SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks. 2008; **1**:511–520
Published online 16 October 2008 in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/sec.62

Early security key exchange for encryption in Mobile IPv6 handoff

Tin-Yu Wu[1*,†], Chi-Hsiang Lo[2,3] and Han-Chieh Chao[2,3,4]

[1]*Department of Electrical Engineering, Tamkang University, Taipei, Taiwan*
[2]*Institute of Computer Science & Information Engineering, National Ilan University, Ilan, Taiwan*
[3]*Department of Electronic Engineering, National Ilan University, Ilan, Taiwan*
[4]*Department of Electrical Engineering, National Dong Hwa University, Hualien, Taiwan*

Summary

Wireless equipment has become ubiquitous. However, in facing various software attacks, wireless linked networks are more vulnerable than wire linked networks. The general problem with Mobile IPv6 (MIPv6) (Table I) is the long handover latency period. To reduce the security latency, we propose early security key exchange for encryption in MIPv6 handoff. In our approach, two issues are addressed in dealing with the latency within the encryption technology during the handover. First, we extend the Early Binding Update (EBU) method to deal with the long security exchange negotiation time for the MIPv6 handoff. Second, we adopt the Security Access Gateway (SAG) to solve the limited computing and memory in the Mobile Node (MN). Copyright © 2008 John Wiley & Sons, Ltd.

KEY WORDS: SAG; MIPv6; security handover latency

1. Introduction

Mobile IPv6 (MIPv6) provides mobile techniques for new IP-based services over wireless networks, allowing users to access on-line services while Roaming. MIPv6 offers more advantages than Mobile IPv4 (MIPv4). In MIPv6, the Mobile node (MN) uses Route Optimization (RO) permits talking directly to its peers while retaining the ability to move around and change the currently used IP addresses. The packets go through a shorter route instead of a triangle route with the other end on the Home Agent (HA). Therefore, MIPv4 confronts extra delays due to the triangular routing and the lack of addresses and high signaling load [1].

The security risks occur because of the binding process. Therefore, under the end-to-end principle, MIPv6 designed a procedure called Return Routability (RR), RFC3775, and RFC3776 to compensate for the differences in trust relationships and authentication between these nodes. Return Routability Binding Updates (BUs) sent to Corresponding Node (CN) do not require a security configuration association or an authentication infrastructure between the MN and CN. Nevertheless, RR has some disadvantages. For instance, RR cannot provide a satisfactory security level or deal with fixed CN while another node is dealing with a mobile CN. This is based on a simple BU signal protection. Furthermore, there must be additional Internet Key Exchanges (IKE) and IP

*Correspondence to: Tin-Yu Wu, Department of Electrical Engineering, Tamkang University, Taipei, Taiwan.
†E-mail: tyw@mail.tku.edu.tw

Table I. Acronyms.

AAA	Authentication, Authorization, Accounting
AR	Access Routers
BUs	Binding Updates
CoA	Care-of-Addresses
CBU	Certificate-based Binding Update
CN	Corresponding Node
CN_{HA}	Correspondent Home Agent
CN_{MN}	Correspondent Mobile node
DKM	Directed Key Migration
EBA	Early Binding Acknowledgement
ECBU	Extended Certificate-Based Update Protocol
EEBU	Extended Early Binding Update
FA	Foreign Agent
HA	Home Agent
HoA	Home of Address
HMIPv6	Hierarchical Mobile IPv6
IETF	Internet Engineering Task Force
IKE	Internet Key Exchanges
IPSec	IP Security
MAP	Mobility Anchor Point
MH	Mobile Host
MIPv4	Mobile IPv4
MIPv6	Mobile IPv6
ML-IPSec	Multi-layered IPSec
PKD	Proactive Key Distribution
QoS	Quality of Service
REQ	Request
RO	Route Optimization
RR	Return Routability
SA	Security Associations
SAG	Security Access Gateway
SAG-CN	Security Access Gateway-Corresponding Node
SAG-MN	Security Access Gateway-Mobile Node

Security (IPSec) to deal with the higher security requirement. IKE requires heavy computing overhead, making it unsuitable for mobile devices [2–4].

Today, numerous researches have focused on authentication and data encryption during handover. Only a few inventions protect all traffic between the MN and CN with limited computing and memory equipment. Wireless networks have major weaknesses due to the handoff latency. Additional secret protocols increase the latency and this is a critical problem in real-time traffic.

We therefore propose an early security key exchange for encryption during MIPv6 handoff. This process is designed to reduce the handover latency. According to the present statistics, additional security procedures will double the encryption latency. Our design is aimed at reducing the latency from encryption technology during the handover. The Extended Early Binding Update (EEBU) procedure is used to deal with the long-term security exchange negotiation in MIPv6 handoff. The IPSec tunnel protects all traffic between the MN and CN.

In our approach three aspects are expressed as follows: (1) define and present how all traffic is protected between the MN and CN; (2) how the Security Access Gateway (SAG) is used to solve the limited MN computing power and memory; and (3) reduces the security exchange latency over handoff [7–9].

Section 2 introduces the related works. Section 3 illustrates the early security key exchange for encryption in MIPv6 handoff and the performance evaluation. Section 4 describes whether the CN is a MN or not. Section 5 presents the performance analysis. The conclusion and the future studies are elaborated in Section 6.

