Internet Draft
Internet Engineering Task Force
draft-jung-mipshop-fhmipv6-00.txt
Expires April 2006

HeeYoung Jung, ETRI
Hesham Soliman, Flarion
SeokJoo Koh, KNU
Noriaki Takamiya, NTT Software

October 2005

Fast Handover for Hierarchical MIPv6 (F-HMIPv6)

Status of this Memo

Copyright Notice

Abstract

This document proposes a scheme to support Fast Handover over HMIPv6 networks. The HMIPv6 was developed to reduce the signaling overhead and delay concerned with Binding Update in Mobile IPv6. Therefore HMIPv6 still need a further handover enhancement for supporting the real-time applications. Currently FMIPv6 is the typical protocol to reduce the handover latency. Accordingly it may be straightforward to simply introduce FMIPv6 into HMIPv6 networks. However, it is noted that such simple approach may induce unnecessary processing overhead. F-HMIPv6, described in this document, considers how to integrate these two protocols and provides a scheme for effective integration.

Table of Contents

1. Introduction

The HMIPv6 [4] was developed to reduce the signaling overhead and delay concerned with Binding Update (BU) in Mobile IPv6 [3]. In HMIPv6, when a MN moves within a MAP region, the MN only sends a local BU to the local MAP, rather than the Home Agent (HA) and Correspondent Node (CN), as done in Mobile IPv6. If the distance from the MN to HA/CN is long, this local BU will considerably reduce the time required for the binding update.

However, the HMIPv6 still need a further enhancement for supporting the real-time applications because HMIPv6 only concern with the latency due to BU and does not touch the latency related to Movement Detection and CoA configuration/Verification. Currently, the FMIPv6 [5] is the typical protocol that was designed to reduce the latency due to these two remaining issues. Therefore, if we want to support the fast handover scheme in HMIPv6 network, the simplest approach will be to apply the FMIPv6 to the HMIPv6 in the straightforward way.

We describe in this document how to use FMIPv6 over HMIPv6 networks so as to provide better handover performance during handover. At a glance, it may be straightforward to simply integrate the FMIPv6 scheme with HMIPv6. However, such simple integration may induce unnecessary processing overhead for re-tunneling at the previous Access Routers and also inefficient usage of network bandwidth. The main reason for this is that the operation of HMIPv6 mainly depends on the functionality of a MAP, while the major functionalities of FMIPv6 are located in Access Routers (AR).

This document describes a Fast Handover scheme for HMIPv6, named F-HMIPv6. In F-HMIPv6, the main operation for handover is accomplished by using MAP, rather than Access Router (i.e. PAR and NAR) like in FMIPv6. For this purpose, the MN exchanges the signaling messages for handover such as RtSolPr, PrRtAdv, FBU, and FBACK with MAP, not PAR. The F-HMIPv6 utilizes the FMIPv6 messages for handover support without further defining any new messages. For the use of F-HMIPv6, it is proposed to define a new flag 'F' in the HMIPv6 MAP option.

2. Terminology

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 [2].

This document uses all the terminology described in the MIPv6, HMIPv6, and FMIPv6 documents. In addition, this document uses the following terms for the on-link Care of Address (LCoA):

PLCoA: MN's LCoA valid on the Previous Access Router (PAR). It corresponds to the PCoA of the FMIPv6.

NLCoA: MN's LCoA valid on the New Access Router (NAR). It corresponds to the NCoA of the FMIPv6.

3. Motivations

A natural and straightforward choice to combine FMIPv6 with HMIPv6 is to directly apply the FMIPv6 handover scheme in HMIPv6 networks, as they are specified. In this case, a bi-directional tunnel will be established between PAR and NAR via MAP by the FMIPv6 procedures. In this case, it may possibly induce inefficient signaling and data forwarding path.

Figure 1 shows the data flow during handover by the simple integration of FMIPv6 with HMIPv6.

