Using Return Routability for Authentication of Fast Handovers in Mobile IPv6*

Youngsong Mun, Kyunghye Lee, Seonggeun Ryu, and Teail Shin

School of Computing, Soongsil University
Sangdo-5dong, Dongjak-gu, Seoul, Korea
mun@computing.ssu.ac.kr,
{lkhmymi,sgryu,nullx}@sunny.ssu.ac.kr

Abstract. IETF published Fast Handovers in Mobile IPv6 (FMIPv6) for efficient mobility management. FMIPv6 has no solutions to protect binding update messages. Previous researches have mainly concentrated on using AAA, public cer-tificates or cryptographic algorithms. However the approaches need a particular infrastructure or heavy processing cost to authenticate binding updates in FMIPv6. Proposed scheme provides authentication for FMIPv6 without infrastructure and costly cryptographic algorithms by the extended Return Routability. Also proposed scheme is able to be used for various existing handover protocol in MIPv6 network.

1 Introduction

The widespread growth of wireless networks has ushered in the era of mobile computing, where handheld computing devices are the predominant choice for users. There is a strong consensus that IP will be the foundation of the next-generation network. Although the IP will be the common denominator, there are many problems. In wireless networks, users change their attachment points frequently while they are connected. In this environment, mobility management is an essential technology for keeping track of the user's current location and delivering data correctly.

The Internet Engineering Task Force (IETF) standardized Mobile IPv6 [1] for the mobility management. Mobile IPv6 (MIPv6) is an IP-layer mobility protocol for a Mobile Node (MN) to maintain connectivity to the Internet during its handover from one Access Router (AR) to another. The basic idea in MIPv6 is to allow a Home Agent (HA) to work as a stationary proxy for an MN. Whenever an MN is away from its home network, the HA intercepts packets destined to MN's home of address (HoA) and forwards the packets by tunneling them to MN's care-of address (CoA). The transport layer uses the HoA as a stationary identifier for the MN. Because a handover procedure in MIPv6 involves movement detection, IP address configuration, and location update, the handover latencies affect real-time applications. Hence,

* This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement) (IITA-2006-C1090-0603-0027).

O. Gervasi and M. Gavrilova (Eds.): ICCSA 2007, LNCS 4706, Part II, pp. 1052–1061, 2007.

MIPSHOP Working Group in IETF published Fast Handovers in Mobile IPv6 (FMIPv6) [2] to reduce the handover latencies. However, current FMIPv6 does not consider authenticating Binding Updates (BUs) between an MN and a previous access router (PAR). By the BU message, PAR learns a binding between Previous CoA (PCoA) and New CoA (NCoA). This binding is used to modify the handling of outgoing and incoming packets. The binding may lead to security risks. An attacker may use a malicious BU to hijack or redirect existing connections.

Other researches for FMIPv6 involve a trusted online server (e.g. AAA) or public key infrastructure (PKI). Authentication needs to work between any MN and any AR. There does not currently exist any infrastructure that could be used for such global authentication. Also the approaches which use asymmetric cryptosystem need heavy processing cost. Therefore, we use the extended Return Routability to provide authentication for FMIPv6 without infrastructure and heavy processing cost.

2 Related Works

2.1 FMIPv6

FMIPv6 reduces handover latency. In MIPv6, if an MN moves in new subnet, the MN should perform movement detection and address configuration and location update. It is called handover latency. In contrast to MIPv6, FMIPv6 finishes movement detection and address configuration for an NCoA in advance of handover. Also, FMIPv6 uses a tunnel to retain connectivity before location update. Therefore FMIP recovers communication fast without latency resulted from movement detection, address configuration and location update. Fig. 1 shows FMIPv6 procedure. FMIPv6 is Make-Before-Break protocol. If radio signal strength from an Access Point (AP) is week, link layer triggers a Link-Going-Down event. Receiving the event, the MN sends a RtSolPr including a scanned AP-ID. The PAR finds an appropriate NAR by the AP-ID and sends a PrRtAdv including the prefix and the address of the NAR. After

