World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:3, No:3, 2009

An Efficient MIPv6 Return Routability Scheme Based on Geometric Computing

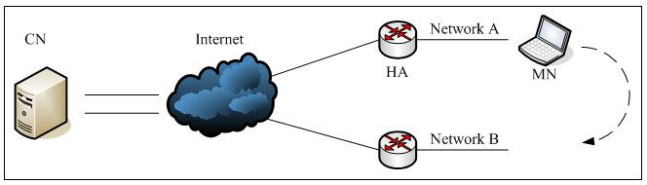
Yen-Cheng Chen, and Fu-Chen Yang

Abstract**—**IETF defines mobility support in IPv6, i.e. MIPv6, to allow nodes to remain reachable while moving around in the IPv6 internet. When a node moves and visits a foreign network, it is still reachable through the indirect packet forwarding from its home network. This triangular routing feature provides node mobility but increases the communication latency between nodes. This deficiency can be overcome by using a Binding Update (BU) scheme, which let nodes keep up-to-date IP addresses and communicate with each other through direct IP routing. To further protect the security of BU, a Return Routability (RR) procedure was developed. However, it has been found that RR procedure is vulnerable to many attacks. In this paper, we will propose a lightweight RR procedure based on geometric computing. In consideration of the inherent limitation of computing resources in mobile node, the proposed scheme is developed to minimize the cost of computations and to eliminate the overhead of state maintenance during binding updates. Compared with other CGA-based BU schemes, our scheme is more efficient and doesn't need nonce tables in nodes.

Keywords**—**Mobile IPv6, Binding update, Geometric computing.

I. Introduction

WITH the rapid development of network and communication technologies, IP address shortage and mobility requirement become more urgent than before. More and more applications and mobile communication services are being provided through IP networks. That is, all-IP based networks are becoming the mainstream common platform for a variety of network applications and services. However, the conventional IP network infrastructure is an obstacle to the development, since it was designed for the fixed and wired Internet. Therefore, Mobile IPv6 is proposed and standardized by the IETF [1] and provides a mobile user an environment to roam over the Internet regardless of her location and without the need of any modifications to existing network devices, as shown in Fig. 1. Normally, a mobile user is unable to send or receive packets in a short period of time during handover, i.e. movement across networks, due to handover latency and required authentication. Handover is the process that one node is away from one network domain to another. It is necessary to keep connections alive even if the mobile one changes its IP address. In Mobile IPv4 (MIPv4), while a mobile node (MN) is in the foreign network, a foreign agent would assign an IP address to it. After that, the MN will send a registration request back to its home agent to keep track of its current address. Subsequently, a corresponding node (CN), not aware of the movement of the MN, sends packets destined to the MN to the home agent, and the home agent forwards those packets to the



MN. Such indirect

Fig. 1 Mobile node handovers to another network domain in MIPv6

forwarding of packets through home agents is called triangular routing. Obviously, triangular routing does cause critical latency because of the transfer in home agent. Therefore, the problem of triangular routing is eliminated in Mobile IPv6 (MIPv6) by the introduction of the Binding Update (BU) message, which enables an MN to update its current location information to the CN. Then, CN is capable of communicating directly with MN. As binding update was first proposed, security issues of binding update were not discussed broadly. Then, a Return Routability (RR) procedure [1] was proposed to assist CN and MN in agreeing a shared secret key for protecting the integrity of the BU message for updating the current IP address.

