Performance Evaluation and Experiments for Host Identity Protocol

Leonardo ARRAEZ[1], Hakima CHAOUCHI [2] and Zeynep GURKAS AYDIN[3]

[1,2] Telecom SudParis, Dept. LOR, CNRS Samovar UMR 5157, Evry, France

[3] Istanbul University, Computer Engineering Department, Istanbul, TURKEY

Abstract

This study firstly presents a review for well known Mobile IP and the recently proposed Host Identity Protocol which inherits the separation of roles of IP addresses in today's internet architecture. Afterwards, several performance evaluations are presented that performed on the testbed based on infraHIP implementation of the Host Identity Protocol. Performance results have been obtained and analyzed regarding the Base Exchange, throughput, round trip times and mobility events of Host Identity Protocol.

Keywords: *Host Identity Protocol, Performance Evaluation, HIP Implementation and Testbed, Mobility*

1. Introduction

Wireless devices, cell phones and the internet, along with the development of new technologies in the fields of electronics have managed to provide a catalog of new devices capable of providing multiple services at the same time and allowed the fusion of voice and data networks and their services. The current horizon unveils a new phase in the evolution of communications, the management of mobility in order for a user to keep connectivity to the network, and hence the word, at all times or at least reduce the amount of time wasted by a person while disconnecting from one point and immediately connecting to a new point of attachment to the networks, which may not be a big time, but continuously interrupts and affects the communication, exchange of data and eventually the overall experience of the end user.

Mobile IP was the first formal effort done by the technological groups (IETF: Internet Engineering Task Force) to satisfy the need of mobility among different networks and an overall better experience in this field, some extensions and enhancements have been gradually added to the original architecture such as "fast mobile IP" and have made the original protocol a more robust and viable solution to the problem. Recently, a new joint effort have been achieved at the Helsinki Institute for Information Technology (HIIT) on a new concept called Host Identity Protocol (HIP) to the problems of separating the IP address from the location of the node using identifiers and thus improving mobility and security in any communications network.

The objective of the study is to perform different tests and evaluations to verify and validate a mobility management platform using one of the current software implementations of HIP (infraHIP: Infrastructure for the Host Identity Protocol), report the results obtained and provide the appropriate feedback of the error and complications encountered, as well as the proposal for improvements in the design of the platform, focused mainly in the management of the handovers of a mobile device.

2. Mobile IP and Fast Mobile IP Anticipation Processes

There are different concepts of mobility, they all depend on the context of discussion, the concept of mobility in telecommunications, especially concerning a node roaming from one network to another, refers to the ability of a node to maintain open communications and a continuous flow of data after having changed the point of attachment from its original network to a new link. The principal elements of a mobile IP infrastructure are the mobile node, the home agent and the foreign agent [1]. In order for a mobile node and the agents using mobile IP to communicate constantly, two main processes have been defined to aid the mobile node in different aspects throughout its mobility events. Those process described below define the discovery of other peers capable of supporting mobile IP, the advertisement of the home and

foreign agents to inform nodes of the service provided by them, and the registration process necessary by any node to quest and register a mobile IP service from an agent.

One of the biggest concerns regarding mobility is the fact that packets and information sent to a mobile node is lost during a mobility event when a node changes its point of attachment to the home link and connects to a foreign link elsewhere, this is due to the mobile node being unreachable during the handover process. The fast handover extensions for mobile IPv4 and IPv6 defined in the IETF RFC 4988 [2] and RFC 4068 [3], describe processes as well as new messages implemented under mobile IP to optimize the handover of a mobile node between home links and foreign links. The original version of mobile IP inherits a reactive approach towards mobility as it was designed for a mobile node to notice a mobility event and inform the home agent link and other peers of the new care-of address only after the node was located in the foreign link. The new approach proposed in the fast mobile IP, aimed to diminish the time taken by a mobile node for the setup of the new care-of address, as well as the agent discovery and association times by searching for the required information of the new link from the home link before the mobility handover event.

The design for the fast mobile IP extension considers a handover of the mobile node from an access router acting as a foreign agent to a new access router that will eventually assume the role of the foreign agent; these two elements are referred to as previous access router (PAR) and new access router (NAR). The extension also considers a previous care-of address (PCoA) and a new care-of address (NcoA) as the addresses of the mobile node prior and after the handover to a NAR. The enhancement of the handover management process in the fast mobile IP extension consists on the mobile node creating a neighborhood access point and subnet map using either the new “Router Solicitation for Proxy Advertisement” (RtSolPr) sent by the mobile node after obtaining a care-of address and registering with the home agent as defined in the original version of mobile IP, or the new “Proxy Router Advertisement” (PrRtAdv) messages sent by the foreign agents. The map created by the mobile node contains the information necessary for the node to select a new point of attachment on the proximity of a handover event, once the next point of attachment is selected and with the information provided by the map, the node may process a new care-of address before the handover event and set up a tunnel to forward temporarily any data sent to it during the handover.

The only difference between a predictive and a reactive handover message flow in fast mobile IP relies on the actual process of the early handover request by the PAR with the HI message, as in a reactive handover management scenario there is no need to confirm the availability of a NcoA, since the mobile node has processed one before requesting a fast binding update to the PAR and only needs for the PAR to create a tunnel with the NAR and forward any packets received on behalf of the PCoA to the NCoA.

