Experimental measurements of host identity protocol for mobile nodes' networks

Maher Ben Jemaa, Nahla Abid, Maryline Laurent, Hakima Chaouchi

Hindawi Publishing Corporation
Journal of Computer Systems, Networks, and Communications
Volume 2009, Article ID 383517, 6 pages
doi:10.1155/2009/383517

Research Article

Experimental Measurements of Host Identity Protocol for Mobile Nodes' Networks

Maher Ben Jemaa,[1] Nahla Abid,[1,2] Maryline Laurent-Maknavicius,[2] and Hakima Chaouchi[2]

[1] *ReDCAD Research Unit, Department of Computer Science and Applied Mathematics Engineering, National School of Engineering of Sfax, BP 1173-3038 Sfax, Tunisia*
[2] *CNRS Samovar UMR 5157, TELECOM Institute, TELECOM SudParis, 9 rue Charles Fourier, 91011 Evry Cedex, France*

Correspondence should be addressed to Maher Ben Jemaa, maher.benjemaa@enis.rnu.tn

Received 2 January 2009; Revised 27 February 2009; Accepted 9 June 2009

Recommended by Sghaier Guizani

The role of Internet Protocol (IP) is becoming more and more problematic especially with the new requirements of mobility and multihoming. Host Identity protocol (HIP) defines a new protocol between the network and transport layers in order to provide a better management to those requirements. The protocol defines a new namespace based on cryptographic identifiers which enable the IP address roles dissociation. Those new identifiers identify hosts rather than IP addresses. Because HIP is a quite recent protocol, we propose to present an experimental evaluation of its basic characteristics.

1. Introduction

The Internet user nowadays is no longer the same one as decades ago. Recent unprecedented growth of the mobile technology market, devices support for more than one of a myriad of technologies and operators, and the need to communicate from anywhere and at any time are the challenges of nowadays networks [1, 2]. Needs are evolving and users are more demanding. Using Internet with the traditional considerations of decades ago is no more appropriate and sufficient. Internet is no longer able to cover all its user needs especially mobility, multihoming, and security ones [3, 4].

Few new Internet generation solutions were proposed last years as attempts to solve this problematic. However, their success was partial and limited for two reasons. First of all, those solutions can be described by "tiny" ones since they were too specialized. For instance, MobileIP (MIP) focuses mainly on mobility issues; IPsec is addressing only security issues, and so forth. All of them look to the problem from one side and none of them treated it as a whole one. Secondly, all the provided solutions were based on the traditional TCP/IP stack and tried just to adapt it [5]. The Host Identity protocol (HIP) is a recent protocol proposal at the IETF [6, 7] that comes to reply to all those questions and provides a complete solution to all those problems, enabling mobility, multihoming in a secured way [8]. The protocol specifies also a secured way to establish HIP-based communications and how it solves the mobility and multihoming issues.

Since the protocol is quite recent, going through its experimental evaluation seems to be interesting and very beneficial to give some conclusions about its performances. The idea of our study turns around that point. In fact, the present paper consists in an experimentation of HIP basic features. Different types of scenarios were performed in order to evaluate the basic characteristics of HIP. The goal of this research is to achieve providing some practical results about HIP.

The remainder of this paper is organized as follows. In Section 2, the current Internet architecture and problematic are outlined. Section 3 presents how HIP can be a possible solution for those problems. The proposed method of the testing scenarios performed is discussed in Section 4. This includes a description of the testing networks set up and experimental results. Finally, a brief conclusion is offered in Section 5.

2. Current Internet Architecture and Its Drawbacks

Currently, two namespaces are used in the Internet architecture: the Domain Name Service (DNS) names [9] and the Internet protocol (IP) addresses. They serve as a basis for

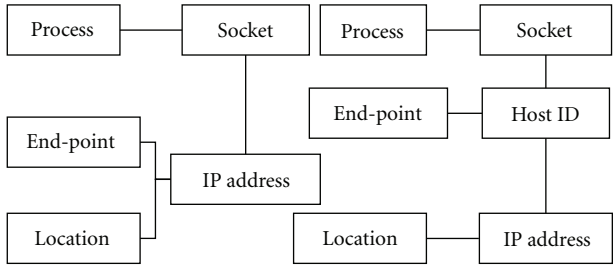

Figure 1: Identity and location roles separation.

the development and large deployment of Internet working technology and were behind its success and flexible use for years. IP addresses namespace plays a dual role of locators and endpoint identifiers. In fact, from the network layer point of view, those addresses are used as routing information serving to identify the topological location of the hosts in the network. Thus, if a host moves, its location changes and consequently its IP address has to change too. This role is called the locator role of an IP address [10]. However, from upper layers point of view, IP addresses play a second role which is identifying the host itself during communications and connections. This role is referred to as the identifier role of an IP address. At that level, IP addresses are not supposed to change during a communication even if the host changes its location. This is what we mean by "dual role of IP addresses" (as shown in Figure 1).