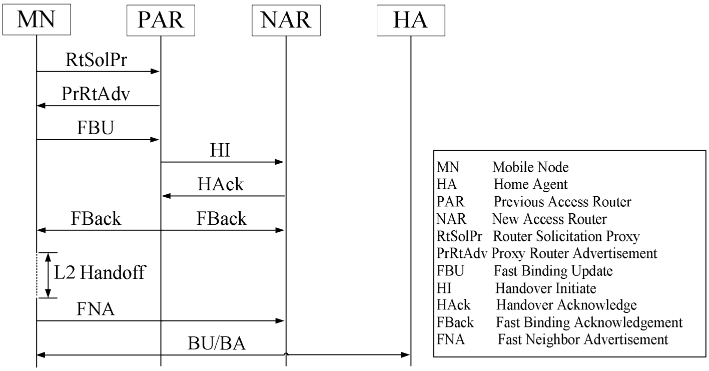

MN
PAR
NAR
HA
RtSolPr
PrRtAdv
FBU
HI
HAck
FBack
FBack
L2 Handoff
FNA
BU/BA
MN Mobile Node
HA Home Agent
PAR Previous Access Router
NAR New Access Router
RtSolPr Router Solicitation Proxy
PrRtAdv Proxy Router Advertisement
FBU Fast Binding Update
HI Handover Initiate
HAck Handover Acknowledge
FBack Fast Binding Acknowledgement
FNA Fast Neighbor Advertisement

Fig. 1. FMIPv6 procedure

receiving the PrRtAdv, the MN performs address auto-configuration to generate an NCoA by the prefix of NAR. Then the MN sends a FBU to start a substantial handover. The PAR and the NAR verify the NCoA by exchanging a HI and a Hack and establish a tunnel between the PCoA and the NCoA. When the MN finishes link switching, the MN sends a FNA for announcing its attachment to the NAR. The NAR delivers packets buffered during disruption. Hence, the MN is able recover connectivity before the MN finishes location update to the HA.

However, there are vulnerabilities in FMIPv6 because the current version of FMIPv6 does not specify authentication for the FBU. If an attacker uses a malicious FBU, packets meant for one address could be stolen or redirected to some unsuspecting node. Therefore, The PAR must verify that the FBU arrive from a node that legitimately owns the CoA.

2.2 Return Routability

MIPv6 requires tunneling through a HA to communicate with a CN, it leads to longer paths and degraded performance. This tunneling is called triangular routing. To alleviate the performance penalty, MIPv6 includes Route Optimization (RO). For RO an MN sends a BU to a CN for registering the binding between a HoA and a CoA in binding cache of the CN. After RO, the CN can forward packets to the CoA directly. Return Routability (RR) is the protocol to authenticate a BU of RO. RR is based on the idea that a node should be able to verify the existence of a node which is able to respond to packets sent to a given address. Successful RR implies that there is indeed a node at the given address.

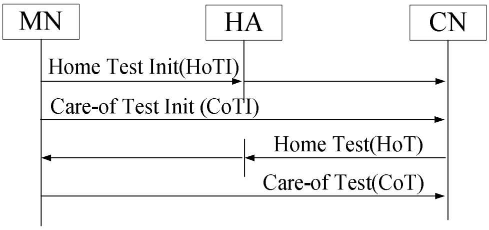


Fig. 2. Return Routability

RR consists of a HoA test and a CoA test. The protocol flow is depicted in Fig. 3. The MN sends a HoTI and a CoTI simultaneously to start a HoA test and a CoA test. The CN replies to both of the messages independently by sending a HoT and a CoT. The HoT has a nonce index and a home keygen token. A Home keygen token is generated by a Kcn, known only by the CN. A CoT has a nonce index and a care-of keygen token. A Care-of keygen token is generated by a Kcn. A Home keygen token and a care-of keygen token are calculated by the following formula.

