Mobile Multicast Support in IP Networks†

Chunhung Richard Lin and *Kai-Min Wang*

Department of Computer Science and Information Engineering, National Chung Cheng University, TAIWAN
Email: chlin@acm.org, wkm86@ms36.hinet.net

Abstract - In this paper, we present an alternative design, *RBMoM* (Range-Based Mobile Multicast), for efficiently supporting multicast for mobile hosts on the Internet. The current version of Mobile IP [12] proposes two approaches to support mobile multicast, which are remote subscription and bi-directional tunneling. The former provides the shortest routes for delivery of multicast datagrams to mobile hosts; the latter hides host mobility from all other members of the group (therefore, no any overhead in the multicast tree maintenance). RBMoM intends to trade off between the shortest delivery path and the frequency of the multicast tree reconfiguration by controlling the *service range* of the *multicast home agent* (MHA). Actually, we will find that remote subscription and bi-directional tunneling are the extremes of RBMoM. From the point of view of the MHA and the service range concepts, RBMoM is a generalization of both approaches and a unifying mobile multicast approach. The simulation results show that RBMoM can adapt to the fluctuation of both host movement and the number of mobile group members, and has much better performance than the current two IP mobile multicast solutions.

1. INTRODUCTION

The mobile multicast protocol must deal not only with dynamic group membership but also with dynamic member location. The current multicast protocols on the Internet, DVMRP [18], MOSPF [9], CBT [2], and PIM [4], implicitly assume static hosts when building a multicast delivery tree. They do not consider the dynamic member location. Reconstructing the delivery tree every time a member moves will involve the overhead, yet leaving the tree unchanged can result in inefficient, incorrect, or even failure of multicast datagram delivery. Thus they are not suitable for the mobile environment. The IETF Mobile IP Working Group proposed the Mobile IP to support unicast IP routing for mobile hosts in an IP internetwork [6-8, 10, 14-15]. The current version of Mobile IP proposes two approaches to support mobile multicast, i.e., bi-directional tunneling and remote subscription. In the former, the mobile host (MH) receives multicast datagrams by way of its home agent (HA) using the unicast Mobile IP tunnels. This approach handles source mobility and recipient mobility, and in fact hides host mobility from all other members of the group [5]. Therefore, the multicast delivery tree will not be updated because of member location change. The main drawback of the approach is the routing path for multicast delivery which can be far from optimal. In addition, the HA must replicate and deliver tunneled multicast datagram to all its MHs, regardless of at which foreign networks they reside. Therefore, the network resource will be wasted. If RSVP [20] is applied, then the waste of bandwidth will be much severe.

In remote subscription, each MH always re-subscribes to its desired multicast group when it enters a foreign network. Therefore its local multicast router must be added to the multicast tree. The update frequency of the multicast tree will depend on how often the mobile handoff occurs. Obviously, remote subscription has better performance if mobile hosts spend a longer time within a network, compared with the join and graft latencies [1]. The main advantage of this approach is that the multicast datagrams are always delivered on the shortest paths. However, the overhead is the cost of reconstructing the delivery tree while a handoff occurs. In addition, this approach implicitly assumes that mobile hosts are only subscribers of a multicast group or that they have a co-located address on the foreign network. The source mobility is not handled.

In this paper, we propose a new protocol which not only offers good (i.e. near shortest path) routes for delivery of multicast datagrams to mobile hosts like remote subscription, but also has less frequent multicast tree reconstruction. Actually, we will find remote subscription and bi-directional tunneling are the extremes of our protocol. The basic idea in our protocol is the use of "multicast home agent" (MHA) and "service range" to limit the length of the routing paths of the multicast datagrams and to control the frequency of reconstructing the multicast tree. That is, our protocol intends to find the balance of the routing path and the tree maintenance overhead.

The rest of the paper is organized as follows. Section 2 presents the previous works which will be compared with our protocol. Section 3 introduces our RBMoM protocol. Section 4 discusses some details of RBMoM. Section 5 evaluates the performance and compares RBMoM with the other protocols. Finally, we conclude this paper in Section 6.

2. PREVIOUS WORKS

Bi-directional tunneling is based on home agent functionality of IETF Mobile IP. Mobile hosts receive multicast data by way of their home agents. MoM [5] based on bi-directional

† This work was supported by the National Science Council, TAIWAN, under Contract NSC-89-2213-E-194-007 "Design of Multicast Support for Mobile Networks".

tunneling was proposed to solve the *tunnel convergence problem*. It results from the fact that multiple Mobile IP tunnels (from different HAs) terminate at a common FA (shown in Figure 1). MoM uses the DMSP (Designated Multicast Service Provider) to avoid duplicate datagram being tunneled to the common FA. In this protocol, the FA performs a selection to appoint one HA as the DMSP. Only DMSP forwards the multicast datagram to the foreign agent. Thus, the FA can only receive one copy of each multicast datagram. For example, in Figure 1, one of home agents HA_a, HA_b, and HA_c is selected as the DMSP. Only one copy (rather than three) of the datagrams will be received by FA. We can find that this protocol has better performance particularly as the number of mobile group members increases.

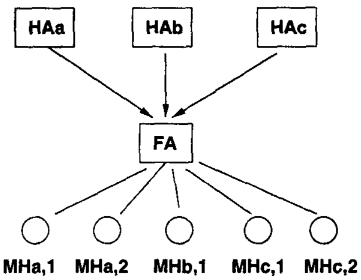

Figure 1: Tunnel convergence problem

A *DMSP handoff* means that the FA reselects its DMSP. A DMSP handoff may occur in two situations. One is that a new mobile host enters a network and its HA is more suitable to be the DMSP; the other is that all DMSP's mobile hosts move away from the network. When a mobile host handoff occurs, its HA can learn the mobile host's new FA immediately by using Mobile-IP. But the previous FA can not know the handoff until timeout. So, before the new DMSP is selected, none will serve the mobile hosts within the previous network. Multicast packets for mobile hosts will be lost during this period. For MoM, if the number of mobile group members is small (i.e. in sparse mode), the DMSP handoff will occur frequently. In the example illustrated in Figure 2 (home agents are assumed to be also the multicast routers), the two MHs, MH_1 and MH_2, are far away from their home agents (HA_1 and HA_2 respectively), and the "tunnels" are quite long. Furthermore, because no two visitors in the foreign network have the same home agent (sparse mode), any MH handoff will make DMSP handoff occur.

