Secure Mobile IP with HIP Style Handshaking and Readdressing

Joseph Yick Hon So, Jidong Wang
School of Electrical and Computer Engineering
RMIT University, Australia
s3071310@student.rmit.edu.au; Jidong.wang @rmit.edu.au

Abstract

Mobile IP allows the mobile node roaming into a new IP network without losing its connection with its peer. Mobile IPv6 is using Mobile IP with Route Optimization to improve performance by avoiding the triangle routing 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 by its new namespace. Its architecture is similar to that of Mobile IP with Route Optimization. In this paper, we have introduced a Secure Mobile IP with HIP Style Handshaking and Readdressing (SMIP), which has stronger security, better performance and lower binding cost in binding update process compared with Mobile IPv6. The dependence of home agent in the new scheme is also shown dramatically decreased. The initiated scheme integrated the primary features of two completely different mobility management solutions and has set up a migration path from mobile-IP based solution to a public-key based solution in mobile IP networks.

1. Introduction

Wireless networks grow rapidly in recently years with advent of new wireless technologies. Both communication networks and computer networks have evolved into hybrid wire and wireless environments and gradually merging together. However, the existing network models and protocols were originally designed for wired networks and some assumptions made are aimed to simplify the network design. For instance, in the current TCP/IP suit, endpoint identifiers are same as network topological locators and IP address takes the dual roles. This feature is not efficient in handling mobility, the dominant issue in wireless IP networks. Many different schemes have been proposed to enhance current network model's support to mobility. Mobile IP [1, 2], the most popular scheme is developed in Internet Engineering Task Force (IETF) and is based on the idea of providing mobility support on top of current TCP/IP architecture without any modifications to the upper layer protocols. Mobile IP is a practical solution even its performance still has potential for further improvement. Host Identity Protocol (HIP) [3] is a new experimental protocol of 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. 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. As there is no support to HIP in the current commercial networks and existing applications, Mobile IP still is the main player in mobility management. In this paper, we are trying to apply some concept of HIP to Mobile IP aiming to improve its performance especially on handover. Our proposal can be seen as the first step to advance mobility management from Mobile IP to eventual HIP.

2. Background

2.1. 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 inherited Mobile IPv4, with some modification. There are many different extensions to improve the performance. Mobile IP with Router Optimization Extension [4] is one of them. It is part of standard in Mobile IPv6.

2.1.1. Mobile IP Basic. In order to minimize the change of the upper layer model in TCP/IP architecture, Mobile IP still uses IP address as the endpoint identifier. Here are some important components of Mobile IP network

- 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 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.

A Home Address will be assigned to a 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 it's 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 has degraded the efficiency of the routing. No matter how close a MN and the CN are, packets from the CN to the MN are always via HA.

2.1.2. Mobile IP with Router Optimization Extension. Mobile IP with Router Optimization (RO) extension is an optional scheme in Mobile IPv4, but it is part of the standard of Mobile IPv6 [1]. This extension provides a better performance by avoiding the triangle routing.
Instead of creating a tunnel between a MN and the HA to forward packets, the MN will send a Binding Update packet to the CN to notify its current CoA. The CN will send all packets directly to MN after the binding update message from MN.

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

2.2. Host Identity Protocol (HIP)

The concept of HIP was first discussed in IETF in 1999. HIP Working Group in IETF and HIP Research Group in IRTF were formed in 2004. To handle mobility, HIP introduces a new namespace into IP network architecture [3, 5]. An IP address takes two roles in current IP networks, i.e. the endpoint identifier and the network topological locator. The duel roles of an IP address become more problematic with increased mobility and multi-homing of hosts. This issue is originally tackled by IRTF NameSpace Research Group (NSRG). Development of HIP is partially based on the study of NSRG. A new cryptographic public key namespace – Host Identifier (HI) is added to current TCP/IP stacks. A 128-bits hash key of HI – Host Identity Tag (HIT) will be used as endpoint identifier in upper layer protocol to simplify the design [3].

Besides mobility support, HIP enables multi-homing[6] as well. Moreover, HIP has also addressed the security issues. After the establishment of a 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 IPv4 and IPv6 interconnection.

HIP was originally designed to use ESP connection, but it is decoupling 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 any kind of signaling.

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

- 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 continue 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. It indicates the completion of the Base Exchange.

