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 multicast source sends a single copy of a data packet and the network duplicates the packet as required until a copy of the packet reaches each one of the intended receivers. This 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, the group of interested receivers should be formed. A multicast group is a set of network devices identified by a common multicast address. On one hand, the senders do not need 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. A receiver initiates its membership request when it learns of the group. A local multicast router periodically sends membership query messages using either Internet Group Management Protocol (IGMP) [1] for IPv4 or Multicast Listener Discovery (MLD) [2] for IPv6. Any host that wishes to join the group replies with a membership report message. A multicast router periodically gathers and manages the membership report messages, and then sends a join message to the upstream multicast routers. Based on multicast membership information, a multicast branch is constructed between two adjacent multicast routers. The chain of multicast branches forms the multicast delivery tree. This tree can be built using different techniques according to the way that it spans between sources and receivers.

Today a multicast member may be a stationary host or a mobile host. Nomadic users require a new kind of network host that can be moved from one attachment point to another without reconfiguration. Hereafter, this kind of network host is defined as a mobile node (MN). When the MN is attached to its home network it is identified by a permanent IP address called the home address (HoA). If the MN is away from home and it is attached to a new IP network, it gets a new temporary care-of address (CoA) from the visited network. The movement from one IP network to another is called a handover. To make this handover transparent to the transport and higher-level communications, the mobile host maintains its HoA while it uses the CoA for routing purpose. The two addresses are then associated and the association is called a binding.

In the case of multicast communication, the scenario of handover is particularly challenging and several issues emerge with most solutions due to the handover impacts. The Internet research community has proposed many routing protocols such as Multicast Extensions to Open Shortest Path First (MOSPF) [3], Distance Vector Multicast Routing Protocol (DVMRP) [4], Protocol-Independent Multicast Sparse Mode (PIM-SM) [5], and Core-based Tree Protocol (CBT) [6] to support efficient multicast by using a multicast tree [7]. 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 either topologically mobile receivers or mobile sources. Unfortunately, when a multicast receiver is mobile it will experience additional delay in receiving multicast packets due to handover delay, join latency, and increased propagation delay to the new location. These impacts depend on the way IP multicast is combined with mobile IP. On one hand, when a mobile receiver moves from one IP network to another, it can continue using in a naive way the mobile IP to receive multicast data from the home network. In this case, the multicast routing may be sub-optimal and the delay may increase. On the other hand, when the mobile receiver simply uses the IP multicast without relying on mobile IP, it uses in this case the multicast infrastructure of the foreign network to subscribe to multicast groups. In this situation the mobile receiver needs to re-subscribe again whenever it moves. During this movement the mobile receiver may miss some multicast packets. This packet loss is frequent and it is estimated to be variable between 1 percent and 30 percent [8]. Similarly, the mobility of the multicast source induces disruption of the multicast session or a reconstruction of the entire multicast tree. Such reconstruction is caused by the change of the source’s address and it seems to be prohibitively expensive in terms of repeated multicast tree set-up cost. When a mobile source moves from one IP network to another while it has an on-going multicast session, the mobile source gets a new IP address (CoA) from the new visited network. Then it uses this new CoA as a source address to send its multicast packets. Since IP multicast is receiver-initiated, the source’s multicast router in the foreign network cannot forward these packets until the receivers explicitly notify it. Without such notification, which can be done with the Multicast Source Dynamic Protocol (MNDP) [9], multicast data will not be forwarded downstream. Furthermore, multicast receivers are not able to interpret the traffic coming from the new CoA as coming from the same source.

In this article we present the challenges of coupling IP multicast with Mobile IP, and we present a comprehensive overview of the existing mobile multicast solutions. The reliable multicast solutions for mobile hosts such as the work of [10] are out of the scope of this work. Because of space limitations we do not address application-layer multicast routing protocols for mobile hosts [11, 12], and we do not focus on multicast infrastructure to support mobility by using IP multicast such as that proposed by [13, 14].

The rest of this article is organized as follows. We introduce the basic concepts of Mobile IPv4 and the Mobile IPv6 protocols and outline their similarities and differences. We introduce the fundamentals of IP multicast, and focus on the challenges of supporting multicast for mobile hosts (receivers and senders) and other related problems. We summarize the proposed solutions to support IP multicast with mobile receivers, describing the solutions to overcome the handover problem of mobile multicast sources. Finally, we draw conclusions and define the requirements that should be met by any efficient implementation of a mobile multicast solution.

**BACKGROUND OF IP MOBILITY**

It is a challenging problem to maintain transparency and reachability of a mobile node when moving from one network to another. To solve these issues many proposals have been introduced either for IPv4 or IPv6. In this section we frame the discussion by giving details about the Internet Engineering Task Force (IETF) proposals: the Mobile IPv6 [15] and the Mobile IPv4 protocols. These two protocols have similar functionalities. We start by introducing their basic concept and then we outline their similarities and differences. We also briefly describe IP hierarchical mobility management in the IPv4 and IPv6 environments.

**BASIC CONCEPTS**

The main goal of both the Mobile IPv4 and the Mobile IPv6 protocols is to allow a MN to continue communicating with its correspondent nodes (CNs) during its movement. The MN can move from its home network to a foreign network without changing its configuration. Each MN is identified by a permanent unicast IP address named HoA in the home network. When the MN moves to a new IP network that is different from the home network, it gets a new temporary unicast address that is routable within the new foreign network. This second address is called a CoA. To form this second address, the MN may use either stateless [16] or stateful address configuration mechanisms [17] with Duplicate Address Detection (DAD) methods. The MN repeats this operation whenever the handover occurs. The handover is a change in MN’s point of attachment to the Internet such that the MN is no longer connected to the same IP subnet as it was previously. The handover can be detected by different facilities including the Neighbor Discovery Protocol [17], signal strength, or signal quality information. The movement detection and the handover itself can be initiated by the MN or by the network. If the MN makes quality measurements of signal strengths and decides to switch to the best one with the help of the network layer, the handover is called Mobile Initiated Handover. In the second scheme called, Network Initiated Handover, the network makes the decision of the handover. In order to maintain the transport and higher-level communications when moving, the MN maintains its HoA and uses the CoA for routing purpose. A binding associates these two addresses on both the MN part and the home network part. Both the MN and the HA learn and cache the binding whenever the MN's CoA changes. To do so, the MN registers its CoA with its home agent (HA). The HA may be a router on the home network. While the mobile node is away from its home link, the HA is responsible for forwarding data addressed to the MN's HoA. The signaling mechanism used during the registration of the CoA differs from the Mobile IPv4 to the Mobile IPv6 protocol. The registration on the Mobile IPv6 protocol is direct (without third-party dependency), whereas in the Mobile IPv4, it may be direct or through a new architectural entity called a foreign agent (FA). The FA is an IPv4 router located on an MN’s visited network, which provides routing services to the MN while registered. When the MN sends IP packets, the FA may serve as a default router. While the MN is away from home, the HA uses proxy Neighbor Discovery [17] to intercept on the home link any packet addressed to the MN’s HoA. The HA uses the Neighbor Discovery protocol to detect the presence and absence of neighboring nodes (hosts and routers), and thus the link connectivity of these nodes. Finally, the HA encapsulates and sends the packet through a bi-directional IP tunnel to the CoA. Compared to the Mobile IPv6, on the Mobile IPv4 the FA may intercept and deliver packets to the MN while it receives them from the HA.

**COMPARISON BETWEEN MOBILE IPv6 AND MOBILE IPv4**

The Mobile IPv6 protocol shares many features and similarities with the Mobile IPv4 protocol, but it offers many improvements. In fact, the Mobile IPv6 protocol does not deploy FA.
Hierarchical Mobility Management

Hierarchical mobility management was proposed by the IETF to reduce the basic Mobile IP signaling load caused by the registering mechanism, minimize handover delay, improve route optimization, and separate the local mobility within a given IP domain from the global mobility among the Internet. For these purposes the IETF has defined two hierarchical mobile routing protocols: the Hierarchical Mobile IPv4 Protocol (HMIPv4) [18] and the Hierarchical Mobile IPv6 Protocol (HMIPv6) [19]. Compared to the basic Mobile IP protocol, these protocols introduce the concept of hierarchy and two new architectural entities. In fact, the HMIPv6 protocol has defined a new entity called the mobility anchor point (MAP). The MAP is a router located in the top level of the hierarchy of a visited IPv6 network. The mobile node uses the MAP as a local HA to hide its micro-mobility. Since the MAP is considered a local HA for the MN, the MN has to register with the local MAP rather than with its HA that is typically further away. Similarly, the HMIPv4 protocol has introduced a new network entity called the gateway foreign agent (GFA). The GFA is a IPv4 router that is placed on the higher headachy of an IPv6 visited domain. When the visited domain supports IPv4 regional tunnel management, the CoA of the MN is the publicly routable address of the GFA. This CoA will not change when the MN changes its FA under the same GFA. While moving within the same MAP or GFA, an MN has to register once with its HA, which reduces the signaling load on the HA side.

Background of IP Multicast

Basic Concepts

Multicasting aims to deliver data to a set of selected receivers. Within the context of multicast, various types of multicast communication can be differentiated, depending on the number of senders and receivers. Multicast applications can be classified into one-to-many and many-to-many applications [20]. The one-to-many multicast application implies one source and a set of receivers. Scheduled audio/video distribution, push media (news headlines, weather updates, sports scores, etc.), file distribution, and caching are the commonly used one-to-many multicast applications. The many-to-many multicast application implies any number of hosts sending to the same multicast group address, as well as receiving from it. For example, multimedia conferencing, shared distributed databases, distributed parallel processing, shared document editing, distance learning, chat groups, multi-player games, etc., are multicast applications in which each member may receive data from multiple senders while it sends data to all of them.

Multicast Addressing

To set up a multicast session and distribute the multicast data, the group of interested receivers should be formed. A multicast address is a topological identifier used to identify a set of hosts to which IP packets are delivered. The multicast address can be allocated from a specific range of IP addresses dedicated to sending to groups. Each address has a specific scope, which limits the flooding of multicast packets. Currently, multicast scoping technique uses either the time to live field in the IPv4 packet header or the scope field in the case of an IPv6 packet header. The scope field is different from the hop limit field.

