Invited Paper

DOI : 10.3745/JIPS.2009.5.3. 117

Providing Efficient Secured Mobile IPv6 by SAG and Robust Header Compression

Tin-Yu Wu*, Han-Chieh Chao**, *** and Chi-Hsiang Lo**

Abstract: By providing ubiquitous Internet connectivity, wireless networks offer more convenient ways for users to surf the Internet. However, wireless networks encounter more technological challenges than wired networks, such as bandwidth, security problems, and handoff latency. Thus, this paper proposes new technologies to solve these problems. First, a Security Access Gateway (SAG) is proposed to solve the security issue. Originally, mobile terminals were unable to process high security calculations because of their low calculating power. SAG not only offers high calculating power to encrypt the encryption demand of SAG's domain, but also helps mobile terminals to establish a multiple safety tunnel to maintain a secure domain. Second, Robust Header Compression (RoHC) technology is adopted to increase the utilization of bandwidth. Instead of Access Point (AP), Access Gateway (AG) is used to deal with the packet header compression and de-compression from the wireless end. AG's high calculating power is able to reduce the load on AP. In the original architecture, AP has to deal with a large number of demands by header compression/de-compression from mobile terminals. Eventually, wireless networks must offer users "Mobility" and "Roaming". For wireless networks to achieve "Mobility" and "Roaming," we can use Mobile IPv6 (MIPv6) technology. Nevertheless, such technology might cause latency. Furthermore, how the security tunnel and header compression established before the handoff can be used by mobile terminals handoff will be another great challenge. Thus, this paper proposes to solve the problem by using Early Binding Updates (EBU) and Security Access Gateway (SAG) to offer a complete mechanism with low latency, low handoff mechanism calculation, and high security.

Keywords: *SAG, RoHC, MIPv6, Handoff Latency, Early Binding Update*

1. Introduction

Although they offer more convenient ubiquitous ways to access the Internet, wireless networks have some problems that traditional networks do not have, such as limited channel, the low calculating power of mobile terminals, continuously evolving resource-hungry technology, and complex security problems, etc. How to achieve "Mobility" and "Roaming", that the Mobile IPv6 (MIPv6) technology [13] is one of choices. But, the general wireless network can only offer mobile terminal Internet connectivity limited to a fixed number of wireless network signals. Some mechanisms have been proposed to solve these problems, but no mechanism as yet focuses on the roaming which the Mobile IPv6 permits. Therefore, we propose these mechanisms to solve the problems.

First, we concentrate on the security problem. At present, encryption is one of the methods used to solve the security problem. According to most researches, the longer the encryption bits are in the key, the higher the security level obtained. Nevertheless, to process a long-bit encryption key requires higher calculating power. While light and thin mobile terminals cannot produce such high calculating power, the Security Access Gateway (SAG) is effective in solving this problem. In its own area, the SAG can assist each the equipment to own high calculating power, fulfill the need to encrypt, and set up a secure domain. To achieve a high security transmitting method such as P2P, multiple-layered encryption technology is necessary to process two encrypttion mechanisms. From the wired side to the Internet, the SAG uses its high calculating power to establish a long-bit encryption key. From the mobile terminal to the SAG, a short encryption key is used to construct the end-to-end security.

Next, in order to improve the bandwidth utilization of wireless networks, the Robust Header Compression (RoHC) [6] technology is adopted. After the RoHC header compression technology compresses the header, a 1 to 2 bytes Context ID (CID) is produced to replace the original packet header. Compressing the header will enlarge the size of each packet's payload.

Finally, Early Binding Updates [3] are used to combine

Manuscript received March 7, 2009; accepted May 15, 2009.

Corresponding Author: Han-Chieh Chao

* Department of Electrical Engineering, Tamkang University, Taipei, Taiwan (tyw@mail.tku.edu.tw)

** Institute of Computer Science & Information Engineering and Department of Electronic Engineering, National Ilan University, I-Lan, Taiwan (hcc@niu.edu.tw, chlo@niu.edu.tw)

*** Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan (hcc@niu.edu)

Copyright ⓒ 2009 KIPS (ISSN 1976-913X)

Mobile IPv6 technology with wireless networks so that users can reduce handover latency while roaming. During the handover process, the transfer argument is used to reestablish communication in the new domain. Thus, users can continue to use a secure channel and RoHC header compression before the handoff. To lower the handoff latency, a better Early Binding Update (EBU) mechanism and a handoff identification mechanism replace the Return Routability (RR) identification mechanism with the complicated Internet Key Exchange (IKE) [2] and a mechanism with low latency, low handoff calculation, and high security.

The rest of this paper is organized as follows: Section 2 introduces related works; Section 3 describes an efficient architecture with early security key exchange and robust header compression for mobile IPv6; Section 4 shows the simulation results; and Section 5 presents the conclusion and suggestions for future works.