3. The Host Identity Protocol Solution

Many efforts have been carried out in order to handle with this problematic. Therefore, many solutions have been proposed solving the problem from different points of view. Decoupling the location from the identity seems to be the most straightforward solution. This idea was discussed, few years ago, in the Internet Engineering Task Force (IETF) [11] and Internet Research Task Force (IRTF) and led to the proposal of a new protocol, named the Host Identity Protocol (HIP). The fundamental idea of the protocol is simple: tackling the problem from the root by getting rid of this confusing and problematic role. In other words, HIP proposes to assign a new static ultimate identity to any host alongside with its location information where both of them are evolving in a totally independent way [3, 4]. As a result, the hosts will keep their identities unchanged even if they change their location over the network. For this purpose, HIP specifies a new namespace for the Internet [9] and a new layering architecture [7, 12]. Also, HIP proposes some modifications to the traditional ISO/OSI networking model. It introduces a new layer between the network and the transport layers. The role of this new layer is to make the mapping between HIs used in upper layers and IP addresses. Current Internet traditional bindings are shown in the left illustration of Figure 2. Transport connections are identified by pairs of IP addresses and ports. Thus if the IP address changes in a mobility scenario, for example, the upper layer connections are affected and have to be reinitialized with the new addresses. This makes the

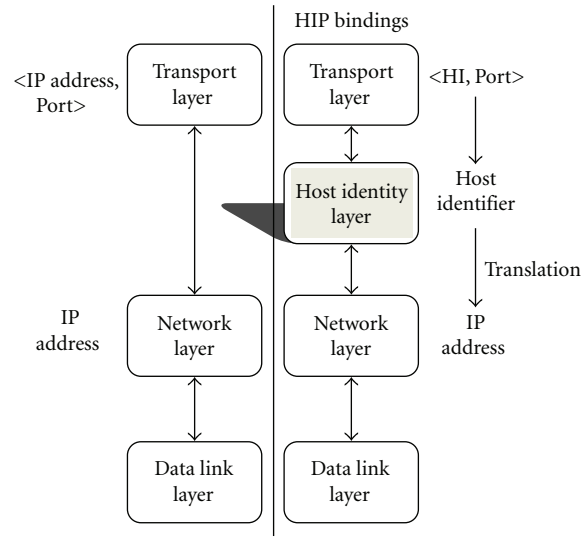

Figure 2: Comparison between current IP and HIP binding.

network and upper layers very dependent. No one can evolve separately from the other. Differently, from a HIP point of view, those connections are no longer bound to IP addresses but rather to the new identities, that is, the HIs. This makes the identification of end-point hosts in any HIP-based communication independent from the location information. IP addresses are used only in the networking level as routing information. Therefore even if the host moves, the mobility becomes transparent to upper layers. This clarifies the basic idea behind HIP: separating location and identification roles.

4. Experimental Setup and Results

Having on the one hand a rich theoretical specification of the protocol, and on the other hand some practical obsolete results about HIP-based on old and expired drafts, this creates the need to investigate an experimental experience of the protocol referring to the last and the most updated HIP implementation. To do this, some tests scenarios were set up and measurements values were collected in order to be able to retrieve some useful conclusions about HIP.

We used the nightly tarball version of HIPL. This version is the most up-to-date one and contains the latest code developed. We installed HIP on two machines; one plays the initiator's role and the other, the responder's role. In fact, HIPL uses a modified version of Linux 2.6 Kernel. Therefore, to install HIPL on any machine, we need first to install the HIPL kernel provided for free download on the site of the project [13]. In our case, we used 2.6.25 kernel version with ubuntu 7.10.

The target of this work is to test the performance of HIP on different networks and hosts types and the impact of introducing the new namespace especially in terms of delays comparing to the performances we dispose now.

