MIPSHOP Working Group
Internet-Draft
Intended status: Informational
Expires: September 11, 2008

Hee-Jin Jang
Samsung AIT
Junghoon Jee
ETRI
Youn-Hee Han
KUT
Soohong Daniel Park
Samsung Electronics
Jaesun Cha
ETRI

March 10, 2008

Mobile IPv6 Fast Handovers over IEEE 802.16e Networks
draft-ietf-mipshop-fh80216e-07.txt

Abstract

This document describes how a Mobile IPv6 Fast Handover can be implemented on link layers conforming to the IEEE 802.16e suite of specifications. The proposed scheme tries to achieve seamless handover by exploiting the link-layer handover indicators and thereby synchronizing the IEEE 802.16e handover procedures with the Mobile IPv6 fast handover procedures efficiently.

Table of Contents

1. Introduction

Mobile IPv6 Fast Handover protocol (FMIPv6) [I-D.ietf-mipshop-fmipv6-rfc4068bis] was proposed to complement the Mobile IPv6 (MIPv6) [RFC3775] by reducing the handover latency for the real-time traffic. FMIPv6 assumes the support from the link-layer technology, however, the specific link-layer information available and its available timing differs according to the particular link-layer technology in use, as pointed out in [RFC4260] which provides an FMIPv6 solution for the IEEE 802.11 networks. So, this document is proposed to provide an informational guide to the developers about how to optimize the FMIPv6 handover procedures, specifically in the IEEE 802.16e networks [IEEE 802.16][IEEE 802.16e].

The proposed scheme achieves seamless handover by exploiting the link-layer handover indicators, and designing an efficient interleaving scheme of the 802.16e and the FMIPv6 handover procedures. The scheme is targeting a hard handover which is the default handover type of IEEE 802.16e. For the other handover types, i.e., the Macro Diversity Handover (MDHO) and Fast Base Station Switching (FBSS), the base stations in the same diversity set are likely to belong to the same subnet for diversity, and FMIPv6 might be no needed. This needs further discussion regarding the MDHO and the FBSS deployment.

We begin with a summary of handover procedures of [IEEE 802.16e], and then present the optimized complete FMIPv6 handover procedures by using the link-layer handover indicators. The examples of handover scenarios are described for both predictive mode and reactive mode lastly.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document is to be interpreted as described in [RFC2119].

Most of terms used in this document are defined in MIPv6 [RFC3775] and FMIPv6 [I-D.ietf-mipshop-fmipv6-rfc4068bis].

The following terms come from IEEE 802.16e specification [IEEE 802.16e].

MOB_NBR-ADV

An IEEE 802.16e neighbor advertisement message sent periodically by a base station.

MOB_MSHO-REQ

An IEEE 802.16e handover request message sent by a mobile node.

MOB_BSHO-RSP

An IEEE 802.16e handover response message sent by a base station.

MOB_BSHO-REQ

An IEEE 802.16e handover request message sent by a base station.

MOB_HO-IND

An IEEE 802.16e handover indication message sent by a mobile node.

BSID

An IEEE 802.16e base station identifier.

3. IEEE 802.16e Handover Overview

Compared with the handover in the WLAN (Wireless Local Area Network), the IEEE 802.16e handover mechanism consists of more steps since the 802.16e embraces the functionality for elaborate parameter adjustment and procedural flexibility.

When a mobile node (MN) stays in a link, it listens to the layer 2 neighbor advertisement messages, named a MOB_NBR-ADV, from its serving base station (BS). A BS broadcasts them periodically to identify the network and announces the characteristics of neighbor BSs. Once receiving this, the MN decodes this message to find out information about the parameters of neighbor BSs for its future handover. With the provided information in a MOB_NBR-ADV, the MN may minimize the handover latency by obtaining the channel number of neighbors and reducing the scanning time, or may select the better target BS based on the signal strength, QoS level, service price, etc.

