# A Robust Secured Mobile IPv6 Mechanism for Multimedia Convergence Services

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

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

***Abstract***

*Mobile IPv6 has been developed to enable mobility in IP networks for mobile terminals. Mobile IPv6 security standardization is still ongoingand security issues are one of the primary considerations that need to be address. In this paper we proposed a mechanism that if will be adopted;MIPv6 will have a better security. This proposed new security mechanism for Mobile IPv6 which to make the RR method more secure is to use IPSec ESP in tunnel mode between the MN and the HA when sending the messages 1(MN to the CN) and 3 (CoA to the CN) and CGA method should be used in parallel with the RR to provide better security. If these messages are also encrypted in addition to authentication, anyone in the foreign network of the MN cannot break the security of the protocol.*

***Keywords:*** *Mobile IPv6, Return Routability Procedure, IPSec, CGA*

## 1. Introduction

Mobile IP (or IP mobility) is an Internet Engineering Task Force (IETF) standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address. The Mobile IP protocol allows location-independent routing of IP datagram on the Internet. Each mobile node is identified by its home address disregarding its current location in the Internet. While away from its home network, a mobile node is associated with a care-of address which identifies its current location and its home address is associated with the local endpoint of a tunnel to its home agent.The transitionto IPv6 is now the obvious solution to a growing problem and this transitionprocess has already begun. And, although Mobile IPv6 has recently beenslowed down in standardization due to security issues, these issues will have tocontinue to get attention, get resolved and integrated into the protocol itself,making every device in tomorrow's Internet, a Mobile IPv6 device, and the MobileInternet, more efficient, robust, and secure. In this paper we discuss first the threats and possible attacks in MIPv6, next is the Mobile IPv6 Security Mechanisms and lastly the proposed mechanism to for more secure MIPv6.

## 2. Mobile IPv6 Security Threats

The security of Mobile IPv6 has been a key issue blocking the standardization of Mobile IPv6. The goal in designing MIPv6 is simply to make IPv6 mobile and at least as secure as MIPv4. However, MIPv6 does introduce several additional security vulnerabilities into IPv6.

The biggest vulnerability, and therefore, the one discussed in this paper, is the authorization of Binding Updates (BUs). As discussed, MIPv6's Route Optimization is built into the IPv6 protocol rather than added as an extension to the protocol as with Mobile IPv4 and it greatly improves the efficiency of routing by eliminating triangle routing. However, Route Optimization also greatly increases the number of Binding Updates sent by a MN to its CNs, and in doing so, it also greatly increases the security risk of MIPv6 Unauthenticated or malicious BUs opens the door for many types of attacks.

### 2.1 False Binding Update Attacks

Spoofed Binding Updates may be sent to home agents and correspondentnodes. As every IPv6 node is expected to be deployed as a MIPv6 node as well,and every MIPv6 node is to be a Correspondent Node (CN), BU security threatscan been seen as applicable to the whole Internet.By spoofing Binding Updates, an attacker can redirect traffic to itself or anothernode and prevent the original node from receiving traffic destined to it. Forexample, let us say nodes A and B have been communicating with each other,then, an attacker, node C, sends a spoofed Binding Update packet to node B,claiming to be node A with a care-of-address of node C. This would cause nodeB to create a binding for node A's CoA and subsequent further traffic to node C,believing it to be node A's new care-of-address. Node A would not receive thedata it was intended to receive, and, if the data in the packets is not protectedcryptographically, node C will be able to see all of node A's sensitive information [3][6].

### 2.2 Man-in-the-Middle Attack

It is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. An attacker may also spoof BUs to two corresponding nodes in order to set itself as a Man-in-the-Middle between a MN and a CN. For example, if node A and node B are communicating, the attacker could send both nodes a spoofed Binding Update with the care-of-address set to its own address. This would cause both nodes A and B to send all packets to node C rather than to each other.

### 2.3 Denial-of-Service Attack

It is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person, or multiple people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. By sending spoofed BUs, an attacker could also send large amounts of unwanted traffic to overwhelm the resources of a single node or that of a network. The attacker could first find a site with streaming video or another heavy data stream and establish a connection with it. Then it could send a BU to the corresponding node, saying to redirect subsequent data traffic to the attacker's new location, that of an arbitrary node. This arbitrary node would be then bombed with a large amount of unnecessary traffic. Similarly, the attacker could also use spoofed BUs to redirect several streams of data to random addresses with the network prefix of a particular target network, thereby congesting an entire network with unwanted data [3].

