A Study of an Integrated Security Handover Scheme for Hierarchical Mobile IPv6 based Multimedia Convergence Networks

Ronnie D. Caytiles[1], Byungjoo Park[1*]

[1]*Multimedia Engineering Department, Hannam University*
133 Ojeong-dong, Daeduk-gu, Daejeon, Korea
rdcaytiles@gmail.com , bjpark@hnu.kr
**Correspondent Author: Byungjoo Park* (bjpark@hnu.kr)*

Abstract

Hierarchical Mobile IPv6 introduces a new node called the Mobile Anchor Point (MAP) to improve the handover speed performance of Mobile IPv6 by reducing the amount of signaling in the ongoing connection between the mobile node, its correspondent nodes, and its home agent. With MAP as an additional node, it's signaling, both received and sent is subject to several security vulnerabilities that needs addressed. Authentication and authorization of Binding Updates (BUs) to the MAP is essential during the registration process.

This paper deals with securing the hierarchical mobile IPv6 handover scheme by adding a cryptography procedure for authenticating the binding updates sent by mobile nodes during the mobile anchor point registration process.

Keywords: H*MIPv6, IPsec, BU, BA, Authentication*

1. Introduction

The binding updates to the Mobile Anchor Point (MAP) do not require confidentiality that may lead to malicious mobile nodes acting as legitimate ones or impersonating a MAP. An unauthenticated or malicious BU messages can provide intruders an easy means to launch various types of attacks that could create serious security breaches [4]. Unauthenticated BU information makes it possible for an attacker to misinform correspondents about the node's location and, thus, to redirect packets intended for the mobile to a wrong destination. This can lead to the compromise of secrecy and integrity as well as to denial-of-service because the target nodes are unable to communicate.

Although the Hierarchical Mobile IPv6 (HMIPv6) introduces a new concept of adding a Mobility Anchor Point (MAP) that acts as a local home agent to Mobile IPv6 (MIPv6), it is essential that security must be given considerations. It is essentially important to secure the exchange of signals between the mobile node and the MAP. The confidentiality of the communication between the mobile node and its correspondent nodes basically depends on how strong the mutual authentication, integrity protection, and protection against replay attacks of the MN-MAP relationship.

The currently method for securing BUs and other HMIPv6 control signals in MAP or HA registration process is the use of IPSec ESP in the transport layer. IPSec ESP or the IP Security Encapsulation Security Payload [2] is designed as the means of securing signaling messages between the Mobile Node and Home Agent for Mobile IPv6 (MIPv6) [5]. Securing the HMIPv6 signaling messages includes the secured authentication of the Binding Updates and Acknowledgement messages used for managing the bindings between a Mobile Node and the Mobile Anchor Point.

Based on the analysis of the security weaknesses that exists in previously proposed protocols, this paper proposes to consider the implementation of an IPsec with mobility message authentication option for a secured authentication of Binding Updates and Acknowledgement messages between MN and MAP [6, 8, 9]. It deals with securing the authentication of the binding updates (the location information sent by the MN to the MAP) during the MAP registration in a HMIPv6 handover procedure. The remainder of this paper is organized as follows; Section 2 explains the basic operations and the standard handover procedure of the HMIPv6, Section 3 deals with the proposed security scheme for binding-update authentication protocol, and Section 4 concludes the study.

2. MIPv6 vs HMIPv6

2.1 MIPv6

A mobile node (MN) is addressed by two IP addresses in MIPv6, that is, a home address (HoA) and a care-of address (CoA) [7, 10]. A Mobile Node (MN) has its static HoA at its home subnet. When moving to a new subnet, the MN will discover the default router, perform address auto-configuration, and use its new address as CoA. The former is an IP address assigned to MN within its subnet prefix on its home link and the latter is a temporary address acquired by MN while visiting a foreign link. This dual address mechanism realizes the design goal of MIP. Mobility support in IPv6 is considered particularly important, since mobile devices are predicted to account for a significant fraction of the population of the Internet during the lifetime of IPv6. Figure 1 shows the MIPv6 Architecture.

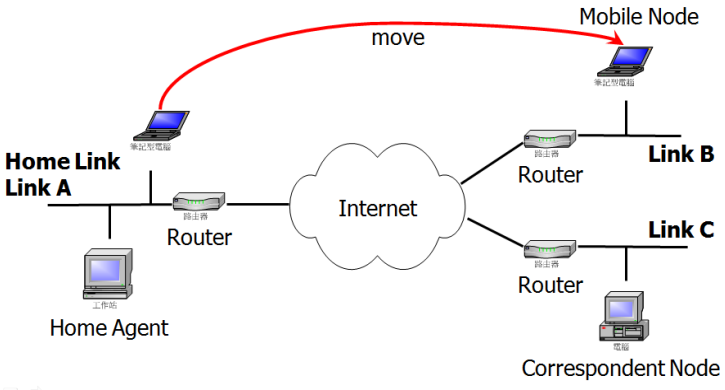

Figure 1. Mobile IPv6 Architecture [10]

2.2 HMIPv6

The HMIPv6 has been introduced for the purpose of reducing the number of signaling messages and thus eliminating additional delays to speed up the handover performance [1, 3]. In MIPv6, MN sends a binding update (BU) message to its home agent (HA) and correspondent nodes (CNs) each time that it changes location or moves. Every time MN moves around where there is a handoff procedure to a new access router (AR) that is being performed, many signaling messages are sent, thus, the handover performance of MIPv6 suffers from a series of delays if the MN moves frequently or the distance between MN to HA is far enough.

