Mobile IPv6 Multicast with Dynamic Multicast Agent

<draft-zhang-mipshop-multicast-dma-01.txt>

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

This document addresses the problem of delivering IPv6 multicast traffic to MNs (Mobile Nodes). An approach named Mobile IPv6 Multicast with Dynamic Multicast Agent is proposed. The approach is a combination of Movement Based Method [2] and Distance Based Method [3]. Such a design allows MNs to optimize multicast routes, and meanwhile reduces the number of handoffs by selecting new multicast agents dynamically. In addition to weakening the triangle route problem and diminishing the influence of handoff to multicast, this approach provides global mobility in the Internet without the restriction on network topologies.
Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [5].

Table of Contents

Status of this Memo.......................................................1
Abstract................................................................................1
1. Introduction.................................................................3
2. Concepts and Framework..................................................4
3. Operation of MSA............................................................5
4. Operation of DMA..........................................................7
5. DMA switch decision-making algorithm in DMA......................9
6. Conclusion.....................................................................9
7. Acknowledgements.........................................................10
8. Informative Reference.....................................................10
9. Normative Reference.......................................................10
10. Authors’ Addresses.......................................................11
11. Intellectual Property Statement........................................11
1. Introduction

Multicast is an efficient way for forwarding data from one node or multi-nodes to multi-nodes. Supporting mobility becomes an inevitable function of multicast technologies.

The mobility support for IPv6 protocol [1] has specified two basic methods for mobile multicast: 1) via a bi-directional tunnel from a MN to its HA (Home Agent), that is called MIP-BT (Mobile IP Bi-directional tunnel); 2) via a (local) multicast router on the foreign link being visited, that is called MIP-RS (Mobile IP Remote Subscription). In MIP-BT, the MN tunnels its multicast group membership control packets to its HA, and the HA forwards multicast packets down the tunnel to the MN [1]. In MIP-RS, the MN MUST use its care-of address and MUST NOT use the Home Address destination option when sending MLD (Multicast Listener Discovery) packets [1,4].

These two basic methods can retain multicast communications when MNs move, but some issues exist.

- First, MIP-BT suffers the triangle route which is composed of MN-HA tunnel and HA-S multicast tree path. When the MN is far from its HA, the data forwarding path of multicast becomes deteriorative.

- Second, multiple tunnels from a subnet to a HA are established in MIP-BT, when some MNs that come from the same home link attach at one AR (Access Router) in the subnet and these MNs join the same multicast group at the same time. This case is called tunnels congregation which leads to more network resources being consumed.

- Third, although the multicast path in MIP-RS is optimal, the frequent handoffs of a MN, which are due to the movement of the MN among subnets, produce much latency. This is because the handoff action makes the MN leave and re-join the multicast group frequently.

This document addresses these above problems. An approach named Mobile IPv6 Multicast with Dynamic Multicast Agent is proposed, which accepts the merits of MIP-BT and MIP-RS. This approach combines Movement Based Method and Distance Based Method to select a new multicast agent dynamically, and the new selected multicast agent is responsible for forwarding multicast data to the MN.
Such a design allows MNs optimize multicast routes and meanwhile reduce the number of handoffs. In addition to weakening the triangle route problem and diminishing the influence of handoff to multicast, this approach provides global mobility in the Internet without the restriction on network topologies.

In the following sections, we will first introduce the concepts and framework of the approach. Then, we will describe the details of Dynamic Multicast Agent switch procedure.

2. Concepts and Framework

In this document, two key roles are defined for Mobile IPv6 Multicast with Dynamic Multicast Agent:

- **MSA**: Multicast Subnet Agent, which is the access router running multicast protocols in a subnet and forwarding the subscribed multicast data to the MN that visits the subnet.

- **DMA**: Dynamic Multicast Agent, which is the current MSA or one of the previous MSAs of the MN acting as the leaf router in a multicast delivery tree the MN subscribed and forwarding the subscribed multicast data to the MN through its current MSA.

