D., Partridge, C., and S. Deering, "Distance Vector Multicast Routing Protocol", RFC 1075, November 1988.

[12] Estrin, D., Farinacci, D., Helmy, A., Thaler, D., Deering, S., Handley, M., Jacobson, V., Liu, C., Sharma, P., and L. Wei, "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification", RFC 2362, June 1998.

[13] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, August 2006.

[14] Handley, M., Kouvelas, I., Speakman, T., and L. Vicisano, "Bidirectional Protocol Independent Multicast (BIDIR-PIM)", RFC 5015, October 2007.

[15] Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 4760, January 2007.

[16] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.

[17] Vida, R., Ed., and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

[18] Arkko, J., Vogt, C., and W. Haddad, "Enhanced Route Optimization for Mobile IPv6", RFC 4866, May 2007.

[19] Koodli, R., Ed., "Mobile IPv6 Fast Handovers", RFC 5568, July 2009.

[20] Soliman, H., Castelluccia, C., ElMalki, K., and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", RFC 5380, October 2008.

[21] Loughney, J., Ed., Nakhjiri, M., Perkins, C., and R. Koodli, "Context Transfer Protocol (CXTP)", RFC 4067, July 2005.

[22] Montavont, N., Wakikawa, R., Ernst, T., Ng, C., and K. Kuladinithi, "Analysis of Multihoming in Mobile IPv6", Work in Progress, May 2008.

[23] Narayanan, V., Thaler, D., Bagnulo, M., and H. Soliman, "IP Mobility and Multi-homing Interactions and Architectural Considerations", Work in Progress, July 2007.

[24] Savola, P. and B. Haberman, "Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address", RFC 3956, November 2004.

[25] Schmidt, T.C. and Waehlisch, M. "Predictive versus Reactive - Analysis of Handover Performance and Its Implications on IPv6 and Multicast Mobility", Telecommunication Systems, 30(1-3), pp. 123- 142, November 2005.

[26] Schmidt, T.C. and Waehlisch, M. "Morphing Distribution Trees - On the Evolution of Multicast States under Mobility and an Adaptive Routing Scheme for Mobile SSM Sources", Telecommunication Systems, 33(1-3), pp. 131-154, December 2006.

[27] Diot, C. et al. "Deployment Issues for the IP Multicast Service and Architecture", IEEE Network Magazine, spec. issue on Multicasting, 14(1), pp. 78-88, 2000.

[28] Eubanks, M. http://multicasttech.com/status/, 2008.

[29] Garyfalos, A, Almeroth, K. and Sanzgiri, K. "Deployment Complexity Versus Performance Efficiency in Mobile Multicast", Intern. Workshop on Broadband Wireless Multimedia: Algorithms, Architectures and Applications (BroadWiM), San Jose, California, USA, October 2004. Online: http://imj.ucsb.edu/papers/BROADWIM-04.pdf.

[30] Garyfalos, A, Almeroth, K. "A Flexible Overlay Architecture for Mobile IPv6 Multicast", IEEE Journ. on Selected Areas in Comm., 23(11), pp. 2194-2205, November 2005.

[31] "Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Set of Specifications for Phase 1", ETSI TS 102 468;

[32] ETSI TS 102 611, "Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Implementation Guidelines for Mobility)", European Standard (Telecommunications series), November 2004.

[33] Chuang, J. and Sirbu, M. "Pricing Multicast Communication: A Cost- Based Approach", Telecommunication Systems, 17(3), 281-297, 2001. Presented at the INET'98, Geneva, Switzerland, July 1998.

[34] Van Mieghem, P, Hooghiemstra, G, Hofstad, R. "On the Efficiency of Multicast", IEEE/ACM Trans. Netw., 9(6), pp. 719-732, Dec. 2001.

[35] Chalmers, R.C. and Almeroth, K.C, "On the topology of multicast trees", IEEE/ACM Trans. Netw., 11(1), 153-165, 2003.

[36] Janic, M. and Van Mieghem, P. "On properties of multicast routing trees", Int. J. Commun. Syst., 19(1), pp. 95-114, Feb. 2006.

[37] Van Mieghem, P. "Performance Analysis of Communication Networks and Systems", Cambridge University Press, 2006.

[38] Fenner, B., He, H., Haberman, B., and H. Sandick, "Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")", RFC 4605, August 2006.

[39] Jeon, H., Jeong, S., and M. Riegel, "Transmission of IP over Ethernet over IEEE 802.16 Networks", RFC 5692, October 2009.

[40] Shin, M-K., Ed., Han, Y-H., Kim, S-E., and D. Premec, "IPv6 Deployment Scenarios in 802.16 Networks", RFC 5181, May 2008.

[41] Patil, B., Xia, F., Sarikaya, B., Choi, JH., and S. Madanapalli, "Transmission of IPv6 via the IPv6 Convergence Sublayer over IEEE 802.16 Networks", RFC 5121, February 2008.

