Invited Paper

DOI : 10.3745/JIPS.2009.5.3. 117

Journal of Information Processing Systems, Vol.5, No.3, September 2009 **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 encryption 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)

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

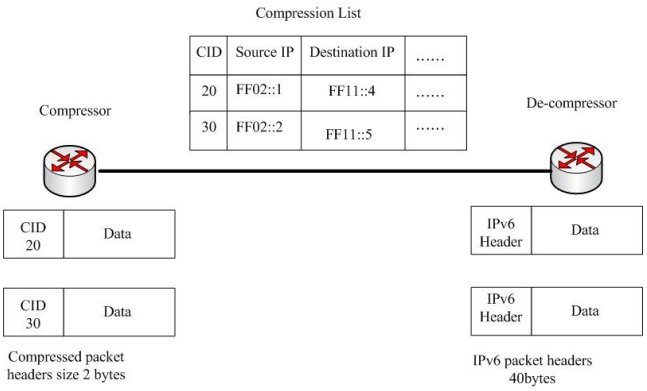

Fig. 1. Header compression operation

predicted. It is designed to work at high Bit Error Ratio (BER) in a high Round Trip Time (RTT) wireless environment.

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

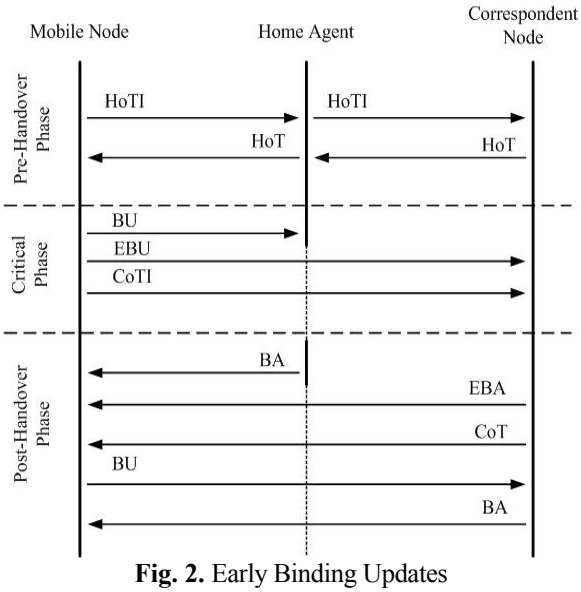

Fig. 2. Early Binding Updates

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]

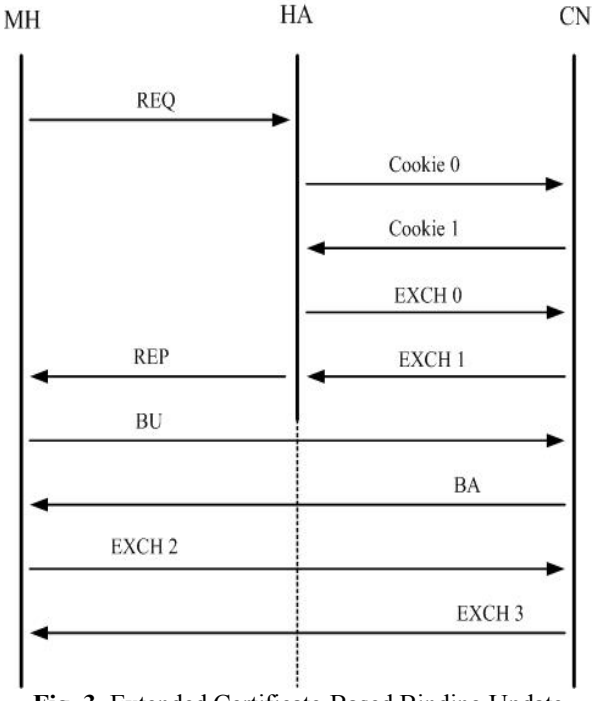

Fig. 3. Extended Certificate-Based Binding Update

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

devices with limited computing power and battery lifetime. On the other hand, the Return Routability function cannot secure the Binding Update (BU) between two mobile nodes.

Next detecting that the MN has moved to a different access network, the mobile node must perform the binding update procedure. An early binding update concept is used to reduce the latency time. At the same time, these two domains are covered between the Security Access Gateway-Mobile Node (SAG-MN) and the Security Access Gateway-Corresponding Node (SAG-CN) to finish the security negotiation. An encryption tunnel is then implemented between the MN and the CN.

A disadvantage of the Return Rountability procedure is that a mobile node must wait for both address tests to conclude before it can register a new care-of address. On the other hand, Return Rountability cannot provide a satisfactory level of security. Based on Mobile IPv6 mechanisms, Early Binding Update can improve these problems and presents an optimization rule to Mobile IPv6 correspondent registrations to reduce the latency of both address tests. Three phases are used throughout the performance evaluation: the pre-handover phase, critical phase, and post-handover phase. As shown in Fig. 4, this approach has three phases.

● Pre-handover phase

When an MN detects that the signal is lower than the threshold and needs to start the route optimization operation with a CN, the MN sends a route optimization request to HA by using IPSec tunneling. In the formula, HA represents the home agents' IP address.

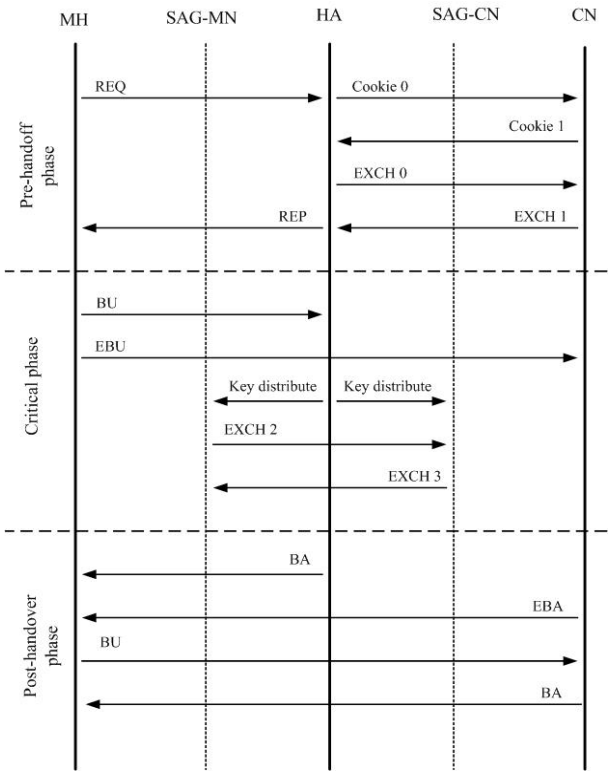

Fig. 4. Early security key exchange in MIPv6 flow chart

$REQ = \{Src=HoA, Des=HA, e(K_{HA}, HoA, CoA, CN, N_0)\}$
K_{HA} : *Session key for the IPSec secure tunnel.*
N_0 : *Random number for counter message replay.*

The HA receives the REQ and verifies that the HoA is from the MN. The HA creates a cookie C_0 to send to the CN. The CN receives the $COOKIE_0$ and creates a nonce N_1 and a cookie C_1, and sends it back to the HA.

$COOKIE_0=\{Src=HoA, Des=CN, C_0\}$
$COOKIE_1=\{Src=CN, Des=HoA, C_0, C_1, N_1\}$

The HA receives the $COOKIE_1$ and replies $EXCH_0$ to the CN. When the CN receives $EXCH_0$, it checks for the equality of the home link subnet prefix strings embedded in both the $Cert_H$ and HoA.

$EXCH_0=\{Src=HoA, Des=CN, C_0, C_1, N_1, N_2, g^x, TS, SIG_H, Cert_H\}$
g^x : *Diffie-Hellman public value.*
$Cert_H$: *Public key certificate of the home link.*
$SIG_H = Sig\ (S_H, HoA\ /CN\ /\ g^x\ /\ N_1\ /\ N_2\ /\ TS\ )$

The CN receives the $EXCH_0$ and CN and sends $EXCH_1$ to the MN. Both parties' MN and CN can identify each other, which will be useful for setting up access control on the MN and CN.