MSA is in charge of the local multicast group membership management and maintenance in a subnet via MLD protocol. MSA periodically sends regular MLD query messages to solicit regular MLD reports from the MNs visiting the subnet.

The MN does regular MLD reports and tell its previous MSA address to the current MSA.

When a MN first subscribes a multicast group G, its current MSA becomes its initial DMA, which joins the subscribed multicast delivery tree as a leaf router and then forwards the subscribed multicast data to the MN.

Within an acceptable roaming distance, the DMA of a MN will not change although its visited MSA changes if its visited MSA doesn’t yet have the group G membership in the subnet. When the MN’s current MSA is different from its DMA, its current MSA receives the group G multicast data from its DMA via a short tunnel, and then forwards the multicast data to the MN.

Beyond this acceptable roaming distance, the MN’s DMA will be switched to the new MSA that the MN currently is visiting.
By introducing the concept of DMA, it is avoidable for all recently visited MSA of the MN along its roaming path to successively join and leave the subscribed multicast delivery tree as a leaf router. In this approach, only MSAs selected as a DMA need to join the subscribed multicast delivery trees as a leaf router.

In comparison with the Static Multicast Agent approach (e.g. MAP in HMIPv6 [5]), this DMA approach is quite distributed. So the risk of Static Multicast Agent being performance bottleneck and resulting long tunnels and large tunnel numbers can be avoided.

In comparison with MIP-BT approach, this DMA approach optimizes multicast transmit paths due to the shortest path from DMA to multicast source. So the triangle routes, long tunnels and large tunnel numbers can be avoided.

In comparison with MIP-RS approach, this DMA is quite effective. The frequency of remote multicast subscription and multicast delivery tree restructuring is quite reduced.

3. Operation of MSA

MSA is in charge of the local multicast group membership management and maintenance in a subnet via MLD protocol. MSA periodically sends regular MLD query messages to solicit regular MLD reports from the MNs visiting the subnet.

MSA maintains a Multicast Route Table used for receiving and forwarding the subscribed multicast data. There are four elements kept in every entry of the Multicast Route Table: Group Address, Membership (INCLUDE or EXCLUDE mode), Tunnel_State, Tunnel_ID, and Outgoing Interface List.

- Tunnel_ID is the identifier of a tunnel between MSA and DMA for MSA to receive the multicast data of the Group from DMA.

- Tunnel_State is a flag that represents whether Tunnel ID is valid and whether MSA has created a tunnel for the Group and is receiving the multicast data of the Group via the tunnel.

MSA also maintains a Visitor Table for support of DMA switch process. There are two elements kept in every entry of the Visitor Table: MN and DMA.

- MN item records the IP address of a MN visiting the subnet and being a multicast subscriber.
o DMA item records the IP address of the MN’s DMA.

---
<table>
<thead>
<tr>
<th>MN</th>
<th>DMA</th>
</tr>
</thead>
</table>

On arriving at a new visited subnet, a MN obtains a new CoA (Care of Address) and registers its current CoA with its Home Agent. Then the MN immediately sends regular MLD reports to its current subnet’s MSA and the IP address of the previous subnet’s MSA. The MSA communicates with the MN’s previous MSA to obtain the IP address of the MN’s previous DMA. When receiving the MLD group membership report sent from a visitor for group G, the MSA operates as follows:

- If there already is an entry for group G in the MSA’s multicast route table, the MSA adds the MN to the entry’s outgoing interface list, and then examines the Tunnel_State. If the Tunnel_State is ‘YES’, it represents that the MSA has already created a tunnel for the group and is receiving multicast data via the tunnel. In this case, it simply forwards the MLD group membership report message to the other end of the tunnel.
  - If there already is an entry for the MN in the MSA’s Visitor Table, then the MSA keeps it.
  - Otherwise, if there is no entry for the MN in the MSA’s Visitor Table, then the MSA creates a new entry for the MN. In order to optimize the delivery path, the DMA of the MN is switched to the MSA itself. And then the MSA informs the previous DMA to clear the states of the MN if available.