$$home\ keygen\ token \quad = hash\left(Kcn \mid HoA \mid nonce \mid 0\right)$$

$$care\text{-}of\ \ keygen\ token = hash\left(Kcn \mid CoA \mid nonce \mid 1\right)$$

The home keygen token received by the MN is used for proving that the MN is indeed at the HoA. And care-of keygen token received by the MN is used for proving that the MN is indeed at the CoA. Each nonce index allows the CN to easily find the nonce which was used during generating keygen token. The MN which has a home keygen token and a care-of keygen token can create a binding management key (Kbm) to verify that the MN stays at the HoA and CoA concurrently.

$$Kbm = SHA1(\mathit{home\ keygen\,token} \mid \mathit{care\text{-}of\ keygen\ token})$$

The tunnel between the MN and the HA is protected by IPsec (ESP), which makes it impossible for the outsiders to learn the contents of a HoT. Therefore RR is secure from a malicious attack.

3 Proposed Scheme

RR is the protocol designed to authenticate BUs in RO. If RR is used for FMIPv6 straightforwardly, there is a problem. An attacker who stays in the same subnet of a target host can initiate RR with his HoA_a and target's CoA. The attacker normally receives a home keygen token and sniffs a care-of keygen token of the target. Hence the attacker can generate a valid Kbm. The FBU with only the Kbm can not be used to authorize to change the destination of packet from PCoA to NCoA.

RR can not guarantee address ownership of a CoA perfectly. A Kbm of RR only allows a CN to change the path of traffic destined to a MN from a HoA to a CoA. However, FMIPv6 needs to change the path of traffic from PCoA to NCoA. Therefore we propose a mechanism that RR can guarantee address ownership of a CoA. To do this, we define the new type of RR and modify the binding cache of the CN.

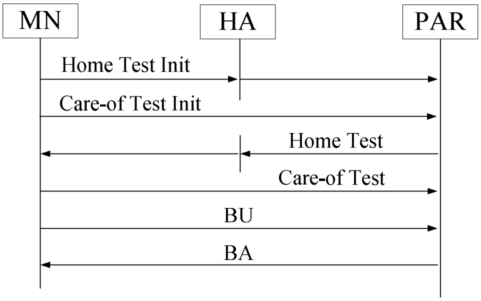


Fig. 3. The Extended Return Routability

In proposed scheme, once an MN newly moves in a subnet, the MN should start the Extended Return Routability (ERR) immediately. Fig. 3 shows ERR. It looks like the procedure of RR. However, when the MN finishes ERR, the MN sends a BU which has an E-flag. If the PAR receives the BU, the PAR does not start route optimization.

The BU has a Message Authentication Code (MAC) singed by Kbm. If the MAC is valid and the requested CoA in the BU does not exist in the binding cache, the PAR registers the unique binding of CoA and HoA in binding cache. This binding is denoted by CoA-HoA. Then, the PAR sends a binding acknowledgement (BA) to indicate successful registration. This CoA-HoA binding assure that the MN retain the ownership of the CoA. Because the PAR does not permit to register the CoA- HoA_a binding if the CoA-HoA binding already exists in the binding cache. Only the MN which has the address ownership of the HoA can updates and deletes the existing CoA-HoA binding. Therefore, with the Kbm and the CoA-HoA binding, the PAR authenticates the FBU in FMIPv6. Fig. 4 is the example in which FMIPv6 uses ERR to Authenticate the FBU. The FBU has the MAC signed by Kbm. When the PAR receives the FBU, the PAR verifies the MAC and the CoA-HoA binding in its binding cache. If the verification is correctly finished, the PAR keeps performing remaining processes.

