A Framework for Handling Multicast Source Movement over Mobile IP

Hrishikesh Gossain, Siddesh Kamat and Dharma P. Agrawal
Center for Distributed and Mobile computing
Dept. of ECECS, University of Cincinnati
Cincinnati, OH 45221-0030

Abstract - Recent proposals to provide multicasting over mobile IP focus mainly on recipient mobility and little attention has been given to the case when the mobile host (MH) is also the source. In this paper, we have attempted to address the case when the MH is a source as well as a recipient of a given multicast session and more than one source is participating in the session. The basic essence of the problem is that the effect of receiver movement on the multicast tree is local while it may be global for source movement and it may affect the complete multicast delivery tree. We have used a MH initiated approach for multicast handoff and introduced a unified solution and made the effect of the MH movement local, irrespective of whether it is working as a source or a recipient of a multicast group. We examine and compare our proposed approach to existing approaches by simulating under various traffic environments and we observe an improved performance.

1. INTRODUCTION

Multicasting [1] is the process of sending messages from one source to multiple destinations using the same IP address, called ‘host group address’. Using IGMP [2], hosts can dynamically subscribe to the group to receive multicast traffic. The multicast router inside the domain then takes care of joining the new member to the ongoing multicast session.

When we think of providing multicasting in wireless, the maintenance of this ‘host grouping’ or the multicast delivery tree becomes a major issue. In a mobile environment, we have to focus not only about dynamic group membership, but also on host movement as the MH moves to different domains, which makes maintaining and determining the ‘optimal’ multicast delivery tree difficult. Multicast forwarding algorithms have been designed considering the static nature of hosts. Source based protocols, like DVMRP [3], create problems if a host’s point of attachment changes, as DVMRP forwards multicast packets only if it receives it on the correct interface. This is a serious drawback in a mobile environment, when a MH moves to a new domain, since its interface to the multicast router changes and packets may be dropped. Reliable delivery and packet loss is another major issue in wireless. Due to host movement to different domains, a host may miss some packets, or there may be packet duplication. Internet Engineering Task Force (IETF) has proposed two methods to provide multicasting over Mobile-IP [4], namely Bi-directional Tunnel and Remote Subscription method. The Bi-directional Tunnel method is immune to source movement, but it causes network overload and non-optimal routing due to anchoring of the path from the Home Agent (HA) of the MH to the MH’s present point of attachment. The Remote Subscription method of providing mobile multicasting is more suitable for the case when the MH is only the recipient of the multicast session. If the MH is also the source, it causes overhead due to frequent reconstruction of the complete multicast tree as the MH moves to each foreign domain. Although there are proposals to provide Diff-Serve [5,6,7,8] based IP multicast, QoS enabled wireless multicasting is still an open issue.

The organization of this paper is as follows. Section 2 provides some background on Mobile-IP (MIP) and IP-Multicast, followed by discussions on existing proposals for multicast over Mobile-IP and their comparison and limitations. Section 3 outlines the approach of our protocol. Section 4 gives the results. Finally, Section 5 summarizes and presents the conclusions of this paper.

2. BACKGROUND

2.1 Multicast Over Mobile-IP

A host in the Internet is identified by a unique IP address. The network part of the IP address is used by the routers to route packets to the destination, while the host part is used by TCP for end-to-end delivery of messages. Due to this fact, if a MH moves to a new domain, it cannot be reached using its previous address. So, it is necessary to design a way by which packet delivery to a MH is possible irrespective of its current location and point of attachment. The Mobile IP protocol, proposed by IETF, addresses this issue of location independent addressing by allowing transparent routing of IP datagrams to MHs, irrespective of their current point of attachment. In Mobile IP, each MH is identified by its home address. This home address remains fixed, irrespective of the MH’s current point of attachment. If the MH moves to a new domain, it associates itself with a care-of address (CoA). There are two different ways to obtain this care-of address. CoA may be the address of the FA (Foreign Agent), or it may be a new address obtained by the MH (e.g., by Dynamic Host Configuration Protocol, DHCP [9]) in the foreign domain. The second type of addressing is called co-located CoA. Once it gets its care-of address in the foreign domain, it registers itself with its home agent indicating its care-of address. Thereafter, all the packets meant for the mobile host are tunneled to this CoA.
Table I: Comparison of Mobile IP based multicast routing protocols

