This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the ICC 2008 workshop proceedings.

Micro-HIP
A HIP-based Micro-Mobility Solution

Joseph Yick Hon So and Jidong Wang
School of Electrical and Computer Engineering
RMIT University
joseph.so@student.rmit.edu.au; jidong.wang@rmit.edu.au

***Abstract*— Smooth, seamless and secure handover for mobile nodes in heterogeneous wireless IP networks is the target of future mobility management. Complete mobile management solutions involve not only the physical and data link layers, but also the network layer and above. Mobility management can be classified into two categories, macro-mobility management and micro-mobility management. The former handles the movement of a node between any two IP addresses and the latter focuses on the handover between different access points under the same domain.**

Mobile IP is a widely discussed macro-mobility management protocol in the network layer. HIP is a newly proposed protocol and has been shown to outperform Mobile IP in handover efficiency. Most of the proposed micro-mobility management solutions are Mobile IP-based. There are some HIP-based micro-mobility management solutions in recent publications. However, the HIP-based proposals so far do not cover all aspects of micro-mobility management. In this paper, we have presented a complete HIP-based micro-mobility management solution, which is smoother and more efficient than any other schemes in pre-session and mid-session mobility handling.

***Index Terms*—HIP, Micro-HIP, micro-mobility management**

I. INTRODUCTION

Mobility management was not an issue in the early stage of IP network protocol design and deployment. With simplicity in mind, the IP address of a network device is used as the node's identifier and its network locator. However, with the IP network's fast expansion in the wireless sector, the handling of mobile nodes has become an important issue. When a node moves from one physical area to another, it acquires a new IP address. Ongoing applications of the mobile node require a smooth handover, i.e., the smooth switching of IP addresses from old to new, so that the applications should not sense any interruption. Additionally, the handover should not use too much of the network resources, e.g. signaling for coordinating the handover. The third consideration in the handover process is security. The handover should not increase the vulnerability of the mobile node and its applications when under potential attack. If the wireless network in question is homogenous and is using a particular wireless technology such as GPRS on GSM, then the mobility can be handled on the physical and data link layers. However, future wireless IP networks, such as the proposed fourth generation (4G) networks, will be heterogeneous. For example, in a 4G network, Wi-Fi and wideband CDMA can coexist. The integration of different wireless networks occurs on the IP level. Therefore, the network layer, and the layers above it, is required to handle the movement of the mobile nodes. The discussion in this paper refers to the mobility management in the network layer. Two representative solutions proposed so far are Mobile IP (MIP) [1, 2] and Host Identity Protocol (HIP) [3].

MIP is the most widely discussed mobility management protocol. It requires minimal addition to fixed IP network architecture. Each mobile node is signed with a home agent which traces the movement of the mobile node. The new IP address is hidden from the corresponding node (CN). The CN uses the MN's home address to communicate with the MN and the home agent is responsible for forwarding the invitation of the CN to the MN's foreign IP address, so that the connection between the CN and the MN can be established. HIP is another mobility management protocol that breaks the dual roles of an IP address as the identifier and the locator of a mobile node. In HIP, a Host Identifier (HI) is introduced as the identifier of a node. The IP address is only used for its location. HIP has been shown to offer more efficient handover than MIP [4].

Mobility management can be divided into macro-mobility management and micro-mobility management. In macro-mobility management, handover between any two IP addresses is treated equally. The movement of the mobile nodes can be either within a domain or across domains. Micro-mobility management handles the MN's handover within a domain. Both MIP and HIP are initially proposed as macro-mobility management protocols. However, in the scenario of an MN's micro movement, the path from the CN to the network gateway of the MN's domain remains unchanged for the MN's intra-domain handover. A macro solution can be used but the signaling message to the CN (indicating the micro handover) is unnecessary. The intra domain handover can be handled internally and there is no impact on the CN. In other words, the movement of an MN within a domain is hidden from the CN. This local handover processing can reduce the handover latency and keep the movement of an MN within a specific domain confidential to the outside world. Most micro-mobility protocols are MIP-based, e.g. Cellular IP [5]. There are discussions and proposals on HIP-based micro-mobility management [6, 7] but these provide partial

978-1-4244-2052-0/08/$25.00 ©2008 IEEE

solutions. The performance of intra-domain handover has been improved but they have not covered all the functionalities or extensions in detail.

