Hybrid SIP-HIP (SHIP) Mobility Management Scheme for heterogeneous wireless IP-based network

Joseph Y.H. So[a], Jidong Wang[b]
RMIT University, Australia

Abstract

In future wireless communication networks such as 4G, different wireless technologies and architectures will coexist. In these heterogeneous network environments, mobility management is a critical issue. Session Initiation Protocol (SIP) is a widely discussed protocol, which is used for signaling and mobility management, especially in a Voice over IP (VoIP) environment. However, its mobility management is restricted to SIP sessions only. To provide a full mobility management for services in future wireless IP networks, SIP can be combined with other protocols. In this paper, a new mobility management scheme based on Host Identity Protocol (HIP) and SIP is proposed. The hybrid SIP and HIP (SHIP) scheme is for all services. SHIP has better performance in handover signaling than SIP. Its signaling overhead is smaller and the signaling delay is much shorter. SHIP has been shown to outperform hybrid SIP and Mobile IP, a widely discussed mobility management scheme, in a number of areas. Many applications can be benefited by applying SHIP, such as UMTS/WLAN integrated network.
Keywords: Host Identity Protocol (HIP), Mobility Management, SIP, vertical handover.

1. Introduction

To access wired IP networks, computers in most cases use one interface. The mobility of terminals is not an issue. However, the advancement of wireless technologies has changed the scenario. Some high-end laptops, PDA models and mobile phones have more than one wireless interface, such as CDMA, Bluetooth and Wireless LAN (WLAN) etc. Future wireless communication will not specify any particular wireless technologies as the carrier standard. It will be heterogeneous IP based networks that integrate with different wireless systems, such as Universal Mobile Telecommunications Systems (UMTS) and WLAN. For mobile devices to have seamless connection from one network to another, networks should provide efficient mobility management. So, handover handling cannot be achieved without the upper layer involvement, with mobility management being conducted on top of IP.

[a] School of Electrical and Computer System Engineering
RMIT University, Australia
joseph.so@student.rmit.edu.au
[b] School of Electrical and Computer System Engineering
RMIT University, Australia
jidong.wang@rmit.edu.au

Session Initiation Protocol (SIP)[1] is a candidate protocol for mobility management in the Application Layer of the OSI model (Layer 7). SIP was initially developed for Voice over IP (VoIP). It can be used for mobility management, which allows the data to reach the host when it changes to a new network. However, SIP can only manage the media sessions created under SIP, it cannot support the mobility management in non-SIP based services.

To break this limit, much research is carried out on integrating SIP and other protocols, such as Mobile IP, to provide a full mobility management for all applications.

Mobile IP[2, 3] is a network layer solution of mobility management. It is developed by an Internet Engineering Task Force (IETF). Mobile IP uses a "home agent" in "home" networks to redirect the packet to a new IP address that is assigned to the mobile device in its new location. The strength of Mobile IP is its backward compatibility with legacy hosts.

The fundamental problem of IP mobility is the overloading of IP addresses, i.e., an IP address identifies the device's location on the network topology in the network layer (Layer 3) and identifies the host in the transport layer (Layer 4). In current IP network architecture, when a host is moving into another network, its IP address will be changed. Mobile IP solves the problem by hiding the new IP address. It uses the home address and Home Agent (HA) for communication with other hosts. However, this structure leads to the performance problem in Mobile IP[4].

Host Identity Protocol (HIP)[5, 6] is a newly drafted secure mobility management protocol by IETF. It aims to handle IP mobility and security using a different approach. HIP introduces a new namespace – Host Identifier (HI) and a new layer – Host Identity Layer, which is seen as a 3.5 layer, i.e. a layer between a Network Layer and Transport Layers in an OSI model, into current network architecture[5, 6]. HI will replace the IP address to be the identification of the host in the Transport layer. The IP address is used to identify the location in the network only. This concept is similar to that of the SIP Universal Resource Identity (URI), which is used to identify the host of an SIP agent.

In the following chapters, the mobility management under SIP and HIP are described. A hybrid scheme SIP and HIP (SHIP) is proposed to provide the full mobility management for all applications. SHIP's performance is analyzed and compared to existing schemes. We will also

provide support on how to enhance the heterogeneous wireless network to be SHIP supported at the end of the paper.

2. Background

Mobility management was not a big issue in current wireless networks, in which most likely there was only one wireless standard used in each network. Wireless management can be handled in Data Link Layer or Physical Layer in the homogenous wireless network. Handover between different base stations and security can be achieved based on the signal strength and coding scheme. However, in the heterogenous wireless networks, different wireless technologies will be involved. Handover between different wireless networks cannot be just handled by Data Link Layer and Physical Layer. Network Layer and Application Layer are the most suitable layers for the mobility management to be positioned in future heterogeneous wireless network environments.

2.1 Session Initiation Protocol (SIP)

SIP is an application layer protocol used to create or tear down multimedia sessions. IETF recommends SIP as signaling protocol for VoIP service. It supports multi-cast and unicast. SIP URI is the namespace used in SIP protocol, which is an extension of Domain Name Systems (DNS) [1].

SIP user agent (UA) registers itself with the SIP URI in the SIP Registrar Server by the REGISTER message. When a mobile UA moves into a visited network, it will send the REGISTER to its Home Registrar about its new location.

SIP can perform mobility support in the Application Layer[7]. UA uses the INVITE message to establish a session with other UA's. The INVITE message contains session a description in Session Description Protocol (SDP)[8] format. When a callee's UA is roaming into the other network, the SIP Redirect Server will reply with SIP 302 (User Temporarily Moved) with the user's new location message to the caller UA. The caller UA will send a new INVITE message to the new location. If a mobile UA is roaming into a new network in the middle of the session, the mobile UA will use the INVITE message with the new location to re-establish the SIP session with the corresponding host. The corresponding host will update the information and acknowledge the mobile UA with its new IP address[7].

