IP mobility enhancements for heterogeneous wireless networks

Zeynep Gurkas Aydin

THESE DE DOCTORAT CONJOINT TELECOM SUDPARIS et L'UNIVERSITE PIERRE ET MARIE CURIE

Spécialité :

Informatique

Présentée par

Gülsüm Zeynep GÜRKAŞ AYDIN

Pour obtenir le grade de

DOCTEUR DE TELECOM SUDPARIS

Améliorations la prise en charge de la Mobilité dans les Réseaux sans fil Hétérogènes

Soutenue le 30 Janvier 2014 devant le jury composé de :

Steven MARTIN	Rapporteur	Maître de Conférences (HDR) à l'université Paris Sud
Nathalie MITTON	Rapporteur	Chargé de recherche (HDR) à INRIA
Rami LANGAR	Examinateur	Maître de Conf. (HDR) à l'université Pierre et Marie Curie
Alexis OLIVEREAU	Examinateur	Ingénieur Chercheur à CEA Saclay
Anis LAOUITI	Examinateur	Maître de Conférences à Telecom SudParis
Hakima CHAOUCHI	Co-directrice	Professeur à Telecom SudParis
Tülin ATMACA	Co-directrice	Professeur à Telecom SudParis
Halim ZAİM	Co-encadrant	Professeur à l'université d'Istanbul

Thèse n° 2014 TELE0006

Doctor of Science Thesis Telecom & Management SudParis and Pierre & Marie Curie University

Specialization

Computer Science

presented by

Gülsüm Zeynep GÜRKAŞ AYDIN

Submitted in partial satisfaction of the requirements for the degree of

Doctor of Science
TELECOM SUDPARIS

IP Mobility Enhancements for Heterogeneous Wireless Networks

30 January 2014, committee in charge:

Steven MARTIN	Reviewer	Associate Professor (HDR) at University of Paris Sud
Nathalie MITTON	Reviewer	Senior Researcher (HDR) at INRIA
Rami LANGAR	Examiner	Associate Prof. (HDR) at University of Pierre & Marie Curie
Alexis OLIVEREAU	Examiner	Research Engineer at CEA Saclay
Anis LAOUITI	Examiner	Associate Professor at Telecom SudParis
Hakima CHAOUCHI	Co-director	Professor at Telecom SudParis
Tülin ATMACA	Co-director	Professor at Telecom SudParis
Halim ZAİM	Co-supervisor	Professor at Istanbul University

Thèse n° 2014 TELE0006

Acknowledgement

First and foremost I wish to thank my advisor Professor Hakima CHOUCHI for her patience, for being inspirational and supportive during this thesis. I would like to thank for her all valuable guidance, willingness to help and knowledge. I wish to gratefully thank to the encouragement of my co-advisor Professor Tülin ATMACA for her great support, observations and ideas during this study. They gave me the opportunity of joining Telecom SudParis and Laboratory Samovar during my thesis.

I would also like to show my gratitude to my co-supervisor Professor Halim ZAIM, who supported me with his great advising during my studies in Istanbul.

I would like to thank my colleague Özgür Can TURNA for his friendly and endless support. I deeply appreciate the help of him in my thesis.

I am also grateful to my friend Apostolia PAPAPOSTOLOU for her generous friendship while I was in Paris. I would like to thank Tara Ali-YAHIYA who we shared many ideas and studied at Telecom SudParis. I have learned various things from her. I also thank to my colleague Ergün GÜMÜŞ for his generous support to my thesis in İstanbul.

I would also like to thank Françoise ABAD; she was always very kind and generous in helping me to solve tedious administrative works.

The work described in this thesis would not have been possible without the generous financial support from Istanbul University, Telecom SudParis, Scientific and Technological Research Council of Turkey and Council of Higher Education (Turkey).

To my family, thank you for your love, support, and unwavering belief in me.

Finally, I would like to thank my husband Ali AYDIN for his unconditional love and support during this study. He endlessly encouraged me to put up with all challenges of doing a PhD. He has been extremely patient, helpful and devoted to me.

G. Zeynep GÜRKAŞ AYDIN
December 2013, Paris

I dedicate this thesis to my beloved daughter Melek Bahar, my husband Ali and my family…

Résumé

Au cours des dernières décennies, le besoin pour des communications multimédia en mobilité est devenu indéniable dans les réseaux de type IP, ainsi la gestion de la mobilité et la continuité de session est depuis plusieurs années un problème de recherche très important aussi bien pour le milieu académique que industriel. Comme l'hétérogénéité des réseaux d'accès est en perpétuelle évolution, l'intégration des différents types de réseaux sans fil au niveau de la couche IP est devenue un domaine de recherche difficile et inévitable. La gestion de la mobilité basée sur des protocoles IP même si elle a une maturité en termes d'âge mais n'est pas encore assez efficace pour être utilisée pour le déploiement de services à grande échelle.