In this paper, we introduce Micro-HIP (mHIP), a micro-mobility solution for HIP. mHIP is inherited from HIP. It introduces new network components into the network architecture. The performance of the intra-domain handover is improved and goes the HIP security level. Besides is, the load of handling intra-domain handover signaling is disturbed among the network. Finally, our scheme can be further extended and developed to support future HIP development. The remainder of this article is organized as follows. Firstly, we briefly describe HIP. Secondly, we mention some related works. Thirdly, we introduce our micro-mobility solution of HIP: mHIP. Finally, we offer an analysis of mHIP.

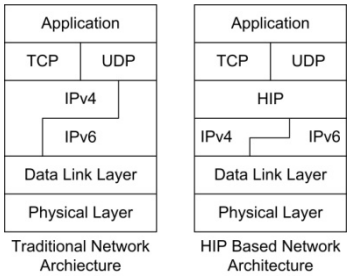

Figure 1: The difference between a Traditional Network and HIP-based Network Architecture.

II. Host Identity Protocol

Host Identity Protocol (HIP) [3, 8] is a new experimental protocol for next generation IP-based networks. HIP provides a secure, mobile and multi-homing environment [9] for IP-based networks. The problem of mobility management of IP networks is the dual roles of the IP address. HIP introduces a 3.5 layer protocol (Host Identity Layer) into the ISO model, as shown in Figure 1. HIP also introduces a new namespace called Host Identifier (HI) to be the node identifier, and the IP address is only for the network locator in the HIP network architecture. HI is a cryptographic public key but the lengths of public keys of various algorithms are different, which is not practical. A 128-bit-long Host Identity Tag (HIT), which contains 28 bits for the Overlay Routable Cryptographic Hash Identifier (ORCHID) and 100 bits for the hash of HI, will be used to represent HI in practice. The upper layer protocols will use HIT instead of the IP address for the node identifier. The mapping of the HIT and IP address can be done by DNS [10] or Rendezvous Server (RVS) [11]. For the higher mobility environment, RVS is recommended for mapping instead of DNS. HIP is currently only a secure signaling protocol that creates, updates or tears down the secure channel. In theory, it can use any secure protocol for upper layer communication, but Internet IP Security (IPSec) Encapsulation Security Payload (ESP) is the only protocol that is well defined in HIP. In this paper, we will only discuss the HIP IPSec ESP scheme [12].

A. HIP Base Exchange

HIP Base Exchange (BE) [8] is necessary for any HIP-based communication. BE is a four-way handshaking process, that contains a Diffi-Hellman (DH) key exchange to establish the HIP connection. A session key is created under the DH process. This session key is used to establish a pair of IPSec Security Associations (SA) between hosts during the HIP BE. A cookie mechanism is used in the BE to protect the responder from denial-of-service (DoS) threats.

B. Mobility and Multi-homing

In theory, HIP mobility and multi-homing are independent from any protocols but only the HIP ESP mobility scheme has been well defined so far.

Since the pair of SAs created by BE are not bounded to the IP address but to the HIT, a host can receive packets that are protected by SA from any IP addresses. After the handover in the lower layers is complete, the MN sends a HIP UPDATE packet with a LOCATOR parameter to its CNs to notify the change of IP address. CN uses the UPDATE packet with an Addressing Check (AC) parameter to request an address check. Once the MN replies to the address check, the handover is complete. The HIP UPDATE packet is protected by the HIP security mechanism, so it does not need any additional mechanisms to guard against security threats, such as Return Routability [13] in Mobile IP.