Mobility support in SIP is independent of the underlying wireless technology and network layer element. 3GPP[9] and 3GPP2[10] have adopted SIP as the session management of the mobile Internet. However, Application Layer protocol will always receive the lowest priority in the networking model and so a long delay in hand-off will occur. Furthermore, the most critical issue in mobility support by SIP is that it does not support mobility in other connections, which are not created under SIP (such as HTTP and FTP). The on-going TCP, UDP or other connections, which are not established by SIP, will be lost. SIP is the best choice for real-time application only. To support all-round mobility management, hybrid SIP and other protocols are considered by many researchers. Hybrid Mobile IP – SIP (MIP-SIP) is one of the widely discussed schemes[11, 12].

```
INVITE sip:SECE@rmit.edu.au SIP/2.0
Via: SIP/2.0/UDP proxy.rmit.edu.au:5060
To: sip:SECE@rmit.edu.au
From: sip:student1@student.rmit.edu.au
Subject: Course Enquiry
Contact: student1@student.rmit.edu.au
```

Figure 1 SIP INVITE request

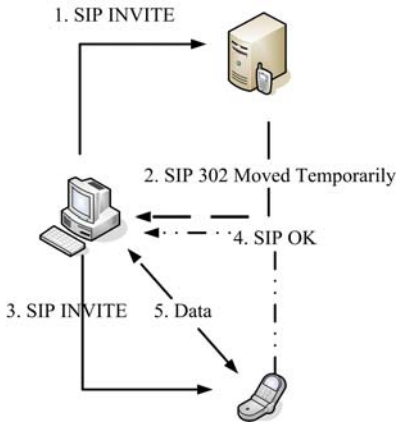


Figure 2 SIP Pre-session Mobility

SIP does not provide any security mechanism to protect the media session. SIP only focuses on the establishment and tear down of communications. Applications need to apply other security mechanisms, such as IPSec[13] and Secure Real Time Protocol (SRTP)[14], to protect the media session.

2.2 Mobile IP

Mobile IP requires minimum change on top of the IP to support mobility of network end devices. There are two different versions of Mobile IP, Mobile IPv4[2] and Mobile IPv6. Mobile IPv6[3] is inherited from Mobile IPv4, with some modifications.

A Home Address will be assigned to a MN in its Home Network. When an 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 Care of Address (CoA) address record in it's HA. When a corresponding node (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 an FA in Mobile IPv4) and forward packets to the MN. This

mechanism provides the mobility support in IP networks. However, the triangle routing has degraded the efficiency of the routing. No matter how close an MN to a CN, packets from the CN to the MN will always be forwarded via HA. Figure 3 show the triangle routing.

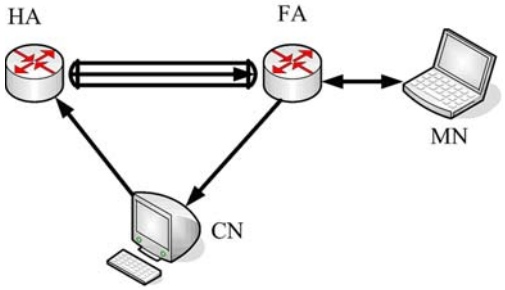


Figure 3 Mobile IPv4 and triangle routing

There are many different extensions to improve the overall performance of Mobile IP, i.e. solving the triangle routing problem. Mobile IP's with Router Optimization (RO) Extension[15] is one of the extensions to solve the triangle routing and it is part of the standard in Mobile IPv6. When an MN is roaming in the foreign network, Mobile IPv6 uses a RO mechanism to improve its performance. MN sends a binding update packet to the CN to notify its current CoA after MN has received the forward packets from HA. The CN will send all packets directly to MN after received the binding update packet from MN. The process is shown in Figure 4.

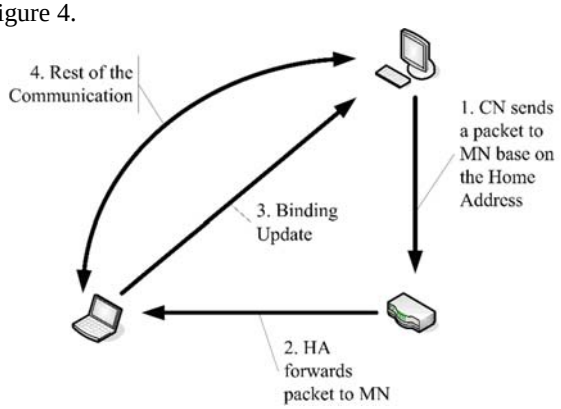


Figure 4 Router Optimization

However, middle man attack and spoofed binding update messages are security problems of the Mobile IP RO progress. 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. 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. So, an IP address needs to be verified before the handover signaling (binding update packet)[16]. Return Routability (RR) is a mechanism for this purpose. Figure 5 shows the Mobile IP RR mechanism.

In the 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 creates 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 Encapsulation Security Payload (ESP)[17] protected tunnel. MN uses both tokens to create a key, K_{bm}, to generate a Binding update packet and send it to CN. Since CN has all the information which was 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[18].

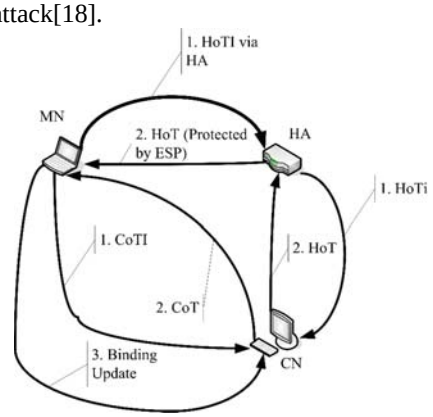


Figure 5 Return Routability

2.3 Hybrid Mobile IP – SIP (MIP-SIP)

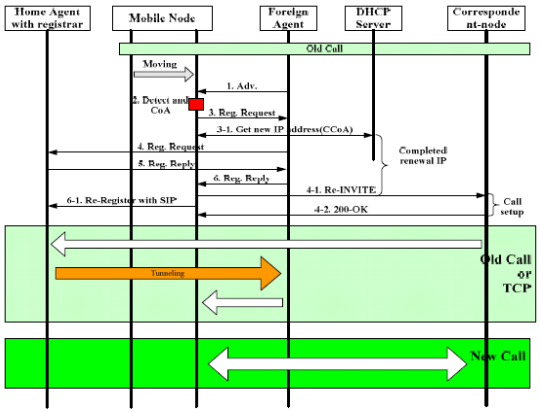


Figure 6 Hybrid Mobile IP-SIP[12]