The handover procedure is conceptually divided into two steps: "handover preparation" and "handover execution" [SH-802.16e]. The handover preparation can be initiated by either an MN or a BS. During this period, neighbors are compared by the metrics such as signal strength or QoS parameters and a target BS is selected among them. If necessary, the MN may try to associate (initial ranging) with candidate BSs to expedite a future handover. Once the MN decides handover, it notifies its intent by sending a MOB_MSHO-REQ message to the serving BS (s-BS). The BS then replies with a MOB_BSHO-RSP containing the recommended BSs to the MN after negotiating with candidates. Optionally it may confirm handover to the target BS (t-BS) over backbone when the target is decided. The BS alternatively may trigger handover with a MOB_BSHO-REQ message.

After handover preparation, handover execution starts. The MN sends a MOB_HO-IND message to the serving BS as a final indication for its handover. Once it makes a new attachment, it conducts 802.16e ranging through which it can acquire physical parameters from the target BS, tuning its parameters to the target BS. After ranging with the target BS successfully, the MN negotiates basic capabilities such as maximum transmit power and modulator/demodulator type. It then performs authentication and key exchange procedures, and finally registers with the target BS. If the target BS has already learned some contexts such as authentication or capability parameters through backbone, it may omit the corresponding procedures. For the details of the 802.16 handover procedures, refer to Section 6.3.22 of [IEEE 802.16e]. After completing registration, the target BS starts to serve the MN and communication via target BS is available. However, in case the MN moves to a different subnet, it should re-configure a

new IP address and re-establish an IP connection. To resume the active session of the previous link, the MN should perform IP layer handover additionally.

4. Network Topology Acquisition and Network Selection

This section describes how discovery of adjacent networks and selection of target network work in the IEEE 802.16e for background information.

An MN can learn the network topology and acquire the link information in several ways. First of all, it can do that via L2 neighbor advertisements. A BS supporting mobile functionality shall broadcast a MOB_NBR-ADV message periodically which includes the network topology information. (its maximum interval is 1 second.). This message includes BSIDs and channel information of neighbor BSs and is used to facilitate the MN's synchronization with neighbor BSs. An MN can collect the necessary information of the neighbor BSs through this message for its future handover.

Another method for acquisition of network topology is scanning, which is the process to seek and monitor available BSs in order to find suitable handover targets. While a MOB_NBR-ADV message includes static information about neighbor BSs, scanning provides rather dynamic parameters such as link quality parameters. Since the MOB_NBR-ADV message delivers a list of neighbor BSIDs periodically and scanning provides a way to sort out some adequate BSs, it is recommended that when new BSs are found in the advertisement, the MN identifies them via scanning and resolves their BSIDs to the information of the subnet where the BS is connected. The association, an optional initial ranging procedure occurring during scanning, is one of the helpful methods to facilitate the impending handover. The MN is able to get ranging parameters and service availability information for the purpose of proper selection of the target BS and expediting a potential future handover to it. The detailed explanation of association is described in Section 6.3.22 of [IEEE 802.16e].

Besides the methods provided by 802.16e, the MN may rely on other schemes. For instance, the topology information may be provided through the MIIS (Media Independent Information Service) [IEEE 802.21] which has been developed by IEEE 802.21 working group. The MIIS is a framework by which the MN or network can obtain network information to facilitate network selection and handovers.

After learning about neighbors, the MN may compare them to find a BS which can serve better than the serving BS. The target BS may be determined by considering various criteria such as required QoS, cost, user preference, and policy. How to select the target BS is not in the scope of this document.

5. Interaction between FMIPv6 and IEEE 802.16e

In this section, a set of primitives is introduced for an efficient interleaving of the IEEE 802.16e and the FMIPv6 procedures as below. The following sections present the handover procedures in detail by using them.

- o NEW_LINK_DETECTED (NLD)

  A trigger from the link layer to the IP layer in the MN to report that a new link is detected.

- o LINK_HANDOVER_IMPEND (LHI)

  A trigger from the link layer to the IP layer in the MN to report that a link layer handover decision has been made and its execution is imminent.

- o LINK_SWITCH (LSW)

  A control command from the IP layer to the link layer in the MN in order to force the MN to switch from an old BS to a new BS.

- o LINK_UP (LUP)

  A trigger from the link layer to the IP layer in the MN to report that the MN completes the link layer connection establishment with a new BS.