Multi-homing allows a host to receive packets from different network interfaces by using one host identity. MIP does not support multi-homing. HIP uses HIP UPDATE packets or HIP BE packets to notify the CN about the additional interface.

III. HIP-Based Micro-Mobility Management

The overall handover performance of HIP has proved better than MIP. HIP outperforms MIPv6 by 69% in the handover between UMTS and Wireless LAN networks [4]. HIP can co-operate with other protocols to provide better communication performance [14]. Additionally, HIP provides a secure environment and multi-homing support for data communication in an IP-based network. Therefore, HIP is a potential candidate for mobility management in future heterogeneous wireless IP-based networks, such as the 4G network.

Although the performance of HIP is better than MIP, HIP is a new draft protocol. Most of the micro-mobility management protocol is based on MIP thus far. There is no complete micro-mobility management solution for HIP but some related works or partial solutions are presented.

A. Current Works

1) Ylitalo's Scheme

Ylitalo et al. of Ericsson Research NomadicLab have discussed the security of IP-based micro-mobility [7]. They proposed Lamport one-way hash chains and secret splitting techniques to implement secure micro-mobility management for IP-based networks. The details of intra-domain handover operations are shown in Figure 2. The scheme is based on the split secret key. However, this solution is not a good micro-mobility management model. It requires the MN to perform a global handover to distribute the split secret key to the AP. Intra-domain handover is impossible to perform

immediately after boot up. Moreover, if the Lamport one-way hash chain reaches the seed value, a global handover is required to create a new Lamport one-way hash chain. Furthermore, all APs need to upgrade to non-dumpy APs, otherwise hackers can set up sniffers to learn split secret keys to perform a Man-in-Middle attack.

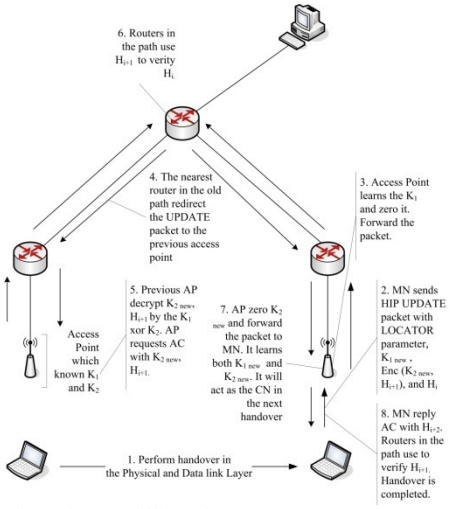

Figure 2: Ylitalo's micro-mobility scheme

Ylitalo's scheme only focuses on the security issue; it does not consider details regarding HIP-based micro-mobility support. The MN still needs to update its information in RVS during the handover. Ylitalo's scheme does not fulfill the requirement of micro-mobility management; it is only a partial solution.

2) Novaczki's Scheme

Novaczki et al. of Budapest University of Technology and Economics have suggested an alternate solution [6]. Local RVS (LRVS), which acts as Mobile Routing Point (MRP) – a micro-mobility management scheme enhanced router, is introduced in their scheme to provide a micro-mobility management scheme for HIP. Their concept is similar to the foreign agent in MIPv4. An MN needs to register itself not only in RVS, but also in LRVS. When an MN performs a handover, it will notify LRVS instead of the CN, to redirect all HIP-based communication streams into its new address. Compared with Ylitalo's scheme, Novaczki's scheme is more comprehensive. The aim of Novaczki's scheme is to provide a micro-mobility solution for HIP. However, they do not discuss the multi-homing scenario in their paper. Moreover, their scheme is based on the IPSec scheme only. In addition, the load of LRVS would be very heavy if there were many MNs in the network.

