ISSN No. 0976-5697

Volume 2, No. 1, Jan-Feb 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

IP Mobile Multicast: Challenges, Solutions and Open Issues

Prof. Jayant N. Patil*
Computer Science Department
Symbiosis College
Pune, India
jayantpatil@symbiosiscollege.edu.in

Dr. Sagar Jambhorkar
Computer Science Department
Swami Ramanand Tirth Marathwada University
Nanded, India
sjambhorkar@yahoo.co.in

Abstract : This paper provides a comprehensive overview of multicast solutions to support Mobile Nodes (IPv4 and IPv6). The goal of this work is to analyze the challenges that IP multicast faces in the Mobile IP environment. This work discusses also open issues in current mobile multicast proposals.

Keywords. IP Mobile Multicast, IP Multicast, Mobile IPv4, and Mobile IPv6

I. INTRODUCTION

Today, the growth of the Internet and network technologies is accompanied by the multiplication of new applications. These bring with them not only new types of data such as video and audio, but also a new kind of users that need to work on the move. To do so, users need a new kind of network host that can move from one attachment point to another without the need to reconfigure it. Such host can be stationary or mobile. We call it a Mobile Node (MN). The MN can move from its home network to a visited or a foreign one without interrupting the ongoing application sessions. This phenomenon is called handover.

In the case of multiparty communications with IP multicast, the scenario of handover is particularly challenging. Every node in a multicast group should remain effectively in the group despite its mobility, so that it can continue to receive packets addressed to the group and send packets to the group. A Mobile Node can be just a simple receiver for a unique or multiple multicast groups. It may also exist another realistic scenario where it can be also a sender for one or different groups. Whatever the status of a mobile multicast receiver, its multicast membership latency should be minimized. Hence, the MN should have enough mechanisms to join quickly the multicast delivery tree. As we will see later, a MN can join a multicast group either via the local multicast router in the visited foreign network or via its Home Agent (HA) in the home network. These two approaches have different advantages and limitations that we will discuss in this paper. When the MN is a sender for a given multicast group, the handover transparency is the primary requirement to satisfy for multicast receivers. As a consequence, the MN should be always identified by its Home Address (HoA) independently of its current point of attachment.

Multicast involves sending messages to a restricted group of nodes and forms the basis for efficient implementation of multiparty applications on a network. Many protocols support efficient multicast by using a multicast tree. The main drawback of these protocols is that they are developed for multicast parties whose members are topologically stationary and they do not consider the extra requirements to support topologically mobile members. In addition, these multicast protocols often do not take into account the Quality of Service (QoS) required by applications. Additional mechanisms are then required to satisfy the QoS parameters between senders and mobile receivers. As it is difficult to satisfy multiple constraints simultaneously, the issue of incorporating QoS routing with various multiple routing protocols for mobile hosts is not yet solved. This subject is out of the scope of our paper.

In this paper, we present a comprehensive overview of multicast solutions to support Mobile Nodes (IPv4 and IPv6) and analyze the challenges that IP multicast faces in the Mobile IP environment. Our paper is organized as follows: in section 2, we present an overview of both the IETF Mobile IP protocols (IPv4 and IPv6) and the IP multicast model. In section 3, we focus on the challenges of supporting multicast for mobile hosts (receivers and senders) and other related problems. Section 4 outlines the requirements of multicast enhancements for MNs. Section 5 gives an overview of some selected approaches that support multicast in Mobile IP environment. We frame the discussion to these approaches because they enhance the Mobile IP protocol to support IP multicast. Section 6 compares qualitatively all the solutions described in the previous section. Finally we conclude with some open issues in section 7.

II. BACKGROUND

As mobile hosts move from one subnet to another, the handover frequency and the maintenance of their reachability are very serious problems to overcome in order to provide a transparent handover with minimum disruption to the ongoing communications.

To solve the IP mobility problem a lot of proposals have been introduced either for IPv4 or IPv6. In the next sections, we frame the discussion by giving details about the IETF proposals.

A. Mobile IPv4

The Mobile IPv4 protocol is proposed by the IETF Mobile IP working group to support unicast IP routing for mobile hosts [11]. A Mobile Node (MN) is a network host that may change its point of attachment from one IP subnet to another. While the MN is at home, it is identified by a topologically correct home address (HoA) and all packets addressed to the MN reach the home link. However, when the MN is attached to a new IP foreign subnet, it acquires a new temporary address (care-of address CoA) that reflects the MN's current point of attachment. The MN forms its CoA by using two different methods. In the first one, the CoA is assigned by a router on a MN's visited network (Foreign Agent, FA), which provides routing services to the MN while registered. In such situation, the CoA will be the address of the FA itself and it is known as a co-located care-of address. In second method, the MN obtains its address through autoconfiguration methods (such as DHCP) and thus the address is not co-located. After this step, the MN registers the CoA with its FA or directly with its Home Agent. The Home Agent (HA), which is a router on the MN's home network, tunnels datagrams to the MN when it is away from home. The HA maintains the current location information from the MN. It maintains and caches an updated association between the MN's HoA and the CoA. This combination is known as a binding. All MN's binding have to be refreshed before the expiration of their lifetime and they are used by the HA and the correspondent nodes to detect the MN's mobility.

When the MN's correspondent is aware about the new temporary address, it can encapsulate its packets and send them directly to the MN. The encapsulated packets can be either decapsulated by the MN when the co-located address is used or decapsulated and forwarded by the FA to the MN using link-level protocols.