- If there is no entry for group G in the MSA’s multicast route table, (i.e. the MN is the first group member of group G in the subnet), then MSA creates a new entry for group G in its multicast route table and adds the MN into the entry’s outgoing interface list.
  - If there already is an entry for the MN in the MSA’s Visitor Table, and if the MSA itself is the DMA of the MN, the MSA simply sends PIM Join messages to the multicast delivery tree. But if the MSA itself is not the DMA of the MN, the MSA creates a tunnel to the DMA of the MN, records the Tunnel_ID, sets the Tunnel_State to ‘YES’, and forwards the MLD group membership report message to the other end of the tunnel.
- If there is no entry for the MN in the MSA’s Visitor Table, the MSA creates an entry for the MN, and asks the MN’s previous DMA if it needs to be switched to the MSA itself. If the MN’s DMA doesn’t need to be switched to the MSA itself, the MSA adds the MN’s DMA into the entry, creates a tunnel to the MN’s DMA, records the Tunnel_ID, sets the Tunnel_State to ‘YES’, and forwards the MLD group membership report message to the other end of the tunnel. If the MN’s DMA needs to be switched to the MSA itself, the MSA adds itself into the entry, acts as the MN’s DMA, and sends PIM Join messages to the multicast delivery tree.

The MSA detects the MN’s departure by the timeout of timer. When the MSA detects that a MN is departing from the current subnet, it deletes the entry for the MN in its Visitor Table. For each multicast group which the leaving MN subscribed, the MSA deletes the MN from the group’s outgoing interface list.

4. Operation of DMA

DMA is in charge of joining the multicast delivery tree of the group G that a MN subscribed via PIM-based protocol as a leaf router. It receives the multicast data of group G and forwards the data to the MN through the MN’s current MSA.

When a MN first subscribes a multicast group G, its current MSA becomes its initial DMA. Within an acceptable roaming distance, the DMA of a MN will not change although its MSA changes if its MSA doesn’t yet have the group G membership in the subnet. So the DMA of a MN may be its current MSA or one of its previous MSAs. At a time only one DMA serves the MN for its subscribed multicast group G.

When receiving the MLD group membership report sent from its served MN for a new group G, the DMA sends PIM Join messages to join the multicast delivery tree of the group G as a leaf router. When DMA switch happens or the MN leaves the group G, the DMA sends PIM Prune messages to prune itself from the multicast delivery tree of the group G.

DMA maintains a table to record the MN’s recent attachment history, which is used for DMA to do DMA switch decision-making for the MN. There are three elements kept in every entry of the Table: MN, MSA and Increment.

- MN item records the IP address of the MN that the DMA serves;
o MSA item records the IP address of the MSA in each subnet that the MN recently roamed through;

o Increment item records the path increment of each MSA.

The first MSA is the DMA itself, which creates the table, initiates the MN item, creates an entry for the first MSA and puts itself in the entry.

When a MN enters into a new subnet, the MSA in this subnet receives the MLD group member report and the IP address of the MN’s previous MSA from the MN. The MSA communicates with the MN’s previous MSA to obtain the IP address of the MN’s previous DMA. To maintain the recent attachment history table of the MN, the MN’s DMA operates as follows:

According to the operation of MSA as described in Section 3,

- if the DMA of the MN is switched to the MSA itself, the MSA informs the previous DMA to clear the states of the MN if available. Then the MSA acts as the MN’s current DMA, creates and initiates the recent attachment history table for the MN. The MN’s previous DMA deletes the recent attachment history table of the MN and prunes itself from the multicast delivery tree of the group G.

