An Integrated Security Handover Scheme for Seamless Convergence Services over IP-based Mobile Networks

Ronnie D. Caytiles[1], Yvette E. Gelogo[1] and Byungjoo Park[1*]

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

Abstract

Mobile IPv6 is a network-layer solution to node mobility for the IPv6 Internet. It allows a mobile node to maintain a continuous connection from one access point to another. MIPv6 introduces several security vulnerabilities such as the authentication and authorization of Binding Updates (BUs) during the home agent registration process. This paper deals with securing the standard mobile IPv6 handover scheme by adding a cryptography procedure for authenticating the binding updates sent by mobile nodes during the home agent registration process.

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

1. Introduction

MIPv6 is an IP-layer mobility protocol for the IPv6 Internet that is designed to provide mobility support on top of the existing IP infrastructure, without requiring any modifications to routers, applications or stationary hosts. It is designed to manage the movement of mobile nodes (MNs) between wireless IPv6 networks [1, 2]. It provides a seamless connectivity to MNs when they move from one wireless point of attachment to another in a different subnet [3]. MIPv6 notifies the correspondent(s) of an MN about its new location by binding the MN addresses.

The process when a mobile node in MIPv6 moves to a new network is shown on Figure 1. While a mobile node is attached to its home network, it is able to receive packets destined to its home address, and being forwarded by means of conventional IP routing mechanism. When the mobile node moves into a new network (visited or foreign network), its movement is detected and a new association is made with mobility agents (foreign agents) in the new domain [10].

Mobility management is an essential technology for wireless network environments wherein users can freely change their service points while they are connected. Connection maintenance for mobile nodes is not done by modifying Transport layer protocols, but by handling the change of addresses at the Internet layer using Mobile IPv6 messages, options, and processes that ensure the correct delivery of data regardless of the mobile node's location [7].

The integration of mobile cell-phones with Internet-based multimedia services is inevitable. The sheer number of potential users of such services within business, industry and the private sector will force a move to the next generation version of IP (IPv6). Companies and countries in the process of building packet-based network infrastructures to provide these services will

want to invest in IPv6 rather than IPv4. To help pave the way for the standardization of mobile IPv6 (MIPv6), a solution should be found to the problem of handoff-induced packet delay and the impact it has on multimedia Quality-of-Service (QoS).

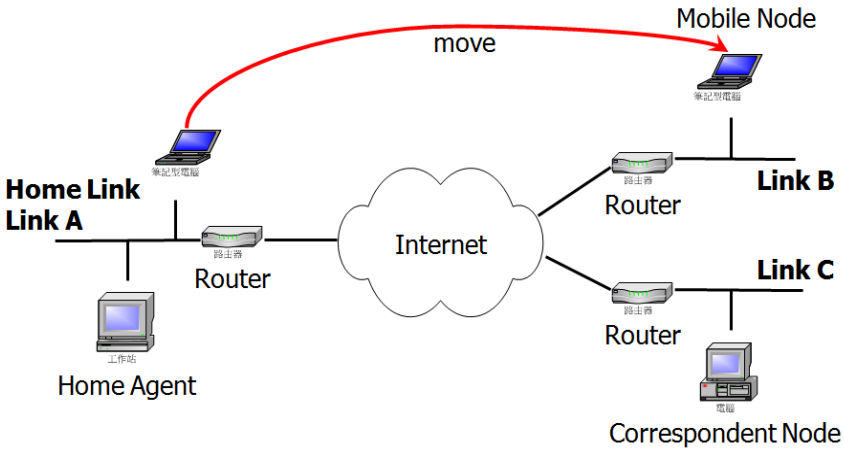

Figure 1. Mobile IPv6 Scenario

This paper deals with securing the authentication of the binding updates (the location information sent by the MN to its correspondents) during the home agent registration in a standard MIPv6 handover procedure. The remainder of this paper is organized as follows; Section 2 explains the basic operations and the standard handover procedure of the MIPv6, Section 3 deals with the proposed security scheme for binding-update authentication protocol, and Section 4 concludes the study.

2. Background

2.1 Standard MIPv6 Protocol

When a mobile node is away from home, it sends information about its current location to the home agent. A node that wants to communicate with a mobile node uses the home address of the mobile node to send packets. The home agent intercepts these packets, and using a table, tunnels the packets to the mobile node's care-of address [2], [3]. Figure 2 shows the basic operations of mobile node communications in MIPv6.

