(Invited to appear in *Journal of Computers*)

IP Multicast Support in Mobile Internetworks

Kuang-Hwei Chi   Chien-Chao Tseng[1]   Ting-Lu Huang

Department of Computer Science and Information Engineering
National Chiao Tung University
1001 Ta-Hsueh Road, Hsinchu, Taiwan 30010
E-mail: {cctseng, chikh, tlhuang}@csie.nctu.edu.tw

Abstract

Multicasting is widely used for information dissemination, which is one of the most important facilities for constructing reliable distributed systems and cooperative applications. The current trend towards mobile computing has driven the research community to integrate multicasting and user mobility into the Internet architecture. This paper investigates alternative approaches to supporting network-layer multicast for mobile hosts. The basic idea behind each respective scheme is described. We then discuss issues and pragmatic considerations pertinent to each approach.

1 Introduction

Multicasting is a useful technique that disseminates information from a single site to a set of destinations. A basic motivation for using multicast is resource conversation via sharing: instead of transmitting information from a sender to each receiver separately, one can arrange for links that are shared to carry the data only once. A multicast delivery path is realized as a tree rooted at the sender with a receiver at each leaf. Paths in the tree diverge and the message delivery is parallelized to the destinations along the branches of the tree. Typical multicast applications include stock trading, teleconferencing, coordinating updates to replicated file systems [8], constructing fault-tolerant distributed systems [19], etc.

---

[1] Responsible for all correspondence. Phone: +886-3-5731867; Fax: +886-3-5724176.

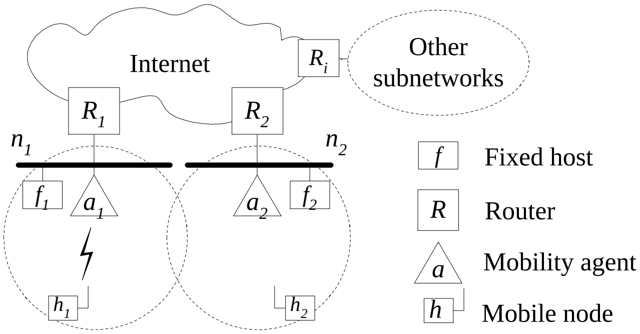


Figure 1: A model of mobile internetworks.

Given the prevalence of portable computing devices and the current trend towards ubiquitous computing, mobile users should be capable of accessing information to the Internet anywhere and at anytime. This leads to the development of wireless Internet, where hosts can roam around freely while retaining networking connectivity over a wireless medium via some fixed processing units. To support seamless communication and transparent routing for mobile hosts, Internet Protocol (IP) has been extended to hide mobility from the transport service.

This article describes proposals for integrating network-layer multicast and mobility into the Internet architecture. We first present IP extensions for host mobility and other extensions for multicasting. We then examine local multicasting mechanisms and protocols for delivering multicast datagrams in a wide area network. Next, alternative designs for supporting multicast for mobile hosts are described. Last, we draw remarks on their applicability and performance considerations.

2 IP Mobility

Host mobility support has been introduced in Internet Protocol [27]. This protocol, known as Mobile IP, allows mobile hosts to change their points of attachment to the network without losing connectivity at the transport layer. As shown in Figure 1, a mobile node (MN) is a host or a router that may move around while retaining accesses to the Internet over a wireless medium. Each MN has a permanent IP address, namely *home address*, on its home network. To support seamless communication, on each local network, there needs to be a router called mobility agent, or agent for short, that acts as a point of attachment to the system for MNs. An agent is said to be the home agent of the MN if the agent has a network prefix matching that of the MN's home address, or a foreign agent otherwise.

Upon movement into a foreign network, a mobile node obtains a *care-of* address from the foreign agent and registers the new address with its home agent. The care-of address indicates the MN's current location and is generally the foreign agent IP address. Datagrams sent by the MN use the foreign agent as a default router and are delivered to their destinations by standard routing mechanisms. In contrast, datagrams meant for the MN are forwarded by the normal routing mechanisms to the MN's home network, where they are intercepted by the MN's home agent. The home agent then encapsulates the datagrams within new IP datagrams directed to the MN's current care-of address. On receiving these datagrams, the foreign agent decapsulates and delivers them to the destination node. The method of encapsulating datagrams to work around normal IP routing is known as *tunneling* in the literature.

Alternatively, on a foreign network an MN may acquire a co-located care-of address locally. In this case, the mobile node itself needs to performs datagram encapsulation and decapsulation. This could cause heavy power consumption on the MN and therefore less preferred for practical use.

Multicast datagram routing may depend upon the IP source address, rather than upon the IP destination address as in unicast routing. Care must be taken when a mobile node sending multicast packets on a foreign network, or they will be dropped otherwise. As an option in Mobile IP, a mobile node under this circumstance is suggested to use a co-located care-of address as the IP source address. This option, however, might result in ambiguity for recipient nodes to determine which particular host originates the multicasts, if the sending host changes its source address from network to network. Such ambiguity can be avoided by using the other option described in Section 4.