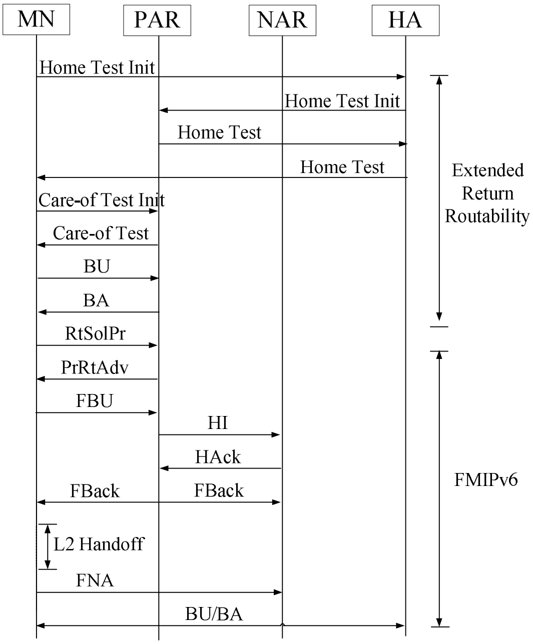


Fig. 4. FMIPv6 applied to the Extended Return Routability

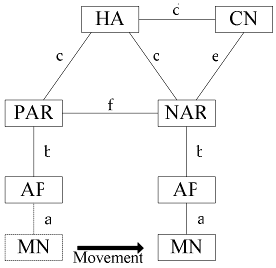
ERR always should be performed prior to FMIPv6. Usually, there must be a long interval until the MN which finishes ERR performs a handover. However, if the MN moves from one subnet to another frequently, ERR may leads to degrade performance of FMIPv6. In the next section, we will analyze performance of proposed scheme. First scenario is normal ERR in which the MN has to procure home keygen token and care-of keygen token. Second scenario is optimized ERR in which the MN that already obtains home keygen token of a next attachment point needs only a care-of keygen token.

As shown in Fig. 4, ERR is made up the period of procuring home keygen token , the period of procuring care-of keygen token and the period of sending a BU to register the CoA-HoA. The HoTI and the CoTI start simultaneously and independently. Hence the processing time of the last finished test is considered total latency . Generally the time to get a home keygen token is longer than the time to get a care-of keygen token. If the home keygen token of a next attachment point is obtained in advance, the latency resulted from ERR significantly reduced. This mode of ERR is called the optimized ERR.

4 Performance Evaluation

4.1 Analysis Model

Fig. 5 shows the analysis model for evaluating performance of ERR. In the analysis model, an MN moves from one subnet to another subnet. In this section, we analyze performance of the normal ERR and the optimized ERR. We assume that a CN generates data packet destined to an MN at λ and the MN moves from one subnet to another at μ. We define packet to mobility ratio (PMR) as the mean number of packets received by the MN from the CN per a movement. The PMR is given by λ / μ. We assume that the cost for transmitting a packet is dependent on the hops between the sender and the receiver. The average length of a data packet is l times greater than the average length of a control packet. The average processing cost for a packet at any node is assumed r .



Parameters	value
a (Wireless link)	1
b,f (Wired link)	1
c,d,e (multi hops)	5

Fig. 5. Analysis Model

4.2 Handover Latency

The handover latency consists of link switching latency, IP connectivity latency and location update latency. Link switching latency is due to layer 2 handoff. IP connectivity latency is the time for an MN to finish movement detection and IP address configuration. Location update latency is the time to send a BU and receive a BA in order to register new CoA. An MN newly moving in a new subnet can send and receive packets after IP connectivity latency.

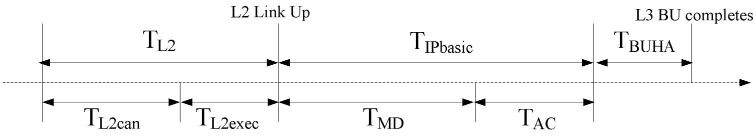


Fig. 6. Timing Diagram of MIPv6

Fig. 7 is the timing diagram of MIPv6 handover. T_{L2} is link switching latency T_{L2Scan} is the scan phase and T_{L2exec} is the execution phase of the layer 2 handover. $T_{IPbasic}$ is the IP connectivity latency. T_{MD} is movement detection latency and T_{AC} is address configuration latency. T_{BUHA} is the location update latency to register a new CoA.