[42] Kim, S., Jin, J., Lee, S., and S. Lee, "Multicast Transport on IEEE 802.16 Networks", Work in Progress, July 2007.

[43] IEEE 802.16e-2005: IEEE Standard for Local and metropolitan area networks Part 16: "Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands", New York, February 2006.

[44] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; "IP Multimedia Subsystem (IMS)"; Stage 2, 3GPP TS 23.228, Rel. 5 ff, 2002 - 2007.

[45] Wasserman, M., Ed., "Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards", RFC 3314, September 2002.

[46] 3GPP2, www.3gpp2.org, "X.S0022-A, Broadcast and Multicast Service in cdma2000 Wireless IP Network, Rev. A.", http://www.3gpp2.org/Public_html/specs/tsgx.cfm, February 2007.

[47] ETSI EN 302 304, "Digital Video Broadcasting (DVB); Transmission System for Handheld Terminals (DVB-H)", European Standard (Telecommunications series), November 2004.

[48] Fairhurst, G. and M. Montpetit, "Address Resolution Mechanisms for IP Datagrams over MPEG-2 Networks", RFC 4947, July 2007.

[49] Montpetit, M.-J., Fairhurst, G., Clausen, H., Collini-Nocker, B., and H. Linder, "A Framework for Transmission of IP Datagrams over MPEG-2 Networks", RFC 4259, November 2005.

[50] Yang, X, Vare, J, Owens, T. "A Survey of Handover Algorithms in DVB-H", IEEE Comm. Surveys, 8(4), pp. 16-24, 2006.

[51] Fairhurst, G. and B. Collini-Nocker, "Unidirectional Lightweight Encapsulation (ULE) for Transmission of IP Datagrams over an MPEG-2 Transport Stream (TS)", RFC 4326, December 2005.

[52] Fairhurst, G. and B. Collini-Nocker, "Extension Formats for Unidirectional Lightweight Encapsulation (ULE) and the Generic Stream Encapsulation (GSE)", RFC 5163, April 2008.

[53] "Draft IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services", IEEE LAN/MAN Draft IEEE P802.21/D07.00, July 2007.

[54] Melia, T., Ed., "Mobility Services Transport: Problem Statement", RFC 5164, March 2008.

[55] Melia, T., Ed., Bajko, G., Das, S., Golmie, N., and JC. Zuniga, "IEEE 802.21 Mobility Services Framework Design (MSFD)", RFC 5677, December 2009.

[56] Janneteau, C, Tian, Y, Csaba, S. et al. "Comparison of Three Approaches Towards Mobile Multicast", IST Mobile Summit 2003, Aveiro, Portugal, 16-18 June 2003.

[57] Suh, K., Kwon, D.-H., Suh, Y.-J. and Y. Park, "Fast Multicast Protocol for Mobile IPv6 in the fast handovers environments", Work in Progress, January 2004.

[58] Xia, F. and B. Sarikaya, "FMIPv6 extensions for Multicast Handover", Work in Progress, March 2007.

[59] Schmidt, T. and M. Waehlisch, "Seamless Multicast Handover in a Hierarchical Mobile IPv6 Environment (M-HMIPv6)", Work in Progress, November 2005.

[60] Miloucheva, I. and K. Jonas, "Multicast Context Transfer in mobile IPv6", Work in Progress, June 2005.

[61] Leoleis, G, Prezerakos, G, Venieris, I, "Seamless multicast mobility support using fast MIPv6 extensions", Computer Comm., 29(18), pp. 3745-3765, 2006.

[62] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[63] Deng, H., Chen, G., Schmidt, T., Seite, P., and P. Yang, "Multicast Support Requirements for Proxy Mobile IPv6", Work in Progress, July 2009.

[64] Zhang, H., Chen, X., Guan, J., Shen, B., Liu, E., and S. Dawkins, "Mobile IPv6 Multicast with Dynamic Multicast Agent", Work in Progress, January 2007.

[65] Romdhani, I, Kellil, M, Lach, H.-Y. et. al. "IP Mobile Multicast: Challenges and Solutions", IEEE Comm. Surveys, 6(1), pp. 18-41, 2004.

[66] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

[67] Waehlisch, M., Schmidt, T.C. "Between Underlay and Overlay: On Deployable, Efficient, Mobility-agnostic Group Communication Services", Internet Research, 17(5), pp. 519-534, Emerald Insight, Bingley, UK, November 2007.

[68] J. Buford, "Hybrid Overlay Multicast Framework", Work in Progress, February 2008.

[69] Waehlisch, M., Schmidt, T., and S. Venaas, "A Common API for Transparent Hybrid Multicast", Work in Progress, October 2009.

[70] Christensen, M., Kimball, K., and F. Solensky, "Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches", RFC 4541, May 2006.

[71] Jelger, C, Noel, T. "Multicast for Mobile Hosts in IP Networks: Progress and Challenges", IEEE Wirel. Comm., 9(5), pp 58-64, Oct. 2002.