Unfortunately, it is found that the key agreement mechanism, the so-called Return Routability procedure, will lead to the leakage of the shared secret key. The principle of RR procedure is based on a weak assumption that it is impossible for intruders to monitor one link and the other at the same time within the triangular routes. In fact, it is easy to launch an eavesdropping attack for an attacker if it is located within the overlapped links of the triangular routes. Although many researches [2,3,4,5,7,8,10,11] have worked on it recently, most of them take advantages of PKI (public key infrastructure) or some pre-relationship conditions, which are hardly applied to the existing MIPv6 protocol and whose computation is considerably heavy. In this paper, we will propose a lightweight Return Routability procedure based on geometric computing. During the RR procedure, nodes generate and verify BU messages by choosing points in Euclidean plane and computing their medians. These geometric computations are simple and can be easily realized in any mobile node. In addition, the geometric approach eliminates the maintenance of nonce indices and nonce tables in nodes. This further simplifies the implementation of the proposed scheme in mobile nodes. Therefore, the proposed scheme is lightweight and stateless compared with previous approaches.

II. Background and Related Works

A. Mobile IPv6

There are three main roles in MIPv6: mobile node (MN), corresponding node (CN) and home agent (HA). HA is located in MN's home network and is in charge of redirecting packets to MN. In fact, an MN in MIPv6 owns two addresses at the same time: Home address (HoA) and Care-of address (CoA). HoA is kept static and indicates the MN's IP address and its identity in its home network. CoA is achieved primarily to locate the MN's current IP address, which can be formed by stateless or stateful address auto-configuration in the foreign network where the MN visit currently. Typically, the first 64 bits of an IPv6 address is the subnet prefix and the other 64 bits is derived from the node's MAC address. When an MN is away from its home network and visits another network, a foreign network, the MN will discover the default router of the foreign network and determines its CoA. Immediately after that, the MN forwards a binding registration message to its home network to notify HA its current CoA. HA then updates the mapping of MN's HoA and CoA, and security associations (bidirectional tunneling) are established between MN and its HA. Suppose MN is going to communicate with another node, i.e. CN, located somewhere in the mobile Internet. It is not necessary for CN to be aware of the current location of the MN except MN's HoA. Then packets sent by CN and destined to MN are first routed to MN's home network. MN's HA will intercept those packets and tunnel them to MN. Such packet forwarding procedure is called triangular routing. Although triangular routing alleviates communications broken by node mobility, it also brings performance issues, because all packets destined to an MN must be first routed through its HA. To avoid triangular routing, the binding update procedure is introduced. Whenever MN changes its CoA, it will send a binding update (BU) message to CN to update its current location. Thus, CN can send subsequent packets directly to MN without the help of MN's HA afterward. Since binding updates tells important address information, it is essential to authenticate binding update messages. Unauthenticated or malicious BU messages are in danger of various attacks. Therefore, the Return Routability (RR) procedure was proposed to protect the integrity of BU messages. RR procedure is a process that helps MN to negotiate a secret key between CN and MN for protecting the integrity and authentication of BU. Once CN receives a BU message, CN can validate the message and send back acknowledgement using the same key. Afterward, they can communicate directly to each other. In the next subsection, we will review the RR procedure in details.

B. Return Routability Procedure

RR procedure, standardized and defined in [1], is proposed to provide a way of sharing a common key between CN and MN for authenticating a binding update and to verify if MN is still alive at its claimed CoA. MIPv6 assumes that there exists a pre-established security association between MN and its HA. It means all messages are tunneled by IPsec in the communication of MN and HA. The procedure is depicted in Fig. 2.

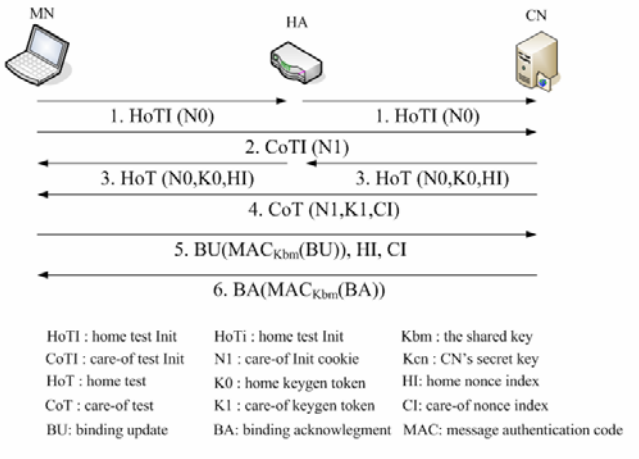


Fig. 2 The Return Routability Procedure

Step 1 and 2:
MN sends a Home Test Init (HoTI) message, including a home init cookie N0 (a nonce), to CN via HA. At the same time, MN also sends a Care-of Test Init (CoTI) message, including a care-of init cookie N1 (another nonce), to CN. The source addresses of HoTI and COTI are HoA and CoA of MN respectively.