Besides, in [11] a protocol is proposed to use a new multicasting-based architecture to support Internet host mobility. Unlike the Mobile-IP approach, each mobile host is assigned a unique Class D address (multicast address). So it can eliminate the address mapping overheads in Mobile-IP. However, modifying the interacting protocols such as ARP, IGMP, ICMP and TCP is the disadvantage of this protocol.

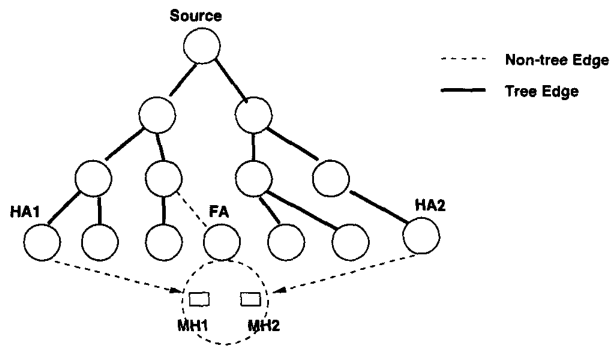

Figure 2: The problem in sparse mode

3. RANGE-BASED MOBILE MULTICAST (RBMoM)

RBMoM intends to trade off between the shortest delivery path and the frequency of the multicast tree reconfiguration. Regardless of what environment parameters (e.g. mobility, the number of mobile goup members, etc.) are, multicast datagrams are delivered on the near-shortest paths without paying the high cost of reconstructing the multicast tree (the main drawback of remote subscription).

Like the home agent in Mobile IP, RBMoM has a router, called *multicast home agent* (MHA), that is responsible for tunneling multicast datagrams to the foreign agent to which the MH is currently attached. Therefore, each MHA must always be one of the multicast group members (this is like bi-directional tunneling in which every home agent must join the multicast group). Every MH can only have one MHA. The HA of a MH is never changed. However, the MHA of a MH is changed according to the MH location. The initial MHA of a mobile host is set to be its HA.

RBMoM addresses a concept of "range" for each MHA. The *range* of a MHA means the service range to its MHs. That is, a MHA can only serve the mobile hosts which are roaming around the foreign networks which are within its service range, or the network to which the MHA is attached. If a mobile host is out of its MHA service range, then the *MHA handoff* will occur. That is, another MHA will take over the multicast service to the mobile host. Consider the example shown in Figure 3. If the service range of each router is one (hop distance), the MHA_1 can only forward multicast datagrams to its MHs which are roaming in the foreign networks 2, 3, 6 or its current network. Similarly, the MHA_2 can only serve its MHs in the networks 8, 12 or its current network. From the point of view of the range concept, we will find both bi-directional tunneling and remote subscription are the extremes of RBMoM. Let R be the service range of a multicast home agent. Thus,

(1) If we let $R = \infty$, then RBMoM is the same as bi-directional tunneling. In this case, the MHA is always the home agent and is never changed. That is, home agents with multiple mobile host group members away from home must replicate and deliver tunneled multicast

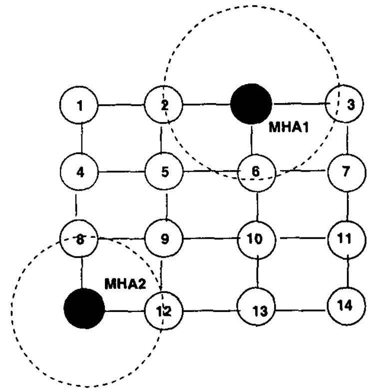

Figure 3: Service range of each base station

datagrams to each of them, regardless of at which foreign networks they reside.

(2) If we let $R = 0$, then RBMoM is the same as remote subscription. That is, when a MH enters a foreign network (i.e. handoff), its MHA must be changed because of out of the service range. The current FA can be the new MHA and will subscribe to the desired multicast group.

(3) RBMoM is a generalization of the above cases and a unifying mobile multicast approach. According to the value of R, a MHA with multiple mobile host group members can determine whether the datagrams should be tunneled to each of them. Actually, the service range restricts the maximal length of the tunnel between a mobile host and its MHA.

The MHA information of a mobile host is recorded at its HA. When a MH reaches a foreign network, it locates the FA and registers with it according to Mobile IP. Then FA contacts its (permanent) HA to locate the MHA serving the MH. The FA calculates the distance to MHA. If it is greater than the service range, a new MHA must be selected to take over the work. For simplicity, we select the current FA to be the MHA. The new MHA has to subscribe to the multicast group (i.e., the multicast router of the foreign network has to join the multicast tree). The FA (also the new MHA) has to inform the HA to update the MHA currently serving the MH (HA must always record the last MHA location). If the MH is still within the service range of its MHA, the FA just informs the MHA of the FA currently serving it. In order to get a shorter delivery path, if the current FA has already been in the multicast group, we can update the MHA to be the FA even though the MH is still within the service range. In Figure 4, the service range is assumed 1. When the MH is out of the service range of MHA, new MHA (i.e. MHA') is setup to serve the MH and the MHA' must join the multicast group. It is notable that all MHAs must be in the multicast group.