After the Base Exchange, IPSec Security Associations (SAs) will be created. The SPIs for the Responder-to-

Initiator and Initiator-to-Responder have been exchanged in I2 and R2 packets.

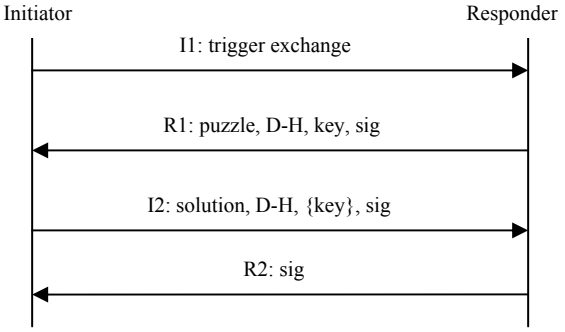

Figure 1. HIP Base Exchange [3]

2.2.2. 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 [8]. However, using the DNS server to look up the mapping between HIT and IP address is not a good solution. DNS server only stores the mapping of Fully-Qualified Domain Name (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 to update immediately. In order to provide a better performance, Rendezvous Server (RVS) [9] is introduced.

The role of RVS is similar to that of a HA in Mobile IP [10]. 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 [9].

2.2.3. 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 address. It enables a host to change its IP address and continues to communicate with its peer. HIP Mobility can be independent of ESP, but in this paper our discussion will only be limited to the ESP based.

When a MN is roaming into a foreign network, it will get a new IP address. The MN will send an update packet to update its record in its own RVS. The CN will start the Base Exchange via RVS if it wants to communicate with MN. This is 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. The LOCATOR parameter contains the new IP address and the SPI associated with the new IP address [6]. The address check is optional; it can help to prevent third party bomb attack. There are three different type of address checking process [6]:

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

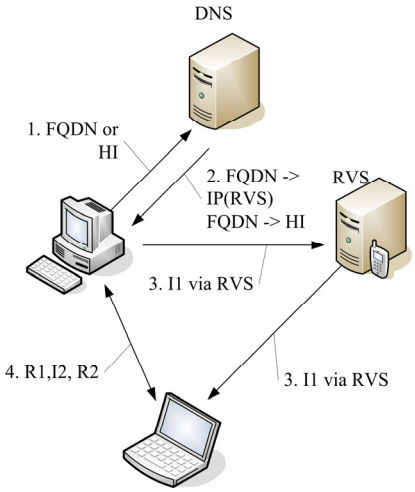

Figure 2. HIP Base Exchange via RVS

2.2.4. Multi-homing support. Multi-homing supported devices can connect to networks with different interfaces built in. Latest mobile devices may have more than one network interfaces. Multi-homing support is an appealing feature in functionality and mobility. HIP offers support to Multi-homing. Host can use UPDATE packet to notify the peer host that it has more than one IP address [6]. In another words, a unique HI of a device can map to multiple IP addresses.

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 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 chapter, we will investigate the feasibility of applying the good features of HIP to Mobile IP while keeping the impact on the existing IP networks and applications to minimum.

3. Secure Mobile IP with HIP style handshaking and re-addressing

In the Mobile IP with Route Optimization extension scenario, attackers can use spoofed binding update messages to corrupt the CN's binding cache and to make packets delivered to a wrong address. Attackers can use this to launch denial-of-service (DoS) to the CN, the MN and the third party node that receives the unwanted

packets. Moreover, the attacker can "steal" the address of MN by sending a spoofed binding update message with its own current address as the new CoA. Attacker can also send two spoofed binding update messages to two communication nodes to launch a Man-in-Middle Attack [11].

To deal the attacks mentioned above, an IP address needs to be verified before the binding update. Return Routability(RR) [1] is a mechanism for that purpose.

In the basic RR mechanism, a MN sends the Home Test Init (HoTI) via the HA to a CN and Care-of Test Init (CoTI) directly to CN. The CN will reply by Home Test (HoT) via the HA to the MN and Care-of Test (CoT) directly to the MN. The HA will forward the HoT to the MN inside the IPSec ESP protected tunnel. Binding update will be processed based on the key generated by the CoT and the HoT. 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 [12].

As descried 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 needs 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 [10].

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. 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[6]. The initial SMIP covers the ESP mode only. Non-ESP modes will be considered in the future.