2. Related Works

A brief overview of the EBU process is given. The mobile Multi-layered IPSec (ML-IPSec) supplies MIPv4 handoff security between the HA and Foreign Agent (FA). The Extended Certificate-based Update (ECBU) Protocol is the HA that handles strong authentication for its MNs and the authentication process between wired devices. Finally, we present two similar researches.

2.1. Early Binding Update [3,4,7]

The RFC 3775 describes the MIPv6 protocol roaming procedure in detail. However, the MN has a weakness; the latency during handover, such as packet loss, latency and out of sequence packets. The above-mentioned situations will become serious within a long-term handover period. When the RR precedes the MN it must wait for both address tests to conclude before it can be registered at a new care of address. The EBU can improve these problems. EBU presents an optimization for MIPv6 correspondent registrations to reduce the latency of both address tests. Generally, three phases are used throughout the performance evaluation: Pre-handover phase, Critical phase, and Post-handover phase.

Figure 1 shows that the EBU uses Pre-handover phases to Pre-procedure Home Keygen Token. Home Keygen Token delivers the MN to the legitimate owner of the home address. During handover, the approach needs to send a HoTI and also to receive a HoT and therefore carry home-address test through the Pre-handover phase.

2.2. Mobile Multi-layered IPSec [10]

In IP layer, security data confidentiality and integrity are measured. The IPSec is usually adopted to encrypt end-to-end data. However, some services are not

DOI:10.1002/sec

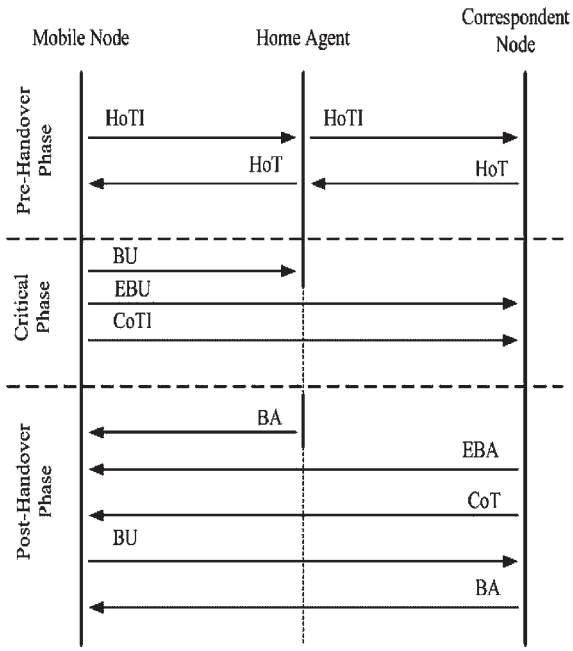

Fig. 1. Early binding updates.

provided; for example, TCP acknowledgment information is not available if the end-to-end encryption is in use or mobile routers cannot use IPSec because the information needed by these algorithms resides inside the encrypted packet. Therefore, the ML-IPSec modifies IPSec so that certain portions of the datagram may be exposed to intermediate network elements.

These authors define and present performance measurements for an efficient key distribution protocol to enable fast ML-IPSec session initialization. There are two protocols that support mobility, Proactive Key Distribution (PKD) and Directed Key Migration (DKM). The PKD focuses on fast handoff by pre-distributing keys through FA. PKDs are neighbors of the current FA. The advantage of this mechanism is that the overhead and handoff latency during handover are reduced and decreased. The disadvantage is that the active key information must be stored in more nodes. The DKM is stored only in the FA, which actively serves the mobile host (MH). When the MH moves to a FA area, the DKM migrates from the old FA to the new FA in a secure manner.

2.3. Extended Certificate-based Update Protocol [11,12]

MIPv6 proposed RR to process BUs. The Internet Engineering Task Force (IETF) suggests bundling IKE to improve the authentication ability and to protect the communication channel MN-HA. The RR provides a simple way to protect the BU signals. The authors proposed the ECBU protocol such that one function of the HA is to act as the security proxy for its MNs. The authentication is based on the HA's certificate and the secret session keys are generated by strong cryptosystems. This approach avoids many security obstacles in the RR protocol and provides a simple, integrated, and efficient security solution for mobile communication and based on a Certificate-based Binding Update (CBU) protocol. Figure 2 shows that the ECBU protocol is able to protect all communication channels in MIPv6 networks.

2.4. Forwarding Scheme Extension for Fast and Secure Handoff in Hierarchical MIPv6 [5]

In this paper, the authors propose that the Hierarchical Mobile IPv6 (HMIPv6) and Authentication, Authorization, Accounting (AAA) protocol has ineffective authenticating and BU procedures that limit its Quality of Service (QoS). Thus, the authors propose a forwarding scheme extension for fast and secure handoff which can reduce a handoff delay while

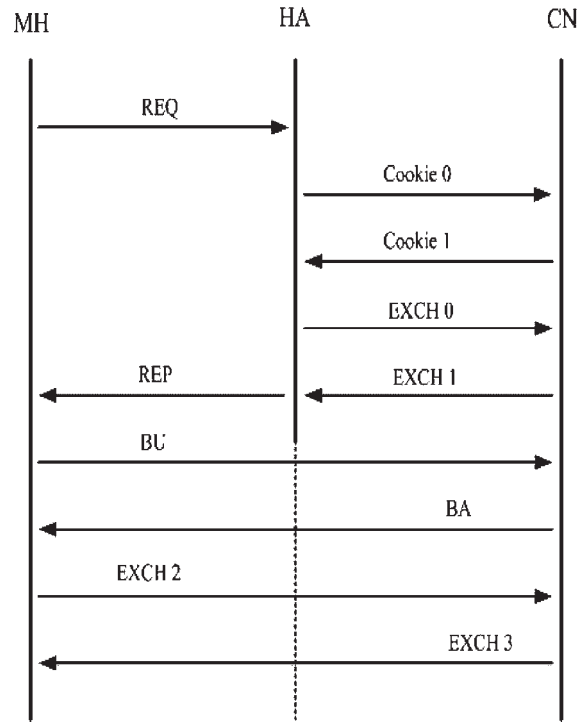

Fig. 2. Extended certificate-based binding update.