$EXCH_1=\{Src=CN, Des=HoA, C_0, C_1, g^y, SIG_{CN}, Cert_{CN}\}$
$SIG_{CN}=Sig\ (S_{CN}, CN\ /\ HoA\ /\ g^y\ /\ EXCH_0)$
$Cert_{CN}=\{CN, P_{CN}, Valid\_Interval, SIG_{CA}\}$
$REP=\{Src=CN, Des=CoA, Payload\}$
$Payload=e(K_{HA}, N_0, K_{BU}, K_{BA}, K_{EN}, K_{HA\text{-}next})$
$K_{HA\text{-}next}=prf\ (z, N_0\ /\ N_1)$ *{IPSec session key between MN and HA tunnel}*

● Critical Phase

The MN moves to a new area and configures a new CoA also. The mobile node then starts a new CoA for the corresponding registrations to use EBU. The MN sends a binding update message to the HA. At the same time, the MN sends EBA to the CN.

$BU_{MN\text{-}HA}=\{Src=CoA, Des=HA, HA, Seq\#, LT_{BU}, MAC_{BU}\}$
$EBU=\{Src=CoA, Des=CN, HoA, Seq\#, LT_{EBU}, MAC_{EBU}\}$
$MAC_{EBU} = prf\ (K_{EBU}, HoA\ /\ CoA\ /\ Seq\#\ /\ LT_{EBU})$
MAC_{EBU} : *Authenticate the EBU message*
Seq# : *Sequence number*
LT_{EBU} : *Lifetime of the binding*

The HA then distributes keys to the Security Access Gateway-MN (SAG-MN) and the Security Access Gateway-CN (SAG-CN).

$Key_{Distribute}\ (SAG\text{-}MN) = \{Src=HA, Des=SAG\text{-}MN, K_{EN} \mid N'_0\}$

$$Key_{Distribute}(SAG\text{-}CN) = \{Src=HA, Des=SAG\text{-}CN, K_{EN} \mid N'_0\}$$

The CN send packets encrypted with K_{EN} to the MN at the CoA address. The SAG-MN and the SAG-CN can use both messages, $EXCH_2$ and $EXCH_3$, to update K_{EN}. The N'_0 is a nonce generated by the MN that is computed by the SAG-CN.

$$EXCH_2=\{Src=SAG\text{-}MN, Des=SAG\text{-}CN, e(K_{EN}, N'_0)$$
$$EXCH_3=\{Src=SAG\text{-}CN, Des=SAG\text{-}MN, e(K_{EN}, N'_0, K_{EN\text{-}new}, LT_{EN\text{-}new})$$

● Post-handover Phase

In this phase, the MN has communicated its CoA to the CN. The MN then sends a BU to the CN in order to confirm. The HA and CN will then reply with a binding acknowledgement and an early binding acknowledgement message.

$$BA_{HA\text{-}MN}=\{Src=HA, Des=CoA, HA, Seq\#, LT_{BA}, MAC_{BA}\}$$
$$EBA=\{Src=CN, Des=CoA, HoA, Seq\#, LT_{EBA}, LT_{EN}, MAC_{EBA}\}$$
$$MAC_{EBA}=prf(K_{BA}, CoA / CN / Seq\# / LT_{EBA} / LT_{EN})$$

$Seq\#$: *Copy from the EBU message.*

LT_{EBA} : *Lifetime of the binding.*

LT_{EN} : *Lifetime of* K_{EN}.

MAC_{EBA} : *To authenticate the BA message.*

$$BU_{MN\text{-}CN}=\{Src=CoA, Des=CN, HA, Seq\#, LT_{BU}, MAC_{BU}\}$$
$$BA_{CN\text{-}MN}=\{Src=CN, Des=CoA, HA, Seq\#, LT_{BA}, MAC_{BA}\}$$

During the handover, the latency was produced due to $T_{Critical\text{-}phase}$ and $T_{Post\text{-}hanover\ phase}$. As a result, we can figure out that this method can reduce the time taken by the Pre-Handover Phase, $T_{Pre\text{-}Handover\ Phase}$.

$$T_{Pre\text{-}Handover\text{-}Phase} = T_{REQ}+T_{Cookie0}+T_{Cookie1}+T_{EXCH0}+T_{EXCH1}+T_{REP}$$

The proposed method improves the early binding update mechanism. According to [11][12][13], the defined mathematical analysis with handoff latency to MIPv6 is:

$$D_{MIPv6}=t_{L2}+t_{RD}+t_{DAD}+2t_{MN,HA}+t_{RR}+2t_{MN,CN}$$

The $t_{MN,CN}$ is the one-way transmission delay of a message of size s between the MN and the CN.

$$t_{MN,CN}(s)=\frac{1-q}{1+q}\left(\frac{s}{B_{wl}}+L_{wl}\right)+\left(d_{MN,CN}-1\right)\left(\frac{s}{B_w}+L_w+\varpi_q\right)$$

q: *The probability of wireless link failure.*

ϖ_q : *The average queuing delay at each router in the Internet.*

B_ω : *The bandwidth of the wireless link.*

$L_{\omega l}$: *The wireless link delay.*

3.2 RoHC over Mobile IPv6 with EBU [6]

Header compression technology could increase the bandwidth utilization of wireless networks. The RoHC technology in MIPv6 improves the high performance Access Gateway (AG) to deal with a mobile terminal that requests RoHC. RoHC over Mobile IPv6 with EBU can solve these bottlenecks, namely by 1) transferring the Pre-established RoHC parameter from the original node to the new node during the handoff procedure; 2) reducing the latency during handoff; and 3) performing RoHC when many mobile terminals are requesting the same service.

The high performance Access Gateway (AG) can deal with a mobile terminal that requests RoHC. The header compression will be applied during the transmission between the access gateway and the mobile terminals. The compression/de-compression parameters will be stored in the access gateway cache.

In the MIPv6 network environment, during the handoff, the parameters of the compression/de-compression stored in the Old-Access-Gateway will be transferred to the New-Access-Gateway. When the mobile terminal is finished with the handoff procedure, the mobile terminal can start communicating directly with the New-Access-Gateway utilizing the original header compression state and parameters. During the access gateway cache parameter transmission, we use the Extended Early Binding Update (EEBU) to reduce the transfer latency, and the Extended Certificate-Based Update Protocol (ECBU) as the authentication method, as shown in Fig. 5.

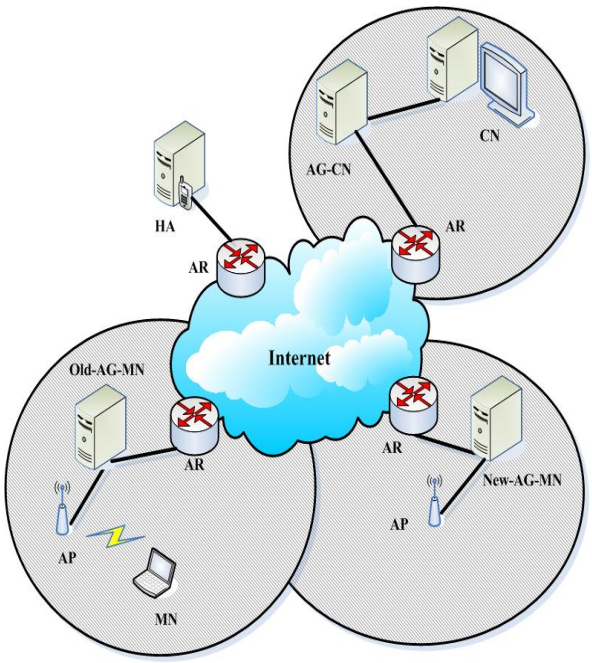

Fig. 5. Transmitting header compression parameter during the handoff

Fig. 6 shows that the mobile node will exchange parameters with Old-AG-MN before transmitting data. The procedure will be IR→CN, ACK, CID only, NACK FO-dynamic, Field→SC, ACK, CID and CID. When the mobile node and Old-SG-MN have finished exchanging parameters, the MN will start to communicate with the acquired Context ID (CID).