4.1. Tests Scenarios Presentation. Here, the different tests that can be performed in the context of this research are

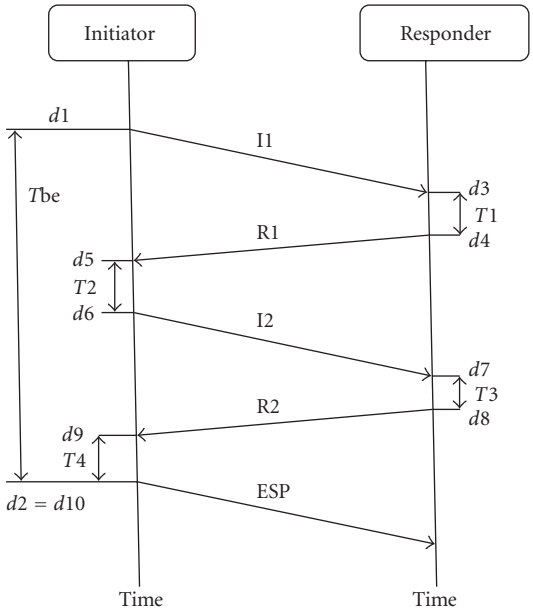

Figure 3: Times measured in A1, A2, and A3 subscenarios.

enumerated. Also, the utility of each proposed scenario will be explained.

4.1.1. Test Scenario A: BE Time Measurement. The BE is the first phase of any HIP communication and it precedes any data exchange. The duration of this step is with relevant importance in evaluating the performance of HIP since it is a mandatory phase whenever two hosts want to communicate in a HIP way and affects roughly the rapidity of communications establishment.

The idea behind varying the technology or the hardware specifications is to see how much HIP behavior, more specifically the BE duration, is affected by the type of the link between the hosts as well as the type of the devices.

Among this test, we are going to measure five times Tbe, $T1$, $T2$, $T3$, $T4$ as shown in Figure 3.

(i) Tbe is the total time of the BE. We consider that this time is equal to the difference between two dates $d1$ and $d2$

$$T\text{be} = d2 - d1 \quad (1)$$

where the $d2$ is date when the first ESP packet leaves the initiator interface. $d1$ is date when the first packet I1 leaves the initiator interface.

Longer the BE is, longer the nodes have to wait to begin the effective data transmission and worst are the performances of the network. This is why it seems interesting to have an idea about the total time required to establish a HIP association and also how this time is distributed between the initiator and the responder. The same test is performed each time by varying a parameter: Network technology (Ethernet, Wifi), types of devices (powerful, lightweight). So we can distinguish 3 subscenarios as shown in Table 1.

Table 1: Subscenarios A1, A2, and A3 features.

Characteristics	Scenario name		
	A1	A2	A3
Initiator	Laptop	Laptop	Laptop
Responder	PC	PC	Tablet
Network technology	Ethernet	Wifi	Wifi

Table 2: Subscenarios B1, B2, and B3 features.

Characteristics	Scenario name		
	B1	B2	B3
Initiator	Laptop	Tablet	Laptop
Responder	PC	Laptop	Tablet
Network technology	Ethernet	Wifi	Wifi

4.1.2. Test scenario B: Round Trip Time Measurements. Round Trip Time (RTT) is the time that a packet needs to travel from a source IP address to a destination IP address and come back. More exactly, the time that we measure here is equal to the time of sending an ICMP ECHO REQUEST packet, processing the packet and receiving its response, an ICMP ECHO RESPONSE. Scenario B is subclassified into three subscenarios: B1, B2 and B3 as shown in Table 2 using correspondingly wired and wireless links.

Since HIP uses encryption to process its data packets. Obviously, the RTT duration will be affected. Using this test, we try to highlight this by making a comparison between RTT with HIP and RTT without HIP.

4.1.3. Test Scenario C: Throughputs Measurements. The throughput can be defined as the average of useful data rate that are transmitted in a communication link. Usually it is measured relatively to a period of time. It depends on the protocols used, the introduced overhead and surely on the type of technology link in use. Since HIP introduces obviously some modifications to the structure of packets transmitted in the network and then surely to the amount of useful data transmitted. Having a look on how does HIP influence the throughput on a link is a relevant test. For this reason, the throughput in different types of communications was measured.

(i) A TCP-based communication without HIP (TCP),

(ii) A UDP-based communication without HIP (UDP),

(iii) A TCP-based communication with HIP (TCP/HIP),

(iv) A UDP-based communication with HIP (UDP/HIP).

The scenario is also divided into two subscenarios: subscenario C1 where only Ethernet link is used and subscenario C2 where a wireless link is introduced as shown in Table 3.

The test consists of sending a 100 Mb file of random data 10 times from the initiator to the responder and measuring each time the throughputs. The goal of the test is to make a comparison between throughputs with and without HIP and for both TCP and UDP connections.