Step 3 and 4:
Upon receiving HoTI and CoTI, CN replies with Home Test (HoT) and Care-of Test (CoT) messages respectively. To prepare the HoT message, CN selects a nonce nonceHI, indexed by HI, for use in generating the home keygen token K0. K0 is calculated as below.

$$K0 = \text{First}(64, \text{HMAC\_SHA1}(KCN, (HoA \mid nonceHI \mid 0))),$$

where | denotes string concatenation, KCN is a secret value only kept in CN, HMAC_SHA1( ) denotes a keyed hashing MAC scheme using hash function SHA1, and First(n, M) denotes the first n bits of message M. Similarly, for CoT, CN selects a nonce nonceCI, indexed by CI, for use in generating the care-of keygen token K1. K1 is calculated as below.

$$K1 = \text{First}(64, \text{HMAC\_SHA1}(KCN, (HoA \mid nonceCI \mid 1)))$$

Then, CN sends out the HoT message, including three parameters N0, K0, and HI, destined to HoA, and sends out the CoT message, including three parameters N1, K1, and CI, destined to CoA. The nonce indices carried in HoT and CoT remind CN of which nonce value is used in generating the K0 and K1. Besides, "0"and"1" are used to distinguish home and care-of cookies. The two tokens exchanges are useful to make sure the liveness of MN on both HoA and CoA.

Step 5:
MN obtains home keygen token (K0) and care-of keygen token (K1) from HoT and CoT. The exchanged tokens test whether packets destined to claimed address are routed to MN. It is assumed that if MN can get these two messages correctly, then

MN is actually at the claimed IP address. When K0 and K1 are both received by MN, MN creates a binding key, denoted by K_{bm}, generated from SHA1(K0|K1). K_{bm} becomes the shared secret key between MN and CN via the RR procedure. Soon After, MN sends a binding update message to CN. The binding update message contains HI, CI, and an MAC = First(96, HMAC_SHA1(K_{bm}, (CoA | CN's address| BU))), where BU indicates the binding update message itself.

Step 6:

While CN receives the binding update with message authentication code using Kbm as MAC key, it can rebuild Kbm dynamically and verify the validity with the help of home and care-of nonce index HI and CI. If it is legal, then CN sends back an acknowledgement with MAC = First96(HMAC_SHA1(Kbm, (CoA | CN's address| BA))). In fact, during the RR procedure the two tokens will be exposed to anyone that can obtain both CoT and HoT messages. Since the two routes between CN and MN might be partially overlapped, an attacker can capture the tokens simultaneously at any overlapped link through eavesdropping, especially in home and target network. One has no reason to assume that an intruder will monitor one link and not the other. For instance, if attackers want to redirect the packets to malicious node, they monitor the CN-HA path to obtain HoT message. When receiving HoT, a malicious node sends a CoTI to CN, which will reply a CoT message back to MN. Hence, the malicious node can hashes pairs of tokens to form the secret key, and send a fake binding update by using the key on behalf of MN. Furthermore, CN must maintain a list of nonce table. Hence, the RR procedure considerably suffers from the weak security requirements.