## 3. Mobile IPv6 Security Mechanisms

Mobile IPv6 provides a number of security features that provide protection against many of the threats posed to Mobile IPv6 as a result of its new features. The Mobile IPv6 security features do not attempt to correct security issues that exist regardless of Mobile IPv6. Many drafts exist that address the various security issues within MIPv6, including 'Security of IPv6 Routing Header and Home Address Options'and 'Privacy Extensions for Stateless Address Auto configuration in IPv6'.

Initially the plan was to use only IPSec Authentication Header (AH) for binding message authentication, without defining and developing any new authentication protocol. This approach encountered many problems and that is why several other methods have also been developed. The current specification defines that IPSec ESP should be used for authentication between MN and HA, and Return Routability (RR) should be used for authentication between MN and CN. The specification makes also possible to use some other, more secure methods than RR for authentication between MN and CN. [4].

### 3.1 IPSec

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. Messages exchanged between the Mobile Node and the Home Agent is protected using IPsec and no new security mechanism exists for this purpose. The use of the mandatory IPSec Authentication Header (AH) and the Encapsulating Security Payload (ESP) and a key management mechanism help to ensure the integrity of the Binding Update messages between the MN and the HA. To prevent the MN from sending a Binding Update for another Mobile Node, the Home Agent must also verify that the Binding Update message contains the correct home address, either as the source of the packet or in an optional field at end of the packet, and the correct security association [1].IPSec can be used to authenticate and encrypt packets at IP level. That is why it was naturally the first proposed method for authentication of the binding messages [4].The biggest problem with the IPSec method is the key distribution. Key distribution of the IPSec, which is called Internet Key Exchange (IKE), uses either pre-sharedsecrets or public keys in the key exchange. After several discussions, IPSec ESP was chosen for binding messageauthentication between MN and HA instead of IPSec AH.

### 3.2 Return Routability Procedure (RRP)

Return Routability (RR) method was developed to provide adequateauthentication between a MN and a CN [4].The basic idea in Mobile IP is to allow a home agent(HA) to work as a stationary proxy for a mobile node (MN). Whenever the mobile node is away from its home network, the HA intercepts packets destined to the node and forwards the packets by tunneling them using IPv6 encapsulation to the node's current CoA.The Return Routability Procedure provides an infrastructure less method for a CN to verify that the MN is reachable at its home and care-of addresses so that Binding Updates sent from the MN to the CN are secure. The procedure involves two steps where tokens are exchanged between the MN and CN. The MN later uses these tokens to provide verification data in its Binding Update message to the CN. The Return Routability Procedure protects against Denial of- Service attacks in which an attacker uses the victim's address as it's care of address, but it does not

defend against attackers that are able to monitor the path between the MN and the CN. First, it ensures that the MN is able toreceive messages with its HoA and CoA, after that it protects the binding messagesbetween the MN and the CN. The MN can receive messages with the HoA only if the MN has created a valid binding to the HA in advance.A CN has a private secret key, $k_{cn}$ and a random number, Nj, which it renews atregular intervals.[4][1].

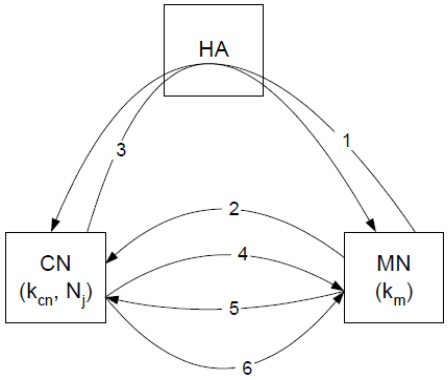


**Figure 1. Return Routability Message Flow**

The first and the second message are sent concurrently by the MN to the CN toinitiate the RR method and they contain only the MN's HoA and CoA respectively. The first message is sent from the HoA and it is sent via a HA by reverse tunnelingthe packet first to the HA and then forwarding it to the CN. The second message issent from the CoA to the CN directly.The third and the fourth messages are sent as responses to the first and thesecond address respectively. They contain the keys K0 and K1, which are used forauthentication of the binding messages, and also the indices of the used randomnumbers and private keys.The fifth message is the binding update message that is sent by the MN to the CN.It is authenticated by using a secret $K_{bu}$, which is calculated with the HMAC SHA1function by using km as a key from the binding message content.The sixth and the seventh messages are optional and they are authenticatedbasically in the same way as the fifth message [4] [1].