3. Host Identity Protocol (HIP)

The Host Identity Protocol is a recently developed protocol that provides a secure end-to-end mobility and multihoming solution just like Mobile IP. However, the approach taken by HIP consists on the separation of the identifier used currently to define both the identity and the location of a host, the IP address of the host. Instead of relying solely on the IP address of a host (like Mobile IP does), the HIP protocol maintains the location of a host related to the IP address specified in its network layer, but it also defines a new identifier named a Host Identity Tag (HIT) as the identity of a host, this identity (generated by a 128 bits public-private key pair) is to be used in the transport and application layers instead of the currently used IP address. This separation of identity/location, allows to easily map a host to different locations (HIT-> IP1, HIT->IP2, and so on), hence allowing an easy implementation of mobility and multihoming.

The origins of the Host Identity Protocol (HIP) go as back as 1999, when Robert Moskowitz from the ICSA Inc. labs proposed and introduced the first draft of the basic architecture of HIP in the IETF on May 1999 [4]. Since then, a working group lead by Pekka Nikander with the additional support of Ericsson Nomadic Lab, Boeing and HIIT started adjusting the details of the draft and were able to deliver the submission of the specification of the protocol by 2004. Shortly afterwards, the IETF working group for HIP started its functions on June 2004 and up to this present day, the architecture of HIP has been thoroughly test-proofed and refined, providing so many alternatives and possibilities that and even a second working group has been created, the HIP research group of the IRTF, the main work of this group consists on the development of new features for the mobility and multi-homing features of HIP as well as the impact on the Internet once HIP is deployed as a standard.

3.1. HIP Functionalities

The basic architecture of the Host Identity Protocol is shown below. The figure, courtesy of Cisco's Internet Protocol Journal, illustrates how a transport or application

layer client can reach out for a host using the host identity tag (HIT) instead of the current IP address as the host identifier, consequently, the HIP layer will perform the corresponding mapping of the host's identity to its current location and reachable IP address.

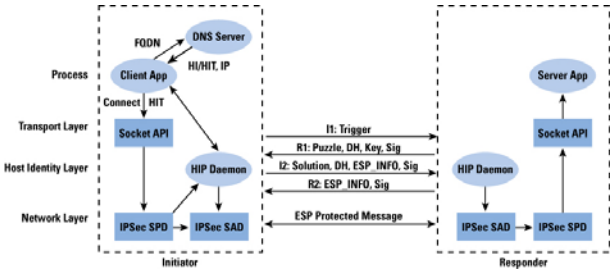

Fig. 1 Basic architecture of HIP (Courtesy of [5])

The process starts with a basic exchange registration where an exchange of information is done in order to create an IPSec security association that assures a secure connection between the hosts throughout the HIP session. The following sections describe more into detail the basic registration process as well as the mobility and multihoming features of HIP.

3.2. Base Exchange

Before any HIP session between hosts is established or any information is transferred, a security check and an exchange of credentials needs to be made to guarantee the identity and the willingness of the initiator host to enter and start a HIP conversation with another host. The figure below illustrates the basic exchange process as an exchange of four HIP messages between two hosts. The host willing to initiate a HIP session is called the Initiator and is the node that sends the first HIP message in the basic exchange. This first message is called I1 and as parameters it contains the host identity tag (HIT) of the source node (being the initiator) and the host identity tag of the destination node that is referred as the Responder node.

When a node receives a HIP message with the message type set to I1, it will automatically send back to the initiator node (in an extremely short time T1) a HIP message type R1 that it has previously prefabricated with the HIT of the initiator, the HIT of the responder, Diffie-Hellman parameters to create the session keys for the security association, the signature to prove the identity of the responder node and most importantly, a puzzle to be solved by the initiator node before in order to continue with the process. The inclusion of a puzzle by the responder node as a cryptographic challenge during the basic exchange registration is done in order to avoid a DoS attack from a bogus node that wishes to saturate a responder node with HIP session initiation messages.

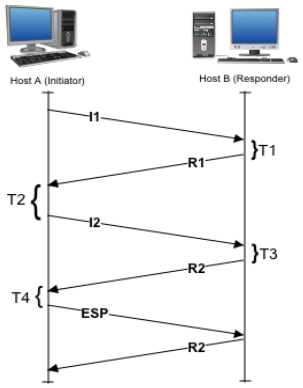

Fig. 2 Basic exchange process in HIP

A responder node will only dedicate resources to enable a HIP session to a node that properly solves the puzzle (with a level of difficulty defined by the responder node) and replies back with the solution to the challenge in the following I2 message. Once the Initiator has spent a T2 time solving the puzzle challenge, it will send the correct solution in the third HIP message (I2) along with its own Diffie-Hellman parameters for the second security association, the HIT keys and the signature to prove the authenticity of the message.

The last step in the basic exchange process will be for the responder node to confirm the HIP session with a signed R2 message which asides from the source and destination HITs of the message may optionally include the registration information of the initiator node to any services(s) provided by the responder node. Usually this T3 time period is very short as well, leaving most of the percentage time of the basic exchange process to the initiator node. Once both nodes have set their IPSec Encapsulated Security Payload (ESP) Security Associations (SAs) and established a HIP session, they will open and transfer the information from the transport and application layers solely through IP Sec ESP Bound End-to-End Mode (BEET) tunnels.

3.3. Mobility and Multihoming

The IETF RFC5206 [6] describes mobility in HIP as the possibility for a node to maintain reachability with all of the other nodes it keeps an open HIP session with, regardless of the possible changes in the point of attachment to a network in the node. This availability of the HIP node is provided b the LOCATOR parameter, which provides a list of all of the possible IP addresses on which a node can be reached at, along with pairing information of the different HIP security association parameters such as the ESP Security Parameter Indexes.

