A New Authentication Scheme of Binding Update Protocol on Handover in Mobile IPv6 Networks

Jung Doo Koo[1], Jungsook Koo[2], Dong Chun Lee[3]

[1]Dept. of Computer Science and Eng., Hanyang Univ., Korea
jdkoo@cse.hanyang.ac.kr
[2]Dept. of Information Security, Kyonggi Univ., Korea
[3]Dept.of Computer Science, Howon Univ., Korea
ldch@sunny.howon.ac.kr

Abstract. We propose a new authentication scheme of binding update protocol, which its Correspondent Node (CN) issues a ticket to Mobile Node (MN) when MN first executes the Binding Update (BU). This ticket assist that it is able to do efficiently the BU whenever MN requires the BU for the future. The proposed protocol need not be repeated equal BU course whenever the MN moves to foreign link or network, and is able to be executed in environment of not operating the Home Agent (HA), and also easies scalability.

1 Introduction

MIPv6 [1] is the protocol of IP layer supporting node's mobility in IPv6. In MIPv6, MN has static Home Address (HoA) reaching without reference to now connected links and extraordinary CoA which is changeable when MN handovers to foreign link [1]. Also, located in foreign link, MN assumes that HA as a substitute of MN exists. When MN acquires new CoA from moving new link, it must register its CoA to HA. By registering this address, other nodes are always able to transfer messages using this node's HoA without reference to physical location of node. When MN isn't located in home link, messages received other nodes are sent to those nodes by using registered address in HA. But, because this method is always formed through HA, it brings about results which use inefficiently network. Accordingly, to solve this problem in MIPv6, MN also registers its Care-of Address (CoA) to its CN. By using this method, the connection between the MN and its CN are able to be optimized. This course which register CoA to HA and its CN, that is, are called “binding”. MIPv6 standard documentation of IETF is recommending to execute the BU to use Return Routability (RR) scheme [1]. But, if it doesn't securely execute the BU course, this course is able to be vulnerable in Denial-of Service (DoS) attack, redirect attack, and neighbor bombing attack [2].

But, RR scheme doesn't fully satisfy MIPv6 security requirements. In case of standard documentation [1], it is recommending to securely execute the BU courses by using IPSec [3, 4] into RR scheme to overcome these problems [5]. IPSec is able to be efficient between MN and HA supporting long-term connections. But, it may be inefficient between MN and its CN which is able to be formed by short-term connections. Also, IPSec can be a burden in case of communication node having low-power and limited computational quantities because of not little calculation costs executing internal key exchange protocol, Internet Key Exchange (IKE) [6], of IPSec. Therefore, it is required of mechanisms which safely execute the BU at low cost between MN and its CN without using IPSec mechanism. To solve this problem, many BU protocols have been proposed. But, the existed BU protocols have some problems.

In Return Routability (RR) [1] scheme, the information of creating session key is forwarded through public channel. Only, an attacker is able to intercept both Home Test (HoT) message and Care-of Test (CoT) message sending by two routers. It is not difficult if two attackers conspire. Child-proof Authentication for MIPv6 (CAM) [7] has problems as follows. First, this protocol takes costs for signing messages in MN and costs for verifying this signature in its CN. Second, it only supplies authentication of MN's HoA. Finally, it just supplies one way authentication.

The existed BU protocols may be iterated equal protocol course whenever MN moves to foreign link. This method has two problems. First, it can reduce the efficiency of entire protocol because of always iterating same protocol course whenever MN gained new CoA from foreign link. Second, because the BU a limited lifetime, MN must update a lifetime.

We propose the secure and efficient TBU protocol, which the BU using the ticket is able to promote efficiency by reducing iterating courses of entire protocol.

2 The Proposed Protocol

We present TBU protocol for secure BU. It is designed for being suitable for almost all environments; in case of which a CN is not only a fixed node but also a portable node. In addition, when the CN is the moving node, the proposed protocol doesn't give computational burden such as public key operation, exponential calculation to MN.

In TBU protocol, we assume that the connection between a MN between it’s HA, between it’s HA and the HA of CN, between a CN and its HA is able to establish secure tunnel using the IPSec. Also, the CN is able to be not only fixed node but also moving node. The detailed protocol is following.