- if the DMA of the MN is not switched to the MSA itself, the MSA communicates with the MN’s previous DMA to ask whether it can continue acting as the MN’s DMA. The MN’s previous DMA creates an entry for the MSA in the recent attachment history table of the MN, and then makes the decision according to the DMA switch decision-making algorithms in DMA as described in Section 5.
- If the decision is ‘Yes’, then the MSA acts as the MN’s current DMA, creates and initiates the recent attachment history table for the MN. The MN’s previous DMA deletes recent attachment history table of the MN and prunes itself from the multicast delivery tree of the group G.

- If the decision is ‘No’, the MN’s previous DMA continues acting as the MN’s DMA. The MSA receives the group G multicast data from the DMA via a tunnel and forwards the data to the MN.

5. DMA switch decision-making algorithm in DMA

In DMA, the key point is the algorithm of DMA switch decision-making based on movement and distance. As described in Section 4, DMA maintains a table to record the MN’s recent attachment history (namely History_Table), which is used for DMA to do DMA switch decision-making for the MN.

The DMA switch decision-making algorithm could be simple or precise. The main principle is that there should not be any DMA switch for an MN within an acceptable roaming distance if the MN’s visited MSA doesn’t yet have the group G membership in the subnet.

Here, we just provide a simple algorithm via checking the path increment of the recently joined MSA.

When the path increment of MSAs in the DMA’s History_Table reaches the assigned threshold, DMA switch happens. So the DMA deletes the recent attachment history table of the MN and prunes itself from the multicast delivery tree of the group G. Meanwhile, the MN’s current MSA acts as its new DMA, which joins the multicast delivery tree of the group G as a leaf router, creates and initiates the recent attachment history table for the MN.

The path increment of a MSA can be defined as:

\[ 1 + \text{Minimum} \{\text{Distance}(\text{MSA}, \text{DMA}), \text{Distance}(\text{DMA}, \text{MN})\}, \]

where Distance[x] is the minimum integer greater than or equal to x. For example, the path increment of a MSA is 1 if the MSA itself is the MN’s DMA.

6. Conclusion

This document has discussed the delivering of IPv6 multicast traffic
to mobile nodes. The presented approach is a compromised approach between MIP-BT and MIP-RS, using a Dynamic Multicast Agent to join the multicast delivery trees instead of a static multicast agent. The use of MSA and DMA is the key feature of the approach. The purpose is to optimize the multicast path to MNs, and meanwhile reduce the latency and the impact on multicast trees which result from the roaming of MNs. By introducing the concept of DMA, it reduces the frequent remote subscription and multicast delivery tree restructuring, and avoids the long tunnels and the large number of tunnels.

7. Acknowledgements

We would like to thank Thomas Schmidt, and Kishore Mundra for their valuable comments and suggestions on this document.

8. Informative References


9. Normative References

10. Authors’ Addresses

Hong-Ke Zhang, Bo Shen, Bing-Yi Zhang
IP lab, Beijing JiaoTong Univ.
Beijing, China, 100044
Tel: +86 10 51685677
Email: hkzhang@center.njtu.edu.cn
bingyizhang@hotmail.com

En-Hui LIU
Huawei Technologies Co., Ltd.
Beijing, China, 100085
Tel: +86-10-82882495
Fax: +86-10-82882537
Email: LEH10814@huawei.com

Spencer Dawkins
Huawei Technologies Co., Ltd.
TX, USA, 75075
Email: sdawkins@futurewei.com

11. Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any
Intellectual Property Rights or other rights that might be claimed to
pertain to the implementation or use of the technology described in
this document or the extent to which any license under such rights
might or might not be available; nor does it represent that it has
made any independent effort to identify any such rights. Information
on the procedures with respect to rights in RFC documents can be
found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any
assurances of licenses to be made available, or the result of an
attempt made to obtain a general license or permission for the use of
such proprietary rights by implementers or users of this
specification can be obtained from the IETF on-line IPR repository at

The IETF invites any interested party to bring to its attention any
copyrights, patents or patent applications, or other proprietary
rights that may cover technology that may be required to implement
this standard. Please address the information to the IETF at ietf-
ipr@ietf.org.