The main difference between the HA and the MHA is that the MHA is dynamically changed according to the location of the MH, but the HA is unchangeable. The MHA

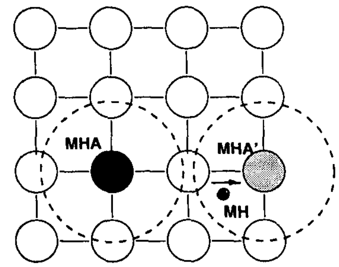

Figure 4: Setup the new MHA

offers the multicast service and the HA offers the unicast service. Both need the FA to cooperate. The current MHA serving the MH is recorded at the home agent. A MHA has to keep a list of mobile hosts which need to be served. When the MHA is changed, the new MHA must inform the old MHA to delete the record of the mobile host. Figure 5 shows the detail operations of the FA when a new visitor enters its network.

```
When a MH arrives at a foreign network:

1. The mobile contacts the FA and registers according to Mobile IP.
2. FA contacts the HA to get the location of MHA.
3. FA computes the hop distance to MHA; and

if (Distance(FA,MHA) > R) /* out of service range */
{
  if (MHA ≠ HA)
  { /*leave MHA's range*/
    if (Distance(FA,HA) ≤ R)
    { /* come back to HA's service range */
      If (FA has been in the multicast tree)
        MHA ← FA;
      else
      {
        MHA ← HA /* Initially, MHA ← HA */
        Join to multicast tree if it is not there.
      }
    }
    else
    {
      MHA ← FA.
      Join to multicast tree if it is not there.
    }
  }
  else
  { /*leave HA's range*/
    MHA ← FA
    (HA may leave the multicast group if necessary)
  }
  Inform HA of the FA currently serving it;
  Inform HA of the MHA currently serving it;
  Informs old MHA to delete all data structures about the MH.
  (The old MHA may leave the multicast group if necessary)
}
else {Inform MHA of the FA currently serving it;}
```

Figure 5: The operations of FA when a mobile arrives at a foreign network

4. RBMoM PROTOCOL DETAILS

The tunnel convergence problem also occurs in RBMoM. That is, multiple MHAs all happen to have mobile hosts (the same multicast group) at the same foreign network, managed by the foreign agent FA. Thus each MHA will forward one copy of every multicast datagram to the FA. The FA will receive duplicate multicast datagram. To solve this problem, the DMSP solution [5] can be applied. The DMSP really solves most, but not all, of the duplicate transmission. For example, if a FA has already been in the same multicast group as its DMSP, then the FA will receive two copies of each multicast datagram. One is from the DMSP; the other is from the source of the multicast group. Thus, in RBMoM, the FA has to check if itself and the MH are in the same multicast group. If they are, then the FA appoints itself as the DMSP. Thus only one copy of each multicast datagram will be received by the FA.

Figure 6 illustrates the data structures needed to implement RBMoM protocol. Each home agent maintains an *Away Table* to keep track of which of its MHs are away, where they are (i.e. at which FA), and when their bindings expire. The *MHA* field in the Away Table is to record the current Multicast Home Agent of each of its own mobile host. The FA has a Visitor Table to keep track of its visitors, their MHA, and when these bindings expire. In addition, there are three lists kept in MHA: the member list, the FA list, and the DMSP list. The member list records the mobile hosts to be served. The locations of these MHs are recorded in the FA list. The DMSP list records which FAs in the FA list need to be forwarded a copy of multicast datagrams. Similarly, there are also three lists in FA: the member list, the MHA list, and the DMSP list. The member list records the visitors; the MHA list records the visitors' multicast home agents; the DMSP list records which MHA in the MHA list is selected as the DMSP.

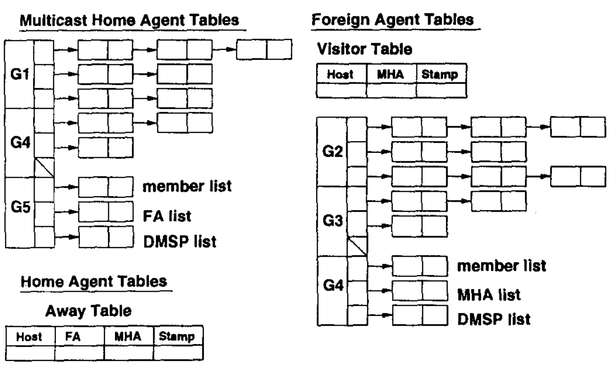

Figure 6: Data structures for RBMoM: these three tables are maintained by HA, FA, and MHA respectively

In RBMoM, when a MH arrives at a foreign network, if the MH is still within the service range of its MHA, both new FA and old FA will perform the DMSP selection. We use the "Near-to-FA" policy to select the DMSP [5]. If the MH is away from the service range of its MHA (i.e. distance(FA, MHA) $\geq$ range + 1), then the FA informs the HA to set the current FA to be the MHA. Instead of performing the DMSP selection, the FA directly appoints itself to be the DMSP since it is acting as a MHA and satisfies the "Near-to-FA" policy.

We assume that CBT [2] which is a receiver-based multicasting protocol is running in the wired network†. We use the receiver-based multicast protocol to tightly combine with the RSVP in the future because the RSVP is also a receiver-based resource reservation protocol. The other reason for using CBT is to satisfy the "common" and "nearest" principles [16] when rejoining the multicast tree occurs. The worst case in rejoining the multicast tree is the path from the core to the current network to be completely different. However, the path from the source to the core is still unchanged. Actually, the worst case seldom happens. An efficient rejoin policy in a multicast tree can alleviate the deterioration of the QoS (Quality of Service) of the receivers [17]. In RBMoM, the policy of rejoining the multicast tree is only to join the core. It is very simple and fast.

In CBT, a QUIT-REQUEST is issued by a multicast router if not only there are no members under any attached subnets, but also it has received QUIT-REQUESTs from all of its children in the tree. The multicast router continues sending a QUIT-REQUEST to its parent in CBT. But in RBMoM, because each MHA has a service range for its mobile hosts. A QUIT-REQUEST is issued by a multicast router only if there are no members under any attached subnets within the service range, and it has received QUIT-REQUESTs from all of its children in CBT. If both conditions are satisfied, then the multicast router sends a QUIT-REQUEST to its parent in CBT.

