A Ticket Based Binding Update Authentication Method for Trusted Nodes in Mobile IPv6 Domain

Ilsun You

School of Information Science, Korean Bible University,
205 Sanggye-7 Dong, Nowon-ku, Seoul, 139-791, South Korea
isyou@bible.ac.kr

Abstract.

With the increasing usage of Mobile IPv6 in the mobile internet environment, the need of binding update authentication methods to protect malicious biding updates becomes more prevalent. The current authentication methods have tried to secure the biding update process between two previously unknown nodes on the assumption that no global security infrastructure available. However, the assumption is improper for a network domain where involved nodes can establish trust with each other. In this paper, for such a network domain, we propose a ticket based BU authentication method. Our proposed method achieves more efficient and secure binding update through tickets that are issued based on pre-established trust among the involved nodes.

1 Introduction

Mobile Internet Protocol version 6 (MIPv6), specified by IETF [1], is a protocol that enables nodes to stay reachable regardless of their movements and locations in the IPv6 Internet. In order to achieve mobility and reacheability, this protocol let mobile nodes (MN) have two addresses: home address (HoA) and care-of address (CoA). Each MN belongs to a home network and is always identified by its HoA permanently allocated from its home network. While a MN visits a foreign network, it is associated with its CoA temporarily assigned by that network. The relation between the MN¡s HoA and CoA is called ¡binding¡ for the MN. Whenever the MN changes its location, it must notify the home agent (HA), a router in the MN¡s home network, and the correspond node (CN), the MN¡s peer node, of its new binding information. For this goal, the MN performs binding update (BU) processes with the CN as well as the HA. MIPv6 provides two possible modes for communications between the MN and the CN. The first mode, called bidirectional tunneling, deploys a HA as a trusted proxy for the MN in order that it may relay packets between the MN and the CN. However, such a triangle routing causes this mode to suffer from critical inefficiencies. For this mode, only the BU process between the MN and HA is needed. The second mode, called route optimization (RO), enables packets from the CN to be routed directly to the MN¡s CoA, thus eliminating the overhead resulted from tunneling via the HA. Before starting this mode, the MN should register its current binding at both the HA and the CN by performing the BU processes. Since, unlike the MN-HA path protected by IPsec, the MN-CN path is insecure, without securing the BU process between the MN and the CN, this mode exposes the involved nodes to various security threats. In order to protect that BU process, the IETF provided the return-routability (RR) method [1], where the CN verifies the MN¡s HoA and CoA while sharing a secret with the MN. Despites its advantages, the method results in the performance and security problems [2-4]. In addition to the RR method, various approaches have been proposed based on the public key cryptography [2-13]. They use their own public key method to enable the MN and the CN to share a strong secret, the lifetime of which is sufficient long to minimize the amount of signaling messages and handover latency.

These current methods have tried to secure the BU process between two previously unknown nodes on the assumption that no global security infrastructure available. However, the assumption is improper for a network domain where involved nodes can establish trust with each other. Thus, more efficient method based on pre-established trust relationship is needed for such a network domain.

In this paper, we propose a ticket based BU authentication method, which enables the secure and efficient BU process for such a network domain. For this purpose, the proposed method uses a ticket that is issued based on pre-established trust among the involved nodes.

The rest of the paper is organized as follows. Section 2 reviews and analyzes the related works. In section 3, we propose a ticket based binding update authentication method. Section 4 analyzes the proposed method, which is then compared with other methods. Finally, section 5 draws some conclusions.