The MIP-SIP scheme is using both Mobile IP and SIP for mobility management[11, 12]. In an MIP-SIP scheme, MIP is used to the under layer mobility management

protocol while SIP is used for the upper layer. MN will start the communication by an SIP INVITE message to establish the communication. When the MN roams into the foreign network, a packet will be forwarded by the home agent to the MN (Mobile IPv4) or Mobile IP binding update will be processed (Mobile IPv6) in order to minimize the handover delay. SIP's re-INVITE message will be sent to CN to give notice to the CN to the changing of IP address. Mobile IP has a higher priority than SIP in the network model, MN and CN still can communication with each other when SIP's re-INVITE progress is in-progress.

2.4 Host Identity Protocol (HIP)

HIP is re-modeling the current TCP/IP network architecture in order to solve the fundamental problem of IP mobility from the other angle of Mobile IP. The concept of HIP was first discussed in IETF in 1999. A HIP Working Group in IETF and a HIP Research Group in IRTF were formed in 2004. HIP is the protocol between current IP protocol and TCP/UDP in the current TCI/IP suit[5, 6]. HIP introduces two new components into current network models, which are a new namespace – Host Identifier (HI) and new layer – Host Identity Layer (3.5 layer)[6].

HI will be used to identify node and endpoint, instead of IP addresses in HIP architecture. It is a public key of an asymmetric key pair. Each host will have at least one HI, which will either be public or anonymous. But due to the various length of HI, it is not practical for HI to be used directly. In order to adopt HIP in the current IPv6 application programming interface, a 128-bit long Host Identity Tag (HIT), which contains 28 bits for the Overlay Routable Cryptographic Hash Identifier (ORCHID)[19] and 100 bits for the hash of HI, will be used to represent HI in practice[6].

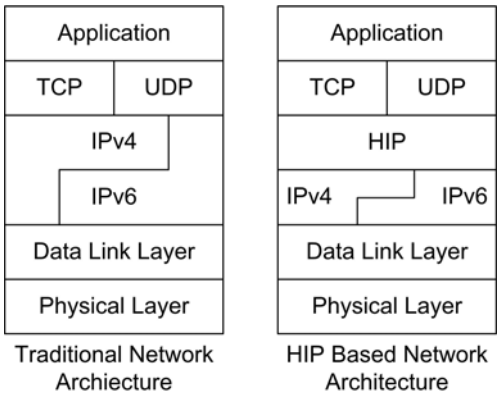


Figure 7 The difference between a Traditional Network and a HIP base Network Architecture

IPSec ESP was proposed to be used to secure the connection in the early version of HIP Internet Draft, however it had been decoupled from the HIP in the latest version[6, 20], in which support is extended to any security scheme, such as SRTP[21]. In this paper, we will focus on the IPsec ESP mode as it is well defined in the IETF HIP Working Group.

HIP uses a four-way handshake, which contains a Diffi-Hellman (DH) key exchange to establish the connection. HIP packets I1, R1, I2 and R2 are used during the four-way handshake. A session key will be created under the DH process, which is used to establish a pair of IPsec ESP Security Association (SA) between hosts. HIP uses the cookie mechanism in the four-way handshake to protect the responder from the denial-of-service (DoS) threats[6]. The detailed description about the handshake progress is as following:

- I1 is the first packet from an Initiator to a Responder. It is a trigger packet, which contains the HIT of Initiator and HIT of Responder, if known.
- R1 is the second packet in the Base Exchange and it is from the Responder to the Initiator. R1 starts the actual exchange. It contains a cryptographic challenge, which is called 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 to 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. It indicates the completion of the Base Exchange.

After the completion of the HIP Base Exchange, SAs will be created. The Security Parameter Indexes (SPIs) for the Responder-to-Initiator and Initiator-to-Responder are exchanged in I2 and R2 packets[6, 20].

HIP supports mobility management and multi-homing in nature[22]. HI/HIT will be mapped to an IP address in HIP architecture. This can be done by DNS[23] or Rendezvous server (RVS)[24]. The mapping of Fully-Qualified Domain Names (FQDN) and IP addresses is stored in DNS, in the current Internet model. DNS does not store the recent direct mapping between HIP and IP in HIP architecture. Instead, the mapping of FQDN to HIT is stored. When a host is looking up a FQDN, the DNS will reply with the IP address and HIT[23]. However, when a host is roaming, the DNS may not be able to update immediately. Based on what the common Internet Service Providers (ISP) suggests to their customers, it requires 48 – 72 hours to update all DNS records on the Internet.

```
www.example.com. IN HIP ( 2 4009D9BA7B1A74DF365639CC39F1D578
                           AwEAAbdxyhNuSutc5EMzxTs9LBPCIkOFH8cIv
                           M4p9+LrV4e19WzK00+CI6zBCQTdtWsuxKbWIy
                           87UOoJTwkUs7lBu+Upr1gsNrut79ryra+bSRG
                           Qb1slImA8YVJyuIDsj7kwzG7jnERNqnWxZ48A
                           WkskmdHaVDP4BcelrTI3rMXdXF5D
                           rvs.example.com )
```

Figure 8 DNS example of a node with a HI, HIT and one RVS[23]

Rendezvous server (RVS) is introduced to solve this problem. The role of RVS is similar to the HA in Mobile IP. DNS will no longer hold the mapping FQDN and IP address of the host; it will carry the mapping between FQDN and the corresponding RVS IP address. Direct mapping between HI and IP addresses of the host will be stored in RVS. A mobile node will register in the RVS and update its record in DNS to update the mapping to the FQDN and IP of RVS. 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. When the other host is looking up the MN in the DNS server, it will get the HIT of the MN and the IP of its RVS[24]. I1 in a four-way handshake will pass through the RVS, but the rest of the messages (R1, I2 and R2) will be communicated between two hosts directly. Pre-session mobility can be achieved by this method.