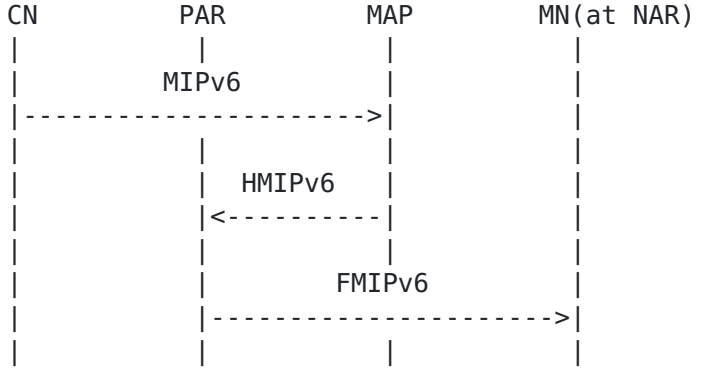

Figure 1: Data flows in the simple scheme

According to the HMIPv6 operations, the data packets sent by CN will arrive at MAP and then be tunneled to MN over PLCoA. When the handover is initiated, a bi-directional tunnel will be established between PAR and NAR according to the FMIPv6 procedures. To forward the data packets to the NAR by using the tunnel, the PAR must first intercept those data packets flowing from the MAP, and then perform the re-tunneling process. This may be done by adding a new outer IP header of <Source = PAR, Destination = NAR> to the data packets sent by MAP according to the HMIPv6 operations.

In the viewpoint of the HMIPv6 operations, the above straightforward approach has the following disadvantages:

(1) The PAR must perform the tunneling operations for fast handover, in addition to the HMIPv6 tunneling from MAP to MN. To do this, the PAR must first intercept the data packets flowing from the MAP, which will be an additional overhead for HMIPv6. It is noted that the data delivery in HMIPv6 is performed based on MAP.

(2) In HMIPv6, the actual data path of the bi-directional tunnel between PAR and NAR may include the MAP (i.e., PAR-MAP-NAR). Accordingly, the data packets will flow twice along the path between ARs and MAP. This induces inefficiency of network bandwidth usage, especially when ARs are connected to the network through bandwidth-limited links.

(3) During handover, the possibility that the tunneled packets from PAR to NAR before F-BU arrive later at NAR than the packet sent directly from MAP by F-BU is relatively high. It will be the cause of the reversed sequence packets in NAR and the packets with reversed sequence makes TCP performance worse.

(4) From such detouring feature, the overall handover latency and tunneling overhead may increase during the handover period. Moreover, it is likely to be difficult to exploit the advantages of FMIPv6 and HMIPv6 as well.

(5) In hierarchical architecture like HMIPv6, the maintenance of information for neighbor ARs in each AR may be overhead.

From the observations described above, it is clear that the fast handover for HMIPv6 needs to be designed by considering the data transport features of the HMIPv6 (i.e., in HMIPv6, all data packets are intercepted by MAP and delivered over the tunnel between MAP and MNs).

4. Overview of F-HMIPv6

4.1 Reference Architecture

Figure 2 illustrates a reference configuration of the F-HMIPv6 network for fast handover support. In the figure, the MAP acts as an aggregation router in the hierarchical domain.

When a mobile node (MN) enters a new HMIPv6 domain, firstly it performs the HMIPv6 registrations procedures with HA and MAP, as per MIPv6 and HMIPv6. Also, if the MN moves from a previous AR (PAR) to a new AR (NAR) within the domain, it will follow the Local Binding Update procedures of HMIPv6. At that time, if the fast handover is required for an on-going data session between MN and CN, then the F-HMIPv6 scheme will apply to the MN, ARs and MAP.

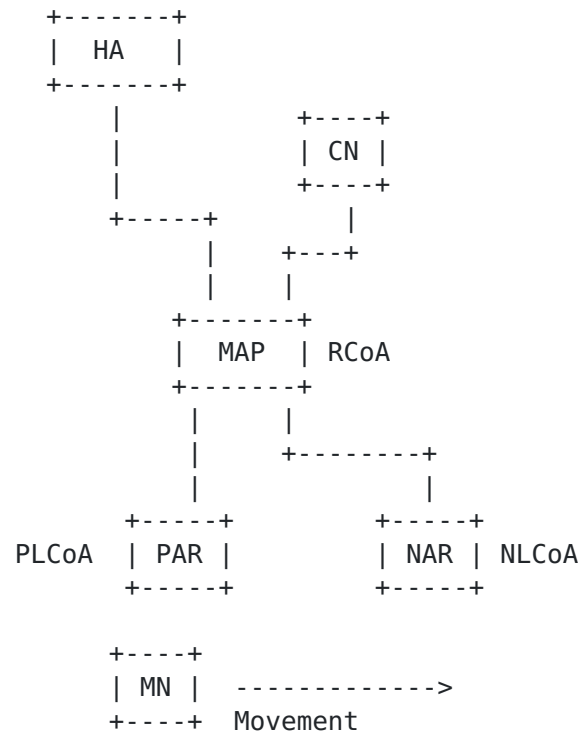

Figure 2: Reference Architecture for F-HMIPv6

4.2
Optimized data Flows in F-HMIPv6

By the F-HMIPv6 scheme, the data packets sent by CN will be tunneled by the MAP toward the NAR during the handover.