5.1. Access Router Discovery

Once a new BS is detected through reception of a MOB_NBR-ADV and scanning, an MN may try to learn the associated access router (AR) information as soon as possible. In order to enable its quick discovery in the IP layer, the link layer (802.16) triggers a NEW_LINK_DETECTED primitive to the IP layer (FMIPv6) on detecting a new BS.

Receiving the NEW_LINK_DETECTED from the link layer, the IP layer tries to learn the associated AR information by exchanging an RtSolPr (Router Solicitation for Proxy Advertisement) and a PrRtAdv (Proxy Router Advertisement) with the PAR (Previous Access Router). According to [I-D.ietf-mipshop-fmipv6-rfc4068bis], the MN may send an RtSolPr at any convenient time. However this proposal recommends that, if feasible, the MN send it as soon as possible after receiving the NEW_LINK_DETECTED for quick router discovery because detection of a new BS usually implies MN's movement, which may result in handover.

Transmission of RtSolPr messages may cause signaling overhead problem which is mentioned in Section 2 of [RFC4907]. To rate-limit the retransmitted RtSolPr messages, FMIPv6 provides a back-off mechanism. It is also possible that attackers may forge a MOB_NBR-ADV message so that it can contain a bunch of bogus BSIDs, or may send a flood of MOB_NBR-ADV messages each of which contains different BSIDs. This problem is mentioned in Section 8.

5.2. Handover Preparation

When the MN decides to change links based on its policy such as the degrading signal strength or increasing packet loss rate, it initiates handover by sending a MOB_MSHO-REQ to the BS and will receive a MOB_BSHO-RSP from the BS as a response. Alternatively the BS may initiate handover by sending a MOB_BSHO-REQ to the MN.

On receiving either a MOB_BSHO-RSP or a MOB_BSHO-REQ, the link layer triggers a LINK_HANDOVER_IMPEND in order to signal the IP layer of arrival of MOB_BSHO-REQ/MOB_BSHO-RSP quickly. At this time, the target BS decided in the link layer is delivered to the IP layer as a parameter of the primitive. The primitive is used to report that a link layer handover decision has been made and its execution is imminent. It can be helpfully used for FMIPv6 as an indication to start handover preparation procedure, that is to send an FBU (Fast Binding Update) message to the PAR.

To avoid erroneous results due to unreliable and inconsistent characteristics of link, for instance, to move to the unpredicted network or to keep staying in the current network after sending an FBU, Section 2 of [RFC4907] advises to use combination of signal strength data with other techniques rather than relying only on signal strength for handover decision. For example, the LINK_HANDOVER_IMPEND may be sent after validating filtered signal strength measurements with other indications of link loss such as lack of beacon reception.

Once the IP layer receives the LINK_HANDOVER_IMPEND, it checks whether the specified target network belongs to a different subnet or not based on the information collected during Access Router Discovery step. If the target proves to be in the same subnet, the MN can continue to use the current IP address after handover and there is no need to perform FMIPv6. Otherwise, the IP layer formulates a prospective NCoA (New Care-of-Address) with the information provided in the PrRtAdv message and sends an FBU message to the PAR.

When the FBU message arrives in the PAR successfully, the PAR and the NAR (New Access Router) process it according to [I-D.ietf-mipshop-fmipv6-rfc4068bis]. The PAR sets up a tunnel

between the PCoA (Previous Care-of-Address) and NCoA by exchanging HI (Handover Initiate) and HAck (Handover Acknowledge) messages with the NAR, forwarding the packets destined for the MN to NCoA. The NCoA is confirmed or re-assigned by the NAR in the HAck and, finally delivered to the MN through the FBack (Fast Binding Acknowledgment) in case of predictive mode.

After the MN sends a MOB_HO-IND to the serving BS, data packet transfer between the MN and the BS is not allowed any more. Note that when a MOB_HO-IND is sent out before an FBack arrives in the MN, it is highly probable that the MN will operate in reactive mode because the serving BS releases the MN's all connections and resources after receiving a MOB_HO-IND. Therefore, if possible, the MN should exchange FBU and FBack messages with the PAR before sending a MOB_HO-IND to the BS so as to operate in predictive mode.