2 Related Works

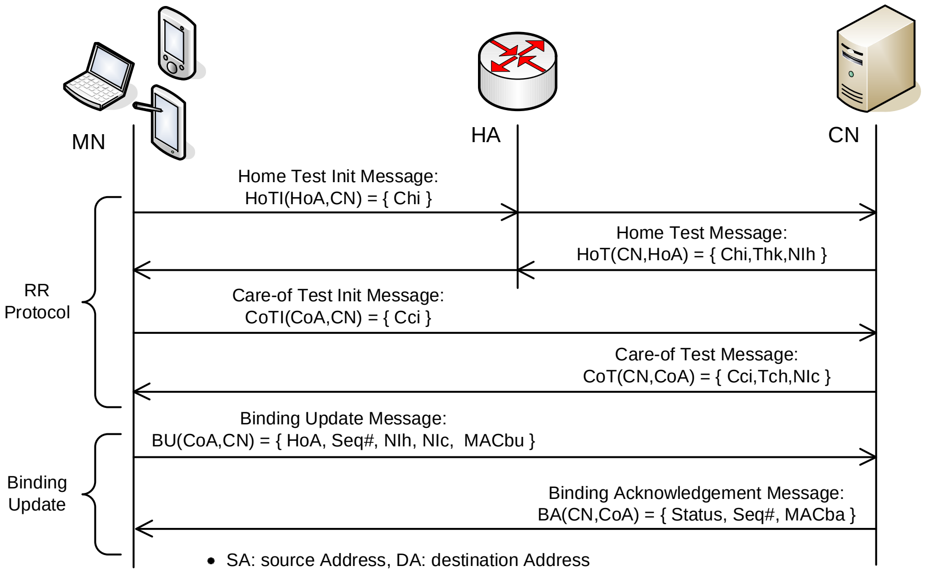
Before starting the RO mode, a MN performs a BU process by sending a BU message to its CN, which then responds with a binding acknowledgement (BA) message. The fundamental requirement for securing the BU process is that the CN authenticates both the MN and its BU message. Unfortunately, it is so difficult to achieve strong authentication between two previously unknown nodes (MN and CN) where no global security infrastructure is available. Thus, the need has arisen for a security solution to enable sufficient authentication between the CN and the MN without traditional secret- or public key based authentication infrastructures.

Several researches have been conducted to address this security issue. The IETF has accepted the RR method as the standard for the secure BU process [1]. Besides the RR method, various approaches have been proposed based on the public key cryptography [2-13]. For exclusion of additional security infrastructure, they attempted to associate the MN¡s HoA with its public key through techniques such as Address Based Keys (ABKs) [14], Cryptographically Generated Address (CGA) [15] and Purpose-Built Keys (PBK) [16]. Recently, in order to improve security and inefficiency problems caused by the RR method, the Optimized Mobile IPv6 (OMIPv6) series have been researched and drafted into the network working group in IETF [3-

8]. Like other public key based approaches, the OMIPv6 series use their own public key techniques to construct a strong secret shared between the MN and the CN while optimizing the RR method.

These current methods have tried to accomplish the secure BU process between two previously unknown nodes on the assumption that no global security infrastructure available. Thus, they require no configuration and no trusted entities except for the MN¡s HA. However, the assumption is not suitable for a network domain where involved nodes can pre-establish trust relationship with each other. That is, more efficient method using pre-established trust can be applied for such a network domain. For such case, the IETF introduces the static shared key method, which requires the configuration of a shared secret between the MN and its CN [17].

In this section, we analyze the static shared key method after reviewing the RR method and the OMIPv6 series.


MN
HA
CN
Home Test Init Message:
HoTI(HoA,CN) = { Chi }
Home Test Message:
HoT(CN,HoA) = { Chi,Thk,NIh }
RR
Protocol
Care-of Test Init Message:
CoTI(CoA,CN) = { Cci }
Care-of Test Message:
CoT(CN,CoA) = { Cci,Tch,NIc }
Binding Update Message:
BU(CoA,CN) = { HoA, Seq#, NIh, NIc, MACbu }
Binding
Update
Binding Acknowledgement Message:
BA(CN,CoA) = { Status, Seq#, MACba }

- SA: source Address, DA: destination Address
- Msg(SA,DA): It means that the message Msg is sent from SA to DA
- Chi: home init cookie, Cci: care-of init cookie
- CN: The IPv6 address of the correspondent node.
- Kcn: The CN¡s secret key
- NIh: home nonce index, NIc: care-of nonce index
- Nh: home nonce , Nc: care-of nonce
- Thk: home keygen token = First (64, HMAC_SHA1 (Kcn, (HoA | Nh | 0))
- Tck: care-of keygen token = First (64, HMAC_SHA1 (Kcn, (CoA | Nc | 1))
- Kbm: SHA1 (Thk | Tch)
- Seq#: Sequence number of the binding update message
- MACbu: First (96, HMAC_SHA1 (Kbm, CoA | CN | BU)
- MACba: First (96, HMAC_SHA1 (Kbm, CoA | CN | BA)
- Status: This value indicates the disposition of the binding update