One of the challenges of developing micro-mobility solutions for HIP is retaining the security level of HIP without degrading the handover performance. Novaczki's scheme only introduces a single network component – LRVS – which re-uses the HIP security mechanism of RVS. Nevertheless, the load of LRVS would be very heavy. Ylitalo's scheme attempts to provide a local balancing solution, using secret splitting techniques and a Lamport one-way hash chain to maintain the security level. However, even though the handover performance is improved, it is still not optimized or completed.

The HIP header is the other challenge in the development of HIP-based micro-mobility management. There is no HIP header in the HIP data packet. The HIP header only exists in the HIP signaling packet and the HIP conceptual data packet. The IPSec header is followed by an IP header in the HIP data packet. In practice, there is no difference between a normal IPSec data packet and an HIP-based IPSec data packet. These structures are shown in Figure 3.

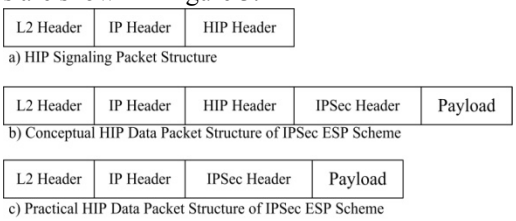

Figure 3: HIP Packet Structure

In the next section, we introduce our novel HIP micro-mobility scheme, which comes with load balancing in the network components and provides better handover performance while retaining the security level.

B. Micro-HIP

Micro-HIP (mHIP) is a novel micro-mobility management solution for HIP. mHIP is an extension of theHIP protocol that reduces the unnecessary signaling and control messages to the external world.

1) mHIP Network Architecture

New network entries of mHIP, which are called mHIP agents, are introduced to the current HIP architecture. There are two different types of mHIP agents: mHIP gateways and mHIP routers. The main roles of the mHIP agents are to handle signaling messages of the intra-domain HIP handover, and to re-direct the HIP-based connections to the correct location. All mHIP agents in the same network can sign the message on behalf of the group. This feature will be discussed below.

a) mHIP Agent

All the network middle boxes enhanced by mHIP are called mHIP agents.

mHIP agents are the MRPs in the mHIP architecture. mHIP agents map the HIT with the intra-domain IP address. mHIP agents under the same network domain can sign messages on behalf of the group. Beside their own HITs, all mHIP agents will share a common HIT to represent the whole mHIP domain. The MN can verify the signature of the group. Similar to the property of HI, the mHIP agent only provides a framework of different signature schemes, such as: Shared Private Key scheme, Group Signature scheme [15], Ring Signature scheme [16] and Proxy Signature scheme [17].

When an MN sends an UPDATE packet to perform an intra-domain handover, the closest mHIP agent that contains the MN information will receive this UPDATE packet and will act as a CN to reply to the UPDATE packet. The MN verifies the reply message if it is from an authorized agent and the mHIP agent will sign the message using the signature scheme of the group.

b) mHIP Gateway

The role of the mHIP gateway is similar to LRVS in Novaczki's scheme. The mHIP gateway is the root of mHIP routers. HIP Network Address Translation (NAT) [18] will also serve as the functionality of the mHIP gateway to provide NAT services of HIP. The mHIP gateway keeps the information of the MN in the domain. The MN needs to register itself in the mHIP gateway. When the mHIP gateway receives the HIP data or signaling packets, it will re-direct those packets to the MN. As well, the mHIP gateway will be the authorization agent of the mHIP domain, and mHIP routers need to be authorized by the mHIP gateway for the different signature scheme. After an mHIP router is authorized, the mHIP gateway will pass the necessary information to the mHIP router, which lets the mHIP router sign the message on behalf of the group.

c) mHIP Router

The mHIP router is a 3.5 layer router, which redirects HIP-based communication to the current MN location. In addition, mHIP routers can also handle the intra-domain handover signaling so that the handover latency is reduced and load of the mHIP gateway is also reduced. Figure 4 shows the simplified mHIP architecture.