<table>
<thead>
<tr>
<th>Mobile-IP Based Protocol</th>
<th>Optimal Routing</th>
<th>Reliability</th>
<th>Packet Redundancy</th>
<th>Multicast Protocol Dependency</th>
<th>Join &amp; Graft delays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Subscription</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Independent</td>
<td>Yes</td>
</tr>
<tr>
<td>Bi-directional Tunneling</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Independent</td>
<td>No</td>
</tr>
<tr>
<td>MMP</td>
<td>No</td>
<td>No</td>
<td>Minimal</td>
<td>Independent</td>
<td>Yes</td>
</tr>
<tr>
<td>MobiCast</td>
<td>Yes</td>
<td>No</td>
<td>Minimal</td>
<td>Independent</td>
<td>Yes</td>
</tr>
<tr>
<td>RM2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Independent</td>
<td>Yes</td>
</tr>
<tr>
<td>MMROP</td>
<td>Yes</td>
<td>Yes</td>
<td>Minimal</td>
<td>Independent</td>
<td>Yes</td>
</tr>
</tbody>
</table>

2.2 Proposals for Multicast over MIP

Before discussing individual proposals, we shall elaborate more on IETF proposed approaches to provide multicast over Mobile IP. As discussed above, in remote subscription, a MH re-subscribes to a multicast group each time it moves to a new foreign network. Bi-directional Tunneling requires that the Home Agent of the MH be a multicast router. If a MH moves to a foreign domain, a bi-directional tunnel is created from its new point of attachment to its home agent (HA). All subscription for the MH is done through the HA. Both these methods address the basic issue of providing multicast over MIP, but they do not address apparent issues when multicast services are extended to mobile IP. Bi-directional tunnel approach creates an interesting situation when mobile hosts, belonging to different HAs, move to the same FA. According to bi-directional tunneling, each of the respective HAs creates a separate bi-directional tunnel to the FA, so that multicast packets can be forwarded to their respective MHs. If these MHs are subscribed to the same group, all the tunnels from different HAs to the FA start carrying the same multicast packet. MoM [10] addresses the issue of the tunnel convergence problem by selecting only one of the HAs among a given set of HAs. The selected HA is called the DMSP (Designated Multicast Service Provider). Other HAs stop sending packets, through their outgoing tunnel to the FA. Although this approach addresses the problem of packet duplication, it may result in temporary disruption of service if the MH belonging to the DMSP moves out of the FA and it is the only MH belonging to the DMSP in the FA. According to Mobile IP specifications, the FA may know about this event only if the registration time expires and till a new DMSP is selected, there may be disruption of service to the MH. Although MoM suggests selecting more than one DMSP at a given time, it results in packet duplication. MMP [11] is used to address micro level mobility for multicasting over MIP. RMDP [12] and RM2 [13] are reliable multicast routing protocols running over mobile IP. MMROP [14] is remote subscription based approach to provide recipient mobility. MobiCast [15] is designed for an internetwork environment with small wireless cells. It adopts a hierarchical mobility management approach to isolate the mobility of the mobile hosts from the main multicast delivery tree. For further details please refer to [10,11,12,13,14,15].

2.3 Problem Definition

This section identifies the problem that we have addressed in this paper. We first start investigating the appropriateness of the IETF proposed standards for the case when the MH is the source as well as the recipient for the same multicast group.

--- Remote Subscription

::: Bi-directional Tunneling

![Initial Multicast tree](image1)

(a) Initial Multicast tree

![Tree after source movement](image2)

(b) Tree after source movement

Fig. 1 Multicast Source Movement

The Bi-directional tunneling solution for multicast over Mobile IP can provide source roaming with no service disruption. Since packets are forwarded from the HA, there is no need of updating the delivery tree due to MH movement. But this method is not so efficient for recipient mobility. Consider Fig. 1a, which shows the initial multicast tree. Fig. 1b shows the anchoring of path from the HA to the MH’s present point of attachment that adds extra delay to packet delivery as well as creates extra network load due to sub optimal path to present point of attachment for the MH. Fig 1b also shows the case of Remote Subscription, where the MH re-subscribes to the multicast group as it moves to a new foreign domain. The re-subscribing in the Foreign Domain builds up an optimal multicast delivery tree, but if the MH is also participating as a source to the multicast group, it may result into network overload due to the rebuilding of the complete multicast delivery tree for each foreign domain that the MH visits. The basic essence of the problem is that the effect of receiver movements on the multicast delivery tree is local, while that of the source movement is global and it may affect the complete multicast delivery tree.