The Host Identity Protocol manages mobility from a reactive perspective in which the mobile node its expected first to notice that it has changed its location (via netlink messages from the lower physical layers), once the node realizes its new location, it will send a HIP packet to inform of it to all of the HIP nodes that have an open session with the initiator node, this HIP packet is called a HIP UPDATE packet and the flow of this message exchange is shown in the figure 3 below.

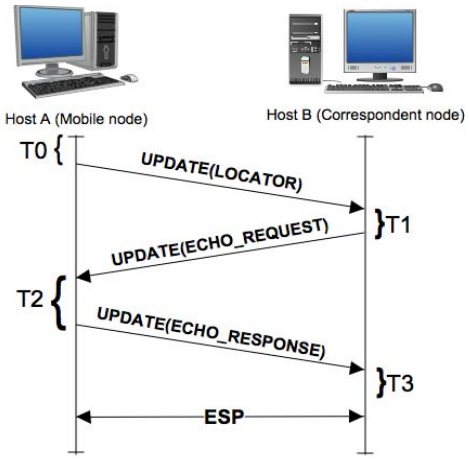

Fig. 3 Basic UPDATE process implemented during a mobility event without re-keying in HIP

The UPDATE packet contains several information of the security association of the HIP sessions in order to show and prove that the node is not a impostor posing for itself, it may also include new information to be used in case the security association needs to be re-keyed or changed as shown in the figure below, as well as a LOCATOR parameter containing the information of the different network interfaces of the HIP node along with the IP addresses where the HIP node can be currently located, hence informing its new location.

Once the initiator node has regained connectivity and sent the UPDATE packet with the LOCATOR parameter information, the responder nodes reply to the initiator node with another UDPATE packet, this time, instead of a LOCATOR parameter, the packet will contain an ECHO_REQUEST parameter in order to prove the validity of the new network location information of the initiator node. Just like the initiator, if a parameter in the security association is going to be changed, the initiator will include it in the UPDATE packet. Until this new location is not verified, the responder node will not update the location of the initiator node and all of the exchange of information will remain addressed to the old location.

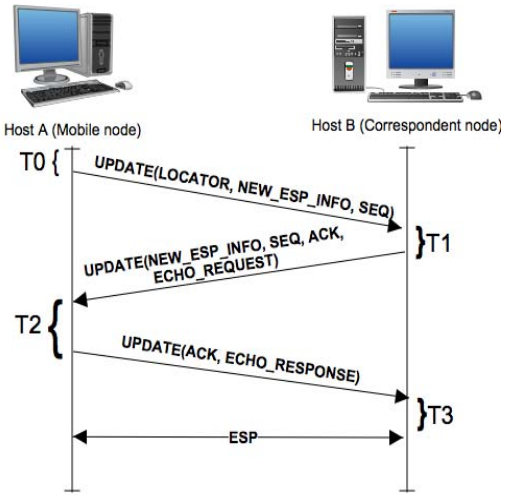

Fig. 4 Basic UPDATE process implemented during a mobility event with re-keying in HIP

Upon receiving an UPDATE HIP packet with an ECHO_REQUEST parameter, an initiator node will automatically respond to it with another UPDATE packet including an ECHO_RESPONSE parameter, only after receiving this last UPDATE packet, will the responder node update the database containing the location information, preferred IP address of contact and the security association information of the initiator node. The figure of the LOCATOR parameter which allows the management of several IP addresses in a HIP node inherently provides the multi-homing feature in the protocol. As it is well-known, multihoming consists on the ability of a network element to be reachable in more than one location specified by multiple IP addresses. The LOCATOR parameter in HIP creates a list of the available IP addresses in the HIP node, and allows mapping the proper relationships between the different IP addresses of the node and the different security associations available. The multihoming capability of HIP allows a node to select and notify peers of the preferred location to be contacted which is a very desirable feature, since the node may decide to be contacted through a network interface with higher throughput, a network interface with less power consumption, a network interface with cheaper access costs or even a more secured network interface behind a firewall and/or a proxy server.

3.4. Host Identity Protocol vs. Mobile IP

Several advantages can be mention as reasons to select the deployment of HIP over mobile IP on a network. Both protocols offer the features of mobility and multihoming to a node, important characteristics in high demand lately due to the rapid development and evolution of mobile data networks on cellular carriers and the recent appearance of

more devices offering portability. However, HIP offers not only the mentioned split of the location and the identity of the node by adding a new namespace based on the host identity tags of the nodes. But also offers an end to end secured connection between hosts that MIP only offers between the home agent and the mobile node.

HIP also provides a relay service that allows a HIP server to relay all HIP packets to a subscribed HIP node just as a home agent would do in mobile IP, which is a very practical feature to be used during the mobility events as only one node needs to be updated of the current location of the mobile node instead of all the peers (just like in mobile IP). Another service provided by HIP is the "Rendezvous" service, a service that allows a HIP server to work as a point of meeting for a HIP node and its peers and designed to act a front-end to receive all I1 messages from any node trying to establish a HIP session with the subscribed host, this I1 message will be forwarded to the current and final destination of the HIP node ending the function of the rendezvous server and leaving the two nodes to continue the basic exchange process. This design allows a subscribed host to move freely between networks and only need to notify of its current location to the rendezvous server and any other node with an open HIP session at the moment of the mobility event, while maintaining the initial location unaltered for future nodes that wish to contact it.