5.3. Handover Execution

If the MN receives an FBack message on the previous link, it runs in predictive mode after handover. Otherwise, it should run in reactive mode. In order for the MN to operate in predictive mode as far as possible after handover, implementations may allow use of a LINK_SWITCH primitive. The LINK_SWITCH is a command in order to force the MN to switch from an old BS to a new BS and the similar concept has introduced for the wireless LAN in [I-D.irtf-mobopts-l2-abstractions]. When it is applied, the MN's IP layer issues a LINK_SWITCH primitive to the link layer on receiving the FBack message in the previous link. Until it occurs, the link-layer keeps the current (previous) link if feasible and postpones sending a MOB_HO-IND message while waiting for the FBack message.

After switching links, the MN synchronizes with the target BS and performs the 802.16e network entry procedure. The MN exchanges the RNG-REQ/RSP, SBC-REQ/RSP, PKM-REQ/RSP and REG-REQ/RSP messages with the target BS. Some of these messages may be omitted if the (previously) serving BS transferred the context to the target BS over the backbone beforehand. When the network entry procedure is completed and the link layer is ready for data transmission, it informs the IP layer of the fact with a LINK_UP primitive.

Note that the LINK_UP should not be sent due to changes in transient link conditions and less sensitive to link conditions according to Section 2 of [RFC4907]. However, the link may experience a intermittent loss. Even in such a case, the following FMIPv6 operation is performed only when the MN handovers to the link with a different subnet and there is no signaling overhead as a result of a intermittent loss.

5.4. Handover Completion

When the MN's IP layer receives a LINK_UP primitive from the link layer, it should check whether it has moved into the target network predicted by FMIPv6. In case the target BS is within the same subnet, the MN does not perform the FMIPv6 operation.

- If the MN discovers itself in the predicted target network and receives an FBack message in the previous link, the MN's IP layer sends a UNA (Unsolicited Neighbor Advertisement) to the NAR (predictive mode).

- If the MN has moved to the target network without receiving an FBack message in the previous link, the IP layer sends an UNA and also an FBU message immediately after sending the UNA message (reactive mode). The NAR may provide a different IP address by using an RA (Router Advertisement) with a NAACK (Neighbor Advertisement Acknowledge) option other than the formulated NCoA by the MN.

- The MN may discover itself in the unpredicted network (erroneous movement). This is the case the MN moves to the network that is not the target specified in the LINK_HANDOVER_IMPEND primitive. For the recovery from such invalid indication which is mentioned in Section 2 of [RFC4907], the MN should send a new FBU to the PAR according to Section 5.6 of [I-D.ietf-mipshop-fmipv6-rfc4068bis] so that the PAR can update the existing binding entry and redirect the packets to the new confirmed location.

In both cases of predictive and reactive modes, once the MN has moved into the new link, it uses the NCoA formulated by the MN as a source address of the UNA, irrespective of NCoA availability. It then starts a DAD probe for NCoA according to [RFC4862]. In case the NAR provides the MN with a new NCoA, the MN MUST use the provided NCoA instead of the NCoA formulated by the MN.

When the NAR receives a UNA message, it deletes its proxy neighbor cache entry if it exists, and forwards buffered packets to the MN after updating the neighbor cache properly. Detailed UNA processing rules are specified in Section 6.4 of [I-D.ietf-mipshop-fmipv6-rfc4068bis].

6. The Examples of Handover Scenario

In this section, the recommended handover procedures over 802.16e network are shown for both predictive and reactive modes. It is assumed that the MN handovers to the network which belongs to a different subnet.

In the follwing figures, the messages between the MN's layer 2 (MN L2) and the BS are the IEEE 802.16 messages while messages between the MN's layer 3 (MN L3) and the PAR, and messages between PAR and NAR are the FMIPv6 messages. The messages between the the MN L2 and the MN L3 are primitives introduced in this document.

6.1. Predictive Mode

The handover procedures in the predictive mode are briefly described as follows. Figure 3 is illustrating these procedures.