[72] Romdhani, I, Bettahar, H. and Bouabdallah, A. "Transparent handover for mobile multicast sources", in P. Lorenz and P. Dini, eds, Proceedings of the IEEE ICN’06, IEEE Press, 2006.

[73] Lin, C.R. et al. "Scalable Multicast Protocol in IP-Based Mobile Networks", Wireless Networks, 8 (1), pp. 27-36, January, 2002.

[74] Chang, R.-S. and Yen, Y.-S. "A Multicast Routing Protocol with Dynamic Tree Adjustment for Mobile IPv6", Journ. Information Science and Engineering, 20(6), pp. 1109-1124, 2004.

[75] Thaler, D. "Supporting Mobile SSM Sources for IPv6", Proceedings of ietf meeting, Dec. 2001.
URL: www.ietf.org/proceedings/01dec/slides/magma-2.pdf

[76] Jelger, C. and T. Noel, "Supporting Mobile SSM sources for IPv6 (MSSMSv6)",Work in Progress, January 2002.

[77] Handley, M., Perkins, C., and E. Whelan, "Session Announcement Protocol", RFC 2974, October 2000.

[78] Vida, R, Costa, L, Fdida, S. "M-HBH - Efficient Mobility Management in Multicast", Proc. of NGC ’02, pp. 105-112, ACM Press 2002.

[79] A. O’Neill "Mobility Management and IP Multicast", Work in Progress, July 2002.

[80] Schmidt, T. C. and Waehlisch, M. "Extending SSM to MIPv6 - Problems, Solutions and Improvements", Computational Methods in Science and Technology, 11(2), pp. 147-152. Selected Papers from TERENA Networking Conference, Poznan, May 2005.

[81] Schmidt, T.C., Waehlisch, M., and Wodarz, M. "Fast Adaptive Routing Supporting Mobile Senders in Source Specific Multicast", Telecommunication Systems, 43(1), pp. 95-108, 2009, http://dx.doi.org/10.1007/s11235-009-9200-y.

[82] Lee, H., Han, S. and Hong, J. "Efficient Mechanism for Source Mobility in Source Specific Multicast", in K. Kawahara and I. Chong, eds, "Proceedings of ICOIN2006", LNCS vol. 3961, pp. 82-91, Springer-Verlag, Berlin, Heidelberg, 2006.

[83] Kovacshazi, Z. and Vida, R. "Host Identity Specific Multicast", Third International Conference on Networking and Services ICNS, IEEE Press, pp. 1-1, June 2007.

[84] Kellil, M, Romdhani, I, Lach, H.-Y, Bouabdallah, A. and Bettahar, H. "Multicast Receiver and Sender Access Control and its Applicability to Mobile IP Environments: A Survey", IEEE Comm. Surveys & Tutorials, 7(2), pp. 46-70, 2005.

[85] Castellucia, C, Montenegro, G. "Securing Group Management in IPv6 with Cryptographically Based Addresses", Proc. 8th IEEE Int’l Symp. Comp. and Commun, Turkey, July 2003, pp. 588-93.

[86] Schmidt, T.C, Waehlisch, M., Christ, O., and Hege, G. "AuthoCast - a mobility-compliant protocol framework for multicast sender authentication", Security and Communication Networks, 1(6), pp. 495-509, 2008.

[87] Fenner, B., Holbrook, H., and I. Kouvelas, "Multicast Source Notification of Interest Protocol (MSNIP)", Work in Progress, November 2001.

[88] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, July 2003.

Acknowledgments

Work on exploring the problem space for mobile multicast has been pioneered by Greg Daley and Gopi Kurup within their early document "Requirements for Mobile Multicast Clients".

Since then, many people have actively discussed the different issues and contributed to the enhancement of this memo. The authors would like to thank (in alphabetical order) Kevin C. Almeroth, Lachlan Andrew, Jari Arkko, Cedric Baudoin, Hans L. Cycon, Hui Deng, Marshall Eubanks, Zhigang Huang, Christophe Jelger, Andrei Gutov, Rajeev Koodli, Mark Palkow, Craig Partridge, Imed Romdhani, Hesham Soliman, Dave Thaler, and last, but not least, very special thanks to Stig Venaas for his frequent and thorough advice.

Authors' Addresses

Thomas C. Schmidt
Dept. Informatik
Hamburg University of Applied Sciences,
Berliner Tor 7
D-20099 Hamburg, Germany
Phone: +49-40-42875-8157
EMail: schmidt@informatik.haw-hamburg.de

Matthias Waehlisch
link-lab
Hoenower Str. 35
D-10318 Berlin, Germany
EMail: mw@link-lab.net

Godred Fairhurst
School of Engineering,
University of Aberdeen,
Aberdeen, AB24 3UE, UK
EMail: gorry@erg.abdn.ac.uk