Another advantage of HIP over MIP, relies on the fact that no additional infrastructure needs to be added to implement the basic architecture of HIP, in contrast to mobile IP where at least a new dedicated element is added to the home link of a mobile device such as the home agent in order to perform the forwarding of packets to the mobile node. Now that the topic of packet forwarding has come up, an additional reason to implement HIP over MIP needs to be mentioned as well, the communication between a mobile node and the correspondent nodes is direct and secured, there is no re-routing of packets through a middle man such as the home agent that will inherently add delay times in the transmission of data and increase the probabilities of being intercepted by a man-in-the-middle attack as the communication between end points is not encrypted and secured as in HIP.

Due to the previously stated advantages and the fact that HIP is a very recent protocol for which new services are being implemented to enhance its functionalities, this report concentrated on the evaluation of the performance of HIP as well as the improvement of current features and the design of new ones.

3.4. HIP Test Bench and Implementation

In order to be able to perform the performance test and evaluations of the basic exchange handshake and mobility update notification scenarios a physical test-bench was assembled. The test-bench consisted of several desktop computers working as fixed HIP nodes, a DNS server and a rendezvous server; one laptop computer and an internet tablet assuming the roles of mobile HIP nodes. Finally, the nodes of the test-bench were connected to each other in a small network created by a wireless router, a wireless access point and a blue tooth access point. Figure 5 and Table 1 illustrate the distribution of the different elements of the test-bench.

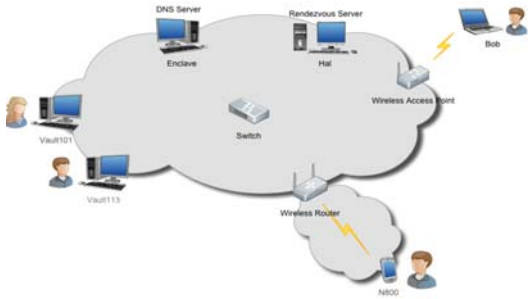

Fig. 5 HIP Test bench

Table 1: Devices used in the HIP Testbench

Role in HIP Test Bench	Host Name	Details of Device
Wireless Router	HTBR	NETGEAR KWGR614
Wireless Access Point	HTBAP1	Cisco Aironet 1100
	HTBAP2	ANYCOM EDR-AP
	HTBAP3	
HIP Node	N800	Nokia Internet Tablet N800
	BOB	DELL Latitude D830
	VAULT101	DELL Precision T3400
	VAULT113	
HIP Rendezvous Server	HAL	DELL Precision 380
DNS Server	ENCLAVE	DELL Precision T3400

4. Performance Evaluation and Results

A set of different tests were performed in the test-bench platform configured, the main intention of these examinations consisted on the verification and validation of the features of HIP on the software implementation HIPL, once the validation and correct deployment of the test-bench was fulfilled, began the process of analysis and

design of the improvements on the mobility management processes of the nodes using HIP. The core of the following procedures is based on the work done at the Helsinki Institute for Information Technology in Finland specified in [7]. However, some variations were performed in order to adapt the procedures to the test-bench and the objectives of the project.

The following tests were performed once the HIP test-bench was assembled and configured with the most recent version of the implementation of HIP from the infraHIP project. There are currently three implementations of HIP available for tests: The HIPL implementation from the infraHIP project at the Helsinki Institute for Information Technology in Finland [8], the openHIP project as an open source project from the IETF and the IRTF [9], and a freeBSD implementation from the Ericsson Nomadic Labs in Finland [10]. Out of the three implementations, the first solution (infraHIP) was selected due to the active community and the quick support provided.

Two main scenarios were defined to perform the tests:

- *Scenario 1:* The first test scenario consisted on two fixed nodes (Bob and Hal) acting as both initiator and responder nodes. Both nodes were isolated and connected via Ethernet to the same router on a private LAN in order to avoid network traffic from other nodes.
- *Scenario 2:* The second scenario consisted on a fixed node (Hal) connected via Ethernet to a wireless router and a mobile node (N800) connected to the same private LAN either through a wireless router, a Bluetooth access point or a wireless access point. The fixed node acted as a responder node to the different messages sent by the mobile node who in this case acted as an initiator node during the basic exchange registration and the different mobility events studied.

4.1. HIP Basic Exchange Times and Durations

The first test performed in the test-bench consisted on the verification and validation of the basic exchange process specified in the HIP protocol. Using the two case scenarios described in the previous section and illustrated in the figures below, the test focused on verifying the correct flow of the I1, R1, I2 and R2 messages involved in the process.

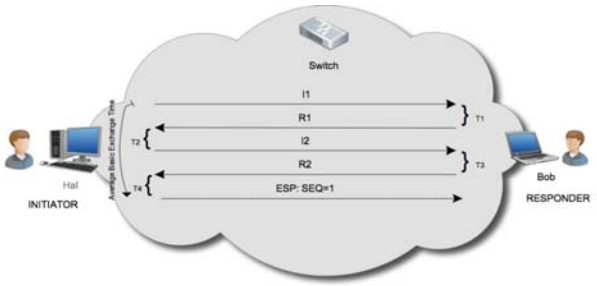

Fig. 6 HIP Basic Exchange Test Scenario 1 (Laptop connected through Ethernet)

In order to evaluate the average performance of the test-bench during the basic exchange process, four indicators were considered: the time T1 taken by the responder node to receive an I1 HIP packet and automatically reply with an R1 packet with a predefined puzzle to be solved, the time T2 taken by the initiator node to receive the puzzle, solve it and send back the answer to the responder. The third time T3 consisted on the time taken by the responder node to receive the answer of the puzzle, process the registration request of the initiator and reply with an R2 message. The last indicator T4 consisted on the time consumed by the initiator once it had received the R2 message to establish the registration and started assembling IP Sec ESP Packets to be sent to the responder on the following exchange of data.