Fig. 1 The RR method

2.1 The Return Routability Method

The RR method enables the CN to verify if the MN is really reachable at its claimed CoA as well as at its HoA. Also, it allows the two nodes to establish a shared secret, which is then used to authenticate the BU and BA messages. Fig. 1 illustrates this method composed of the Home Test Init (HoTI), Care-of Test Init (CoTI), Home Test (HoT) and Care-of Test (CoT) messages. While the HoTI and HoT messages are relayed via the HA, the CoTI and CoT messages are directly exchanged between the MN and the CN. In order to start this method, the MN sends the HoTI and CoTI messages to its CN at the same time. In response to them, the CN transmits the MN the HoT and CoT messages, which include keygen tokens Thk and Tck. By hashing the tokens together, the MN builds a binding management key Kbm, and concludes the RR method. Derived from Thk and Tck, Kbm allows the CN to verify that the MN is addressable at its HoA and CoA. Thus, the key can be used to protect the subsequent BU process between the MN and the CN. After the RR method, the MN executes the binding process by exchanging the BU and BA messages with the CN.

Though this method satisfies the security requirements for the RO mode, it leads to the following problems [1-4]. First, because of security reasons, the Kbm¡s lifetime is limited to maximum 420 seconds. That makes Kbm updated at a high frequency, thus causing the number of mobility signaling messages and handover latency to be increased. Second, the method doesn¡t protect its messages on the MN-CN path as well as the HA-CN path. Such vulnerability exposes the RO mode to various security threats every few minutes during the ongoing session.

2.2 The OMIPv6 Series

The OMIPv6 series have been proposed to improve the security and inefficiency problems caused by the RR method. This series typically consist of the initial phase and the subsequent movement phase as shown in Fig. 2. The initial phase includes the RR test and BU steps. While the RR test step allows a MN to validate its own two addresses through the RR method, the BU step allows its CN to authenticate its public key, verify the BU message through the digital signature and establish the long-term key, Kbmperm. Since the CN has strong assurance about correctness of the MN¡s HoA during the phase, it can accept that the HoA test is eliminated from the successive binding processes. Thus, in the subsequent movement phase, the MN and its CN need to execute at most the CoA test before exchanging the BU and BA messages. In order to achieve the maximum efficiency, the first version of the OMIPv6 series [3] lets only the BU and BA messages communicated during the subsequent movement phase. But, that makes the first method vulnerable to redirection-based flooding attacks while not allowing the CN to verify the MN¡s CoA. To address this problem, the phase needs to include the CoA test, which results in a considerable effect on the amount of handover latency and signaling messages. Consequently, the OMIPv6 protocol series have tried to optimize the test as described in Table 1 [4, 7, 13].