B. IPv6 Mobility

To support IPv6 mobility, the IETF (Internet Engineering Task Force) have proposed the Mobile IPv6 protocol [15]. Its main goal is to allow a MN to continue communicating with its correspondent node while moving. The MN can move from its home link to a foreign one without changing its identity (HoA). Furthermore, its movement is transparent to higher-layer protocols and applications. A mobile IPv6 node is identified by its IPv6 home address (HoA). When the MN is away from its home link, it gets one or more care-of addresses from an Access Router (AR) located on the visited subnet. In order to maintain the transport and higher-level communications when moving, the MN maintains its HoA and registers one of the CoAs with its HA. The registered address is called the primary care-of address and the association between this address and the HoA is called a binding. To perform the registration of the primary CoA, the MN sends a packet containing a binding update destination option, which is an extension to the IPv6 destination option. The MN's HA uses proxy Neighbor Discovery to intercept any packet addressed to the MN's HoA on its home link. It then encapsulates and sends the packet through an IPv6 tunnel to the primary CoA on the MN's visited link. When the MN receives a tunneled packet, it sends a binding update to notify the correspondent node of its primary CoA. The correspondent node caches and dynamically updates this binding, and can request a new binding update before the expiration of the existent one by sending a binding update request to the MN. Similarly, the MN's HA learns and caches the binding whenever the MN's CoA changes.

When sending a packet to a MN, the correspondent node checks its binding cache whether it has a binding entry for the MN's HoA. If a cached entry is found, the correspondent sends the packet to the primary CoA, otherwise, the packet is sent as usual to the MN's HoA.

C. IP Multicast

Multicasting falls between unicasting and broadcasting. Rather than sending data to a single receiver (unicasting), or to all the receivers on a given network (broadcasting), multicasting aims to deliver the data to a set of selected receivers. In IP multicast, a single data packet is sent by the source. The network duplicates the packet as required until a copy of the packet reaches each one of the intended receivers. Thus, IP multicast avoids processing overheads associated with replication at the source and the bandwidth overheads due to sending duplicated packets on the same link.

To set-up a multicast session and distribute the multicast data, the group of interested receivers should be formed. A multicast group is a set of network devices sharing a common multicast address. The senders need not to be members of the group and have no prior knowledge of the group membership. On the other hand, the receivers have to join the group by different procedures. In one case, a receiver initiates the membership request when it learns of the group. In another case, local multicast router periodically send membership queries using either IGMP [9] for IPv4 or MLD [34] for IPv6. Any host that wishes to join the group responds to the query by sending its membership report. Once the multicast Designated Router (DR) gathers and manages the membership, it sends a join to the upstream multicast routers in the higher hierarchies. Based on the multicast join, a multicast branch (multicast link) is constructed between two adjacent multicast routers. The chain of multicast branches forms the multicast delivery tree, which can be built using different techniques according to the way that the tree spans between multicast sources and receivers.

When a leaf multicast router has no receivers to serve, it attempts to remove itself from the tree. On-tree router may also prune itself from the tree when it does not have interested downstream multicast routers for the given group.

Different multicast routing protocols are proposed for the use on the Internet. Since the early routing protocols such as DVMRP [37] and MOSPF [25] were designed to handle dense multicast groups, new other protocols are proposed to offer better scalability. Sparse-mode protocols like PIM-SM [8,16] provides efficient communication between members of sparsely distributed groups. A major approach used by sparse-mode protocols was to use a single shared tree that is shared by all members of a group. Consequently, multicast traffic for each group is sent and received over the same delivery tree, regardless of the source.

Although multicasting is a good way of saving bandwidth, it still has some problems and shortcoming that should be addressed in the Mobile IP environment. In fact, IP multicast requires some issues to be solved, including how to join or leave a group, how to discover sources, how to efficiently deliver multicast packets, and especially how to cope with dynamic changes in both group membership and host locations. Furthermore, it is necessary to consider the scalability problems related to the density of group members (dense or sparse groups). On other hand, the time-sensitive delivery of multicast traffic is a great challenge to support real-time multiparty multimedia communications. Security is another important issue to be addressed. Until now, most of these issues do not yet have satisfactory solutions, and much research work is needed to support mobile hosts. In fact, the mobility introduces several issues to be addressed [14], [19], [24], [30], [41]. The basic difficulty for IP multicast in a Mobile IP environment is the frequent change of membership and topological locations. However, the current multicast routing protocols are designed for stationary members but not for mobile ones. Thus, coupling IP multicast with Mobile IP is a challenging problem either for multicast routers, mobile receivers or mobile sources. In the next section, we outline the multicast routing problems and the specific issues for both mobile receivers and senders.

III. MOBILE MULTICAST CHALLENGES

In this section, we outline several problems introduced by coupling IP mobility and IP multicast to support IP multicast for MNs. The problems are classified into four classes: general multicast routing problems, specific mobile receiver problems, specific mobile source issues, and deployment limitations and difficulties.

A. *Multicast routing problems*

The movement of the group member (receiver or sender) induces the following problems:

- Network inactivity: the foreign network visited by mobile receivers may be an inactive network where the multicast service is prohibited. Thus, mobile receivers will face a multicast traffic disruption.
- Multicast encapsulation/decapsulation: as we will see in the next sections, several approaches use tunnels to support multicast for mobile hosts. Using tunnels involves multiple encapsulation and decapsulation operations. To perform such delicate tasks, multicast router requires an extra cost of CPU time and memory. In addition, the multiple encapsulations increase the multicast packet size and can cause both fragmentation and large bandwidth consumption.
- Routing state maintenance: the routing of multicast packets intended for mobile receivers could change frequently. Thus, the branches of the multicast delivery trees should be dynamically refreshed and built accordingly. The cost associated with making changes to the multicast tree is large because this incurs significant routing overhead and needs to be accomplished quickly and harmonized with the handover frequency of mobile receivers.