C. Other Improved RR Procedures

Recent studies have shown many novel mechanisms to deal with the security weakness of the above RR procedure. We can roughly divide the researches into two categories. One is certificate-based protocol, such as CBU[7], HCBU[7] and ETBU[11]. The role of Certification Authority (CA) is introduced here, and every HA, under trust delegation, is able to validate its MN. Hence, HA can prove to CN of MN's ownership of its HoA and that the BU request is indeed sent by MN. However, these require heavy computing power via the operations of asymmetric encryption and key agreement. The other category is CGA-based protocols, such as CAM-DH[4], Child-proof Authentication and Improved RR procedure[3]. To prove the ownership of an address, CGA (Cryptographically Generated Address) is introduced. Nodes can construct their addresses by combing the subnet prefix and interface identifier, where the interface identifier is computed via a cryptographic one-way hash function from public key and auxiliary parameters. No one can claim the ownership of the address unless the corresponding private key is compromised. Hence, the security of BU messages can be assured. CGA can be seen as IP-layer platform for developing secure mobile IP applications. Our scheme is also developed based on the CGA platform.

III. The Proposed Scheme

The shortages in RR procedure are widely discussed in current years owing to the increased proportion of mobile users. Many papers have proposed improved mechanisms in terms of security enhancement, but few of them take the MN's computing power into consideration. In practice, MN might be a very power-limited node. Therefore, there is a demand for a lightweight RR procedure. In this section, we propose an efficient RR scheme, whose major operations are based on hash and simple geometric computations. A remote login authentication scheme based on a geometric approach [12] was firstly presented by Wu in 1995 and modified by Chien et al [13].The prime feature is that no verification table is required. Wu's scheme is very efficient and low power consumption because it cleverly exploits the simple geometry property. By taking advantage of the features, we propose a more lightweight return routability procedure based on the geometric approach to prevent the heavy computations and meets the same security requirements as well. In addition, for better security, the HoA in our protocol is also obtained from the CGA scheme. Note that this scheme is also developed to minimize the overhead of MN and CN in storing keys and data.

TABLE I
NOTATIONS

Notation	Description
pk	MN's public key used in CGA
sk	MN's private key used in CGA
x_0, y_0	CN's secret point on the Euclidean plane
N_{MN}	Nonce created by CN for each MN
T	timestamp
K_{DH}	Shared key generated by Diffie Hellman key agreement
$MAC_x(\ )$	Message authentication code using key x

Table I lists the notations used in the proposed scheme. The proposed scheme consists of four steps, described as follows.

Step 1:

MN randomly chooses X_A and computes $Y_A = g^{X_A} \bmod p$. Then, MN uses its private key sk to generate $S_{sk}(T_1, Y_A)$, where T_1 is a timestamp. MN appends $S_{sk}(T_1, Y_A)$ with public key pk in test init messages HoTI and CoTI, and then sends these two messages to CN. Note that HoTI is routed via MN's home agent first, however, CoTI is directly delivered to CN from MN's current CoA. There exists a pre-established security association between MN and its HA. MN's HoA is formed by CGA, and then thus, CN can validate MN by the attached public key pk.

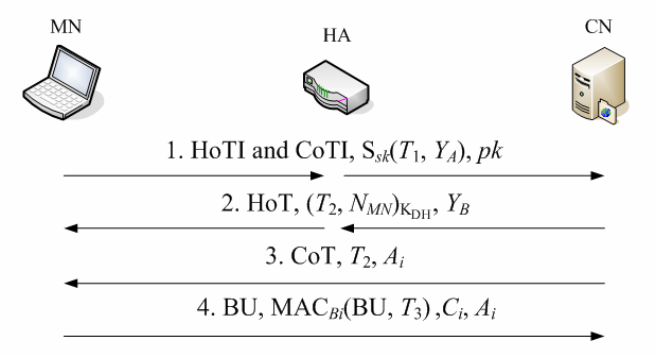


Fig. 3 A RR procedure based on geometric computations

Step 2 and 3:

