Secure Mobile IP with HIP Style Handshaking and Readdressing for public-key based IP network

Joseph Yick Hon So, Jidong Wang, Deddy Chandra
School of Electrical and Computer System Engineering
RMIT University
Melbourne, VIC, Australia
S3071310@student.rmit.edu.au, {Jidong.wang, Deddy.Chandra}@rmit.edu.au

***Abstract*— Mobile IP allows a mobile node to roam into a foreign IP network without losing its connection with its peer. Mobile IPv6 uses Route Optimization to improve the routing performance by avoiding the triangle routing problem and adopting Return Routability as a secure process for binding update. Host Identity Protocol (HIP) is an experimental security protocol which provides mobility management and multi-homing with new namespace. HIP has a similar architecture to the Mobile IP with Route Optimization. In this paper, we introduce a Secure Mobile IP with HIP Style Handshaking and Readdressing (SMIP), which provides stronger security, better performance and lower binding cost than Mobile IPv6 does in binding update process. The dependency of the home agent in the new scheme is dramatically decreased. The initiated scheme integrates the primary features of two completely different mobility management solutions and sets up a migration path from mobile-IP based solution to a public-key based solution in mobile IP networks.**

***Index Terms*—Credit Base Network, HIP, Mobile IP, Mobility Management.**

I. INTRODUCTION

Wireless networks have grown rapidly in recent years with the advent of new wireless technologies. Both communication networks and computer networks have evolved into hybrid wire and wireless environments and are gradually merging together. Moreover, different types of networks, such as telegraphic networks and data networks are converging into one network to handle all types of traffic. The existing network models and protocols were originally designed for wired networks and some assumptions are aimed to simplify the network design. For instance, in the current TCP/IP suit, IP address takes dual roles as endpoint identifiers and network topological locators. IP address identifies a host in the transport layer protocols while it also identifies a location on the network topology in the network layer. This feature is not efficient in handling mobility issues in wireless IP networks. Many schemes have been proposed to enhance the mobility support toward current network model.

The first approach to solve the mobility management is by disguising the change of network location, the IP address. Mobile IP[1, 2], the most popular scheme was developed by the Internet Engineering Task Force (IETF) and it is based on the idea of providing mobility support on top of current TCP/IP architecture without any modifications to the upper layer protocols. It tries to redirect data packages to new IP address when the mobile node is roaming in the foreign network. Mobile IP is a practical solution even its performance has potential for improvement.

The second approach is remodeling the current IP network architecture to separate network locator and end-host identifier. Host Identity Protocol (HIP)[3] is a new experimental protocol from the IETF and Internet Research Task Force (IRTF). HIP introduces a new namespace – Host Identifier (HI) and a new layer – Host Identity Layer into current TCP/IP protocol stack[3, 4]. Under HIP, a mobile node's identifier and its topological locator are taken by HI and IP address separately. HIP based applications should use HI instead of IP address to address the mobility[5]. Since there is no support to HIP in the current commercial networks and existing applications, Mobile IP is still used in mobility management. In this paper, we propose to apply some concepts of HIP into Mobile IP and aim to improve its performance especially on handover. Our proposal can be seen as the first step to advance the mobility management from Mobile IP to eventual HIP.

II. BACKGROUND

A. Mobile IP

Mobile IP requires minimum change on top of IP to support mobility of network end devices. There are two different versions of Mobile IP, Mobile IPv4[2] and Mobile IPv6[1]. Mobile IPv6 is inherited from Mobile IPv4, with some modifications. There are many different extensions to improve the overall performance of Mobile IP. Mobile IP with Router Optimization Extension is one of the extensions which improved the routing performance and it is part of standard in Mobile IPv6.

1) Mobile IP Basics

In order to minimize the change of the upper layer model in TCP/IP architecture, Mobile IP uses the IP address as the endpoint identifier. Some important components of Mobile IP network include:

- Mobile Node (MN): A host or router that changes the attachment between networks or sub-networks.
- Correspondent Node (CN): A peer with that the mobile node is communicating.
- Home Network: A network that assigns a Home Address to the MN.
- Home Address: IP address assigned to a MN in the Home Network. This IP address will not change when the MN is roaming.
- Foreign Networks: Any networks other than the Home Network.
- Home Agent (HA): The router on a MN's Home Network, this router keeps the record of the MN and will redirect packets of the MN to its foreign network when the MN is roaming in foreign networks.
- Foreign Agent (FA): The router on a MN's Foreign Network, which receives packets from the HA and forwards to the MN. This exists only in Mobile IPv4.
- Care of Address (CoA): The IP address that is assigned to the MN (Mobile IPv6) or the IP address of the FA (Mobile IPv4). A HA forwards the MN's packets based on the CoA record.