3. Proposed Approach

This section summarizes the basic operation of our multicast scheme and this is an extension of the work proposed in [16]. We propose a unique solution to handle the case when the MH is both source and recipient for the multicast session. It is based on IETF proposed methods for providing multicasting over mobile IP. As mentioned earlier, to handle the case when the MH is both the source and recipient of a multicast session, we have to minimize the possibility of rebuilding the source multicast tree.
In our approach, we use only a reverse tunnel from the MH’s current point of attachment to its HA to forward multicast packets. To receive multicast traffic, we use remote subscription. Consider a source based multicast tree as shown in Fig. 2, with ‘S’ as one of the multicast sources. Assume ‘S’ moves to a foreign domain, which is not presently a member of the multicast group subscribed by ‘S’. ‘S’ sends a multicast join message in its foreign domain and a notify message to its HA. In steps 2 and 3, a bi-directional tunnel is created between HA and FA. In the meantime, it initiates the multicast tree join (4). It should be noted that the existence of bi-directional tunnel is temporary and it is kept till the multicast agent at the foreign domain starts receiving packets from its tree-joining request. Once the FA starts receiving packets from its new branch (5), it checks the packet sequence number from that tunneled to it from the bi-directional tunnel. If there is some missing packet, it waits till the packet is forwarded from the HA. Consequently, it requests to discontinue the forward tunnel from the HA to FA (6) and keeps only the reverse tunnel. By this way, we localize the effect of the MH movement, which is serving both as a source as well as a receiver for the multicast group.

### 3.1 Multicast Handoff

We use a smooth handoff technique to reduce the service disruption for the multicast session during the handoff. The service disruption period due to handoff is mainly contributed by three main entities: 1) Duration at which MH has no network connectivity 2) MH registration period in Foreign Domain 3) Multicast Tree Join in the Foreign Domain. In a given handoff, depending on the group membership in the foreign domain and signal strength, any or all of the above entities may contribute to multicast service disruption.

#### In our approach, we assume a MH initiated handoff. Based on the beacon strength received by the MH, it decides if it needs to handoff to the new FA (Fig. 3). If it is true, it sends a *greet* message to the FA. The *greet* message consists of registration information as well as information relating to the multicast group that the MH is presently subscribed to and the ID of the last received multicast packet. It also sends a *notify* message to its HA indicating the last packet received by it and the ID of the FA. This helps the HA to create a bi-directional tunnel from the HA to FA. The HA replies to the MH with a *Notify Ack* and starts forwarding packets through the forward tunnel. The FA keeps track of the multicast packet ID that it receives in its domain. Once the FA starts receiving multicast packets from its multicast tree join, it compares the packet ID of the multicast data received from both the branches. In case the Tunnel-Packetid >= TreeJoin-Packetid, it sends a *STOPc* message with zero offset to the HA to stop forwarding packets for the groups subscribed by the MH. To avoid the duplicate packets being forwarded to the MH, the FA deletes the packet already forwarded to MH by negative caching. If Tunnel-Packetid < TreeJoin-Packetid, FA sends a *STOPc* message with an offset equals to the packet ID gap between HA and FA. After receiving the *STOPc*, HA forwards the packets requested and then deletes the forward tunnel to FA. This way we avoid packet duplication, which may occur because of reception of packets from two branches. It also prevents sending multiple copies of the same data to the MH and hence saves precious wireless bandwidth. In case FA is already member of the group, it checks the packet ID of the last message received by MH. If MH has missed any packet, FA takes care of forwarding it. There is no forward tunnel created in this case.

In case the MH is also working as a sender for the group, it takes an optimistic approach. Until the MH gets a *greet ack* from FA, it sends multicast packets to HA. Once it receives a *greet ack*, it starts sending multicast packets through FA reverse...
tunnel. Since the packets are forwarded through HA, HA knows exactly if it has missed any packet. If that is the case, it sends a request to retransmit the offset to FA. It is to be noted that the above condition may only happen if the MH has no network connectivity for some time during handoff. By assuming a soft handoff mechanism we can minimize this effect.

4. PERFORMANCE EVALUATION

To simulate our proposed protocol, we have used the LEDA [17] software, which generated a connected graph of 400 multicast enabled nodes. The information contained in the MH and the multicast nodes is as shown in the Table 2.