On arriving at a new foreign network, a MH contacts the new FA and registers with it according to the Mobile IP (the FA adds a new entry in its Visitor Table). Next, the FA will ask the HA to get the data of the MHA (the HA consults its Away Table). Then the FA determines if the MHA needs to be updated by checking the hop distance to the current MHA. If the distance is more than the service range, the FA appoints itself as the MHA and asks the HA to update this data in its Away Table. Our DMSP selection algorithm will consider whether the FA has already been in the multicast group. If the FA is in the multicast group, it will appoint itself as the DMSP and all visitors' MHAs must be updated to be the FA to shorten the delivery path of the multicast datagram (the FA must inform all visitors' HAs to update the data of MHA).

Here, we take an example in Figure 7 to explain how RBMoM protocol works. Initially, the MH is in its home network and the current multicast home agent is the HA. After step (1), it goes to a foreign network. The foreign network is still within the service range of the HA. Assume the foreign agent appoints the HA as the DMSP (supposedly, the HA satisfies the "Near-to-FA" policy). At present, the MH receives the multicast datagram from its multicast home agent (= HA).

† This is not necessary. Any multicast routing protocols are also workable.

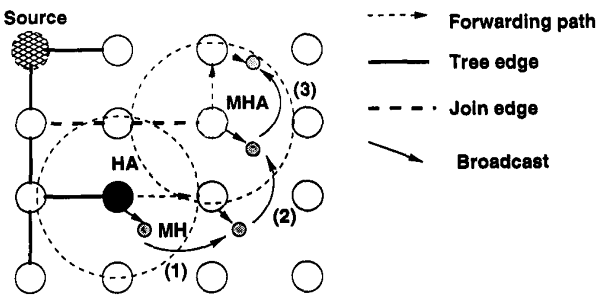

Figure 7: The execution of RBMoM

But in the step (2), the MH enters a network which is out of the service range of the HA. So, the current FA becomes the multicast home agent and joins the multicast group. The old multicast home agent (i.e. the HA) needs to leave the multicast group if all of its MHs are out of its service range. From now on, the MH will receive the multicast datagrams via the MHA. In step (3), the MH enters another foreign network. Here, the MH is still served by the MHA.

The HA is for the unicast service and the MHA is for the multicast service. The multicast datagrams are always via the DMSP to the FA and the DMSP is dynamically selected from the MHA list in the Foreign Agent Tables by the FA. However, the unicast datagrams are always via the HA to the FA. We summarize these cases in Figure 8.

1)For unicast:
0.When a unicast packet arrives at the HA,
1.If the MH is at home network,
the HA just forwards the packet to it.
Otherwise, HA forwards the packet to FA.
2)For multicast:
0.When a multicast packet arrives at the MHA,
broadcast the packet to the local members.
1.Consult the DMSP list.
2.Forward the packet to those away MHs' FAs.

Figure 8: Summary of the packet delivery in RBMoM

5. PERFORMANCE EVALUATION

The network topology in our simulation is randomly constructed at each time. The topology is based on a 5×5 mesh network which is similar to the one in Figure 4 (a 4×4 mesh). In order to generate our topology, we use a topology generation algorithm (modified from Prim's algorithm) shown in Figure 9. In this algorithm, we build a tree first, and then randomly turn on or off each non-tree edge with the equal probability. The topology shown in Figure 10 is a possible output of the algorithm. Each node acts as a multicast router of a local network and also acts as a base station. The power range is 75 meters, and the distance between two nearby base stations is 100 meters long.

In our simulation, we randomly place mobile hosts among 25 (5×5) local networks. For simplicity, there is only one multicast group in which only one source is assumed.

E, V: the set of all edges and the set of all vertices of a 5×5 mesh

1. $S \leftarrow T \leftarrow \emptyset$
2. $S \leftarrow S \cup \{v_i\}$, where $v_i \in V$ is the tree root and is randomly chosen
3. While $S \neq V$ do
4. Randomly chooses an edge $(u, v_j) \in E$, $u \in S$, $v_j \in V - S$
5. $T \leftarrow T \cup (u, v_j)$
6. $S \leftarrow S \cup \{v_j\}$
7. END
8. Each edge in $E - T$ has probability 0.5 to be selected into T.

Figure 9: Network topology generator in our simulation

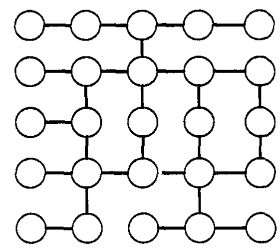

Figure 10: An example of the network topology

The interarrival time of the multicast packets is an exponential distribution with mean λ. The amount of the group members (the number of the mobile group members) varies from 10 to 50. The mobility is another parameter of concern, because the speed can affect the frequency of DMSP handoff, tree maintenance overhead, and the delivery path length severely. In addition, our simulation environment includes wired and wireless networks. Because they have quite different bandwidth inherently, two system clocks in our simulation are needed. We let the ratio of wired clock to wireless clock be α. Here, the wireless clock is assumed to be 1 second. That is, the packet transmission time in a wireless link is 1 second. Each mobile host moves at each clock in any direction uniformly. We summarize all above parameters in Table 1.

Parameters	Description	Value
N	Number of LANs	25 (5×5)
P	Power range of base station (meters)	75
D	The distance between two nearby BS (meters)	100
M	Number of multicast group	1
g	Number of multicast members	$10 \cdots 50$
s	Sources per multicast group	1
λ	Multicast packets generating rate (pkts/time unit)	0.1
α	The ratio of wired to wireless clock	10
m	Mobile host's speed (hectometer/10 seconds)	$0.1 \cdots 0.5$

Table 1: Simulation parameters

We do several experiments to assess the performance of RBMoM. It is compared with MoM (i.e. bi-directional tunneling) [5] and Pure-Join (i.e. remote subscription) by changing the parameters (mobility, group size, etc.). We get each simulation result by running over 1000 wired network topologies and 10000 time clocks per topology.