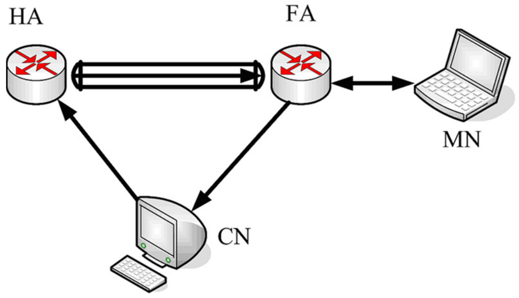


Fig. 1 Mobile IPv4

A Home Address will be assigned to an MN in its Home Network. When a MN moves into a foreign network, it will get a new IP address from the foreign network. The MN sends a packet to update the CoA address record in its HA. When a CN starts a communication with the MN, the CN will send a packet to the Home Address of the MN. When the HA receives this packet, it will create a tunnel to the MN (via a FA in Mobile IPv4) and forward packets to the MN. This mechanism provides the mobility support in IP networks. However, the triangle routing degrades the efficiency of the routing. No matter how close a MN to a CN, packets from the CN to the MN will always be forwarded via HA. Figure 2 show the triangle routing.

2) *Mobile IP with Router Optimization Extension*

Mobile IP with Router Optimization (RO) extensions[6] is an optional scheme in Mobile IPv4, but it has become part of the standard of Mobile IPv6[1]. This extension provides better performance by avoiding triangle routing.

Instead of creating a tunnel between a MN and the HA to forward packets, the MN sends a Binding Update packet to the CN to notify its current CoA after the MN has received the forward packets from HA. The CN will send all packets directly to MN after received the binding update message from MN. Those processes are shown in Fig. 3.

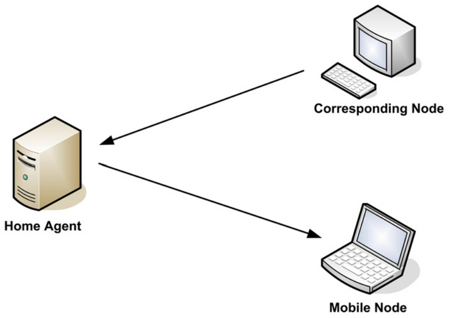


Fig. 2 Triangle Routing

The Mobile IP RO provides the optimal handover if security is not an issue. However, after security mechanism is added on top of Mobile IP RO, the performance will degrade dramatically. This will be discussed in section III.

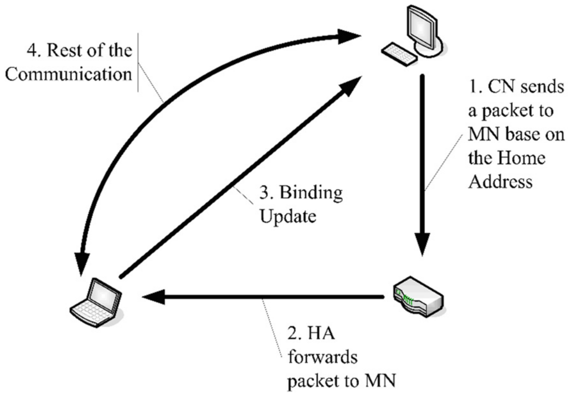

4. Rest of the Communication
1. CN sends a packet to MN base on the Home Address
3. Binding Update
2. HA forwards packet to MN

Fig. 3 Mobile IP Route Optimization

B. *Host Identity Protocol (HIP)*

HIP is re-modeling the current TCP/IP network architecture in order to solve the fundamental problem of IP mobility. The concept of HIP was first discussed in IETF in 1999. The HIP Working Group in IETF and the HIP Research Group in IRTF were formed in 2004. To handle mobility, HIP introduces a new namespace into IP network architecture[3, 4]. An IP address takes two roles in current IP networks, i.e. the endpoint identifier and the network topological locator. The dual roles of an IP address become more problematic with the increase of mobility and multi-homing. This issue is originally tackled by IRTF NameSpace Research Group (NSRG). The development of HIP is partially based on the study of NSRG. IP address is now only used for network topological locator in HIP network architecture. A new cryptographic public key namespace – Host Identifier (HI) is added to current TCP/IP stacks. The lengths of public keys of various algorithms are different. This will become a problem in the practical design, therefore a

128-bits hash key of HI – Host Identity Tag (HIT), which has the same length as IPv6 IP address, will be used as an endpoint identifier in the upper layer protocol to simplify the design[3]. Transport Layer and the layers above it will use HI/HIT to represent a host while the Network Layer will still use IP address to route packets.

Besides mobility support, HIP also supports multi-homing and handles security issues. After the establishment of an HIP connection, packets will be protected by Encapsulation Security Protocol (ESP)[3, 7]. Furthermore, HIP has offered solutions for some IP network problems, such as handover between IPv4 and IPv6 network[8].