Figure 3 illustrates the data flows that F-HMIPv6 is willing to achieve.

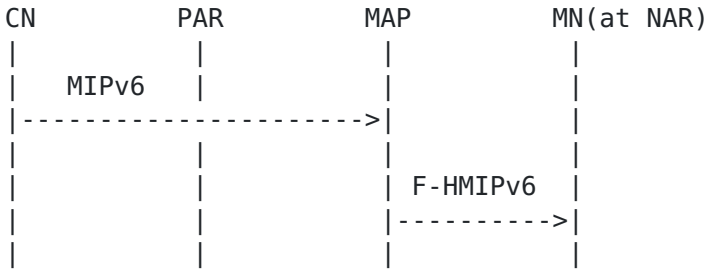

Figure 3: Optimized data flows by F-HMIPv6

Before handover, according to the HMIPv6 operations, the data packets sent by CN are tunneled by MAP to MN with the following IP fields:

- o Inner IP header: <Source = CN, Destination = RCoA of MN>
- o Outer IP header: <Source = MAP, Destination = PLCoA of MN>

When the F-HMIPv6 handover is triggered (e.g., by receiving the FBU message from the MN), the MAP will establish a bi-directional tunnel with the NAR, and then begin to forward the data packets to the NAR over the tunnel. By the tunnel, each data packet has an additional outer IP header to the normal HMIPv6 headers with the following IP fields:

- o Additional outer IP header: <S = MAP, Destination = NAR>

When receiving the tunneled data packets from the MAP, the NAR will de-capsulate them and then be caching the decapsulated data packets. When the MN moves into the NAR region, the NAR will deliver the cached data packets to the MN, as done in FMIPv6.

5. F-HMIPv6 Operations

In this section, we describe the generic F-HMIPv6 operations. It is assumed that the handover anticipation is supported with appropriate layer 2 triggers; and that the MNs as well as ARs are aware of the F-HMIPv6 scheme described in this document.

The F-HMIPv6 procedures described in this section are based on the assumption that the MAP already has the information necessary for handover support about the ARs located in the HMIPv6 domain. It could be achieved by operators manual configuration, or with the help of a signaling operation between ARs and MAP, which will be described in Section 6.4. This information should include the link-layer address (or identifier) and network prefix of each AR.

5.1 Mobile-Initiated Handover

Figure 4 illustrates the generic procedures for F-HMIPv6 operations.