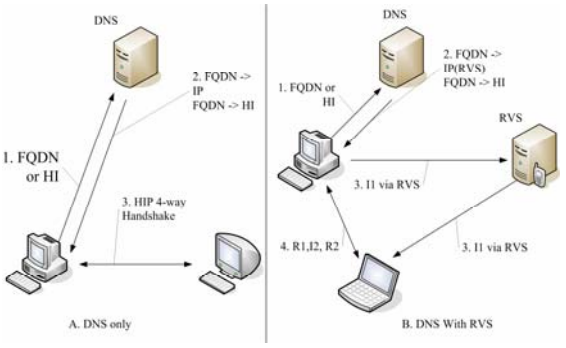


Figure 9 a) HIT-IP mapping with DNS only
b) HIT-IP mapping with DNS and RVS

Since the pair of SA's created by the 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. Mobility of HIP can be independent of ESP in future, but we will only discuss the ESP based HIP mobility in this paper.

If an MN changes its IP address during a communication session, besides the pre-session handling mentioned above, the MN will also send an UPDATE packet with a LOCATOR parameter to notify the CN. 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 a third party bomb attack[22].

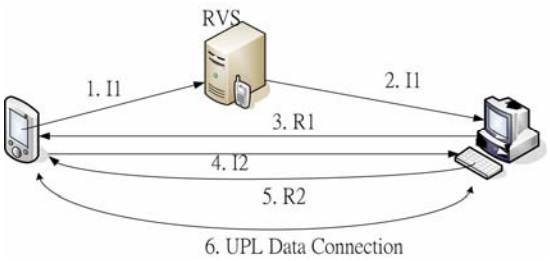


Figure 10 HIP four-way handshake via RVS

In the future wireless communication networks and mobile devices will have more than one network interface. Packets can reach the mobile device by different interfaces, which is called multi-homing. There are many different drafts in the IETF discussing the multi-homing support in an IPv6 network. HIP is one of the candidates[22, 25, 26]. In HIP, MN notifies the CN of the additional interface by using the LOCATOR parameter in the UPDATE packet. The ESP_INFO in the LOCATOR parameter will keep both "Old SPI" and "New SPI" values to indicate to the peer that the SPI is not replacing the exciting one. Besides using the UPDATE packet, nodes can also add the additional interfaces in the HIP Base Exchange.

Furthermore, HIP also supports simultaneous multi-access (SIMA)[27]. HIP uses a SIMA_FLOW_BINDING parameter in the UPDATE message for SIMA. A multi-homing host can use different network interfaces to connect with its peer on different situations. For example, in an application (or a service) the slow but reliable interface can be used for signaling packets and a high-speed (maybe unreliable) interface can be used for the data packets.

3. Hybrid SIP-HIP (SHIP)

To provide full mobility support, we propose the hybrid SIP-HIP (SHIP) scheme, which is an alternative solution to current MIP-SIP. This scheme extends SIP to support HIP.

To provide a better performance of the SHIP environment, SIP needs to be modified to support HIP in nature. In the SDP message, it will have a 'k' parameter to carry the HI/HIT as following structure[28]:

k=host-identity:<HI>

or

k=host-identity-tag:<HIT>

Figure 11 shows the example of SHIP based SIP INVITE message with SDP.

Besides the SIP needing to be extended to support HIP, we also need to enhance the functionality of HIP RVS server to provide a better performance. SIP Registrar Servers will be enhanced in HIP RVS. It can help the CN to communicate with the MN directly to utilize the setup performance, similar modification is also done in MIP-SIP scheme.

Figure 12 shows the basic scenario of SHIP procedures with the RVS server involved. SIP UA knows the HIT and wants to create a SHIP session directly. In the current SIP network model, SIP UA needs to send the re-INVITE message to a CN when a UA roams into a visiting network during the communication. In the SHIP environment, an SIP media session is created under HIP connection with HI. The header of UDP is using HIT instead of an IP address. It shows no differences for the upper layer protocols even though the IP address is changed. MN does not need to send an SIP re-INVITE message to its CN. HIP will be in charge of updating the mapping between HIT and the IP address. HIP UPDATE packet with LOCATOR parameters will be sent to the CN to notify of the IP address update. The media stream will be redirected to the new IP address after the HIP update is completed.

```
INVITE sip:SECE@rmit.edu.au SIP/2.0
Via: SIP/2.0/UDP proxy.rmit.edu.au:5060
Max-Forwards: 70
To: sip:SECE@rmit.edu.au
From: sip:student1@student.rmit.edu.au
Call-ID: a50b4c76f46738
CSeq: 218153 INVITE
Contact: student1@student.rmit.edu.au
Content-Type: application/sdp
Content-Length: ...

v=0
o=student1 63914747 4753907367 IN IP4
proxy.rmit.edu.au
s=Session SDP
t=0 0
c=IN IP4 proxy.rmit.edu.au
m=audio 3456 RTP/AVP 0 1 3 99
a=rtpmap:0 PCMU/8000
k=host-identity-
tag:6094194E04DFAFE2FA9038003D31AB2F
```

Figure 11 SHIP based SIP INVITE (with SDP)

If the SIP UA does not know its CN current location and its HIT, it can be via SHIP RVS with SIP Registrar Sever to do the address resolve and set up the call, as shown in Figure 13.

SIP signaling message (i.e. SIP INVITE, SIP 100 Trying) will be via the RVS with SIP Registrar Server to the CN. When the MN is roaming in the foreign network, MN will update its own record in the RVS with the SIP Registrar Server. When a SHIP UA wants to communicate with the MN, it will send an SIP INVITE to MN's RVS with the SIP Registrar Server to lookup the location of the MN. HI/HIT will be exchanged in the SDP message of the SIP signaling[28]. After HI's/HIT's are exchanged, the two UA's will communicate with each other directly without the RVS with SIP Register Server; a HIP four-way handshake will be established and the media session will be created. If the MN roams during the session, it will process the HIP location update which has been mentioned previously.