HIP was originally designed to use ESP connection, but it has been decoupled from ESP recently. ESP connection is optional in the latest Internet Draft (I-D)[3, 7]. A HIP based protocol can be a secure carrier for many kinds of signaling, such as SRTP/MIKEY[9]. The rest of this paper will discuss an HIP scheme with ESP. Fig. 4 shows the architecture of a traditional network and an HIP based network.

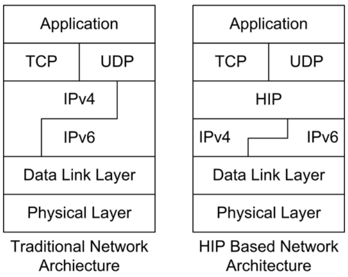


Fig. 4 Traditional Network Architecture and HIP based Network Architecture

1) *HIP Base Exchange*

HIP Base Exchange is a four-way handshake process with Diffie-Hellman type key exchange, which is shown in Fig. 5. Before a HIP connection is established, the HIP Base Exchange process needs to be carried out. The process carries a quick authentication check between the communicating parties and provides a Denial of Service (DoS) protection[3].

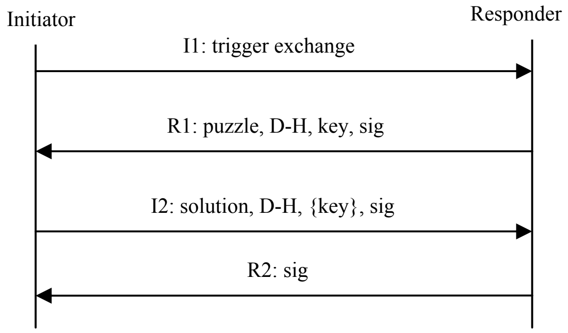


Fig. 5 HIP Base Exchange

- I1 is the first packet from an Initiator to a Responder. It is a trigger packet, which contains the HIT of the Initiator and the HIT of the Responder, if known.
- R1 is the second packet in the Base Exchange and it is sent from the Responder to the Initiator. R1 starts the actual exchange. It contains a cryptographic challenge, which is called a puzzle. The Initiator must solve the puzzle before continuing the Base Exchange. This puzzle makes the Base Exchange resistant to DoS attacks. Besides the puzzle, R1 also contains Diffie-Hellman parameters and a signature.
- I2 is the third packet in the process and it is sent to the Responder by the Initiator with the solution of the puzzle. I2 is discarded by the Responder if the solution is incorrect. I2 also contains the Diffie-Hellman parameter signed by the Initiator.
- R2 is the final packet in the process. It is signed by the Responder and indicates the completion of the Base Exchange.

After the completion of HIP Base Exchange, IPSec Security Associations (SAs) will be created. The Security Parameter Indexes (SPIs) for the Responder-to-Initiator and Initiator-to-Responder have been exchanged in I2 and R2 packets.

2) *Rendezvous Server (RVS)*

HIT binds to IP addresses automatically. In the current HIP architecture, a HIT can be mapped to an IP address by its DNS server[10](Fig. 6). However, using the DNS server to look up the mapping between HIT and IP address is not an efficient solution. A DNS server only stores the mapping of Fully-Qualified Domain Names (FQDN) to HIT and also FQDN to IP address. It does not store the direct mapping between HIT and IP. Besides, records in DNS servers may not be able updated immediately. In order to provide a better performance, a Rendezvous Server (RVS)[11] is introduced.

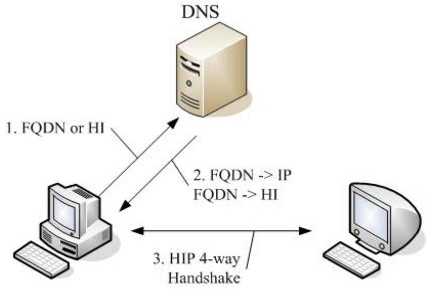


Fig. 6 Mapping between HI/HIT and IP by DNS

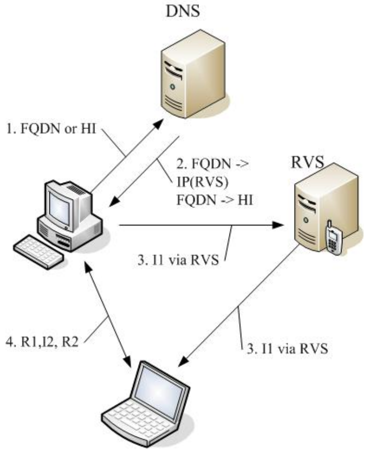


Fig. 7 HI/HIT and IP mapping and HIP Base Exchange via RVS

The role of RVS is similar to that of an HA in Mobile IP[12]. It stores the mapping between HIT and IP directly. Instead of storing the mapping between FQDN to the host IP address in a DNS server, it stores the mapping between FQDN and IP address of the host's RVS. The I1 packet of HIP Base Exchange will go via RVS. Those processes are shown in Fig. 7.