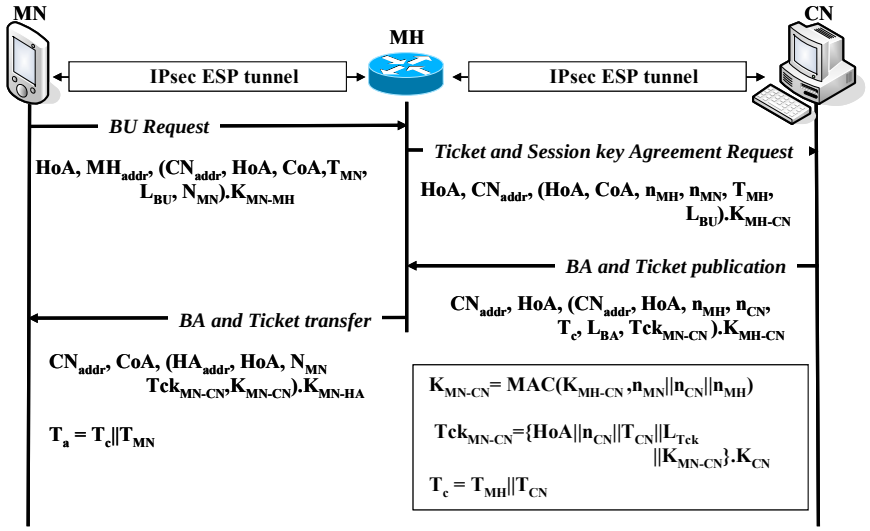

Fig. 1. The basic TBU protocol at first between MN and its CN via Mobile Host (MH)

The following notation is used in describing our protocol.

- *BU/BA*: A binding update/binding acknowledgement.
- *MN*/*MH*: Mobile node/its home agent
- *CN*/*CH*: Correspondent node/ its home agent
- *HoA*/CoA_A: A home address of MN and care-of address of a node *A*.
- MH_{addr}/CH_{addr}/CN_{addr}: The address of MH/CH/CN.
- $K_{A\text{-}B}$: A secret key between *A* and *B*.
- K_A: A secret key of *A*.
- $Cookie_A$: A cookie generated by *A* (the parameter for preventing DoS).
- $L_{BU/BA}$: A lifetime of BU/BA.
- T_A: A timestamp generated by *A*.
- *MAC (M, K)*: Keyed hash of message *M* with key *K* for authenticating message *M*.
- $Tck_{A\text{-}B}$: A ticket between *A* and *B*.
- n_A: A nonce generated by *A*.
- *a* ‖ *b*: A bit concatenation of message *a* and *b*

The nodes which participated in basic protocol are MN, Mobile Host (MH), and CN. But, the BU protocol at the future only participates in MN and its CN. The role of MH is to create the secret key and the ticket with CN instead of the MN. The detailed basic protocol is same to Fig. 2. The connection between MN and MH, between MH and CN is protected securely via ESP tunnel. We describe some of the features of TBU protocol.

Message 1. This message which sends to MH is to request BU to MH and CN. The MN creates a nonce n_{MN} and associates the nonce with its CN in its binding update list. It is used to prevents messages from replay attack and create secret key. T_{MN} and L_{BU} is a timestamp and a lifetime generated by MN, respectively. A lifetime of BU has a fixed time. Accordingly, even though MN doesn't move to a foreign link or network, the lifetime of BU must be re-updated before the lifetime is over. $K_{MN\text{-}MH}$ is IPSec secret key between MN and MH.

$$HoA, MH_{addr}, (CN_{addr}, HoA, CoA, n_{MN}, T_{MN}, L_{BU})K_{MN-MH}$$

Message 2. Upon receiving message 1, MH registers CoA of MN and stores binding information into binding cache. MH creates nonce n_{MH} for preventing a message from replay attack and creating secret keys. It sends a message to CN communicating with MN to request ticket creation and BU. This message is also sent to MN's CN via the secure protected ESP tunnel. It is a message which request for creating ticket and executing BU between MN and CN. The MH forwards other parameters received from MN to CN.

$$HoA, CN_{addr}, (HoA, CoA, n_{MN}, n_{MH}, T_{MH}, L_{BU})K_{MH-CN}$$

Message 3. The MN's CN first validates nonce, timestamp, and lifetime received from MH. It then generates a symmetric key $K_{MN\text{-}CN}$ between MN and its CN, which will be used as the ticket key. Also, it creates $Tck_{MN\text{-}CN}$ that will be used by the node with HoA. The ticket consists of HoA of node's address using ticket, nonce n_{MN}, timestamp $T_{CN,}$ ticket's lifetime L_{Tck}, a symmetric key $K_{MN\text{-}CN}$ between MN and its CN. It is able to use the purpose of authenticating MN when MN moved to foreign link. By publishing ticket, the BU between MN and its CN for the future becomes very simply. The protocol's efficiency then is raised by reducing the iteration of entire protocol course. The CN registers CoA of MN. Then, the binding information is stored into binding cache of CN.

$$CN_{addr}, HoA, (CN_{addr}, HoA, n_{MH}, n_{CN}, T_c, L_{BA}, Tck_{MN-CN})K_{MH-CN}$$
$$T_c = T_{MH} \,||\, T_{CN}$$

$$K_{MN-CN} = MAC(K_{MH-CN}, n_{MN} \,||\, n_{CN} \,||\, n_{MH})$$
$$Tck_{MN-CN} = (HoA \,||\, n_{CN} \,||\, T_{CN} \,||\, L_{Tck} \,||\, K_{MN-CN})K_{CN}$$