We distinguish two IP multicast models: the Any-Source Model (ASM) and the Source-Specific Model (SSM) [21]. These models have different multicast address ranges and different terminologies. In fact, the pair (S, G) identifies a unique SSM channel, where S is a specific multicast source and G is a multicast address in the SSM range. This implies that receivers have to subscribe to this channel when they want to receive multicast data from the source S and unsubscribe when they leave the group. With the ASM model, a receiver joins the group and leaves it at will.

The IETF has particularly defined guidelines that explain how to assign and allocate IP multicast addresses for both the ASM and the SSM models. To allocate a multicast address, two mechanisms can be used. The first mechanism is centralized in which the allocation is carried out by an authorized institution. Hence, a multicast address has to be requested from this authority and cancelled when the multicast session ends. The second mechanism is distributed, in which the allocation is performed locally through multicast address allocation servers and requires a specific protocol such as the Multicast Address Dynamic Client Allocation Protocol (MADCAP) [22]. Compared to the centralized mechanism, the distributed mechanism does not guarantee the uniqueness of the multicast address, but it is more flexible than the centralized mechanism. To avoid confusion and reduce the probability of IP multicast address collision, the IPv6 multicast address architecture [23] has been revised and new extensions have been introduced to simplify the dynamic allocation of multicast addresses and embed IPv6 unicast prefixes in multicast addresses [24]. By delegating multicast addresses at the same time as unicast prefixes, network operators will be able to identify their multicast addresses without running an inter-domain allocation protocol.

Multicast Membership Protocols

To join or leave a multicast group at any time, multicast receivers require a membership protocol. The IETF defined the MLD (2) protocol to be used by IPv6 routers to discover the presence of interested receivers of a given multicast group. Similarly, it proposed the IGMP (2) to be used by IPv4 hosts and routers. The current versions of IGMP (IGMPV3) and MLD (MLDV2) have similar functionalities and contain two parts. The first part is the host part, which specifies how receivers learn the existence of a multicast router, how they discover groups, and how they express their interest in listening to a given group. The second part is the router part, which specifies how multicast routers manage membership information and how they exchange this information in order to build the multicast delivery tree. Since the two membership protocols are similar, we will explain the membership mechanism by choosing the MLD protocol. The current version of MLD (MLDV2) overcomes the limits of the previous version (MLDV1) and offers the opportunity for receivers to filter specific multicast sources. The MLDV2 specifies two types of messages: multicast listener query (MLQ) and multicast listener...
The multicast listener query (also called the membership query in IGMP) is sent periodically by multicast routers to all the local hosts to determine for each multicast address whether or not they have listeners on that link. Source-specific queries add the capability for a multicast router to discover which multicast sources have listeners among the neighboring nodes. The multicast listener queries are used to build and refresh the multicast state of routers on attached links. As a response to the multicast listener query message, multicast receivers respond to these queries by sending a M LR (in IGMP, receivers use membership report messages). These reports are sent with an IPV6 link-local source address, which allows other neighbors to delay their report messages. The multicast receiver may express interest in receiving traffic from particular sources by sending specific reports to explicitly notify the multicast router about the changes. At the same time, each multicast receiver maintains and computes the multicast listening state for each of its interfaces. This state contains the IPV6 multicast address, the filter mode, and the source list. Based on the membership information, multicast routers join the multicast delivery tree of the specified multicast group by using the appropriate multicast routing protocol.

To avoid deploying multicast routers and multicast routing protocols inside a given network, the IETF has proposed to use IGMP/MLD Forwarding Proxy entities [25]. Each IGMP/MLD proxy performs membership management and acts as a multicast querier for its subnet and as a host for an upstream proxy or multicast router. Each proxy periodically sends membership queries in its downstream interfaces. When it receives multicast report messages, it forwards only one membership report message to the upstream proxy. To cope with membership dynamics efficiently, an IGMP/MLD proxy maintains an up-to-date membership database that reflects membership information of all the nodes in its downstream interfaces. As Fig. 1 shows, the IGML/MLD proxies can be organized into a manually configured spanning tree. The root of this tree is a multicast router (R1). This router, which may be located at the border of the network, joins the multicast delivery tree on behalf of all the proxies. When the multicast router joins the multicast delivery tree, it floods data into its downstream interfaces. In return, the first-hop proxies, with respect to the multicast router location, forward the data to local receivers and to other downstream proxies. Finally, leaf proxies deliver multicast data to their local receivers.

Multicast members can leave multicast groups at will either explicitly or implicitly. With the explicit approach, a multicast receiver sends a membership report message in which it excludes all the groups and sources to which it was listening. In the implicit approach, a multicast receiver ignores the membership query messages and does not reply with a membership report message to its multicast router. When a lifetime expires and there is no response from the receivers, the multicast router assumes that there is no interested receiver in its downstream interfaces and may remove itself from the multicast delivery tree.

**Multicast Routing Protocols**

Multicast routing protocols are responsible for the construction of the multicast delivery tree. For this purpose, multicast routers need some routing algorithms to distribute the membership information and to build the necessary multicast tree on which multicast packets are sent. Several multicast routing protocols are proposed for use on the Internet. Since the early routing protocols such as DVMRP [4] and MOSPF [3] were designed to handle dense multicast groups, new protocols have been proposed to offer better scalability. Sparse-mode protocols such as PIM-SM [5, 26] provide efficient multicast communication between members that are sparsely distributed. Such protocols 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. When a leaf multicast router has no receivers in all its subnets, it attempts to remove itself from the tree. An on-tree router may also prune itself from the tree when it does not have interested downstream multicast routers for the given group.

**MOBILE MULTICAST CHALLENGES**

In this section, we outline several problems introduced by coupling IP mobility and IP multicast to support IP multicast for mobile hosts. These problems are classified into four categories: general multicast routing problems, specific mobile source issues, specific mobile receiver problems, and deployment difficulties. Figure 2 summarizes this classification.

**Multicast Routing Problems**

The movement of the group member (receiver or sender) induces the following multicast routing 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 not receive multicast traffic.

- **Multicast Encapsulation/Decapsulation:** As we will see in the next sections, several approaches use tunneling to support multicast for mobile hosts. Using IP tunnels involves multiple encapsulation and decapsulation operations, which require an extra cost of central processing unit (CPU) time and memory.
In addition, multiple encapsulations increase the multicast packet size and can cause 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 tree should be dynamically refreshed and built accordingly. The cost associated with the reconstruction of a multicast tree is important because this incurs significant routing overhead. To maintain a multicast tree, two approaches may be used: the soft state approach, in which branches are deleted if not refreshed within a timeout; and the hard state approach, which requires explicit leave requests when members leave or relocate. The soft tree maintenance scheme seems to be better adapted to mobile environments than the hard state scheme, especially when shared trees are used [27].

**Core Placement:** When establishing a multicast tree, existing multicast protocols implicitly assume that the group members are topologically stationary. However, in Mobile IP networks, the members (receivers or senders) are mobile and may move from one IP subnet to another. As some core routers (rendezvous point (PIM-SM) [5], core router (CBT) [6]) are statically configured prior to multicast tree construction, frequent handovers can lead to a situation in which these essential multicast routers are off center. This situation further induces the non-optimality of the multicast routing paths. To overcome this problem, relocation [28], anycast routing approaches [29], tree migration, and evolution techniques [30] are the major proposed solutions.

**MOBILE RECEIVER PROBLEMS**

The challenges of a mobile multicast receiver can be classified into the following issues.

**Multicast Latency:** When a receiver is mobile, it will experience additional delay in receiving multicast packets due to handover, multicast membership protocol, multicast tree computation, and increased propagation delay to the new locations. In many cases, a mobile receiver is considered a new receiver after moving to a new IP foreign subnet, so it needs to re-join the multicast group. In such a situation, the mobile receiver should first discover the presence of the multicast router and wait for the next membership query message to express interest in receiving multicast traffic. Thus, the mobile host will experience an extra delay and cannot proceed to group communications instantaneously. For some time-sensitive applications, this increased latency is undesirable.

**Packet Loss:** The current Mobile IP specification does not provide mechanisms to enable local multicast sessions to support seamless handover. During the handover from one IP subnet to another, the MN needs to receive multicast packets unceasingly while moving. However, the handover is unpredictable and there is no forwarding mechanism for multicast traffic addressed to mobile members. Since multicast packets continue to be delivered to the previous foreign network after the mobile leaves, a mobile receiver may miss some multicast packets due to its movement. Multicast packet loss can also be caused by the scoping problem. When the multicast scope is restricted to a given IP domain, the macro-mobility of the multicast member will induce a multicast service disruption. A mobile receiver that is out-of-the-scope needs to “break” the boundary scope to continue receiving multicast data.

**Packet Duplication:** Multicast packet duplication can occur when a mobile receiver is receiving the same multicast data from different multicast router or base stations.

**Packet out of Order:** Due to the handover, the mobile receiver may receive its multicast packets out of order.

**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.
Mobile Source Problems

When an 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: Transparency is a major issue for mobile multicast sources [31–33]. When a mobile source moves from one IP network to another while it has an ongoing multicast session, it receives a new IP address (CoA) from the new visited network. Then the mobile source uses this CoA as a source address when sending multicast packets. Unfortunately, the new multicast router to which the source is attached cannot forward the multicast packets sent with this new CoA address until the receivers explicitly notify it. Without this notification, multicast data will not be forwarded downstream. Moreover, multicast receivers are not able to interpret the traffic coming from the new CoA as coming from the same source due to the address change. If handover transparency is ignored, multicast receivers and multicast routers will be in the wrong direction, especially when the SSM model is used. In the case of handover notification, this notification would need to be done periodically, so that new receivers will be informed about the source’s address change.