DOI:10.1002/sec

maintaining a security level using a forwarding and session key exchange mechanism. According to their mechanism, the MN sends BU messages to a previous Mobility Anchor Point (MAP), and next, the previous MAP forwards packets to a new MAP. The session key exchange mechanism substantially essentially reuses the previously assigned session keys and such advantage can reduce the handoff delay. However, the weakness is that the mechanism requires that a trusted third party supports the key exchange between the Access Routers (AR) and uses only the intra-handoff within the same domain.

2.5. Authenticated Fast Handover Scheme in the Hierarchical Mobile IPv6 [6]

In this paper, the authors propose an efficient and secure authentication method for global and local BU in HMIPv6 as well as a fast handover in HMIPv6. The mechanism uses authenticate local BU message and group key management scheme among MAP and ARs in a MAP domain for the protocol efficiency based on AAA. The authors analyzed the random-walk mobility model.

3. Early Security Key Exchange for Encryption in Mobile IPv6 Handoff

In this section, the authors proposed early security key exchange for encryption in MIPv6 handoff to circumvent the long latency of additional encryption during handoff. Our approach considers how to protect all traffic between MN and CN and solve the limited computing power of mobile terminal. Consequently, we designed this method to combine EBU and mobile Multi-IPSec protocol.

During roaming, the MN usually has low computing efficiency and long latency and these disadvantages undoubtedly influence the security mechanism. Thus, an SAG is proposed to deal with mobile device limited computing power. Generally, a longer key brings higher security reliance irrespective of symmetric or asymmetric encryption. However, most researches believe that a longer key will consume more computing power efficiency and this is a very serious problem with portable devices because longer key uses a pair of SAGs to protect security communications between the MN and CN. The encryption servers have high computing power and will supply highest security to both domains.

Some studies point out that IKE is not suitable for mobile devices, because the IKE protocol needs heavy computing overheads. Our proposal uses the ECBU protocol and SAG to precede key exchange and encryption. Handoff latency is a serious problem in a mobile computing network, and unfortunately using security protocol increases handoff latency.

Therefore, our approach uses early security key exchange encryption to reduce the latency in MIPv6 handoff. This mechanism protects all traffic channels in the MIPv6 network. RR cannot provide a satisfactory level of security. It just provides a simple way to protect the BU signals. IKE is not suitable for mobile devices with limited computing power and battery power. It is very difficult to improve the secure BU function between two MNs in RR.

In Figure 3, when the MN detects that it itself has moved to a different access network, the MN must perform BU procedure and rely on EBU concept to reduce latency time. At the same time, the two domains between the Security Access Gateway-Mobile Node (SAG-MN) and Security Access Gateway-Corresponding Node (SAG-CN) finish the security negotiation. The SAG then implements an encryption tunnel between the MN and CN.

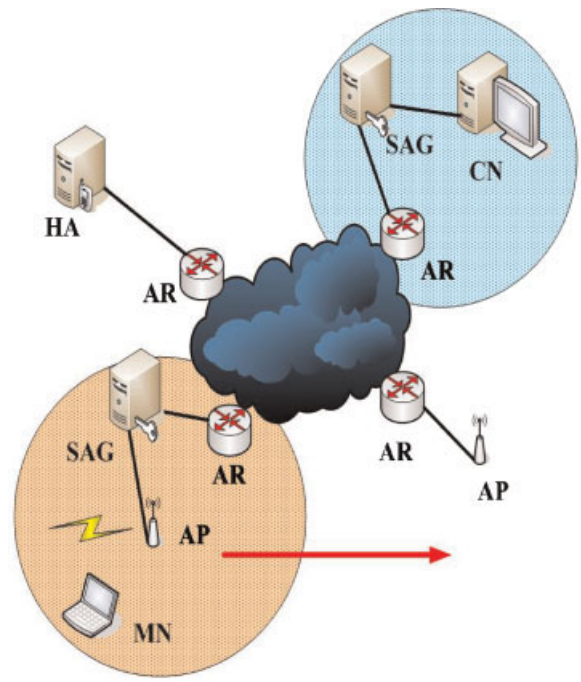

Fig. 3. Early security key exchange in MIPv6 handoff.

DOI:10.1002/sec

We designed some methods to solve these problems. We adopted an early security key exchange for the encryption procedure to reduce the handover latency. The MN is weak at the IKE and IPSec protocol. Therefore, we design SAG, a high computing powered service, to improve the limited computing power and memory issues.

One disadvantage of the RR procedure is that a MN must wait for both address tests to conclude before it can register a new care-of-address (CoA). However, RR cannot provide a satisfying level of security. In the following, we will introduce how our approach solves these problems. EBU can improve these problems and it is based on MIPv6 mechanisms. EBU presents an optimization to MIPv6 associated registrations to reduce the latency of both address tests. Three phases will be used throughout the performance evaluation: Pre-handover phase, Critical phase, and Post-handover phase. (Shown in Figure 4).