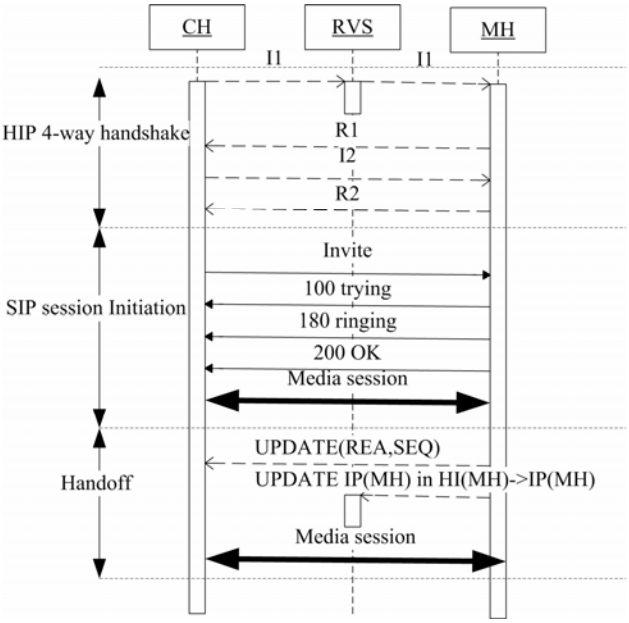


Figure 12 SHIP procedures

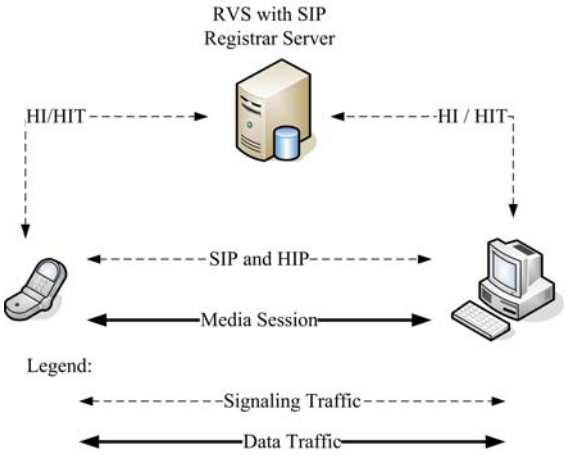


Figure 13 SHIP Based Initial connection via RVS with SIP Register Server

Compared with traditional SIP based communication, SHIP is more secure. All SHIP based communication will be protected by HIP security mechanisms, such as IPSec ESP or SRTP, so no additional security process is needed.

For other non-real time based communications in the SHIP environment, the process will be the as same as the normal HIP process.

4 SHIP Performance Analyses

4.1 Handover Signaling Analysis

Handover signaling is one of the critical factors to the performance of wireless networks. It will affect the overall handover delay. Handover signaling analysis in this part will be based on the analysis of [29], this analysis is only

focusing on the signaling of notification of change in IP address. Figure 14 shows the basic scenario of the handover process, $D_{handover} = D_{dhcp} + D_{notice}$.

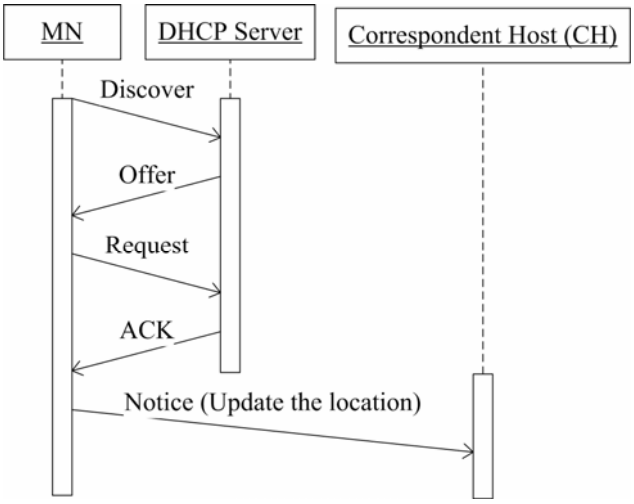


Figure 14 Handoff signaling flow

Table 1 shows the parameters and their typical value[29]. SIP and HIP are working at different layers; overhead header of lower layer protocols (LLP) is different. This analysis is focused on the notice message of the protocol itself without overhead header of LLP.

In the formula, D_{notice} depends on the distance between the MN and CN. The formula can be rewritten as follows:

$$D_{handoff} = D_{dhcp} + \left(\frac{L \times (H-1)}{BW_{wired}} + \frac{L}{BW_{wireless}} + L_{wired} + L_{wireless}\right) \quad (1)$$

Figure 15 shows the handover signaling delay. Comparatively speaking, SIP has the worst performance and Mobile IP provides the best. HIP and SHIP (they are using the same method to notify the change of IP) is slightly worse than Mobile IP. The performance of MIP-SIP is the same as Mobile IP[11, 12]. However, the MIP-SIP solution needs to use a home agent to re-direct the packet until the SIP re-INVITE progress is completed, this means, two handover processes are needed in one handover. Handover only needs to be processed once in SHIP. Handover signaling efficiency of SHIP is better than that of MIP-SIP. Due to a various packet size of HIP_SIGNATURE (typically 40 bytes) is needed for each HIP UPDATE packet (typically 80 bytes with LOCATOR, SEQ and HIP_SIGATURE)[6, 22], it makes HIP/SHIP require a longer handover signaling delay than Mobile IP and MIP-SIP .