Table 3: Subscenarios C1 and C2 features.

Characteristics	Scenario name	
	C1	C2
Initiator	Laptop	Laptop
Responder	PC	PC
Network technology	Ethernet	Wifi

Table 4: Scenario A–BE time measurements (milliseconds).

Average Time (milliseconds)	Sub scenario A1	Sub scenario A2	Sub scenario A3
$T1$	17.037	16.648	14.419
$T2$	98.849	90.599	1073.322
$T3$	64.684	56.019	52.729
$T4$	6.016	5.878	256.823
Tbe	188.418	170.144	1409.971

4.2. Experimental Results.

4.2.1. Scenario A–BE Time Measurement. Scenario A was performed in the purpose of measuring the total duration of the HIP Base Exchange as well as the time intervals spent both on the initiator and responder's sides. Here, the different mean values obtained from the tests are depicted in Tables 4 and 5, and Figure 4.

Based on the measurements values, the following conclusions were made.

(i) With a fast look at the values obtained, it can easily notice the following. The BE duration in A3, when a tablet is involved, exceeds greatly the time obtained in the first two subscenarios. In addition, we remark that in the three experiences, $T2$ is the longest time among all the other times measured.

(ii) The average time elapsed to establish the HIP association using wired links is about 188.5 milliseconds. However, in the presence of a wireless link, it takes approximately 170 milliseconds, which means about 18 milliseconds less. The difference is considered as a small one. Thus, the introduction of a wireless link does not affect the protocol. The difference can be due to the use of different network cards and the number of hops in the test network.

(iii) Referring to the measurements values in A1 and A2, the responder takes 81.721 milliseconds (resp., 72.667 milliseconds) to process I1 packet, create R1, process I2 and create R2. However, an average of 104.865 milliseconds (resp., 96.477 milliseconds) is needed by the initiator to process R1, create I2, process R2 and create the first ESP packet. In terms of percentages, about 43% (resp., 42%) of the BE time is consumed by the responder and approximately 55% (resp., 56.702%) consumed by the initiator. This stands for the basic idea behind the Base Exchange in HIP, which is avoiding DoS attacks by making the initiation of the communication expensive to perform in terms of CPU cycles. The initiator has to spend much more time than the responder to establish the HIP association. However, the result is a bit surprising because the difference between the two percentages is a thin one, about 14% in both cases. This can be explained by the difference of computation capabilities between the two hosts. In fact, in our case, the initiator is more powerful than the responder in terms of hardware specifications. This is why it can process and create its packets relatively in a rapid way compared to the responder even though it has much more work to do. For instance, the same test being performed with two hosts having the same hardware specifications gives the following results: 75% of the time is consumed by the initiator, and only 25% by the responder.

Table 5: Scenario A–BE time measurements (%)

%T tot	Sub Scenario A1	Sub Scenario A2	Sub Scenario A3
$T1$	9.042%	9.784%	1.022%
$T2$	52.462%	53.248%	76.109%
$T3$	34.33%	32.924%	3.739%
$T4$	3.192%	3.454%	18.214%

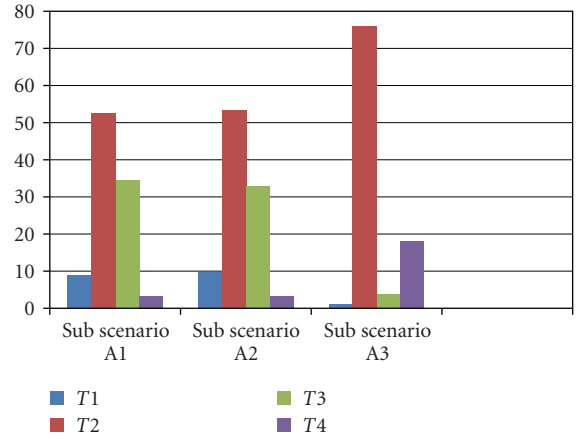

Figure 4: Scenarios a results—BE time measurements (%).

Hence, the hardware characteristics of both used hosts for these experiments are highly influencing the distribution of BE time between the two parties even if the protocol was designed to engage the initiator more.

(iv) In all the subscenarios under run, we remark that $T2$, time to process R1 and create I2, is the most expensive part of the BE. It takes more than 50% of the total time.

This result is expected, because this step includes solving the puzzle and generating the D-H keying material which is a bit demanding, especially if the puzzle difficulty is a high one.

