Integration of a Cohesive Multimedia Transmission Scheme for Hierarchical Wireless/Mobile Networks

Ronnie D. Caytiles[1] and 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

A number of security issues have been brought by the emergence of mobility that allows devices to move to other networks without losing its connectivity. These security issues have been addressed by deploying different schemes that ensures the network's confidentiality, authenticity, and integrity. This paper deals with securing the hierarchical mobile Internet Protocol version 6 (HMIPv6) handover by the integration of a cohesive security transmission scheme that includes the implementation of digital signature and key agreement algorithms. The digital signature algorithm is used to authenticate mobile nodes or the messages sent by these mobile nodes. The session key agreement algorithm on the other hand is used to provide a shared secret session key for the two communicating parties that can be used for private key algorithms.

Keywords: *HMIPv6, digital signature, key agreement*

1. Introduction

The increasing demand for mobility and connectivity provided by ubiquitous networks has brought a lot of issues with regards to security. Digital contents and resources could be vulnerable to different threats from viruses, hackers, eavesdroppers, and other adversaries in the network environment. The evolution of the IP-based Mobile Network's from IPv4 to IPv6 to HMIPv6 with a predefined Internet Protocol Security (IPSec) was not a mere solution for securing data confidentiality, data integrity, authentication, and nonrepudiation [4].

The Hierarchical Mobile IPv6 (HMIPv6) is designed to reduce the amount of signaling between the mobile node, correspondent nodes, and its home agent for Mobile IPv6 [1, 2]. It introduces a new concept of adding a Mobility Anchor Point (MAP) that acts as a local home agent to Mobile IPv6 (MIPv6). Securing the handshake between the mobile node and the MAP is essentially important to maintain a seamless connection for a mobile node to its correspondent nodes and home agent. IPv6 security features are implemented by extension headers namely: the Authentication Header (AH) and the Encrypted Security Payload (ESP) that both exploit the concept of security association (SA) to agree on the security algorithms

and parameters between the sender and the receiver. The AH header is was designed to ensure authenticity and integrity of IP packets while the ESP header provides data encapsulation with encryption to ensure that only the destination node can access the payload conveyed by the IP packet. However, these security mechanisms are not a complete solution when the applications to be protected are user-oriented instead of network-oriented. The binding updates sent by the mobile node to the Mobile Anchor Point (MAP) needs to be authenticated to prevent an attacker to misinform correspondents about the node's location and, thus, to redirect packets intended for the mobile to a wrong destination which can compromise the confidentiality and integrity as well as can lead to denial-of-service.

This paper deals with securing the HMIPv6 handover by the integration of a cohesive security transmission scheme that includes the implementation of digital signature and key agreement algorithms. The digital signature algorithm is used to authenticate mobile nodes or the messages sent by these mobile nodes. The session key agreement algorithm on the other hand is used to provide a shared secret session key for the two communicating parties that can be used for private key algorithms.

The rest of this paper is organized as follows: Section 2 explains the basic operations and the standard handover procedure of the HMIPv6; Section 3 identifies some related security algorithms; the proposed scheme for integrating the cohesive security transmission scheme is outlined in Section 4; and the concluding remarks in Section 5.

2. The Hierarchical Mobile IPv6

The issue that a lot of signaling messages have to be exchanged between the mobile node (MN) and its home agent (HA) in MIPv6, a new Mobile IPv6 node, called the Mobility Anchor Point (MAP), is introduced and can be located at any level in a hierarchical network of routers, including the Access Router (AR). Every time the mobile node moves in MIPv6, the MN sends a binding update (BU) message to its home agent (HA) and correspondent nodes (CNs). The MAP can limit the amount of Mobile IPv6 signaling outside the local domain [2].

The MAP 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). The 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 auto-configured by the MN when receiving the MAP option. The LCoA on the other hand is an address configured on an MN's interface based on the prefix advertised by its default 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 [2, 3].