Reverse Path Forwarding (RPF): For a mobile multicast 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. Hence, any change of location and source address will invalidate the source-specific tree due to the RPF check test. The RPF check compares the packet source’s address against the interface upon which the packet is received. When the handover occurs, the mobile multicast source cannot use its HoA as the source address to route multicast packets from the foreign network due to the ingress filtering problem and the RPF check failure. So, the multicast routing states should be modified to reflect the new IP address and to avoid dropping packets due to RPF failure.

Packet Loss: During the migration from one source-specific tree to another due to the address change, the mobile multicast source might not send multicast packets unceasingly while moving. Due to tree migration, the multicast receiver may miss some multicast packets.

Multicast Scoping: When scoping is used after a handover, the mobile source can be out of the range of the multicast traffic distribution. The border router in the previous network to which the source was attached prior to the handover can filter incoming multicast packets and deny access to local multicast groups since the mobile source will be considered a foreign source. Hence, local receivers will not receive multicast data any more.

Source Active Problem: The inter-domain multicast branches have to be reconstructed whenever the source moves into a new domain. An extra signaling mechanism is also required by border multicast routers to exchange the new source’s address and to dynamically update their inter-domain multicast forwarding tables accordingly. Border multicast routers have to know permanently which are the active sources for all the served groups. For example, in the case of the Multicast Source Discovery Protocol (MSDP) [34], the mobility of the multicast source within a PIM-SM domain will cause a source active problem since the MSDP peers have to increase the source announcements by using source active messages to reflect dynamically the source’s address change.

Deployment Problems

As mobile multicast hosts may be highly dynamic, several deployment problems may arise, such as service pricing, service agreements between Internet Service Providers (ISPs), quality of service (QoS) assurance, interoperability, scalability, and security considerations. All these issues are out of the scope of this survey.

IP Multicast Solutions for Mobile Receivers

This section describes the behavior of an MN that is away from its home link and wants to join a given multicast group. The MN may already be a multicast member before its handover, as it may want to join the group for the first time. To do so, several solutions were proposed by the Internet research community to support one-to-many IP multicast with mobile receivers. We classify these solutions into four classes. The first class includes home subscription-based solutions, which use the home network infrastructure. The second class includes remote subscription-based solutions. With this sec-
IEEE Communications Surveys & Tutorials • First Quarter 2004

Advantages and Limitations: The advantage of the home subscription approach is its simplicity and the transparency of handover to the multicast operation since the mobile receiver does not need to re-join the multicast group whenever it moves from one foreign network to another. However, this approach suffers from triangle routing across the home network, which may increase the join latency. Moreover, tunneling via the HA incurs overheads at the home network. The other drawback of this approach is that it relies on a central point of failure, which is the HA. In the case where multiple MNs of the same HA want to join the same multicast group, the HA needs to establish one bi-directional tunnel per remote MN, duplicate it, and forward multicast packets to each one. This situation may lead to a congestion problem when a significant number of mobile receivers are within the same foreign network. The last main issue is that in the current specification of the Mobile IP protocol, there is no recovery mechanism on the HA side that ensures that the membership report message sent by the mobile receiver is correctly received by the multicast router, since this message is not explicitly acknowledged. In addition, an IPv6 mobile receiver should wait for the reception of a multicast query message from its HA before sending its report via the IP tunnel [15]. This requirement is needed to prevent the HA from being overwhelmed with unsolicited membership report messages.

Mobile Multicast Protocol
Overview: In order to adapt the Mobile IPv4 protocol so that it can handle multicast forwarding with adequate scalability, the authors in [21] have proposed a new approach called the Mobile Multicast Protocol (MoM). This approach introduces a new entity called the designated multicast service provider (DMSP) and uses a foreign agent entity. The key idea is to reduce the number of duplicated multicast packets on the HA side. Both the MoM and the home subscription approaches use the same procedure to join a multicast group. However, multicast data delivery between the home network and the foreign network is different. Instead of establishing one IP bi-directional tunnel per mobile receiver when an HA has several receivers within the same visited network, the MoM protocol uses a single tunnel between the HA and the FA. In return, the FA uses link-level multicast to complete the delivery. In the case where several HAs have their remote receivers with the same FA, MoM suggests that the FA selects one HA as a DMSP candidate for the given multicast group. The DMSP is an HA dedicated to all the membership-related issues and it is responsible for forwarding multicast packets via a tunnel to the FA on behalf of all the other HAs. As Fig. 6 shows, the FA entity on the foreign network chooses HA2 as the DMSP. Thus, it is not necessary for HA1...
and H A 3 to join the multicast group since their receivers M N 1 and M N 3 will receive multicast data from H A 2.

**Advantages and Limitations:** Compared to the home subscription approach, the MoM protocol solves the tunnel convergence problem. However, this protocol suffers from sub-optimal multicast routing since all multicast packets sent or received by a mobile receiver always traverse the home network. This solution also appears to be vulnerable to frequent handovers. When the mobile receivers of the selected D M S P move away from the foreign network, the rest of the mobile receivers of other H A s will be affected. As Fig. 6 illustrates, when M N 2 leaves the foreign network, the F A should select a new D M S P between H A 1 and H A 3, otherwise multicast traffic will be disrupted. This operation requires the F A to perform complicated management of D M S P selection according to the mobile receivers and the requested multicast groups. The efficiency of this approach is affected by the excessive overheads compared to the home registration approach on which MoM is based. In addition, it introduces the problem of “D M S P handover” [36]. As a consequence, this approach has two points of failure, the F A and the D M S P.

**Range-Based Mobile Multicast**

**Overview:** The Range-Based Mobile Multicast (RBM o M ) protocol is based on the Mobile IPv4 protocol and it aims to find an optimal tradeoff between shortest delivery path and low frequency of multicast tree reconfiguration [37, 38]. Compared to the home subscription approach, this solution adds a new architectural entity called the multicast home agent (M H A) in order to limit the bi-directional tunnel length between the H A and mobile receivers. The M H A is an H A or an F A except that it is configured with a fixed service range. The concept of service range is based on the hop distance between the H A and the M N. This protocol works as follows. The M H A is assigned to the H A if the mobile member roams between foreign networks within the service range; otherwise, the F A will become the M H A. Thus, the M H A changes dynamically according to the location of the M N. Compared to the MoM protocol, RBM o M uses the same concept as the D M S P entity [35] to avoid multiple tunnels resulting from different M H A s, which have receivers within the same F A.

**Advantages and Limitations:** The RBM o M protocol introduces significant complexity without obvious advantages. The key idea of using the M H A is to limit the functionality of the H A to forwarding only unicast packets. It is not clear if the concept of service range optimizes multicast routing path and reduces the join latency. In addition, the optimal service range is not given. According to [39], when the service range is reduced for optimal routing, the number of multicast tree reconstructions is increased since every M H A has the same service range. Besides, using the D M S P entity is doubtful, as discussed in the MoM section.

**Multicast Protocol With Dynamic Service Range**

**Overview:** The authors in [39] and [40] have proposed a new approach, which enhances the RBM o M protocol [37] in the Mobile IPv6 environment. Initially, the RBM o M was designed for the Mobile IPv4 protocol as discussed above. The main goals of this approach are to determine an optimal service range.
range and avoid service disruption. To do so, this approach uses the RSVP signaling mechanism and introduces three architectural entities. In addition to the MHA entity introduced by the RBMoM protocol, a second entity called the core source node (CSN) is proposed. The CSN is initially set to the multicast source node and it is responsible for delivering multicast packets. This approach also defines two parameters: the service range and the dynamic service range. The service range is maintained by the CSN and is defined as the maximum tunneling path length tolerated from the multicast source. When the source moves out of this scope, the multicast tree is reconstructed. The dynamic service range is defined as the maximum tunneling path length in terms of hop distance that satisfies the maximum tolerable transfer delay. This second parameter is maintained by each MHA and is used to control the multicast data transmission delay (Fig. 7).

To avoid long service disruption times, this approach employs the RSVP protocol and defines a third architectural entity called the boundary foreign agent (BFA). The BFA is an agent located at equal distance to the dynamic service range value away from an MHA. To eliminate the possible disturbance that is triggered by a handover procedure, the mobile receiver pre-joins the multicast group prior to the handover in a similar manner as that of the mobility support agent (MSA) [101]. As Fig. 8 shows, if the mobile receiver (MN) moves to the BFA, it sends a Join_multicast_group message to its neighboring access routers (AR1 and AR2). In response to the Join_multicast_group message, neighboring access routers send a Pre_join message to join the multicast group.

Advantages and Limitations: Compared to the RBMoM approach, the current approach reduces the number of multicast tree reconstructions and multicast service disruption time. On one hand, this architecture addresses some of the mobile receiver’s problems, such as service disruption and join latency. On the other hand, it modifies the basic functionalities of the mobile receiver and introduces three new architectural entities: MSA, BFA, and CSN. These new entities should be well defined and well placed. Movement prediction and discovery of these entities either by the mobile receiver or the mobile source are the major issues. Moreover, this solution is not compatible with existing multicast membership protocols since it introduces new membership control messages (Join_multicast_group, Pre_join and Release_join). In addition, it is unclear how these messages are used with RSVP signaling. As far as the application field is concerned, this solution seems to be suitable for intolerant and time-sensitive multicast applications, which need an absolute bound on multicast packet delay.

Comparison: We can compare the home subscription-based solutions by using some criteria such as tunnel convergence, join latency, and point of failure [42]. Table 1 shows that most of the proposed solutions have common limits such as non-optimal routing and long join latency. They also add complexity and modify the basic function of the HA, the FA, and the mobile receiver. Compared to all solutions, the RBMoM protocol attempts to eliminate the possible disturbance that is triggered by a handover procedure by using the pre-join mechanism. However, this protocol changes the philosophy of the Internet membership protocol since new membership control messages are introduced.