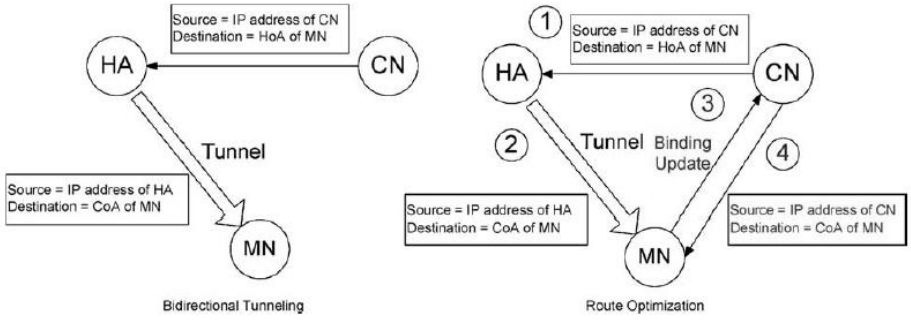

Figure 2. Mobile IPv6 Basic Operations

There are two fundamental modes of communication for a mobile node (MN) and its corresponding nodes (CN), the bidirectional tunneling and the route optimization [4]. In the *bidirectional tunneling mode*, the packets from the CN are routed to the home agent and then tunneled to the MN. Packets to the CN are tunneled from the MN to the home agent (HA) and then routed normally from the home network to the CN.

A router called the home agent (HA) at the home network acts as the mobile's trusted agent and forwards IP packets between the mobile's home network and its current location called the care-of address (CoA). The home agent intercepts packets sent by correspondents to the HoA and forwards them to the CoA over an IPIP tunnel, i.e., encapsulated in another IP packet. When the mobile wants to send packets to a correspondent, it sends them to the home agent over the reverse tunnel. The home agent decapsulates the packets and forwards them to the correspondent.

When the mobile moves to a new location, it tells the home agent its new care-of address by sending a binding update (BU) message. The binding update causes the home agent to update the IPIP tunnel in such a way that the tunneled packets are routed to and from the new CoA. The binding update and the following binding acknowledgement (BA) are authenticated using a preconfigured IPsec security association between the mobile and the home agent.

The *route optimization mode* also uses the binding update and binding acknowledgement messages. When the mobile changes its current address, it sends BUs to its correspondents to notify them about the new location. The binding update contains the mobile's home address and current care-of address. The correspondent acknowledges the binding update and stores the location information in a binding cache, which is effectively a routing table: it tells that packets destined to the HoA should instead be sent to the CoA. The binding needs to be refreshed every few minutes by sending a new BU even if the mobile stays at the same CoA.

Route Optimization provides MN the opportunity to eliminate the inefficient triangle routing and bidirectional MN–HA tunneling. On receiving a tunneled packet from its HA, MN knows that CN that sent the packet is unaware of its current CoA. MN may choose to inform CN its new CoA using a Binding Update (BU) message, thereby allow CN to send subsequent packets directly to MN.

2.2 Standard MIPv6 Handover Scheme

A mobile node (MN) is addressed by two IP addresses in MIPv6, that is, a home address (HoA) and a care-of address (CoA). 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.

The MIPv6 handover procedure scheme wherein the MIPv6 allows the home agent (HA) to work as a stationary proxy for a mobile node (MN) is shown in Figure 3. Whenever the mobile node is away from its home network, the home agent intercepts packets destined to the node, and forwards the packets by tunneling them to the node current address, the care-of-address (CoA). The transport layer (TCP, UDP) uses the home address as a stationary identifier for the mobile node.