When the mobile node is roaming from the Old-Access-Gateway through the New-Access-Gateway with MIPv6, the Early Binding Update mechanism will divide the handoff into three phases: Pre-handoff phase, Critical-phase, and Post-handoff phase. During the Pre-handoff phase, the following procedures will be performed accordingly: *REQ, COOKIE$_0$, COOKIE$_1$, EXCH$_0$, EXCH$_1$* and *REP*. In the Critical-phase, the procedures will be BU, EBU, Context relocation, and CID. Because of the Extended Early Binding Update mechanism, when the MN sends EBU to the Corresponding Node (CN), the MN can start transmitting the compressed header to the New-AG-MN by using the Care-of Address. Finally, during the Post-handover phase, BA, EBA, BU and BA will be performed to finish the handoff procedure.

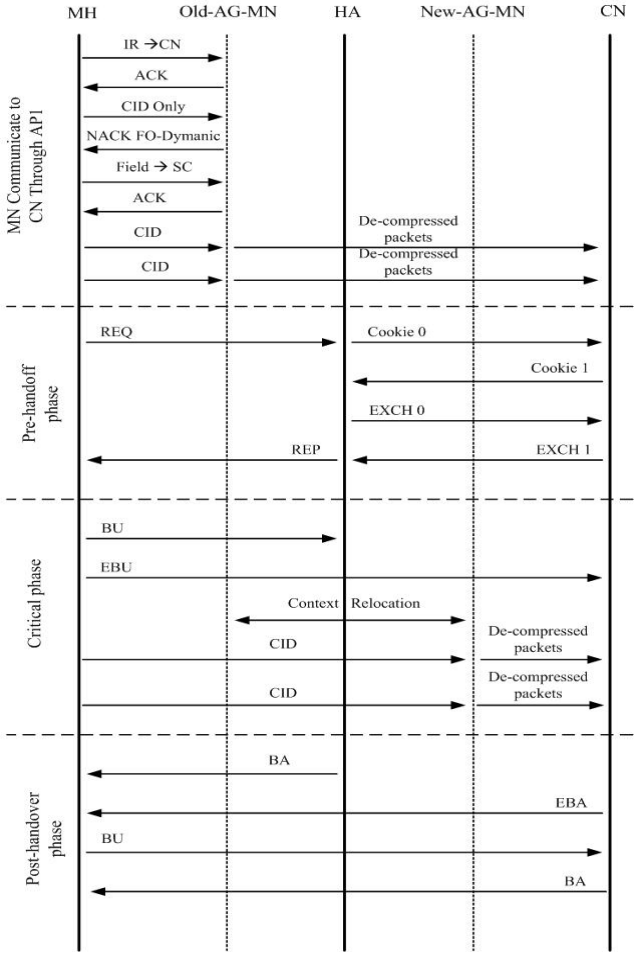

Fig. 6. Context relocation process by RoHC

According to the analysis, the Extended Certificate-Based Update Protocol is adopted to replace the Return Routability mechanism provided by RFC 3775. It is able to reduce the exhausted computation needed by the RR mechanism. Using the Extended Early Binding Update will reduce the time taken by the Pre-handoff phase when sending the EBU during the critical phase. It will be able to use the Context ID parameters with the new CoA. Therefore, the latency will be $T_{Critical\ phase}$.

$$Latency\ time = T_{Critical\ phase} = T_{BU} + T_{EBU} + T_{Context\ Relcoation} + T_{CID}$$

On the other hand, the RoHC can improve the wireless environment performance. The RoHC header compression bandwidth is measured to define the mathematical analysis as [14]:

$$BW = \left[2 + \frac{C \times (1+\beta)}{P+H} + \frac{2 \times (p+\beta H)}{P+H}\right] \times R$$

P, H: The length in bytes of the packet header and packet payload.
C: The size of the compression context.
β : The compression factor.
R: The fixed link rate.

3.3 End-to-End Transmission via SAG to Improve Security and Header Compression Tunnel

RoHC technology is used to set up the compressor and de-compressor devices between the mobile node and the access point to compress and de-compress data. If two nodes want to transfer data between the compressor and the de-compressor, the initial signal must be finished and the two nodes could receive a CID first.

After analyzing, this transmission character is more suitable for huge transmission flows. If a smaller sized packet transmission is more suitable, because small sized packet will get the best transmission effort. However, after analyzing all kinds of network transmission data, we found that most network users transmit data in the network by using more than one type of transmission pattern, such as long-term or high throughput packet transmission patterns, such as FTP and VoIP, or short-term, light packet transmission traffic patterns, like normal website browsing, MSN and SMTP. If we use a header to compress the transmission data, it will not obtain the advantage of header compression because using RoHC header compression to raise the quality of transmission only works with an abundance of data transmitted over a long time. Conversely, if we transmit few data within a short time, the cost will increase due to the initial signal coordination and the related argument storage. Next, wired networks sliding on the Internet will be introduced

and encryption will solve most security concerns. Our observations show that most users' choose not to encrypt all of their data, but encrypt only part of a packet.

High-security encryption data must encrypt longer key bits, and a more robust key encryption process requires more CPU operating power. However, not every terminal can provide high security operating power, especially mobile terminals. To solve this problem, this paper proposes a Security Access Gateway (SAG) with high operating power within the domain Access Router (AR) to encrypt the data moving in and out of the Security Domain (SD). This process is shown in Fig. 7. [10]

The Security Access Gateway (SAG) is also responsible for RoHC header compression. According to the standard, the lay over range of an access point in the wireless network may have many connection requests from many mobile terminals at the same time. If all mobile terminals ask the access point to adopt the RoHC technology to process header compression, the present access point design may not satisfy such requests. Hence, we take the flow to the SAG to encrypt the flow according to the user encryption at the same time. [17,19]

When a mobile terminal connects to the access point and starts to transmit a large number of packets, the RoHC will be used in this traffic stream because the source IP, destination IP and port number of the same stream will be identical. When the transmission flow is transmitted, the MN could initialize RoHC negotiation with the Security Access Gateway (SAG). After acquiring the Context ID (CID), the MN starts to transmit the compressed packets. If the MN needs to encrypt the data during the transmission, it will exchange encryption keys with the SAG located in the Corresponding Node (CN) domain and later establish an encrypted tunnel. The SAG plays two important roles in this mechanism, namely those of (1) the compressor/de-compressor RoHC backbone and (2) the high-speed encryption terminal.

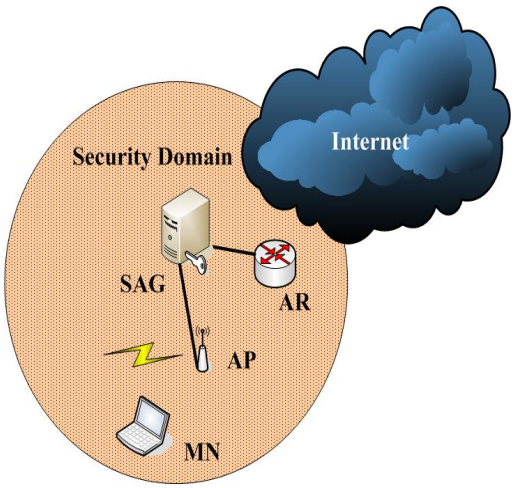

Fig. 7. The SAG set up a security domain

To efficiently use this method, the outward flow of data from the mobile terminal is divided into three kinds of queues: real time, non-real time, and general. The RoHC is only applied to real-time and non-real time queues to increase the compression efficiency. The SAG then encrypts the data according to the mobile terminal request. If the RoHC compresses the encrypted data, the SAG can accelerate the look it up in a table and compute according to the information contained in the CID. This process is shown in Fig. 8.