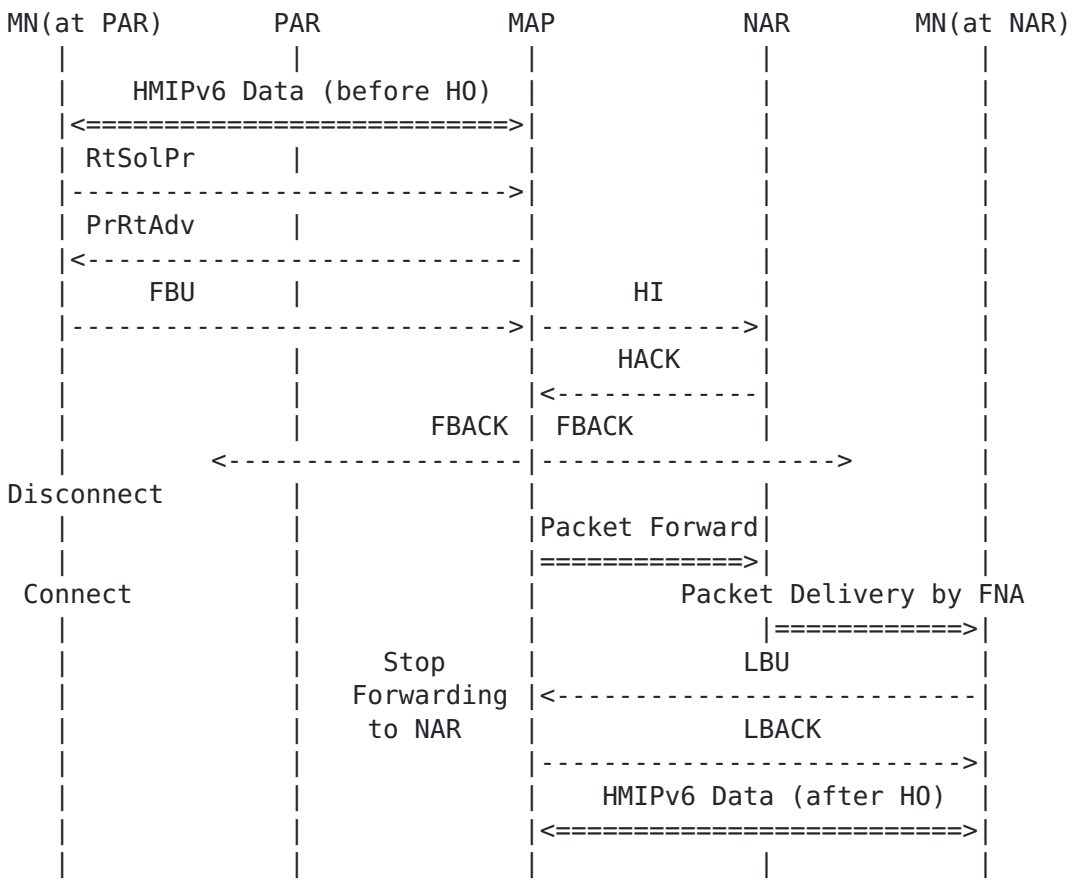

Figure 4: F-HMIPv6 for Mobile-Initiated Handover

Note that the control messages depicted in Figure 4 have identical format to those in FMIPv6; only the contents (the IP source and destination fields) are different. These values are described more in details in Section 6.

The detailed description for the control flows are given below:

1) Based on L2 handover anticipation, the MN sends RtSolPr message to MAP. The RtSolPr SHOULD include information about the link layer address or identifier of the concerned NAR.

2) In response to the RtSolPr message, the MAP sends the PrRtAdv message to the MN, which SHOULD contain information about NLCoA for the MN to use in the NAR region; i. e, NARs network prefix for stateless auto-configuration or NLCoA for stateful configuration.

3) Note in F-HMIPv6 that the MAP SHOULD already know the network prefix and link layer address of the associated NAR.

4) The MN sends Fast Binding Update (FBU) message to MAP. The FBU message contains PLCoA and IP address of the NAR.

5) After receiving the FBU message from MN, the MAP will send a Handover Initiate (HI) message to the NAR so as to establish a bi-directional tunnel.

   In response to the HI message, the NAR will set up a host route entry for the MN's PLCoA and then respond with a Handover Acknowledge (HACK) message.

   As a result, a bi-directional tunnel between MAP and NAR will be established. Over the tunnel, the data packets sent by MAP have the additional outer IP header with the following IP fields of <Source = MAP, Destination = NAR>. The NAR may cache those data packets flowing from the MAP, until it receives the RS (possibly with FNA option) message from the newly incoming MN.

6) The MAP sends Fast Binding ACK (FBACK) messages toward the MN over PLCoA and NLCoA. Then, the MAP will begin to forward the data packets destined to MN to the NAR by using the established tunnel.

7) The MN sends FNA messages to NAR, when it detects that it is moved in the link layer, and receives the responding RA from the NAR. Then, the NAR delivers the buffered data packets to the MN over NLCoA.

8) The MN then follows the normal HMIPv6 operations by sending a Local Binding Update (LBU) to MAP, as per HMIPv6.

   When the MAP receives the new Local Binding Update with NLCoA from the MN, it will stop the packet forwarding to NAR and then clear the tunnel established for fast handover.

9) In response to LBU, the MAP sends Local Binding ACK (LBACK) to MN, and the remaining procedures will follow the HMIPv6.

5.2 Network-Initiated Handover

This section describes the F-HMIPv6 operations for the network-initiated handover. In the network-initiated case, it is assumed that the PAR or NAR detects the movement of the MN from the PAR toward the NAR.