The process of SMIP, shown in Figure 4, is described in the following. Before the connection is established, a "downgraded" HIP Base Exchange for IP addresses, instead of HIT, will be processed. When two nodes prepare to 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, such as in the circumstance when the MN is in a foreign network. Responder replies the Initiator by R1, which includes the Diffie-Hellan value. However, the puzzle used to protect the host from DoS attack and signature is optional [10]. After the Base Exchange is completed, SPI will be exchanged. An ESP protected connection will be created. Like in HIP, the ESP sequence number and SPI are essential components in SMIP. When the CN receives the binding update packet, the address checking will be conducted to verify the IP addresses.

In SMIP 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 the R1 and I2 are used, its defense against DoS attack will be further strengthened.

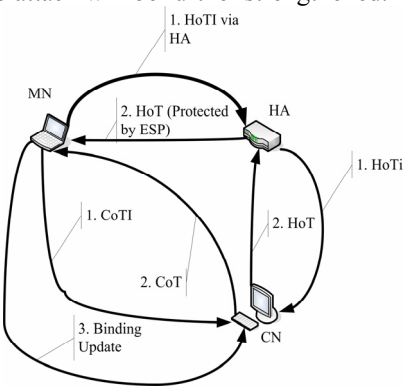

Figure 3. Return Routability (RR)

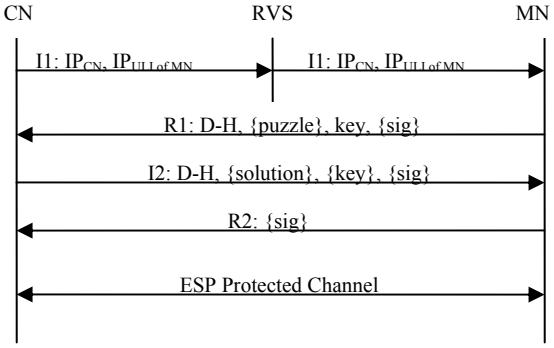

Figure 4. SMIIP Base Exchange initialed by CN via RVS

4. Security and performance analysis of SMIP

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 a 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(Figure 5). It takes only 1.5 $RTT_{MN,CN}$ in SMIP (Figure 6). The improvement is obvious.

BC is defined as the cost of handover handling which includes the binding packet transmission and the binding computation conducted in the nodes. Before we go to detailed discussion, some notions are defined in the

following. Let

- 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 one (CT). MN sends a HoTI via HA to CN. CN will generate a home nonce after it receives 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

$$PBC_{HT} = CT_{HoTI,HA,MN} + CP_{HoTI,HA} + CT_{HoTI,HA,CN} + CP_{HoTI,CN} + CT_{HoT,HA,CN} + CP_{HoT,HA} + CT_{HoT,HA,MN} \quad \text{……..…(1)}$$

As the process HA only forwards the packets to MN and CN, so CPHoTI,HA is equal to CPHoT,HA. Similarity, the transmission cost of HoTI and HoT packets are almost equal, so the formula can be simplified as following:

$$PBC_{HT} = 2\left(CT_{HT,HA,MN} + CT_{HT,HA,CN}\right) + 2CP_{HT,HA} + CP_{HoTI,CN} \quad \text{……..(2)}$$

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.

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

Similar to 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:

$$PBC_{CT} = 2CT_{CT,MN,CN} + CP_{CoTI,CN} \quad \text{……...(4)}$$

The total cost of RR can be summarized as the sum of BCHT and BCCT. The cost of generation of home nonce and care-of nonce in CN are similar, so the total cost of RR is

$$PBC_{RR} = 2\left(CT_{HT,HA,MN} + CT_{HT,HA,CN} + CT_{CT,MH,CN}\right) + 2(CP_{HT,HA} + CP_{RR,CN}) \quad (5)$$

The cost of 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.

$$PBC_{BU} = 2CT_{BU,MN,CN} + CP_{BU,MN} + CP_{BU,CN} \quad \text{….(6)}$$

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:

$$BC_{MIP} = 2\left(CT_{MIP,HA,MN} + CT_{MIP,HA,CN}\right) + 4CT_{MIP,MH,CN} + 2(CP_{MIP,HA} + CP_{RR,CN}) + CP_{BU,CN} + CP_{MIP,MN} \quad \text{…….……(7)}$$

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. As 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:

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

As shown in the equations (1) ~ (8), SMIP requires less BC than Mobile IP. Furthermore, in the circumstance of frequent handover, the overhead of processing in nodes in Mobile IP will be even higher than that in SMIP. In RR, to defend the messages from eavesdropping attack and time shifting attack, the key and state have a short life time. Binding update for a MN's frequent IP address changing has heavy processing cost. SMIP relies on SAs and nodes do not need 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 the handover progress. The independence of HA/RVS in SMIP leads to its shorter handover delay and lower binding cost.