3.1. Pre-handover Phase

During the Pre-handover phase the MN still uses its old CoA. When the signal is lower than the threshold at which the MN might sense a new access point with a better signal-to-noise ratio, the link layer signaling for inter-access-point switching has not yet been initiated. Therefore, we pre-process the negotiation with a security certificate to the new SAG. A digital signature cryptosystem is used [3,4]

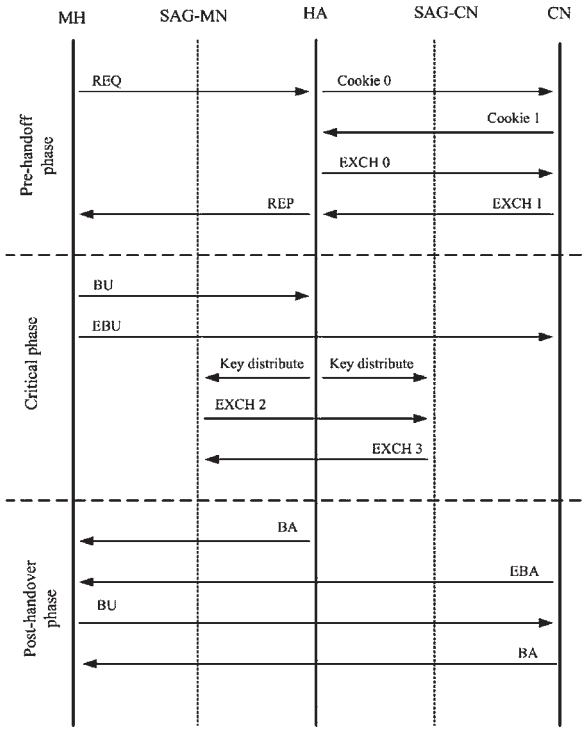

Fig. 4. Flow chart of early security key exchange in MIPv6.

$$Cert_H = \{HLSP, PH, Valid\_Interval, SIG_{CA}\}$$

Cert_H : Public key certificate of the home link

HLSP : Home link subnet prefix

Valid_Interval : Valid duration of the certificate

CA : Certification Authority

SIG_CA : The CA′s signature on HLSP, PH, *and Valid*_Interval

When a MN detects that the signal is lower than the threshold necessary to start the RO operation with a CN, the MN sends a RO request to the HA using IPSec tunneling. In the formula, HA represents the IP address of the HA.

$$REQ = \{Src = HoA, Des = HA, e(K_{HA}, HoA, CoA, CN, N_0)\}$$

K_HA : Session key for the IPSec secure tunnel

N_0 : Random number for counter message replay

The HA receives the REQ and verifies Home Address (HoA) 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 then sends them back to the HA.

$$\text{COOKIE}_0 = \{\text{Src} = \text{HoA}, \text{Des} = \text{CN}, C_0\}$$
$$\text{COOKIE}_1 = \{\text{Src} = \text{CN}, \text{Des} = \text{HoA}, C_0, C_1, N_1\}$$

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

$$\text{EXCH}_0 = \{\text{Src} = \text{HoA}, \text{Des} = \text{CN}, C_0, C_1, N_1, N_2, g^x, \text{TS}, \text{SIG}_\text{H}, \text{Cert}_\text{H}\}$$

g^x : Diffie-Hellman public value

Cert_H : Public key certificate of the home link

DOI:10.1002/sec

$$\begin{aligned}\mathrm{SIG_H} &= \mathrm{Sig}(S_{\mathrm{H}}, \mathrm{HoA/CN}/g^x/N_1/N_2/\mathrm{TS})\\ &\quad \mathrm{KDH} = (g^x)^y \ \{\text{Diffie-Hellman key}\}\\ &\quad K_{\mathrm{master}} = \mathrm{prf}(K_{\mathrm{DH}}, N_1/N_2) \ \{\text{Master secret}\}\\ &\quad K_{\mathrm{BU}} = \mathrm{prf}(K_{\mathrm{master}}, N_1/N_2/0)\\ &\quad \text{Binding key } (\mathrm{MN} \rightarrow \mathrm{CN})\}\\ &\quad K_{\mathrm{BA}} = \mathrm{prf}(K_{\mathrm{master}}, N_1/N_2/1)\\ &\quad \{\text{Acknowledgement key } (\mathrm{CN} \rightarrow \mathrm{MN})\}\\ &\quad K_{\mathrm{EN}} = \mathrm{prf}(K_{\mathrm{master}}, N_1/N_2/2)\\ &\quad \{\text{Encryption key } (\mathrm{MN} \leftrightarrow \mathrm{CN})\}\end{aligned}$$

The CN receives the $\mathrm{EXCH_0}$ and CN sends $\mathrm{EXCH_1}$ to the MN. Both parties can now identify each other and this will be useful for setting up access control on the MN and CN.