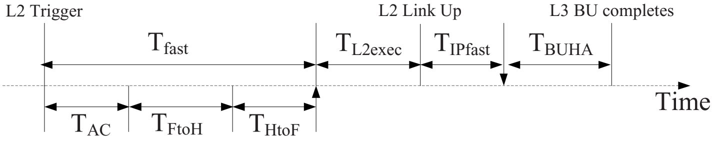


Fig. 7. Timing Diagram of FMIPv6

Fig. 8 is the timing diagram of FMIPv6. FMIPv6 performs movement detection and IP address configuration (T_{AC}) before the link switching. T_{FtoH} is the latency between sending a FBU and receiving a HI, and T_{HtoF} is the latency between sending a Hack and receiving a FBack. Because FMIPv6 performs a L2 scan periodically, link switching latency is T_{L2exec}. T_{IPfast} is a latency transmitting a FNA message.

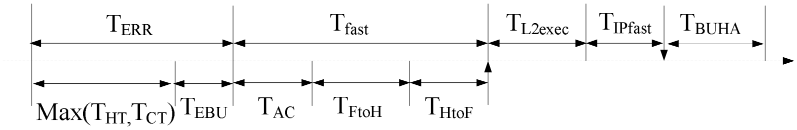


Fig. 8. Timing Diagram of Extended Return Routability

Fig. 9 is the timing diagram of FMIPv6 using ERR. The timing diagram of proposed scheme is similar to that of FMIPv6 except that proposed scheme has T_{ERR} before starting FMIPv6. In normal ERR, T_{ERR} consists of T_{HT} ,T_{CT} and T_{EBU}. T_{HT} means the latency to obtain home keygen token and T_{CT} means the latency to obtain a care-of keygen token. T_{EBU} is the latency to register the CoA-HoA binding. The latency of the normal ERR is $T_{HT} + T_{EBU} + T_{IP} + T_{L2exec} + T_{IPfast} + T_{BUHA} + T_{BUCN}$.

In optimized ERR, an MN already has the home keygen token of the PAR. Hence the latency of the optimized ERR is $T_{CT} + T_{EBU} + T_{IP} + T_{L2exec} + T_{IPfast} + T_{BUHA} + T_{BUCN}$.

4.3 Cost Analysis

We analyze performance of FMIPv6 using ERR by overall handover cost (CO). Overall handover cost (CO) consisting of signaling cost and delivery cost is given by

$$CO = CS + CD \tag{1}$$

CS is the sum of costs for signal messages, and CD is the sum of costs for delivering data packets during a handover. Signaling costs are given by

$$CS_{FMIPv6} = CS_{fast} + CS_{IPfast} + CS_{BUHA} + CS_{BUCN} \tag{2}$$

$$CS_{ERR} = CS_{HT} + CS_{CT} + CS_{EBU} + CS_{fast} + CS_{IPfast} + CS_{BUHA} + CS_{BUCN} \tag{3}$$

CS_{FMIPv6} is signaling cost of FMIPv6 and CS_{ERR} is signaling cost for FMIPv6 using ERR. Normal ERR and optimized ERR have the same signaling cost. CS_{IPfast} is signaling cost spent to perform the same operation of T_{IPfast}. Other signaling costs have the same meaning of the operations mentioned in the timing diagrams.