REMOTE SUBSCRIPTION-BASED SOLUTIONS

In this section we present solutions based on the remote subscription approach. For each solution, we outline its strengths and weaknesses and discuss whether or not it solves the relevant problems of the mobile receiver. Finally, we compare all the solutions in a similar manner as was done in the previous section.
Mobile IP Remote Subscription Overview: In order to receive packets sent to a given multicast group, a mobile receiver needs to first join that multicast group. With the remote subscription approach, the mobile receiver joins the multicast group via a local multicast router on the foreign network. To join a multicast group, an MN sends its membership report message to the local multicast router located on the visited network. The local multicast router intercepts this membership report message and joins the requested multicast group. Following this approach, the MN in Fig. 9 uses its CoA as the IP source address when sending its membership report message to the multicast router MR1. After handover to the foreign network 2, MN again sends a new membership report message to MR2 by using its new CoA. While the MR2 constructs a new multicast branch for the MN, the MR1 may tear down its multicast branch if it has no receivers. During the handover phase, the MN may miss some multicast data packets.

Advantages and Limitations: The remote subscription approach is particularly advantageous when the MN stays in the foreign network for a relatively long period of time. Whenever a mobile receiver moves to a new network, it needs to re-join again the multicast group. Compared to the home subscription approach, in this approach a mobile receiver can join the multicast group without waiting for the registration of its CoA. Thus, join latency is reduced and multicast routing is optimal [43]. However, this approach assumes that each foreign network contains an enabled multicast router. In other words, the remote subscription does not rely on the HA entity, but it is vulnerable to multicast service inactivity on foreign networks (Fig. 10).

Remote Subscription with Multicast Agent Overview: In [44], the authors have introduced the concept of the multicast agent (MA) for mobile members to enhance the remote subscription in the Mobile IPv4 context. The MA may be considered to be the coordinator of different FAs. In fact,
Figure 11. MMA protocol operation.

Overview: To reduce tree reconstruction overhead and optimize the route, the authors in [36] and [48] have proposed a new multicast protocol for the Mobile IPv4 environment. This protocol, called the Timer-Based Mobile Multicast Protocol (MMA), solves the problem of duplicated packets and avoids the disruption of the multicast service during the handover. However, it introduces complex data structure on the mobile member that has to update its MF value and change the form of its membership report message. Join latency may be reduced if somehow coordination exists between MAs prior to the handover. Finally, the discovery of the MAs is another crucial issue of this protocol.

Advantages and Limitations: Unlike the MoM protocol, the MMA protocol solves the problem of duplicated packets and avoids the disruption of the multicast service during the handover. However, it introduces complex data structure on the mobile member that has to update its MF value and change the form of its membership report message. Join latency may be reduced if somehow coordination exists between MAs prior to the handover. Finally, the discovery of the MAs is another crucial issue of this protocol.

Advantages and Limitations: Using the pre-registration mechanism prior to the handover reduces multicast packet loss and join latency. The other key feature of this solution is that pre-registration is simple and is built over UDP. However, movement detection and prediction are two major concerns for the protocol design [45]. This could potentially benefit from seamless handover work such as Fast Mobile IP [46]. Besides, the underlying link technologies may be able to provide such information. In all cases, substantial co-ordination is needed between the MAs of the old and new networks. In brief, this protocol may be suitable for wireless networks with adjacent cells.

Advantages and Limitations: This solution solves the tunnel convergence problem and avoids long tunnels. However, no procedure is described to select the MA entity and to determine its proximity to mobile receivers. In addition, the MA location would affect the performance of this approach. As a consequence, the MA entity constitutes the single point of failure of this approach.

Mobility Support Agent

Overview: To avoid disruption of the multicast communication of a mobile member, the authors in [41] have proposed a solution based on pre-registration. This solution defines a new IPv4 architectural entity called the mobility support agent (MSA). The MSA is a router located in the foreign network and is dedicated to the multicast pre-registration procedure. During handover, the mobile receiver triggers the pre-registration procedure immediately by sending a membership report message to the MSA in the new foreign network. Upon receiving the pre-registration message, the MSA sends an IGMP join message to the local multicast router and starts delivering multicast packets to the mobile receiver once the handover is accomplished.

Advantages and Limitations: The MSA maintains a list of multicast groups that have members in its service area. For each multicast group, the MSA maintains a list of FAs that have visiting mobile receivers. To handle mobile receivers, the MSA joins the multicast group on behalf of them and then tunnels the multicast packets to the corresponding FAs. A given FA delivers the multicast packets using local multicast to its local mobile receivers.

Overview: As we stated above, the pre-registration technique to minimize packet loss. On the opposite side, the authors in [47] have suggested an efficient multicast routing protocol called Multicast By Multicast Agent Protocol (MMA) that uses a forwarding technique between foreign networks instead of the pre-registration method. To do so, two multicast agents are defined. The first agent is called the multicast agent (MA), which joins the multicast group on behalf of mobile members. The second agent is called the multicast forwarder (MF), which is responsible for forwarding multicast data when the handover occurs and thus offers the reliability feature of the MMA protocol. For a given multicast group, each MA selects a single MF. Figure 11 illustrates an example of this solution. The mobile member MN joins the multicast group through the closer MA1. MA1 delivers the multicast data to the MN and configures the MF value with itself. Similarly, the MN stores the MF information. When the MN moves from Foreign Network 1 to Foreign Network 2, it sends its MF information and its membership report message to MA2. If MA2 is an on-tree multicast router prior to the handover, MA2 becomes the MF. Otherwise, MA2 sends the membership information to the upstream multicast router and compares its MF information if it exists with that of the MN to choose one optimal MF that is closer to Foreign Network 2. While setting the connection to the multicast delivery tree, MA2 establishes a tunnel to forward multicast data from the closer MF, which is, in this case, MA1. To establish the tunnel, MA2 and MF (MA1) exchange forwarding request and forwarding stop messages. The forwarding request message initiates the forwarding process of multicast data and the forwarding stop ends it.

Overview: To avoid disruption of the multicast communication of a mobile member, the authors in [41] have proposed a solution based on pre-registration. This solution defines a new IPv4 architectural entity called the mobility support agent (MSA). The MSA is a router located in the foreign network and is dedicated to the multicast pre-registration procedure. During handover, the mobile receiver triggers the pre-registration procedure immediately by sending a membership request message to the MSA in the new foreign network. Upon receiving the pre-registration message, the MSA sends an IGMP join message to the local multicast router and starts delivering multicast packets to the mobile receiver once the handover is accomplished.

Advantages and Limitations: Using the pre-registration mechanism prior to the handover reduces multicast packet loss and join latency. The other key feature of this solution is that pre-registration is simple and is built over UDP. However, movement detection and prediction are two major concerns for the protocol design [45]. This could potentially benefit from seamless handover work such as Fast Mobile IP [46]. Besides, the underlying link technologies may be able to provide such information. In all cases, substantial co-ordination is needed between the MSA s of the old and new networks. In brief, this protocol may be suitable for wireless networks with adjacent cells.

Advantages and Limitations: This solution solves the tunnel convergence problem and avoids long tunnels. However, no procedure is described to select the MA entity and to determine its proximity to mobile receivers. In addition, the MA location would affect the performance of this approach. As a consequence, the MA entity constitutes the single point of failure of this approach.

Mobility Support Agent

Overview: To avoid disruption of the multicast communication of a mobile member, the authors in [41] have proposed a solution based on pre-registration. This solution defines a new IPv4 architectural entity called the mobility support agent (MSA). The MSA is a router located in the foreign network and is dedicated to the multicast pre-registration procedure. During handover, the mobile receiver triggers the pre-registration procedure immediately by sending a membership report message to the MSA in the new foreign network. Upon receiving the pre-registration message, the MSA sends an IGMP join message to the local multicast router and starts delivering multicast packets to the mobile receiver once the handover is accomplished.
(TBMOM), is inspired by the MoM, RBMoM, and MFA protocols. However, this protocol tries to find a tradeoff between providing low tree reconstruction overhead and fast data delivery for mobile members. The TBMOM protocol selects a foreign multicast agent (MFA) to store the membership information of mobile members. The MFA is an enabled multicast FA located on the foreign network. During handover the mobile receiver dynamically selects a MFA. The MFA address may be piggybacked in the advertisement message. In the TBMOM protocol the mobile receiver uses the same mechanism to join the multicast group as that of the remote subscription. However, the mobile receiver is served differently depending on both its handover frequency and its speed. In fact, when a mobile receiver moves fast passing many foreign networks in a relatively short time, the mobile receiver is served with fast unicast tunneling between MFA s. Otherwise, the local FA joins the multicast group in a similar manner as in the remote subscription approach. While constructing a new branch on the multicast delivery tree, the MFA is responsible for serving the mobile member for a certain period of time. To achieve this, TBMOM introduces two timers: the join timer and the group timer. The mobile member keeps the join timer and the FA keeps the group timer. The join timer value is set to a pre-determined value that decreases and keeps turning around throughout the multicast session lifetime. When arriving at a new foreign network the mobile member registers its remaining join timer with the FA . The new FA sets its group timer to the smallest remaining join timer among those of all the visiting mobile members that requested to join the same multicast group. The new FA continues to receive tunnelled multicast data from the MFA until the group timer expires. When the group timer expires, the new FA becomes the MFA and joins the multicast group on behalf of the mobile member. It then informs all the mobile members within its service range of the change of the MFA.

Compared to the MoM protocol, the FA may select one MFA as a DMSP among the MFA candidates in order to avoid packet duplication. To launch the DMSP handoff process, the TBMOM protocol proceeds in the same manner as the MFA protocol. In fact, the FA sends a forwarding request message to the new MFA and a forwarding stop message to the old MFA. The mobile member itself can initiate this DMSP handoff if the current MFA of the mobile member is the optimal DMSP.

**Advantages and Limitations:** Compared to the remote subscription approach, the TBMOM protocol reduces multicast packet loss and tree reconfiguration overhead since unicast tunnels can be set between FMA s of different foreign networks. This protocol also solves the tunnel convergence problem by using the DMSP concept of the MoM protocol. However, it introduces complex data structures and depends on the speed of the mobile members. This speed parameter may vary from one network to another. In addition, the optimal join timer is not fixed since it depends on many parameters such as network topology, handover latency, and especially the speed of the mobile member.