Figure 5 illustrates the F-HMIPv6 operations for the network-initiated handover case.

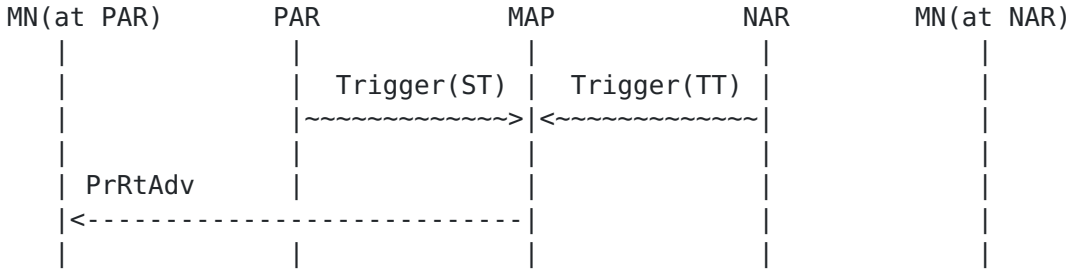

Figure 5: F-HMIPv6 for Network-Initiated Handover

When the PAR receives a source trigger or the NAR receives a target trigger from the network, it sends a handover indication signal to the MAP, possibly via an out-of-band signaling. Such the signal SHOULD include information about the link layer address and PLCoA of the concerned MN as well as the link layer address or identifier of the associated NAR.

When a network-initiated handover is indicated, the MAP sends the PrRtAdv message to the concerned MN. The PrRtAdv message SHOULD contain information about NLCoA for the MN to use in the NAR region.

The remaining procedures are identical to those for the mobile-initiated handover case, as shown in Figure 4.

6. Considerations for F-HMIPv6 Implementations

In this document, it is assumed that the MNs and ARs (including MAP) in the network are aware of the F-HMIPv6 described in this document as well as HMIPv6 [4]. For realizing the F-HMIPv6, the messages and functionality (e.g., triggers and tunnels) defined in FMIPv6 [5] will be used with slightly different procedures.

The F-HMIPv6 is basically designed to exploit all the messages defined in FMIPv6 and HMIPv6 with the following exceptions:

- A new flag is defined in the HMIPv6 MAP option, so as to indicate whether the MAP supports the F-HMIPv6 or not within the HMIPv6 domain.

- Some of the FMIPv6 messages have different IP source and destination addresses in the respective IP fields. In particular, the MAP address is used instead of the PAR address.

6.1 A New Flag in the HMIPv6 MAP Option

Figure 6 shows the MAP option used for HMIPv6. A new flag 'F' is added for F-HMIPv6.

When a MN moves into a new MAP domain, it receives the Router Advertisement with a MAP option from an access router. When the F bit is set in the MAP option, the MN MAY use F-HMIPv6. If the MN is not aware of F-HMIPv6, or the F bit is not set, it SHOULD NOT use F-HMIPv6.

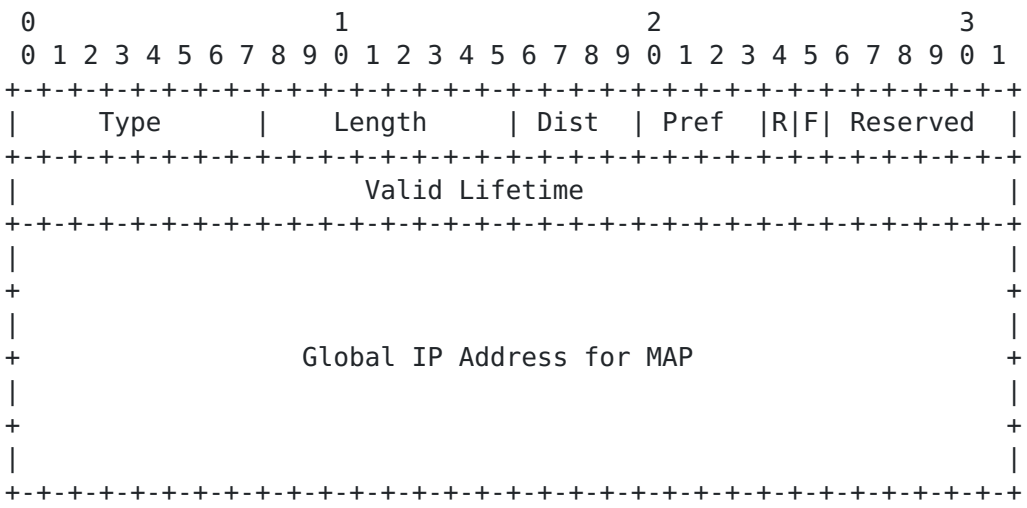

Figure 6: A new flag in the MAP option

Fields:

F When set indicates that the MAP support fast handover by F-HMIPv6.