L'un des problèmes les plus importants liés à l'exécution de la gestion de la mobilité concerne le fait que la couche d'application souffre de la modification d'adresses IP au cours du mouvement du nœud mobile alors que celle-ci construit sa session sur la base de l'adresse IP de connexion au réseau. Une nouvelle approche d'amélioration de la prise en charge de la mobilité propose de séparer l'identification de session et l'identification de l'emplacement ou l'attachement au réseau. Plus précisément, jusqu'à présent, l'adresse IP jouait ces deux rôles : comme localisateurs de l'attachement de la machine au réseau et comme identificateurs de cette machine qui sert justement à l'identification de la session sur laquelle se construit l'application. Donc, par la séparation de ces deux concepts, les sessions ne sont pas identifiés par les adresses IP qui elles sont dynamiques puisque la mobilité dans le réseau impose le changement d'adresse IP, mais les nouveaux identificateurs uniques qui définissent un nœud et qui ne change pas à cause de la mobilité ce qui offrirait une stabilité pour le niveau applicatif. Cette nouvelle approche doit introduire une nouvelle couche dans la pile protocolaire TCP / IP, juste au-dessus de la couche IP. Celle-ci gérera les nouveaux identificateurs des nœuds.

Selon ces concepts, Host Identity Protocol (HIP) est l'une des solutions dominantes en recherches qui est proposé par l'IETF (Internet Engineering Task Force) et l'IRTF (Internet Research Task Force). Ce protocole se propose de résoudre le problème de localisation / identification en incluant également le support de la sécurité au niveau du nœud.

Dans cette thèse, le protocole HIP est principalement examiné et de nouvelles améliorations de la mobilité sur la base de ce protocole ont été conçus et mises en place.

Dans la première partie de la thèse, une structure hiérarchisée du réseau pour le protocole HIP et un nouveau mécanisme de gestion de transfert[1] ont été conçus dans le but de proposer une solution pour les imperfections existantes pour le support de la mobilité par le protocole HIP. Ce nouveau procédé vise à démarrer la mise à jour d'emplacement d'un nœud mobile de façon proactive dans HIP de façon à améliorer le temps de transfert intercellulaire (Handover) et la latence dues aux procédures d'enregistrement des nouvelles adresses IP d'attachement au réseau. Une évaluation de cette approche est proposée pour montrer les avantages de cette nouvelle méthode quant à l'amélioration de la continuité de session de bout en bout en mobilité du nœud. En deuxième partie de cette thèse, une extension du processus d'enregistrement proactif a été conçue avec le protocole eHIP. Cette extension, a pour but de déclencher le début de la mise à jour de l'adresse d'un nœud mobile en recherchant le trajet durant sa mobilité le plus tôt possible. Les performances d'eHIP ont aussi été analysées en considérant la vitesse du nœud mobile. Dans la troisième partie, une proposition de déploiement de nœud de capteur sur la topologie du réseau mobile montre l'amélioration de la phase de détection de mouvement d'eHIP et par conséquent de la proactivité d'enregistrement lors de la mobilité.

Dans la quatrième de cette thèse, une évaluation de l'architecture et du protocole est proposée sous simulation. L'algorithme proposé a été comparé avec des algorithmes similaires de sélection de chemin d'accès hiérarchique. Dans la cinquième partie de l'étude, le protocole HIP a été testé sur une plateforme réelle du réseau et l'utilisation de la mise en œuvre d'infraHIP. Divers paramètres sur deux scénarios différents ont été observés et les résultats ont été obtenus.

Mots clés

Mobilité, gestion de la mobilité, la gestion de transfert, Handover, la fonction de décision de transfert, la détection de mouvement, Host Identity Protocol, localisateur / identifiant, HIP

[1] "Handover" et les termes de "transfert intercellulaire (handoff) " sont utilisés alternativement dans cette thèse car ils se réfèrent à un même contexte et le sens.

Abstract

Over the last decades, with rapid and tremendous growth of IP networks in mobile and wireless environments, mobility management and session continuity has become a more important issue. As the heterogeneity increases in network environments and gradual spread of Internet of Things wave, the integration of different types of wireless networks in the IP layer became a challenging and inevitable research area. Mobility management based on IP protocols is not yet efficient enough to be used for large-scale service deployment.