3) *HIP Mobility Support*

Since the pair of SAs created by HIP Base Exchange is not bound to IP addresses, a host is able to receive packets that are protected by ESP SA from any addresses. It enables a host to change its IP address and continues to communicate with its peer. HIP Mobility can be independent of ESP, we will only discuss the ESP based HIP mobility in this paper.

When an MN is roaming into a foreign network, it will be assigned a new IP address. The MN will send an update packet to update its record in its own RVS. Hence, the CN will start the Base Exchange via RVS if it needs to communicate with MN. This is known as the pre-session mobility handling.

If a MN changes its IP address during a communication session, besides the pre-session handling mentioned above, the MN will also send a UPDATE packet with a LOCATOR parameter to notify the CN[13]. The LOCATOR parameter contains the new IP address and the SPI associated with the new IP address. The whole handover process is protected by ESP, which prevents the third party bomb attack. There are three different types of address checking process[13]:

1. Readdress without re-keying, but with address check;
2. Readdress with mobile-initiated rekey; and
3. Readdress with peer-initiated rekey.

4) *Multi-homing support*

The multi-homing supported devices can connect to networks with different built-in interfaces. The latest mobile devices may have more than one network interface. Multi-homing support is an appealing feature in functionality and mobility. HIP offers support to Multi-homing. Host can use the UPDATE packet to notify the peer host that it has more than one IP address. In another words, a unique HI of a device can map to multiple IP addresses.

C. *Summary*

Mobile IP is a widely adopted protocol for mobility management in current IP network architecture. The upper layer protocols do not need to be modified in order to co-operate with Mobile IP. HIP is a new protocol for the future public-key based IP network architecture. It provides a better performance and strengthened security. However, the upper layer protocols need to use HI/HIT instead of IP address. In next section, we shall investigate the feasibility of applying HIP features to Mobile IP while keeping the impact on the existing IP networks and applications to minimum.

III. Secure Mobile IP with HIP style Handshaking and Readdressing

In the Mobile IP with Route Optimization extension scenario, when the mobile node is moving from one network into another, it will send the binding update packet to its corresponding node. However, attackers can use spoofed binding update messages to corrupt the CN's binding cache and cause packets to be delivered to a wrong address. Attackers can use this action to launch denial-of-service (DoS) to the CN, the MN, or the third party node to receive the unexpected packets. The attacker may send a fake binding update packet with the third party IP address to CN. On the receipt of this fake packet, CN re-directs the communication stream to the third party. The communication between CN and MN is broken and the third party receives a lot of unexpected packets. Moreover, the hacker can "steal" the address of MN by sending a spoofed binding update message with its own current address as the new CoA, so the hacker pretends to be a MN and continues the communication with CN. A hacker may also send two directional spoofed binding update messages to two communicating nodes which is known as a Man-in-Middle Attack[14].

To deal the attacks mentioned above, an IP address needs to be verified before the binding update. Return Routability(RR) is a mechanism for this purpose. Fig. 8 shows the Mobile IP RR mechanism.

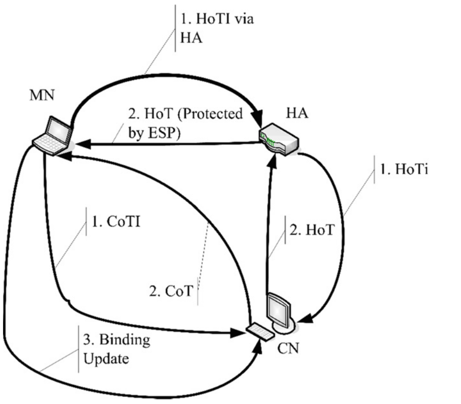


Fig. 8 Mobile IP RR mechanism

In the basic RR mechanism, four processes, Home Test Init (HoTI), Care-of Test Init (CoTI), Home Test (HoT) and Care-of Test (CoT) are needed to be processed before sending the binding update packet. MN sends the HoTI via the HA to a CN and CoTI directly to CN. CN generates a nonce every two minutes based on the key, $K_{cn,}$ which was generated when CN booted up. CN will create two tokens and send one token to the Home Address (by HoT) and one to the CoA (by CoT), so CN will reply by HoT via the HA to the MN and CoT directly to the MN. The HA will forward the HoT to the MN inside the IPSec ESP protected tunnel. MN uses both tokens to create a key, K_{bm}, to generate a Binding update packet and sends it to CN. Since CN has all the information which used to create the key, it can reproduce the key and authenticate the Binding update packet. The lifetime of the state created at the CN for the binding update is restricted to a few minutes to reduce the threat of the time shifting attack[15].