Upon receiving HoTI and CoTI, CN first verifies the correctness of MN's HoA using public key *pk*. If succeeds, CN retrieves T_1 and Y_A from both HoTI and CoTI, checks their consistence, and determines the freshness of HoTI and CoTI by comparing T_1 with the current time. If the above tests pass, CN randomly chooses X_B, computes $Y_B = g^{X_B} \bmod p$, and determines shared key $K_{DH} = Y_A^{X_B} \bmod p$. In addition, CN computes $r_{i0} = (h(\text{HoA}*x_0), h(\text{CoA}*y_0))$ and prepares a nonce N_{MN} to generate $r_{iw} = (0, h(N_{MN}))$. Points r_{i0} and r_{iw} determines straight line L_i in the Euclidean plane. Then CN finds the median point A_i of r_{i0} and r_{iw} through line L_i, as illustrated in Fig. 4. Suppose the current time is T_2. CN appends $(T_2, N_{MN})_{K_{DH}}$ and Y_B in a HoT message, and puts A_i and T_2 in a CoT message. HoT message is sent to MN's HoA, and the CoT message is sent to MN's CoA. These two messages are delivered in the meantime. Once MN can correctly receive and decrypt messages, the aliveness of the claimed address is confirmed. In these two steps, Diffie Hellman key agreement is applied once and all the other parameters are generated through simple hash and geometric operations. Note that CN doesn't store nonce N_{MN}, except the secret point (x_0, y_0) on the Euclidean plane.

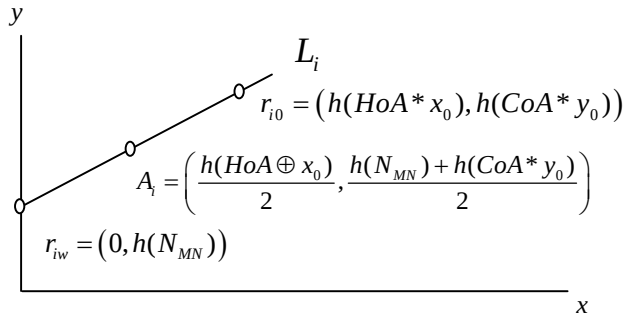


Fig. 4 Graphical result for binding update request

Step 4:

After receiving both HoT and CoT messages, MN computes $K_{DH} = Y_B^{X_A} \bmod p$, and uses K_{DH} to retrieve the nonce N_{MN} from the HoT message for generating $r_{iw} = (0, h(N_{MN}))$ In addition, MN obtains point A_i from the CoT message. Now, line L_i can be reconstructed from points r_{iw} and A_i. Then, MN finds the median point B_i of A_i and r_{iw}, as illustrated in Fig. 5. Suppose the current time is T_3. MN then finds $r_{iT} = (0, h(N_{MN}) \oplus h(T_3)))$ and constructs line L_{WT} from points r_{iT} and B_i. On the line L_{WT}, MN randomly chooses a point C_i distinct from points r_{iT} and B_i. B_i is taken as the shared secret key between CN and MN. MN further computes MAC_{B_i}(HoA, CoA, T_3). Finally, MN prepares a BU message, containing T_3, HoA, CoA, C_i, A_i and MAC_{B_i}(HoA, CoA, T_3), and the message is sent to CN.

Upon receiving the BU message, CN checks the freshness of the message by T_3, and then re-computes r_{i0} according to the HoA and CoA in the binding update message. Point r_{iw} is immediately found by reconstructing line L_i through points A_i and r_{i0}. By an exclusive OR operation on $h(T_3)$ and the *y*-axis value of point r_{iw}, point r_{iT} is determined. Then, line L_{WT} is reconstructed from point r_{iT} and the C_i given in the BU message. CN finds the intersection point B_i of lines L_i and L_{WT}, and determines whether B_i is also the median point of A_i and r_{iw}. If the correspondence holds, then CN verifies the MAC using B_i. As long as the verification succeeds, CN updates the binding of MN's HoA and CoA. The RR procedure is done.