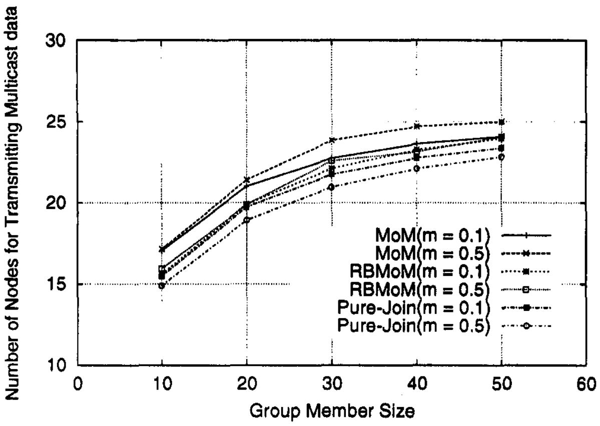

Figure 11: Comparison of multicast traffic load

The first experiment is to evaluate the multicast traffic load to the system. The number of nodes which are involved in forwarding multicast data packets (i.e. the nodes in the multicast tree and the nodes on the "tunnels") can indicate the traffic load. Let the service range of RBMoM be one. Figure 11 shows the simulation result. Pure-Join produces the lowest traffic load, because the new foreign agents must join the multicast group and there is no need to tunnel. For MoM, the multicast tree is stable and independent of the MH movement. It has the better performance when the mobility is low, because the tunnels are shorter. For RBMoM, it nearly keeps pace with Pure-Join. This is because the multicast tree is slowly reconstructed with the host movement, and the maximal tunnel length is one (the service range = 1). So, the number of nodes involved in tunneling datagrams is less than MoM and greater than Pure-Join.

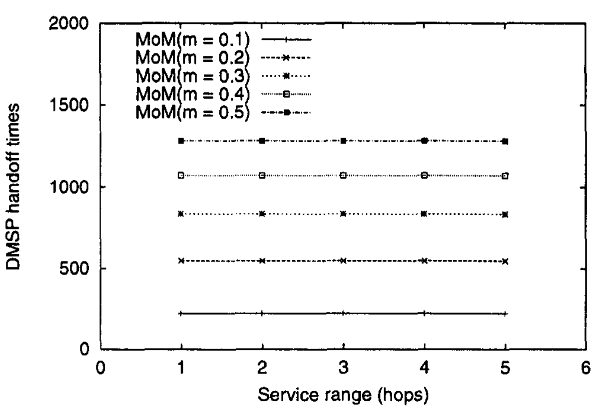

Figure 12: The number of DMSP handoff in MoM (g = 10)

Figure 12 - 15 show the number of DMSP handoff during the total simulation period in MoM and RBMoM. In high mobility, since mobile hosts' handoffs take place easily, the DMSP handoff is therefore more frequent. Figure 12 and 13 show the results. Because MoM protocol is a special case of RBMoM with the service range ∞, the multicast tree

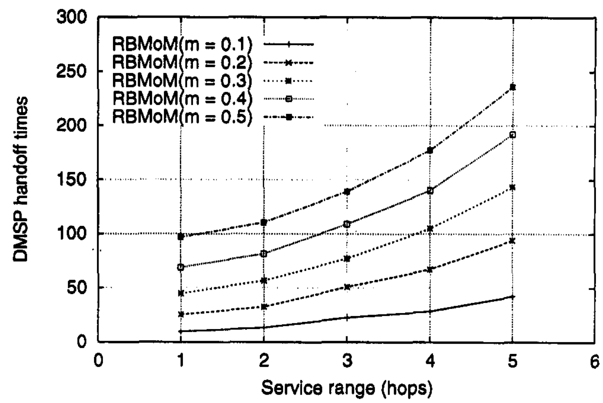

Figure 13: The number of DMSP handoff in RBMoM (g = 10)

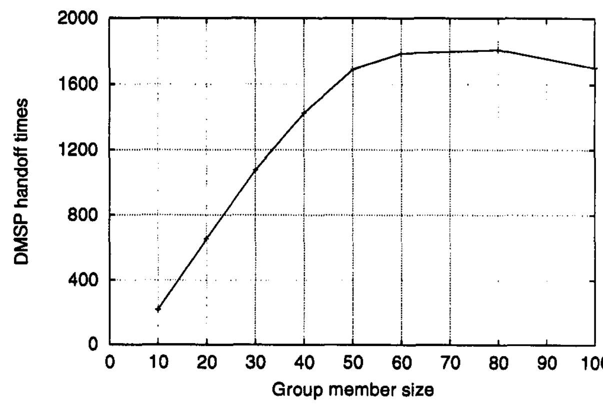

Figure 14: The number of DMSP handoff in MoM (m = 0.1)

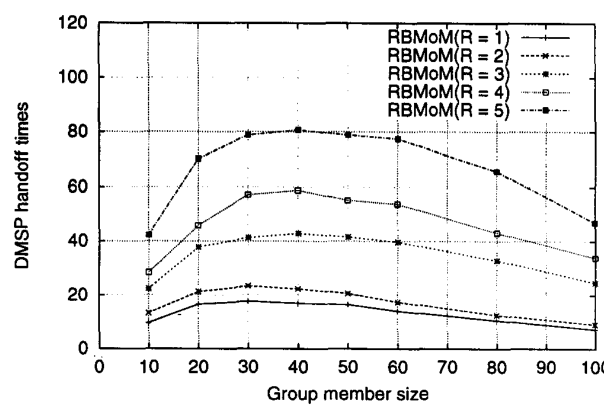

Figure 15: The number of DMSP handoff in RBMoM (m = 0.1)

reconfiguration is independent of the mobile host locations and all MHAs are never changed. For a FA, if the service range is large, then the number of possible DMSP candidates will be large. Thus when a MH moves in a foreign network, if its MHA is "better" than the current DMSP then the DMSP handoff will occur. This is the reason why in Figure 13, the larger the service range is, the more the DMSP handoffs occur. In Figure 14 and 15, when the number of mobile group members increases, the number of DMSP handoffs of MoM and RBMoM increases first and then decreases. This is because when the mobile population is large enough, more visitors in a foreign network are served by the same multicast home agent. Therefore, a handoff of a mobile host may not cause the DMSP handoff immediately.