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

3.2. Critical Phase

During the Critical phase, the MN moves to a new area and configures a new CoA. The MN then starts a new CoA to the correspondent registrations by EBUs. The MN sends a BU message to HA and at the same time, MN sends early binding acknowledgement (EBA) to CN.

$$\begin{aligned}\mathrm{BU_{MN\text{-}HA}} &= \{\mathrm{Src} = \mathrm{CoA}, \mathrm{Des}\\ &\quad = \mathrm{HA}, \mathrm{HA}, \mathrm{Seq\#}, \mathrm{LT_{BU}}, \mathrm{MAC_{BU}}\}\end{aligned}$$

$$\begin{aligned}\mathrm{EBU} &= \{\mathrm{Src} = \mathrm{CoA}, \mathrm{Des}\\ &\quad = \mathrm{CN}, \mathrm{HoA}, \mathrm{Seq\#}, \mathrm{LT_{EBU}}, \mathrm{MAC_{EBU}}\}\end{aligned}$$

$$\begin{aligned}\mathrm{MAC_{EBU}} &= \mathrm{prf}(K_{\mathrm{EBU}}, \mathrm{HoA/CoA/Seq\#/LT_{EBU}})\\ &\quad \mathrm{MAC_{EBU}}: \text{Authenticate the EBU message}\\ &\quad \mathrm{Seq\#}: \text{Sequence number}\\ &\quad \mathrm{LT_{EBU}}: \text{Lifetime of the binding}\end{aligned}$$

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

$$\begin{aligned}&\text{Key Distribute (SAG-MN)} = \{\mathrm{Src} = \mathrm{HA}, \mathrm{Des}\\ &\quad = \text{SAG-MN}, K_{\mathrm{EN}} | N'_0\}\\ &\text{Key Distribute (SAG-CN)} = \{\mathrm{Src} = \mathrm{HA}, \mathrm{Des}\\ &\quad = \text{SAG-CN}, K_{\mathrm{EN}} | N'_0\}\end{aligned}$$

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

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

3.3. Post-handover Phase

At the beginning of the Post-handover phase the MN has communicated its CoA to the CN and sends a BU to the CN to confirm. The HA and CN will then reply with a binding acknowledgement (BA) and EBA message.

$$\begin{aligned}\mathrm{BA_{HA\text{-}MN}} &= \{\mathrm{Src} = \mathrm{HA}, \mathrm{Des}\\ &\quad = \mathrm{CoA}, \mathrm{HA}, \mathrm{Seq\#}, \mathrm{LT_{BA}}, \mathrm{MAC_{BA}}\}\end{aligned}$$

$$\begin{aligned}\mathrm{EBA} &= \{\mathrm{Src} = \mathrm{CN}, \mathrm{Des}\\ &\quad = \mathrm{CoA}, \mathrm{HoA}, \mathrm{Seq\#}, \mathrm{LT_{EBA}}, \mathrm{LT_{EN}}, \mathrm{MAC_{EBA}}\}\end{aligned}$$

$$\begin{aligned}\mathrm{MAC_{EBA}} = \ & \mathrm{prf}(K_{\mathrm{BA}}, \mathrm{CoA/CN/Seq\#/LT_{EBA}/LT_{EN}})\\ & \mathrm{Seq\#}: \text{Copy from the EBU message}\\ & \mathrm{LT_{EBA}}: \text{Lifetime of the binding}\\ & \mathrm{LT_{EN}}: \text{Lifetime of } K_{\mathrm{EN}}\\ & \mathrm{MAC_{EBA}}: \text{To authenticate the BA message}\end{aligned}$$

$$\begin{aligned}\mathrm{BU_{MN\text{-}CN}} &= \{\mathrm{Src} = \mathrm{CoA}, \mathrm{Des}\\ &\quad = \mathrm{CN}, \mathrm{HA}, \mathrm{Seq\#}, \mathrm{LT_{BU}}, \mathrm{MAC_{BU}}\}\end{aligned}$$

DOI:10.1002/sec

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

We implemented an SAG to deal with the limited computing in MNs by adopting the ECBU. The IPSec cannot be used without modification because the HoA is not deployed as a source/destination address in the IP packet headers.

Figure 5 shows that the encryption parameter stored in the Old SAG-MN will be transferred to the New SAG-MN through HA during the Critical phase. The encryption will be performed before establishing communications between the New SAG-MN and SAG-CN. Afterwards, the MN and CN can establish secure communication with the assistance of New SAG-MN and SAG-CN and the total delay time is

$$T_{delay} = T_{BU} + T_{EBU} + T_{key\ transfer} + T_{EXCH2} + T_{EXCH3}$$

.

4. The Corresponding Node is a Mobile Node

As mentioned above in our proposed two MNs, BU becomes a complex matter in the RR process. In our solution, the secured BU deals easily between two MNs and we extend the message exchange method.

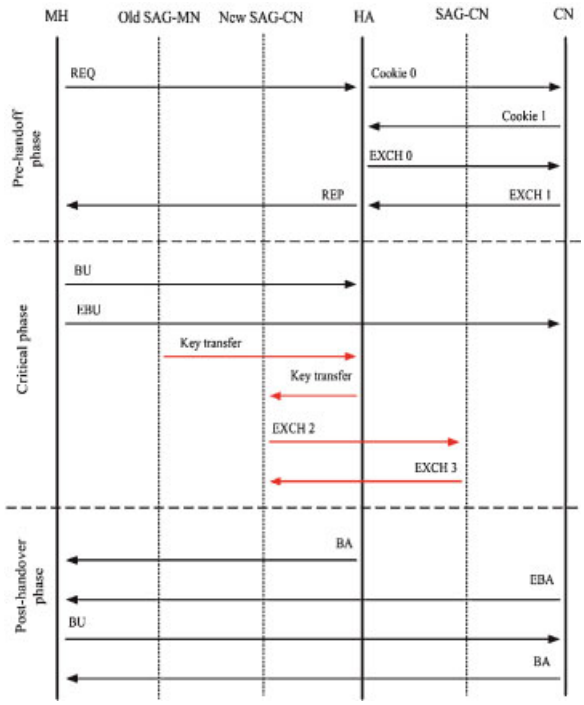

Fig. 5. Early security key exchange during handoff.