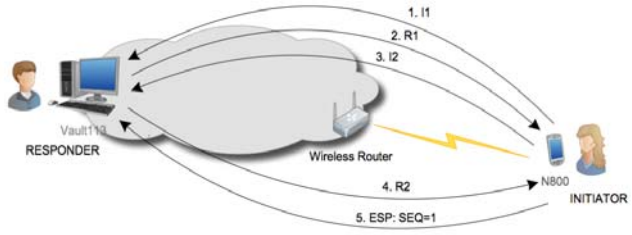

Fig. 7 HIP Basic Exchange Test Scenario 2 (N800 connected through WiFi 802.11g)

With these metrics into consideration, a pool of samples were taken to measure T1, T2, T3, T4, the derivative average duration of the basic exchange process BeT (BeT=T1+T2+T3+T4) and the corresponding standard deviations for each. The procedure for both test case scenarios is practically the same once the mobile node in test scenario 2 is connected via wireless to the same network of the responder node.

Figures 8 and 9 display the average of T1, T2, T3, T4 and BeT. In both case scenarios can be seen that the shortest processing times belong to T1 and T4, which affirmatively correspond to the processing times for predefined messages I1 and setting the status of the SA to "established" after receiving an R2 message as determined by the protocol [11]. The main differences between the

results of both test case scenarios correspond mainly to the time T2 in the initiator node in the mobile node N800.

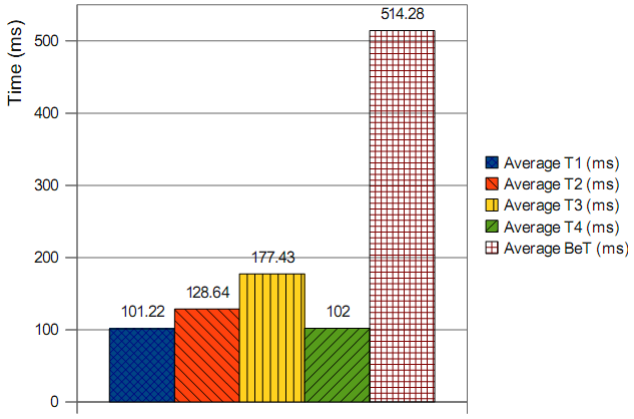

Fig. 8 Average Times for HIP Basic Exchange (Scenario 1)

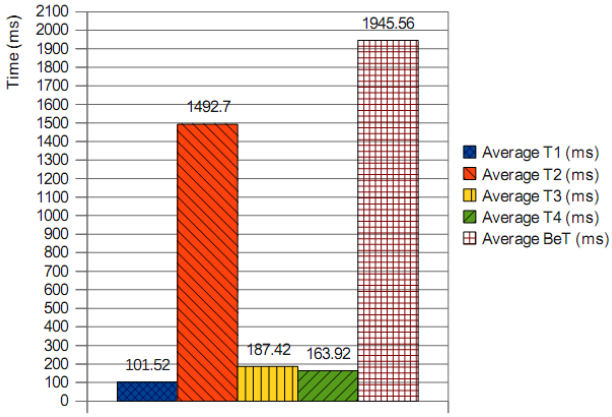

Fig. 9 Average Times for HIP Basic Exchange (Scenario 2)

4.2. Round Trip Time Estimates

The second set of tests performed involved the measurement of the round trip time of an ICMPv4 ECHO/RESP and both regular IPv4 encapsulation and ESP over HIP encapsulation of the message.

The figures below illustrate the results obtained from the RTT estimates tests, where it can be easily seen the difference in times in both test case scenarios 1 and 2 of the RTT of an ICMP message sent over regular IP encapsulation and the RTT of an ICMP message sent over a secured ESP/HIP encapsulation. In both scenarios; the RTT of the message sent over regular IP is lower than the RTT message sent over ESP/HIP, this is due to the overhead added by the ESP/HIP encapsulation, which creates larger messages that need to be fragmented into smaller packets during their transmission, hence, actually incrementing the amount of packets transmitted in contrast to the first case.

Both figures 10 and 11 validate the initial assumption that HIP packets should take more time to reach their final destination due to the additional tasks required to process the messages through the IP Sec ESP tunnels. The graphs also confirm the assumption that a connection between two nodes over Ethernet as described in test scenario 1 should be much faster than a connection between nodes over a wireless network, or where at least one of the nodes is connected via wireless to the network as in test scenario 2.