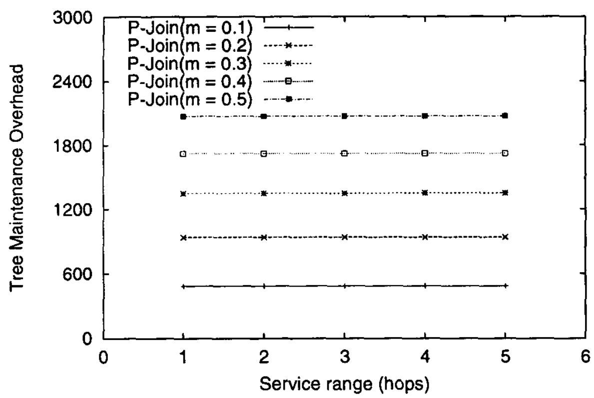

Figure 16: Tree maintenance cost in Pure-Join (g = 10)

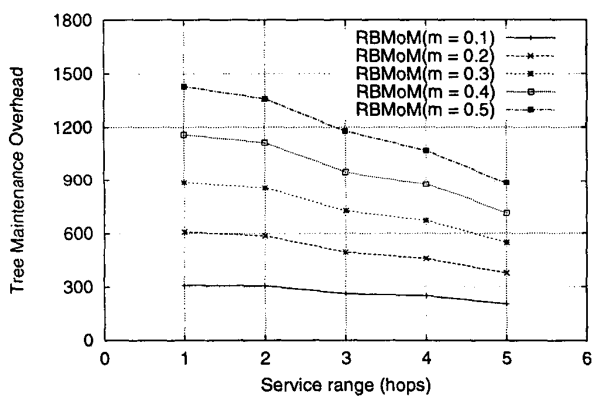

Figure 17: Tree maintenance cost in RBMoM (g = 10)

Figure 16 - 19 compare the multicast tree maintenance overheads of RBMoM and Pure-Join. The overhead of concern is the join and quit operations to the multicast tree. Thus we measure the total number of the join and quit requests during the simulation period as the multicast tree maintenance overheads. Pure-Join is the special case of RBMoM with the service range 0. Thus when a handoff takes place (i.e. a MH moves to a new network), the current multicast router must join to the tree because of the new subscriber MH. On the other hand, the multicast router in its previous network must quit from the tree if there is no any subscribers in its LAN. Obviously, the tree maintenance cost will increase when the mobility is getting higher. That is, the multicast tree reconfigures more frequently. Pure-Join has more overheads than RBMoM since each new FA has to join the multicast group. In Figure 17, when the mobility is higher, the impact of the change of the service range to the tree maintenance overheads is more obvious. This is because in the larger service range the mobile host will spend more time to stay within the service range of its current MHA. Only when the mobile host leaves the service range and enters another foreign network, a new MHA (i.e. the current FA) then serves it. At this time, the new FA needs to join the multicast group. Therefore we can find that the tree update frequency is slow as the service range is large. Consider Figure 18 and 19. When the number of mobile group members is large, the tree update frequency is slow. This is because more mobile hosts are populated uniformly in the environment, and then most of base stations are in the multicast group. Thus the multicast tree is hard to be changed owing to the mobile host handoff. Obviously, the larger service range in RBMoM will let the tree update be much slowed down. However, the multicast datagram will be forwarded along a longer tunnel.

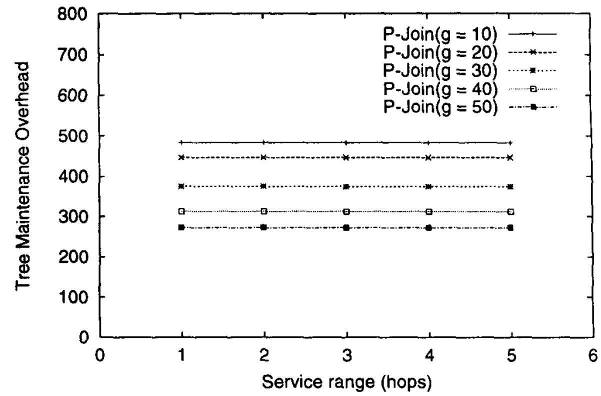

Figure 18: Tree maintenance cost in Pure-Join (m = 0.1)

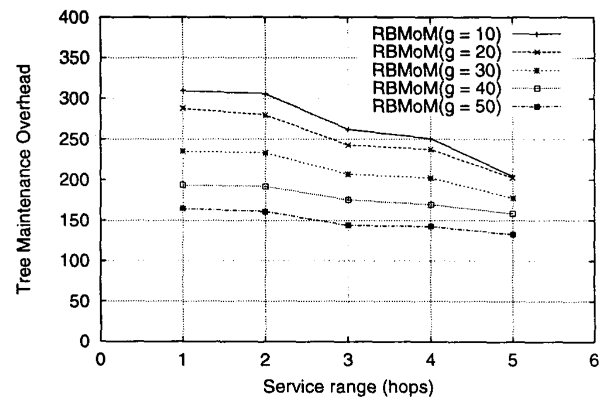

Figure 19: Tree maintenance cost in RBMoM (m = 0.1)