Symbol	Meaning	Typical value
D_{dhcp}	Delay of DHCP address assignment	1s
D_{notice}	Delay for MH to notify CH of its new location	
BW_{wired}	Bandwidth of wired links	100Mb/s
$BW_{wireless}$	Bandwidth of wireless links	11Mb/s (802.11b)
L_{wired}	Latency of wired links (propagation delay + link-layer delay)	0.5ms
$L_{wireless}$	Latency of wireless links (propagation delay + link-layer delay)	2ms
H	Distance between MH and CH in hops	
L	IP packet length of notice message	140 bytes (SIP re-Invite's SDP message) 80 bytes (HIP UPDATE with REA, SEQ parameters) 56 byes (Mobile IP binding update)
Ts	Average time for which MH remains in a subnet	

Table 1 Input parameters for handover

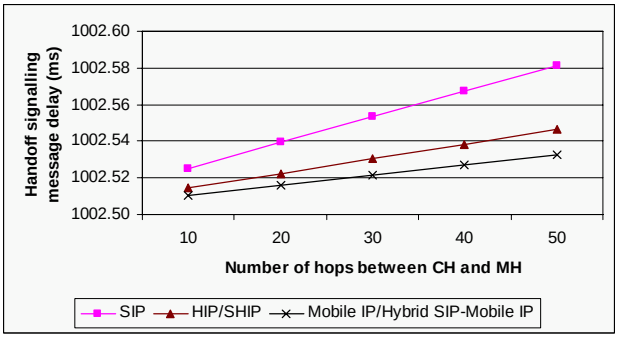


Figure 15 Handover Signaling Delay

The signaling overhead for handover can be shown by $\frac{L \times H}{Ts}$ [29]. Figure 16 shows the overhead of handover signaling of different protocols. Similar to the result of handover signaling delay, SIP has the largest overhead, while Mobile IP has the smallest one in a homogeneous protocol environment. However, SHIP is smaller in signaling overhead packets than MIP-SIP. Overhead of the MIP-SIP scheme will be the sum of the Mobile IP and SIP as two handover processes are needed in a MIP-SIP scheme.

Generally speaking, SIP has the worst performance in this analysis. SHIP has been shown to outperform MIP-SIP in major areas.

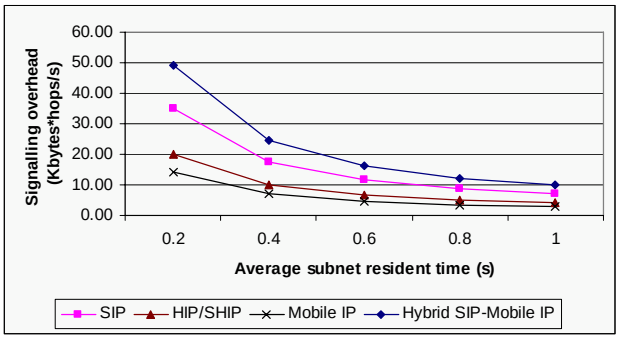


Figure 16 Handover signaling overhead (H=50)

4.2 Handover Process Delay Analysis between hybrid protocols scheme

MIP-SIP seems to outperform SHIP in the handover signaling delay, but if the token of RR process is expired, MIP-SIP needs to have an RR process to get the new tokens in order to generate the building update packet; this will be a drawback on the overall handover process. In this session, we are going to analyze the overall handover cost.

The general handover processing time is defined as

$$\text{Handoff}_{\text{process}} = T_t + T_p \qquad (2)$$

where T_t is the sum of transmission duration of all handover control packets and T_p is the processing time, including packet buffering.

The handover delay of hybrid protocol schemes is independent from upper layer protocols (SIP), it is only depended on lower layer protocols (such as Mobile IP and HIP), so in the following part, we will compare the Mobile IP and HIP directly, instead of MIP-SIP and SHIP.

The overall handover binding cost in HIP is:

$$BC_{HIP} = 2CP_{HIP,CN} + CP_{HIP,MN} + 3CT_{HIP,MN,CN} \quad (4)[30]$$

where

- BC_x is the total binding cost for scheme x,
- $CP_{x,A}$ is the processing cost for scheme x at node A,
- $CT_{x,A,B}$ is the binding packet transmission cost in scheme x between node A and B.

The overall handover binding cost of a Mobile IP scheme with an RR process is:

$$BC_{MIP} = 2\left(CT_{MIP,HA,MN} + CT_{MIP,HA,CN}\right) + 4CT_{MIP,MH,CN} + 2(CP_{MIP,HA} + CP_{RR,CN}) + CP_{BU,CN} + CP_{MIP,MN} \qquad (5)[30]$$

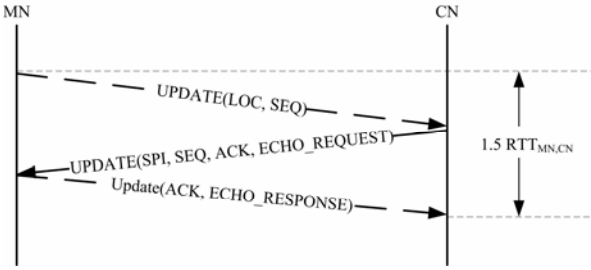


Figure 17 RTT of SHIP handover

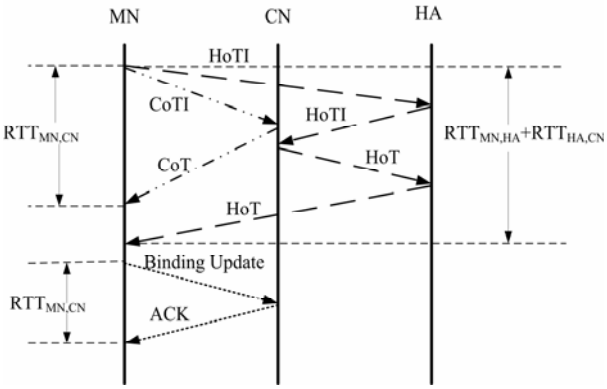


Figure 18 RTT of MIP-SIP handover

From Figure 17 and Figure 18, it is obvious that the transmission time of HIP/SHIP is less than the transmission time of Mobile IP/MIP-SIP. HIP uses 3 UPDATE packets for the whole vertical handover (handover signaling, address checking and acknowledgment), while Mobile IPv6 uses 6 packets to prepare the handover (RR process) and 2 packets to complete the handover (Binding update and acknowledgement), if tokens of RR progress are expired. In addition, MIP-SIP still needs to have an extra SIP re-INVITE message for SIP handover (MN can communicate with CN by a new IP address after Mobile IP handover, so the equation (4) does not include the extra SIP re-INVITE cost in MIP-SIP scheme). Although the handover signaling delay of MIP-SIP handover delay is smaller than SHIP, Mobile IP needs to have additional RR process to obtain tokens to generate the key, K_{bm}, for the binding update. Moreover, the RR progress of Mobile IP is more complex than the HIP progress, it is easy to find the process time of packets in Mobile IP/MIP-SIP is longer than in HIP/SHIP. So, the overall handover process performance of SHIP is better than that of MIP-SIP. SHIP can outperform MIP-SIP by 69% in vertical handover[31].