In the two first subscenarios, $T3$ comes on the second rank with about 30%. This value seems understandable too since the responder has to create there the R2 packet which includes the HMAC and signature calculations. $T3$ is also influenced by the responder's capabilities which are, as we mentioned, less than the initiator's ones in our case.

(v) The results of A1 and A2 are compared to A3's ones. In fact, A1 and A2 were performed using the same types of devices, PC and laptop. How much does network technology

Table 6: Test Scenario B results-RTT measurements (milliseconds).

RTT (milliseconds)	Sub Scenario B1	Sub Scenario B2	Sub Scenario B3
IPv6	0.430	1.242	1.867
HIP	0.539	1.614	2.841

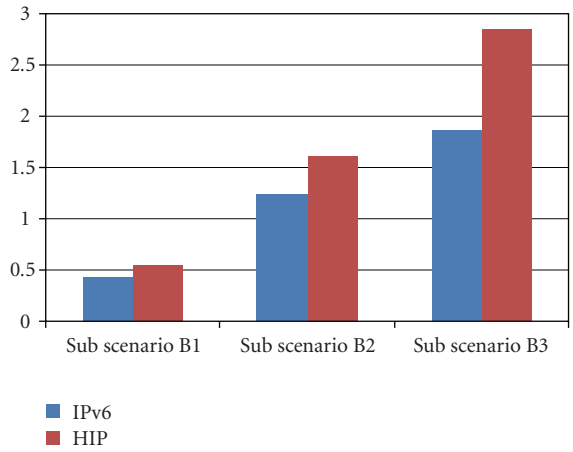

Figure 5: Test Scenario B results—RTT measurements (milliseconds).

Table 7: Scenario C test results-throughputs (Mb/s).

Throughputs Mbits/s	Ethernet	Wireless
TCP	8.773	4.443
TCP + HIP	8.538	4.199
UDP	9.419	5.295
UDP + HIP	8.973	4.998

affect on HIP? Using the third subscenario, it is shaded the light on HIP with lightweight devices which is an important point to study for any next generation protocol. In fact, the performance of the protocol when used with limited power environments, like tablets, is very important because such devices are the essential components of the future Internet. So the most relevant result to mention is that the laptop outperforms remarkably the tablet. In fact, the BE takes about 1.5s, which is about 7 times the duration calculated in the first subscenarios.

(vi) $T2$ in A3 is far longer than $T2$ in A1 and A2. This is due to the limited computation capacities of the tablet compared to the laptop. The tablet needs more than 1 second to solve the puzzle and generate the D-H keys. In this first test, the puzzle difficulty used is the one by default which is equal to 10. An average of 1,5 seconds can be acceptable for applications, but how does it go if a little level of trust exists between the hosts. Surely, once higher values of puzzle difficulty are used, it will take more time. This is the objective of the second scenario performed (scenario B).

4.2.2. Scenario B—RTT Measurements. Test scenario B was performed in order to measure the influence of the introduction of HIP on RTTs. It is interesting here too to measure

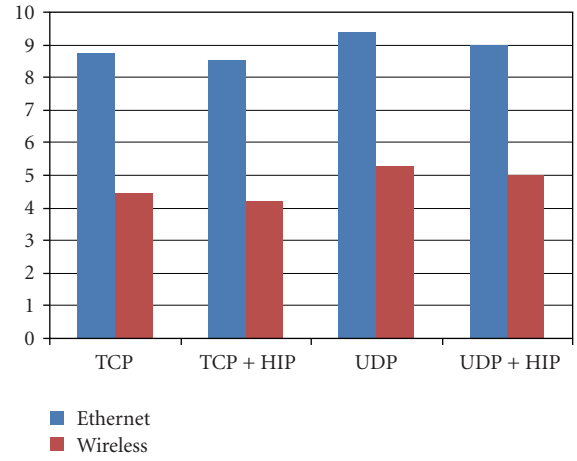

Figure 6: Test Scenario C results—Throughput (Mbits/s) for different protocols.

the RTTs with Internet tablets and compare that to the results found with the laptop Table 6 shows the RTT measurements for the different sub scenarios (see Figure 5).

(i) A fast look at the measurements obtained permits to affirm that HIP increases the RTTs values on the network. This can be explained by the ESP header added by HIP. In fact, having the packet encrypted requires more time at the hosts to decrypt and process them.

(ii) The first RTT measured in each scenario with HIP is the biggest one among all the other values obtained. This is understandable since during the first RTT, the two parties have to establish the HIP association to be able later to exchange the encrypted ICMP packets.