To do so, two approaches may be used: the “soft state” approach in which branches are deleted if not refreshed within a timeout and the “hard state” that requires explicit leave requests when members leave or relocate. The soft tree maintenance scheme seems to be better adapted to mobile environment than the hard one especially when shared trees are used [30].

- Core placement: when establishing the multicast tree, existing multicast protocols implicitly assume that the group members are topologically stationary. However, in IP Mobile environment, the mobile members (receivers or senders) may be highly moving from one IP subnet to another. As some core routers (Rendezvous Point (PIM-SM), Core (CBT) are statically configured prior to multicast tree construction, frequent IP mobility handovers can cause that these essential multicast routers are “of center”. This situation further aggravating the non-optimality of paths to these routers. To overcome this problem, relocation [26], and any cast routing approaches [18] are the major proposed solutions.

B. *Mobile receiver problems*

The problem of a mobile multicast receiver can be classified into the following issues:

- Multicast latency: when a multicast member is mobile, it will experience additional delay in receiving multicast packets due to mobility handover, multicast membership protocol, multicast tree computation, and increased propagation delay to the new locations of the mobile members [21]. In many cases, a mobile receiver is considered as a new receiver after moving to a new IP foreign subnet, so it needs to re-join again the multicast group. In such situation, the mobile receiver should first discover the presence of the multicast Designated Router. Once the multicast service is discovered, the MN may wait for the next membership query to express interest in listening to multicast traffic from particular multicast group and sources [13]. Thus, the mobile host will experience a delay in constructing new routes and cannot proceed group communications instantly [28]. For some time-sensitive applications, this increased latency is undesirable.
- Packet loss: unfortunately, the current Mobile IP specification does not provide mechanisms to enable local multicast session to survive hand-off and to seamlessly continue from a new CoA on each foreign link. During the handover from one IP subnet to another, the MN needs to receive multicast packets unceasingly while moving. However, the mobile’s multicast handover is unpredictable and there is no forwarding mechanism of multicast traffic addressed to mobile members. Since multicast packets still to be livered to the previous foreign network after the mobile leaves, a mobile receiver may miss some multicast packets due to its movement.
- Packet duplication: the multicast packet duplication can occur when a mobile receiver is getting the same multicast data from different Designated Routers or base stations.
- Packet out of order: due to the handover, the mobile receiver may get its multicast packets out of order. For some multicast applications, this miss order is unacceptable.
- Leave latency: before moving from one foreign network to another, mobile receivers may not have enough time to leave the multicast groups to which they have been previously subscribed. During the handover time, multicast router can forward unnecessary multicast packets. Thus, the designated router will wait the last query report timeout to leave the multicast group.

C. *Mobile source problems*

When a MN wants to send data to a multicast group, it inherits some problems of the mobile receiver that we discussed in the previous section. In addition, a mobile source will experience the following problems:

- Transparency: the transparency is a major issue for mobile multicast sources [22]. As a mobile source moves from one IP subnet to another, both multicast routers and receivers should be able to interpret the traffic coming from the new CoA as coming from the same entity (i.e. the same MN) without the need to re-build the multicast delivery tree or re-join the multicast group. Unfortunately, the established multicast routes are always based on the address of the mobile source. Thus, using CoA will not guarantee the transparency of the mobile source’s handover.
- Reverse Path Forwarding: for a mobile source, direct sending from the visited IP foreign subnet is only applicable while the mobile source is at the foreign link because the associated multicast tree is specific to the source location [20], [22], [30]. Hence, any change of location and source address will invalidate the source specific tree or branch and the application context of other multicast group members. As a consequence, the multicast routing states should be modified to reflect the new locations and to avoid dropping packets due to RPF failure [5]. Typically,

when a mobile SSM source moves to a new subnet, it must inform the multicast receivers about its new CoA (nCoA) [10], [20]. Receivers will subsequently join the new (nCoA, G) channel [35] and thus they will not be in "wrong direction" [39].

- Jitter delay: during the migration from the old CoA specific tree to the new one due to address change, the mobile multicast source cannot send multicast packets unceasingly while moving because the new CoA cannot be used until the source's HA validates it. The delay variation of the multicast packets transfer caused by the address change and registration process will be highly influenced by the handover frequency of the mobile source. For TCP multicast applications, this variation can affect the TCP window in both sender and receiver side and hence degrades TCP performance.

D. Service pricing problems

As the IP mobile multicast is very dynamic, the multicast service pricing is an open issue that causes several deployment problems. It is hopeful that the pricing of commercial multicast service is centralized at the owner. Service agreements are also needed to ovoid the problem of inactive networks where the IP multicast service is prohibited or not secured.

In brief, new mechanisms have to be proposed to take into account the impact of fast moving MNs on the Internet multicast routing protocols and their ability to maintain the integrity of source specific multicast trees and branches. The multicast join latency and the mobile source handover transparency are the major issues. The QoS and the security as well as the multicast service deployment requirements are other important issues to be considered either for mobile or stationary multicasting.