3 IP Multicasting

IP multicasting is based on the host group model [14], where a dynamic set of hosts are identified by a single class D IP address, ranging from 224.0.0.0 to 239.255.255.255. There are no restrictions on the physical locations or the number of members in a group. A host may be a member of more than one multicast group and does not need to belong to a group to send datagrams to a given group. To deliver multicast datagrams, multicast-capable routers, i.e., *multicast routers*, are introduced for group management and Internet-wide delivery service, as described in the two subsections below.

3.1 Group Management and Local Multicast Delivery

Multicast routers learn which groups have members on each of their attached subnetworks, using the Internet Group Management Protocol (IGMP) [17]. Each local network designates one multicast router, if any, as the group manager. This router periodically transmits query messages in its administered areas, as shown in Figure 2. In response, local hosts send a report message for each group to which they belong, within a specified period. (When a host first joins a group, it transmits a report for the group rather than waiting for a router query.) If a host wishing to leave a group was

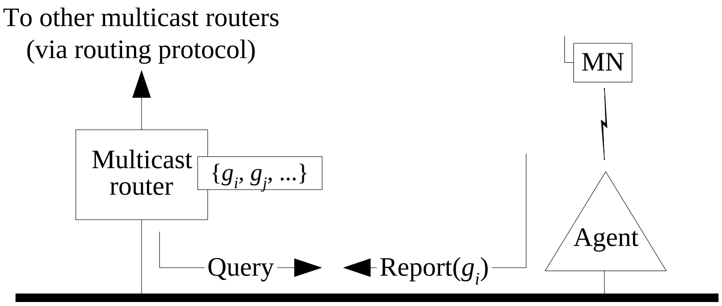


Figure 2: Group management on a local network.

the last host that replied to an IGMP query with a membership report for that group, it initiates a *leave-group* message. This causes the local router to send a group-specific query onto the subnetwork. If no reports are received within 10 seconds, the router removes the group and will not forward remotely-originated multicasts for that group onto the subnetwork.

IGMP and local multicast delivery architecture were designed for Ethernet-based networks, where packets are broadcast on the physical medium, so *native* multicast is available. IGMP queries are multicast to an address to which everyone is listening and each report is sent to the multicast address in question. The router and all local hosts can thus overhear IGMP messages, so the router can learn of the need for the group and other members can suppress their reports. In this manner, a multicast router need only record the presence of a group on each attached subnetwork rather than the detailed knowledge of its recipients.

IGMP provides the final step in a multicast packet delivery service since it is only concerned with the forwarding of multicast traffic from the local router to group members on directly attached subnetworks. In conjunction with IGMP, a multicast routing mechanism is responsible for the construction of multicast delivery trees and perform multicast packet forwarding, to support an Internet-wide delivery service.

3.2 Multicast Routing Mechanisms

Multicast routing offers a significant paradigm change from unicast routing. In contrast, routing decision are made based on the destination. Conversely, multicast routing decision are based on the source. A router will look at the source of the traffic and determine which network interface is closest to the source. This is called a Reverse-Path Forwarding (RPF) check. Each router, from receiver to source, will perform RPF checks to determine the best path to the source.

Several routing protocols are in common use or in some stage of development [2]. For the rationale and deployment of such protocols, we refer the reader to [**?**, **?**, 30].

Effectively a multicast route in the form of a spanning tree is established to locate all participant hosts of a group. Joining a group means that a user must be *grafted* into the tree. The existing routing protocols are capable of seamlessly providing both (join) graft and leave (prune) functions.

Multicast routing protocols can generally be classified into two categories, sparse mode and dense mode. Dense mode assume that most subnetworks in the system will be interested in multicast traffic. To inform other routers of multicast sources, it floods the traffic to all routers in the network. A router without recipients in this traffic will then tell its upstream router to stop forwarding multicasts or to prune this branch from the tree, as illustrated in Figure 3. This mechanism allows these protocols to establish a multicast distribution tree rooted at each source per group. A source-rooted tree guarantees the shortest and most efficient path from source to receivers. While this could be ideal for enterprise or corporate intranets, the reliance on broadcast and flooding across the Internet will not scale. Examples of dense mode protocols are Distance Vector Multicast Routing Protocol (DVMRP) [14, 28], Multicast Open Shortest Path First (MOSPF) [24], and Protocol-Independent Multicast Dense Mode (PIM-DM) [15].

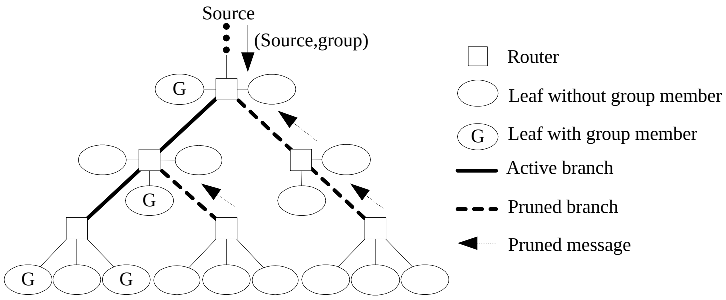


Figure 3: Broadcast and prune operations, where prune messages travel toward upstream from leaf routers.