(iii) The RTT increases by 25% in a totally wired network, 30% in a network where a wireless link is introduced and 52% in the presence of an Internet tablet as a HIP host. Therefore, it can be concluded that HIP affects greatly the non powerful devices compared to other devices. However, normally the increase caused by HIP in C1 and C2 should be the same. A different result was found in these tests. Because the length of the packets after introducing HIP is the same in C1 and C2, this difference is caused by the access point and the time it requires to process the packets to the host.

(iv) RTT values are increased in the presence of a wireless link. This is due too to the presence of the access point too.

4.2.3. Scenario C—Throughputs Measurements. This scenario was run for the following purpose: measuring the impact of HIP on throughputs. The results obtained are collected in Table 7 and Figure 6.

(i) The introduction of HIP decreases the throughput values in both TCP and UDP communications. This can be explained by the overhead introduced by HIP which corresponds to the ESP encryption.

(ii) UDP throughput decreases by about 5% in the case of wired and wireless networks. However, for TCP, the decrease is 2.75% in wired and about 5.8% in wireless. The reduction is bigger in the case of TCP because this latter sends acknowledgments whenever packets are lost.

Also the difference of throughput between TCP and TCP with HIP is due to the ESP header added in addition to the acknowledgments packets sent.

(iii) An interesting point to mention is that HIP influences greatly the throughput on tablet. For instance, it turns from 3.012 Mb/s to 1.979 Mb/s, which corresponds to a decrease of about 50% of the later throughput. And it is almost the same thing in the case of UDP.

5. Conclusion

The experimental results about HIP gave the opportunity to make some conclusions related to the basic properties of this new protocol. After analyzing in depth the protocol specifications, the study was fixing the test scenarios to perform depending on the selected features to be studied. Some practical results about HIP basic properties were drawn. HIP seems to present an interesting solution and a promising feature in next generation networks. The strong point of the protocol resides in a high degree of security, eventhough it increases the time of the communication in the case of powerfull devices; it is still understandable and acceptable since the security is added

A final conclusion about HIP is early to be drawn now, the protocol developments are still ongoing works. However, the work and the results presented can help to evaluate partially the current development status of HIP and surely serve for future works intending to improve the protocol performance.

References

[1] G. Andrealis, "Providing internet access to mobile ad hoc networks," in *Proceedings of the London Communications Symposium*, London, UK, September 2002.

[2] V. D. Hoang, Z. Shao, M. Fujise, and H. M. Nguyen, "A novel solution for global conectivity," in *Proceedings of the 60th IEEE Vehicular Technology Conference (VTC '04)*, 2004.

[3] A. C. Snoeren, H. Balakrishnan, and F. M. Kaashoek, "Reconsidering Internet mobility," in *Proceedings of the 8th Workshop on Hot Topics in Operating Systems*, p. 41, 2001.

[4] H. Tschofenig, A. Gurtov, J. Ylitalo, A. Nagarajan, and M. Shanmugam, "Traversing middleboxes with the Host Identity Protocol," vol. 3574 of *Lecture Notes in Computer Science*, pp. 17–28, 2005.

[5] P. Ratanchandani and R. Kravets, "A hybrid approach to Internet connectivity for mobile ad hoc networks," in *Proceedings of the IEEE Wireless Communications and Networking (WCN '03)*, 2003.

[6] R. H. Thomas, M. A. Jeffrey, and J. H. Kim, "Experience with the Host Identity Protocol for secure host mobility and multihoming," *Wireless Communications and Networking*, vol. 3, pp. 2120–2125, 2003.

[7] S. Nováczki, L. Bokor, and S. Imre, "Micromobility support in HIP survey and extension of host identity protocol," in *Proceedings of the Mediterranean Electrotechnical Conference (MELECON '06)*, pp. 651–654, Spain, May 2006.

[8] F. Al-Shraideh, "Host Identity Protocol," in *Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL '06)*, IEEE Computer Society, 2006.

[9] P. Jokela, Ed., T. Henderson, R. Moskowitz, and P. Nikander, Host identity protocol, RFC 5201, 2008.

[10] R. H. Thomas, "Host mobility for IP networks: a comparison," IEEE Network, November-December 2003.

[11] http://www.ietf.org/html.charters/hip-charter.html.

[12] T. Aura, A. Nagarajan, and A. Gurtov, "Analysis of the HIP base exchange protocol," vol. 3574 of *Lecture Notes in Computer Science*, pp. 481–493, 2005.

[13] http://infrahip.hiit.fi.