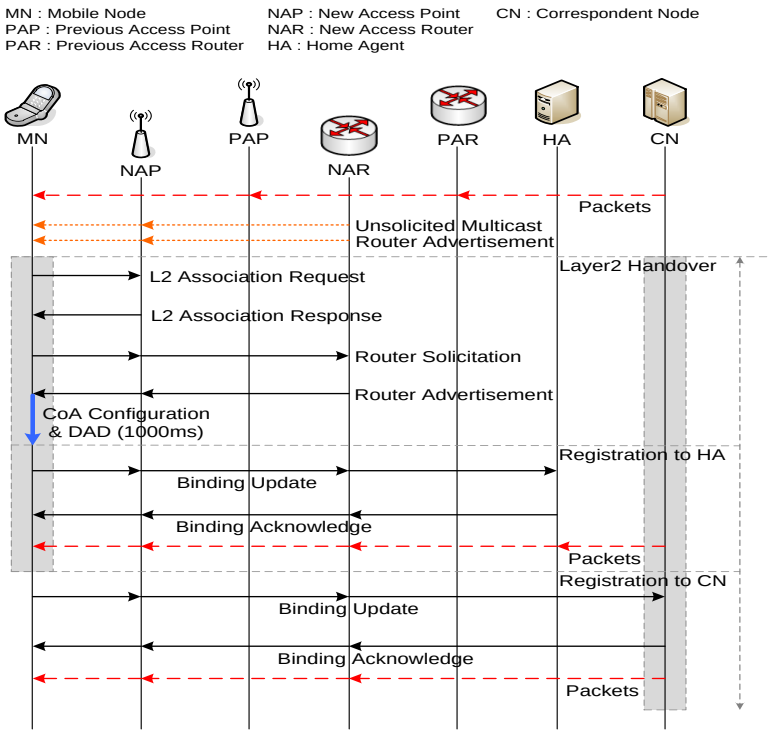

Figure 3. Mobile IPv6 Handover Procedure Scheme

2.3 Binding Update

The binding updates described in the previous section was unauthenticated, thus, an unauthenticated or malicious BU messages can provide intruders an easy means to launch various types of attacks that could create serious security vulnerabilities [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.

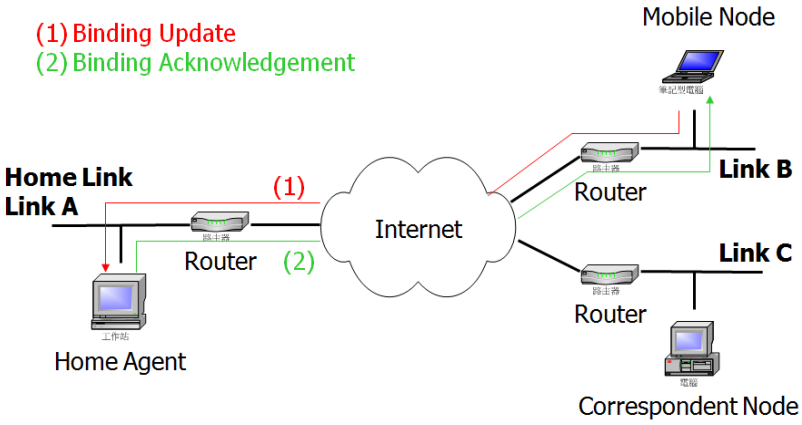

Figure 4. Home Agent Registration needs a Secured Authentication

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 HA [6, 8, 9]. This Proposed scheme is further discussed in the next section.

3. Proposed Secured Standard MIPv6 Handover Scheme

This section defines a new mechanism in mobility message authentication option that can be use to secure Binding Update and Binding Acknowledgement messages in standard mobile IPV6 networks. This mechanism is able to be used along with the IPsec or preferably as a new mechanism to authenticate Mobile node in communication with Home agent or foreign agent to Binding Update and Binding Acknowledgement messages whenever IPsec infrastructure in a network does not exist.

The currently method for securing BUs and other MIPv6 control signals in 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 MIPv6 signaling messages includes the secured authentication of the Binding Updates and Acknowledgement messages used for managing the bindings between a Mobile Node and its Home Agent.

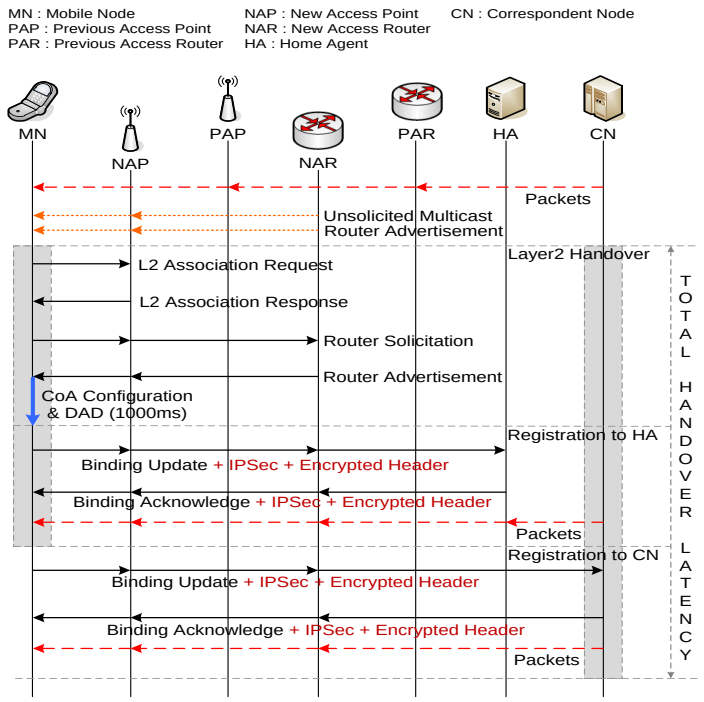

Figure 5. Proposed MIPv6 Handover Scheme implemented with IPsec (mobility message authentication option)