Finally, we compare the average routing distance of the multicast datagrams from the source to the mobile hosts in these three protocols. For multicast applications, a shorter

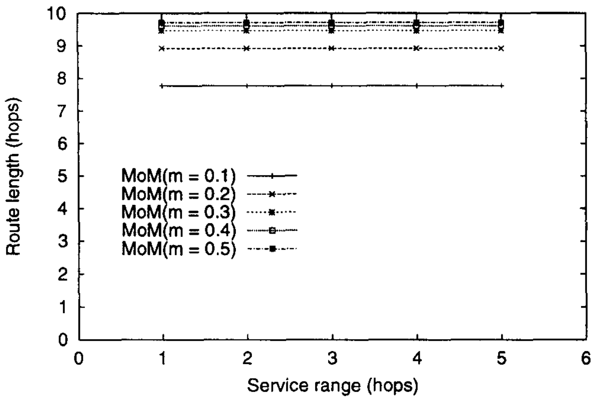

Figure 20: Average path length of MoM (g = 10)

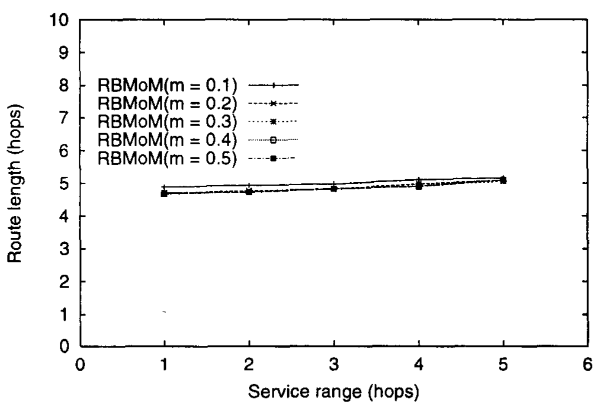

Figure 21: Average path length of RBMoM (g = 10)

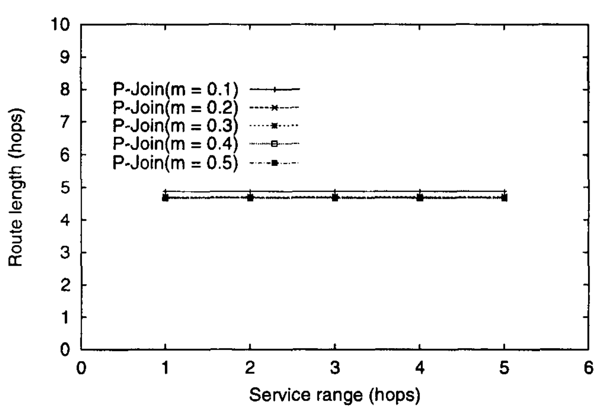

Figure 22: Average path length of Pure-Join (g = 10)

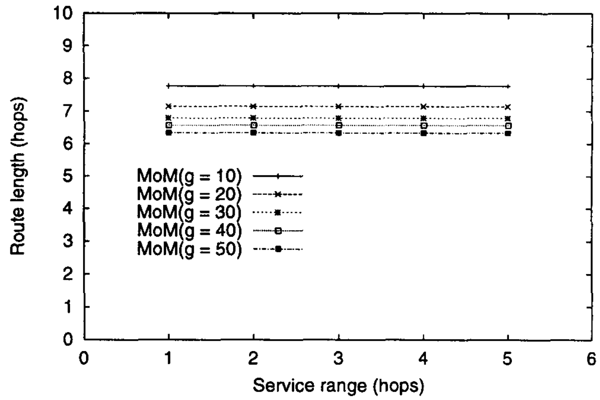

Figure 23: Average path length of MoM (m = 0.1)

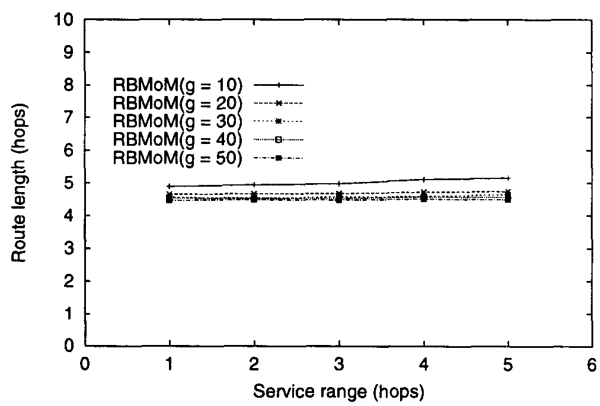

Figure 24: Average path length of RBMoM (m = 0.1)

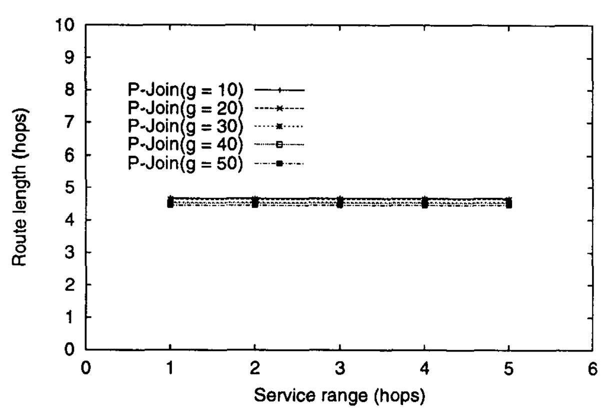

Figure 25: Average path length of Pure-Join (m = 0.1)