Sparse mode protocols employ a shared distribution tree. Here, the multicast distribution tree is rooted at a core router in the network called a *rendezvous point* (RP.) When a source begins actively sending multicast traffic, its directly connected router registers with the RP. The RP will keep track of all active sources in a domain. When a host wishes to receive a multicast group, the local router issues explicit requests towards the RP to join the group tree, and will use RPFs to determine the shortest path to the RP. While the RP builds a tree to the source, all receivers join the tree at the RP. As long as all routers know which router is the RP, broadcast is not needed to distribute multicast route information. Additionally, this limits the amount of routing state that all non-RP routers need to know. Protocol-Independent Multicast Sparse Mode (PIM-SM) [15] and Core-Based Trees (CBT) [7] are examples of a sparse mode routing protocol.

Multicast routing protocols construct distribution trees by examining a unicast reachability protocol's routing table. It is desirable that a multicast routing protocol should be able to use any underlying unicast routing protocol to build the multicast distribution tree. Protocol-Independent Multicast Sparse Mode serves as a popular choice, since group members could be widely dispersed, as might be the case for most multicasts in the Internet. Indeed, PIM flexibly supports and provides the primary benefits of both sparse and dense mode functions. PIM-SM allows a router to switch from the RP-based tree to a source-rooted tree if traffic levels reach a configured threshold, say zero. This means that a router with a directly connected receiver will initially build a tree to the RP. After receiving the first multicast packet, it will switch to a tree rooted at the source.

4 Multicasting Schemes for Mobile Hosts

In a mobile environment multicast delivery paths tend to be transient in nature and may need to adapt accordingly when participants move. It is nontrivial to restructure the paths along with host movements all the way because a large number of multicast routers could be involved for update. Also, message delivery within a group can be disrupted because multicast delivery paths can become obsolete upon host migrations. Hence most of the previous schemes avoid adjusting multicast routes to group members' locations, by hiding host mobility from multicast tree constructions.

4.1 Acharya's Approach

A scheme in [1] treats the Internet to consist of campus networks, where an abstraction of link-layer connectivity among all agents on a campus is simulated. In other words, each multicast packet is forwarded to all the agents, resulting in campus-wide broadcast. Therefore mobile nodes are able to receive multicasts without modifying multicast routes upon each move.

This approach operates as follows. When a datagram is multicast from an MN, the local agent of the MN encapsulates the datagram and sends it to all other agents on the campus. Each agent then forwards a copy of this datagram to its wireline interfaces as dictated by DVMRP, and a copy to its wireless interface if it serves some mobile members. If an MN is a multicast recipient, all agents on the campus will be kept on the multicast trees for the group. For this, each agent sends IGMP queries to MNs in its coverage area, collects the group-specific membership reports locally, and then sends its reports to all other agents. As a result, even if none of its local MNs belong to a group, an agent does not prune itself from the multicast trees as long as any MN within the campus remains in the group. In this manner, a mobile member can receive its multicast traffic of interest within the campus. However, as a framework designed for an obsolete version of mobile Internet protocol [20], this scheme is less popular nowadays.

4.2 Mobile-IP Multicast Options

The current standard Mobile IP specifies two multicast options [27, pages 119-120]. A mobile node at its home subnetwork functions identically to any other fixed host. Thus this subsection describes the behavior of a mobile host that is residing on a foreign subnetwork.

An option is that a visiting MN uses a co-located care-of address to conduct multicast message delivery. Hence the mobile node acts as a local host participating in group communication. This technique, also known as *remote subscription*, allowing subscription on the foreign subnetwork, is a simple leverage for obtaining multicast service since it operates using only existing protocols. This method is beneficial when communication delay is crucial, or mobile hosts are likely to be stationary for a long period of time. Remote subscription provides efficient delivery of multicast datagrams, but may come at a high price for the networks involved in managing multicast routes. The system could suffer from frequent multicast route reconstructions, especially when group members are highly mobile.

Alternatively, the other multicast option in Mobile IP builds delivery paths as if mobile members were always situated at their home subnetworks. Each mobile host maintains a bi-directional tunnel with its home agent via which multicasts are sent and received. This approach tackles the problem of topologically incorrect source addresses in datagrams by requiring traffic from the mobile hosts to be routed back to home through a foreign agent to home agent tunnel. When forwarding messages to a mobile host, the home agent first encapsulates the multicast datagram in a unicast packet destined for the host. Then the packet is encapsulated again and sent to the foreign agent care-of address (Figure 4a.) The foreign agent will decapsulate the received datagram and, after examining the inner packet header, will know to whom the message is intended. On the contrary, multicast datagrams by the visiting host are encapsulated and unicast to the home agent, from where normal multicast routing