This paper proposes a scheme for securing the Binding Update and Binding Acknowledgment messages between the Mobile Node and Home Agent 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 HA. It enables IPv6 mobility in a host without having to establish an IPsec SA with its Home Agent. A Mobile Node can implement Mobile IPv6 without having to integrate it with the IPsec module, in which case the Binding Update and Binding Acknowledgement messages between the MN and HA 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 MIPv6 signaling messages to prepare a secured communication between MN and CN. The algorithm is able to detect and prevent attackers from eavesdropping and modifying packets intended to specific nodes.

The overall implementation is based on home station, correspondent node and mobile agents. Mobile IPV6 agent finds the advertisement and registers with home agent and foreign agent based on the proposed scheme. The Mobile Node as a personal computer has some specific information that is included in the message authentication option as a file and then encrypts the file. The Home Agent includes this option in the Binding Acknowledge message if it received this option in the corresponding Binding Update and Home Agent has a shared public-key certificate-based mobility security association with the Mobile Node.

4. Conclusion and Future Works

This study defines a secured authentication scheme of Home Agent (HA) registration for standard MIPv6 Handover scheme and used in the standard protocol such as IPSec. This secured authentication scheme is an alternate method for securing MIPv6 signaling messages between Mobile Nodes and Home Agents. It consists of a MIPv6-specific mobility message authentication option that can be added to MIPv6 signaling messages.

The quantitative and qualitative analysis and design of Mobile IPV6 authentication with respect to the IPSec 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 (2011-0026286).

References

[1] D. Johnson, C. Perkins, J. et al., “Mobility Support in IPv6”, IETF RFC 3775, **(2004)** June.

[2] http://ipv6.com

[3] Americas Headquarters: “Implementing Mobile IPv6”, Cisco Systems, Inc., **(2005)** March 28.

[4] K. Ren, W. Lou, K. Zeng, F. Bao, J. Zhou, R. H. Deng, “Routing optimization security in mobile IPv6”, Computer Networks, Elsevier B.V., **(2005)** September 19.

[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, 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, J. 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] Huachun Zhou, Hongke Zhang and Yajuan Qin, An authentication method for proxy mobile IPv6 and performance analysis, Institute of Electronic Information Engineering, Beijing Jiaotong University, **(2008)**.

[10] Vasos Vaassiliou and Zinon Zinonos, An Analysis of the Handover Latency Components in Mobile IPv6, Journal of Internet Engineering, vol. 3, no.1, **(2009)** December.

Authors

Ronnie D. Caytiles

1995-2000 Bachelor of Science in Computer Engineering, – Western Institute of Technology, Iloilo City, Philippines

2008-2010 Master of Science in Computer Science – Central Philippine University, Iloilo City, Philippines

Currently, Integrated Course for M.S. and Ph.D. in Multimedia Engineering, Hannam University, Daejon, Korea.

Research Interests: Mobile Computing, Multimedia Communication, Information Technology Security, Ubiquitous Computing, Control and Automation.

Yvette E. Gelogo

2006~2010 Bachelor of Science in Information Technology, Western Visayas College of Science and Technology, Philippines

Currently, Master of Science in Multimedia Engineering, Hannam University, Daejon, Korea

Research Interests: Mobile Computing, Multimedia Communication, Ubiquitous Healthcare, Ubiquitous Learning, Biometrics, Information Security.

Byungjoo Park

He received the B.S. degree in electronics engineering from Yonsei University, Seoul, Rep. of Korea in 2002, and the M.S. and Ph.D. degrees (first-class honors) in electrical and computer engineering from University of Florida, Gainesville, USA, in 2004 and 2007, respectively. From June 1, 2007 to February 28, 2009, he was a senior researcher with the IP Network Research Department, KT Network Technology Laboratory, Rep. of Korea. Since March 1, 2009, he has been a Professor in the Department of Multimedia Engineering at Hannam University, Daejeon, Korea. He is a member of the IEEE, IEICE, IEEK, KICS, and KIISE. His primary research interests include theory and application of mobile computing, including protocol design and performance analysis in next generation wireless/mobile networks.