One of the most important issues related to the performance of mobility management is related to the fact that the application layer suffers from the changing of IP addresses during the movement of the mobile node. It is expected the network layer and above layers to be aware of movement of mobile nodes. In fact, the application layer established and ongoing sessions rely on the current IP address and the port number pair. New wave in the improvement ideas on this concept is separating the session identification and the location identification in the network. More precisely, up to now the IP address was playing these two roles: as locators and as identifiers. So, by separating these two concepts, the sessions are not identified according to IP addresses but the new unique identifiers that define a node. This avoids the applications to suffer when the IP address changes during the mobility. This new approach needs to introduce a new layer in the TCP/IP protocol stack, on top of the IP layer that will handle the new identifiers that correspond to the current IP address or new complete architecture designs which are inheriting locator/identifier separation idea.

According to these concepts, Host Identity Protocol (HIP) is one of the dominant and prominent researches work that was proposed by the IETF (Internet Engineering Task Force) and IRTF (Internet Research Task Force). This protocol proposes to solve the locator/identifier split problem by also including the security support which is a serious issue in securing mobile nodes new registrations to the network. In this thesis, predominantly HIP protocol is examined and new mobility enhancements based on this protocol have been designed and introduced.

In the first part the thesis, a hierarchical network structure for HIP protocol and a new handover[2] management mechanism have been designed in order to propose a solution for especially HIP's existing imperfections about mobility management. This new method aims to start the location updates of a mobile node earlier than the way defined in HIP during its real time mobility and so to enhance the handover time and latency. The advantages of this new method have been observed in accordance with HIP's end-to end mobility management.

In this thesis's second part, a prediction extension has been designed for eHIP method. This extension, aims to trigger the early update of a mobile node by investigating the path during its mobility earlier than eHIP. The success of this method has been examined with integration of this extension to eHIP method and successful decisions made both with and without taking into account the mobile node's speed. Besides, it the third part, a sensor node deployment over the network topology has been considered to improve movement detection phase of eHIP. This scheme embraces some principle positioning techniques and location estimation assisted handoff decision support for eHIP.

In the fourth part of this thesis, a system model and a related mobility algorithm considering QoS factor has been investigated where the network structure is taken into consideration as a mesh network and suitable for network architecture proposed for eHIP. The proposed algorithm has been compared with similar hierarchical path selection algorithms. In the fifth part of the study, HIP protocol has been tested on a real network testbed and using infraHIP implementation. Various parameters on two different scenarios have been observed and results have been obtained about HIP's behaviors on real network environments.

Key Words

Network mobility, mobility management, handoff management, handover decision function, early update, movement detection, Host Identity Protocol, locator/identifier split idea, wireless communications, HIP

[2] "Handover" and "handoff" terms are used alternately in this thesis since they refers to the same context and meaning.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AP : Access Point
ANP : Access Network Protocol
BE : Base Exchange
BNP : Backbone Network Protocol
CN : Corresponding Node
DDMS : Dynamic Distributed Mapping System
DH-HIP : Dynamic Hierarchical HIP
DNS : Domain Name Server
eHIP : Early Update for HIP
EID : Endpoint Identifier
ESP : Encapsulating Security Payload
ETR : Egress Tunnel Router
EU : Early Update
FMIP : Fast Mobile IP
FU : Finish Update
H1 : Hierarchy Level 1
H1H : H1 Handover
H2 : Hierarchy Level 2
H2H : H2 Handover
HI : Host Identity
HILL : Host Identifier and Local Locator
HIP : Host Identity Protocol
HIT : Host Identity Tag
HL : Handover Latency
HO : Handover/Handoff
I : Initiator
ICMP : Internet Control Message Protocol
IETF : Internet Engineering Task Force

ILNP : Identifier Locator Network Protocol
INET FW : INET Framework
IRTF : Internet Research Task Force
ITR : Ingress Tunnel Router
LISP : Locator/Identifier Separation Protocol
LISP_ALT : LISP-Alternative Topology
LRVS : Local Rendezvous Server
LSI : Local Scope Identity
MCP : Mobility Control Protocol
MIP : Mobile IP
MN : Mobile Node
MOFI : Mobile Oriented Future Internet
NGWN : Next Generation Wireless Networks
NLS : Network Location Server
p-eHIP : Predictive eHIP
PMIPv6 : Proxy Mobile IPv6
QFDD : Query-First Data Delivery
QoS : Quality of Service
R : Responder
RA : Router Advertisement
RS : Router Solicitation
REGR : Registrar
REQR : Requester
RLOC : Routing Locators
RVS : Rendezvous Server
SA : Security Association
SAP : Service Announcement Packet
URP : User Identifier Resolution Protocol
TCP/IP : Transmission Control Protocol/Internet Protocol
UMTS : Universal Mobile Telecommunications System