1. A BS broadcasts a MOB_NBR-ADV periodically.

2. If the MN discovers a new neighbor BS in this message, it may perform scanning for the BS.

3. When a new BS is found through the MOB_NBR-ADV and scanning, the MN's link layer notifies it to the IP layer by a NEW_LINK_DETECTED primitive.

4. The MN tries to resolve the new BS's BSID to the associated AR by exchange of RtSolPr and PrRtAdv messages with the PAR.

5. The MN initiates handover by sending a MOB_MSHO-REQ message to the BS and receives a MOB_BSHO-RSP from the BS. Alternatively, the BS may initiate handover by sending a MOB_BSHO-REQ to the MN.

6. When the MN receives either a MOB_BSHO-RSP or a MOB_BSHO-REQ from the BS, its link layer triggers a LINK_HANDOVER_IMPEND primitive to the IP layer.

7. On reception of the LINK_HANDOVER_IMPEND, the MN's IP layer identifies that the target delivered along with the LINK_HANDOVER_IMPEND belongs to a different subnet and sends an FBU message to the PAR. On receiving this message, the PAR establishes tunnel between the PCoA and the NCoA by exchange of HI and HAck messages with the NAR, and forwards packets destined for the MN to the NCoA. During this time, the NAR may confirm NCoA availability in the new link via HAck.

8. The MN receives the FBack message before its handover and sends a MOB_HO-IND message as a final indication of handover. Issue of a MOB_HO-IND optionally may be promoted by using a LINK_SWITCH command from the IP layer. Afterwards it operates in predictive mode in the new link.

9. The MN conducts handover to the target BS and performs the IEEE 802.16e network entry procedure.

10. As soon as the network entry procedure is completed, the MN's link layer signals the IP layer with a LINK_UP. On receiving this, the IP layer identifies that it has moved to a predicted target network and received the FBack message in the previous link. It issues a UNA to the NAR by using NCoA as a source IP address. At the same time, it starts to perform DAD for the NCoA.

