Network Working Group
Internet Draft

Hong-Ke Zhang
Xiao-Hua Chen
Jian-Feng Guan
Bo Shen
Beijing Jiaotong University
En-Hui Liu
Spencer Dawkins
Huawei Technologies Co.,Ltd.

Expires: July 2007 January 29, 2007

Mobile IPv6 Multicast with Dynamic Multicast Agent
draft-zhang-mipshop-multicast-dma-03.txt

Status of this Memo

Abstract

This document addresses the problem of delivering IPv6 multicast traffic to MN (Mobile Node). An approach named Mobile IPv6 Multicast with Dynamic Multicast Agent is proposed which combines Movement Based Method [2] and Distance Based Method [3], Such a design allows MN to optimize multicast route, and meanwhile reduce the handoff frequency by selecting new multicast agent dynamically. In addition to weakening the triangle route problem and diminishing the influence of handoff to multicast, this approach provides global mobility in Internet without limitations on network topology. This draft is the same as the earlier version, it is just an update of it.

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

1. Introduction

Multicast is an efficient way for forwarding data from one node or multi-nodes to multi-nodes. mobility support 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 MN to its HA (Home Agent), which is called MIP-BT (Mobile IP Bi-directional Tunnel); 2) via a (local) multicast router on the foreign link being visited, which is called MIP-RS (Mobile IP Remote Subscription). In MIP-BT, 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, 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 MN moves, but some issues still exist.

- First, MIP-BT suffers from 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 will consume more network resources.

- Third, although the multicast path in MIP-RS is optimal, frequent handoffs of MN among subnets will produce much latency. Because when MN handovers , it will leave and re-join the multicast tree and multicast group frequently.

This document addresses these above problems. An approach named Mobile IPv6 Multicast with Dynamic Multicast Agent is proposed. This approach combines the advantages of MIP-BT and MIP-RS, selecting a new multicast agent based on both movement and distance dynamically, and the new selected agent is responsible for forwarding multicast data to the MN.

Such a design optimizes the multicast routes and reduces handoff frequency. Beside releasing triangle route problem and diminishing the influence of handoff to multicast, it can also provide global mobility without limitation on network topology.

In the following sections, we will first introduce the concepts and framework of this 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.

The whole procedure of this approach is shown in Figure1.

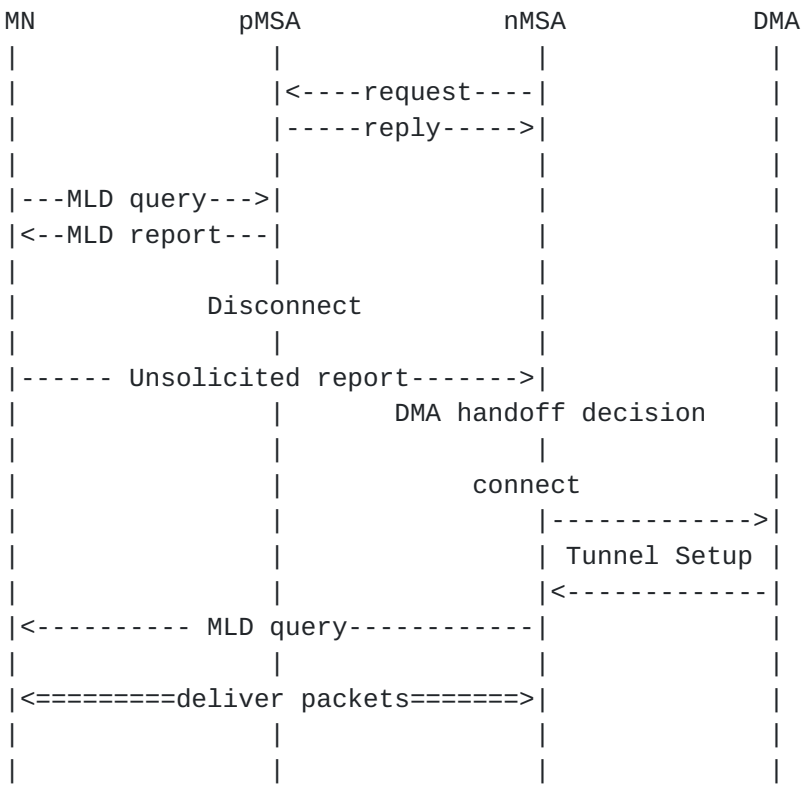


Figure 1 Operation process of MSA and DMA

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. To learn address information of neighbor MSAs, each MSA sends request message(e.g. PIM Hello message etc.) periodically, receivers send reply message to the sender, informing it their address information.

In this approach, tunnel between nMSA and DMA is setup after MN has attached to nMSA. In order to shorten MN's handover latency, Fast Handover protocol[6] and CARD(Candidate Access Router Discovery) protocol[7] can be adopted. In these two approaches, tunnel is setup before the handover process, so after MN attaches to the nMSA, it can transmit data immediately, handover latency can be reduced Dramatically.

When MN first subscribes a multicast group G, its current MSA becomes its initial DMA, which runs multicast protocol and 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 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 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. Then the MSA will run multicast protocol and operate as DMA. In this case, multicast packets will be delivered from DMA directly to MN without tunnel.