List of Symbols

S_d	: Set of detected sensor nodes
x_n, y_n	: Position of a detected sensor node
x_m, y_m	: Estimated location for MN
N	: Number of detected sensors
x_r, y_r	: Position of reference APs
d_{mr}	: Distance between estimated location of MN and reference AP
PoA_{est}	: Estimated best appropriate AP for MN
T_D	: Discovery delay of L2 handoff.
T_{AUT}	: Authentication delay of L2 handoff.
T_{AS}	: Association delay of L2 handoff.
T_{L2}	: Total L2 handoff delay
T_{probe}	: Probe delay
T_{HIP}	: Total HIP UPDATE delay
T_{UF}	: Delay for generating the first UPDATE packet
T_{U2}	: Delay on responder side to process an UPDATE message
T_{U3}	: Delay on initiator to respond to the echo request
T_{HIP}^{HO}	: Total handoff delay of HIP
T_{LE}	: Location Estimation Time
T_{SP}	: Time for sensing all sensors within coverage and creating the SENSOR_ID
T_{MN-NLS}	: Time for sending SENSOR_ID list to NLS

T_{est} : Time for location estimation on NLS

T_{NLS-MN} : Time for sending the EST_LOC_POA to MN

E_{scan} : Total consumed energy during IEEE 802.11 scanning

T_{total}^{MN} : Total duration of mobile node's movement

T_{scint} : Scanning interval

P_{scan} : Power consumed during scanning phase

E_{SP} : Total consumed energy during sensing phase

T_{spint} : Sensing interval

P_{sense}^{MN} : Power consumption during T_{spint}

T_{wt} : Waiting time

$P_{recSensor}^{MN}$: Power consumption during T_{wt}

α : The proportion of the amount of signaling messages generated by MN

β : The proportion of data packets among the total traffic generated by MN

m_{sig} : The average size of signaling messages used for registration updates

m_{data} : The average size of data packets used for registration updates

$1/\mu$: The mean sojourn time of a MN in a subnet

λ : Downlink packet transmission rate (packets/s)

Π_i : The probability that the MN is located at the subnet AP_i

N_l : The total number of directional links in the whole network

D_{max} : The maximum tolerable delay for the VoIP application when handing over from one domain to another

T_{start} : The time when the MN starts to send the first packet of registration

T_{end} : The time when the CN starts to receive the first packet of data.

1 Introduction

Due to the complexity of wireless environments, it is hard to provide efficient quality of service, seamless connectivity and high data rate among others. Indeed, to provide anytime and anywhere connectivity for mobile users is an increasing need in current legacy Internet. Also, heterogeneous environments that gather up several radio access technologies such as WiFi, GSM, GPRS, WiMax etc. and lately LTE (Long Term Evolution), reveals several issues to be addressed such as mobility, multi homing, ,security, high quality of service (QoS) and seamless handover. Under the influence of all these advances on communication technologies, users also demand anywhere-anytime connectivity for different types of applications and devices without sensing the heterogeneity of underlying environments.

One of the most attractive challenges on next generation networks (NGN) has been mobility management techniques. In traditional TCP/IP architecture, a host/node is identified by its IP addresses. These addresses also define the host location in the network; meaning its network attachment. When mobile devices move in the network, they change their IP addresses, and consequently, their transport, application and session layers fell to be interrupted because of these frequent changes of IP addresses. Besides, during their movement, mobile hosts need to prove their identity to their peers in a secure way. For this purpose, legacy IP architecture needs to be modified to include the secure mobile host notification to its peers. IP address space is vulnerable to different types of security threats. TCP protocol of TCP/IP stack provides secure and reliable connection oriented services which are strictly bound to IP addresses for connection establishment. The need for updating the IP address for successful routing of packets on network layer, suffers the transport and application layer establishments.

Mobility management is used for all steps of mobility related issues which are handoff and location management. Location Management term defines the updating operating of a mobile node to concerning system elements, while handoff management defines set of operation related to moving between two different point of attachments within a network even during ongoing communications. Handoff management solutions are both literally respect to link layer and network layer. The main aim of mobility management techniques is simply providing seamless connectivity while moving across different point of attachments. In addition, handoff management and identification of hosts are strictly related to each other because all current handoff solutions are affected by mobile node's identification method in current TCP/IP architecture (TUNCER, et

al., 2012). Mobility management also can be classified as macro and micro mobility scopes. While macro mobility refers to movement across different administrative network domains, micro mobility is related to movement among different access points in the same administrative domains (ZEKRI, et al., 2012) .