11. When the NAR receives the UNA from the MN, it delivers the buffered packets to the MN.

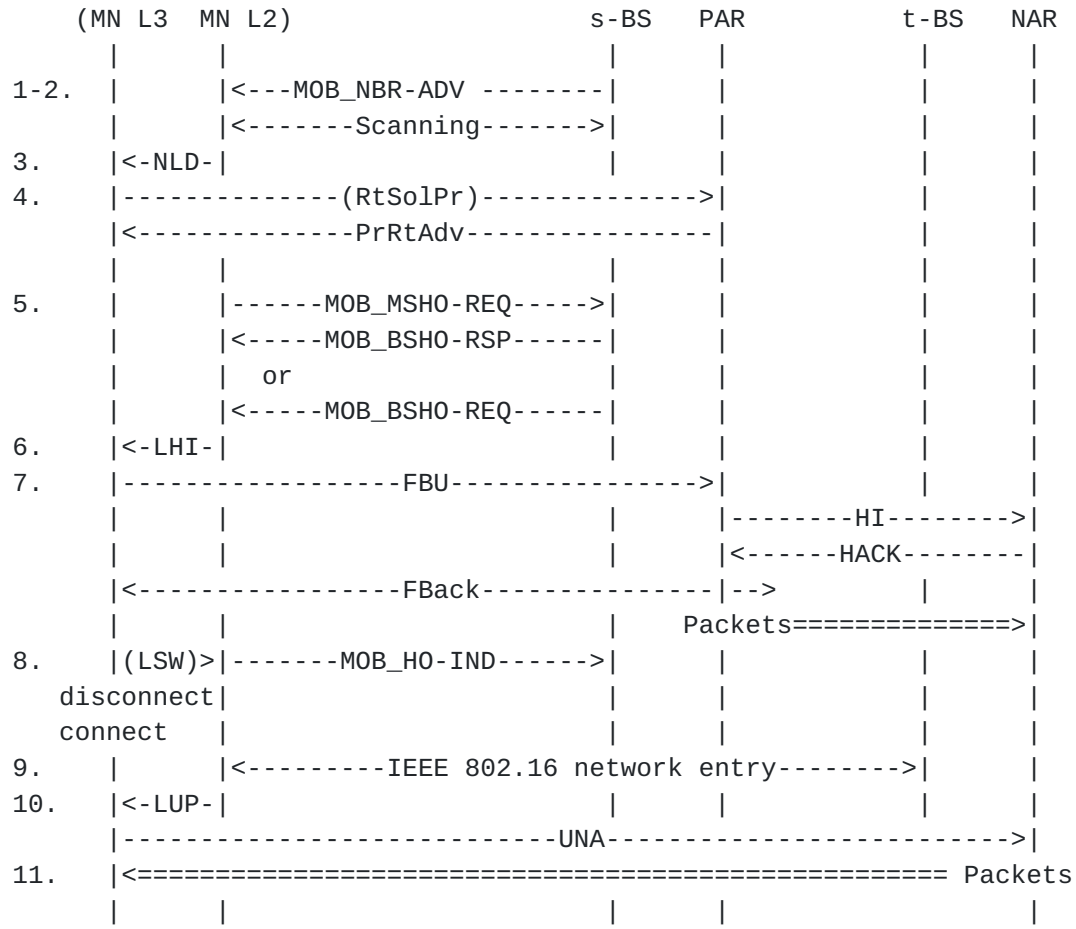

Figure 3. Predictive Fast Handover in 802.16e

6.2. Reactive Mode

The handover procedures in the reactive mode are described as follows. Figure 4 is illustrating these procudures.

1.~ 7. The same as procedures of predictive mode.

8. The MN does not receive the FBack message before handover and sends a MOB_HO-IND message as a final indication of handover. Afterwards, it operates in reactive mode in the new link.

9. The MN conducts handover to the target network and performs the 802.16e network entry procedure.

10. As soon as the network entry procedure is completed, the MN's link layer signals the IP layer with a LINK_UP. On receiving this, the IP layer identifies that it has moved to the predicted target network without receiving the FBack in the previous link. The MN issues a UNA to the NAR by using NCoA as a source IP address and starts to perform DAD for the NCoA. Additionally, it also sends an FBU to the PAR in the reactive mode.

11. When the NAR receives the UNA and the FBU from the MN, it forwards the FBack to the PAR. The FBack and Packets are forwarded from the PAR and delivered to the MN (NCoA) through the NAR. The NAR may supply a different IP address than the NCoA by sending an RA with a NAACK option to the MN.