The delivery cost is estimated by forwarding costs and packets loss cost. Delivery costs of FMIPv6, FMIPv6 using the normal ERR and FMIPv6 using the optimized ERR are given by

$$\begin{aligned} CD_{FMIPv6} = {} & P_{suc.} \times \lambda \times \{CD_{preNet} \times (T_{AC} + T_{FtoH}) + CD_{newNetTunnel} \times T_{FMIPv6Tunnel}\} \\ & + \eta \times P_{fail} \times \lambda \times CD_{preNet} \times T_{MIPv6} \end{aligned} \tag{4}$$

$$\begin{aligned} CD_{ERR1} = {} & P_{suc.} \times \lambda \times \{CD_{preNet} \times (T_{ERR1} + T_{AC} + T_{FtoH}) + CD_{newNetTunnel} \times T_{FMIPv6Tunnel}\} \\ & + \eta \times P_{fail} \times \lambda \times CD_{preNet} \times T_{MIPv6} \end{aligned} \tag{5}$$

$$\begin{aligned} CD_{ERR2} = {} & P_{suc.} \times \lambda \times \{CD_{preNet} \times (T_{ERR2} + T_{AC} + T_{FtoH}) + CD_{newNetTunnel} \times T_{FMIPv6Tunnel}\} \\ & + \eta \times P_{fail} \times \lambda \times CD_{preNet} \times T_{MIPv6} \end{aligned} \tag{6}$$

CD_{preNet} is forwarding cost while an MN stays in a PAR before handover. $CD_{newNetTunnel}$ is forwarding cost while the MN in a NAR communicates with a CN through a tunnel. If the FMIPv6 handover fails, all packets are lost during the handover and the MN starts a MIPv6 handover instead of FMIPv6 handover. T_{MIPv6} means total handover latency of MIPv6 for considering packets loss cost. Delivery cost of FMIPv6 using ERR is similar to that of FMIPv6 except for the latency (T_{ERR}) to processing ERR. T_{ERR1} is the latency of the normal ERR and T_{ERR2} is the latency of the optimized ERR. The success rate of FMIPv6 handover is denoted by $P_{suc.}$. The failure rate of FMIPv6 handover is denoted by P_{fail}. η is a weight factor for retransmission due to lost packets. To calculate $P_{suc.}$ and P_{fail}, we refer to section 4.3 in [5] which shows a failure probability of FMIPv6.

4.4 Numerical Results and Analysis

$$T_{wired-RT}(h,k) = 3.63k + 3.21(h-1) \tag{7}$$

$$T_{wireless-RT}(k) = 17.1k \tag{8}$$

We use formulas derived from empirical communication delay model in [3]. Regression analysis of the collected data yields Eq. (7) and Eq. (8). k is the length of the packet in KB, h is the number of hops, and $T_{wired-RT}$ is the round-trip time for a wired link. $T_{wired-RT}$ is the round-trip time for a wireless link.

$$\lim_{p\to\infty}\frac{CO_{ERR1}}{CO_{FMIPv6}} = \lim_{p\to\infty}\frac{CS_{ERR}+CD_{ERR1}}{CD_{FMIPv6}+CD_{FMIPv6}} \approx 1.347 \tag{9}$$

$$\lim_{p\to\infty}\frac{CO_{ERR2}}{CO_{FMIPv6}} \lim_{p\to\infty}\frac{CS_{ERR}+CS_{ERR2}}{CD_{FMIPv6}+CD_{FMIPv6}} \approx 1.116 \tag{10}$$

We verify the performance of the proposed scheme by the rate of cost. Eq. (9) is the rate of FMIPv6 using the normal ERR. Through Eq. (9), we can get the result illustrated in Fig. 9. In the figure, the abscissa and ordinate show PMR and the rate of cost. The result converges to 1.289 in vehicle (μ=0.2) and 1.347 in pedestrian (μ=0.01). Therefore, in pedestrian, the normal ERR has approximately 34.7% overhead in comparison with only FMIPv6.