Message 4. The MH intercepted this message creates the symmetric key $K_{MN\text{-}CN}$ like CN. It adds the nonce n_{MN} received from MN at first to message. After it concatenated each node's timestamp, it forwards this message to MN via secure ESP tunnel. MN received message 4 first checks the nonce n_{MN} created itself. Then, MN stores securely the ticket $Tck_{MN\text{-}CN}$. As a result, our protocol is first performed simul-

taneously both the key distribution and the BU courses via secure ESP tunnel recommending in IETF. By using ticket, the next BU is able to be executed with only two messages such as a BU and a BA message. It aims to upgrade a performance of BU protocol by minimizing the courses of the entire protocol.

$$CN_{addr}, CoA, HoA, (n_{MN}, T_a, Tck_{MN-CN}, L_{BA}, K_{MN-CN})K_{MN-MH}$$
$$T_a = T_c \,||\, T_{MN}$$

When MN again moves to foreign link or network, it doesn't perform all basic TBU protocol courses. MN executes BU by using only two messages like BU message containing the ticket and BA message. So, the TBU protocol is able to elevate the efficiency of entire protocol and to reduce abilities witch are attacked from attackers by decreasing message number. The protocol is illustrated as Fig.2.

***BU* message**. MN directly sends this message to CN to register new CoA which gains in foreign link or network. Because the connection between MN and its CN isn't protected by secure ESP tunnel, there may be various attacks. Accordingly, it creates and adds security parameters to message. After created a cookie $Cookie_1$, It sends it to its CN. The aim of cookie is to first filter attacks such as DoS or flooding attack etc. It also inserts a ticket Tck_{MN-CN} generated by CN in the message. It then sends the BU message to CN directly.

***BA* message.** Upon receiving BU message, CN first checks on the validity of a cookie $Cookie_1$ whether attack is or not. Also, it generates the cookie $Cookie_2$ and then sends it to MN. And, it verifies the validity of the ticket by decrypting and checking the validation period and the MN's HoA included in the ticket. Then, it verifies the MAC using the ticket key. Also, CN checks a lifetime of BU message and inserts the lifetime of BA L_{BA}, n'_{MN} generated by MN in BA message. If everything is ok, CN stores the nonce and BU information in its binding cache. It then responds to BU message by sending the BA message.

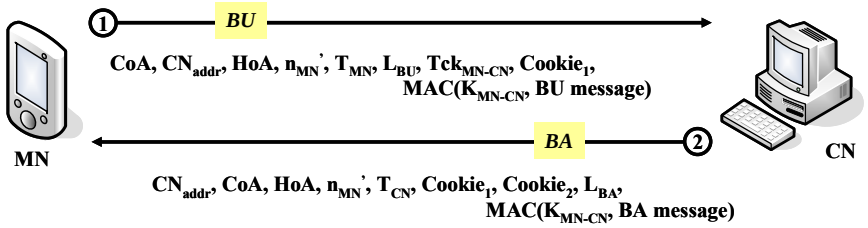

Fig. 2. The basic TBU protocol for the future between MN and its CN.

3 The Protocol Analysis

In MIPv6, in case of not executing safely the binding update courses, there are various attacks such as DOS attack, redirect attack, and neighbor bombing attack, etc. Therefore, The BU must be satisfied with the security requirements as follows.

• **An authentication of requester:** The HA and MN's CN must be able to confirms whether it is the request of MN possessed HoA or not before they recognize the BU request of MN. If it isn't confirmed from nodes, attackers can be various redirect attacks by executing the BU in disguise with a justified MN.

• **An authentication of responder:** MN must be able to affirm whether the response message for BU request is the acknowledgement message of its CN communicating now with itself or not. If not, MN is able to mistake that the binding update was successful. In this case, the directly delivered message through routing optimization is dropped.

• **Integrity of binding information:** It must support the integrity of CoA information of MN. If doesn't supply, attackers is able to be various attack by changing CoA of MN.

• **A location authentication of requester**: MN's CN must be able to verify whether MN really exists in suggesting current location (CoA of MN) or not. If not, by using address of other nodes, attackers can be bombing attack against target node.

Now, we will discuss how strong our protocol TBU is against various attacks such as Denial-of Service (DoS) attack and Redirect attack.

DoS attack is that a justified users is not able to execute the protocol. It can be divided with resource depletion attack and connection depletion attack. The former is attack of targeting nodes not using fixed resource like mobile node as the attack for consuming calculation resource of server. But, the latter is attack for exhausting the connection of being able to permit in server.