### Hierarchical SSM-Based Approach

**Overview:** When a mobile receiver uses the remote subscription as the basis to join a multicast group, it cannot receive multicast data during the handover. That is why the authors in [49] have proposed a new solution based on SSM and the hierarchical architecture for the Mobile IPv4 environment. The solution consists of splitting the multicast path from the multicast source to the receiver into two levels. The first level is called the macro level, which is defined as multicast from the source to the border gateway router (BGR) in an autonomous system (AS). The second level is the micro level and it is defined as multicast from the BGR to the FA, which the mobile member is attached to. As shown in Fig. 12, the mobile member (MN) sends a source-specific request to subscribe to the (S,G) channel. The FA forwards this subscription request until it reaches BGR 1. After that, BGR 1 ignores this subscription request and sends a registration request message to the source. In return, the multicast source acknowledges the registration by sending back a registration reply message and stores the (S,G) state and the BGR 1 address in its cache table. The cache table is a new proposed data structure that contains the multicast group identifiers and the BGRs to which the source sends. After this step, the multicast source encapsulates and tunnels its multicast data packets to BGR 1, which decapsulates and sends them down the source-specific tree in its service area (micro level). When the mobile receiver moves to FA 2, which is located on AS 2, tree re-construction may be limited to the micro level, which helps to minimize multicast service disruption.

**Advantages and Limitations:** This solution is very similar to the remote subscription approach. Its main advantage is that join latency may be reduced if the BGR has already joined the multicast group. The BGR may be considered as a permanent on-tree router for mobile receivers that roam inside the same autonomous system.
MobiCast Protocol

Overview: The authors in [50] have proposed a new protocol to support mobile receivers roaming between small wireless cells. The new protocol, called MobiCast, attempts to minimize the re-computation of the multicast delivery tree and reduces packet loss when a mobile receiver crosses cell boundaries during a multicast session. Compared to the remote subscription approach, the proposed solution requires hierarchical mobility management and uses a new translated multicast address for each multicast group. The form and the description of the translated address are not given; however, it is stated that it is unique within a given domain. The other main difference between them is that the MobiCast protocol uses a buffering mechanism on the new visited network.

To hide the micro-mobility of the mobile receiver, the MobiCast protocol introduces a new architectural entity called the domain foreign agent (DFA). The DFA is a boundary multicast router located on the foreign network and it represents the mobile receiver in the multicast tree. As Fig. 13 illustrates, when MN wants to join the multicast group defined by the (S, G) pair, the DFA orders BS1 and BS2 to subscribe to the translated multicast group G'. BS1 and BS2 are two base station routers. When the MN is attached with BS2, it receives buffered multicast from it. Thus, DFA hides the handover of the mobile receiver within the foreign domain.

Advantages and Limitations: The MobiCast protocol makes the handover of a mobile receiver transparent to the multicast delivery tree. By using a translated multicast address and a buffering technique on leaf base stations prior to the handover, both multicast packet loss and join latency are reduced. However, unnecessary multicast traffic is always forwarded to adjacent base stations. This solution is thus suitable for a micro-mobility case with prior knowledge of the receiver’s mobility specification. The mobility specification is defined as the set of locations the mobile receiver is expected to visit during the lifetime of the multicast session.

Comparison: Similar to home subscription-based solutions, we can compare remote subscription-based solutions in light of join latency, point of failure, tunnel convergence, architectural entities, etc.

Table 2 shows that this second class of solutions has the advantage of offering the shortest routing path and the nonexistence of IP tunnels to deliver multicast data to mobile receivers. Some solutions, such as the hierarchical SSM approach and the MobiCast protocol, have attempted to improve route optimization and reduce the management of the multicast delivery tree when a mobile receiver is roaming within a given domain. These two solutions require hierarchical mobility management. In order to reduce multicast packet loss for highly mobile receivers, the MSA and the MMA schemes have introduced respec-
tively the concept of forwarding and buffering. These techniques are designed to compensate for the deficiencies of the remote subscription approach since an extra delay incurred from rebuilding a multicast delivery tree can create the possibility of a disruption in multicast data delivery. In brief, most of the proposed solutions that are derived from the remote subscription introduce significant changes to the basic functionalities of the mobile receiver, and this latter is no longer considered as a stationary receiver [42]. Compared to a stationary receiver, the mobile receiver requires additional signaling mechanisms to discover and authenticate the introduced multicast routing agents.

**HYBRID SOLUTIONS**

In addition to mobile IP-based solutions, new solutions have been proposed. The new approaches combine the architectural entities and the different multicast operations to benefit from their advantages, reduce join latency, and avoid packet loss during the handover. Here we describe some of these hybrid solutions. For each solution we outline its advantages and weaknesses and discuss in which scenario it can be applied.

<table>
<thead>
<tr>
<th>IP Mobility</th>
<th>Join latency</th>
<th>Point of failure</th>
<th>Hierarchical mobility</th>
<th>Tunnel convergence</th>
<th>Architectural entities</th>
<th>Comparison with RS(^1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile IP remote subscription</td>
<td>IPv4 and IPv6</td>
<td>Slow</td>
<td>FA in the case of Mobile IPv4</td>
<td>No</td>
<td>Does not use IP tunnel</td>
<td>FA and LMR(^2)</td>
</tr>
<tr>
<td>Multicast agent</td>
<td>IPv4</td>
<td>Slow</td>
<td>MA</td>
<td>No</td>
<td>One IP tunnel is established between an FA and the MA</td>
<td>FA, MLR, and MA</td>
</tr>
<tr>
<td>MSA</td>
<td>IPv4</td>
<td>Very slow since pre-registration is used</td>
<td>MSA</td>
<td>No</td>
<td>Does not use IP tunnel</td>
<td>MSA</td>
</tr>
<tr>
<td>MMA</td>
<td>IPv4</td>
<td>Very slow</td>
<td>MA and MF</td>
<td>No</td>
<td>One IP tunnel is established between a MA and the MF</td>
<td>MA and MF</td>
</tr>
<tr>
<td>TBMoM</td>
<td>IPv4</td>
<td>Slow</td>
<td>DMSP</td>
<td>No</td>
<td>Does not use IP tunnel</td>
<td>FA, FMA, and DMSP</td>
</tr>
<tr>
<td>Hierarchical SSM approach</td>
<td>IPv4</td>
<td>Slow</td>
<td>BGR</td>
<td>Yes</td>
<td>One IP tunnel is established between the multicast source and the BGR</td>
<td>FA and BGR</td>
</tr>
<tr>
<td>MobiCast</td>
<td>IPv4</td>
<td>Very slow since buffering is used</td>
<td>DFA</td>
<td>Yes</td>
<td>Does not use IP tunnel</td>
<td>DFA</td>
</tr>
</tbody>
</table>

1 RS: Remote subscription  
2 LMR: Local multicast router

**Table 2.** Comparison of remote subscription-based approaches.

**Dual Subscription**

**Overview:** The dual subscription approach aims to offer a smooth handover between the home subscription and the remote subscription approaches. This approach was proposed by [32]. The main objective of this approach is to minimize multicast packet loss in the mobile IPv6 environment. In this approach, a mobile receiver keeps a permanent home subscription with its HA and establishes a temporary remote subscription in the visited network. The home subscription is kept active by a new membership message called the MLD listener hold sent by the mobile receiver to its HA. When the handover is finished, it switches quickly from the home multicast tree to the remote one once it starts getting the first multicast data packets (Fig. 14).

**Advantages and Limitations:** This approach uses the same architectural entities as the home subscription and remote subscription approaches. However, the HA must remain a multicast of the group on behalf of the mobile receiver during the entire lifetime of the multicast session. While the MN registers a new CoA with its HA, some multicast packets may be tunneled from the HA to the old CoA prior to the arrival of the binding message. As a consequence, the home subscription is vulnerable to CoA
Changes, and the permanent subscription cannot survive without interruption of multicast service. The dual subscription inherits the limitations of the home subscription and it is not cost effective since mobile receivers need two multicast branches. The first branch is from the HA, whereas the second branch is established from the multicast router on the visited network. The maintenance of these branches per mobile receiver requires extra processing time. It will be more effective if the migration from the home multicast path to the remote is not simply based on multicast connectivity but also on the QoS requirements of the mobile receiver in terms of join latency and packet loss. For reliability purposes, the mobile receiver may require multiple migrations between the two trees.

**Mobile Multicast with Hierarchical Local Registration**

**Overview:** Solutions using the home subscription cannot be applied directly on a hierarchical model. That is why the authors in [51] have proposed an IPv4 model that supports multicast for this scenario. The proposed model uses hierarchical and local registration. This registration consists of having a root FA and lower FAs. The root FA is a new architectural entity that implements the functionalities of a basic FA and is located on the boundary of the foreign network. Lower FAs are simple FAs. While the MN is moving within the same IP domain, it registers its CoA with the root FA. All the FAs exchange summary reports that indicate the common multicast group of interest on the lower levels. Then, the root FA joins the requested groups on behalf of the mobile receivers. Compared to the dual subscription, the proposed model uses either the home subscription approach or the remote subscription approach. The remote subscription consists of distributing the burden of joining multicast groups among different strategically chosen FAs. These latter are called local multicast service providers (LMSP). To choose the LMSPs, the authors have proposed two approaches. The first one is a topology-based selection where the domain is divided into different hierarchical segments. On each segment an FA is assigned to be the LMSP and is responsible for joining multicast groups requested by lower FAs. The second approach is a selection based on the density of mobile receivers (density-based). The FAs on the bottom of the hierarchy send their summary reports to their higher FAs. Each FA indicates the count of mobile receivers within its service area. A threshold is fixed and a given FA in the higher level can be selected as a LMSP if the threshold is reached. Then the LMSP joins the multicast group on behalf of lower FAs.