The method of improving the RoHC mechanism and classifying packets into different queues for process header compression uses M/G/1 delay models to provide the mathematical analysis and assumes that Xn, which symbolizes "n" packets, completes the header compression in time tn. We found the number of packets remaining in the queues. An+1 refers to the number of incoming packets when the n+1 packet waits in the queue. According to Little's law, the average waiting time is:

$$E\left[\widetilde{D}\right]=\frac{4E\left[\widetilde{S}\right]+\lambda\alpha_3^2-3\lambda E^2\left[\widetilde{S}\right]}{2\left(1-\lambda E\left[\widetilde{S}\right]\right)}$$

If one client is in the mobile terminal, the service time for the packets is X by using the following formula.

$$f_R(t)=\frac{1-F_s(t)}{E\left[\widetilde{s}\right]}$$

Then $F(\infty)=1$

$$E\left[R^n\right]=\frac{E\left[\widetilde{S}^{n+1}\right]}{(n+1)E\left[\widetilde{S}\right]}$$

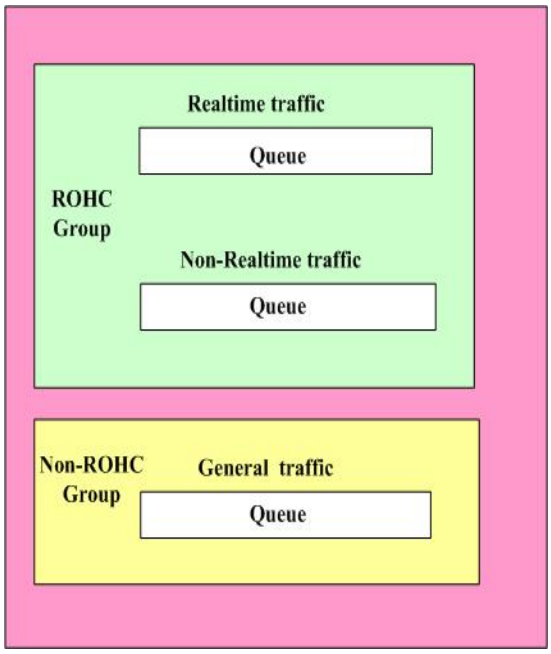

Fig. 8. The mobile terminal has three kinds of queues for the RoHC

In this paper calculate the time function because the system uses a First-come-First-Served (FIFS) mechanism. The following delay time function formula is used.

$$P_L(z) = D(\lambda - \lambda_z) = \frac{a_0 s(\lambda - \lambda_z)(1-z)}{S(\lambda - \lambda_z) - z}$$

$$P_L(z) = D(\lambda - \lambda_z) = \frac{a_0 s(\lambda - \lambda_z)(1-z)}{S(\lambda - \lambda_z) - z}$$

In this approach, two parts are processed: the wireless network part and the Robust Header Compression (RoHC) technology for compressing/de-compressing the packet header. The RoHC transmitting rule can improve the effort of wireless transmission. Therefore, the SAG is a very important rule between the wireless and wired networks. The RoHC and encryption are stored in the SAG. The section uses Early Binding Update to process all parameters from the old SAG to the new SAG. The mobile terminal relies on low latency and according to SAG can to provide high efficiently secure transmissions over Mobile IPv6. Fig. 9 shows the negotiation process during the handover.

The standard RoHC will only compress the header between two nodes. Until now, mainstream researches have focused on the wireless environment not stationary wireless environment. Our research applies the proposed method to a mobile environment such as MIPv6. It develops the RoHC functions and proposes the connection of two mobile terminals through the Internet. Both mobile terminals use RoHC, so we designed an extended RoHC version that will work as a security gateway.

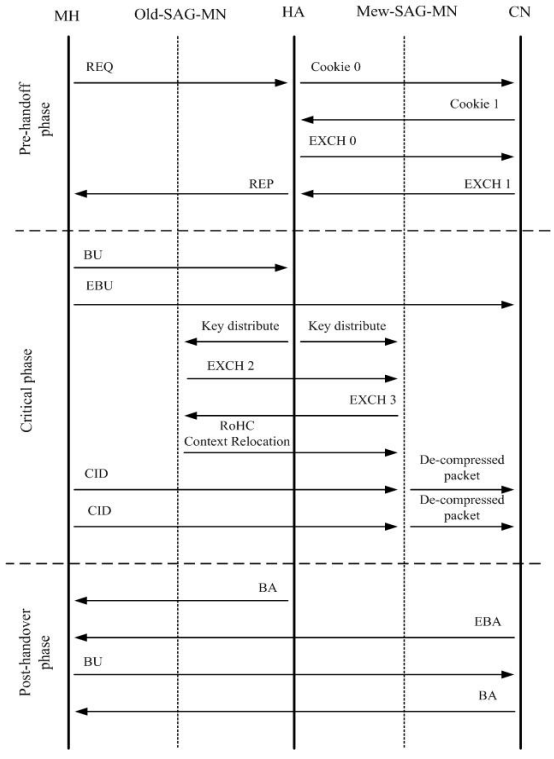

Fig. 9. The negotiation process during handover

The Security Access Gateway (SAG) between both the source and the destination functions as the de-compressor and the compressor. When a mobile node starts with RoHC negotiation, the de-compressor and compressor devices are followed by Context ID (CID) RoHC negotiation at the corresponding node. If CID is not repeated, this CID will be applied and later negotiate the usage of this CID between the SAGs of the two corresponding nodes.

As shown in Fig. 10, when a mobile terminal needs to transmit a significant amount of packets over an extended period of time and the packet flow needs to be encrypted, the negotiation will be performed between (1) MN←→RoHC-MN, (2) RoHC-MN←→RoHC-CN, and (3) RoHC-CN←→CN. As shown in Fig. 11, when the mobile terminal uses RoHC technology to compress the packet and sends it to the SAG of the MN, it will not decompress. The SAG will add another encrypted ESP header to the CID header of the packet and send it to the SAG of the CN. At this time, the SAG of the CN will remove the packet ESP header, decrypt it, and use the CID header to send the packet to the CN.

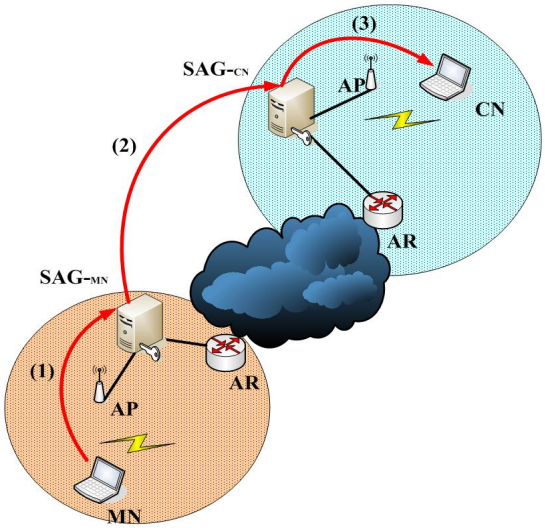

Fig. 10. The two ends are mobile terminals connected by RoHC

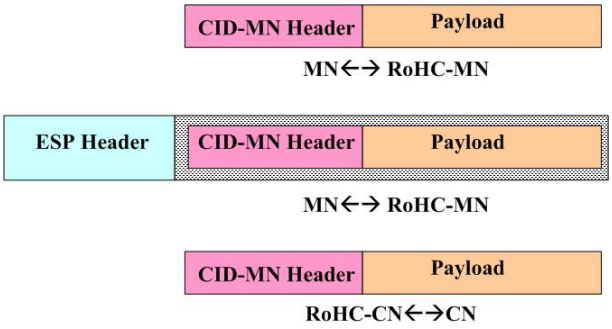

Fig. 11. The CID insert ESP header using the IPSec tunnel mode

4. Simulation Results

The simulation scenes were designed by using OPNET simulation software to verify the proposed method. In session 4.1, we used the SIP protocol to test the RoHC and SAG header compressing mechanisms. The SIP packet size is short with a long transmission time. This simulation can be used to observe the efficiency of the RoHC and SAG mechanisms while transmitting this kind of packet. Session 4.2 used two types of packet protocols: SIP & FTP. SIP is used as the background flow and FTP as the mainstream flow. In session 4.3, the effect of classifying different types of packets into different queues in the mobile terminal was tested.

4.1 Testing RoHC and Encryption Mechanism by VoIP Traffic

Fig. 12 shows the emulation structure. Both the MN and CN are mobile terminals. The AP_MN and AP_CN are access points. The SAG_MN and SAG_CN are two gateways with a security channel established between the two gateways. Both of them perform RoHC header field compression/de-compression procedures between the MN and CN. The MN and CN will use SIP to establish a videoconference and the packets transferred with SIP will be of the UDP type, small in size but with a large amount of packets. The following six scenarios were designed for the simulation.

(1) **Normal**：No RoHC encryption mechanism is used.

(2) **Normal_IPSec**：The data transmitted between the MN and CN will be encrypted with IPSec. The MN and CN will perform de-encryption.