Acting as a local HA, the MAP will receive all packets on behalf of the mobile node it is serving and will encapsulate and forward them directly to the mobile node's current address. 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. This makes the mobile node's mobility transparent to correspondent nodes it communicates with.

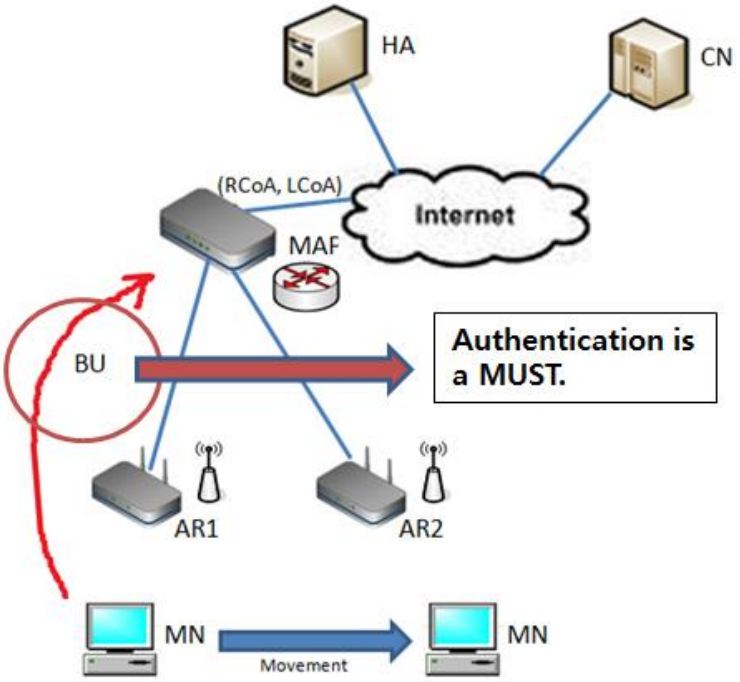

Figure 1. Hierarchical Mobile IPv6 Architecture

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 as shown in Figure 1.

3. Cryptography Schemes

Cryptography is an art of information protection. It is the practice and study of techniques for secure communication in the presence of third parties or adversaries. It is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet. It also refers to the construction and analysis of protocols that overcome the influence of adversaries and which are related

to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation [5].

3.1. Symmetric-key Encryption

In symmetric-key encryption [8], also refers to secret-key encryption, both the sender and receiver share the same key to encrypt and decrypt data as shown in Figure 2. Both the sender and receiver must agree upon the key, keeping it secret between themselves in order for them to communicate. The process is faster, however, the distribution of the shared key can have persistent problems. Sending the key from the sender to receive can easily be intercepted by adversaries resulting to the leak of information that is to be protected.