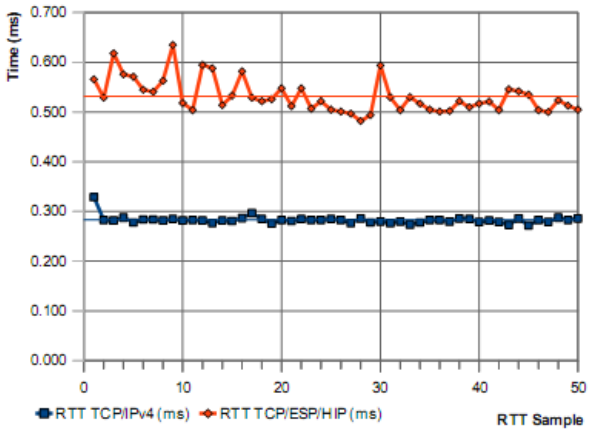

Fig. 10 HIP round-trip (RTT) performed under Test Scenario 1 (Laptop connected through Ethernet)

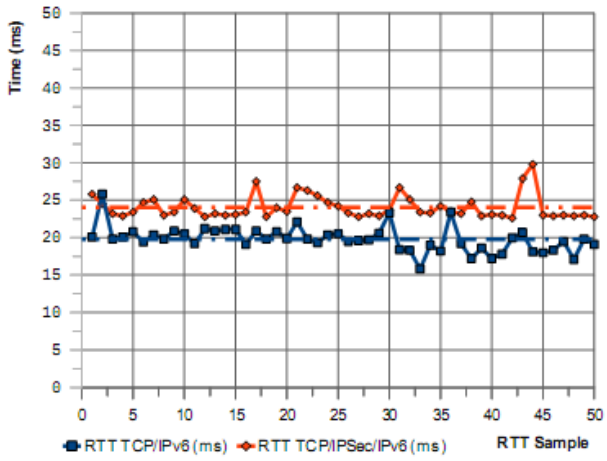

Fig. 11 HIP round-trip (RTT) performed under Test Scenario 2(N800 connected through WiFi 802.11g) Times

4.3. Throughput Values

The tests performed on the measurement of the average throughput in the communication between two HIP nodes. For each test scenario, a set of samples were gathered representing each one the average throughput in the transmission of a large file between the initiator and the responder nodes during one hundred (100) seconds. As the most common modes of transportation of packets are TCP and UDP, both modes were measured over a regular IPv4 and over an IP Sec ESP/HIP encapsulation. The figures below (12-15) illustrate the results of the throughput measurements, as it was expected, due to the differences in the natures of the TCP and UDP transport protocols, in both test scenarios the throughput of the messages sent via UDP is higher than then messages sent using TCP. Also in a continuation to the behavior shown during the RTT examinations, the throughput of the messages sent via HIP, is lower than the throughput of the messages sent via regular IP, this is due, in a similar case, to the overhead added by the ESP and HIP encapsulations, which increase the amount of data needed to transmit the original information. It's to be noted that the throughput values for the test scenario 1 correspond satisfactory to the throughput of a node connected via Ethernet to a network, while the throughput shown in the test scenario 2 corresponds logically to a wireless node connected via 802.11b to a network.

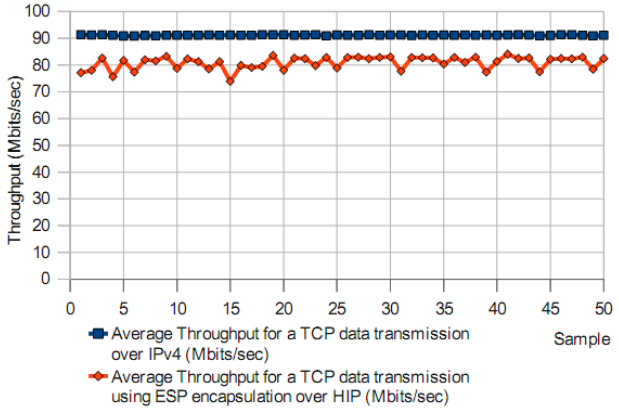

Fig. 12 HIP-TCP Throughput Test Scenario 1 (Fixed Node)

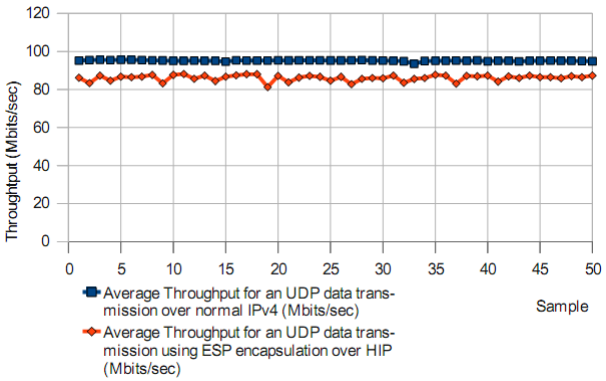

Fig. 13 HIP-UDP Throughput Test Scenario 1 (Fixed Node)

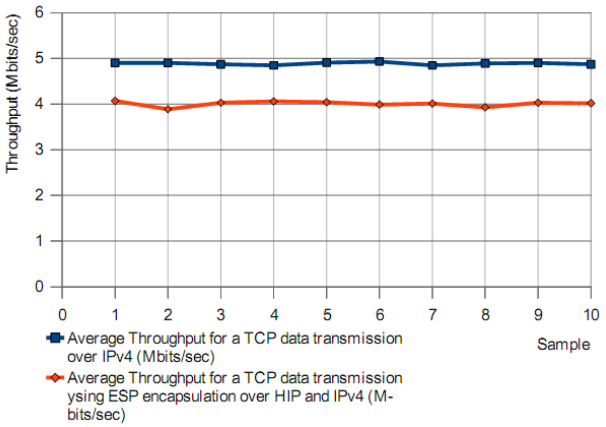

Fig. 14 HIP TCP Throughput Test Scenario 2 (N800 connected through WiFi 802.11g)