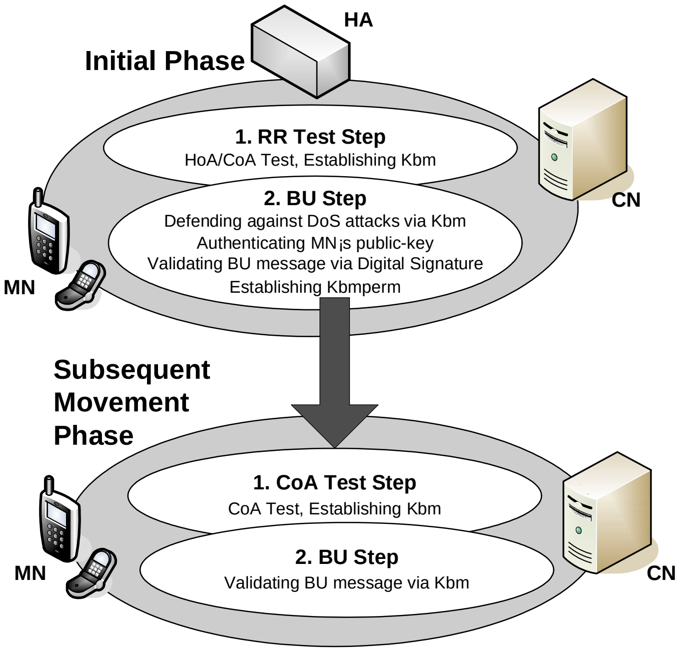

HA
Initial Phase
1. RR Test Step
HoA/CoA Test, Establishing Kbm
2. BU Step
Defending against DoS attacks via Kbm
Authenticating MN¡s public-key
Validating BU message via Digital Signature
Establishing Kbmperm
CN
MN
Subsequent Movement Phase
1. CoA Test Step
CoA Test, Establishing Kbm
2. BU Step
Validating BU message via Kbm
MN
CN

Fig. 2 The Route Optimization Mode of the OMIPv6 Series

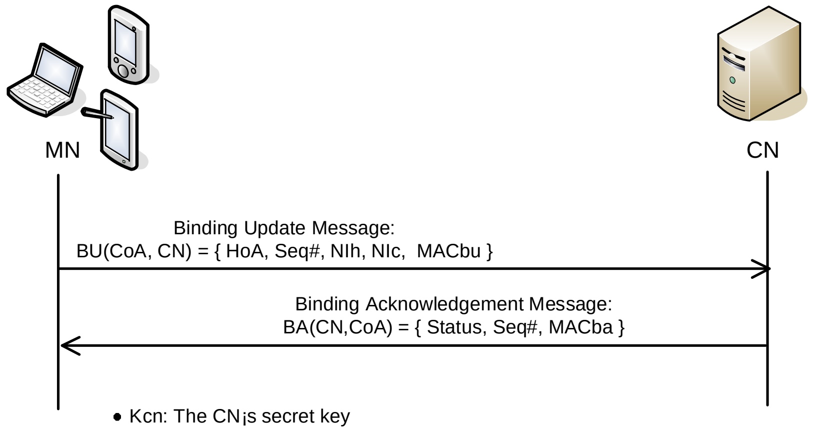
Table 1 Comparison of subsequent movement phases of the OMIPv6 series

Method	Technique for the CoA verification	Additional messages for the CoA verification	Latency until the MN starts to receive data packets
(1)	CoA test	CoTI and CoT	3 RTT
(2)	×	×	1 RTT
(3)	CoA test	CoTI and CoT	2 RTT
(4)	Early BU and CBA(credit-based authorization)	Early BU and BA messages including the CoA test option	1 RTT (only if the complete BU process is successful)
(5)	CoA test delegation	- RtMoSol and RtMAck - Prefix Test Init (PreTI) and Prefix Test (PreT)	between 1 RTT and 2 RTT (except for the first BU process in the MN¡s access network infrastructure)

* (1) The RR Protocol [1], (2) The OMIPv6 [5], (3) The OMIPv6-CGA Protocol [6], (4) The OMIPv6-CGA-CBA Protocol [8], (5) The CoA Test Delegation Protocol [13]

2.3 Static Shared Key Method

Recently, the IETF proposed the static shared key method for network environments where each MN can establish trust with its CNs [17]. In particular, this method is highly suitable for the case that MNs and CNs are administered within the same domain. As shown in Fig. 3, in this method, the MN and its CN preshare key materials such as Kcn, nonces and nonce indexes, which are used for generating a Binding Management Key (Kbm). Through the preconfigured key materials, this protocol can omit signaling messages relating to the routability tests, thus minimizing the handover latency and the amount of signaling messages caused by the RR method.


MN
CN
Binding Update Message:
BU(CoA, CN) = { HoA, Seq#, NIh, NIc, MACbu }
Binding Acknowledgement Message:
BA(CN,CoA) = { Status, Seq#, MACba }

- Kcn: The CN¡s secret key
- NIh: home nonce index, NIc: care-of nonce index
- Nh: home nonce, Nc: care-of nonce
- **Kcn, NIh, NIc, Nh and Nc are preshared between a MN and its CN**
- Thk: home keygen token = First (64, HMAC_SHA1 (Kcn, (HoA | Nh | 0))
- Tck: care-of keygen token = First (64, HMAC_SHA1 (Kcn, (CoA | Nc | 1))
- Kbm: SHA1 (Thk | Tch)
- Seq#: Sequence number of the binding update message
- MACbu: First (96, HMAC_SHA1 (Kbm, CoA | CN | BU)
- MACba: First (96, HMAC_SHA1 (Kbm, CoA | CN | BA)
- Status: This value indicates the result of the binding update