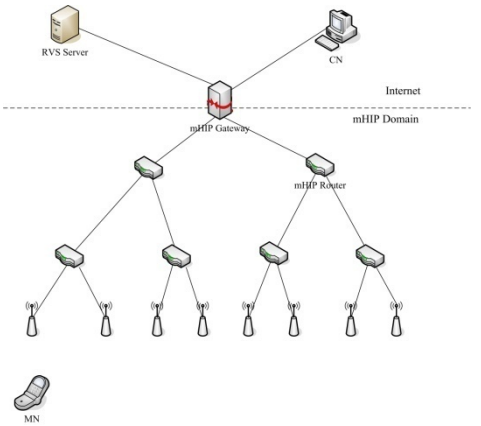

Figure 4: mHIP Architecture

2) Initiation

When an MN enters an mHIP domain network, the MN needs to register itself in the mHIP gateway. Similar to Novaczki's scheme, APs periodically send out the modified ICMP advertisement messages that contain the HIT and IP address of the mHIP gateway. The MN uses the HIP registration process to register its HIT and IP address at the mHIP gateway. The mHIP gateway and the MN also exchange information, which allows the MN to verify the message signed by any mHIP agents in this domain during registration. All mHIP gateways on the path also learn both the HIT and IP address of the MN, or the next hop of the mHIP agent, simultaneously. The MN registers itself with the HIT of the mHIP gateway in its RVS.

3) Idle Intra-Domain Handover/Paging

When the MN performs the intra-domain handover without any active connections, the MN sends an UPDATE packet to the mHIP gateway to notify the change of IP address. The UPDATE packet is processed by the nearest mHIP agent, which is on the path between the mHIP gateway and the old location of the MN (NmHIPA). NmHIPA requests the address check and signs the UPDATE packet using the signature of the group scheme adopted in the network. The MN can then verify the packet is issued by the authorized mHIP agent in this network. The MN replies to the address check and the intra-domain handover process is complete. The mHIP agents on the path that did not previously know the MN, learn the HIT of the MN and the IP address of the MN or the next hop of the mHIP agent. NmHIPA also notifies their neighboring mHIP agents to update the record of MN. Those mHIP agents that are no longer in the path between the mHIP gateway and the MN, delete the MN record and notify their neighboring mHIP agents to update their records.

The mHIP agent closest to the AP broadcasts ICMP packets from time to time. When the MN receives this ICMP packet, the MN sends a HIP NOTIFY packet to the mHIP gateway to notify that it is still alive in the network. The closest mHIP agent receives and handles this message. If the closest mHIP agent does not receive a HIP NOTIFY packet for a specific MN after timeout, it removes the record and notifies the mHIP gateway about it. mHIP routers on the path will remove that MN record and forward the packet to the mHIP gateway, unless it knows that the handover was performed by the MN.

The above mechanisms can keep the mapping between the HT and IP address of the MN up to date. The load is dispersed among the mHIP agents in the network, and load balancing for the mHIP gateway is achieved.

4) Handover with Active Connections and Multi-homing

HIP BE is required before every HIP-based communication is established. When the CN wants to start communication with the MN, the CN will get the MN's RVS server from the DNS server. The CN starts the HIP BE with the MN via RVS. RVS forwards the HIP I1 packet to the mHIP gateway. I1 is forwarded to the MN using the mapping information in the mHIP agents. The rest of BE will operate via a similar process. The mHIP gateway and routers learn the information of the HIP communication. mHIP is a protocol that is able to extend so that it supports any HIP-based communication. In the remainder of this session, we discuss the handover in HIP ESP scheme; the only schemes that are well defined at this moment.

In theory, every HIP communication is with the HIP conceptual header, as shown as Figure 3(b). This HIP conceptual header is between the IP header and the header of the upper layer protocol, which has the source HIT and destination HIT. However, in practice, unlike the HIP signaling packet, there is no HIP header in the HIP data packet. The IPSec ESP header is the only header that can be used to identify the packet. mHIP agents remember the mapping between the source (CN) IP address and the Security Parameters Index (SPI) to map the IP address of the MN and provide the mHIP service. A modified SPINAT [19] device will be implemented in the mHIP gateway and mHIP routers to allow the overlay routing based on SPI.