To support the home subscription, the authors have proposed that lower FAs send upward their membership report messages to the root FA. The root FA selects one HA as the multicast service provider (MSP). Figure 15 shows that the HA of the mobile receiver MN1 is chosen as the MSP. This HA will be defined as the primary MSP, and it is designated HA_MSP. The root FA may select another HA as a secondary HA_MSP in order to avoid failure or bottleneck. Once the HA_MSP is selected, the root FA sends the join request to it. The HA_MSP joins the multicast groups and sends back the multicast data packets. The root FA forwards downward these packets to the lower FAs. Similarly, lower FAs send the received packets to the mobile receivers by using link-local multicast.

**Advantages and Limitations:** This approach attempts to combine both home and remote subscription approaches to benefit from the advantages they offer. The subscription is transparent to the mobile receiver; however, an extra cost is required to select the HA_MSP and to choose the LMSP entities. In addition, the identity of each receiver’s HA is exchanged between FAs.

**Mobile Multicast Gateway**

**Overview:** In [52] the authors have suggested a new alternative to solve the tunnel convergence problem. The key idea of their solution is that when a mobile receiver joins a multicast group by using the home subscription approach from the visited network, the receiver’s multicast connectivity may be used by a mobile multicast gateway (MMG) to serve other local receivers independent of their way of joining. The MMG is a multicast router with mobile IP functions. It is generally located on the boundary of the foreign network. The MMG gets multicast traffic on behalf of all FAs within the foreign network and manages the multicast operation in its region. To get multicast data, the MMG can either explicitly join a multicast group or receive multicast data implicitly from an HA that has a mobile receiver located within the foreign network. Hence, the MMG is considered a rendezvous point in the foreign network except that it can directly tunnel multicast data packets to mobile receivers. The MMG entity can also be located on the home network with responsible for checking all the membership control packets between a mobile receiver and the HA. However, no mechanisms are described related to how the MMG intercepts these packets. As Fig. 16 shows, MMG2 can join the multicast group G if it receives a join message from FA2. If we assume that FA1 is not an enabled...
multicast router, the mobile receiver M N 2 can join the multicast group by sending its membership report to its H A (H A 1). If M M G 2 is not already on the multicast delivery tree, it can obtain multicast data from M M G 1, which is located on the home network. Otherwise, M M G 2 ignores the membership report message from M N 1 and establishes a bi-directional tunnel with it on behalf of its H A.

Advantages and Limitations: The proposed solution introduces a new architectural entity to eliminate the tunnel convergence problem and optimize route efficiency. However, it is not explained how the M M G receives a copy of multicast data by intercepting multicast packets exchanged between a mobile receiver and its H A. Without an explicit notification between the mobile receiver and the M M G located on the foreign network, this interception seems to be difficult to realize. The other drawback of this approach is that it relies on the M M G entity, which constitutes the single point of failure.

**Mobile Multicast Proxy**

Overview: The authors in [53] have proposed a hybrid solution based on a new architectural entity called the mobile multicast proxy (M M P). The primary goal was to find a generalization of the Mobile IP solution and reduce packet loss after handover. A multicast proxy (M P) is similar to a designated router with respect to the P I M-SM definition. However, it is located outside the subnet of receiver or source. The M P is designed to forward multicast messages to its receivers using unicast, multicast, or limited scope broadcast. To prevent the overhead of encapsulation, the authors assume the forwarding M P replaces the multicast address with the receiver’s unicast (multicast/broadcast) address. Whenever a receiver changes its point of attachment, it must send a binding update message to its M P informing it of its new location. Depending on the location of the M P, the authors have defined and implemented three categories of proxies:

- **Home multicast proxy (H M P):** The H M P is located in the receiver’s home network. It is different from the H A and it allows mobile nodes to use their home addresses when sending to the multicast group.
- **Remote multicast proxy (R M P):** The R M P is located close to the rest of receivers, and may be located on the foreign network.
- **Foreign multicast proxy (F M P):** The F M P is located close to the receivers in the foreign network. When a mobile receiver moves from the domain of a given F M P to another, it requires discovering the new F M P.

Advantages and Limitations: Using multicast proxies is the best solution in a dynamic environment such as an army tactical environment. However, the authors do not describe how to locate a R M P and F M P. Different techniques similar to locating a core router in a core-based tree can be used to locate these architectural entities. The main shortcut of this approach is that mobile nodes require some modifications to discover these entities and additional signaling is needed between them.

**Logical Addressing and Routing Protocol**

Overview: The Logical Addressing and Routing Architecture (L A R) [54] is intended to provide efficient multicast communication for IPv6 mobile nodes. In addition to the IP routing address, the L A R protocol introduces a new type of address called the L A R address. This new logical address is used to identify logical network entities such as L A R routers and L A R nodes. Compared to the classic IP routing address, the L A R address remains unchanged despite the mobility of the L A R host. To use these addresses, two separate IP headers are required on the IP packet. The usual network level is the lowest one, whereas the L A R level is the second level.

To support IP multicast, the proposed architecture defines the L A R group. Every L A R group has a manager, which deals with the address group allocation. This manager may be the creator of the group and it is responsible for gathering membership information from all the members and advertising the name of the group and the associated logical address of the group. The L A R protocol uses a mechanism similar to Mobile IP to support IP multicast with mobile nodes. In fact, the mobile receiver maintains a L A R cache in which it stores the association between the L A R addresses of its neighbors with their usual routing IP addresses. When a mobile receiver wants to joins a group, it checks the logical address of the group and the address of the manager from the local D N S. Then it sends a membership query message to the manager. The manager acknowledges this membership and replies with a L A R_join message. The mobile receiver will receive the L A R_join message from its close neighbor. The close neighbor also sends its logical address to the mobile receiver and by this way a logical branch is constructed. When the handover occurs, the mobile node changes its usual IP address but not the L A R address. As a consequence, the mobile receiver can continue to receive multicast data during the handover. To
leave the group, the mobile receiver sends a LAR_leave message to its neighbor. This neighbor deletes the LAR entry of the mobile receiver from its LAR cache. Similarly, a mobile source sends data to the manager if it is not an on-tree member. If the source is a member, the multicast data is forwarded along the LAR tree.

Advantages and Limitations: The LAR architecture proposes a seamless multicast communication for mobile nodes with minimum packet loss. However, this architecture introduces a new addressing scheme and new complex data structure, which causes an interoperability problem with the existing IP infrastructure.

Comparison: The hybrid solutions use both the home subscription and remote subscription approaches with additional mechanisms and new architectural network entities. Table 3 summarizes our qualitative comparison.

### Table 3. Comparison of hybrid approaches for mobile receivers.

<table>
<thead>
<tr>
<th>IP Mobility</th>
<th>Join latency</th>
<th>Point of failure</th>
<th>Hierarchical mobility</th>
<th>Tunnel convergence</th>
<th>Architectural entities</th>
<th>Comparison with Mobile IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dual subscription</td>
<td>IPv6</td>
<td>Slow if remote subscription is used</td>
<td>HA</td>
<td>No</td>
<td>One bi-directional tunnel between the HA and the mobile receiver</td>
<td>HA and local multicast router</td>
</tr>
<tr>
<td>Hierarchical local registration</td>
<td>IPv4</td>
<td>Very slow</td>
<td>Root FA</td>
<td>Yes</td>
<td>Does not use IP tunnels</td>
<td>FA, HA, Root FA, HA_MSP</td>
</tr>
<tr>
<td>Mobile multicast gateway</td>
<td>IPv4</td>
<td>Very slow if the MMG is already added to the multicast tree</td>
<td>MMG</td>
<td>No</td>
<td>One bi-directional tunnel between the MMG and the mobile receiver</td>
<td>HA, FA, and MMG</td>
</tr>
<tr>
<td>Mobile multicast proxy</td>
<td>IPv6 and IPv4</td>
<td>Slow if the RMP and FMP have already joined the multicast group</td>
<td>HMP, RMP, and FMP</td>
<td>Yes if FMP is used</td>
<td>One bi-directional tunnel between a Multicast Proxy and a mobile receiver can be required</td>
<td>HMP, RMP, and FMP</td>
</tr>
<tr>
<td>LAR</td>
<td>IPv6</td>
<td>Slow</td>
<td>LAR manager</td>
<td>No</td>
<td>Does not use IP tunnels</td>
<td>LAR router, LAR manager and DNS server</td>
</tr>
</tbody>
</table>

Advantages and Limitations: The Efficient Explicit Mobile Multicast Routing Protocol (E2MMP) is an extension of the XMMP protocol described above. This protocol attempts to overcome the weakness of the XMMP protocol and support few-to-few multicast with mobile nodes. The other shortcut is that it introduces complexities and overheads on the HA and inherits the home subscription deficiencies in terms of point of failure.

### Explicit Multicast Protocol

Overview: In [55] the authors have proposed a new approach to support IP multicast when groups are of limited size. The proposed solution is based on Xcast, which requires that the source keeps track of the destinations and creates a packet header that contains a list of destination addresses. As a consequence, there is no need for multicast group membership and multicast routing protocols. The list of destination addresses is updated from the source to the destinations. The intermediate routers forward within their areas the packets with relevant IP addresses and remove the other irrelevant addresses. This procedure is done hop-by-hop until all the receivers are reached.

To support mobile multicast receivers, the proposed approach, Explicit Multicast Protocol (XMMP), uses Xcast-capable HA. The HA in Fig. 17 receives the Xcast packet from the source S on behalf of the mobile receivers MN1 and MN2. Then it looks up the CoAs bound with the HoAs listed in the Xcast packet (HoA1 and HoA2). Depending on the current location of the MNs, the HA separates the CoAs into small subset addresses, replicates the intercepted packet, and tunnels it to the CoA1 and CoA2. The CoA1 and the CoA2 match, respectively, the temporary addresses of MN1 and MN2.

Advantages and Limitations: This approach is not scalable since it may be practical for a small and closed/pre-established multicast group. The other shortcut is that it introduces complexities and overheads on the HA and inherits the home subscription deficiencies in terms of point of failure.