IV. MOBILE MULTICAST REQUIREMENTS

To overcome all the above problems, any proposed solution for mobile multicast should satisfy the following criteria:

- Scalability: the solution should work well when the number of mobile members is large. It should work for small and large multicast groups, spreading topologically densely or sparsely.
- Robustness: the disruption of the multicast service due to MN's handover must be as small as possible. The solution should maintain the quality of service requirement of MN.
- Routing algorithm independence: the multicast routing protocol should be (if possible) independent of the underlying unicast routing architecture.Access technology independence: the solution should work regardless of the link access technology used by the MN (wire or wireless). Also, it has to operate with any access wireless technology (i.e.: IEEE 802.11, Bluetooth, etc.).
- Mobility transparency: the multicast solution should work transparently not only to both micro-mobility (mobility within the same domain) and macro-mobility (mobility between different domains) but also to the frequent change of CoAs. In other words, it should support mobile sources.
- IP Mobility independence: the IP multicast routing entities (Designated Router, Rendezvous Point [7,8,16], Core router [3, 4], etc.) should be independent of the IP mobility entities (e.g. HA, FA). It is not necessary that these entities are co-located.
- Compatibility: the solution should interoperate with existing Internet protocols and mechanisms with as few changes as possible.
- Security: exchanging the membership information and the security keys should be well protected and efficient.

V. MOBILE MULTICAST SOLUTIONS

The well known multicast routing protocols like DVMRP [37], MOSPF [25], PIM [7,8,16], and CBT [3,4] work well when the multicast group members are quite stationary. When the members are mobile, these protocols have limited capability in handling the group membership. In general, a mobile multicast receiver has this typical scenario: it first joins the multicast group, receives multicast packets, it dwells in the foreign IP subnet for a period of time and moves away (into another IP foreign subnet), and rejoins the same multicast group after the handover to continue to receive multicast traffic.

In this section, we investigate some solutions that were proposed to support multicast for IP MNs. For each solution, we discuss its strengths and weaknesses. By the end of this paper, we compare qualitatively all the solutions by fixing different criteria.

A. Mobile IP solutions

This section describes the behavior of a MN, which is away from its home link and wants to join a given multicast group. The MN may be already a multicast member before its handover, as it may want to join the group for the first time. To do so, the IETF proposed two common approaches to be used by a MN (IPv4 and IPv6) either to send or to receive multicast traffic. The first approach is called "the bi-directional tunneling or the home subscription" and the second one is "the remote subscription" approach. In the next sections, we illustrate the advantages and drawbacks of them.

1) Home subscription

The MN may join multicast groups via a bi-directional tunnel to its HA. In this approach called "home subscription", the MN tunnels its multicast group membership control packets as well as its outgoing multicast packets to its HA. In return, the HA forwards the incoming multicast packets down the tunnel to the MN. When the HA receives the MN's tunneled multicast packets, it decapsulates them and forwards them to the multicast router. The Home Designated Router (HDR) intercepts these packets and sends them to the multicast group (see figure 1).

The advantage of the home subscription approach is its simplicity and the transparency of handover of MNs to multicast operation. In other words, the MN does not need to re- subscribe to the multicast group whenever it moves from one network to another. The main drawback is that the routes between the MNs and their designated multicast routers are not optimal, and incur the overheads of tunneling via their HAs. According to us, it could be optimal that the HA and the multicast router functions co-locate. It also relies on a central point of failure (HA) of the multicast delivery tree. In case where multiple MNs of the same home network belong to the same multicast group, the HA needs to duplicate and forward individual multicast packets to them, which may cause congestion at the access router of the visited network. As shown in figure 1, the three MNs (MN1, MN2 and MN3) subscribe to the same multicast group, and the Home Agent (HA) needs three bi-directional tunnels to forward the same multicast traffic to them.

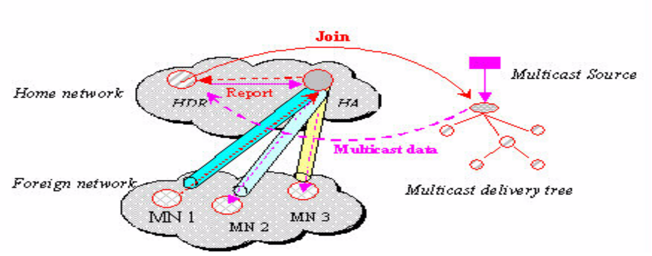

Figure 1: Several bi-directional tunnels from the HA.

*2) **Remote subscription***

In order to receive packets sent to a given multicast group, a MN needs first to join that multicast group. Unlike the home subscription, with the remote subscription approach, the MN joins the multicast group via a local multicast router on the visited foreign network (i.e. the Remote Designated Router RDR) (see figure 2). Following this approach, the MN uses its CoA as the IP source address in its multicast group membership control messages. Thus the multicast routing operation is maintained optimal with the direct use of topologically correct addresses of MNs; and this is the main advantage of this approach.

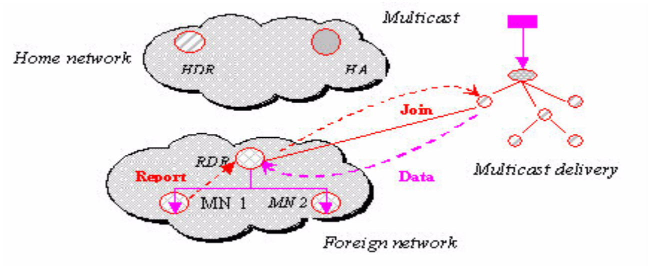

Figure 2: Remote Subscription.