Figure 5 shows the mHIP handover mechanism. The MN sends an UPDATE packet to the CN during the handover.

Similar to mHIP paging, NmHIPA will handle this UPDATE packet instead of the CN in the mHIP domain. NmHIPA replies to the MN UPDATE packet by requesting an address check. It signs the packet using the signature of the group. The intra-domain handover is complete after the MN replies to the address check. NmHIPA updates the mapping between HIT, the SPI, and the IP address of MN. NmHIPA will also notify its neighboring mHIP agents about the change of IP address for certain SPIs of HIT. Those mHIP agents in the path also learn the mapping during the handover. The HIP communication stream of the MN uses the new mapping to send to the new location.

Multi-homing is similar to the handover. The MN sends information to the UPDATE packet about the new interface; the NmHIPA will learn about it and forward it to the new interface.

The mHIP handover is based on the connection instead of the interface. Using our scheme, the MN is able to perform a handover for all connections, or partial connections, by moving them from one interface into another. Multi-homing can be achieved using the basic HIP mechanism, which performs handovers for a specific connection by assisting mHIP agents in the mHIP domain.

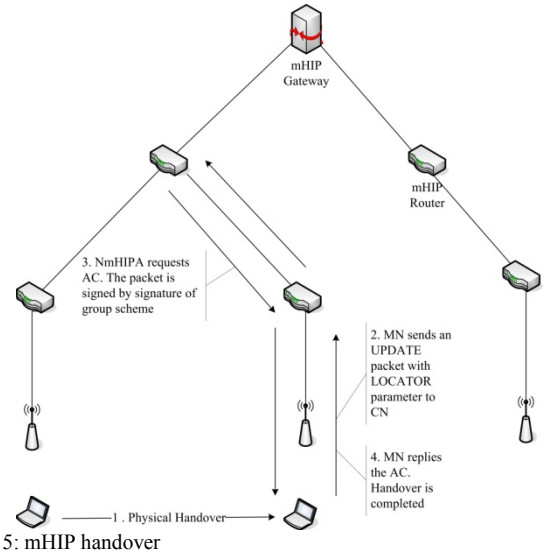

Figure 5: mHIP handover

IV. Performance Analysis

In this section, we present an analysis of mHIP performance. mHIP provides a framework in which any number of security schemes can be adopted. The performance will vary when different security schemes are applied, so we assume that the computation performance power of all nodes in the network, such as gateway and MN, is very strong; the delay related to computation (e.g. the processing delay) tends towards zero. Our analysis only focuses on the delay in the network transmission. We use Round Trip Time (RTT) as the measure for the propagation delay. One RTT is defined as the time required for the source transfer to and from the destination. We use $RTT_{A,B \text{ via } C}$ to represent the RTT between node A and node B, which is via node C and $RTT_{A,B}$, to represent the packet sent directly from A to B. In addition, RTT is also based on cross over distance between the source and the destination, for example the number of hop in between.

mHIP, and all related work, is targeted at providing a better handover performance environment than HIP for the micro-mobility environment. All schemes aim to reduce the signaling to the external network. The CN and RVS are not notified for the intra-domain handover process.

We now present the analysis of the performance of pre-session mobility and mid-session mobility. Pre-session mobility can be defined as the way in which the CN establishes a connection with the MN when it moves into a new location. Mid-session mobility is the handover performed in the middle of communication. We will also compare the performance with Ylitalo's scheme and Novaczki's scheme.

A. Performance of Pre-session Mobility

The MN uses the HIP UPDATE packet to notify the mHIP gateway about the change of IP address instead of updating the RVS record in our proposed mHIP scheme. NmHIPA will handle this packet. In the worst case, the mHIP gateway is NmHIPA. The mHIP gateway is located at the normal gateway to the external network. HIP uses three packets to complete the whole handover, so the handover latency of pre-session mobility is 1.5 $RTT_{MN,NmHIPA}$, which is smaller or equal to 1.5 $RTT_{MN,Gateway}$.