DoS attack is not problem of solving certainly in BU protocol because it is able to occur in all communication protocols. Also, to protect completely it is very difficult. Besides, this attack is not attack which is able to settle in satisfyingness of security requirements on contrary to redirect attack and neighbor bombing attack. To alleviate DoS attack, a generally used scheme is divided as follow. First, it comprise protocol so not to be necessary that nodes are able to support the status information for reducing cases that services are rejected from the exhaustion of buffer sustaining connection status datum. Second, nodes authenticate the communicated messages for reducing cases of maintaining unnecessary connection information. Third, to be difficult the attack, those use client puzzle. Second scheme requires adding costs of authenticating messages. So, it is used generally with more and more increased method.

TBU protocol uses cookie to prevent this attack. MN first creates cookie, then on receiving the cookie its CN checks on the validity of it. If is not right this information, CN drops a message.

Various attackers may try to redirect the mobile node's traffic to some other nodes including itself. If the attacker can procure the private key of the victim or the ticket key of the victim’s ticket, the attacker is able to be successful at this attack. We as-

sume that both are infeasible if the attacker is attempting a passive cryptanalysis attack.

Table 2. The satisfaction of security requirement of protocols

	mutual authentication		message integrity	location authentication
	MN	CN		
RR	×	×	×	△
ECBU	○	○	○	△
CAM	○	×	○	△
CBID/SUCV	○	○*	○	△
Proposed Method	○	○	○	△

We will first argue that our protocol and existing BU protocol satisfy the security requirements of the BU protocol. In Table 2, all protocols with the exception of CAM [7] and RR protocol supplies a mutual authentication. In case of SUCV protocol, it is able to settle mutual authentication by IPSec only. Also, TBU protocol and ECBU protocol provide the mutual authentication by using HA. The integrity of BU message can be authenticated by encrypting the securely established session key and making signature the BU request message. There are not securely confirming methods whether MN exists in MN's CoA or not. But all schemes have a certain amount of devices to solve this problem.

4 Conclusion

In this paper we presented solution to elevate efficiency by reducing iterating BU courses via ticket. The ticket-based binding protocol takes diverse advantages. First, the CN need not maintain the status information of session key between MN and its CN because it encrypts the ticket using its private key. Second, both MN and its CN is able to perform BU in environments on not operating a HA of MN such as P2P circumstances.

Also, proposed TBU protocol satisfies the safety of protocol and security requirements such as mutual authentication, the integrity of the BU message and a certain amount of location authentication because this ticket is only able to create in CN or HA of CN and the session key between MN and its CN is contained in it.

Acknowledgements

This work was supported by Fund of ITRC at Korea Univ., 2006.

References

1. D. Johnshon, C. Perkins, J. Arkko, “Mobility Support in IPv6,” IETF RFC 3775, 2004.
2. P. Nikander, J. Arkko, T. Aura, G. Montenegro, E. Nordmark, “Mobile IP Version 6 Route Optimization Security Design Background,” IETF RFC 4225, December 2005.
3. S. Kent, R. Atkinson, “IP Authentication Header,” IETF RFC 2402, November 1998.
4. S. Kent, R. Atkinson, “IP Encapsulating Security Payload (ESP),” IETF RFC 2406, November 1998.
5. J. Arkko, V. Devarapalli, F. Dupont, “Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents,” IETF RFC 3776, June 2004.
6. D. Harkins, D. Carrel, “The Internet Key Exchange (IKE),” IETF RFC 2409, 1998.
7. G. O'Shea, M. Roe, “Child-proof Authentication for MIPv6 (CAM),” ACM Computer Communications Review, Vol. 31, pp. 4-8, July 2001.
8. T. Aura, “Cryptographically Generated Addresses (CGAs),” IETF RFC 3972, 2005.
9. G. Montenegro, C. Castelluccia, “Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Address,” ISOC Symposium on Network and Distributed System Security (NDSS 2002), February 2002.
10. G. Montenegro, C. Castelluccia, “Crypto-Based Identifiers (CBID): Concepts and Application,” ACM Transaction on Information and System Security, Vol. 7, pp. 97-127, February 2004.
11. R. Deng, J. Zhou, F. Bao, “Defending against Redirect Attack in Mobile IP,” Proc. of the 9th ACM Conference on Computer and Communications Security, Washington D.C., November 2002.
12. Y. Qiu, J. Zhou, F. Bao, “Protecting All Traffic Channels in Mobile IPv6 Networks,” In Proceeding of WCNC ‘04, Vol. 1, pp. 160-165, March 2004.
13. S. Thomson, T. Narten, “IPv6 Stateless Address Auto-configuration,” IETF RFC 2462, December 1998.
14. R. Droms, “Dynamic Host Configuration Protocol (DHCP),” IETF RFC 2131, March 1997.