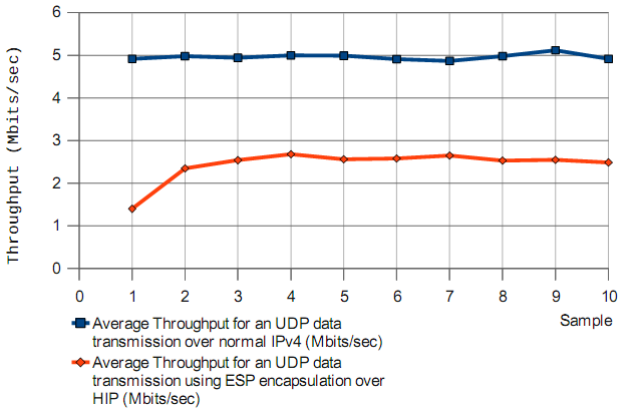

Fig. 15 HIP UDP Throughput Test Scenario 2 (N800 connected through WiFi 802.11g)

4.4. HIP Mobility Events

The last performance evaluation consisted on the measurement of the processing times of the different UPDATE HIP packets defined in the protocol and specified in the RFC 5206 [11]. In order to verify and validate the correct flow of the messages, a mobility event was generated in both test scenarios 1 and 2 in figures 16 and 17 respectively. For the test scenario 2, the attachment point to the network of the mobile HIP node (N800) was changed from a wireless router, to a wireless access point or a blue tooth access point.

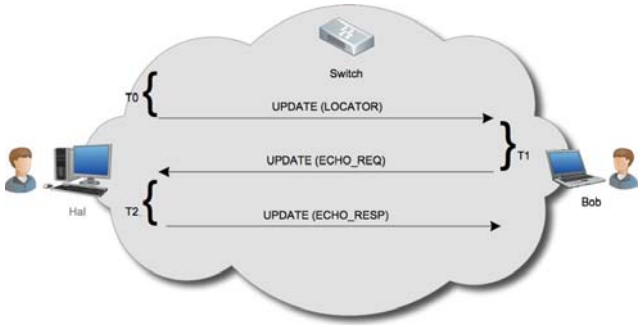

Fig. 16 HIP Mobility Event Test Scenario 1

Meanwhile, for the test scenario 1, even though a test script that enabled or disabled the network interface of the initiator node (Bob) would have been sufficient, it was decided to follow a more practical approach and actually proceed to disconnect physically the network interface and wait for a brief instant before connecting once again the network interface, this time to a second point of attachment (port) of the same access router.

As specified by the RFC [11], in order for an initiator node to properly notify the new location to a responder node, there needs to be a previous basic registration exchange and a valid security association between the nodes. Taking these considerations into account, the different times measured included the time T0 taken by the initiator node to realize that its current location has changed, update the LOCATOR parameter with the new IP addresses available, assemble the UPDATE packet with the proper source and destination HITS, and send the message to all of the HIP nodes with whom the initiator node maintains an open communication.

The second time measured was related to the time T1 taken by the responder node to process an UPDATE message with an updated LOCATOR parameter sent by the initiator and respond to it with an UPDATE message requesting the echo of certain random data. As the design of HIP suggests, the objective of the echo request by the responder is to confirm the reachability of the initiator node before updating the database and mapping of the LOCATOR of the initiator. The last time measured was the time T2 corresponding to the time taken by the initiator node to respond to the echo request of the responder node with an UPDATE message which includes the data requested.

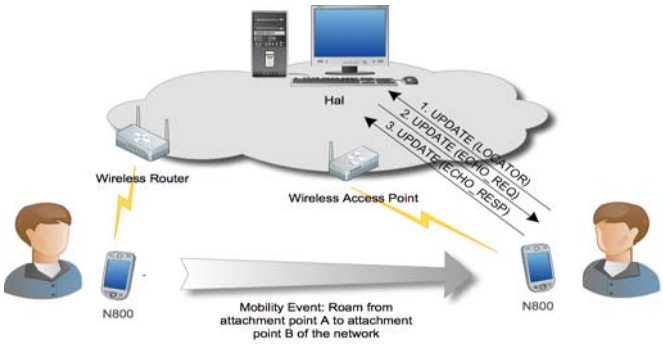

Fig. 17 HIP Mobility Event Test Scenario 2 (N800 connected through WiFi 802.11g)

The set of tests performed during this section validated the correct execution of the LOCATOR parameter update process for both test scenarios as described in the architecture of HIP [11] and the mobility and multihoming extensions defined in [6]. The figures 18 and 19 show an average time of 100-120 milliseconds taken by each node (HAL and Bob) to process a HIP packet such as the UPDATE message.