SMIP's has 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 HoT from HA to MN.

Another new feature of SMIP is its support for multi-homing., which is lacked 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 Figure 7.

5. 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 is improved from the original Mobile IPv6. In SMIP, there is no need to modify the upper layer protocol and it can still offer excellent features in mobility management by adopting the

improved binding update process and the strengthened security. Its impact on the interconnection between IPv6 and IPv4 also needs to be further studied. Overall, SMIP can be considered as an initial step in the migration from Mobile-IP-based networks to public-key based future networks.

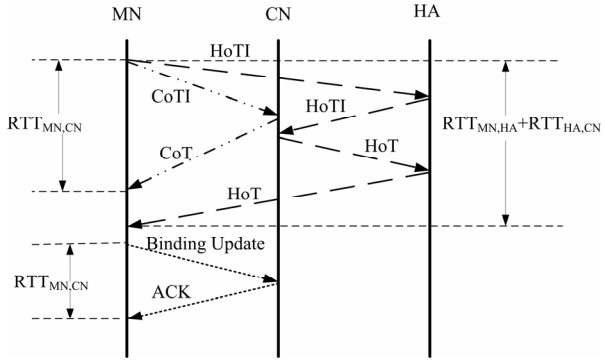

Figure 5. Mobile IPv6 Handover Performance Analyses

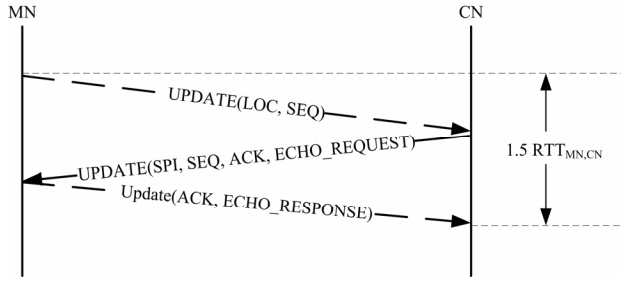

Figure 6. SMIP Readdress Performance Analyses (Readdress without Rekeying, but with Address Check)

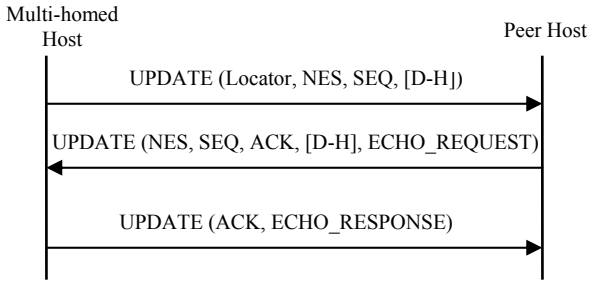

Figure 7. Basic Multi-homing Scenario [6]

12. 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-02 (work in process), Internet Draft, IETF, 21 February 2005

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

[5] R. Moskowitz and P. Nikander, "Host Identity Protocol Architecture", draft-ietf-hip-arch-00 (work in process), Internet Draft, IETF, 16 October 2004

[6] P. Nikander, J. Arkko, and T. Henderson, "End-Host Mobility and Multi-Homing with Host Identity Protocol", draft-ietf-hip-mm-01 (work in process), Internet Draft, IETF, 20 February 2005

[7] P. Jokela, R. Moskowitz, and P. Nikander, "Using ESP transport format with HIP", draft-jokela-hip-esp-00 (work in process), Internet Draft, IETF, 11 February 2005

[8] P. Nikander and J. Laganier, "Host Identity Protocol (HIP) Domain Name System (DNS) Extensions", draft-ietf-hip-dns-01 (work in process), Internet Draft, IETF, 20 February 2005

[9] J. Laganier and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extensions", draft-ietf-hip-rvs-01 (work in process), Internet Draft, IETF, 18 February 2005

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

[11] 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

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