### 3.3 Cryptographically Generated Addresses

Cryptographically Generated Addresses is an Internet Protocol Version 6 (IPv6) address that has a host identifier computed from a cryptographic one-way hash function.This procedure is a method for binding a public signature key to an IPv6 address in the Secure Neighbor Discovery Protocol.This method is based on the idea that apart of the IPv6 address is derived somehow from the public key of the node. The length of the IPv6 address is 128 bits. It consists of a 64-bit network prefix anda 64-bit interface identifier. The network prefix is used for routing in the network anda specific node in a link is identified with the interface identifier, which must be ofcourse unique in the link.Theadvantage of this method is that no certificate is needed to convince another nodein the network that the address is used by the owner of the public key that is included in the packet [4].

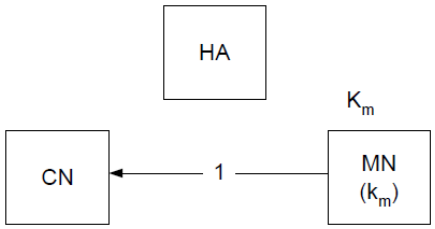


**Figure 2. Binding Update Authentication with CGA**

After receiving this message, a CN can now be certain that the message reallycame from a MN that owns the public key $K_m$ by first verifying that the HoA was really derived from $K_m$. The validity of Km can be checked by forming a CGAaddress from the public key and then comparing the received HoA and the formed address. After that the CN can verify that the MN really sent the message byverifying the signature. The signature can be checked by calculating the hashedvalue and then comparing it to the one that is recovered from the signature by usingthe public key $K_m$[1][5][4].

## 4. ProposedSecurity Mechanisms

With the current status of the Mobile IPv6 Security Mechanisms there are still a lot of security flaws to be address. In this paper we proposed a new security mechanism for Mobile IPv6 to make the RR method more secure, this is to use IPSec ESP in tunnel modebetween the MN and the HA when sending the messages 1(MN to the CN) and 3 (CoA to the CN) and CGAmethod should be used in parallel with the RR to provide better security.If thesemessages are also encrypted in addition to authentication, anyone in the foreignnetwork of the MN cannot break the security of the protocol.The specified RR method provides some level of security for the Mobile IPv6, butthere have been some discussions that this is not enough.Having the security involved in the RRP that uses CGAs makes message spoofing more difficult. It makes very difficult for an attacker to execute a redirection attack, since the attacker must now knowthe public/private key pair that matches the CGA for the MN's home address. This idea does not require additionalprotocol messages but requires some additional processing to replace the regular IPv6 addresses inthe RRP messages with CGAs and additional fields to send the public key and signature.

## 5. Conclusion

Mobile IPv6 specification is still ongoing and security issues are one of the primary considerations that need to be address.After studying the current MIPv6 security mechanism, we proposed the security mechanism that can address the security threats and attacks for mobile IPv6. Having the RR method with IPSec ESP in tunnel mode between the MN and the HA when sending the messages 1(MN to the CN) and 3 (CoA to the CN) and CGAmethod should be used in parallel with the RR plus messages are also encrypted in addition to authentication, it can be a better security for MIPv6.

**Acknowledgments**

This research was supported by Basic Science Research Programthrough the National Research Foundation of Korea(NRF) fundedby the Ministry of Education, Science and Technology(2011-0026286).

## References

[1] Mobile IPv6 SudhaSudanthi GSEC Version 1.4b, SANS Institute InfoSec Reading Room.

[2] Perkins, Charle s E., Johnson, David B. "Route Optimization in Mobile IP". 6 Sept 2001URL:http://www.ietf.org/proceedings/02mar/I-D/draft-ietf-mobileip-optim-11.txt (2 Feb. 2003).

[3] Aura, Thomas. "Mobile IPv6 Security". Microsoft Research. 18 Sept 2002.URL:http://research. microsoft.com/users/tuomaura/MobileIPv6/Mobile-IPv6-Security-18Sep2002.pdf (2Feb. 2003).

[4] TimoKoskiahde, Tampere University of Technology, 8306500, "Security protocols, Security in Mobile IPv6", 18.4.2002

[5] Andre Encarnacao, Greg Bayer, "Mobile IPv6 Binding Update - Return Routability Procedure", March 2008

[6] Martin Ehmke, et al. "Securing Control Signaling in Mobile IPv6 with Identity-Based Encryption", Issues in Informing Science and Information Technology Volume 6, 2009

[7] R Radhakrishnan, et al. "A Robust Return Routability Procedure for Mobile IPv6", IJCSNS International Journal of Computer 234 Science and Network Security, VOL.8 No.5, May 2008

## Authors

**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.

**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.

**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.