Mobile IP has been the key protocol in order to overcome the limitation of original TCP/IP architecture and other well-known protocols have revealed based on Mobile IP. While some of them can be categorized as host-based mobility solutions such as Hierarchical Mobile IP (HMIPv6) and Fast Handovers for Mobile IP (FMIPv6), some of them can be categorized as network based solutions such as Proxy Mobile IP (PMIPv6) and Network Mobility support in IPv6 (NEMO). However, all Mobile IP based protocols still use IP addresses to identify mobile nodes and try to improve mobility capabilities in all-IP networks.

Based on the existing challenges and works on this problem, the need for a new mobility context which provides both host based and network based support for mobility was introduced (KAFLE & INOUE, 2010).Locator/Identifier Split idea has been proposed by IETF community as a sweeping new approach for Internet architecture to solve the common usage of IP address space as host identifiers and locators (GURTOV, et al., 2009). Several proposals are under considerations which are summarized in Chapter 2 of this thesis, but the most intense solutions are HIP and LISP from two different point of views. Although they are both protocol type designs, HIP is concentrated on host based, end-to-end and secure mobility and multi homing support, LISP is concentrated on optimizing new features of routing plane which is not the purpose of this thesis.

1.1 Research Objective

The main objective of this thesis is concentrating on mobility management issues for Host Identity Protocol (HIP), which is the dominant and most comprehensive approach for locator/identifier separation idea. Since HIP embraces macro mobility features regarding to mobility management, it lack from capacity of handling micro mobility in an effective manner. Seamless handoff has always been a challenging issue for IP based networks and as the heterogeneity increases, the demand on anywhere-anytime connection also grows.

Regarding the micro mobility problem of HIP, in this thesis we aim to propose a handoff enhancement that also meets QoS requirements. Our first goal is to design an appropriate network architecture that adopts a hierarchical approach and to use this architecture for our handoff enhancement. After introducing the handoff enhancement, we followed the idea of improving this handoff mechanism by inheriting the prediction idea. With this predictive approach, we aimed to improve the movement detection phase. Also, regarding the path selection problem in network hierarchy, we aim to propose an algorithm that meets QoS requirements.

1.2 Organization of the thesis

This thesis is organized as follows. Chapter 2 present the state of the art of locator/identifier split paradigm and related protocols.

In chapter 3, a hierarchical network structure for HIP protocol and a new handoff management mechanism have been presented. In Chapter 4, a prediction extension has been depicted for eHIP method that aims to trigger the early update of a mobile node by investigating the path during its mobility earlier than eHIP. Chapter 5 also introduce a new improvement on eHIP to advance movement detection phase of eHIP by deployment of sensor nodes in the network and using some principle positioning techniques and location estimation algorithms. A system model and a related mobility algorithm considering QoS factor has been investigated where the network structure is taken into consideration as a mesh network and this model has been presented in Chapter 6. In Chapter 7, HIP protocol has been tested on a real network testbed and using infraHIP implementation to observe HIP's behaviors on real network environments. Finally Chapter 8 concludes and summarizes our contributions and points out some future directions for our work.

2 State of the Art

2.1 Locator/Identifier Split Paradigm

The transition attempts from current Internet architecture to Internet of Things (IoT) where heterogeneous wireless networks are co-existing in the network access, brings out many changes in network environments and communication area. The development of IoT environments is growing as expected from individuals to industrial environments. By this development, importance of communication of different objects reveals out, although they were not supposed to interact with each other under normal circumstances. Connecting this large set of heterogeneous elements brings out many needs such as discovering, identifying or communication with each other at any time.

IoT also brings out the necessity of identification of nodes throughout the Internet globally and successful accomplishment of mapping operations. Locator/identifier split paradigm drew attention especially for IoT due to these necessities. In today's Internet architecture, two namespaces are used: Domain Name Service (DNS) and IP addresses. These two namespaces serve an important function for Internet based technologies for years. IP addresses have two main functionalities for host. They are used for both as locators and identifiers of a node in the network.

While considering network layer, these addresses identify the topological information of the host and guides to the routing procedures. This common usage of IP address space brings out problems for both session identification and network routing scalability especially for mobile nodes. Regarding to mobility, whenever a host changes its point of attachment, its IP address changes and the location of this host is defined by this new address. When viewed from the aspect of transport and upper layers, IP addresses have another role as identifying the host during their communications and connections. This is the identifier role of IP addresses. From this point of view, these ongoing communications and connection suffer from IP address changes even when the host changes its location (SO-IN, et al., 2012).