As described in the previous section, the architecture of Mobile IP with Route Optimization is similar to that of HIP. Both of them use an "agent" to redirect the initial packet and use an update message to notify the CN of the MN's current IP address. However, the Mobile IP RR heavily depends on home agents. It also creates a lot of overhead packets before handover. A state created by RR lasts only a few minutes. The RR process is required to start again in the next handover. In the following, a Secure Mobile IP (SMIP) scheme with HIP style handshaking readdressing is proposed. It is also considered as an attempt of generalizing the HIP base protocol promoted by IETF[12].

It is impossible to shift from IP based network into public-key based network without any stepping stone solutions. SMIP provides a solution with better performance than the traditional Mobile IP network. IP addresses are still used in the SMIP scheme. Home Address is generalized as an upper layer identifier (ULI), this is a permanent address of MN in the network. ULI will be used to identify the host in the upper layer, however the routing paths between the MN and the CN are based on the current MN's IP address which is mapped to ULI. The binding updates is similar to HIP, in which, the mobility mechanism is only defined in ESP mode at the moment. The initial SMIP covers the ESP mode only. Non-ESP modes will be considered in the future.

The roles of HA in Mobile IP (Home Address) and RVS in HIP (HI/HIT) are similar[12]. They provide the mapping between ULI to the current IP of the MN (CoA in the Mobile IP). In the SMIP, we integrate HA and RVS together. This enables the network to process traditional Mobile IP, SMIP and HIP at the same time. Thus, it provides the service from traditional IP network to the Credit based IP network.

Before the connection is established in SMIP, a "downgraded" HIP-style four-way handshake process will take place between MN and CN (Fig. 9). When two nodes establish the connection, the initiator sends the I1 packet with the IP address of the CN and ULI of the MN. This I1 packet can go via RVS server if necessary, in such circumstances as when the MN is in a foreign network. The responder replies to the Initiator with R1, which includes the Diffie-Hellan value. However, the puzzle used to protect the host from DoS attack and signature is optional. SPIs are exchanged during the SMIP Base Exchange. An ESP protected connection will be created. As in HIP, the ESP sequence number and SPIs are essential components in SMIP. When the CN receives the binding update packet, the address checking will be conducted to verify the IP addresses.

SAs pair is created for the communication in SMIP, the host will be verified by the SAs pair. It is more difficult to launch home address "stealing", man in middle and DoS attacks based on the spoofed binding updates because of the ESP protection. If the puzzle option in R1 and I2 is used, its defense against DoS attack will be further strengthened.

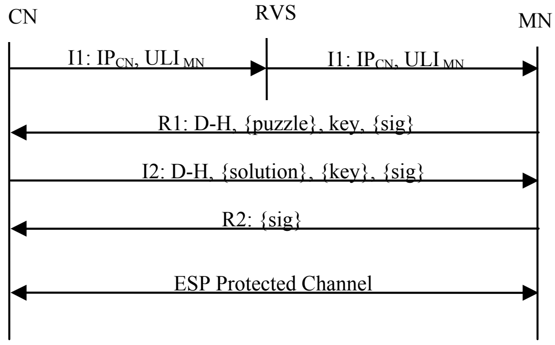

CN
RVS
MN
I1: IP_{CN}, ULI_{MN}
I1: IP_{CN}, ULI_{MN}
R1: D-H, {puzzle}, key, {sig}
I2: D-H, {solution}, {key}, {sig}
R2: {sig}
ESP Protected Channel

Fig. 9 SMIIP Base Exchange initialed by CN via RVS

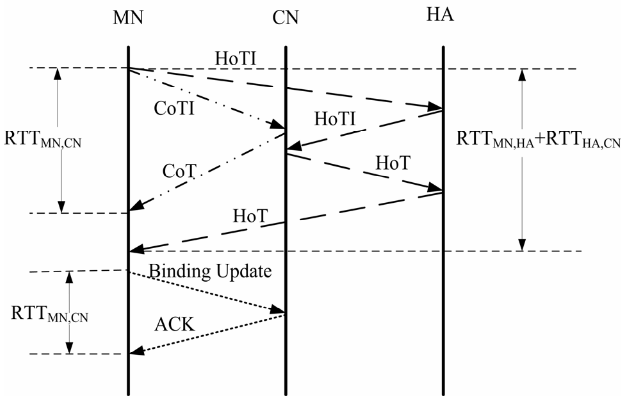


Fig. 10 RR Performance Analyses

V. Security and Performance Analysis

The performance of SMIP can be assessed on the Round Trip Time (RTT) and Binding Cost (BC). RTT is defined as the elapsed time for transmitting data over a closed path. Let $RTT_{A,B}$ represent the RTT between A and B. In Mobile IPv6, a handover requires an RR process and a binding update, it takes

$$\max\{(RTT_{MN,HA}+RTT_{HA,CN}),RTT_{MN,CN}\}+ RTT_{MN,CN}$$

to complete the process (Fig. 10). It takes only 1.5 $RTT_{MN,CN}$ in SMIP (Fig. 11). The improvement is obvious.