This approach is particularly advantageous when the MN stays in the foreign network for a relatively long period of time, because remote subscription is vulnerable to frequent handover. Whenever the MN moves to a new network, it needs to re-join again the same multicast group with its new CoA. Thus, in this approach, handover of MNs is not transparent to multicast operation. To guarantee the transparency in the high-layer multicast applications, a Mobile IPv6 multicast source has to insert a Home Address Destination Option [16] in its outgoing multicast data packets to associate its HoA with the new CoA. This transparency is not guaranteed with a Mobile IPv4 source, since it does not make use of the previous destination option.

For the rest of this paper, the two previous approaches will be referred to as the basic mobile IP multicast approaches. These approaches can be similarly applied to both Mobile IPv4 and Mobile IPv6.

*B. **Enhanced home subscription for Mobile IPv4***

In [19], authors suggest an enhanced home subscription for Mobile IPv4. The FA gathers membership information and arranges for a unique tunnel to be set up for each multicast group for the MNs from the same home network. The tunnel is set up from the HA whose MN first asks to join a multicast group. Since the tunnel is unique for all the MNs within the foreign network, when all the MNs of this HA (i.e. from which the tunnel is established) move from the foreign network to another, the tunnel is torn down. The FA has to set up a new tunnel from another HA.

The key advantage of this approach is that, in contrast to home registration, only a single tunnel is needed to deliver multicast packets to the MNs which are from the same home network, belong to the same multicast group and are in the same foreign network. This solves partially the tunnel convergence problem. In fact, individual tunnels between the MNs and the HA are still necessary to allow the MNs to be multicast sources. Besides, it still suffers from sub-optimal multicast routing. Finally, this approach needs a dynamic management of the tunnel based on group membership, which introduces complexities and overheads on the FA side. Some modifications are required in order to apply this approach to the Mobile IPv6 context where the FA entity does not exist.

*C. **Uni-directional tunnel***

The enhancement of the home subscription approach for the Mobile IPv6 protocol with the use of a uni-directional tunnel instead of the bi-directional tunnel between the HA and the MN is suggested by [13]. When away from home network, the MN sends multicast packets via the local multicast router and receives multicast packets via a uni-directional tunnel with its HA. The relative advantage concerns the case in which the MN is a multicast source. There is no need of change in the HA to help the MN to forward its multicast packets. Besides, when the MN sends its multicast packets to the local multicast router directly, the multicast routing is more efficient.

*D. **Mobile Multicast Protocol (MoM)***

In order to adapt the Mobile IPv4 protocol so that it can handle multicast forwarding with adequate scalability, [39] proposed a new approach called Mobile Multicast Protocol (MoM). This approach is different from the two basic mobile IP multicast solutions. The key idea is to handle in different ways multicast source mobility and multicast destination mobility. If the MN is the source of a multicast group, MoM suggests that the MN uses link-level multicast to send packet to its HA whenever the MN is at home. If the MN is away from home, it has to use a tunnel to deliver the multicast packet to its HA.

In case of multicast mobile receivers belonging to a given group G, [39] suggests that the HA sends to each concerned FA one copy of multicast packets into an IP tunnel. The FA then uses link-level multicast to complete the delivery.

In case where several HAs have their MNs with the same FA, MoM suggests that the FA select one HA as the Designated Multicast Service Provider (DMSP) for a given multicast group. Thus, the DMSP forwards only one copy of multicast packets into the tunnel to the FA.

As in the home subscription approach, this approach suffers from sub-optimal multicast routing because all multicast packets sent or received by a MN always traverse the home network. This solution also appears to be vulnerable to MN handover: a new DMSP needs to be selected and this may affect the other MNs in both the old and new networks. This operation requires the FA to make complicated management of DMSP selection according to the MNs and their multicast group. We believe that the efficiency of this approach is affected by the excessive overheads compared to the home registration approach on which MoM is based.

*E. **Multicast Agent***

In [41], authors introduce the concept of Multicast Agent for mobile members. A Multicast Agent (MA) is a multicast router that provides multicasting to multicast MN members in multiple foreign networks. The MA maintains a list of multicast groups that have MN members in its service area. For each multicast group, it also maintains a list of FAs that have visiting MN multicast members.

The MA joins the multicast group on behalf of the MN members and then tunnels the multicast packets to the corresponding FAs. A given FA delivers the multicast packets using local multicast. Thus, both the tunnel convergence and long tunnel are avoided. However no procedure is described to select the MA and to determine its proximity to MNs. In addition, the MA location would affect the performance of this approach.

F. Range-Based Mobile Multicast (RBMoM)

Range-Based Mobile Multicast (RBMoM) is based on Mobile IPv4 and intends to find an optimal tradeoff between shortest delivery path and low frequency of multicast tree reconfiguration [14]. This solution is based on a Multicast Home Agent (MHA). The MHA is a multicast router with a fixed service range. The concept of service range is based on the hop distance between the HA and the MN to limit the length of tunnel between them to forward multicast traffic. In other words, the HA is the MHA if the mobile member roams between foreign networks within the service range. Otherwise, the FA will become the MN's MHA. Thus the MHA of the MN changes dynamically according to the location of the MN after the handover (see figure 3). Similar to the MoM protocol [39], RBMoM uses the same concept of Designated Multicast Service Provider (DMSP) to avoid multiple tunnels from different MHAs that have MNs within the same FA.

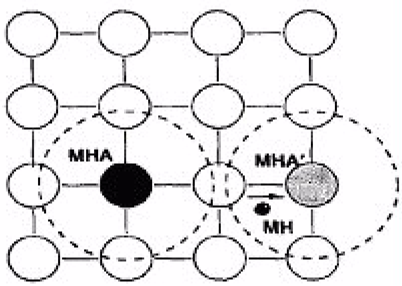

Figure 3: RBMoM Protocol.