(3) **SAG**：Data will be transmitted between the MN and CN, with both gateway SAG-MN and SAG-CN establishing a secured IPSec channel.

(4) **SAG_RoHC**：The transmission between the MN and CN will be performed with SAG-MN and SAG-CN. All transmitted packets will use RoHC on a secure channel established between SAG-MN and SAG-CN.

(5) **SAG_RoHC_Integrated**：At both ends, the MN and CN will use RoHC to compress the header field. Both gateways, SAG-MN and SAG-CN, will perform header compression/de-compression and also establish a secure IPSec channel. CID encrypts a new packet header between SAG-MN and SAG-CN. The packet is then transmitted to the CN and decompressed. This approach performs header compression only once between both ends.

(6) **SAG_RoHC_Integrated_WEP**：At both ends, the MN and CN will use RoHC to compress the header field. Each end will establish the first encryption with SAG-MN and SAG-CN correspondingly. Between SAG-MN and SAG-CN, it will not perform header compression, but will perform a second encryption by establishing an IPSec Tunnel. There is multi-layer encryption with the packet CID encrypting a new header. Therefore, this approach performs only one header compression between the two ends.

The data encryption effect on transfer throughput is shown in Fig. 12. The result is shown in Fig. 13. The figure shows the wireless network data transfer throughput for ***Normal***, ***Normal_IPsec*** and ***SAG*** between the MN and CN. The transmission throughput from high to low order is ***Normal_IPSec, SAG*** and ***Normal.*** The ***Normal_IPSec*** increase the throughput by encrypted on the MN or the CN. There are no ***SAG*** and ***Normal*** processes, just common data transfer, so the throughput is almost even on both.

Fig. 14 also shows the wireless network data transfer throughput of ***Normal***, ***Normal_IPsec*** and ***SAG*** between the MN and CN, but presents the average result. The order of the throughput from high to low is ***Normal_IPsec***, ***SAG*** and ***Normal***. The effect of using RoHC header compression and SAG encryption in a wireless network measured.

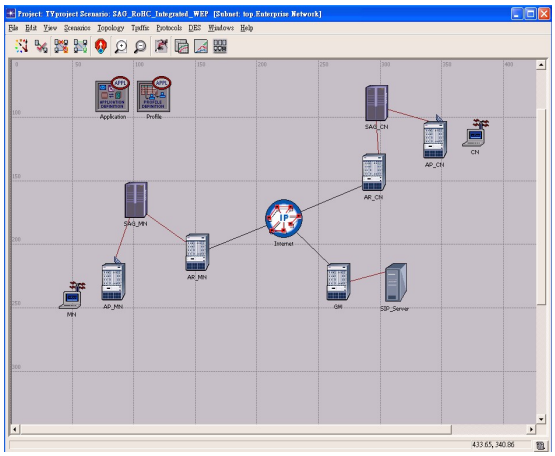

Fig. 12. The topology with RoHC and encryption mechanism testing

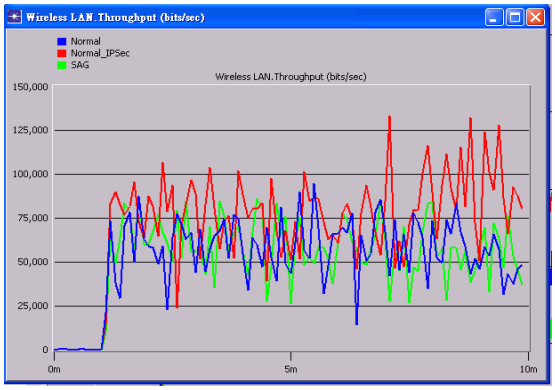

Fig. 13. The data encryption effect on MN and CN are mobile terminals

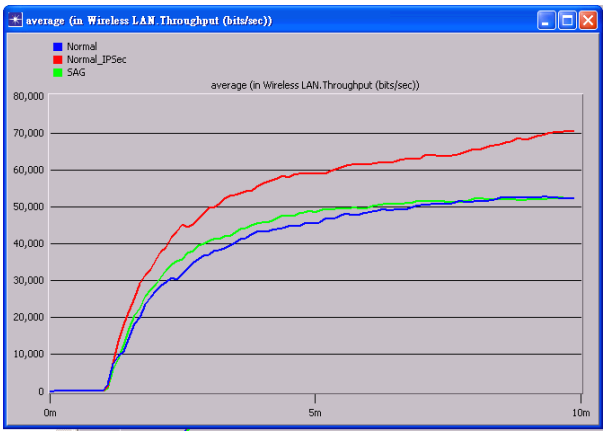

Fig. 14. The data encryption effect (1)

Fig. 15 shows the wireless network data using RoHC header compression and SAG encryption as ***SAG***, ***SAG_RoHC***, ***SAG_RoHC_Integrated*** and ***SAG_RoHC_Integrated_WEP*** between the MN and CN. We can see that the throughput order from high to low is ***SAG, SAG_RoHC, SAG_RoHC_Integrated*** and ***SAG_RoHC_integrated_WEP***.

Fig. 16 shows the end-to-end delay statistics for the MN and CN. As shown in the figure, the length order for the delay time is ***Normal_IPsec***, ***SAG,*** and ***Normal***. ***Normal_IPsec*** shows the highest delay because, between the MN and CN, IPSec encryption is used between the MN and CN. This encryption was processed by using a mobile terminal. Both the MN and CN are mobile terminals. The mobile terminal has low processing ability and needs more time to process encryption, so its delay is the longest. The delay times of ***SAG*** and ***Normal*** are almost even. SAG Gateway is a server with high processing power, so its encryption time is shorter.

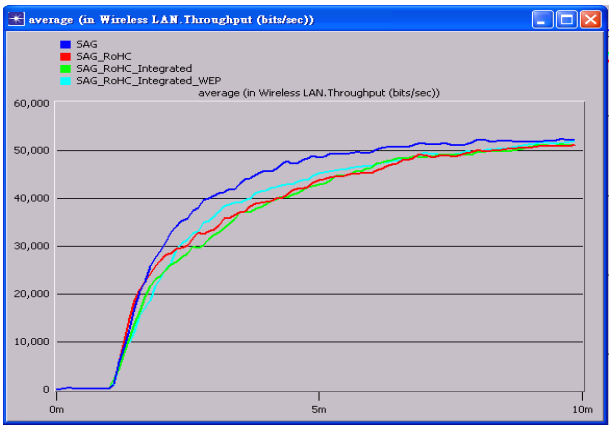

Fig. 15. The data encryption effect (2)

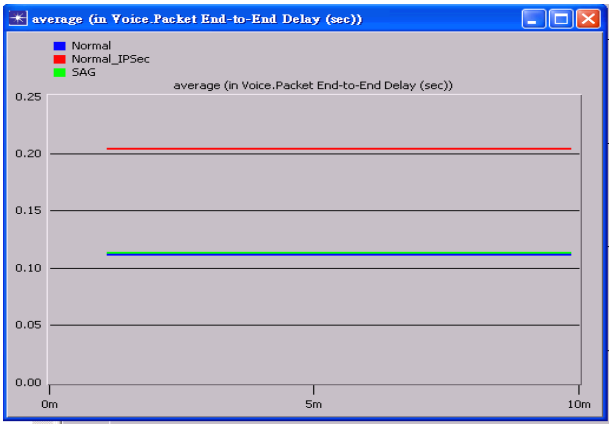

Fig. 16. The effect of both MN and CN end-to-end average delay time

Fig. 17 shows the end-to-end data transfer delay time, from long to short order as ***SAG_RoHC***, ***SAG***, ***SAG_RoHC_Integrated_WEP*** and ***SAG_RoHC_Integrated***. In ***SAG_RoHC***, SAG Gateway encryption and two RoHC header compression /de-compression processes are required. There will be more processing time and delay. In the ***SAG_RoHC_Integrated_WEP*** delay, the mobile terminal handles header compression/de-compression and multiple- layer two-part encryptions. Because the header compression/de-compression is only processed once, the delay is shorter than that of ***SAG_RoHC***. The ***SAG_RoHC_Integrated*** encryption processed in the wireless part is not required. The header compression/ de-compression is only performed once, so the delay is short.