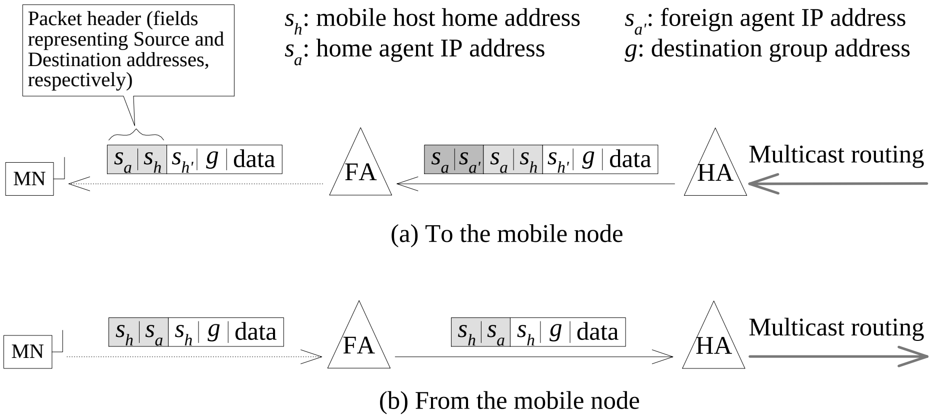


Figure 4: Message delivery in bi-directional tunneling.

proceeds (Figure 4b.)

Bi-directional tunneling works when mobile hosts are unable to acquire co-located addresses or foreign subnetworks are not multicast-capable. Nevertheless, several drawbacks arise. First, this scheme may result in multiple encapsulations on a single datagram, increasing the packet size, at the expense of network bandwidth and transmission delay. Second, mobile hosts could be unduly burdened with repeatedly processing tunneled packets. This costs power consumption. Third, a multicast datagram may be delivered as a unicast packet to mobile hosts separately, even though several of them sharing the same home agent happen to visit a common subnetwork. Duplicate multicast messages will thus arrive at that subnetwork. If RSVP [29, 35] is applied, the waste of network resource will be much severe.

4.3 Chikarmane's Scheme

Similar to the bi-directional tunneling option, Chikarmane *et al.* [10, 11] presented a scheme that maintains delivery paths on the basis of MNs' home agents, while with an important distinction as follows. When a home agent serves the mobile hosts of a given group at several foreign subnetworks, it tunnels only one copy of the received multicast datagrams to each such foreign subnetwork. Link-level multicast is used by the local agents at these subnetworks to complete the last-mile delivery. When the MNs of different home agents are attached to a particular foreign agent, multiple tunnels will terminate at that foreign agent. To avoid duplicate multicasts being directed to that subnetwork in this case, the foreign agent designates one of these MN home agents to forward multicast traffic. Other non-designated home agents suppress traffic re-direction.

As an optimization of Mobile IP multicasting, Chikarmane's scheme is very general: it uses home agents to accommodate mobile host memberships and supports administratively-scoped (private) multicasts on home networks. The performance evaluation of this scheme is approached by simulations in [33].

A flaw in the afore-mentioned research is the maintenance of multicast routes regardless of the mobile participants' whereabouts. Message exchanges among MNs that are away from home can thus traverse a long delivery path. Figure 5 illustrates an example. Suppose that mobile hosts h_1 and h_2 are attached to foreign agents FA_1 and FA_2, respectively. Multicast packets from h_1 are first tunneled from FA_1 to its home agent, HA_1, and are thereafter propagated over the established tree. When the packets arrive, h_2's home agent HA_2 tunnels them to FA_2, thereby to the destination h_2. Such message re-direction increases communication delay substantially, waste network bandwidth, and place a burden on the network entities along the delivery paths. As a remedy, several cost-effective schemes that allow for dynamic adjustment of multicast trees to mobile hosts' locations are proposed, to be described below.

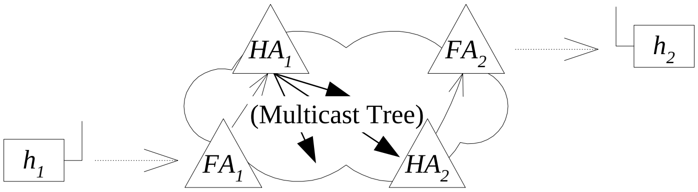
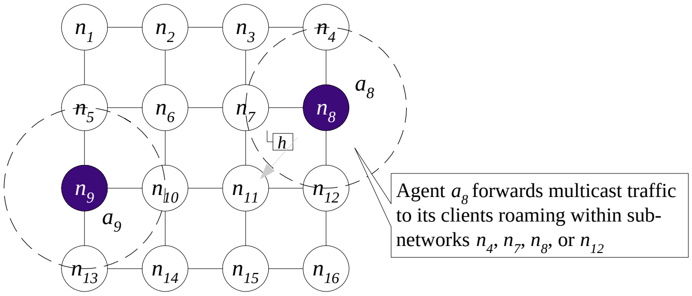


Figure 5: Schematic diagram of quadrangle routing.

4.4 Lin and Wang's Scheme

Lin and Wang proposed to trade off the shortest delivery path and the frequency of the multicast tree reconfiguration [22]. The proposal, referred to as Ranged-Based Mobile Multicast, lies between remote subscription and bi-directional tunneling, in the following lines. Each mobile node designates a router, as a service provider, that is responsible for tunneling multicast datagrams to its current foreign agent. Such routers remain on multicast distribution trees. The service provider of a mobile host is changed according to the host location and is initialized to its home agent.