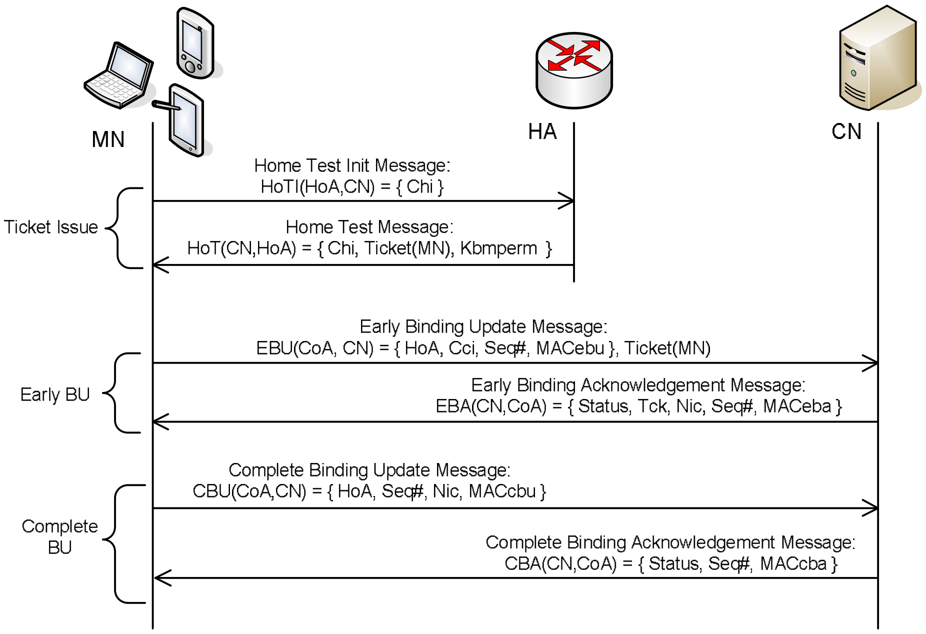
Fig. 3 Static Shared Key Method

Though this method achieves good efficiency, it has the following problems:

- Each CN needs the additional cost because it should preconfigure and maintain the key materials for its MNs. Such cost is more critical in an environment where every CN can be a MN.
- The elimination of the routability tests causes this method to be vulnerable to the redirection-based flooding attack, which the legitimate MN launches maliciously.
- This method depends on the sequence number Seq# to prevent the reply attack. When the sequence number rolls over, the involved nodes should configure new key materials.

3 Ticket Based Binding Update Authentication Method

In this section, we improve the static shared key method by employing a HA as a ticket issue server. For this goal, the proposed method requires the HA to pre-share a secret key with each CN. With such a pre-shared key, the HA securely distributes Kbmperm, a long-term key for binding management, between its MN and CN. That makes it possible for each MN to launch a binding update process with CNs, which establish trust relationship with its own HA. Thus, with the help of the HA playing a role of a ticket issue server, each CN can eliminate the cost for preconfiguring and maintaining the key materials for its MNs.


MN
HA
CN
Ticket Issue
Home Test Init Message:
HoTI(HoA,CN) = { Chi }
Home Test Message:
HoT(CN,HoA) = { Chi, Ticket(MN), Kbmperm }
Early BU
Early Binding Update Message:
EBU(CoA, CN) = { HoA, Cci, Seq#, MACebu }, Ticket(MN)
Early Binding Acknowledgement Message:
EBA(CN,CoA) = { Status, Tck, Nic, Seq#, MACeba }
Complete BU
Complete Binding Update Message:
CBU(CoA,CN) = { HoA, Seq#, Nic, MACcbu }
Complete Binding Acknowledgement Message:
CBA(CN,CoA) = { Status, Seq#, MACcba }