### Efficient Explicit Mobile Multicast Routing Protocol

Overview: The Efficient Explicit Mobile Multicast Routing Protocol (E2MMP) is an extension of the XMMP protocol described above. This protocol attempts to overcome the weakness of the XMMP protocol and support few-to-few multicast with mobile nodes. The key idea of this work is to use the CoAs of mobile receivers instead of their home addresses on the HA and the mobile receivers that are already joined the multicast group. The CoAs of mobile receivers that are not already joined the multicast group are required.
Advantages and Limitations: The advantage of this approach is that it reduces the path between the source and the receivers. Compared to XMIP, E²MMP significantly improves the delay. However, this approach does not use the traditional IP multicast model since it does not rely on any multicast membership protocol.

Explicit Multicast over Mobile IPv6 Overview: In [57] the authors extend the explicit multicast protocol for IPv6 (Xcast6+) to support mobile receivers. To do so, the Xcast6+ extension was integrated into the Mobile IPv6 protocol. The result of this combination is a new protocol named Explicit Multicast over Mobile IPv6 (X+MIPv6) that aims to maintain the optimal delivery path without multicast tree reconfiguration. This new protocol uses stateless multicast between mobile routers since the list of mobile receivers is updated in a hop-by-hop manner. Hence, a multicast receiver needs only to send a membership report message that contains the addresses of the source and the group to its local multicast router. The multicast router adds its own IPv6 address and sends the membership report message toward the source's multicast router. To send back multicast data, the multicast source sends its packets without specifying explicitly the IPv6 addresses of the receivers, but only the address of the multicast group. Since the source's multicast router maintains the list of all the leaf multicast routers that have mobile receivers within their subnets, it explicitly encodes the addresses of these routers by adding an Xcast6+ header. When a mobile node roams into a new visited network, it registers again with the multicast source by using a new message called registration update (RU). Simultaneously, the new multicast router in the visited network sends a RU message to the receiver's HA. In return, the HA updates its cache and forwards further Xcast packets to the new location. The forwarding through the HA is temporary since the registration update message will update the list of multicast routers in the cache table of the source's multicast router.

Advantages and Limitations: The advantage of this solution is that it offers optimal path and reduces the multicast packet loss. Compared to the XMIP protocol, X+MIPv6 incorporates the MLDv2 protocol. The X+MIPv6 is not scalable since the source's multicast router has to keep a long list of IPv6 addresses of leaf multicast routers that have interested members.

M-HBH Protocol Overview: The M-HBH protocol extends the Hop-by-Hop Protocol (HBP). This protocol is designed to handle the mobility of both multicast receivers and sources [58]. Instead of using a multicast destination address, M-HBH uses a recursive unicast addressing mechanism. Compared to explicit multicast addressing, the multicast packets have unicast destination addresses. These addresses are updated in hop-by-hop manner with respect to the multicast forwarding table entries. In this protocol, the multicast tree is composed of two trees: the control tree, which is formed by multicast routers that exchange control messages, and the data tree, which is used by multicast routers to deliver multicast data from the source. To update these trees, two multicast control messages are required: the traditional join message, and a new tree message used by the multicast source.

To handle the mobility of receivers, the mobile receivers have to send join messages through their HAs. Intermediate multicast routers extract the HoA and the CoA of the multicast receivers and update their multicast forwarding tables (MFTs). When a branching router (which was previously responsible for a receiver prior to the handover) receives the join message, it updates its MFT, creates a packet copy, and sends it to the receiver.
Advantages and Limitations: The advantage of this protocol is that it offers optimal routing but with an extra cost. In fact, two multicast trees coexist (i.e., control trees and data trees) and two types of multicast control messages have to be used (i.e., join messages and tree messages).

Comparison: The non-IP multicast-based solutions are designed for small multicast groups. The list of receivers may be constructed either by the source or multicast routers. When the source builds this list, it may reference either the H oA s as done by the X M IP protocol or the C oA s as in the E 2 M P protocol. In addition, these solutions require new membership and signaling protocols to update the list of receivers and construct the multicast branches.

IP MULTICAST SOLUTIONS FOR MOBILE SOURCES

The Internet community has made a great effort to support mobile receivers in multicast sessions, but less interest was given to the problem of mobile sources. The mobile source problems are more important, since the handover of the source may affect multicast group communication, while the handover of a receiver has a local and single impact on the receiver only. To clarify this point, we describe in this section the behavior of an M N that is away from its home link and wants to send data to a given multicast group. The M N may already be a multicast source before its handover, as it may want to send to the multicast group for the first time. Compared to the solutions of the mobile receivers, we classify the multicast solutions for mobile sources into three classes. A s shown in Fig. 19, the first class includes home-based approaches in which the mobile source uses its H oA . The second class includes remote-based approaches in which the mobile source sends multicast data from the visited network. The last hybrid class combines the two previous classes. In the last section, we compare all the solutions using common criteria and the source’s issues such as handover transparency, IP mobility, R PF check, etc.

Mobile IP Bi-directional Approach

Overview: In order to send packets to a given multicast group, an M N does not need to join that multicast group. With the M obile IP bi-directional tunnel approach (applicable for both the M obile IPv4 and the M obile IPv6 protocols), the mobile source can send its multicast data to the multicast group by using its home network infrastructure. Following this approach, when the mobile source is away from home, it uses its C oA as the source address to tunnel the multicast packets to its H A . The enclosed data contains the H oA as the source address and the multicast group address as the destination address. In return, the H A decapsulates the tunneled packets and forwards the enclosed data to the multicast delivery tree.

Advantages and Limitations: This approach does not offer the optimal multicast routing operation since it suffers from triangle routing across the home network. Furthermore, this approach is inefficient in packet delivery, wastes system resources of the H A entity, and results in long service latency. However, it preserves the transparency of the handover of the mobile source. The source-specific tree will always be built with reference to the H oA and not the C oA . Consequently, the entire multicast delivery tree is rooted in the source’s home network and there is no need to reconstruct it whenever the handover of the source occurs.

Mobile IP Remote Approach

Overview: With the remote approach, the mobile source can use the foreign network infrastructure to send multicast data to the multicast group and thus avoid triangle routing across the home network. To do so, the mobile source uses its current C oA as the source address to send multicast packets to the local multicast router, which forwards them to the multicast delivery tree. Hence, the multicast delivery tree will be built with routing states that use the C oA and not the H oA , as in the bi-directional approach.

Advantages and Limitations: The main issue with the remote approach is that both multicast routers and receivers should be able to interpret the traffic coming from a new C oA as coming from the same multicast source. In addition, the multicast routes should be updated to optimize the multicast routing paths and to avoid dropping multicast packets coming from the source’s C oA since the R PF check will fail if the H A is used. As a consequence, the entire source-specific tree has to be reconstructed. Waiting for such reconstruction, the mobile source cannot send data immediately, which leads to multicast disruption [59].

SSM Source Handover Notification Approach

Overview: To support mobile multicast sources in M obile IPv6 with source-specific multicast, the authors in [32, 60] have suggested adding a new sub-option to the basic IPv6 binding destination option. The new option is called SSM source handover notification and it is used to notify the multicast receivers to subscribe to the new channel when the handover occurs. When the mobile source moves into a new foreign network, the mobile source receives a new C oA (nC oA ), which is different from the old C oA (oC oA ). To avoid multicast disruption, the mobile source sends a binding update message, which contains the source handover notification sub-option, to all the receivers to inform them about the nC oA . Simultaneously, the mobile source sends natively multicast data by using its nC oA . Upon reception of this explicit notification from the old multicast delivery tree rooted on the previous foreign network, multicast receivers initiate the reconstruction of the new source-specific tree by sending new M LD membership report messages that specify the nC oA instead of the oC oA . A s a consequence, a new multicast delivery tree will be built, and it will be referenced by (cC oA , G ) states instead of (oC oA , G ) states.

Figure 19. IP multicast solutions for mobile sources.
In this section we compared all the solutions option called. As mentioned above, sending messages back to the source.

Table 4. Comparison of non-IP multicast based approaches.

<table>
<thead>
<tr>
<th>Approach</th>
<th>Protocol</th>
<th>Construction of the list of receivers</th>
<th>Point of failure</th>
<th>Tunnel convergence</th>
<th>Architectural entities</th>
</tr>
</thead>
<tbody>
<tr>
<td>XMIP</td>
<td>IPv4</td>
<td>The list is constructed by the source</td>
<td>HA</td>
<td>One tunnel for all MNs</td>
<td>HA, Xcast routers, and multicast source</td>
</tr>
<tr>
<td>E2MMP</td>
<td>IPv4</td>
<td>The list is constructed by the source</td>
<td>Multicast source</td>
<td>Does not use IP tunnel</td>
<td>Multicast source</td>
</tr>
<tr>
<td>X+MIPv6</td>
<td>IPv6</td>
<td>The list is constructed by multicast router in hop-by-hop manner</td>
<td>The source’s multicast router</td>
<td>Does not use IP tunnel</td>
<td>Xcast+ router</td>
</tr>
<tr>
<td>M-HBH</td>
<td>IPv4 and IPv6</td>
<td>Constructed by multicast routers</td>
<td>Branching multicast router</td>
<td>Does not use IP tunnel</td>
<td>HBH routers</td>
</tr>
</tbody>
</table>

Advantages and Limitations: This approach is straightforward. However, it is not clear how the movement 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. In addition, the handover of the mobile source induces a reconstruction of the entire source-specific tree and requires mobility-aware receivers since they have to process IPv6 destination options (i.e., binding update, home option, and source handover notification sub-option). Receivers have to be kept informed about each change of the source’s address and to modify routing states in sympathy with such change.

PIM-SM with RPF Redirect Message

Overview: In PIM-SM [5], when a mobile source starts sending multicast packets from the foreign network, it uses its CoA. The multicast designated router (DR) to which the source is attached must deliver each packet to the rendezvous point (RP) for distribution down the RP tree. The source’s DR initially encapsulates each data packet and unicasts it to the RP by using a register message. The DR uses its wide reachable IP address to send the register message. The RP decapsulates each register message and forwards the enclosed data packet natively to downstream members on the shared RP tree. To stop the encapsulation and decapsulation operations, the RP builds a source-specific branch with the source’s DR. This branch will be identified by (CoA, G) states. Similarly, leaf multicast routers can switch to the source path tree (SP tree) to optimize multicast routing.