Each service provider takes care of its surrounding area of subnetworks where mobile nodes can roam about. The area is specified by hop count, termed *service range* $\mathcal{R}$, between the server and its mobile clients. Figure 6 depicts an example of $\mathcal{R}$ being 1.



Agent a_8 forwards multicast traffic to its clients roaming within sub-networks n_4, n_7, n_8, or n_{12}

Figure 6: Service range of each agent.

The information on the service provider of a mobile host h is recorded at its home agent. Whenever a handoff occurs, the new local agent, namely a_{11} in this example, contact h's (permanent) home agent to locate its service provider, a_8, and then calculates its distance to a_8. If the new distance is greater than $\mathcal{R}$, a_{11} is selected as the new service provider. The new agent will join the multicast group tree accordingly, and notify h's home agent to update the current service provider of the mobile node. If h still resides in its original service range, a_{11} simply informs a_8 of h's new care-of address. Given that a_{11} is already in the multicast group, h's new service provider is reset to the local agent. In summary, when $\mathcal{R} = \infty$, this protocol operates like the bi-directional tunneling option; while $\mathcal{R}$ is zero, this proposal functions as the remote subscription option. The scheme is adaptive to the dynamics of the system by controlling $\mathcal{R}$.

4.5 Foreign Agent Routing Scheme

The objective of this scheme is to deliver multicast packets directly to and from where MNs are currently situated, bypassing home agents. Each fixed or mobile host originates multicast packets using its own home address as the IP source address so that recipients can distinguish the multicast senders. To this end, it is necessary to support multicast delivery from visiting mobile nodes for those routing protocols, such as DVMRP or MOSPF, that forward multicasts according to the datagram source address. One could use the IP-in-IP encapsulation technique [26] as follows. As shown in Figure 7, the local mobility agent intercepts and encapsulates the multicast datagrams

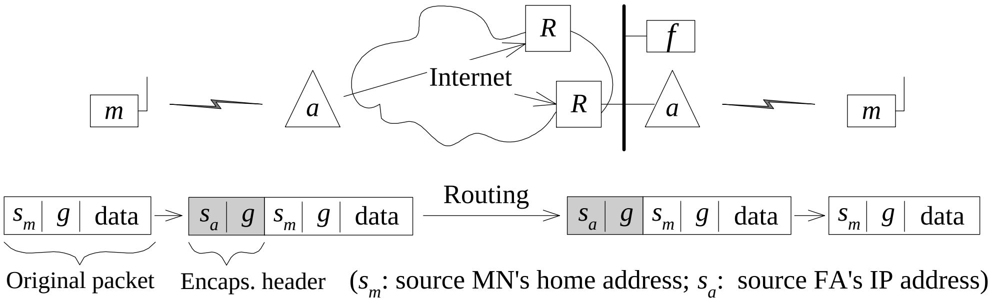


Figure 7: A paradigm of multicast routing.

whose IP source addresses are foreign to the subnetwork, and re-sends these datagrams using its own IP address. Here the encapsulation of a datagram means that an outer IP header is inserted in front of the original datagram. The outer IP header's Source Address and Destination Address specify the agent IP address and the destination multicast group address, respectively. In this way, packets will be routed along the established paths toward the downstream subnetworks and routers, hop by hop, to group members.

On receiving a multicast datagram forwarded to a subnetwork, the local mobility agent examines whether or not the datagram has been encapsulated, i.e., whether an integer 4 has been assigned to the Protocol Number field in the datagram's IP header. If so, the outer IP header is removed and the resultant datagram is forwarded to the intended MNs on the subnetwork, over wireless media.

Here mobility agents are assumed to be multicast-aware so that multicast datagrams originating from a visiting MN will not be dropped but processed for outgoing delivery. Besides, fixed hosts are assumed to know IP-in-IP so as to determine whether they should decapsulate the received multicast datagrams beforehand. Such multicast routing requires the delivery paths to be adjusted upon host mobility. To curtail the potential costly overhead, two methods are proposed, as described in the following two subsections respectively.

4.5.1 Exploiting Movement Locality

It is observed that user mobility patterns mostly possess locality property [12, 21] — a subnetwork visited by an MN tends to be re-visited in the near future. A *locality* refers to the set of subnetworks that were visited by mobile hosts of a group during the most recent Δt time units [32]. Besides, a subnetwork is said to be *active* on a multicast route if it is included in the route, or *inactive* otherwise. In this scheme, each subnetwork in a locality is kept active for Δt time units after the corresponding group of MNs has moved off. If a host of the group moves into such a subnetwork before Δt expires, this subnetwork is revived. Otherwise the subnetwork will be dropped from the locality. Hence a locality specifies an area where hosts of a multicast group are able to migrate without altering delivery paths. This benefit is effective unless the locality changes, upon which multicast delivery paths are adjusted accordingly.

To capture the notion of localities, mobility agents are designated to learn local MN group memberships and perform IGMP reports for Δt time units on behalf of those MNs that have moved away. This will hold the subnetworks in a locality from being pruned from multicast delivery paths for a period of time. In practice, each mobility agent keeps track of local MN group memberships, using a triple $< g, \Delta t, mn\_ids >$ per group g, where mn_ids denotes a set of local MNs in group g.