- Chi: home init cookie, Cci: care-of init cookie
- Kbmperm: a long-term key for binding management
- Kcn: The CN’s secret key
- NIc: care-of nonce index
- Nc: care-of nonce
- Tck: care-of keygen token = First (64, HMAC_SHA1 (Kcn, (CoA | Nc | 1))
- Kbm: SHA1 (Thk | Kbmperm)
- MACebu: First (96, HMAC_SHA1 (Kbmperm, CoA | CN | EBU)
- MACeba: First (96, HMAC_SHA1 (Kbmperm, CoA | CN | EBA)
- MACcbu: First (96, HMAC_SHA1 (Kbm, CoA | CN | CBU)
- MACcba: First (96, HMAC_SHA1 (Kbm, CoA | CN | CBA)

Fig. 4 Proposed Protocol

On the other hand, this method prevents the redirection-based flooding attacks by using the CoA test, which results in one additional round trip time (RTT) delay. Especially, in order to optimize the CoA test, it adopts the early binding update and credit-based authorization (CBA) techniques [7].

Fig. 4 shows the proposed method, which is divided into three phases as follows: ticket issue, early binding update and complete binding update phases.

Ticket Issue Phase: In this phase, when requested by the MN, the HA generates Kbmperm, a long-term key for binding update, and issues a ticket including the generated key in encrypted form. The MN uses both the long-term key and the ticket to perform binding update with the CN. In order to initialize this method, the MN sends the CN a HoTI message, which is forwarded via the HA. When arriving at the MN¡s home-link, the message is intercepted by the HA, which then checks if there is a secret key pre-shared between itself and the CN. If such a key does not exist, the RR method is performed from this point. Otherwise, the HA generates Kbmperm and issues a ticket for the MN. As depicted in Fig. 5, the ticket is composed of the MN¡s HoA, the HA¡s IPv6 address, the CN¡s IPv6 address, the life-time, EKey and MACticket. Especially, because EKey and MACticket are computed through Khc, the CN having Khc can verify the ticket and retrieve Kbmperm from it. In stead of forwarding the HoTI message to the CN, the HA responds the MN with a HoT message including Kbmperm and the ticket. Once the MN receives the ticket from the HA, the MN can omit this phase in each binding update process until its ticket is expired.

HoA	HA	CN	LT	EKey	MACticket

- HoA: the MN's home address
- HA: the HA's IPv6 address
- CN: the CN's IPv6 address
- LT: the period during which the ticket is valid
- Khc: a secret key shared between the HA and the CN
- EKey = E_{Khc}(Kbmperm)
- MACticket = HMAC(Khc, HoA|HA|CN|LT|EKey)

Fig. 5. Ticket Structure

Early Binding Update Phase: After the first phase, the MN and the CN execute the early binding update phase by exchanging the EBU and EBA messages. During the phase, the CoA test is applied to prevent the redirection-based flooding attacks. Especially, the CoA is performed in parallel with the data transmission from and to the MN¡s new CoA while minimizing the handover delay caused by itself. That is, the MN starts the data transmission immediately after sending the EBU message to the CN while the CN starts the data transmission immediately after sending the EBA message to the MN. In order to initiate the early binding update phase, the MN sends the CN the EBU message and its own ticket. When receiving them, the CN uses Khc, a secret key pre-shared between itself and the HA, to verifies the ticket. If the verification is successful, the CN decrypts EKey with Khc to retrieve Kbmperm, which is then used to check if the EBU message is valid. In the case of the valid EBU message, the CN not only learns the MN¡s new CoA but also believes that the MN is the legitimate owner of the HoA. While starting using the new CoA from this time, the CN concludes this phase by sending the MN the EBA including Tck, a care-of keygen token.

Complete Binding Update Phase: After the second phase, in spite of knowing the MN¡s new CoA, the CN still cannot be sure that the MN is actually present at the new address. Thus, the MN should proof that it is really reachable at its claimed CoA. For this goal, the MN performs the complete binding update phase. In order to start this phase, the MN sends the CN the CBU message, which can be authenticated through MACcbu computed with Kbm. Because Kbm is derived from Tck in addition to Kbmperm, the valid MACcbu lets the CN ensure that the MN receives the EBA message at its claimed CoA. Thus, if the CBU message is verified successfully, the CN believes the MN¡s presence at the new CoA. Finally, it concludes this phase by responding to the MN with the CBA message. As mentioned above, during the second phase, the data transmission is started though the MN¡s CoA is not verified. That causes the proposed method to be vulnerable to the misuse of unverified CoAs. To solve this security problem, the credit-based authorization (CBA) technique [7] is adopted. This technique limits the amount of the data transmission until the complete binding update phase finishes. In other words, if the amount of the data transmission is more than the specified value, the RO mode is postponed until the CBU message is verified successfully.