For recent years, IETF and IRTF has deep discussions on locator and identifier separation idea. They mainly propose to use two different namespaces as end system identifiers and routing locators (QUOITIN, et al., 2007). Besides the main advantages mention until now, it is also aforementioned to have benefits such as reduced routing table size in core network and enhancing traffic engineering features.

There are many prominent works about locator identifier split paradigm such as Host Identity Protocol (HIP), Locator Identifier Separation Protocol (LISP), and Identifier Locator Network Protocol (ILNP), and Mobile Future Internet (MOFI) that we summarize hereafter.

2.1.1 Host Identity Protocol (HIP)

Host Identity Protocol (HIP) is proposed by IETF (Internet Engineering Task Force) (IETF, 2013) and IRTF (Internet Research Task Force) (IRTF, 2013) as a locator/identifier separation solution.

HIP also brings extra features as an alternative to Mobile IP for security, mobility etc. HIP approach requires adding a new layer in the TCP/IP stack between the transport layer and the IP layer. The role of this layer is to make mapping between host identities, which are used in upper layers of TCP/IP stack. With the fast spreading of Internet usage and new demands, some traditional TCP/IP technologies became insufficient. The need of moving between different networks and connecting to different types of networks at the same time has been revealed in time. Besides, security holes have also been revealed with the rapid improvement of Internet and these security holes affect the improvement of the existing IP mobility management systems. HIP is also fully compatible with TCP/IP architecture and has been developed to be a solution to all these problems (GURTOV, 2008).

HIP approach requires adding a new layer in the TCP/IP stack between the transport layer and the IP layer (MOSKOWITZ, et al., 2008). The role of this layer is to make mapping between host identities, which are used in upper layers of TCP/IP stack. One of the design choices defined in HIP is, that the Host Identity (HI) is the public key from a public/private key pair. This key can be represented by the Host Identity Tag (HIT), a 128-bit hash of the HI, and has to be globally unique in the whole Internet universe. Another representation of the HI is the Local Scope Identity (LSI), which is 32-bits size and can only be used for local purposes. Host Identity (HI) is the public key from a public/private key pair. HIP and its basic functionalities are defined in RFCs numbered between 5201 and 5206. Figure 2.1 shows the HIP layers and the main difference from traditional IP stack in terms of introducing host identities.

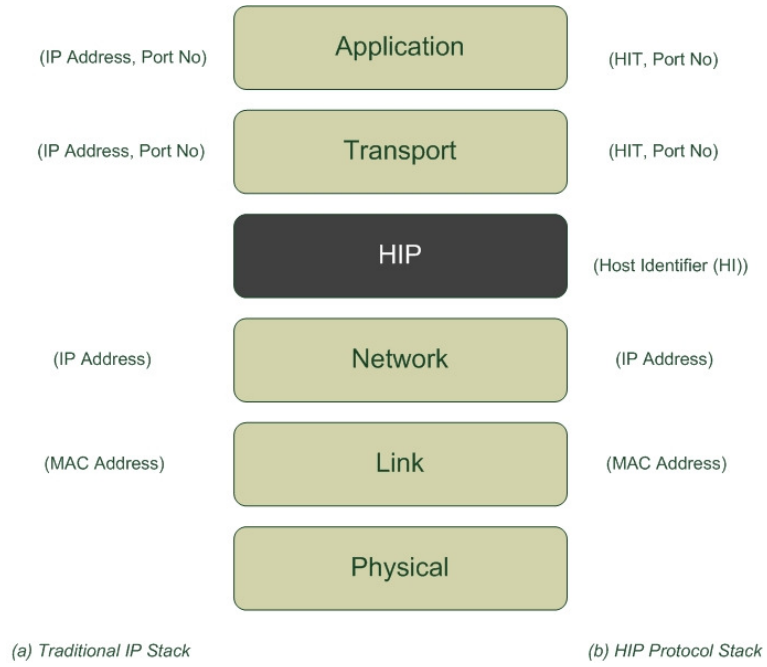


Figure 2.1: Host Identity Protocol in TCP/IP protocol stack

2.1.1.1 HIP Namespace

HIP introduces a new namespace composed of Host Identities (HIs). A Host Identity is a cryptographic entity, which corresponds to an asymmetric key-pair. The public identifier associated to a HI is consequently the public key of the key-pair. A host may have more than one HI's but this HIs are uniquely related to a single host. HIs will assume the identifier role in upper layers. HIs become public if they are stored in DNS. The length of the HI depends on the cryptographic algorithm used. In order to cope with the problems that may occur in upper layers, two fixed length identifiers are defined in HIP.