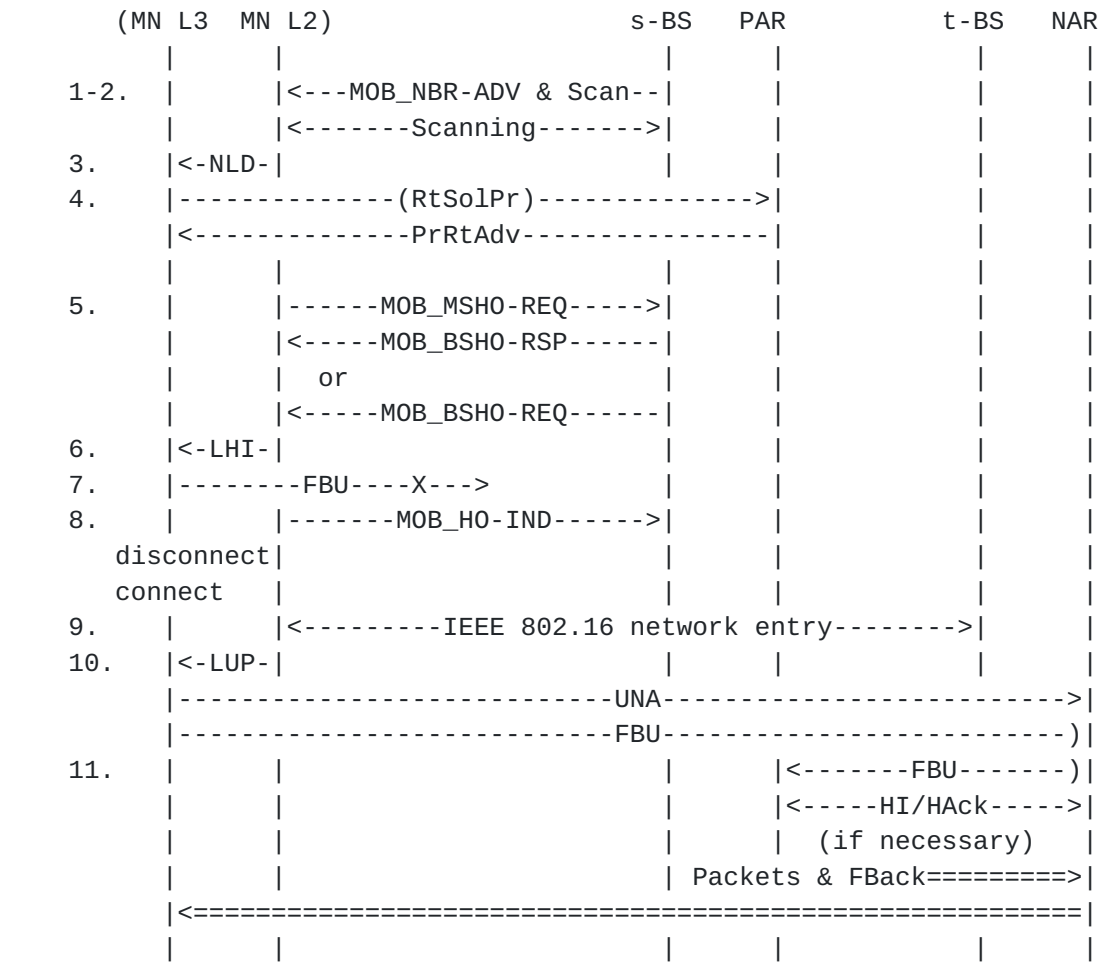

Figure 4. Reactive Fast Handover in 802.16e

7. IEEE 802.21 Considerations

It is worth noting that great researches have been conducted on defining generic services in the IEEE 802.21 working group that facilitate handovers between heterogeneous access links. The standard works are named as a Media Independent Handover (MIH) Service [IEEE 802.21], and propose three kinds of services, that is Media Independent Event Service (MIES), Media Independent Command Service (MICS), and Media Independent Information Service (MIIS).

An MIES defines the events triggered from lower layers (physical and link) to higher layers (network and above) in order to report changes of physical and link layer conditions. On the other hand, an MICS supports the commands sent from higher layers to lower layers, and provides users with a way of managing the link behavior relevant to handovers and mobility. An MIIS provides a framework by which the MN or network can obtain network information to facilitate network selection and handovers.

Although the purpose of IEEE 802.21 has been developed to enhance user experience of MNs roaming between heterogeneous networks, the results may be utilized to optimize the handover performance in a homogeneous network. When the MIH primitives are available for handover in the 802.16e network, the MN can use them instead of the primitives proposed in this document. The Table 1 shows examples of the mapping between the proposed primitives and the MIH primitives.

Proposed primitives	MIH primitives
NEW_LINK_DETECTED	LINK_DETECTED
LINK_HANDOVER_IMPEND	LINK_HANDOVER_IMMINENT
LINK_SWITCH	HANDOVER_COMMIT
LINK_UP	LINK_UP

Table 1. The proposed primitives and MIH primitives

8. Security Considerations

The primitives defined in this document are used only for local indication inside of the MN, so no security mechanism is required to protect those primitives. However, FMIPv6 messages and IEEE 802.16e messages which may trigger the primitives need to be protected.

Security considerations of the FMIPv6 specification [I-D.ietf-mipshop-fmipv6-rfc4068bis] are applicable to this document. It is also worthwhile to note that the IEE802.16e has a security sub-layer which provides subscribers with privacy and authentication over the broadband wireless network. This layer has two main component protocols: a privacy key management protocol (PKM) for key management and authentication, and an encapsulation protocol for encrypting data. From the perspective of the 802.16e, FMIPv6 messages are considered as data and delivered securely by using those protocols.