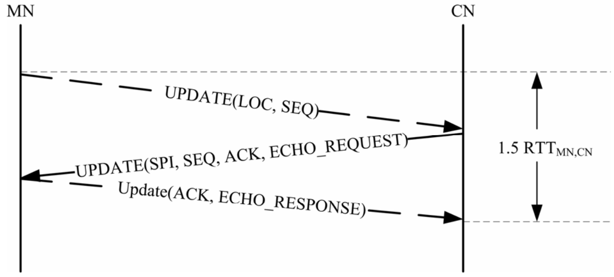

MN
CN
UPDATE(LOC, SEQ)
UPDATE(SPI, SEQ, ACK, ECHO_REQUEST)
Update(ACK, ECHO_RESPONSE)
1.5 $RTT_{MN,CN}$

Fig. 11 SMIP Readdress Performance Analyses

BC is defined as the cost of handover handling which includes the binding packet transmission and the binding computation conducted in the nodes. Before going into detail, some notions are defined in the following:

- BC_x be the total binding cost for scheme X,

- PBC_y be the binding cost incurred in process Y,
- $CP_{i,A}$ be the processing cost for process i at node A,
- $CT_{i,A,B}$ be the binding packet transmission cost in process i between node A and B.

The BC of Mobile IP is the sum of the cost of RR process and the cost of Binding Update. In the RR process, there are 4 different sub-processes, HoTI, CoTI, HoT and CoT. We can group HoTI and HoT into one combined sub-process (HT) and CoTI and CoT into another sub-process (CT). MN sends a HoTI via HA to CN. CN will generate a home nonce after it has received it and send it back to MN via HA. MN will wait for the care-of nonce in CoT to create the Binding Update packet, so

$$\begin{aligned} PBC_{HT} &= CT_{HoTI,HA,MN} + CP_{HoTI,HA} + \\ &CT_{HoTI,HA,CN} + CP_{HoTI,CN} + CT_{HoT,HA,CN} + \\ &CP_{HoT,HA} + CT_{HoT,HA,MN} \end{aligned} \tag{1}$$

As the process of HA only forwards the packets to MN and CN, so $CP_{HoTI,HA}$ is equal to $CP_{HoT,HA}$. Similarly, the transmission cost of HoTI and HoT packets are equal, so the formula can be simplified as follows:

$$\begin{aligned} PBC_{HT} &= 2\left(CT_{HT,HA,MN} + CT_{HT,HA,CN}\right) + \\ &2CP_{HT,HA} + CP_{HoTI,CN} \end{aligned} \tag{2}$$

At the same time HoTI is sent out, MN sends a CoTI to CN directly. When CN receives the CoTI, it will generate a care-of nonce and sends it back to MN directly. After MN receives both HoT and CoT, it will use the home nonce and care-of nonce to create the Binding Update packet.

$$PBC_{CT} = CT_{CoTI,MN,CN} + CP_{CoTI,CN} + CT_{CoT,MN,CN} \tag{3}$$

Similar to the HT process, the cost of CoTI and CoT packet transmission between MN and CN are close. Therefore, the cost of CT can be simplified as following:

$$PBC_{CT} = 2CT_{CT,MN,CN} + CP_{CoTI,CN} \tag{4}$$

The total cost of RR can be summarized as the sum of BC_{HT} and BC_{CT}. The cost of generation of home nonce and care-of nonce in CN are similar, so the total cost of RR is

$$\begin{aligned} PBC_{RR} &= 2\left(CT_{HT,HA,MN} + CT_{HT,HA,CN} + CT_{CT,MH,CN}\right) + \\ &2(CP_{HT,HA} + CP_{RR,CN}) \end{aligned} \tag{5}$$

The cost of the Binding Update process is the cost of generation of the Binding Update packet by home nonce and care-of nonce in MN. MS sends it to CN. CN checks the validation of the packet and replies MN.

$$PBC_{BU} = 2CT_{BU,MN,CN} + CP_{BU,MN} + CP_{BU,CN} \tag{6}$$

The cost of packet transmission between MN and CN are similar in both processes, so the BC of Mobile IPv6 handover process is the sum of PBCRR and PBCBU, that is:

$$\begin{aligned} BC_{MIP} &= 2\left(CT_{MIP,HA,MN} + CT_{MIP,HA,CN}\right) + \\ &4CT_{MIP,MH,CN} + 2(CP_{MIP,HA} + CP_{RR,CN}) + \\ &CP_{BU,CN} + CP_{MIP,MN} \end{aligned} \tag{7}$$