Figure 2 shows the hierarchical Mobile IPv6 architecture wherein it introduces a new node, the MAP that serves as an intermediary or proxy for the Home Agent (HA) in foreign network. As the Mobile Node (MN) enters a MAP domain, it can receive Router Advertisements that contain information for existing local MAPs. It then configures its current location through two care-of-addresses (CoAs), the regional CoA (RCoA) and an on-link CoA (LCoA).

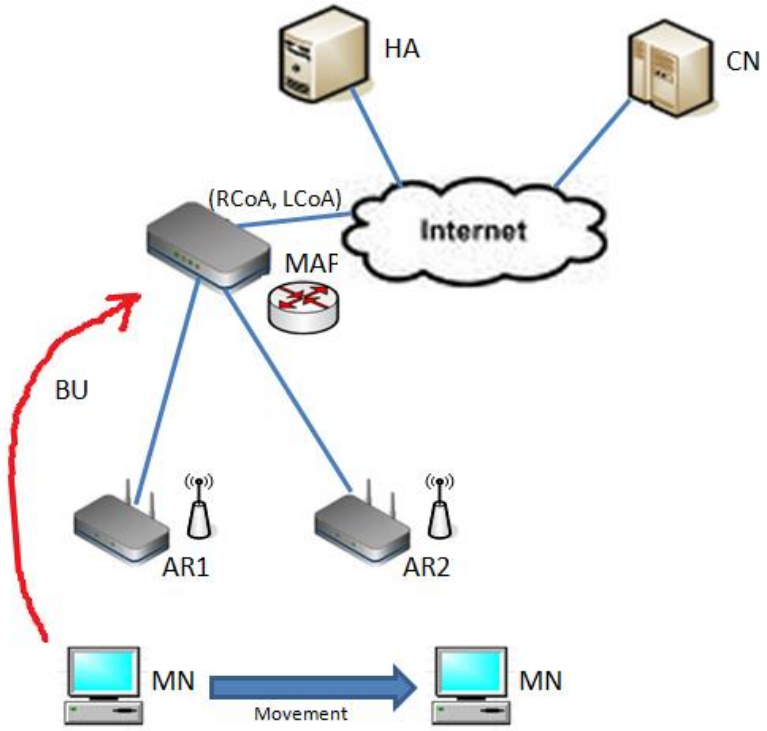

Figure 2. Hierarchical Mobile IPv6 Architecture

The Regional Care-of Address (RCoA) is an address on the MAP's subnet based on the prefix in the MAP option of the router advertisement (RA) message sent by MAP. It is an address obtained by the mobile node from the visited network. It is auto-configured by the MN when receiving the MAP option.

The On-link CoA (LCoA) is an address configured on an MN's interface based on the prefix advertised by its default router (AR). When an MN first enters an MAP domain, it sends a BU message to the HA and CNs through the MAP. While the MN moves within the same MAP domain, it only sends the BU message to the MAP. The MAP is essentially a local HA. It is sometimes simply referred to as the Care-of-address.

The MAP receives all packets on behalf of the mobile node it serves and will encapsulate and forward them directly to the mobile node's current address instead of the HA (MAP acting as local HA). If the mobile node changes its current address within a local MAP domain (LCoA), it only needs to register the new address with the MAP. Hence, only the Regional CoA (RCoA) needs to be registered with correspondent nodes and the HA. The RCoA does not change as long as the MN moves within a MAP domain, thus making the mobile node's mobility transparent to the CN where it exchanges signals with.

3. Integrated Security HMIPv6 Handover Schemes

The main focus of this study is to have a strong confidentiality on the exchange of signals between the new node introduced by the Hierarchical Mobile IPv6 (HMIPv6), known as the Mobility Anchor Point (MAP) that acts as a local home agent to Mobile IPv6 (MIPv6), and the mobile node. The foundation of confidentiality in the communication between the mobile node and its correspondent nodes basically depends on how strong the mutual authentication, integrity protection, and protection against replay attacks of the MN-MAP relationship.

This section identifies security considerations for the exchange of signals between the MN and the MAP [1]. First, an initial authorization of MN to be able to use the MAP service can be done based on the identity of the mobile node exchanged during the security association (SA) negotiation process. The authorization may be granted based on the mobile node's identity or based on the identity of a Certificate Authority (CA) that the MAP trusts. For instance, if the mobile node presents a certificate signed by a trusted entity (*e.g.*, a CA that belongs to the same administrative domain, or another trusted roaming partner), it would be sufficient for the MAP to authorize the use of its service. This guarantees that the mobile node and the MAP are authenticated for address allocation and future binding updates without the need for identity authentication [1].