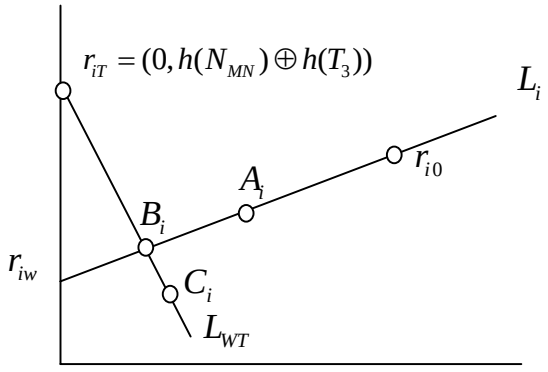


Fig. 5 Graphical result for BU authentication

IV. Security and Performance Analysis

It can be seen that the above return routability procedure mainly applies one-way hashing function and geometric operations and also gets rid of the maintenance of a nonce table in CNs. To demonstrate the superiority of the proposed scheme, we take two related schemes, Yang et al.[3] and CAM-DH[4], in the performance comparison in terms of asymmetric/symmetric cryptography, Diffie Hellman key agreement, message authentication code operation, and the maintenance of a nonce table. Both the previous schemes are also CGA-based and serve the same security requirements as ours. As shown in Table II, our scheme achieves fewer operations and also eliminates the maintenance of nonce tables in CNs.

TABLE II
PERFORMANCE ANALYSIS

	Our scheme	Yang et al.	CAM-DH
Asymmetric Crypto. Op.*	Once	Once	Once
Symmetric Crypto. Op.	Zero	Twice	Zero
Diffie-Hellman key agreement	Twice	Four times	Twice
MAC operation + Hash function	Ten times	Twelve times	Fourteen times
Nonce table maintenance	No	No	Yes

* Required in CGA operation

In addition to the superiority in performance, security protection is also assured by the proposed scheme. Suppose an attacker obtains point A_i in the phase of binding update request, but still fails to decrypt nonce N_{MN}, or even trace back the secret point of CN. If the attacker obtains the given C_i, A_i, HoA and CoA in the phase of BU authentication, the secret key B_i is impossible to be revealed. Moreover, with timestamps, the freshness of messages is assured. In the following, we discuss how our protocol withstands various known attacks.

- **Replay Attack:** Suppose an MN have updated the current location again, but an attacker might reply a previous binding update to make MN's new BU in vain. However, it is not workable because the shared key includes a timestamp, which implies that it's impossible to receive the same message in a certain period of time; likewise, each shared key B_i will be different for each mobile user and a different nonce N_{MN}. As a result, even if somebody gets the same pair of HoA and CoA, the shared key will vary.
- **Eavesdropping Attack:** An attacker might stay in MN's home network or the current visited network to passively capture all conversations between CN and MN. Even though the all given information is disclosed, there is no way to trace back the secret key of CN and the shared secret key between CN and MN owing to the simple properties of geometry.
- **Resource Exhausting Attack:** The original RR procedure requires nonce indices that remind CN which nonce is to be used in generating tokens. In spite of the stateless advantage of nonce indices, a nonce table is required in CN. In our scheme, neither any nonce value nor the nonce table is needed anymore. Thus, CN can prevent a resource exhausting attack issued by tons of faked binding updates.
- **Location Authentication:** CN should confirm if MN is at the claimed IP address, otherwise, an attacker could mount DoS attacks using someone's IP address. RR procedure is done by sending two messages separately from two routes to assure if MN is still alive or at the claimed address. Besides, the HoA in our protocol is obtained from the CGA scheme, so that MN is proven to legally assert the ownership of the address.
- **Modification Attack:** A shared secret key between CN and MN is securely exchanged and can be used for verification and further authentication. Then they can validate the BU messages by verifying the integrity through MAC.