- Host Identity Tag (HIT)

A Host Identity Tag is a 128-bit representation for a HI. It is a cryptographic hash over HI. There are two advantages of using a hash:

1. It is fixed length, so it is easier to use in upper layer protocols.
2. It represents the HI in a consistent format to the protocol.

HITs identify the sender and recipient of HIP packet. It is unique. It is rarely possible that a single HIT may represent more than one HI.

- Local Scope Identifier (LSI)

A Local Scope Identifier (LSI) is a 32-bit or 128-bit local representation of HI. It may be needed to use in existing APIs or protocols. It is shorter than HIT as an advantage but just available for a local scope. The 32 bit long version is IPv4 compatible and a 128 bit long version is IPv6 compatible. The relationship between Host Identities and two types of tags are represented in Figure 2.2.

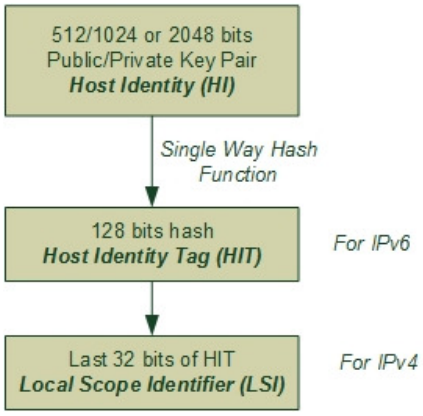


Figure 2.2: Types of Host Identity Tags

2.1.1.2 HIP Packets and Messages

HIP employs eight fundamental packets. Four of them are used in the HIP Base Exchange procedure, one of them is used for the HIP UPDATE procedure, one of them for notifying peers about important information and two of them are used for connection close procedures. These

packets are their basic functionalities are summarized in Table 2.1. Section 2.1.1.3 also analyze the details of the first four packets regarding to the Base Exchange procedure. UPDATE is the packet used for mobility management in HIP and also examined in Section 2.1.1.7.

Table 2.1: HIP Packets and their functionalities

I1	HIP Initiator Packet
R1	HIP Responder Packet
I2	Second HIP Initiator Packet
R2	Second HIP Responder Packet
UPDATE	Update Packet
NOTIFY	Notify Packet
CLOSE	HIP Connection Close Packet
CLOSE_ACK	HIP Connection Close Acknowledgement Packet

2.1.1.3 Base Exchange (BE)

The HIP Base Exchange is a cryptographic key-exchange procedure performed at the beginning of the HIP communication establishment. The HIP Base Exchange is built around a classic authenticated Diffie-Hellman key exchange. The BE is four-way packet exchange between the Initiator (I) and the Responder (R). The four-way handshake of HIP BE is shown in Figure 2.3.

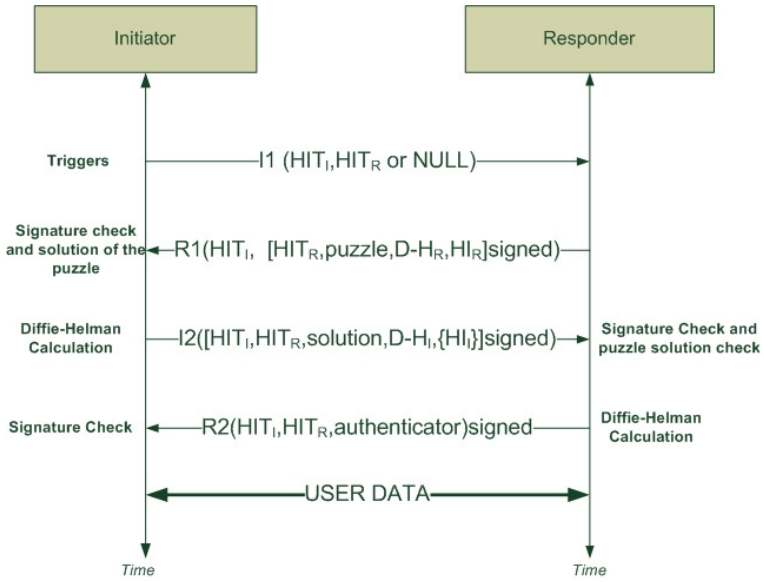


Figure 2.3: HIP Base Exchange

The Base Exchange between two HIP enabled hosts is triggered by an *I1 message*. It contains the HIT of the initiator and HIT of the responder if known. This is the only packet that is not signed during Base Exchange. The responder decides to accept the HIP association request and *R2 message* starts the actual procedure by sending a cryptographic puzzle for initiator, the first part of Diffie-Hellman key exchange and Host Identity (HI). The whole message except puzzle is signed. When the initiator receives the *R1 message*, it solves the puzzle and sends the solution of the puzzle, next step of Diffie-Hellman key exchange, its public authenticator and a signature. The whole packet is

signed and is discarded if the solution of the puzzle is incorrect. The responder calculates its Diffie-Hellman session key. R2 packet ends the BE procedure and Diffie-Hellman key exchange and contains a signature of whole packet in order to protect the initiator from replay attacks.