In this solution, MHA introduces significant complexity without obvious advantages. The key idea of using the MHA is to limit the functionality of the HA to forwarding only unicast packets. It is not clear if the concept of service range optimize multicast routing path. In addition, the optimal service range is not given. Besides, using the DMSP entity is doubtful, as discussed in the MoM section.

G. MobiCast

A solution to support MNs roaming between small wireless cells is proposed in [12]. This proposal attempts to minimize the re-computation of the multicast delivery tree and reduce packet loss when a MN multicast member of a given group crosses cell boundaries during a multicast session. The proposed solution requires hierarchical mobility management and uses translated multicast address. The form and the description of the translated address are not given, however it is stated that it is unique within a given domain.

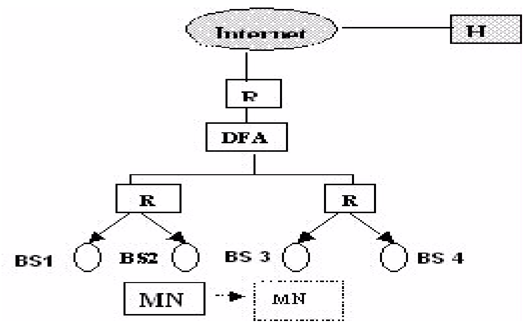

Figure4: Mobicast architecture.

This solution introduces the Domain Foreign Agent (DFA) to represent the MN in the multicast tree to hide the MN's mobility within the foreign domain (see figure 4). The subscription of the base station to a translated multicast group prior to the handover seems to be similar to the proposals in [1] and [2]. When the MN is the source of the multicast group, the IP address of the DFA is used as the IP source address of the multicast packets. As a consequence, higher level protocols in the application of multicast receivers cannot identify the original source of the packets.

H. Mobifity Support Agent (MSA)

To avoid disruption of the multicast communication of a mobile member, [23] proposes a solution based on pre-registration. This solution defines an IPv4 Mobility Support Agent (MSA) in the new visited network. While this MN is in the midst of handover to the new network, the MSA joins the multicast group. This reduces the loss of multicast packets to the MN during handover. The protocol for the pre-registration is simple and it is built over UDP. However, the MN needs to know in advance when handover will occur and to which new network it is moving, in order to trigger the pre-registration procedure immediately before the handover. Upon receiving the pre-registration message, the MSA sends an IGMP join message to the multicast router.

In this approach, the discovery of the new network for handover is a major issue. This could potentially benefit from the seamless handover work such as Fast Mobile IP. Besides, the underlying link technologies may be able to provide such information. In all cases, substantial co-ordination is needed between the MSAs of the old and new networks. It is unclear if the extra protocol overheads are low enough to be efficient and effective.

I. Explicit Multicast over Mobile IP (XMIP)

In [24] authors proposed a new scheme to support IP multicast when groups are of limited size. The proposed solution is based on Explicit Multicast (Xcast), which requires that the source keeps track of the destinations and creates a packet header that contains a list of destination addresses. Thus, there is no need for multicast group membership and multicast routing protocols. From the source to the destinations, the list of destination addresses is updated. The intermediate routers forward within their areas the packets with relevant IP addresses and remove the other addresses. This procedure is done hop-by-hop until all the receivers are reached.

This approach enhances Xcast for Mobile IP to support multicast to MN receivers, with Xcast-capable HA. This HA receives the Xcast packet on behalf of its MN. Then, it looks up the CoAs bound with the HoAs listed in the Xcast packet. Then, depending on the current location of the destinated

MNs, it separates the care-of-addresses into small subset addresses and replicates the intercepted packet and tunnels it to the set of MNs that match the subset of CoAs. This approach is not scalable. However, it may be practical for a small and closedSpre-established multicast group.

J. Source-Specific Multicast (SSM)

The Source-Specific multicast (SSM) protocol is another model for IP multicasting that differs from the Any-Source Multicast (ASM) [20]. In addition, it defines a new terminology for group membership operations and for identifying the multicast group. For a given multicast address G in the SSM range and an IP source address S, the couple (S, G) represents a channel. Thus, the multicast members that wish to receive multicast traffic only from the specified source S have to subscribe to the channel (S,G). When a multicast member wants to leave the multicast session, it can unsubscribe from the channel.

To support mobile multicast source in Mobile IPv6 with SSM, [10] suggests adding a new sub-option in the basic IPv6 binding destination option [15]. This new option is called SSM Source Handover Notification and it is used to notify the multicast receivers to subscribe to the new channel (S's CoA, G) whereas CoA is the new CoA of the source node S.

This approach is straightforward. However, it is not clear how the move of the multicast source and the migration of the receivers to the new channel can be synchronized in order to minimize the disruption of the multicast session during the handover of the multicast source.

VI. COMPARISON

Establishing a quantitative comparison of the described solutions is difficult since they have different assumptions and goals. Nevertheless, we can compare qualitatively these solutions by using the following criteria (see table 1). The choice of such criteria is justified by the nature of the problem to overcome.