5 Application: SHIP Aware UMTS/WLAN Integrated Network

In the integrated UMTS and WLANs networks, smooth handover across two networks is targeted. We propose to use SHIP in the upper layer and the objective is to design architecture for seamless vertical handover. An RVS with a SIP Registrar Server is added into the UMTS/WLAN architecture. In an UMTS system, each GGSN has a Mobile IP home agent. As the functionality of home agents of Mobile IP is similar to that of RVS of HIP, we propose to add a RVS with SIP Registrar Server to each GGSN. This makes network management easier and the architecture is backward compatible to MNs, which do not support HIP.

In this proposed UMTS/WLAN architecture, tight coupling is used. WLAN can reuse the authentication, mobility and billing infrastructures of UMTS directly. This architecture can make routing of the packets from the CN to the network by using the same path during handover. It will minimize the effect of the external factors on handover performance. Also, additional features can be implemented in GGSN to have further improvement on the handover performance. For example, local mobility management can be added. However, that is not in the scope of this paper and will not be discussed. Furthermore, the loose coupling can also be added in the architecture for load balancing of GGSN and Internet connection backup.

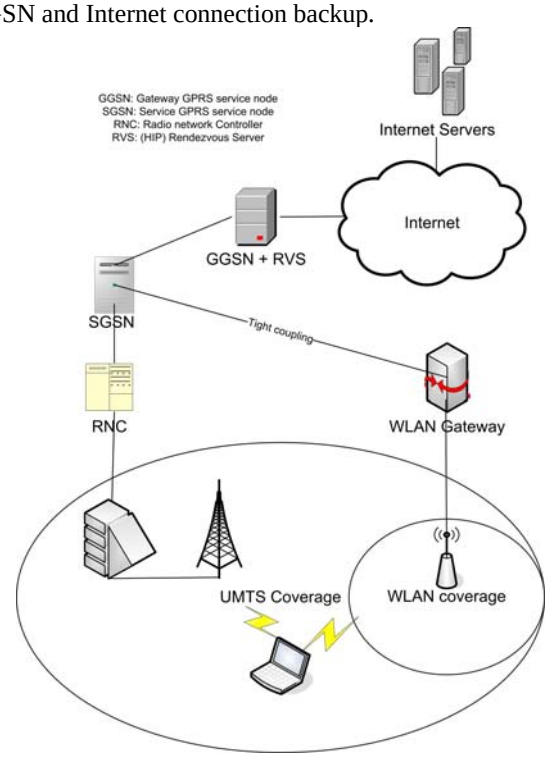


Figure 19 Integrated UMTS/WLAN SHIP based Network Architecture

An MN has at least two interfaces for the vertical handover between UMTS and WLANs. By the multi-homing feature of SHIP, the MN can use these two IP addressees for the vertical handover, by applying Make-Before-Break strategy for the handover process, the handover delay can be further improved. The original communication media session does not need to be torn down until the media session with the new interface is established, the handover delay can be tended to zero if the overlap area of UMTS/WLANs is large enough. A details mid-session SHIP handover with Make-Before-Break strategy is shown in Figure 20.

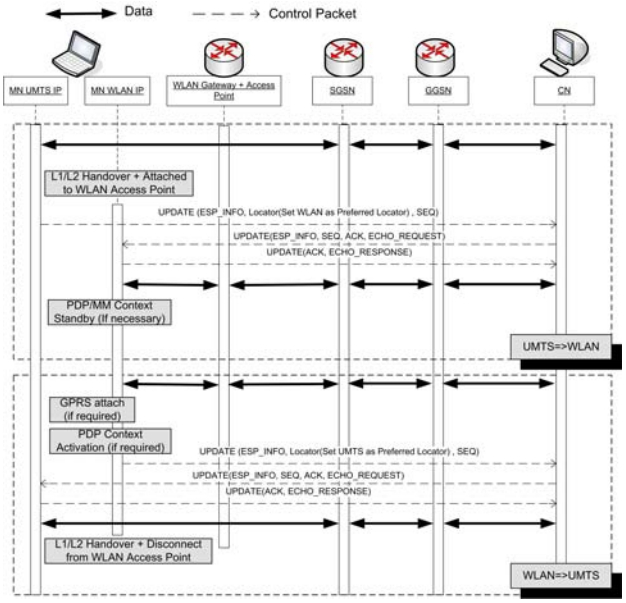


Figure 20 SHIP based vertical handover in UMTS/WLAN architecture

6 Conclusion

In this paper, we have proposed a new mobility management scheme, SHIP, for future IP based wireless networks. It is a hybrid scheme of SIP and HIP and it can provide a complete mobility management for all services.

Compared this with MIP-SIP, which is a widely discussed mobility management scheme for all services, SHIP is better in handover signal processing efficiency. In the MIP-SIP scheme, handovers need to be processed in both Mobile IP and SIP, with home agents redirecting the packets until the SIP re-INVITE process is completed. SHIP avoids the re-INVITE message in SIP and therefore, its signaling message is smaller. Beside of that handover in SHIP is less complex than MIP-SIP, as no need to verify the MN before the handover, so the overall delay of SHIP is less than MIP-SIP. In addition, SHIP provides multi-homing support, which does not exist in MIP-SIP. Its performance and functions could be further enhanced with a future version of HIP. Many applications can be benefited by applying SHIP to have a better performance, such as UMTS/WLAN integrated wireless network. We believe that SHIP can be a good candidate scheme for all-round mobility management in future wireless IP networks.