Compared with other schemes, the mHIP solution is an improvement. Ylitalo's scheme does not fulfill the requirement of micro-mobility support; the MN needs to notify its RVS about the change of the IP address. The performance is the same as the HIP solution. In Novaczki's scheme, the MN needs to notify the LRVS, which is also located as a gateway to the network. Unlike our mHIP scheme, the HIP signaling packet must be processed by the LRVS. So, it takes 1.5 $RTT_{MN,Gateway}$ to complete the handover. Therefore, our scheme outperforms the other two schemes in terms of pre-session mobility.

B. Performance of Mid-session Mobility

The mid-session handover performance of Novaczki's scheme is the same as the pre-session handover. All the intra-domain handover signaling packets are handled by LRVS. The MN sends the UPDATE packet to LRVS, notifying the change of IP address for the mid-session handover.

Unlike Novaczki's scheme, Ylitalo's scheme and mHIP distribute the load to other network devices. The nearest MRP in the old path (NROP) takes an important role in both schemes. The MN sends the UPDATE packet to the CN to notify the change of IP. In Ylitalo's scheme, NROP redirects this UPDATE packet to the PAP to handle this signaling packet. This takes 1.5 $RTT_{MN,PAP \text{ via NROP}}$.

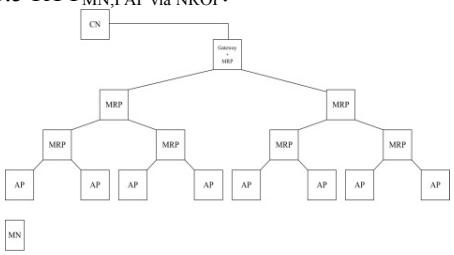

Figure 6: Balanced Binary Tree Structure with three-level depth

In our proposed mHIP scheme, the NmHIPA is the NROP.

The intra-domain handover signaling is handled by NROP instead of being forwarded to other nodes in the network. The mid-session handover signaling delay is only 1.5 $RTT_{MN,NROP}$.

If the domain network is followed as a tree structure and all the APs are leaf nodes at the same level, such as the balanced binary tree in Figure 6, the distance between PAP and NROP is the same as that between AP and NROP. If the links between nodes are identical, the cross-over distance of the HIP UPDATE packet in the mHIP scheme is 50% less than Ylitalo's scheme, because the HIP UPDATE packet is processed in the NROP. Figure 7 shows the result of the simulation of the average cross-over distance of the HIP UPDATE packet of mid-session mobility for different schemes in the same handover with different levels of balanced binary tree structures. We found that the average crossover distance of the HIP packet in Novaczki's scheme is shorter than Ylitalo's scheme at a depth of level four, and mHIP requires the least distance.

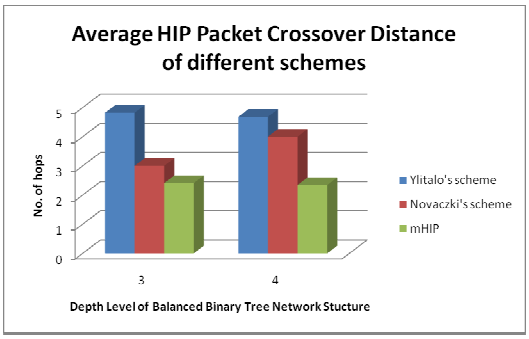

Figure 7: Simulation results for average cross over distance of HIP UPDATE packet transfers in different depth levels of Balanced Binary Tree structure of different schemes.

Overall, mHIP provides better performance in terms of pre-session mobility management and mid-session mobility management, and reduces the load of the gateway for the micro-mobility management environment of HIP.