4 Analysis

This section analyzes the proposed method in terms of the management cost, the handover latency and the security. In particular, we focus on the management cost that each CN needs to preconfigure and maintain the key materials for its all MNs.

4.1 Management Cost

We use the following notations to derive the management cost of the proposed method.

- C_{MN}: the cost for the preconfiguration and maintenance of one node¡s key materials.
- C_{CN}: the management cost of all CNs
- C_{HA}: the management cost of the HA
- n: the number of MNs
- m: the number of CNs.
- o: the number of CNs that are a MN

The management cost of the static shared key method can be derived as follows:

$$C_{CN} = o(n-1)C_{MN}+(m-o)nC_{MN} = (on-o+mn-on)\ C_{MN} = (mn-o)C_{MN} \quad (1)$$

$$C_{HA} = nC_{MN} \quad (2)$$

$$C_{Total} = C_{CN}+C_{HA} = (mn+n-o)C_{MN} \quad (3)$$

The management cost of the proposed method can be derived as follows:

$$C_{CN} = mC_{MN} \quad (4)$$

$$C_{HA} = (n+m-o)C_{MN} \quad (5)$$

$$C_{Total} = C_{CN}+C_{HA} = (2m+n-o)C_{MN} \tag{6}$$

The difference between the proposed method and the static shared key method is as follows:

$$C_{Diff} = (mn+n-o)C_{MN} - (2m+n-o)C_{MN} = (n-2)mC_{MN} \tag{7}$$

According to the equation (7), we can know that if *n* is more than 2, the proposed method¡s management cost is less than that of the static shared key method. Because in general the number of MNs is much more than 2, the proposed method is more efficient than the static shared key method in terms of the management cost.

4.2 Security

Redirection-Based Flooding Attack: During the early binding update phase, the proposed method executes the CoA test to defend against this attack. That is, through the care-of keygen token Tck included in the EBA message, the CN can check if the MN is actually present at its claimed CoA. Also, this method adopts the CBA technique to guard against the misuse of unverified CoAs. With this technique, the method controls the amount of data transmission from and to the unverified CoA during the period between the early binding update and complete binding update phases. Such a strategy optimizes the trade-off between security and efficiency

Reply Attack: Because the HMAC values such as MACebu, MACeba, MACcbu and MACcba are computed freshly through Kbmperm randomly generated by the HA as well as the sequence number Seq#, they enable this method to prevent the reply attack. Thus, though the sequence number rolls over, the involved nodes do not need to configure new key materials.

4.3 Handover Latency

In Table 1, we derive the handover latencies of the proposed method, the RR method and the static shared key methods. While the static shared key method, which runs the binding update process without any address tests, has the optimized handover latency, the RR method including both the CoA and HoA tests has the worst handover latency. On the other hand, the proposed method can achieve the same handover latency as that of the static shared key method if the first phase is omitted. Because in most cases the proposed method runs without the first phase, it can provide the optimized performance.

Table 1. Handover latencies of the proposed method and others

Method		(1)	(2)	(3)	
				including the 1st phase	excluding the 1st phase
Handover Latency	Lsend (RTT)	Max(RTTcot, RTThot) = 2RTT	0 RTT	1RTT	0 RTT
	Lrecv (RTT)	Max(RTTcot, RTThot) + 1RTTbu = 3RTT	RTTbu = 1RTT	1RTT + RTTbu = 2RTT	RTTbu = 1RTT

* (1) the RR method (2) the static shared key method (3) the proposed method
RTTcot: the RTT for the CoA test (=1RTT),
RTThot: the RTT for the HoA test (=2RTT)
RTTbu: the RTT for exchanging the BU and BA messages (=1RTT)
Lsend: the latency until the MN starts to send data packets
Lrecv: the latency until the MN starts to receive data packets