2. Related Works

Several related works are discussed in this section. A brief overview of the Robust Header Compression (RoHC) process is given first, followed by an introduction of the Early Binding Update (EBU). Finally, the Extended Certificate-Based Update (ECBU) protocol is presented.

2.1 Robust Header Compression (RoHC)

The number of mobile devices in use is increasing rapidly. Most users demand more services, with most of the new demands involving multimedia services. The codec used in multimedia services must have a very high compression rate. In each multimedia packet, the payload is compressed into very small sizes ranging from 20 to 160 bytes. As a result, if moving from IPv4 to IPv6, the header size will increase from 40 bytes in IPv4 to 60 bytes in IPv6, and to 80 bytes in IPv6 with encryption encapsulation. In a wired network, this will not cause any serious problems because of the extensive network resources that are currently available. On the contrary, a wireless network has limited resources and variations might occur according to its environmental factors. The increase of the header size will require significant bandwidth, but this will be not acceptable in a wireless network. Therefore, IETF proposed a Robust Header Compression (RoHC) scheme. Fig. 1 shows the operating parameters of RoHC. [7,8]

RoHC is defined in RFC 3095. The main goal of RoHC is to avoid sending redundant information and to be static or dynamic in the header field. In the new version, the source address, destination address and flow label occur in the static header field. The dynamic field can be the sequence number for particular packets with a pattern that can be easily predicted. It is designed to work at high Bit Error Ratio (BER) in a high Round Trip Time (RTT) wireless environment.

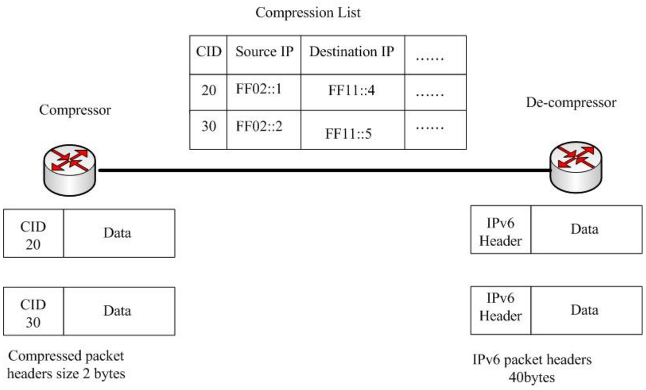

Fig. 1. Header compression operation

2.2 Early Binding Update

RFC 3775 describes the Mobile IPv6 protocol roaming procedure in detail. The mobile terminal has a weakness, namely its latency during the handover, which causes packet loss, latency and out-of-sequence packet delivery. These situations become serious during a long-term handover. Moreover, when the Return Routability precedes Mobile Node (MN), it must wait for both address tests to conclude before it can be registered at a new care of address. Nevertheless, Early Binding Updates can improve these problems. Based on Mobile IPv6 mechanisms, Early Binding Updates presents an optimization rule for the Mobile IPv6 correspondent registration to reduce the latency of both address tests. Throughout the performance evaluation, three phases will be used: the Pre-handover phase, the Critical phase, and the Post-handover phase; and this approach has three phases. Fig. 2 shows that the Early Binding Update uses the

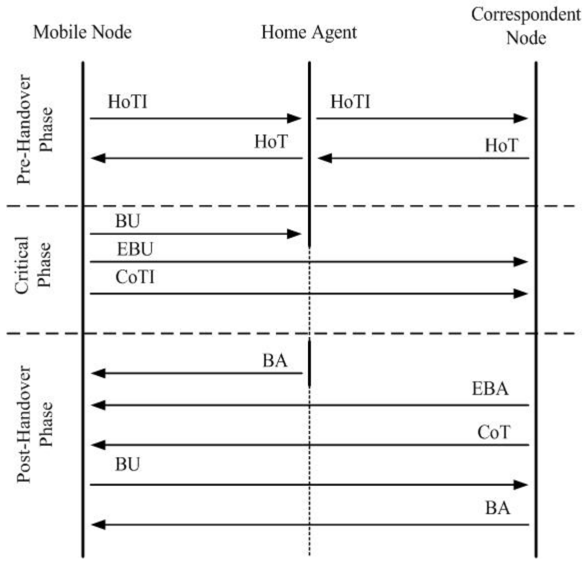

Fig. 2. Early Binding Updates

Pre-handover phases that Pre-procedure Home Keygen Token. Home Keygen Token delivers to the mobile node the legitimate owner of the home address. During the handover, MN needs to send a HoTI and also receive a HoT. Therefore, the carry home-address test lasts through the Pre-handover phase. [10,11]