Whenever MN m_i moves and changes its agent, say from a_j to a_k, the associated membership information with m_i will be handed from a_j to a_k locally. To begin, a_k sends a_j a Membership Binding message, indicating the identities of groups to which a_k currently belongs. In response, a_j returns a Binding Reply message, containing the group identities for m_i. Then a_k immediately joins those groups present in the Binding Reply message, but absent from the Membership Binding message, in the same way as a normal host joins a group. Meanwhile a_j re-directs multicast datagrams in flight to a_k (thereby to m_i) for the new groups that a_k joins, until a designated timer expires.

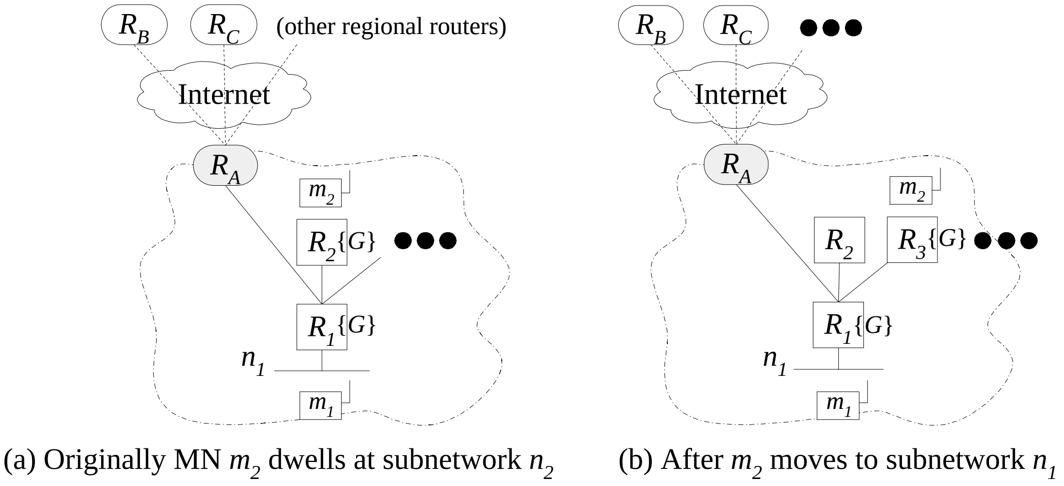
Whenever all MNs of a group have moved off a subnetwork, the local mobility agent determines the value of Δt in the group's triple and will issue IGMP reports for the group for Δt time units. If any host of the group arrives before Δt has expired, this subnetwork is revived. The local agent is suppressed from originating IGMP reports, since the host will do that. On the other hand, if none of the group returns before Δt time units have elapsed, the local mobility agent sends a *leave-group* message to the local multicast router, to depart from the group. As a result, the subnetworks that the MNs of a group visited most recently are kept active as the group locality.

4.5.2 Partitioning the Multicast Backbone

As another method for saving the cost of modifying multicast routes, one can partition the mobile environment into regions, so changes in the multicast delivery paths due to MNs' intra-region movements are isolated to the same region, rather than throughout the multicast backbone.

The Internet can be viewed to be composed of regions that contains some number of subnetworks and routers in a geographical area, e.g., an enterprise. In essence, each region is treated as if it were a single subnetwork as a whole. Within a region, each router manages its group and periodically exchanges route information with each of its neighbors as usual. Such route information is propagated over the region, thereby to the regional router. A regional router is in general a gateway interconnecting nodes in different regions. Then the regional router initiates the aggregated route information of its own downstream, on behalf of local routers. Hence routers outside a region are only aware of the regional router and its attached whole network. Observe that host intra-region movements do not change the membership aggregated within the region and thus the delivery paths off the region remain. In other words, the changes in multicast routes due to MNs' intra-region movements are limited to that region.

For example, in Figure 1, suppose that MNs m_1 and m_2 of group G are both located in a region whose regional router is R_A. First, MN m_1 uses a route to distribute multicasts from subnetwork n_1, as depicted in Figure 8(a). As the route information originating from R_1 arrives, the regional route R_A sends R_A-initiated route information to the neighboring routers off the region. When m_2 later moves to subnetwork



(a) Originally MN m_2 dwells at subnetwork n_2 (b) After m_2 moves to subnetwork n_1

Figure 8: The multicast delivery path sourced from subnetwork n_1.

n_3 without group members, the local router R_3 will detect membership for group G (instantly by some means) and grafts paths onto the multicast routes rooted at other subnetworks, say n_2, as shown in Figure 8(b). Since the graft message issued by R_3 is propagated within but not outside of the region, the changes in multicast routes due to host intra-region movements are hidden from the routers off the region.