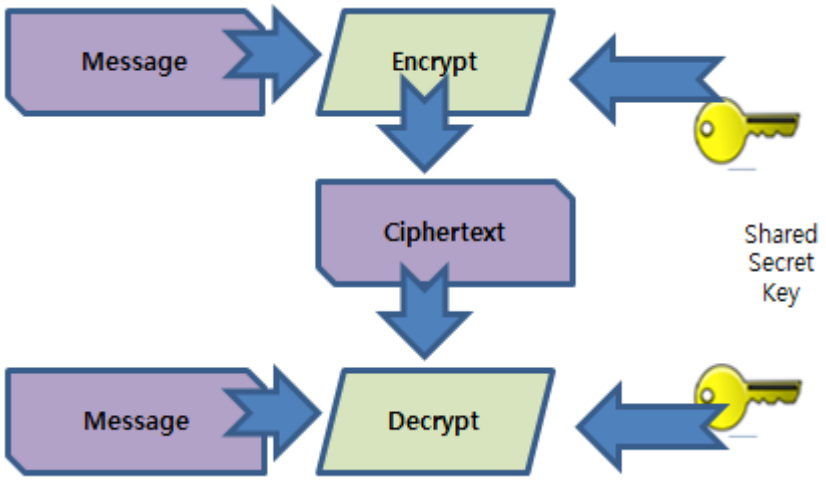

Figure 2. Symmetric-key Encryption

3.2. Public-key Cryptography

Public-key cryptography [7] (Figure 3) refers to an asymmetric scheme that uses two separate keys, one of which is secret – for decryption, and one of which is public – encrypts data. The sender and the received has a private key that is kept secret and the public key is known to everyone. Public-key encryption eliminates the need for the sender and the receiver to share the secret key as indicated by the symmetric-key encryption. The problem with this method is that it is computationally intensive, thus, some systems include the combination of both the symmetric-key and public-key together to speed up the process.

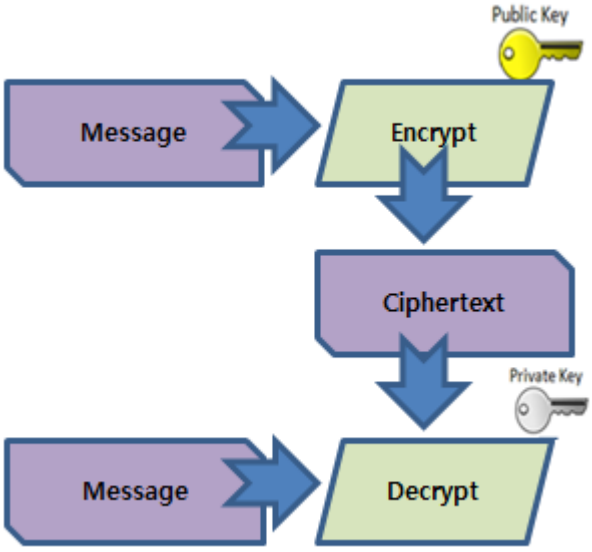

Figure 3. Public-key Encryption

3.3. Digital Signatures

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering [6].

A digital signature scheme typically consists of three algorithms:

- A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
- A signing algorithm that, given a message and a private key, produces a signature.
- A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.

Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party without knowing that party's private key.

4. The Cohesive Security Transmission Scheme

A strong authenticity 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 is a much needed concern to provide confidentiality in the communication between the mobile node and its correspondent nodes. This can be done by employing cryptographic mechanism (both the symmetric-key encryption and public-key encryption) for the Authentication process that can help prevent adversaries from gaining unauthorized and illegal access [9].

Mobile nodes (MN) must secure their passwords as they are requesting access for information or services to recognize the validity of the authentic or true user. To prevent passwords transmitted via communication lines to be sniffed or exposed to adversaries, it will be encrypted before they will be delivered over the network. As authenticated mobile nodes provided their passwords, session keys will then be provided for them in order for them to start the service they requested. Figure 4 shows how session keys are generated and distributed through public-key encryption mechanism. The proposed scheme has to authenticate the session key sent by the Sender with a digital signature using its private key. This signature as it reaches the receiver has to be verified using the sender's public key. That means the sender has a pair of the private key and the public key. As shown from Figure 2, the message that has to be sent is encrypted using the ECC technique into hash or cipher texts then it is signed with a digital signature. Both cipher text and digital signature is sent to the receiving end. Before the receiver can decrypt the message, the digital signature has to be verified to provide for authenticity whether the session key really comes from a valid sender using the sender's public key. After the verification of its authenticity, the cipher text then is decrypted for the receiver, thus, assuring its confidentiality, integrity, and non-repudiation.

The encryption inputs consist of the session key to encrypted, some shared information between the Sender and the Receiver, and some cryptographic technique parameters.