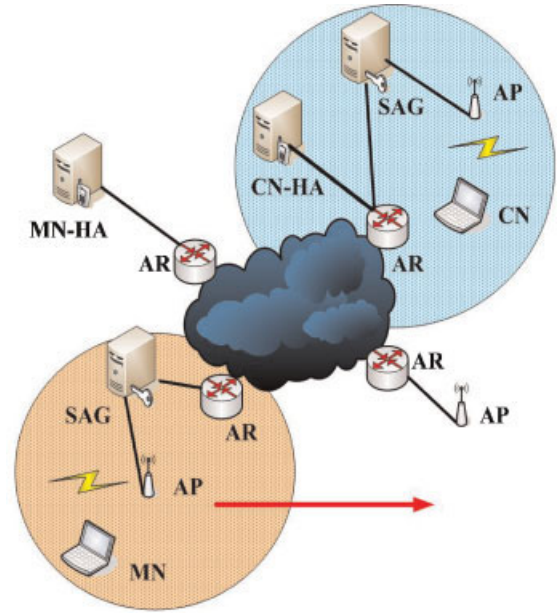

Fig. 6. The MN and CN are mobile nodes.

Figure 6 shows the CN_{MN} is a mobile correspondent node with home address CN_{HoA} and care-of-address CN_{CoA} while CN_{HA} is its home agent.

4.1. Pre-handover Phase

In Figure 7 the MN detects that the signal is lower than the threshold necessary to start the RO operation with a CN. Thus, MN sends a RO request to the HA using IPSec tunneling. In this formula HA represents the IP address of the HA. The HA-CN sends TEST to the CN and checks the location of the CN to test whether CN is alive.

$$REQ = \{Src = HoA, Des = HA, e(K_{HA}, HoA, CoA, CN, N_0)\}$$

$$COOKIE_0 = \{Src = HoA, Des = CN_{HA}, C_0\}$$

$$TEST = \{Src = CNHA, Des = CNCoA, test\_flag\}$$

$$ALIVE = \{Src = CN_{CoA}, Des = CN_{HA}, N_3\}$$

TEST and ALIVE : To testing CN is alive

N_3 : Generating from CN_{MN}

DOI:10.1002/sec

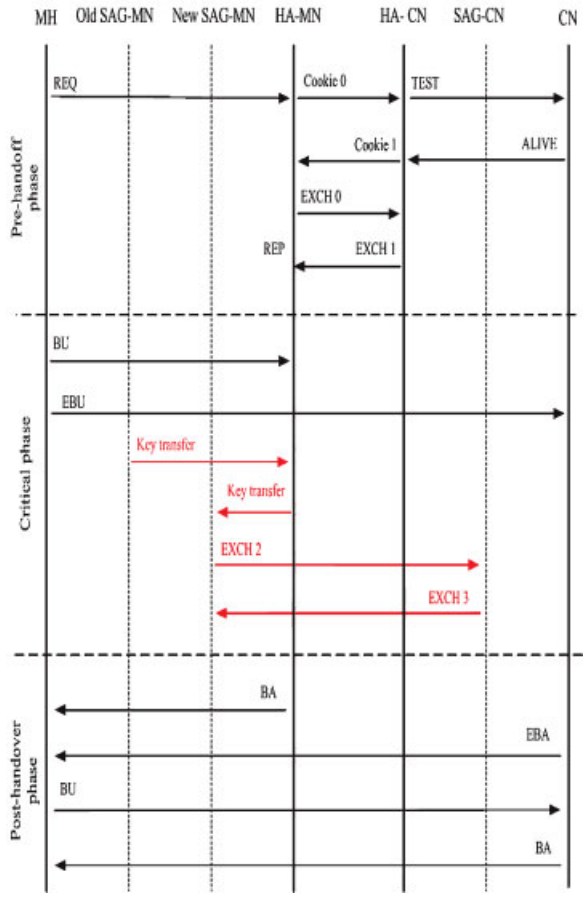

Fig. 7. Early security key exchange for encryption during handoff between two mobile nodes.

$$\mathrm{COOKIE}_1 = \{\mathrm{Src} = \mathrm{CN}_{\mathrm{HA}}, \mathrm{Des} = \mathrm{HoA}, C_0, C_1, N_1\}$$

$$\mathrm{EXCH}_0 = \{\mathrm{Src} = \mathrm{HoA}, \mathrm{Des} = \mathrm{CN}_{\mathrm{HA}}, C_0, C_1, N_1, N_2, g^x, \mathrm{TS}, \mathrm{SIG}_{\mathrm{H}}, \mathrm{Cert}_{\mathrm{H}}\}$$

$$\mathrm{EXCH}_1 = \{\mathrm{Src} = \mathrm{CN}_{\mathrm{HA}}, \mathrm{Des} = \mathrm{HoA}, C_0, C_1, g^y, \mathrm{SIG}_{\mathrm{CN}}, \mathrm{Cert}_{\mathrm{CN}}\}$$

$$\mathrm{REP} = \{\mathrm{Src} = \mathrm{CN}, \mathrm{Des} = \mathrm{CoA}, \mathrm{Payload}\}$$

4.2. Critical Phase

In the Critical phase, the MN moves to a new area and configures a new CoA. The MN starts at a new CoA to the correspondent registrations using EBUs. The MN sends a BU message to HA and at the same time, MN sends EBA to CN.