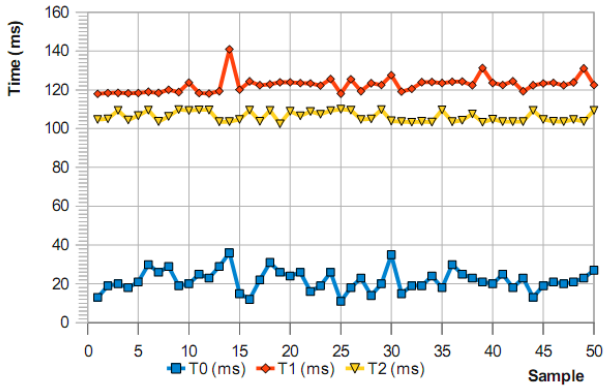

Fig. 18 HIP Time Results for Mobility Event Test Scenario 1 (Laptop connected through Ethernet)

The figures 18 and 19 show an average time of 100-120 milliseconds taken by each node (Hal and Bob) to process a HIP packet such as the UPDATE message. The figure 18 also allows to detail the short amount of time T0 (approximately 21ms in average) required by a fixed node of these characteristics to be aware of its new location, update its current LOCATOR and notify its peers of the

recent change. Figure 20 and 21 also show stacked times graphical results and percentages results for scenario and scenario 2 respectively.

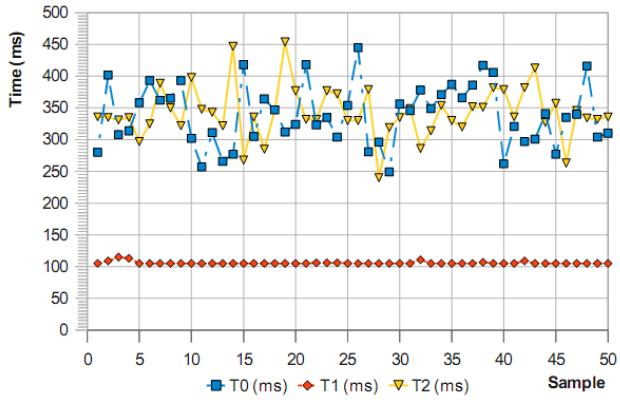

Fig. 19 Time results for HIP Mobility Event Test Scenario 2 (N800 connected through WiFi 802.11g)

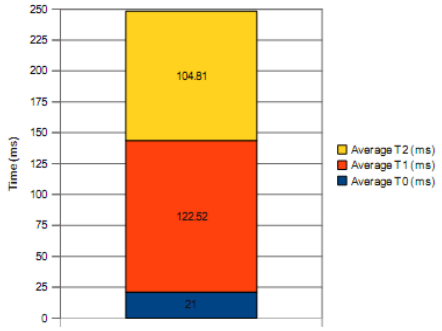

Fig. 20 Stacked time results for HIP Mobility Event Test Scenario 1(Laptop connected through Ethernet)

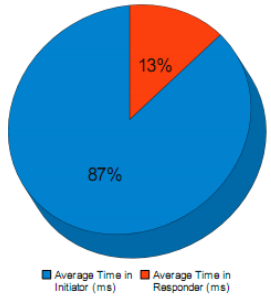

Fig. 21 Average percentages of time consumption of Initiator and Responder during a HIP Mobility Event Test Scenario 1(Laptop connected through Ethernet)

5. Conclusions

The solution proposed by HIP to the location/identifier dilemma in current mobile networks concerns a division of the location/identity identifier used currently in networks (IP address) for a new namespace that will be in charge solely of the identity layer of a node (by means of 128 bits cryptographic identifiers) and leaving the layer of the location of the nodes to the current IP layers, hence, allowing a mobile node to roam between different locations without interfering or changing its identity. This new concept opens a new world of opportunities for new network architectures, services and improvements for mobile devices. Throughout this study, it has been possible to review the basic architecture of the host identity protocol, and achieve a deep understanding and comprehension of the features and advantages provided to solve the current paradigm of location, identity and security on the communications of a mobile node. A test-bench was assembled and configured using one of the best implementations of HIP currently available, the HIPL implementation from the infraHIP project in the Helsinki Institute for Information Technology (HIIT).

The tests performed to verify and validate the main features and characteristics of the protocol such as the basic exchange process, the round trip times for a HIP message, the average throughput for a HIP communication and the process in charge of the LOCATOR parameter update used by mobile nodes. The results obtained in the evaluations were in accordance to the expected results of HIP. Being able to study and evaluate the performance of the protocol guidelines under different scenarios, allowed to obtain a perspective of the different limitations the current implementation of HIPL and the architecture of HIP have.

References

[1] C. Perkins, RFC 2002: “IP Mobility Support”, 2002
[2] R. Koodli, C. Perkins, RFC 4988: “Mobile IPv4 Fast Handovers”, 2007
[3] R. Koodli, RFC 4068: “Fast Handovers for Mobile IPv6”, 2005
[4] Andrei Gurtov, “Host Identity Protocol (HIP): Towards the Secure Mobile Internet”,2008, Wiley, ISBN: 978-0-470-99790-1
[5] Andrei Gurtov, Miika Komu and Robert Moskowitz, “Host Identity Protocol”, Cisco The Internet Protocol Journal, Volume 12, No.1 2009
[6] P. Nikander, T. Henderson, C. Vogt, J. Arkko, RFC 5205, “End-Host Mobility and Multihoming with the Host Identity Protocol”, 2008
[7] Andrei Khurri, Ekaterina Vorobyeva, Andrei Gurtov, “Performance of Host Identity Protocol on Lightweight” Hardware”, ACM/IEEE MobiArch '07 2007
[8] InfraHIP. Infrastructure for HIP, 2009, http://infrahip.hiit.fi/index.php?index=download
[9] OpenHIP Project, , http://www.openhip.org/
[10] FreeBSD implementation of HIP, 2009, http://www.hip4inter.net
[11] R. Moskowitz, P. Nikander, P. Jodela, T. Henderson, RFC5201: “Host Identity Protocol”, 2008