In this approach, not all visited MSA along MN's roaming path will join the subscribed multicast delivery tree by introducing the concept of DMA. only that selected as DMA need join the delivery trees as a leaf router.

In comparison with other Agent selection approaches (e.g. MAP in HMIPv6 [5]), this DMA selection method is quite distributed, so the problem of performance bottleneck can be released.

In comparison with MIP-BT approach, this DMA approach optimizes multicast transmission path by using shortest path from DMA to multicast source. So disadvantages of MIP-BT such as triangle route, large amount and long distance of tunnels can be avoided.

In MIP-RS, every MSA is a leaf router of the subscribed multicast tree. once MN moves from the coverage of one MSA to another, it will leave the old MSA and attach to new MSA, which will consume more network resources. This DMA approach can reduce the frequency of remote multicast subscription and that of multicast delivery tree reconstructing dramatically, simplifying MN's signaling procedure, network performance is enhanced.

3. Operation of MSA

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

MSA maintains a Multicast Route Table used for receiving and forwarding the subscribed multicast data. There are six components kept in every entry of the Multicast Route Table: Group Address, Filter Modes(INCLUDE or EXCLUDE mode), Source_Address List, Tunnel_State, Tunnel_ID, and Egress Interface List.

- Filter Modes defines host and router parts of the protocol respectively to support the source filtering function.

- Source_Address List records all source addresses which should be included or excluded according to the filter modes.

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

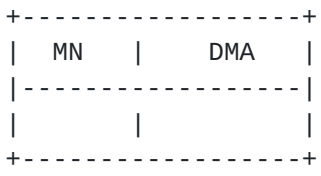
- Tunnel_State is a flag that represents whether Tunnel ID is valid and whether MSA has created a tunnel for the Group and is receiving the multicast data of the Group via the tunnel.

- Egress Interface List composes all receivers egress interface of this group. multicast data should be forward to these interfaces.

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.

- DMA item records the IP address of the MN's DMA.



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 unsolicited report message 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 ingress 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.

- o 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.

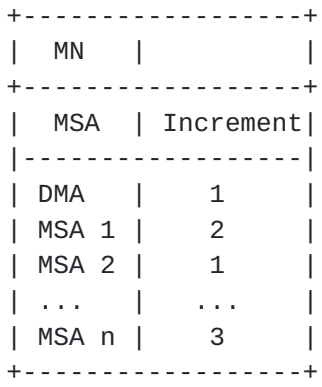
When a MN first subscribes a multicast group G, its current MSA becomes its initial DMA. Within an acceptable roaming distance, the DMA of a MN will not change although its MSA changes if its MSA doesn't yet have the group G membership in the subnet. So the DMA of

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 called History-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;
- MSA item records the IP address of the MSA in each subnet that the MN recently roamed through;
- 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 + Minimum [Distance(MSA,DMA),Distance(DMA,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. Security Considerations

This specification introduces a new concept to Mobile IPv6, namely, a Dynamic Multicast Agent that acts as a multicast agent. It is crucial that the security relationship between the Multicast Source Agent and the DMA is strong; it MUST involve mutual authentication, integrity protection, and protection against replay attacks. Confidentiality may be needed for payload traffic. The absence of any of these protections may lead to malicious mobile nodes impersonating other legitimate ones or impersonating a DMA. Any of these attacks will undoubtedly cause undesirable impacts to the mobile node's communication with all correspondent nodes.

7. IANA Considerations

See [9] for instructions on IANA allocation.

8. Conclusions

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.

9. Acknowledgments

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

10. References

10.1. Normative References

[1] Johnson, D., Perkins C., and Arkko, J., "Mobility Support in IPv6", RFC 3775, June 2004.

[2] Zhang, J. Y. "Location Management in Cellular Networks". 2001.

[3] Bar-Noy, A. Kessler, I. and Sidi, M. "Mobile Users: To update or not to Update?", Wireless Networks Journal, 1995,1(2):175-86.

[4] Deering, S., Fenner, W. and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.

[5] Soliman, H., Castelluccia, C., El-Malki, K., Bellier, L. "Hierarchical Mobile IPv6 mobility management", draft-ietf-mipshop-hmipv6-04 (work in progress), December 2004.

[6] Koodli, R., Ed., "Fast Handovers for Mobile IPv6", RFC4068, July 2005.

[7] M. Liebsch, Ed., A. Singh, Ed.,H. Chaskar.,D. Funato.,E. Shim "Fast Handovers for Mobile IPv6", RFC 4068, July 2005.

10.2. Informative References

[8] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[9] Kempf, J., "Instructions for Seamoby and Experimental Mobility Protocol IANA Allocations", RFC 4065, July 2005.

Author's Addresses

Hong-Ke Zhang, Bo Shen, Bing-Yi Zhang
IP lab, Beijing JiaoTong Univ.
Beijing, China, 100044

Phone: +86 10 51685677
Email: hkzhang@center.njtu.edu.cn
bingyizhang@hotmail.com

En-Hui LIU
Huawei Technologies Co., Ltd.
Beijing, China, 100085

Phone: +86-10-82882495
Fax:+86-10-82882537
Email: LEH10814@huawei.com

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

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.