Second, IKEv2 must be supported by the mobile node and the MAP. IKEv2 allows the use of Extensible Authentication Protocol (EAP) as a mechanism to bootstrap the security association between the communicating peers. EAP can be used with IKEv2 to leverage the Authentication, Authorization, and Accounting (AAA) infrastructure to bootstrap the SA between the mobile node and the MAP. Such a mechanism is useful in scenarios where an administrator wishes to avoid the configuration and management of certificates on mobile nodes.

Third, HMIPv6 uses an additional registration between the mobile node and its current MAP. When a mobile node moves into a new domain (*i.e.*, served by a new MAP), it obtains an RCoA and an LCoA and registers the binding between these two addresses with the new MAP. The MAP then verifies the BU and creates a binding cache entry with the RCoA and LCoA. Whenever the mobile node gets a new LCoA, it needs to send a new BU that specifies

the binding between its RCoA and its new LCoA. This BU needs to be authenticated; otherwise, any host could send a BU for the mobile node's RCoA and hijack the mobile node's packets.

Lastly, The IPsec Peer Authorization Database (PAD) entries and configuration payloads for allocating dynamic home addresses can be used by the MAP to allocate the RCoA for mobile nodes. Binding updates between the MAP and the mobile node must be protected with either Authentication Header (AH) or Encapsulating Security Payload (ESP) in transport mode.

This paper proposes a scheme for securing the Binding Update and Binding Acknowledgment messages between the Mobile Node and Mobile Anchor Point using a mobility message authentication option that is included in these messages. This scheme implements the IPSec with mobility message authentication option for a secured authentication of Binding Updates and Acknowledgement messages between MN and MAP. It enables HMIPv6 mobility in a host without having to establish an IPsec SA with its Home Agent. A Mobile Node can implement HMIPv6 without having to integrate it with the IPsec module, in which case the Binding Update and Binding Acknowledgement messages between the MN and MAP are secured with the mobility message authentication option. This scheme makes use of public key certificate-based strong authentication technique to ensure data integrity. The enhanced security algorithm is developed and embedded as a mobility message authentication option that is appended to the HMIPv6 signaling messages to prepare a secured communication between MN and CN. The proposed scheme is able to detect and prevent attackers from eavesdropping and modifying packets intended to specific nodes.

4. Conclusion and Future Works

This study identifies the secured authentication schemes of Mobile Node (MN) to Mobile Anchor Point (MAP) registration for HMIPv6 Handover scheme. To ensure a strong confidentiality in the exchange of signals between the mobile node and its correspondent nodes, it is essentially important to have a strong relationship between the mobile node and the MAP. The MN and MAP must have a strong mutual authentication, integrity protection, and protection against replay attacks, thus cannot lead to the compromise of secrecy and integrity as well as to denial-of-service because the target nodes are unable to communicate.

The quantitative and qualitative analysis and design of HMIPv6 authentication with respect to the IPSec and IKEv2 will create more challenges about the authentication in IPv6 wireless networks in the future.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2010-0024401, 2011-0026286, 2012-0007273).

References

[1] H. Soliman, C. Castelluccia, K. ElMalki and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", IETF, RFC No. 5380, **(2008)** October.

[2] http://ipv6.com.

[3] http://searchmobilecomputing.techtarget.com/definition/Hierarchical-Mobile-IPv6.

[4] K. Ren, W. Lou, K. Zeng, F. Bao, J. Zhou and R. H. Deng, "Routing optimization security in mobile IPv6", Computer Networks, Elsevier B.V. 2005.09.019, **(2005)**.

[5] J. Arkko, "Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents", IETF RFC 3776, **(2004)**.

[6] H. Krawczyk, M. Bellare and R. Canetti, "HMAC: Keyed-Hashing for Messaging Authentication", IETF RFC 2104, **(1997)**.

[7] J. Davies, "Understanding IPv6", Microsoft Press, Redmond, WA, **(2003)**.

[8] L. Wang, M. Song and J. -d. Song, "An efficient hierarchical authentication scheme in mobile IPv6 networks", School of Electronic Engineering, The Journal of China Universities of Posts and Telecommunications, China, **(2008)** October.

[9] H. Zhou, H. Zhang and Y. Qin, An authentication method for proxy mobile IPv6 and performance analysis, Institute of Electronic Information Engineering, Beijing Jiaotong University, **(2008)** September.

[10] R. D. Caytiles, Y. E. Gelogo and B. J. Park, "An Integrated Security Handover Scheme for Seamless Convergence Services over IP-based Mobile Networks", International Journal of Control and Automation, vol. 4, no. 4, SERSC, **(2011)** December, pp. 55-62.