2.3 Extended Certificate-Based Update Protocol (ECBU)

Mobile IPv6 proposed the Return Routability to process the binding updates. The IETF suggests bundling the Internet Key Exchange (IKE) to improve the authentication ability and to protect the communication channel Mobile Node (MN) through the Home Agent (HA). The Return Routability provides a simple way to protect the binding update signals. However, the Return Routability has some innate defects. For example, all handshake processes use the Dynamic Care of Address (DCoA), whereas IKE needs a fixed IP address as a Security Association (SA) index. The Extended Certificate-Based Update Protocol (ECBU) proposed that one of the home agent's functions to act as the security proxy for its mobile nodes. The authentication is based on the home agent's certificate and the secret session keys are generated by using strong cryptosystems. This can avoid many security obstacles in the Return Routability protocol and provide a simple, integrated and efficient security solution for mobile communications. ECBU is based on a Certificate-based Binding Update (CBU) protocol. Fig. 3 shows that the Extended Certificate-Based binding update (ECBU) protocol can protect all communication channels in mobile IPv6 networks. [12]

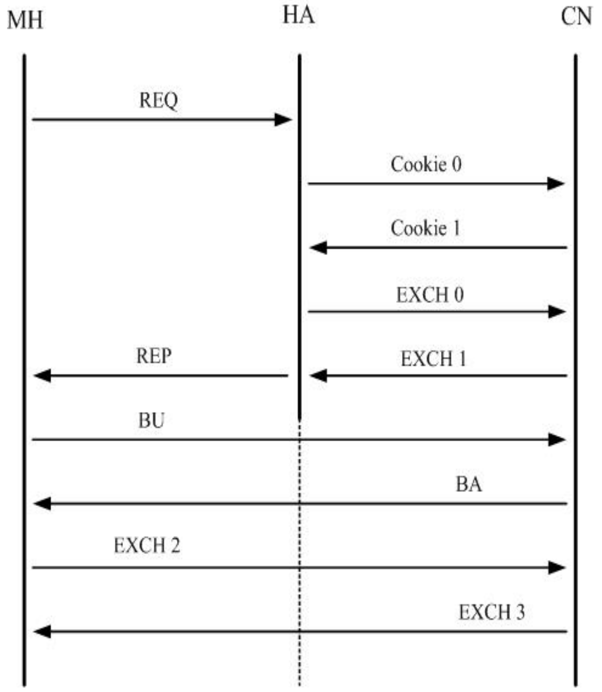

Fig. 3. Extended Certificate-Based Binding Update

3. Efficient Architecture With Early Security Key Exchange and RoHC for MIPv6

The wireless network channel is a valuable resource and cannot offer high bandwidth like a wired network. Therefore, a wireless network poses greater security risks than a wired network. However, adopting RoHC and a security access gateway reduces this problem. The RoHC can compress the packet header in the transmission flow and increase the bandwidth utilization of wireless transmission. In a wireless network, the RoHC mechanism can save about 50% of the bandwidth by using small-sized packets.

In addition, the computing power of the wireless terminal devices cannot compete with fixed servers. Most Internet researches on security have pointed out that in order to achieve high security, a long-bit key must be used to encrypt. The stronger the key encryption process is, the more CPU resources are needed for the encrypted equipment. The primary characteristic of the action terminal is its mobility. To attain such a characteristic, the mobile terminal must be light, thin, short, and small, which results in the problems of low battery power supply and low operational efficiency.

Wireless transmission has not more efficient than wired transmission. If safety is taken into consideration, there will be more problems in using encrypted transmission. This paper propos method could improve these problems. The approach consists of two parts: a wireless network and a hard wired network (backbone networks). As below, we will describe in detail how the SAG improves early key exchange, RoHC with Early Binding Update, and improves security and header compression tunneling.

3.1 Early Security Key Exchange for Encryption in Mobile IPv6 Handoff

According to most researches, the longer the encryption bits in the key are, the higher the security level is. Nevertheless, to process a long-bit encryption key requires higher calculating power. While light and thin mobile terminals cannot produce such high calculating power, the Security Access Gateway (SAG) is effective in solving this problem. Within its area, the SAG can assist each the equipment to own high calculating power, fulfill the need to encrypt, and set up a secure domain. To achieve a high security transmitting method such as P2P, multiple-layered encryption technology is needed to process two encryption mechanisms. From the wired side to the Internet, the SAG with high calculating power establishes a long-bit encryption key. From the mobile terminal to the SAG, a short encryption key is used to construct the end-to-end security.

This paper uses early security key exchange for the encryption function to reduce the latency in the Mobile IPv6 handoff and to protect all traffic channels in the Mobile IPv6 network. Return Routability alone cannot provide a satisfactory level of security. The early security key exchange provides a simple way to protect the binding update signals, but early security key exchange is now used with IKE and IPSec for a higher security requirement. IKE is not suitable for mobile