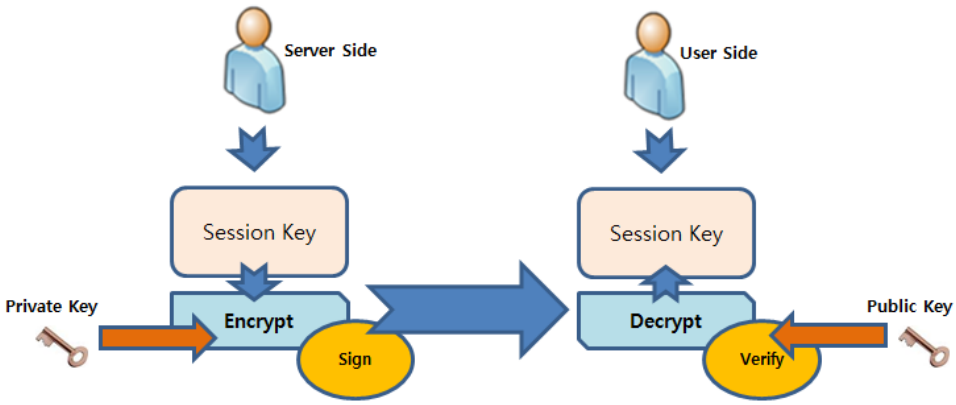

Figure 4. Session Key Generation and Distribution

Session keys will be used by the mobile nodes to request for a particular session (e.g., exchange of packets or messages), the information being processed is encrypted using

symmetric-key encryption with the session key used as its encryption and decrypting key as shown in Figure 5.

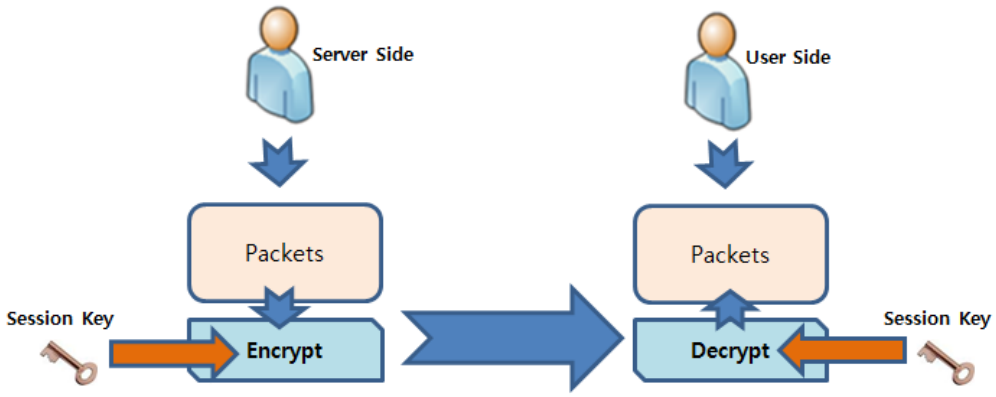

Figure 5. Packet Encryption and Distribution

Since sessions are only validated for authenticated mobile nodes using the session keys, packets and message contents being accessed is encrypted using the symmetric-key mechanism only to prevent the process from slowing down.

5. Conclusion and Future Works

This study has employed both the symmetric-key encryption and public-key encryption for the Authentication process, session key generation and packet transmission for HMIPv6. The integration of a cohesive security transmission scheme includes the implementation of digital signature and session key agreement algorithms. The digital signature algorithm is used to authenticate mobile nodes or the messages sent by these mobile nodes. The session key agreement algorithm on the other hand is used to provide a shared secret session key for the two communicating parties that can be used for private key algorithms.

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).

This paper has been supported by the 2013 Hannam University Research Fund.

References

[1] D. Johnson, C. Perkins, *et al.*, "Mobility Support in IPv6", IETF RFC 3775, June 2004.

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

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

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

[5] http://en.wikipedia.org/wiki/Cryptography.

[6] http://en.wikipedia.org/wiki/Digital_signature.

[7] http://en.wikipedia.org/wiki/Public-key_cryptography.

[8] http://en.wikipedia.org/wiki/Symmetric-key_algorithm.

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