5 Remarks and Discussions

This section briefly discuss some other pragmatic considerations that arise when implementing the above multicast schemes. For comparing these scheme in some other regards, we refer the reader to [34]. First, an advantage of Mobile IP multicast options is their interoperability with existing networks. In this architecture, multicasting is completely transparent to the various foreign agents that an MN may use, while the MN and home agent are generally under the same administrative control and therefore may be modified at the same time. Nonetheless, two disadvantages result: 1) datagram delivery can be suboptimal due to triangle or quadrangle routing; 2) native multicasting cannot be exploited even when supported by the network. The latter is because multiple MNs receiving the same group need separate tunnels, originating from the same or different home agent. Since multicasts are doubly encapsulated, they cannot be recognized as duplicates by an unmodified foreign agent.

Chikarmane's approach optimizes Mobile IP multicast options, using link-level multicast mechanisms and reducing duplicated messages considerably. However, this approach still suffers from suboptimal routing. Another disadvantage is the overhead associated with dynamic tunnel management and double encapsulation. Namely, we need to determine when a home agent should start and stop tunneling datagrams, if the home agent and foreign agent are under separate administrative control and unlikely to trust each other. The major defect, however, relates to the scheme's applicability: as both the foreign agent and home agent must be modified to handle multicasts using a nonstandard protocol, interoperability is limited.

The foreign agent routing scheme has the benefit of complete transparency. By simply gathering membership information from its local network, the foreign agent can interoperate with other routers using any protocol. The main drawback is that the local network owner may be not willing to provide multicast service to visiting MNs, due to resource considerations. Although routing in this scheme will always be optimal, there needs multicast delivery paths to adapt to mobile host locations, at the expense of potentially significant overhead. One approach to saving the overhead is to exploit the locality in user movement behaviors. This approach reduces packet losses experienced by migrant hosts, since within active subnetworks, the hosts are able to receive multicasts without disruption from each of these subnetworks locally. However, in this model, a subnetwork without group members remains active for up to extra Δt time units. Multicast traffic directed to such subnetworks during this period is wasted. The choice of Δt is thus important to this scheme; the longer Δt is, the fewer multicast routes are reconstructed, yet the more multicast traffic is likely to be wasted for delivery to subnetworks without recipients. Indeed, another form of wasting network bandwidth is present in previous schemes like [10, 11, 27], in the sense that they may use longer paths to deliver multicast datagrams.

Partitioning the multicast backbone into regions was studied previously [14, 31].

Those work considered a stationary networking system rather than a mobile environment. As a remark, in [31], Thyagarajan and Deering used region identifiers that are not encoded in the addresses and use encapsulation for the inter-region forwarding of datagrams. This method is amenable to incremental deployment and reduces the amount of topological information that routers must store and exchange. However, regional routers can be overloaded in performing a decapsulation and encapsulation to each multicast packet. When a region contains a large number of members, the regional router is vulnerable to heavy traffic load.

The concept of regionalizing the network also appears in hierarchical mobile IP by Perkins [27, pages 187-199]. In the hierarchical mobile IP, an MN's registration can be transacted with a regional agent without requiring approval by or rebinding at the home agent to smooth the registration procedure. The localized registration of mobile IP is not in the context of multicasting and the issues specific to multicast group communications remain. However, our scheme is orthogonal to the hierarchical mobile IP and could be regarded as an augmentation to that proposal which deals with multicast packet routing.

6 Conclusion

This paper presented different approaches to IP multicasting support for mobile hosts. We have seen how multicasting and mobility can interoperate in the Internet. Although performance and compatibility problems as well as trade-offs among them remain thorough investigation, the existing proposals are adequate to support full participation of MNs in group communication. Simple modifications to these proposals can further improve performance, easing the migration of multicast-based applications to mobile hosts.

Acknowledgements

We thank Dr. W. Fenner, from AT&T Research in Menlo Park and T. Maufer, from 3Com for their valuable help and comments. This work has been supported by the National Science Council, ROC, under grant NSC89-2213-E009-028, and by the MOE Program of E. Research under grant 89-E-FA04-1-4.

References

[1] A. Acharya, A. Bakre and B.R. Badrinath, "IP Multicast Extensions for Mobile Internetworking," *IEEE INFOCOM'96*, pp.67-75, 1996.

[2] K.C. Almeroth, "The Evolution of Multicast: from the MBone to Interdomain Multicast to Internet2 Deployment," *IEEE Network*, 14(1): 10-20, 2000.

[3] K.C. Almeroth, "A Long-term Analysis of Growth and Usage Patterns in the Multicast Backbone (MBone)," INFOCOM 2000, 19th Ann. Joint Conf. IEEE Comput. and Commun. Societies, *Proc. IEEE*, Vol. 2, pp. 824-833, 2000.

[4] K.C. Almeroth *et al.*, The *Mantra* project, http://imj.ucsb.edu/mantra.

[5] A. Acharya and B.R. Badrinath, "A Framework for Delivering Multicast Messages in Networks with Mobile Hosts," *ACM/Baltzer Mobile Networks and Applications*, 1(2): 199-219, 1996.

[6] B.R. Badrinath, A. Acharya, and T. Imielinski, "Impact of Mobility on Distributed Computations," *ACM Oper. Syst. Rev.*, 27(2): 15-20, 1993.