Fig. 18 shows the CPU utilization statistics for the SAG

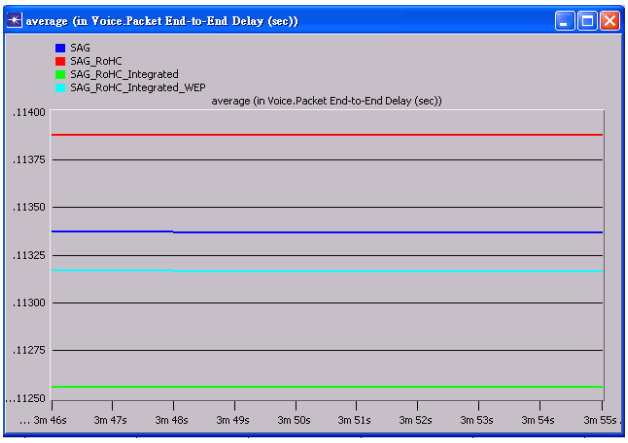

Fig. 17. The end-to-end average delay time

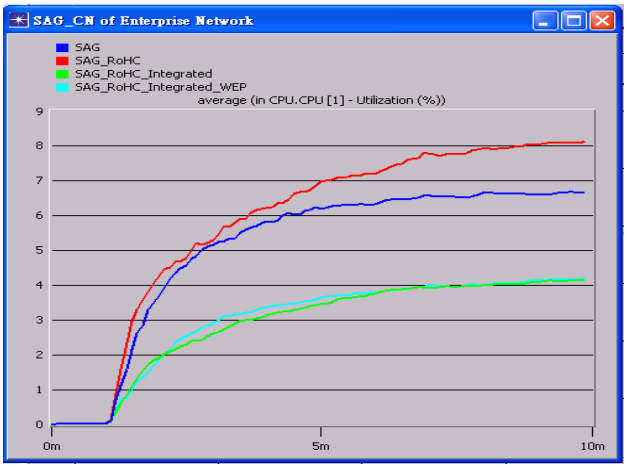

Fig. 18. The average CPU utilization statistics

gateway. The CPU utilization placed from the highest to the lowest is ***AG_RoHC***, ***SAG***, ***SAG_RoHC_Integrated*** and ***SAG_RoHC_Integrated_WEP***. In ***SAG_RoHC***, when the SAG gateway needs to perform encryption and process the header compression/decompression at the same time, the CPU utilization is the highest. In the two scenarios ***SAG_RoHC_Inegrated*** and ***SAG_RoHC_Integrated_WEP***, the SAG gateway is used to perform WEP, but not RoHC header compression, which lowers the CPU utilization.

4.2 Testing RoHC and Encryption Mechanism by using both VoIP and FTP Traffic

Fig. 19 is the simulation structure. In the simulation structure, both MN1 and CN1 are mobile terminals and transmit SIP traffic. CN2 is the sending node that transmits the FTP protocol. MN2 is the receiving node. The SAG_MN and SAG_CN are two gateways with a security channel established between the two gateways. For the simulation, we have designed six scenarios ***Normal, Normal_IPSec, SAG, SAG_RoHC, SAG_RoHC_ Integrated and SAG_RoHC_ Integrated_WEP***.

The result is shown in Fig. 20. The figure shows wireless network data transfer throughput of ***Normal***, ***Normal_IPsec*** and ***SAG*** between MN and CN. The throughput includes both SIP and FTP traffic. The SIP transmits traffic for a longer time. The FTP transmits for a shorter time. The test traffic use SIP and FTP that to compare effect on both SIP and FTP with different transmission types. The transfer time from high to low order is ***Normal_IPSec, Normal and SAG.*** The ***Normal_IPSec*** encrypted on MN or CN and need more processing time than ***SAG*** and ***Normal*** to transmit FTP files.

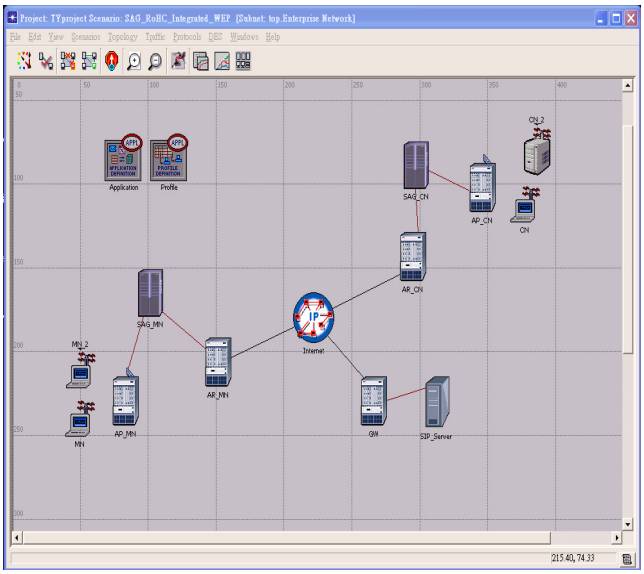

Fig. 19. Testing RoHC and encryption mechanism by VoIP and FTP traffic

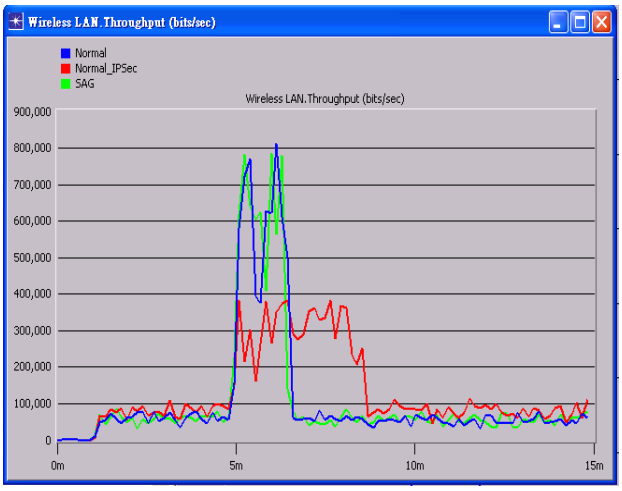

Fig. 20. The FTP throughput effect when MN and CN are mobile terminals

Fig. 21 also shows the FTP data transfer throughput of ***Normal***, ***Normal_IPsec*** and ***SAG*** between MN and CN, but only presents the average. The order of the transfer time from high to low is ***Normal_IPsec***, ***SAG*** and ***Normal***. Fig. 22 shows the statistic of voice end-to-end delay. According to the figure the order of delay time length is ***Normal_IPsec***, ***SAG***, and ***Normal***. ***Normal_IPsec*** features the highest delay. This encryption was processed by using a mobile terminal with low processing ability; thus, more time for encryption is needed and its delay is the longest. The delay time for ***SAG*** and ***Normal*** is almost even. As a server with high processing power server, the encryption time of SAG gateway is shorter.

Fig. 23 shows the results of the end-to-end data transfer delay time, from long to short as ***SAG_RoHC***, ***SAG***, ***SAG_RoHC_Integrated_WEP*** and ***SAG_RoHC_Integrated.*** The mobile terminal handles header compression/de-compression and multiple-layer two-part encryption because the header compression/de-compression only occurs once. The delay