References

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, et al., "SIP: Session Initiation Protocol," *IETF RFC3261*, June 2002

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

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

[4] S. Cheshire and M. Baker, "Internet mobility 4x4," *SIGCOMM Comput. Commun. Rev.*, vol. 26, pp. 318--329, 1996.

[5] R. Moskowitz and P. Nikander, "Host Identity Protocol (HIP) Architecture," *IETF RFC4423*, May 2006

[6] R. Moskowitz, P. Nikander, P. Jokela, et al., "Host Identity Protocol", draft-ietf-hip-base-06 (work in process), Internet Draft, IETF, 15 June 2006

[7] E. Wedlund and H. Schulzrinne, "Mobility support using SIP," in *Proceedings of Proceedings of the 2nd ACM international workshop on Wireless mobile multimedia*, 1999

[8] M. Handley and V. Jacobson, "SDP: Session Description Protocol," *IETF RFC2327*, April 1998

[9] 3GPP, "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3."

[10] 3GPP2, "All-IP Core Network Multimedia Domain: IP Multimedia Call Control Protocol Based on SIP and SDP Stage 3."

[11] C. Politis, K. A. Chew, and R. Tafazolli, "Multilayer mobility management for all-IP networks: pure SIP vs. hybrid SIP/mobile IP," in *Proceedings of Vehicular Technology Conference, 2003. VTC 2003-Spring. The 57th IEEE Semiannual*, 2003.

[12] J.-W. Jung, R. Mudumbai, D. Montgomery, et al., "Performance evaluation of two layered mobility management using mobile IP and session initiation protocol," in *Proceedings of Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE*, 2003.

[13] S. Kent and K. Seo, "Security Architecture for the Internet Protocol," *IETF RFC4301*, December 2005

[14] M. Baugher, D. McGrew, M. Naslund, et al., "The Secure Real-time Transport Protocol (SRTP)," *IETF RFC3711*, March 2004

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

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

[17] S. Kent, "IP Encapsulating Security Payload (ESP)," *IETF RFC4303*, December 2005

[18] P. Nikander, T. Arua, J. Arkko, et al., "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

[19] P. Nikander, J. Laganier, and F. Dupont, "An IPv6 Prefix for Overlay Routable Cryptographic Has Identifiers (ORCHID)", draft-laganier-ipv6-khi-02 (work in process), Internet Draft, IETF, 21 June 2006

[20] P. Jokela, R. Moskowitz, and P. Nikander, "Using ESP transport format with HIP", draft-ietf-hip-esp-03 (work in process), Internet Draft, IETF, 15 June 2006

[21] H. Tschofenig, F. Muenz, and M. Shanmugam, "Using SRTP transport format with HIP", draft-tschofenig-hiprg-hip-srtp-03 (work in process), Internet Draft, IETF, 6 March 2006

[22] T. Henderson, "End-Host Mobility and Multi-Homing with Host Identity Protocol", draft-ietf-hip-mm-04 (work in process), Internet Draft, IETF, 23 June 2006

[23] 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

[24] J. Laganier and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extensions", draft-ietf-hip-rvs-05 (work in process), Internet Draft, IETF, 7 June 2005

[25] T. R. Henderson, J. M. Ahrenholz, and J. H. Kim, "Experience with the host identity protocol for secure host mobility and multihoming," in *Proceedings of Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE*, 2003.

[26] P. Nikander and T. Henderson, "Considerations on HIP based IPv6 multi-homing", draft-nikander-multi6-hip-01 (work in process), Internet Draft, IETF, 15 July 2004

[27] S. Pierrel and P. Jokela, "Simultaneous Multi-Access extension to the Host Identity Protocol", draft-pierrel-hip-sima-00 (work in process), Internet Draft, IETF, 19 June 2006

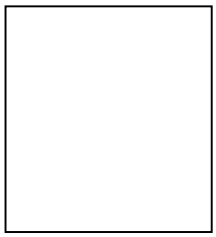
[28] H. Tschofenig, J. Ott, H. Schulzrinne, et al., "Interaction between SIP and HIP", draft-tschofenig-hiprg-host-identities-03 (work in process), Internet Draft, IETF, 6 March 2006

[29] N. Banerjee, W. Wu, and S. K. Das, "Mobility support in wireless Internet," *Wireless Communications, IEEE [see also IEEE Personal Communications]*, vol. 10, pp. 54-61, 2003

[30] J. Y. H. So, J. Wang, and D. Chandra, "Secure Mobile IP with HIP Style Handshaking and Readdressing for Public-Key Based IP Networks,"

African Journal of Information & Communication Technology, vol. 2, 2006

[31] P. Jokela, T. Rinta-aho, T. Jokikyyny, et al., "Handover performance with HIP and MIPv6," *1st International Symposium on Wireless Communication Systems, 2004*, vol. 3, pp. 324 - 328, 2004



Joseph Yick Hon So received his bachelor's degree in Electronic Engineering (Information and Communication Engineering) from the Hong Kong University of Science and Technology (HKUST), Hong Kong in 2003 and his graduate certificate's degree in Computer Systems Engineering from RMIT University, Australia in 2004. He has worked as Researcher Assistance in HKUST and the Chinese University of Hong Kong. From 2004, he is researching for his PhD degree at the RMIT University. His PhD topic deals with mobility management in 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 worked as a senior engineer/specialist in OmniVision Technology, USA and the Ericsson Asia Pacific Laboratory. He worked as a lecturer in the Department of Electrical and Electronic Engineering, at the Victoria University of Technology, from 1992~1997. From 2003, Dr Wang joined the School of Electrical and Computer Engineering, RMIT University, Australia, as a senior lecturer. His research areas include network management, network security and industrial informatics.