Table I: Handover Performance Summary of Different Schemes

	Pre-session Handover	**Mid-session Handover**
Ylitalo's scheme	N/A, same as HIP	$1.5RTT_{MN,Pre\ AP} = 1.5RTT_{MN,NROP} + 1.5RTT_{NROP,Pre\ AP}$
Novaczki's scheme	$1.5RTT_{MN,Gateway}$	$1.5RTT_{MN,Gateway}$
mHIP scheme	$1.5RTT_{MN,NmHIP}$ ($<=1.5RTT_{MN,Gateway}$)	$1.5RTT_{MN,NROP}$ ($<=1.5RTT_{MN,Gateway}$)

V. Conclusion

Mobility management in wireless IP networks deals with the problem caused by the dual roles of IP addresses, i.e., node identifiers and their network locators. MIP and HIP are two mobility management solutions that use different strategies. Handover efficiency of HIP, the newer of the two, is better than MIP in macro-mobility management, for which HIP was initially proposed. The study on HIP-based micro-mobility management has just started, with limited, partial solutions published recently. We have introduced a complete HIP-based micro-mobility management protocol: mHIP. It supports all existing functionalities and features offered by HIP. It can also extend to accommodate the future evolution of HIP. In mHIP, one or more mHIP agents in a local area network are introduced to handle the intra-domain handover, update signaling and load balancing. mHIP has better handling in both pre-session and mid-session signaling than any other proposals found so far. With its consideration of various aspects of possible HIP development in the future, mHIP provides a sound architecture for micro-mobility management in future HIP-based wireless IP networks.

References

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

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

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

[4] 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 - 28, 2004.

[5] A. G. Valko, "Cellular IP - A New Approach to Internet Host Mobility," *ACM Computer Communication Review,* vol. 29, pp. 50-65, Jan 1999.

[6] S. Novaczki, L. Bokor, and S. Imre, "Micromobility support in HIP: survey and extension of host identity protocol," 2006, pp. 651-54.

[7] J. Ylitalo, J. Melén, P. Nikander, et al., "Re-thinking Security in IP-based Micro-Mobility," in *Proc. of the 7th Information Security Conference (ICS'04)*, Palo Alto, CA, USA, 2004, pp. 318-29.

[8] R. Moskowitz, P. Nikander, P. Jokela, et al., "Host Identity Protocol", draft-ietf-hip-base-08 (work in process), Internet Draft, IETF, 11 June 2007

[9] 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

[10] P. Nikander and J. Laganier, "Host Identity Protocol (HIP) Domain Name System (DNS) Extensions", draft-ietf-hip-dns-09 (work in process), Internet Draft, IETF, 13 April 2007

[11] 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

[12] P. Jokela, R. Moskowitz, and P. Nikander, "Using ESP transport format with HIP", draft-ietf-hip-esp-06 (work in process), Internet Draft, IETF, 11 June 2007

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

[14] J. Y. H. So, J. Wang, and D. Jones, "SHIP Mobility Management Hybrid SIP-HIP Scheme," in *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, p. 226.

[15] D. Chaum and E. v. Heyst., "Group signatures," *Advances in Cryptology -- EUROCRYPT '91,* vol. 547 of Lecture Notes in Computer Science, pp. 257- 65, 1991.

[16] R.L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," *Advances in Cryptology-Asiacrypt 2001,* pp. 552-65, 2001.

[17] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signature: Delegation of the power to sign messages," *IEICE Trans. Fundamentals,* vol. E79-A, pp. 1338-53, Sep. 1996.

[18] M. Komu, S. Schuetz, M. Stiemerling, et al., "HIP Extensions for the Traversal of Network Address Translators", draft-ietf-hip-nat-traversal-01 (work in process), Internet Draft, IETF, 5 March 2007

[19] J. Ylitalo, P. Salmela, and H. Tschofenig, "SPINAT: Integrating IPsec into Overlay Routing," in *First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005*, 2005, pp. 315-26.

View publication stats