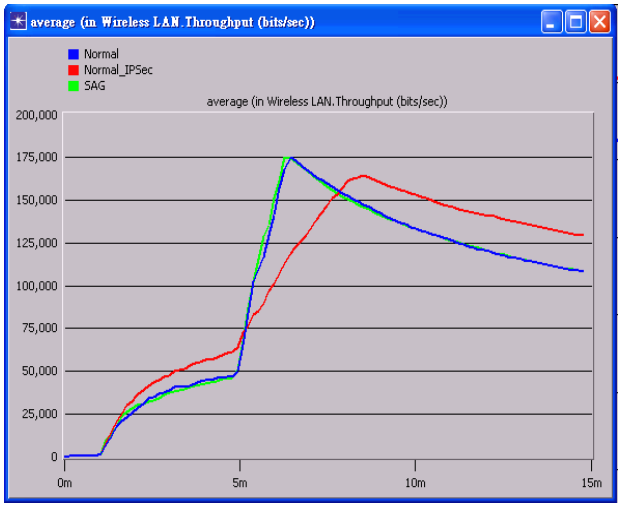

Fig. 21. The average effect of FTP and SIP throughput

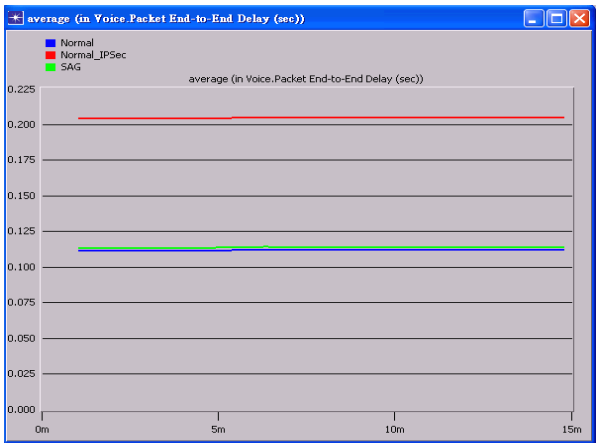

Fig. 22. The average delay time end-to-end voice

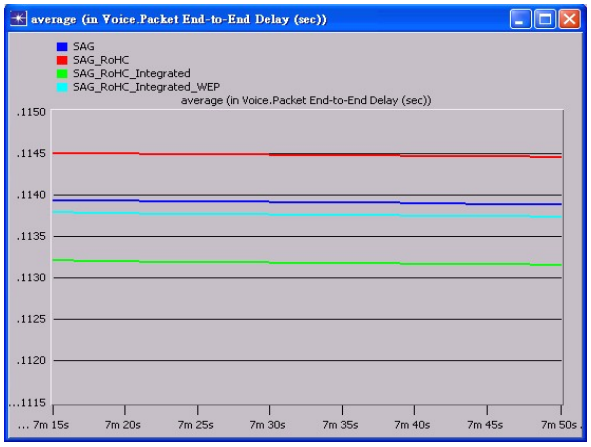

Fig. 23. The average voice end-to-end time delay

is shorter than that for ***SAG_RoHC***. For ***SAG_RoHC_Integrated***, the encryption in the wireless part is not required and the header compression/de-compression only occurs once, which shortens the delay.

Fig. 24 shows the CPU utilization statistics for the SAG gateway. The CPU utilization, placed in the order of highest to lowest, is ***SAG_RoHC***, ***SAG***, ***SAG_RoHC_Integrated*** and ***SAG_RoHC_Integrated_WEP***. In the ***SAG_RoHC*** scenario, the SAG gateway performs the encryption and the header compression/decompression at the same time; thus, the CPU utilization is the highest. The two scenarios ***SAG_RoHC_Inegrated*** and ***SAG_RoHC_Integrated_WEP*** use the SAG gateway to perform the encryption, but not the RoHC header compression process, so the CPU utilization is lower.

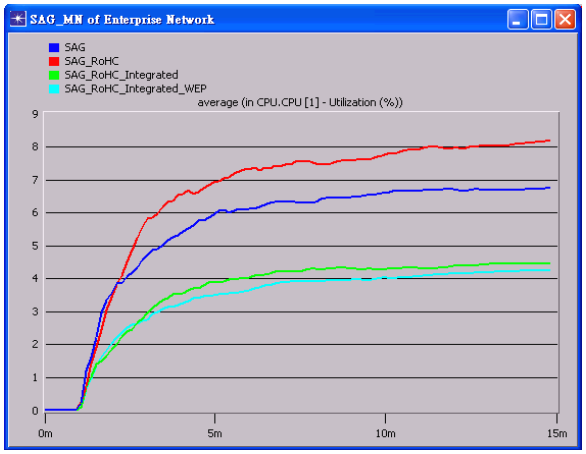

Fig. 24. The average FTP and SIP throughput effect for CPU utilization statistics

4.3 Classifying Different Types of Packets to Different Queues

We found that most users usually use the same type of network services, but that not all traffic flow types are suitable for the RoHC mechanism. Therefore, this paper classifies the inflow data in the mobile terminal to sort and store the data in different queues to be processed later.

During the experiment, the traffic flow is divided into three types: real time, non-real time, and general. For real-time data, the queues are stored with real-time data and long-term packets like VoIP. These small-sized packets need a long time to be processed and display very good performance. For non-real-time data, the queues need a long time for transmission, like the FTP protocol. These middle-sized packets need a long transmission time because they are non-real time. Therefore, the transmission priority is the lowest. For the general type, the queue stores few packets during a short period of time because these services have low traffic flow and are not suitable for RoHC use.

Fig. 25 shows that we use different sizes of packets to compare the header compression rate. In this scenario, we define the packet sizes as 64bytes, 128bytes, 256bytes, 512bytes and 1024bytes for classification into three kinds of queues.

In Fig. 26, we compare the RoHC performance with packet sizes of 64bytes, 128bytes, 256bytes, 512bytes and 1024bytes. During a short time period spent transmitting small-sized data packets, the processing time will increase due to the time wasted during the RoHC initialization and compression. From Fig. 27, by comparing the general queues with and without RoHC, it is obvious that the processing time without using RoHC is shorter.

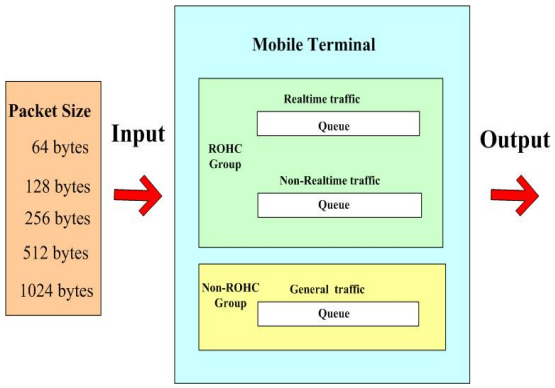

Fig. 25. Packet types classified into different queues in mobile terminals

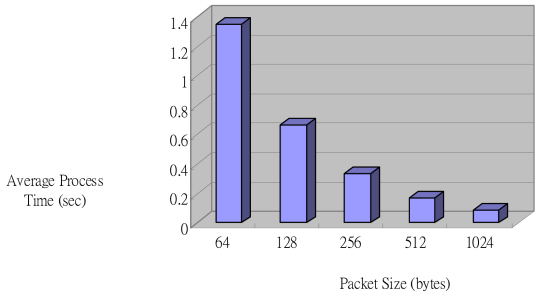

Fig. 26. The RoHC performance for each packet size

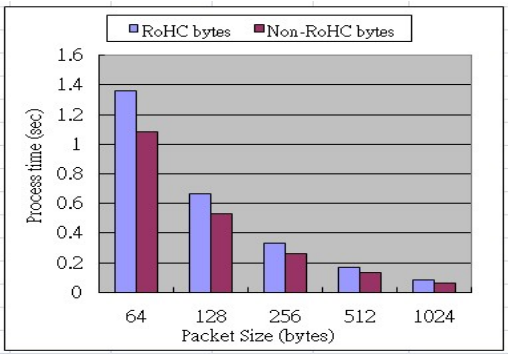

Fig. 27. Comparing RoHC and Non-RoHC processing times

5. Conclusions

This paper proposed a Security Access Gateway (SAG) mechanism to complete two missions: (1) The SAG is responsible for the encryption process between the wired terminal and the Internet to offer high security encryption. (2) The SAG is responsible for the packet header compression/ de-compression of the mobile terminal wireless edge. The advantages of the SAG mechanism are as follows: (1) The SAG offers transmitted data encryption by calculating a long-bit encryption key to establish a secure tunnel between the Mobile Node (MN) and the Corresponding Node (CN). (2) The SAG can fulfill the requests from all MN header compressions for the wireless terminal under the same wireless network signals. (3) While the MN and CN nodes transmit data, both use Robust Header Compression (RoHC) technology to compress the header to save bandwidth. The SAG helps the the MN and CN to establish the end-to-end security tunnel. Compared to the original RoHC procedure, SAG With RoHC can process packet compression/de-compression together. To achieve the abovementioned advantages, the SAG must cope with RoHC and encryption at the same time. Before being transmitted, the arguments the procedures use will be coordinated by the SAG and saved in the cache memory. Therefore, when the mobile terminal starts to handoff, the Early Binding Update (EBU) technology is used to transfer the arguments in the old SAG cache into the new SAG cache. Once mobile terminal handoff has been completed, the Mobile terminal continues to transmit data by using header compression and encryption before the handoff. While transferring the arguments in the cache, the Mobile terminal does not follow the Return Routability (RR) identification mechanism identified by RFC 3775 because the Internet Key Exchange (IKE) mechanism used in this mechanism needs greater calculating power and is not suitable for mobile terminals. Thus, using an identification method with low calculating power for security identification during the handoff is necessary.