[7] A. Ballardie, J. Crowcroft, and P. Francis, "Core Based Trees (CBT) – An Architecture for Scalable Inter-Domain Multicast Routing." *Comput. Commun. Rev.*, 23(4): 85-95, 1993.

[8] K.P. Birman, *Building Secure and Reliable Network Applications*, Manning Publications Co., 1996.

[9] K.H. Chi, C.C. Tseng, and T.L. Huang, "A Framework for Mobile Multicast Using Dynamic Route Reconstructions", *the Comp. Journal*, 42(6): 522-533, 1999.

[10] V. Chikarmane, R. Bunt, and C. Williamson, "Mobile IP-Based Multicast as a Service for Mobile Hosts." *Proc. 2nd IEEE Int'l Wksp. Services in Distributed and Network Environments*, pp.11-18, 1995.

[11] V. Chikarmane *et al.*, "Multicast Support for Mobile Hosts Using Mobile IP: Design Issues and Proposed Architecture," *ACM/Baltzer Mobile Networking and Applications*, 3(4): 365-379, 1999.

[12] G. Cho and L.F. Marshall, "An Efficient Location and Routing Scheme for Mobile Computing Environment." *IEEE Journal on Selected Areas in Commun.*, 13(5): 868-879, 1995.

[13] K. Cho and K.P. Birman, "A Group Communication Approach for Mobile Computing," *Proc. Wksp. Mobile Computing and Applications*, Santa Cruz, California, Dec 8-9, 1994.

[14] S.E. Deering, "Multicast Routing in a Datagram Internetwork," Ph.D. Thesis, Stanford University, 1991.

[15] S.E. Deering *et al.*, "An Architecture for Wide-Area Multicast Routing," *Comput. Commun. Rev.*, 24(4): 126-135, 1994.

[16] P. Dupont, "Local Mobility Management in IP Networks." Motorola Wireless Data Group, Sep 1993.

[17] W. Fenner, "Internet Group Management Protocol, Version 2," *RFC 2236* (Updates *RFC 1112*), 1997.

[18] T.G. Harrison *et al.*, "Mobile Multicast (MoM) Protocol: Multicast Support for Mobile Hosts." *Proc. 3rd Annual ACM/IEEE Conf. Mobile Comput. and Networks*, pp.151-160, 1997.

[19] V. Hadzilacos and S. Toueg, "Fault-Tolerant Broadcasts and Related Problems," *Distributed Systems*, 2nd Ed. (S. Mullender, ed.) ACM Press, pp.97-145, 1993.

[20] J. Ioannidis, D. Duchamp, and G.Q. Maguire Jr., "IP-Based Protocol for Mobile Internetworking." *SIGCOMM'91*, pp.235-245, 1991.

[21] R. Jain *et al.*, "A Caching Strategy to Reduce Network Impacts of PCS," *IEEE Journal on Selected Areas in Commun.*, 12(8): 1434-1444, 1994.

[22] C. R. Lin and K. M. Wang, Mobile multicast support in IP networks, *Proc. IEEE INFOCOM 2000*, pp. 1664–1672, Mar 2000.

[23] T.A. Maufer, *Deploying IP Multicast in the Enterprise*, Prentice-Hall, Inc., Upper Saddle River, 1998.

[24] J. Moy. "Multicast Extensions to OPSF," *RFC 1584*, 1994.

[25] J. Mysore and V. Bharghavan, "A New Multicasting-based Architecture for Internet Host Mobility," *Proc. 3rd Annual ACM/IEEE Conf. Mobile Comput. and Networks*, pp.161-172, 1997.

[26] C. Perkins, "IP Encapsulation within IP," *RFC 2003*, Network Working Group, Oct 1996.

[27] C. Perkins, *Mobile IP Design Principles and Practices,* Addison-Wesley Longman, 1998.

[28] T. Pusateri, "Distance Vector Multicast Routing Protocol," Internet Draft, <draft-ietf-imdr-dvmrp-v3-08>, Internet Working Group, 1999.

[29] USC Information Sciences Institite, RSVP, http://www.isi.edu/div7/rsvp/rsvp.html.

[30] C. Semeria and T. Maufer, "Introduction to IP Multicast Routing," http://www.3com.com/nsc/501303.html

[31] A.S. Thyagarajan and S.E. Deering, "Hierarchical Distance-vector Multicast Routing for the MBone," *Comp. Commun. Rev.*, **25**, 60-66, 1995.

[32] C.C. Tseng, K.H. Chi, and T.L. Huang, “A New Locality-based IP Multicasting Scheme for Mobile Hosts,” (to appear in) *Comp. Commun.*

[33] C.L. William *et al.*, “Performance Evaluation of the Mom Mobile Multicast Protocol,” *ACM/Baltzer Mobile Network and Applications*, 3(4): 189-201, 1998.

[34] G. Xylomenos and G.C. Polyzos, “IP Multicast for Mobile Hosts,” *IEEE Commun. Magazine*, 35(1): 54-58, 1997.

[35] L. Zhang *et al.*, RSVP: a new resource reservation protocol, *IEEE Network*, Sep 1993.