The BC of SMIP is less complex than Mobile IP. MN sends the Update Package with Locator parameter to the CN, CN replies MN and requests ACK for the address checking. MN replies an ACK to CN. Since all processes are based on SA, so each node only processes the packet and replies with correct parameters. The BC of SMIP is given below:

$$BC_{SMIP} = 2CP_{SMIP,CN} + CP_{SMIP,MN} + 3CT_{SMIP,MN,CN} \tag{8}$$

It has been shown in equations (1) ~ (8) that SMIP requires less BC than Mobile IP. Furthermore, in the circumstance of frequent handover, the processing overhead in Mobile IP nodes will be even higher than that in SMIP. To avoid an eavesdropping attack and time shifting attack in RR, the key and state have a limited life time. Binding update for a MN that frequently changing its IP address has higher processing cost. SMIP relies on SAs and nodes are not required to do any extra computation when a MN is moving from one sub network to another until it requires the Readdress with re-keying in the SA. It is obvious that SMIP requires less processing in binding update.

SMIP is independent of HA/RVS. In Mobile IP RR, HoT and HoTI are processed via HA, that will slow down the handover progress. The independence of HA/RVS in SMIP leads to its shorter handover delay and lower binding cost.

SMIP provides stronger security as the connection between a MN and the CN is protected by ESP. In Mobile IP RR, a connection is protected by ESP only in forwarding HoT from HA to MN.

By using SMIP, we can also benefit from the advantage of HIP, such as in Voice over IP environment. As the Home Address is generalized as an ULI in SMIP, similar to that of HIP, SIP[16] will use this ULI to identify the host. When the MN is roaming in the foreign network, it only requires using the update packet to update the routing path. “Re-invite” is no longer necessary for handover of SIP in SMIP environment[17, 18]. SIP uses ULI in the SDP message, when the SMIP update the mapping between ULI and IP address, SIP also maps the ULI to the new IP address automatically, thus, the “Re-invite” of SIP can be avoided. This can reduce the handoff signaling overhead for hybrid SIP and Mobile IP environment[17].

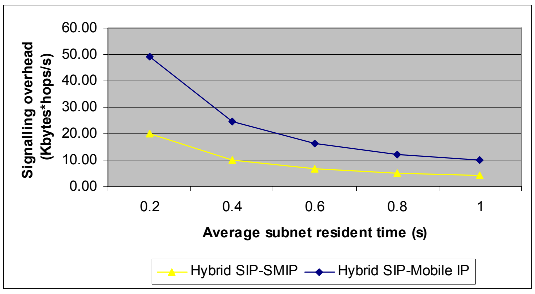


Fig. 12 Handover Signalling Overhead (Distance between MH and CH in hops = 50)

Furthermore, since Home Address is only a ULI, it can be mapped to either IPv4 or IPv6. Hence, handover between IPv4 and IPv6 network without tunneling can be achieved by using the same concept as in HIP[8].

Another new feature of SMIP is multi-homing, which is unsupported in the current Mobile IP. By using the Update packet, the MN can notify the CN with more than one interface. The process is shown in Fig. 13.

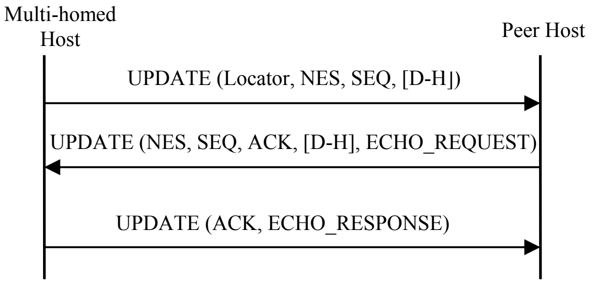

Multi-homed Host
Peer Host
UPDATE (Locator, NES, SEQ, [D-H])
UPDATE (NES, SEQ, ACK, [D-H], ECHO_REQUEST)
UPDATE (ACK, ECHO_RESPONSE)

Fig. 13 Basic Multi-homing Scenario

IX. Conclusion

In this paper we have discussed the mobility management in Mobile IP and HIP. A new mobility management scheme SMIP has been proposed. Our discussion and analysis have shown that the handover performance and security of SMIP has improved from the original Mobile IPv6. In SMIP, there is no need to modify the upper layer protocols and it can still offer excellent performance in mobility management by adopting the improved binding update process and the strengthened security. Its impact on the interconnection between IPv6 and IPv4 requires a further study. In conclusion, SMIP can be considered as an initial step in the migration from Mobile-IP-based networks to public-key based future networks.