delivery route is very important, specially for those delay sensitive applications. Figure 20 - 25 show the average path length of all packets. Consider Figure 20 to 22. For the same number of mobile hosts, MoM has the worst performance among the three protocols because there is no limit for the tunnel length. Pure-Join has the optimal performance because each delivery path is always shortest. RBMoM has the similar performance as Pure-Join. There are two reasons for the results. First, the service range limits the tunnel length. Second and more important, when the FA has already been in the multicast group, all visitors' MHA will be updated to the FA. Thus the delivery paths are shortest. In average, the routing path is near optimal. In Figure 23 to 25, the experiments are done based on the same mobility. Similarly, MoM still has the worst performance owing to the tunneling overhead. In Figure 23, the more mobile members result in better performance. This is because the candidates of the DMSP are limited while the mobile population in the environment is smaller. Therefore, the distance from the selected DMSP to the destination is longer. For RBMoM and Pure-Join, both are dynamic multicast tree policy. The only difference of both is the tree update frequency. RBMoM exploits the service range to control the frequency. The large service range can decrease the tree update frequency. We can compare the results in Figure 21, 22, 24, 25. The path length of RBMoM is near optimal (i.e. similar to Pure-Join) when either the mobility is high or there are more mobile members.

6. CONCLUSIONS

In this paper, we propose a new protocol, RBMoM, which has distinct performance advantage over two other approaches proposed for the mobile multicast problem, namely remote subscription and bi-directional tunneling. Actually, remote subscription and bi-directional tunneling are the extremes of RBMoM. RBMoM intends to trade off between the shortest delivery path and the frequency of the multicast tree reconfiguration by controlling the service range of the multicast home agent. Unlike bi-directional tunneling in which the tunnel length is unlimited, RBMoM uses the service range and MHA to restrict the tunnel length to reduce the cost of tunneling. Only when a mobile host is within the service range of its MHA, it can get the tunneling service from the MHA. When a mobile host is out of the service range of its MHA and moves to a new foreign network, the current FA becomes the new MHA and joins the multicast group. Thus the multicast tree update is not as frequent as remote subscription. The tree maintenance overhead can be much reduced. Importantly, the service range can be controlled in order to adapt to the change of the mobility and the number of the mobile members. In high mobility, the service range is inclined to be large to alleviate the deterioration of the performance because of the multicast tree reconfiguration. However, the cost of the tunneling is increased. If the number of the mobile members is small, the service range is inclined to be small in order to switch the focus on the shorter delivery paths. Furthermore, our protocol has less DMSP handoff. The only cost we should pay in RBMoM is to maintain a MHA and the data structures in the HA.

REFERENCES

[1] A. Acharya, A. Bakre, and B. Badrinath, "IP Multicast Extensions for Mobile Internetworking", *Proc. INFOCOM '96*, San Francisco, CA, March 1996.

[2] A. Ballardie, P. Francis, and J. Crowcroft, "Core Based Trees: An Architecture for Scalable Inter-Domain Multicast Routing", *Proceedings of ACM SIGCOMM '93*, August 1993.

[3] S. Deering and J. Hinden. "Internet Protocol, Version 6 (IPv6) Specification", *RFC 1883*, December 1995.

[4] S. Deering, D. Estrin, et al., "Protocol Independent Multicast-Sparse Mode (PIM-SM): Motivation and Architecture", draft-ietf-idmr-pim-arch-04.ps, October 1996.

[5] T.G. Harrison, C.L. Williamson, W.L. Mackrell, and R.B. Bunt, "Mobile Multicast (MoM) Protocol: Multicast Support for Mobile Hosts", *Proceedings of ACM/IEEE MOBICOM '97*, September 1997.

[6] J. Ioannidis, *Protocols for Mobile Internetworking*, Ph.D. Thesis, Columbia University, 1993.

[7] D. Johnson, "Scalable and Robust Internetwork Routing for Mobile Hosts", *Proceedings of the 14th International Conference on Distributed Computing System*, June 1994.

[8] D. Johnson, A. Myles, and C. Perkins, "The Internet Mobile Host Protocol (IMHP)", *Internet Draft*, February 1994.

[9] J. Moy. "Multicast Extension to OSPF", *Internet Draft*, September 1992.

[10] A. Myles and C. Perkins, "Mobile IP Extensions (MIP)", *Internet Draft*, October 1993.

[11] J. Mysore, V. Bharghavan, "A New Multicasting-based Architecture for Internet Host Mobility", *Proceedings of ACM/IEEE MOBICOM '97*, Budapest, Hungary, September 1997.

[12] C. Perkins, "IP Mobility Support", *RFC 2002*, IBM, October 1996.

[13] C. Perkins, "Mobility IP", *IEEE Communications Magazine*, pp. 84-99, May 1997.

[14] C. Perkins and Y. Rekhter, "Short-cut Routing for Mobile Hosts", *Internet Draft*, IBM T.J. Watson Research Center, 1992.

[15] F. Teraoka, Keisuke Uehara, Hideki Sunahara, and J. Murai, "VIP: A Protocol Providing Host Mobility", *Communications of the ACM*, Vol. 37, No. 8, pp. 67-75, August 1994.

[16] C-K Toh, "A Unifying methodology for Handovers of Heterogeneous Connections in Wireless ATM Networks", *ACM SIGCOMM Computer Communication Review*, pp. 12-30, 1996.

[17] C-K Toh, "Crossover Switch Discovery for Wireless ATM LANs", *ACM Journal of Mobile Networks and Applications*, special issue on routing in mobile communication networks, 1(2):141-165, October 1996.

[18] D. Waitzman, C. Partridge, and S. Deering (editors), "Distance Vector Multicast Routing Protocol", *RFC 1075*, BBN STC and Stanford University, November 1988.

[19] G. Xylomenos and G.C. Ployzos, "IP Multicast for Mobile Hosts", *IEEE Communications Magazine*, pp. 54-58, January 1997.

[20] L. Zhang, S. Deering, D. Estrin, S. Shenker, and D. Zappala, "RSVP:A new Resource ReSerVation Protocol", *IEEE Network*, September 1993.