However, some of IEEE 802.16e management messages are sent without authentication. There is no protection to secure 802.16e broadcast messages. It may be possible for the attacker to maliciously forge a MOB_NBR-ADV message so that it contains the bogus BSIDs, or send a flood of MOB_NBR-ADV messages having different bogus BSIDs toward the MN. As a result of this, the MN may send the useless consecutive RtSolPr messages to the PAR and result in wasting the air resources. Therefore, the MN SHOULD perform scanning lest it should issue a NEW_LINK_DETECTED primitive when receiving the forged MOB_NBR-ADV messages from attackers. It is also possible that attackers try a DoS (Denial-of-Service) attack by sending a flood of a MOB_BSHO-REQ messages and triggering LINK_HANDOVER_IMPEND primitives in the MN. But the IEEE 802.16e provides a message authentication scheme for management messages involved in handover as well as network entry procedures by using a message authentication code (MAC) such as HMAC/CMAC (hashed/cipher MAC). Therefore those management messages are protected from the malicious use by attackers for triggering LINK_HANDOVER_IMPEND or LINK_UP primitives.

9. IANA Consideration

This document does not require any new number assignment from IANA.

10. Acknowledgment

Many thanks IETF Mobility Working Group members of KWISF (Korea Wireless Internet Standardization Forum) for their efforts on this work. In addition, we would like to thank Alper E. Yegin, Jinhyeock Choi, Rajeev Koodli, Soininen Jonne, Gabriel Montenegro, Singh Ajoy, Yoshihiro Ohba, Behcet Sarikaya, Vijay Devarapalli and Ved Kafle who have provided the technical advice.

11. References

11.1. Normative References

[I-D.ietf-mipshop-fmipv6-rfc4068bis]
Koodli, R., "Mobile IPv6 Fast Handovers", draft-ietf-mipshop-fmipv6-rfc4068bis-06 (work in progress), February 2008.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[IEEE 802.16] IEEE Standard for Local and Metropolitan Area Networks, "Part 16 - Air Interface for Fixed Broadband Wireless Access Systems", IEEE Std 802.16-2004, June 2004.

[IEEE 802.16e] IEEE Standard for Local and Metropolitan Area Networks, "Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1", IEEE Std 802.16e-2005 and IEEE Std 802.16 -2004/Cor 1-2005, February 2006.

11.2. Informative References

[I-D.irtf-mobopts-l2-abstractions]
Teraoka, F., "Unified L2 Abstractions for L3-Driven Fast Handover", draft-irtf-mobopts-l2-abstractions-07 (work in progress), February 2008.

[RFC4260] McCann, P., "Mobile IPv6 Fast Handovers for 802.11 Networks", RFC 4260, November 2005.

[RFC4907] Aboba, B., "Architectural Implications of Link Indications", RFC 4907, June 2007.

[IEEE 802.21] IEEE 802.21 Working Group Document,"Draft IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services", IEEE P802.21 D9.0, February 2008.

[SH-802.16e] Kim, K., Kim, C., and T. Kim, "A Seamless Handover Mechanism for IEEE 802.16e Broadband Wireless Access", International Conference on Computational Science, vol. 2, pp. 527-534, 2005.

Authors' Addresses

Hee-Jin Jang
Samsung Advanced Institute of Technology
P.O. Box 111
Suwon 440-600
Korea

Email: heejin.jang@samsung.com

Junghoon Jee
Electronics and Telecommunications Research Institute
161 Gajeong-dong, Yuseong-gu
Daejon 305-350
Korea

Email: jhjee@etri.re.kr

Youn-Hee Han
Korea University of Technology and Education

Email: yhhan@kut.ac.kr

Soohong Daniel Park
Samsung Electronics
416 Maetan-3dong, Yeongtong-gu
Suwon 442-742
Korea

Email: soohong.park@samsung.com

Jaesun Cha
Electronics and Telecommunications Research Institute
161 Gajeong-dong, Yuseong-gu
Daejon 305-350
Korea

Email: jscha@etri.re.kr

Full Copyright Statement

Intellectual Property