Table 2: Data Structures for the MH and Multicast Nodes

<table>
<thead>
<tr>
<th>ID of the mobile node</th>
<th>HostID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID of its parent</td>
<td>Parent</td>
</tr>
<tr>
<td>Group membership (boolean)</td>
<td>groupMember</td>
</tr>
<tr>
<td>Source for group (boolean)</td>
<td>Source</td>
</tr>
<tr>
<td>ID of current FA node</td>
<td>currentFA</td>
</tr>
</tbody>
</table>

(a) Information in the MH

<table>
<thead>
<tr>
<th>ID of the Multicast node</th>
<th>nodeID</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of FAs for forwarding</td>
<td>FA_list</td>
</tr>
<tr>
<td>List of new MHs that have moved in</td>
<td>MH_list</td>
</tr>
</tbody>
</table>

(b) Information in the Multicast node

Each HA maintains an ‘away list’ to keep track of which of its MHs are away. Similar to the HA, each Foreign Agent maintains a ‘visitor list’ of MHs that have moved into its domain.

After moving to a new domain, a MH wishing to receive the multicast packets for a specific group, informs the FA that it wishes to join the multicast group. To join a group, an Internet host sends an IGMP reply to the multicast router’s membership query. This is addressed to the multicast group it is attempting to join. Once a FA receives the group join request, it checks if it is presently serving the multicast group requested by the mobile host. If not, it creates a list for the group ‘G’ and adds the MH in its multicast-forwarding list. Then, it creates a bi-directional tunnel to the MH’s HA. In the meantime, it also sends a tree join request. The existence of bi-directional tunnel is temporary and as soon as the FA starts receiving packets from its tree join request, it sends a request to the serving HA to discontinue forwarding packets for the group ‘G’. The HA discontinues forwarding to the FA by negative caching, but it keeps its membership in order to forward the multicast packets for its MHs that will be moving into new domains.

4.1 Results

We have used discrete event simulation in order to compare the relative performance of our approach with bi-directional tunneling and MoM with 1 DMSP. The simulation parameters are given in Table 3.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>Number of Nodes</td>
<td>400</td>
</tr>
<tr>
<td>H</td>
<td># MH/Node</td>
<td>1-30</td>
</tr>
<tr>
<td>MR</td>
<td>MH Mobility Rate</td>
<td>0.1-0.5</td>
</tr>
<tr>
<td>S</td>
<td>Service Time</td>
<td>1</td>
</tr>
<tr>
<td>J</td>
<td>Join Delay</td>
<td>1</td>
</tr>
<tr>
<td>T</td>
<td>Simulation Time</td>
<td>100</td>
</tr>
</tbody>
</table>

The number of hosts in a domain receiving the multicast packets may vary. We have varied the number of mobile hosts at each domain from 1 to 30. Fig. 4 compares the results of our approach with that of MIP-BT and MoM at low mobility rate (0.1).

![Fig.4: Network Load (# Nodes = 400, MR=0.1)](image1)

As shown in Fig. 4, for the case when the MH is both the source and recipient of the multicast group, the network performance is better for the proposed approach. Fig. 5 shows the results with very high mobility rate (0.5).

From the result, we can conclude that the proposed approach is scalable with the number of mobile hosts in a domain as well as with the host moving probability.

![Fig.5: Network Load (# Nodes = 400, MR=0.5)](image2)
Fig. 6 shows the routing distance of a MH from a static source/receiver.

As is evident from the graph, performing remote subscription at each foreign agent reduces the routing distance (the number of hops) needed to receive the multicast packet by the MH from multicast sources. For sending packets, the MH uses reverse tunnel due to which it may have greater number of routing hops needed to reach a particular static host.

5. CONCLUSION

This paper outlines a framework that supports multicast over mobile IP when the mobile host is a sender as well as a receiver for a multicast group. Unlike previous work, which mainly concentrates on recipient mobility, we have considered the case when the MH is also the source. This is a valid assumption, keeping in mind the development of the Internet and the demand of applications like video-conferencing and multiplayer online gaming, which need a multicast framework for groups where members work both as senders and receivers for the same multicast group. The proposed solution has negligible packet duplication. To conclude, we feel that this work is an important initiative towards designing a multicasting framework for handling the source and receiver movement together.

ACKNOWLEDGEMENTS

This work is supported by the Ohio Board of Regents Doctoral Enhancement Funds.

REFERENCES