V. CONCLUSION

To keep communication continuously despite the movement of nodes, MIPv6 provides mobility support in the IPv6 network environment and makes sure that packets destined to a mobile node can be successfully delivered. In order to avoid triangular routing due to the indirect packet forwarding thought home networks, MIPv6 mandates a binding update message to be sent from MN to CN to update MN's location information kept by CN as MN changes its CoA. For protecting the binding update message, an RR procedure was proposed to make a shared secret key for authenticating binding updates. However, the shared secret keys derived from RR may be revealed to anyone since they are all delivered in plaintext. In this paper, we have proposed a lightweight RR procedure, based on simple geometric computation. Therefore, the proposed scheme can achieve better performance than previous approaches. Our scheme also eliminates the maintenance of nonce table. Therefore, the proposed scheme is lightweight and stateless. Moreover, the proposed mechanism is developed to follow the current MIPv6 standard. Therefore, it can be implemented without any modification of the current MIPv6 specification.

REFERENCES

[1] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6," *Request for comments* 3775, IETF, June 2004
[2] Feng Yong, Wu Zhongfu, Zhong Jiang, Ye Chunxiao, Wu Kaigui, "A Novel Authentication Mechanism Based on CGA for BU Message Disposal in Mobile IPv6," International Conference on Networking, Architecture, and Storage
[3] Fu-Chen Yang, Yen-Cheng Chen, "A stateless Return Routability Scheme in Mobile IPv6," International Conference on E-Business and Information System Security 2009, IEEE, Wuhan, China
[4] M. Roe, T. Aura, G.O'Shea, J. Arkko, "Authentication of Mobile IPv6 Binding Updates and Acknowledgements", IETF internet draft, February 2002
[5] Tuomas Aura, Michael Roe, "Designing the Mobile IPv6 Security Protocol," Technical Report, April 2006.
[6] T. Aura, "Cryptographically generated addresses(CGA)," *Request for Comments 3972*, IETF, 2005.
[7] Kui Ren, Wenjing Jou, Kai Zeng, Feng Bao, Jianying Zhou, Robert H. Deng, "Routing *optimization security in mobile IPv6," Computer Network, 2006, pp: 2401-2419*
[8] Khaled Elgoarany, Mohamed Eltoweissy, "Security in Mobile IPv6: A survey," Information Security Technical Report, ELSEVIER, March 2007.
[9] Ruidong Li, Jie Li, Kui Wu, Yang Xiao, Jiang Xie, "An Enhanced Fast handover with Low Latency for Mobile IPv6," IEEE Transaction on Wireless Communications, Vol. 7, No. 1, Jan 2008
[10] Warodom Werapun, Apinetr Unakul, "Secure Mobile IPv6 Binding Updates with Identiy-based Signature," *international conference on Electronics Packaging*, Jan 2004
[11] Jung-Doo Koo, Dong-Chun Lee, "Extended Ticket-based Binding Update(ETBU) Protocol for Mobile IPv6(MIPv6) Networks," IEICE TRANS. COMMUN., VOL.E90-B, NO. 4, APRIL 2007
[12] Tzong-Chen Wu, "Remote login authentication scheme based on a geometric approach," Computer Communications, Vol 18, No. 12. december 1995
[13] Hung-Yu Chien, Jinn-Ke Jan, Yuh-Min Tseng, "A modified remote login authentication scheme based on geometric approach" The journal of Systems and Software 55, 2001 (287-290)

Yen-Cheng Chen Yen-Cheng Chen received the Ph.D. degree in computer science from the National Tsing Hua University, Taiwan, in 1992. He was an associative researcher of the ChungHwa Telecom Labs. from 1992 to 1998. From 1998 to 2001, he was an assistant professor of the Department of Information Management, Ming Chuan University, Taiwan. Currently, he is an associate professor of the Department of Information Management, National Chi Nan University, Taiwan. His current research interests are network management, wireless networks, and security.

Fu-Chen Yang received the BS degree in information management from National Kaohsiung First University of Science and Technology in 2007. He is currently pursuing his master degree in information management at National Chi-Nan University, Puli, Nanto. His interests include network security and management as well as Mobile IPv6.