- Optimal Routing: This is the major important criteria because it may affects all others factors. The joining path is optimal if multicast packets are received (or sent) quickly and through the shortest path.
- Tunnel Convergence: In some circumstances, several end-point multicast tunnels end on the same network entity (for example FA) or the same network (same foreign IP subnet). This cause multicast packet duplication and overwhelmed the receiving entity.
- Tunneling: in addition to the tunnel convergence problem, using tunnel-based solution needs extra cost of time processing on the multicast routers (multiple encapsulations and decapsulations).
- Transparency: the handover of both multicast receiver and sender should be transparent to the multicast routing protocols and to the construction of the multicast delivery tree. The acquisition of a new CoA may disturb the multicast routing states (i.e. they need to be updated or changed) and cause the re-building of the main multicast delivery tree especially for source specific trees.
- Seamless handover: a smooth handover and rejoin is required to overcome the high dynamic nature of membership in IP mobile multicast.
- Multicast latency: the join latency depends on the hop count between the multicast router to which the mobile receiver addresses its join membership report and the nearest on-tree multicast router. It depends also on the approach used for subscribing (home or remote). The multicast latency does not take into account the time required by multicast router to process join membership reports. We assume that this time is constant.
- Packet loss: The packet loss is caused by both the handover and the multicast joins latencies. This metric should be minimized to support IP multicast with IP mobile members.
- Agents involved: Some approaches require some modifications to the current Mobile IP specification (Mobile IPv4 and Mobile IPv6) and they involve more than one Mobile IP entity. In some approaches, new entities are added.
- Mobility Agents independence: some solutions require mobility agents, which are coupled with multicast routers. In general, there are no assumptions that the IP mobility entities (HA and FA) are co-located with multicast routers (Designated Router, Rendezvous Point, Core, etc.).
- Applicability: some solutions are suitable either to Mobile IPv4 or to Mobile IPv6. Others may be applicable to both protocols. They may require some modifications to the current Mobile IP specification (Mobile IPv4 and Mobile IPv6).

VII. CONCLUDING REMARKS

In this paper, we conducted a brief overview of multicast solutions for MNs. The home and remote subscription approaches serve as the basic techniques. The majority of the proposed enhanced solutions attempt to optimize the home subscription approach for Mobile IPv4. As most proposed solutions are specific to Mobile IPv4, they cannot be easily adapted to the Mobile IPv6 context since they make use of FAs, which does not exist in Mobile IPv6. Moreover, there is few evaluation of these interesting solutions in somehow realistic scenarios. Their deployment should take into account the existing multicast architectures and the wireless infrastructures.

Supporting multicast for MNs is complex. The challenges are inherited from the multicast problems for stationary nodes as well as from IP mobility problems. For both stationary nodes and MNs, there are some common open issues such as reliable multicast, QoS support and multicast group security. In case of MNs, dynamic management of multicast group and efficient re-computation of multicast route are essential. In particular, tunnels should be avoided to optimize multicast routes, and the multicast router operations should be made as simple as possible. The most important is to minimize the disruption of the multicast session during the handover of multicast source and receivers, with respect to packet loss. In addition, enhancements should focus on related security and QoS issues.

Finally, we believe that coupling IP multicast with mobile routing entities (like Mobile Router and Mobile Networks) will complicate the situation. This perspective wells worth the effort to be studied and the architectural issues have to be considered in order to deploy IP Multicasting in IP Mobile Networks.

VIII. ACKNOWLEDGEMENT

We would like to thank Dr. Kunal Bhattacharya for his interesting comments.

IX. REFERENCES

[1] Ahmed Helmy, "Multicast-based Architecture for IP Mobility Support", ACM SIGCOMM Second

International Workshop on Networked Group Communication (NGC 2000), Palo Alto, November 2000.

[2] Ahmed Helmy, "Multicast-based Architecture for IP Mobility: Simulation Analysis and Comparison with Basic Mobile IP", featured in Technology Research News (TRN) Journal, issue 1, June 21, 2000.

[3] A. Ballardie, "Core Based Trees (CBT) Multicast Routing Architecture", Internet RFC 2201, September 1997.

[4] A. Ballardie, "Core Based Trees (CBT version 2) Multicast Routing Protocol Specification", internet RFC 2189, September 1997.

[5] A O'Neill, "Mobility Management and IP Multicast", Internet Draft, draft-oneill-mip- multicast-00.txt, 5 July 2002.

[6] Arup Acharya, and B.R. Badrinath, "A Framework for delivering multicast messages in networks with mobile hosts", Mobile Networks and Applications, p. 199-219, 1996.

[7] Andrew Adams, Jonathan Nicholas, "Protocol Independent Multicast – Dense Mode (PIM-DM): Protocol Specification (Revised)", Internet draft, draft-ietf-pim-dm-new- v2-01.txt, February 15, 2002.

[8] Bill Fenner, Mark Handley, Hugh Holbrook, Isidor Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", Internet Draft, daft-ietf-pim-sm-v2-new-05.txt, 1 March 2002.

[9] Brad Cain, Steve Deering, Bill Fenner, Isidor Kouvelas, and Ajit Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, Obsoletes: 2236, October 2002.

[10] C. Jelger and T. Noel, "Supporting Mobile SSM Sources for IPv6 (MSSMv6)", Internet Draft, draft-jelger-mssmv6-00.txt, January 2002.

[11] C. Perkins, "IPv4 Mobility Support", RFC 2002, October 1996.

[12] Cheng Lin Tan and Stephan Pink, "Mobicast: A Multicast Scheme for Wireless

[13] Networks", Mobile Networks and Applications (MONET), Volume 5, Number 4, 2000.

[14] Christian Bettsteller, Anton Riedl, and Gerhard Ge ler, "Interoperation of Mobile IPv6 and Protocol Independent Multicast Dense Mode", ICPP Workshop 2000, pp. 531-540,2000.

[15] Chunhung Richard Lin and Kai-Min Wang, "Mobile Multicast Support in IP networks", IEEE INFOCOM 2000, pp. 1664-1672, March 2000.