$$\mathrm{BU}_{\mathrm{MN\text{-}HA}} = \{\mathrm{Src} = \mathrm{CoA}, \mathrm{Des} = \mathrm{HA}, \mathrm{HA}, \mathrm{Seq\#}, \mathrm{LT}_{\mathrm{BU}}, \mathrm{MAC}_{\mathrm{BU}}\}$$

$$\mathrm{EBU} = \{\mathrm{Src} = \mathrm{CoA}, \mathrm{Des} = \mathrm{CN}, \mathrm{HoA}, \mathrm{Seq\#}, \mathrm{LT}_{\mathrm{EBU}}, \mathrm{MAC}_{\mathrm{EBU}}\}$$

The HA and $\mathrm{CN}_{\mathrm{HA}}$ then distribute keys to the SAG-MN and SAG-CN.

$$\mathrm{Key}_{\mathrm{Distribute}}(\mathrm{SAG\text{-}MN}) = \{\mathrm{Src} = \mathrm{HA}, \mathrm{Des} = \mathrm{SAG\text{-}MN}, K_{\mathrm{EN}}/N'_0\}$$

$$\mathrm{Key}_{\mathrm{Distribute}}(\mathrm{SAG\text{-}CN}) = \{\mathrm{Src} = \mathrm{CN}_{\mathrm{HA}}, \mathrm{Des} = \mathrm{SAG\text{-}CN}, K_{\mathrm{EN}}/N'_0\}$$

The SAG-MN and SAG-CN can use both EXCH_2 and EXCH_3 messages to confirm K_{EN}.

$$\mathrm{EXCH}_2 = \{\mathrm{Src} = \mathrm{SAG\text{-}MN}, \mathrm{Des} = \mathrm{SAG\text{-}CN}, e(K_{\mathrm{EN}}, N'_0)\}$$

$$\mathrm{EXCH}_3 = \{\mathrm{Src} = \mathrm{SAG\text{-}CN}, \mathrm{Des} = \mathrm{SAG\text{-}MN}, e(K_{\mathrm{EN}}, N'_0, K_{\mathrm{EN\text{-}new}}, \mathrm{LT}_{\mathrm{EN\text{-}new}})\}$$

4.3. Post-handover Phase

At the beginning of the Post-handover phase the MN communicates its CoA to the CN and sends a BU to the CN to confirm. The HA and CN then reply with a BA and EBA message.

$$\mathrm{BA}_{\mathrm{MN\text{-}HA}} = \{\mathrm{Src} = \mathrm{HA}, \mathrm{Des} = \mathrm{CoA}, \mathrm{HA}, \mathrm{Seq\#}, \mathrm{LT}_{\mathrm{BA}}, \mathrm{MAC}_{\mathrm{BA}}\}$$

$$\mathrm{EBA} = \{\mathrm{Src} = \mathrm{CN}, \mathrm{Des} = \mathrm{CoA}, \mathrm{HoA}, \mathrm{Seq\#}, \mathrm{LT}_{\mathrm{EBA}}, \mathrm{LT}_{\mathrm{EN}}, \mathrm{MAC}_{\mathrm{EBA}}\}$$

$$\mathrm{BU}_{\mathrm{MN\text{-}CN}} = \{\mathrm{Src} = \mathrm{CoA}, \mathrm{Des} = \mathrm{CN}, \mathrm{HA}, \mathrm{Seq\#}, \mathrm{LT}_{\mathrm{BU}}, \mathrm{MAC}_{\mathrm{BU}}\}$$

DOI:10.1002/sec

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

After receiving the messages from the BU and BA, the MN and CN_{MN} separately create a binding cache entry for each other that include the CoA for the two peers, session keys and lifetimes. The two MNs then start sending packets encrypted with K_{EN} to each other at their CoA.

The HA therefore always negotiates with a fixed peer, either a fixed CN or the home agent (CN_{HA}) of a mobile CN. When the initial MN sends its current CoA in the BU message to the Correspondent_Home Agent (CN_{HA}), the CN_{HA} will forward MN's CoA to its Correspondent_Mobile Node (CN_{MN}), and the CN sends its current CoA directly to the MN. Next, the HA confirms SAG-HN with key distribute. The other CN_{HA} will confirm SAG-CN. Both the SAG-MN and SAG-CN take charge of encryption/decryption between the MH and CN.

Figure 7 shows that the encryption parameter originally stored in Old SAG-MN will be transferred from the HA-MN to the New SAG-MN through Old SAG-MN during the Critical phase. In this scenario, the MN is the node that makes the requests. The transfer of the key argument is therefore processed through the HA-MN. Afterwards, the encryption transfer is completed before the New SAG-MN and SAG-CN are setup. Immediately, the MN and CN have encryption communications with the assistance of the new SAG-MN and SAG-CN. The entire delay time is only

$$T_{delay} = T_{BU} + T_{EBU} + T_{key\text{-}transfer} + T_{EXCH2} + T_{EXCH3}$$

.