6.2 Use of FMIPv6 messages in F-HMIPv6

F-HMIPv6 uses the messages for fast handover defined in FMIPv6, with different source and destination IP addresses. Table 1 summarizes the use of these messages.

Table 1. Use of FMIPv6 Messages in F-HMIPv6

F-HMIPv6 Messages	Source IP address	Destination IP address	Usage in FMIPv6
RtSolPr (Mobile-Ini.)	MN	MAP	Destination = PAR Source = MN
RtSolPr (Network-Ini.)	PAR	MAP	Destination = PAR Source = MN
PrRtAdv	MAP	MN	Source = PAR
FBU	MN	MAP	Destination = PAR
FBACK	MAP	MN (via PAR/NAR)	Source = PAR
HI	MAP	NAR	Source = PAR
HACK	NAR	MAP	Destination = PAR

6.3 AR-based RtSolPr/PrRtAdv

F-HMIPv6 assumes that a MAP has all the necessary information about its serving ARs such as IP address and link layer ID, as seen in the conventional mobile networks hierarchically configured.

In particular, if an access network supports the information sharing between ARs within its domain, the direct exchange of RtSolPr/PrRtAdv between an MN and an AR may be more effective. It is expected that the shorter signaling path can bring the lower latency.

6.4 AR Information Message (ARInfoMsg)

As previously described, F-HMIPv6 assumes that a MAP has all the necessary information about its serving ARs such as IP address and link layer ID. It can be achieved by a certain signaling procedure between MAP and ARs specified by network operator.

To facilitate this, a new ICMPv6 message could be defined, named 'AR Information Message (ARInfoMsg)' in this document. When each AR receives the MAP option with the flag 'F' set from the MN, it can send its link information to the MAP using the ARInfoMsg message.

If the MAP receives an ARInfoMsg message from an AR, the MAP MAY store this information until the lifetime reaches to 0. This information can also be used by AR to send PrRtAdv to the MN. If the MAP can't recognize this message, this message is silently discarded.

When the AR receives MAP option with 'F' flag set, it MAY send the ICMPv6 ARInfoMsg to the MAP in the following format.

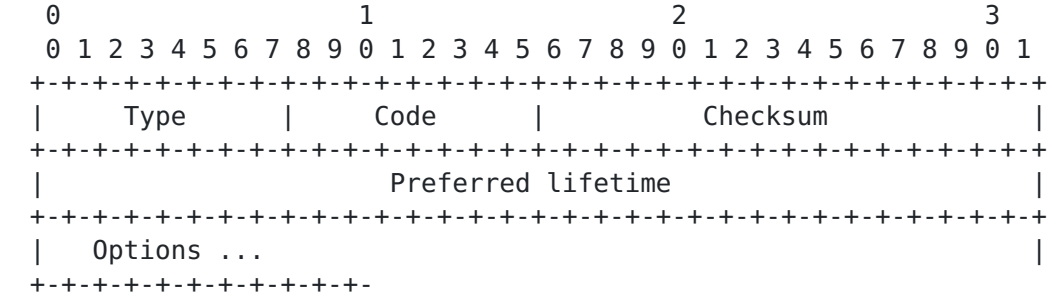

Figure 7: ICMPv6 ARInfoMsg Message

IP fields:

Source Address
The IP address of the AR, which is attached to the access network.

Destination Address
The IP address of the MAP.

Type
<TBD>

Code
<TBD>

Preferred lifetime

It is the same value of the preferred lifetime in the Router Advertisement message at the access network.

Options

AR can include the option defined in the 6.4.3 in [5]. The available options are the same as PrRtAdv:
- New Access Point Link-Layer Address
- New Router's Link-Layer Address
- New Router Prefix Information option

7. Variants of F-HMIPv6

7.1 F-HMIPv6 with Bicasting

In this section as a variant of F-HMIPv6, the F-HMIPv6 with bicasting is considered. When a handover is indicated in the F-HMIPv6 domain, the MAP will provide the MN with the bicasting [6] toward both PAR and NAR. This variant could be applied to both mobile-initiated and network-initiated handover cases.