[16] David B. Johnson, C. Perkins, "Mobility support in IPv6", IETF Internet Draft, draft- ietf-mobileip-ipv6-18.txt, 1 June 2002.

[17] D. Estrin, D. Farinacci, et Al., "Protocol independent Multicast-Sparse Mode (PIM- SM): Protocol Specification", RFC 2362, June 1998.

[18] D. Kosiur, "IP Multicasting: the complete guide to interactive corporate networks", Wiley Computer Publishing, 1998.

[19] Dorian Kim, Verio, David Meyer, et al., "Anycast RP mechanism using PIM and

[20] MSDP", Internet Draft, draft-ietf-mboned-anycast-rp-08.txt, May 2001.

[21] George Xylomenos and George C. Polyzos, "IP Multicast for Mobile Hosts", IEEE Communications Magazine, Volume 35, Number 1, pp. 54-58, 1997.

[22] H. Holbrook, B. Cain, "Source-Specific Multicast for IP", Internet Draft, draft-ietf- ssm-arch-00.txt, November 21, 2001.

[23] Hrishikesh Gossain, Carlos de Morais Cordeiro, and Dharma P. Agrawal, "Multicast: Wired to Wireless", IEEE Communications Magazine, June 2002.

[24] Hrishikesh Gossain, Siddesh Kamat, and Dharma P. Agrawal, "A Framework for Handling Multicast Source Movement over Mobile IP", ICC 02, May 2, 2002.

[25] Jiang Wu and G. Q. Maguire Jr., "Agent based seamless IP multicast receiver handover", Proceedings of the IFIP Conference on Personal Wireless Communications PWC'2000, September 2000.

[26] Jiwoong Lee and Myung-Ki Shin, "Explicit Multicast over Mobile IP (XMIP)", Internet Draft, draft-lee-xcast-mobileip-00.txt, November 8, 2001.

[27] J. Moy, "Multicast Extensions to OSPF", Internet RFC 1584, March 1994.

[28] J. William Atwood, and Ritesh Mukherjee, "RP Relocation in PIM-SM Multicast", Internet-Draft, draft-atwood-pim-sm-rp-02.txt, June 27, 2002

[29] Jiwoong Lee, "Multicast Avalanche Avoidance in Mobile IP (MAAMIP)", Internet Draft, draft-lee-maa-mip-00.txt, December 27, 2001.

[30] Kuang-Hwei Chi, Chien-Chao Tseng, and Ting-lu Huang, "A Framework for Mobile Multicast Using Dynamic Route Reconstructions", The Computer Journal, Vol. 42, No. 6, 1999.

[31] Luis Henrique M. K. Costa1, Serge Fdida, and Otto Carlos M. B. Duarte, "Hop By Hop

[32] Multicast Routing Protocol", SIGCOMM Conference, San Diego, CA, USA, August 2001, pp. 249-259.

[33] Mario Gerla, Ching-Chuan Chiang, and Lixia Zhang, "Tree Multicast Strategies in Mobile, Multihop, Wireless Networks", ACM/Baltzer Journal of Mobile Networks and

[34] Applications (MONET), pages 193-207, Vol. 4, No. 3, 1999.

[35] Maria Ramalho, "Intra- and Inter-Domain Multicast Routing Protocols: A survey and taxonomy", IEEE Communications Surveys & Tutorials, First Quarter 2000, vol.3 no.1.

[36] Noel Cantenot and all, "State-of-the-art Survey of Multicast Routing", Technical Information, EDIN 0054-1010, December 2000.

[37] Rick Boivie and Nancy Feldman, "Small Group Multicast", Internet Draft, draft- boivie sgm-02.txt, February 2001.

[38] Rolland Vida, Luis Costa, Remi Zara, Serge Fdida, Steve Deering, Bill Fenner, Isidor Kouvelas, and Brian Haberman, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", Internet Draft, darft-vida-mld-v2-05.txt, October 16, 2002.

[39] S. Bhattacharyya, C. Diot, L. Giuliano, R. Rockell, J. Meylor, D. Meyer, G. Shepherd, B.Haberman, "An Overview of Source-Specific Multicast (SSM)", Internet draft, draft- ietf-ssm-overview-03.txt, March 2002.

[40] T. Noel, J.J. Pansiot, "A Multicast Architecture for Mobile Nodes", International Journal of Computer and Information Science, Vol.3 No.2, 2002.

[41] T. Pusateri, "Distance Vector Multicast Routing Protocol", Internet draft, draft-ietf- idmr-dvmrp-v3-10.txt, August 2000.

[42] Magret and V. Kumar Choyri, "Multicast Micro-Mobility Protocol (MMM)", Internet Draft, draft-magret-mobileip-mmm-00.txt, July 1, 2000.

[43] Vineet Chikarmane, Carey L. Williamson, Richard B. Bunt and Wayne L. Mackrell, “Multicast support for mobile hosts using mobile IP: design issues and proposed architecture (MoM protocol)”, ACM/Baltzer Mobile Network and Applications, vol. 3, no. 4, pp. 365-379, 1999.

[44] Weijia Jia, Wanlei Zhou, M. A. Livani, Joerg Kaiser, “Anycast Group Algorithms for Mobile Multicast Communications”, Proc. 11-th IASTED Int. Conference on Parallel and Distributed Computing and Systems (PDCS '99), Boston, MA, Nov. 1999.

[45] Yu Wang and Weidong Chen, “Supporting IP Multicast for Mobile Hosts”, Southern Methodist University, May 8, 1998.