References

[1] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," IETF RFC3775, June 2004

[2] C. Perkins, "IP Mobility Support," IETF RFC2002, October 1996

[3] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, "Host Identity Protocol", draft-ietf-hip-base-05 (work in process), Internet Draft, IETF, 02 March 2006

[4] R. Moskowitz and P. Nikander, "Host Identity Protocol Architecture", draft-ietf-hip-arch-03 (work in process), Internet Draft, IETF, 1 August 2005

[5] P. Nikander, J. Arkko, and T. Henderson, "End-Host Mobility and Multi-Homing with Host Identity Protocol", draft-ietf-hip-mm-03 (work in process), Internet Draft, IETF, 24 February 2006

[6] C. Perkins and D. Johnson, "Route Optimization in Mobile IP", draft-ietf-mobileip-optim-12 (work in process), Internet Draft, IETF, 2002

[7] P. Jokela, R. Moskowitz, and P. Nikander, "Using ESP transport format with HIP", draft-jokela-hip-esp-02 (work in process), Internet Draft, IETF, 2 March 2006

[8] P. Jokela, P. Nikander, J. Melen, J. Ylitalo, and J. Wall, "Host Identity Protocol: Achieving IPv4 - IPv6 handovers without tunneling," in *Proceedings of Evolute workshop 2003: "Beyond 3G Evolution of Systems and Services"*, University of Surrey, Guildford, UK, 2003.

[9] H. Tschofenig, F. Muenz, and M. Shanmugam, "Using SRTP transport format with HIP", draft-tschofenig-hiprg-hip-srtp-01 (work in process), Internet Draft, IETF, 23 October 2005

[10] P. Nikander and J. Laganier, "Host Identity Protocol (HIP) Domain Name System (DNS) Extensions", draft-ietf-hip-dns-06 (work in process), Internet Draft, IETF, 24 February 2006

[11] J. Laganier and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extensions", draft-ietf-hip-rvs-04 (work in process), Internet Draft, IETF, 10 October 2005

[12] T. Henderson, "Generalizing the HIP base protocol", draft-henderson-hip-generalize-00 (work in process), Internet Draft, IETF, 13 February 2005

[13] P. Nikander, J. Arkko, and T. Henderson, "End-Host Mobility and Multi-Homing with Host Identity Protocol", draft-ietf-hip-mm-02 (work in process), Internet Draft, IETF, 17 July 2005

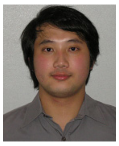
[14] P. Nikander, J. Arkko, A. T., G. Montenegro, and E. Nordmark, "Mobile IP version 6 Route Optimization Security Design Background", draft-ietf-mip6-ro-sec-02 (work in process), Internet Draft, IETF, 15 October 2004

[15] P. Nikander, T. Arua, J. Arkko, and G. Montenegro, "Mobile IP version 6 (MIPv6) Route Optimization Security Design -- Extended abstract," in *Proceedings of IEEE Semiannual Vehicular Technology Conference,VTC2003 Fall, IP Mobility Track*, Orlando, Florida, 2003.

[16] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session Initiation Protocol," IETF RFC3261, June 2002

[17] J. Y. H. So, J. Wang, and D. Jones, "SHIP Mobility Management Hybrid SIP-HIP Scheme," in *Proceedings of Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, 2005 and First ACIS International Workshop on Self-Assembling Wireless Networks. SNPD/SAWN 2005.*, Maryland, USA, 2005.

[18] H. Tschofenig, J. Ott, H. Schulzrinne, T.Henderson, and G. Camarillo, "Interaction between SIP and HIP", draft-tschofenig-hiprg-host-identities-03 (work in process), Internet Draft, IETF, 6 March 2006



Joseph Yick Hon So received his bachelor’s degree in Electronic Engineering (Information and Communication Engineering) from Hong Kong University of Science and Technology(HKUST), Hong Kong in 2003 and graduate certificate’s degree in Computer Systems Engineering from RMIT University, Australia in 2004. He has worked as Researcher Assistance in HKUST and Chinese University of Hong Kong. From 2004, he has been doing his PhD degree in RMIT University. His PhD topic deals with mobility management in the heterogeneous wireless networks.

Jidong Wang received his BE, ME and PhD in Electronic and Communication Engineering from Beijing University of Posts and Telecommunication in 1982, 1985 and 1989 respectively. From 1989~1993, he has worked as senior engineer/specialist in OmniVision Technology, USA and Ericsson Asia Pacific Laboratory respectively. He has worked as a lecturer in the Department of Electrical and Electronic Engineering, Victoria University of Technology , from 1992~1997. From 2003, Dr Wang joined School of Electrical and Computer Engineering, RMIT University, Australia, as a senior lecturer. His research areas include network management, network security and industrial informatics.

Deddy Chandra received B.Eng in Industrial Engineering from Trisakti University, Indonesia in 1999. He received M.Eng degree in 2000 and this was followed by a PhD (in the area of transport protocol for wireless networks) at Royal Melbourne Institute of Technology (RMIT) University, Australia in 2004. His research interests include transport protocol, Internet technology, fixed network, wireless and mobile networks, Ad-hoc and Sensor networks. He currently with RMIT University in Software and Network and Deakin University as Research Assistant in the area of Sensor Network.