The bicasting along with simultaneous binding [6] can be used to enhance the handover performance, in particular, for addressing the ping-pong effect. In F-HMIPv6, it is strongly recommended that the bicasting be used for stable handover.

Figure 8 illustrates the F-HMIPv6 operations with bicasting.

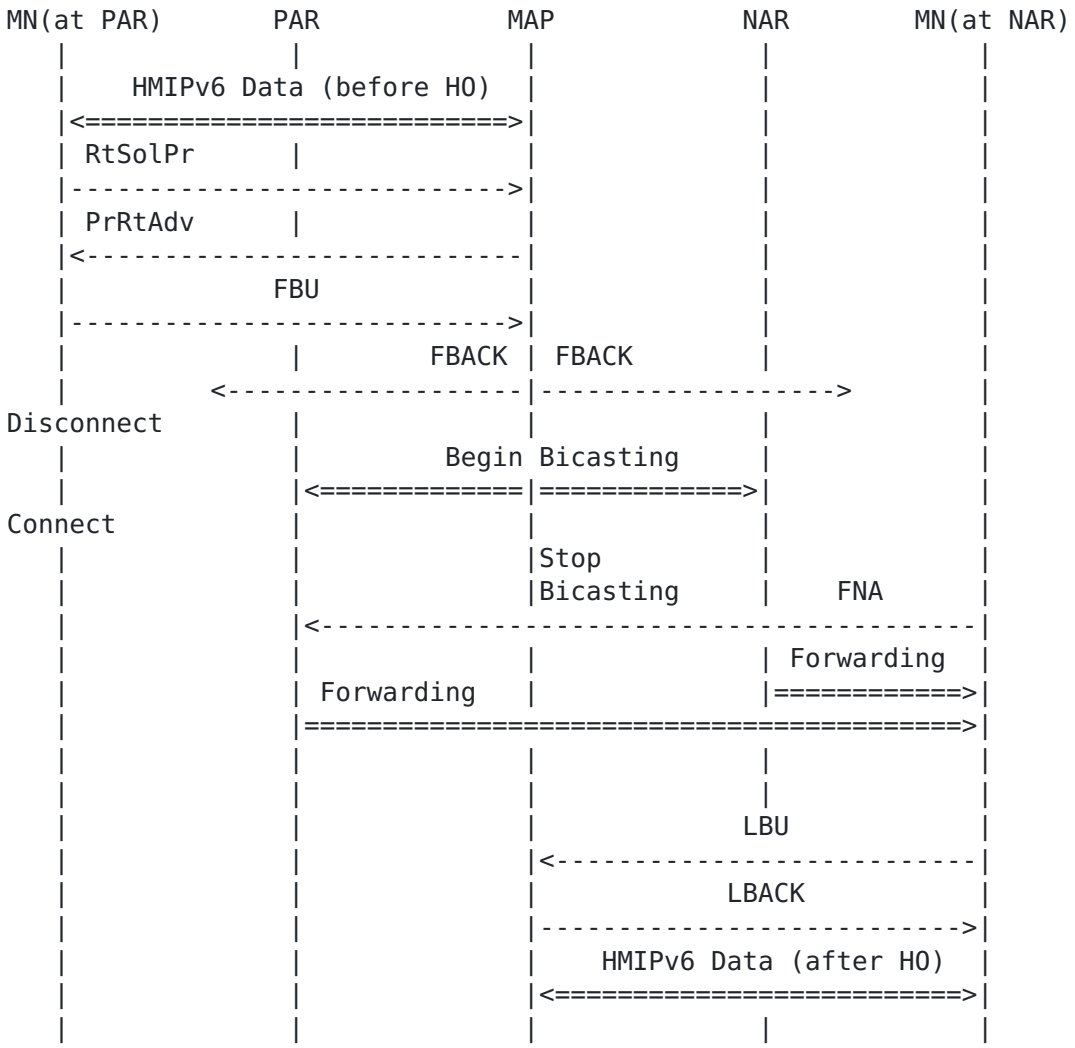

Figure 8: F-HMIPv6 with Bicasting

As shown in the figure, the basic control flows are identical to those for the generic F-HMIPv6 as described in Section 4, except that the bi-directional tunnel for handover is not used.