Eq. (10) is the rate of FMIPv6 using the optimized ERR. Through Eq. (10), we can get the result illustrated in Fig. 10. The result converges to 1.096 in vehicle and 1.116 in pedestrian. Therefore, in pedestrian, the optimized ERR has approximately 11.6% overhead in comparison with only FMIPv6. By the results we know that the proposed scheme has acceptable overall cost to supports real-time services. In addition to the overall cost overhead, the latency of normal ERR(T_{ERR1}) is 40.69 msec and the latency of optimized ERR (T_{ERR2}) is 12.09 msec. If a network with high processing power does not care the overhead and the handover interval of an MN is longer than T_{ERR1}, normal ERR is able to be authentication method for FMIPv6 sufficiently. Especially, optimized ERR is excellent authentication method for FMIPv6 in terms of the overall cost and the latency.

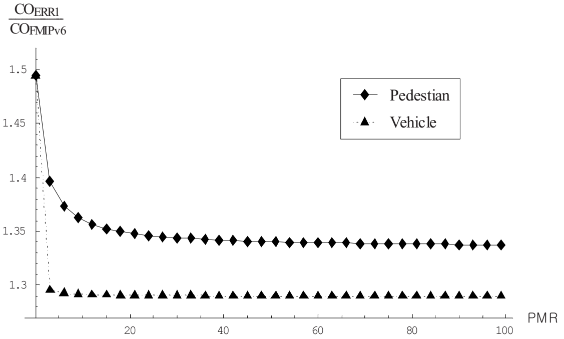


Fig. 9. Cost rate of FMIPv6 using normal ERR

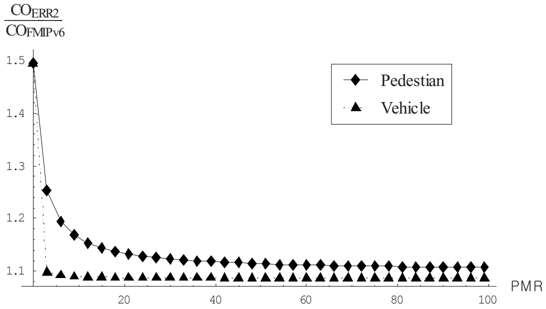


Fig. 10. Cost rate of FMIPv6 using optimized ERR

5 Conclusion

Most of the IPv6 handover protocols in IETF are designed without considering authentication between a mobile node and its serving node. Previous works on the authentication for handover protocol have mainly concentrated on studies using AAA, public certificates or cryptographic algorithms. However the approaches does not provide a generic authentication mechanism since the approaches need a particular infrastructure or a heavy processing cost to setup secure associations for handovers. Therefore, we extend the Return Routability so that our scheme could be a generic authentication mechanism for various IPv6 handover protocol without pre-configured infrastructure and heavy cryptosystem. Our scheme does not introduce a new entity for authentication, because it only uses fundamental entities for Mobile IPv6. And it does not introduce a new cryptosystem. In addition, as shown in the previous section, our scheme has acceptable latency and overhead. Especially, the optimized ERR has little latency and cost. We recommend to use the optimized ERR as long as an MN is able to know its serving node for handovers in advance.

References

1. Johnson, D., Perkins, C., Arkko, J.: Mobility Support in IPv6, RFC 3775
2. Koodli, R.: Fast Handovers for Mobile IPv6, RFC 4068
3. Jain, R., Raleigh, T., Graff, C., Bereschinsky, M.: Mobile Internet Access and QoS Guarantees using Mobile IP and RSVP with Location Registers. In: Proc. ICC'98 Conf., pp. 1690–1695 (1998)
4. Information technology-Telecommunications and information exchange between systems Local and metropolitan area networks-Specific requirement – Part 11: IEEE Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications, ANS/IEEE Std 802.1, Edition (1999)
5. Vatn, J.: An experimental study of IEEE 802.11b handover performance and its effect on voice traffic. SE Telecommunication Systems Laboratory Department of Microelectronics and Information Technology (IMIT) (July 2003)