5. Performance Analysis

In this section, we apply the EBU to Pre-establish the security tunnel. The roaming procedure is divided into three phases namely Pre-handover phase, Critical phase, and Post-handover phase. The Pre-handover phase is performed before the handover and it does not occupy any handover time therefore, during the handover the latency produced is due to the $T_{Critical\text{-}phase}$ and $T_{Post\text{-}handover}$ phase. As a result, we conclude that our method can reduce the latency time caused 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 research improves the EBU mechanism. According to References [13–15], we define the mathematical analysis with handoff latency to MIPv6 as

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

$t_{MN,CN}$ is one-way transmission delay of a message size between MN and CN:

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

where q is the probability of wireless link failure, ϖ_q the average queuing delay at each router in the Internet, B_{wl} the bandwidth of wireless link, and, L_{wl} the wireless link delay.

6. Conclusion

Our approach presents some solutions for reducing latency with encryption technology during the handover. The proposed method extends the EBU method to deal with the long-time security exchange negotiation for MIPv6 handoff. We adopted the SAG for encrypting/decrypting the traffic between the MN and CN. Generally speaking, our proposal has three contributions: (1) defines and presents how SAG protects all traffic between the MN and CN; (2) uses the SAG to solve the MN limited computing power and memory; and (3) reduces the security exchange latency over handoff.

References

1. Johnson D, Perkins CE, Arkko J. Mobility support in IPv6. *RFC 3775*, June 2004.
2. Brower E, Ertekin E, Christou CA, O'Keeffe S. The application of header compression to IPsec encrypted networks. *Military Communications Conference, 2005. MILCOM 2005*, Vol. 5 IEEE, 2005; 2844–2850.
3. Zhuo Chen, Xiao-Wei Chen, Zheng-Wen Zhang, Mu-Xiang Yang. The improving of IKE in WLAN. *2005 International Conference on Wireless Communications, Networking and Mobile Computing, 2005. Proceedings*, Vol. 2, 2005; 1128–1131.
4. Vogt C, Bless R, Doll M, Kuefner T. Early binding updates for Mobile IPv6. *2005 International Conference on Wireless Communications, Networking and Mobile Computing. 2005. Proceedings*, Vol. 3, 2005; 1440–1445.
5. Hoseong J, Jungmuk L, Hyunseung C. Forwarding scheme extension for fast and secure handoff in hierarchical MIPv6. *ICCS 2005, Lecture Notes in Computer Science* 2007; **3515**: 468–476.

DOI:10.1002/sec

6. Hyun-Sun K, Chang-Seop P. Authenticated fast handover scheme in the Hierarchical Mobile IPv6. *Lecture Notes in Computer Science* 2007; **4298**: 211–224.
7. Kent S, Atkinson R. Security architecture for the Internet Protocol (IPSec). *RFC 2401*, November 1998.
8. Kent S, Atkinson R. IP Encapsulating Security Payload (ESP). *RFC 2406*, November 1998.
9. Kent S, Atkinson R. IP Authentication Header (AH). *RFC 2402*, November 1998.
10. Choi H, Song H, Cao G, La Porta T. Mobile multi-layered IPsec. *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies*, Vol. 3, 2005; 1929–1939.
11. Deng R, Zhou J, Bao F. Defending against redirect attacks in mobile IP. *Proceedings of 9th ACM Conference on Computer and Communications Security*, ACM Press: Washington, DC, 2002; 59–67.
12. Qiu Y, Zhou J, Bao F. Protecting all traffic channels in Mobile IPv6 network. *WCMC 2004/IEEE Communications Society*, 2004; 160–165.
13. Xie J, Akyildiz IF. A novel distributed dynamic location management scheme for minimizing signaling costs in mobile IP. *IEEE Transactions on Mobile Computing* 2002; **1**(3): 163–175.
14. Pack S, Choi Y. Performance analysis of fast handover in Mobile IPv6 networks. *Proceedings of IFIP on Personal Wireless Communications, LNCS*, Vol. 2775, 2003; 679–691.
15. Lai WK, Chiu JC. Improving handoff performance in wireless overlay networks by switching between two-layer IPv6 and one-layer IPv6 addressing. *IEEE Journal on Selected Areas in Communications* 2005; **23**(11): 2129–2137.

Authors' Biographies

Tin-Yu Wu is an Assistant Professor at the Department of Electrical Engineering, Tamkang University, Taipei, R.O.C. He received his Ph.D degree in Electrical Engineering from NDHU in 2007. His research interests focus on the next generation Internet Protocol, Mobile Computing and Wireless Networks.

Chi-Hsiang Lo received the 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.

Han-Chieh Chao is a jointly appointed Full Professor of the Department of Electronic Engineering and 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 Director of Computer Center for 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 the Beijing Jiaotong University, China. His research interests include High Speed Networks, Wireless Networks, IPv6 based Networks, Digital Creative Arts and Digital Divide. He received his M.S. and Ph.D. degrees in Electrical Engineering from Purdue University in 1989 and 1993, respectively. He has authored or co-authored four books and has published about 140 refereed professional research papers. He has supervised 50 MSEE students and one Ph.D. student. 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 NSC, Ministry of Education (MOE), RDEC, Industrial Technology of Research Institute, Institute of Information Industry and 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 R&D division of the NICI (National Information and Communication Initiative, a ministry level government agency which aims to integrate domestic IT and Telecom projects of Taiwan), Co-Chair of the Technical Area for IPv6 Forum Taiwan, the executive editor of the Journal of Internet Technology and the Editor-in-Chief for International Journal of Internet Protocol Technology and International Journal of Ad Hoc and Ubiquitous Computing. Dr. Chao has served as the Guest Editors 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 Chartered Fellow of British Computer Society (FBCS).

Home page: http://www.ndhu.edu.tw/∼comput/HCC/index.htm

DOI:10.1002/sec