References

[1] Brower E., Ertekin E., Christou C.A., O'Keefe S., "The Application of Header Compression to IPsec Encrypted Networks", Military Communications Conference, 2005. MILCOM 2005. Vol. 5, pp. 2844-2850, IEEE 17-20 Oct. 2005.

[2] Chen Zhuo, Chen Xiao-Wei, Zhang Zheng-Wen, Yang Mu-Xiang, "The Improving of IKE in WLAN", Wireless Communications, Networking and Mobile Computing 2005. Proceedings. 2005 International Conference, Vol. 2, 23-26, pp. 1128-1131, Sept. 2005.

[3] Christian Vogt, Roland Bless, Mark Doll, Tobias Kuefner, "Early Binding Updates for Mobile IPv6", Wireless Communications and Networking Conference, 2005 IEEE, Vol. 3, 13-17, pp. 1440-1445, Mar. 2005.

[4] C. Vogt, J. Arkko, R. Bless, M. Doll, and T. Kuefner., "Early Binding Updates for Mobile IPv6", Internet Draft draft-vogt-mip6-early-binding-updates, Feb. 2004.

[5] C. Vogt, J. Arkko, R. bless, M. Doll, and T. Kuefner., "Credit-Based Authorization for Mobile IPv6 Early Binding Updates", Internet Draft draft-ietf-send-cga, May. 2004.

[6] C. Bormann, C, Burmeister, M. Degermark, "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed", RFC 3095, July. 2001.

[7] Changwen Liu, Soliman, H., "Local Key Exchange for Mobile IPv6 Local Binding Security Association", Vehicular Technology Conference, 2004. VTC 2004-Spring. 2004 IEEE 59th, Vol. 5, 17-19, pp. 2647-2655, May. 2004.

[8] Chin-Fu Kuo, Chi-Ying Chen, Chi-Sheng Shih, Tei-Wei Kuo, "Threat-Based Configuration Architecture for Security Gateways", Networks, 2006. ICON '06. 14th IEEE International Conference, Vol. 1, pp. 1-6, Sept. 2006.

[9] Chih-Mou Shih, Shang-Juh Kao, "Security Gateway for Accessing IPv6 WLAN", Computer and Information Science, 2006. ICIS-COMSAR 2006. 5th IEEE/ACIS International Conference, pp. 83-88, July. 10-12, 2006.

[10] C. Bormann, "Robust Header Compression (ROHC) over PPP" RFC 3241, Apr. 2002.

[11] D. Taylor, A. Herkersdorf, A. Doring, G. Dittmann,

"Robust Header Compression (RoHC) in Next-Generation Network Processors", IEEE/ACM Transactions on Networking, Vol. 13, NO. 4, Aug. 2005.
[12] D. Harkins and D. Carrel, "The Internet Key Exchange Protocol", IETF RFC 2409, 1998.
[13] D. Johnson, C. E. Perkins, and J. Arkko., "Mobility Support in IPv6", RFC 3775, June. 2004.
[14] E. Ertekin, C. Christou, B. Allen Hamilton, "Internet Protocol Header Compression, Robust Header Compression, and Their Applicability in the Global Information Grid", IEEE Communication Magazine, Nov. 2004.
[15] E. Martinez, A. Minaburo, L. Toutain, "RoHC for Multicast Distribution Services", IEEE International Symposium on Personal, Indoor and Mobile Radio Communication, 2005.
[16] Eltoweissy, M., Moharrum, M., Mukkamala, R., "Dynamic key management in sensor networks", Communications Magazine, IEEE, Vol. 44, Issue 4, pp. 122-130, Apr. 2006.
[17] G. O'Shea and M. Roe, "Child-Proof Authentication for MIPv6 (CAM)", SIGCOMM Comput. Commun. Rev., Vol. 31, NO. 2, pp. 4-8, 2001.
[18] J. Vilhuber, "IP Header Compression in IPSec ES", Internet draft, draft-vilhuber-hcoesp-01.txt, July. 2004.
[19] R. Deng, J. Zhou, and F. Bao, "Defending against Redirect Attacks in Mobile IP", Proceedings of the 9th ACM Conference on Computer and Communications Security, ACM Press, pp. 59-67, Washington, DC, Nov. 2002.
[20] Tin-Yu Wu, Chi-Hsiang Lo and Han-Chieh Chao, "Early Security Key Exchange for Encryption in Mobile IPv6 Handoff", Security and Communication Networks, Volume 1 Issue 6, pp. 511–520, October. 2008.

Tin-Yu Wu
Tin-Yu Wu currently works as an Assistant Professor in the Department of Electrical Engineering, Tamkang University, Taipei, Taiwan. He received his M.S., and Ph.D. degrees in the Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan in 2000 and 2007 respectively. His research interests focus on the next-generation Internet protocol, mobile computing and wireless networks.

Han-Chieh Chao
Han-Chieh Chao is a jointly appointed Full Professor of the Department of Electronic Engineering and the Institute of Computer Science & Information Engineering, National Ilan University (NIU), I-Lan, Taiwan. He also serves as the Dean of the College of Electrical Engineering & Computer Science for NIU and as the Director of the Computer Center for the Ministry of Education. Currently he holds the joint professorship of the Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan and the honorary adjunct professorship of Beijing Jiaotong University, China. His research interests include High-Speed Networks, Wireless Networks, IPv6- based Networks, Digital Creative Arts and the Digital Divide. He received his MS and Ph.D. degrees in Electrical Engineering from Purdue University in 1989 and 1993 respectively. He has authored or co-authored 4 books and has published about 240 refereed professional research papers. He has completed 80 MSEE and 2 PhD thesis students. Dr. Chao has received many research awards, including Purdue University SRC awards, and NSC research awards (National Science Council of Taiwan). He also received many funded research grants from the NSC, Ministry of Education (MOE), RDEC, Industrial Technology of Research Institute, Institute of Information Industry and the FarEasTone Telecommunications Lab. Dr. Chao has been invited frequently to give talks at national and international conferences and research organizations. Dr. Chao is also serving as an IPv6 Steering Committee member and co-chair of the R&D division of the NICI (National Information and Communication Initiative, a ministry level government agency which aims to integrate the domestic IT and Telecom projects of Taiwan), as Co-chair of the Technical Area for IPv6 Forum Taiwan, as the executive editor of the Journal of Internet Technology and as the Editor-in-Chief for the International Journal of Internet Protocol Technology and the International Journal of Ad Hoc and Ubiquitous Computing. Dr. Chao has also served as the guest editor for Mobile Networking and Applications (ACM MONET), IEEE JSAC, IEEE Communications Magazine, Computer Communications, IEE Proceedings Communications, Telecommunication Systems, Wireless Personal Communications, Computer Journal and Wireless Communications & Mobile Computing. Dr. Chao is an IEEE senior member, a Fellow of the Institution of Engineering and Technology (FIET), and a Chartered Fellow of the British Computer Society (FBCS).

Homepage : http://www.ndhu.edu.tw/~comput/HCC/index.htm

Chi-Hsiang Lo
Chi-Hsiang Lo received a B.Ed. degree in Industrial Education (majoring in Electronic Engineering) from the National Taiwan Normal University, Taipei, Taiwan in 1975, and the M.S. and Ph.D degrees in Computer Science from the Texas A&M University, Commerce, TX, and Kent State University, OH, USA, in 1992 and 2003, respectively. Since August 1975, he has been with National Ilan University and he is currently an Associate Professor of Electronic Engineering and the Secretary General. His research interests are Image Processing, Medical Imaging, Algorithm Analysis and Logical Design.