When the source moves to a new foreign network, all the previous operations should be repeated. Particularly, leaf multicast routers need to re-switch again to the new SP tree if they are aware of the source’s CoA. Otherwise, they will be in the “wrong direction” and the multicast session will be disrupted.

To overcome this problem, the author in [33] has suggested extending the register message to inform the RP not to send PIM join messages back to the source’s network and hence avoid wasted PIM join and register-stop signaling. However, no mechanism is described to reach this goal. The author also introduced a new IPv6 hop-by-hop option called RPF redirect option. This option is used to update the RPF check point between the source’s DR in the old foreign network and the DR of the new visited network and bypass the RPF check. The old DR needs to send a RPF redirect message down the multicast tree to first seek out the crossover router. The crossover router is the intersection of the old DR’s path and the new DR’s path. The RPF point of the crossover router should be set to the new DR before starting data transmission. The RPF redirect message aims to inform the leaf DRs to substitute the (HoA, G, <OldDR) state by the (HoA, G, <newDR) state.

Advantages and Limitations: This solution attempts to solve the RPF check failure problem in case of PIM-SM. However, it introduces an expensive signaling and state refresh mechanism. Moreover, the location of the crossover router is dynamic and the format of the PIM-SM join message should be modified.

Framework for Handling Mobile Source

Overview: Compared to the home subscription and remote subscription approaches, the authors in [31] have proposed a framework that supports multicast over Mobile IP when the mobile host is a sender as well as a receiver for a multicast group. This framework is designed for Mobile IPv4 entities and is based on a bi-directional tunnel between the HA and the FA (foreign agent). The FA and the HA keep track of the identifier (ID) of the multicast packets sent by the mobile source. In case the mobile node is also working as a sender for the group, the proposed solution takes an optimistic approach. Until the mobile source gets a “greet ack” message from the FA, the mobile source sends unicast packets to its HA. The greet message is a registration message that contains the ID of the last multicast packet received and the multicast group address. Once the source receives a “greet ack” message, it starts sending multicast packets through the FA reverse tunnel.

Advantages and Limitations: As mentioned above, sending from the foreign network is optimal, but the change of the source’s address causes overhead due to frequent reconstruction of the complete multicast tree.

Comparison: In this section we compared all the solutions proposed to handle the mobility of the multicast source. The comparison is based on the following criteria: the transparency of the source’s handover, IP mobility, the architectural entities, and the RPF check. As Table 4 shows, the handover of the multicast source is only transparent to the multicast operation only when the home subscription approach is used. Otherwise, additional mechanisms such as the handover notification and the RPF redirection are required to hide the source movement (Table 5).

Conclusion

In this survey we discussed many of the operational features associated with mobile multicast after providing an overview of Mobile IPv6/IPv4 and IP multicast. We first introduced different components in a gradual manner. Then we presented details about multicast issues and approaches that have been investigated so far. We classified the mobile multicasting
Table 5. Comparison of multicast solutions for mobile source.

<table>
<thead>
<tr>
<th></th>
<th>IP Mobility</th>
<th>Handover transparency</th>
<th>RPF problem</th>
<th>Architectural entities</th>
<th>Comparison with Mobile IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home subscription</td>
<td>IPv4 and IPv6</td>
<td>Yes</td>
<td>No</td>
<td>HA</td>
<td>—</td>
</tr>
<tr>
<td>Remote subscription</td>
<td>IPv4 and IPv6</td>
<td>No</td>
<td>Yes</td>
<td>FA, local multicast router</td>
<td>Uses the remote approach</td>
</tr>
<tr>
<td>Handover notification</td>
<td>IPv4 and IPv6</td>
<td>No</td>
<td>No</td>
<td>Multicast source</td>
<td>Uses the remote approach</td>
</tr>
<tr>
<td>RPF redirection</td>
<td>IPv6</td>
<td>No</td>
<td>No</td>
<td>PIM-SM rendezvous point, RPF crossover router</td>
<td>Uses the remote approach</td>
</tr>
<tr>
<td>Hybrid solution</td>
<td>IPv4</td>
<td>No</td>
<td>Yes</td>
<td>HA and FA</td>
<td>Uses the home approach and the remote approach</td>
</tr>
</tbody>
</table>

issues as well as the corresponding proposed solutions into different classes based on the nature of the multicast members (sources or receivers) and the way the network infrastructure is used.

We believe that the provision of multicast services to mobile nodes is a challenging problem, and several issues emerge with most proposed solutions due to the problems introduced by the mobile handover. Most of the proposed solutions attempt to enhance the support of multicast with either mobile receivers or mobile sources by combining the advantages of the home subscription and remote subscription approaches without providing a global architecture. These solutions seem to be hardly deployable in very large networks since they rely on newly introduced architectural agents [43]. In addition, the exact mechanisms used by a mobile receiver are usually not described.

To overcome the above problems, we propose that any suggested solution for mobile multicast should satisfy the following requirements.

- **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.
- **Mobility transparency:** The 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.
- **Mobility-independent:** The IP multicast routing entities should be independent of the IP mobility entities (e.g., HA, FA, etc.). It is not necessary that these entities are co-located.
- **Compatibility:** The solution should interoperate with existing Internet membership and routing protocols.
- **Security:** Exchanging the membership information and the security keys should be efficient and well protected. The impact of the handover on security issues should be minimized.

Given the dynamics of mobile members, mobile multicast solutions must be able to cope with these dynamics efficiently while at the same time yielding good performance and requirements assurance. Whichever multicast data delivery method is used for mobile nodes, there is an urgent need to keep mobile nodes simple. In addition to these issues, there are also concerns about protocol complexity, practicality, and communication performance. Particularly, great attention should be paid to the impact of mobile multicast protocol on the communication performance of a mobile node since the battery resources of mobile devices are generally scarce. Moreover, significant research effort is needed to evaluate the complexity and to simulate the performance of all the described solutions in terms of multicast tree reconstruction overhead, protocol signaling cost, packet loss, and join latency. For this purpose, the extension of the current network simulators and the use of mathematical approaches to model mobile movement, multicast membership [61–64], and tree structure and size [64, 65] are recommended. Queuing and graph theories may be helpful to reach this goal. In addition, protocol implementation, conformance tests, and the building of realistic testbeds are crucial to these performance and practicality issues.

We also believe that many-to-many mobile multicasting applications are becoming more popular and interesting to mobile users [66]. An effort is also required to couple IP multicast with mobile routing entities such as mobile routers [67] to take into consideration the movement of a set of users. This perspective has to be considered in order to deploy IP multicasting in IP mobile networks.

**ACKNOWLEDGMENTS**

Our first and most heartfelt thanks go to Martin Reisslein and to the anonymous reviewers who took time out of their busy schedules to send pertinent comments and feedback about this work. Without their concise and constructive criticism, this survey would not have been achieved. Next, a note of gratitude to the folks at the Research Center of Motorola at Paris and at the University of Technology of Compiegne for their help and encouragement.

**REFERENCES**

ADDITIONAL READING


BIographies

IMED ROMDHANI (Imed.Romdhani@motorola.com) is a Ph.D. student and research engineer at Motorola Labs-Paris, and a member of the networking team of the HeuDiaSyc Laboratory of the University of Technology of Compiegne (UTC), France. He received an engineer diploma in computer sciences from the National School of Computer Sciences (ENS), Tunis, Tunisia in 1998, and a M.Sc. in networking from the Louis Pasteur University of Strasbourg (ULP), France in 2001. His current research interests include multicasting, wireless networks, mobile IP, and QoS.

MOUIN KELLIL (Mouin.Kellil@motorola.com) is a Ph.D. student and research engineer in Motorola Labs-Paris, and a member of the networking team of the HeuDiaSyc Laboratory of the University of Technology of Compiegne (UTC), France. He received an engineer diploma in computer sciences from the University of Science and Technology Houari Boumediene (USTHB), Algiers in 1998, and a M.Sc. in networking from the University of Versailles (UVSQ), France in 2001. His current research interests include multicasting, wireless networks, Mobile IP, wireless security, and multicast security.

HONG-YON LACH (Hong-Yon.Lach@motorola.com) received a BS degree in computer science, with a minor in economics, in 1987 from the American University of Paris, France. He is currently
managing a team of researchers at Motorola Labs-Paris, working on IP-based mobile multiparty multimedia networking. He has extensive experience in the research and development of OSI and IP communication protocols. He is a contributor to standardization projects, including ETSI Project HIPERLAN Type 1, ETSI Project MESA, and IETF. He also participates in many EU projects in the ESPRIT, ACTS, FP5, and FP6 programs.

ABDELMADJID BOUABDALLAH (Bouabdal@utc.fr) received the engineer diploma in computer science from the University of Technology of Algiers (USTHB) in 1986, and received the Master (DEA) degree and Ph.D. from the University of Paris-sud Orsay (France) in 1988 and 1991, respectively. From 1992 to 1996 he was assistant professor at the University of Evry-Val-d’Essonne, France. Since 1996 he has been a professor in the department of computer engineering at the University of Technology of Compiègne (UTC), where he leads the networking and optimization research group. His research interests include Internet QoS and security, unicast/multicast communication, and fault tolerance in wired/wireless networks and distributed systems.

HATEM BETTAHAR (Hatem.Bettahar@utc.fr) received the M.S. degree and Ph.D. degree in computer science for work on multicast routing and QoS in IP networks from the University of Technology of Compiègne (UTC), France in 1998 and 2001, respectively. Since 2001 he has been an assistant professor in the department of computer engineering at UTC. He is a member of the networking and optimization research group within the Heudiasyc UMR-CNRS-6599 Laboratory. His research interests include Internet QoS routing, multicast communication, multicast security, and Mobile IP.