On the other hand, the following rules for bicasting support apply to the basic F-HMIPv6 operations.

1) The PrRtAdv message sent by MAP SHOULD contain a valid NLCoA with the help of an appropriate NLCoA configuration scheme such as optimistic DAD [7] or stateful NLCoA configuration [8].

2) The FBU message is used only for triggerring the bicasting by MAP. It is not concerned with the bi-directional tunnel establishment or HI/HACK messages. The FBACK message MAY be omitted.

3) The MAP begins the bicasting the data packets destined to MN (RcoA) via both PLCoA and NLCoA, as soon as it receives the FBU from the MN.

4) The MAP stops the bicasting when it receives the FNA message from MN via NAR.

5) The PAR and NAR forward the buffered packet to MN after receiving FNA message.

Note in this scheme that a bi-directional tunnel between MAP and NAR is not established, as done in the normal HMIPv6. Note also that the HI/HACK messages are not used. For this purpose, this scheme assumes an appropriate CoA configuration scheme such as 'optimistic DAD' [7] or 'address pool based stateful NLCoA configuration' [8], to ensure that the NLCoA confirmation (via the DAD process) is not needed in the NAR.

7.2 Reactive F-HMIPv6 without Anticipation

When the handover anticipation cannot be supported from the underlying link layer, the F-HMIPv6 will follow the normal HMIPv6 operation. The MN just sends the Local BU to MAP. In fact, the fast handover cannot be supported.

As an option to recover the data packet loss by handover, when the MAP receives a new Local BU from the MN, it MAY request the corresponding PAR to forward the data packets (destined to the PLCoA and buffered by PAR until then) to the NLCoA. For this purpose, the PAR MAY have queued the data packets that were destined to the PLCoA of MN.

7.3 Handover support between MAPs

There may be the requirement of handover support for the MN moving to another MAP region. For supporting it, F-HMIPv6 may establish forwarding tunnel from old MAP to new MAP. The forwarding packets are buffered in new MAP and delivered to MN via an AR after new local BU. In this case, the handover latency may higher than it in case of the handover within a MAP.

8. Security Considerations

The security issues of F-HMIPv6 are basically in line with those of FMIPv6 and HMIPv6.

Note that the MN and MAP could have an IPsec security association in HMIPv6, thus the RtSolPr and PrRtAdv messages can also be protected with IPsec. This feature actually provides an advantage over FMIPv6 where ND messages cannot be secured in its present form.

In addition, the MAP MUST ensure that the RtSolPr and FBU packets arrived from an MN that legitimately owns the RCoA. Otherwise, a bogus node could attempt to disrupt packets meant for the MN and redirect them to some access router.

Further security issues will be identified, as the F-HMIPv6 work is progressing.

9. References

9.1 Normative References

[1] S. Bradner, " Intellectual Property Rights in IETF Technology", BCP 79, RFC 3668, February 2004.

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

9.2 Informative References

[3] D. Johnson, et al., "Mobility Support in IPv6", RFC 3775, June 2004.

[4] H. Soliman, et al., "Hierarchical Mobile IPv6 mobility management (HMIPv6)", RFC 4140, August 2005.

[5] R. Koodli, et al., "Fast Handovers for Mobile IPv6", draftRFC 4068, July 2005.

[6] K. ElMalki and H. Soliman, "Simultaneous Bindings for Mobile IPv6 Fast Handoffs", draft-elmalki-mobileip-bicasting-v6-03, June 2003.

[7] N. Moore, "Optimistic Duplicate Address Detection for IPv6", draft-ietf-ipv6-optimistic-dad-05, February 2005.

[8] H. Jung, et al., "Address Pool based Stateful NCoA Configuration for FMIPv6", draft-jung-mipshop-stateful-fmipv6-00, August 2003.

Author's Addresses

Hee Young Jung
hyjung@etri.re.kr
Protocol Engineering Center, ETRI

Hesham Soliman
H.Soliman@flarion.com
Flarion

Seok J. Koh
sjkoh@knu.ac.kr
Kyungpook National University

Noriaki Takamiya
takamiya@po.ntts.co.jp
NTT Software

Full Copyright Statement

Intellectual Property

made any independent effort to identify any such rights. Information