5 Conclusions

In this paper, we propose a ticket based BU authentication method for a network domain where trust relationship can be established among involved nodes. Especially, we improve the static shared key method, which IETF introduces for such a network domain. For this goal, our proposed method employs a HA as a ticket issue server, which issues tickets based on pre-established trust. Such an employment requires the CN to make trust relationship with the HA instead of the MN, thus reducing the management cost of the CN. Also, our proposed method adopts the early binding update and CBA techniques in order to optimize the CoA test. Consequently, it is showed that our proposed method is efficient in terms of the management cost and security while achieving the almost same handover latency as that of the static shared key method.

References

1. D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6," IETF RFC 3775, June 2004
2. Kui Ren, Wenjing Lou, Kai Zeng, Feng Bao, Jianying Zhou, and Robert H. Deng, "Routing optimization security in mobile IPv6," Computer Networks, vol. 50, issue 13, pp. 2401-2419, Elsevier, Sep. 2006
3. I. You, "Improving the CGA-OMIPv6 Protocol for Low-Power Mobile Nodes," ICCSA 2006, Springer-Verlag LNCS 3983, pp. 336-343, May 2006
4. I. You and J. Lim, "Advanced Agent-Delegated Route Optimization Protocol for Efficient Multimedia Services at Low-Battery Devices," MMM 2007, Springer-Verlag LNCS 4352, Part II, pp. 479?486, Jan. 2007

5. W. Haddad, F. Dupont, L. Madour, S. Krishnan and S. Park, "Optimizing Mobile IPv6 (OMIPv6)," IETF Internet Draft, draft-haddad-mipv6-omipv6-01.txt, Feb. 2004 (Work in progress)
6. W. Haddad, L. Madour, J. Arkko and F. Dupont. "Applying Cryptographically Generated Addresses to Optimize MIPv6 (CGA-OMIPv6)," IETF Internet Draft, draft-haddad-mip6-cga-omipv6-04, Nov. 2005 (Work in progress)
7. J. Arkko, C. Vogt and W. Haddad, "Enhanced Route Optimization for Mobile IPv6," IETF RFC 4866, May 2007
8. F. Dupont and W. Haddad, "Optimizing Mobile IPv6 (OMIPv6)," IETF Internet Draft, draft-dupont-mipshop-omipv6-00.txt, Feb. 2006 (Work in progress)
9. G. O'Shea and M. Roe, "Child-proof authentication for MIPv6 (CAM)," ACM Computer Communications Review, Vol. 31, No. 2, April 2001
10. M. Roe, T. Aura, G. O'Shea, and J. Arkko, "Authentication of Mobile IPv6 Binding Updates and Acknowledgments," Internet Draft, draft-roe-mobileip-updateauth-02.txt, Feb. 2002 (Work in progress)
11. G. Montenegro, C. Castelluccia, "Crypto- Based Identifiers(CBIDs): Concepts and Applications", ACM Transations on Information and System Security, Vol. 7, No. 1, pp. 97-127, Feb. 2004
12. I. You and K. Cho, "A Security Proxy Based Protocol for Authenticating the Mobile IPv6 Binding Updates," ICCSA 2004, Springer-Verlag LNCS 3043, pp. 167-174, May 2004
13. W. Haddad, S. Krishnan and F. Dupont, "Mobility Signaling Delegation in OptiSEND," IETF Internet Draft, draft-haddad-mipshop-mobisig-del-02.txt, October 2006, (Work in progress)
14. S. Okazaki, A. Desai, C. Gentry and et. el., "Securing MIPv6 Binding Updates Using Address Based Keys (ABKs)," IETF, draft-okazaki-mobileip-abk-01.txt, Oct. 2002 (Work in progress)
15. T. Aura, "Cryptographically Generated Addresses (CGA)," IETF RFC 3972, March 2005
16. S. Bradner, A. Mankin and J. Schiller, "A Framework for Purpose-Built Keys (PBK)," IETF Internet Draft, draft-bradner-pbk-frame-06.txt, Oct. 2003 (Work in progress)
17. C. Perkins, "Securing Mobile IPv6 Route Optimization Using a Static Shared Key," IETF RFC 4449, June 2006