2.1.1.4 Rendezvous Servers (RVS)

The initial IP address of a HIP host should be stored in order to make the host reachable. Traditionally, the DNS is used for storing this information. The problem with the DNS system is the latency; updating the location information each time the MN moves, the update is not fast enough.

The Rendezvous Mechanism is designed to solve this problem. The Rendezvous Server (RVS) keeps all the related information of HIP communication (LAGANIER & EGGERT, 2008b). The location information of RVS is just stored in a DNS. If a MN wants to communicate with other MNs, those nodes have to register previously with their RVS. Figure 2.4 shows the HIP Base Exchange with RVS.

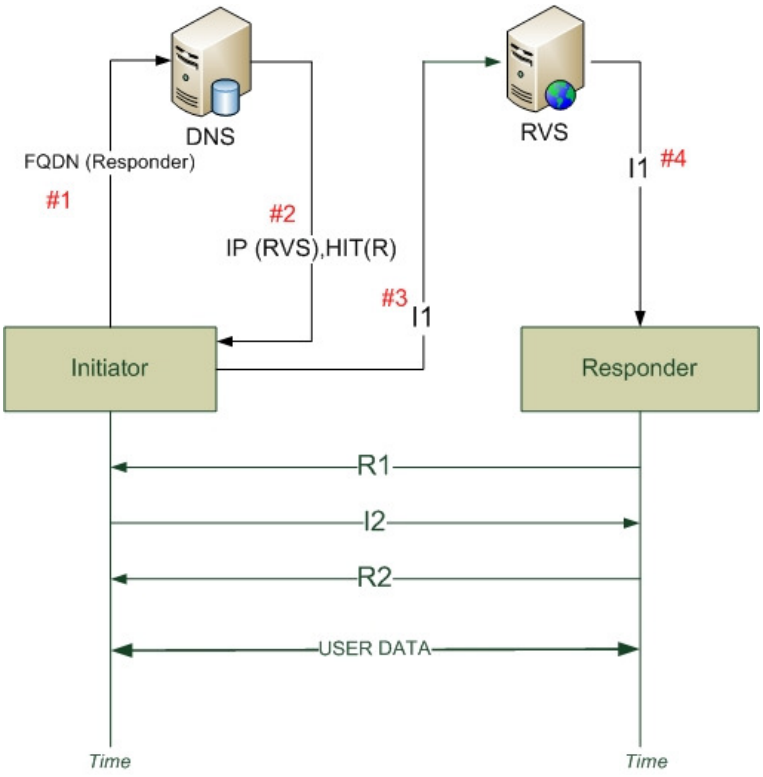


Figure 2.4: HIP Base Exchange with RVS

The HIP enable Responder(R) should register to the RVS with its HIT and current IP address. Firstly, the initiator queries about the responder with FQDN (Fully Qualified Domain Name) message from DNS and DNS response to it with the IP address of RVS that the responders belongs to and the HIT of responder. When Initiator (I) wants to establish a connection with Responder (R), it first sends the I1 packet to one of the Responder's rendezvous servers or to one of IP addresses (if it can be learnt via DNS). The Initiator gets the IP address of Responder's RVS from DNS and sends the I1 packet to the RVS for Base Exchange. RVS checks weather it has the HIT of I1 packet. If HIT belongs to itself, it sends the I1 packet to related IP address. Responder sends the R1 packet directly to Initiator without RVS.

2.1.1.5 Registration Mechanism

The most relevant context regarding HIP registration mechanism is as follows:

- Requester (REQR): HIP node that requests to register for services from registered HIP REGR.
- Registrar (REGR): HIP node that provides registration mechanism for other services or other nodes.
- Service: Service can shortly be defined as activities of HIP protocol.

The procedure, which REGR and the node that requests HIP service use in common, is called registration mechanism (LAGANIER & KOPONEN, 2008a). Each HIP registration has a lifetime. REQR can extend this registration by renewing or updating this procedure.

After REQR discovers new REGR, it starts a HIP BE between them or use an existing HIP connection of REGR. In both cases, REGR examine additional parameters to decide accepting or rejecting this registration. REQR also uses required parameters for registering to provide services. Both REQR and REGR can use special HIP parameters in their messages to specify the registration type.

If a host wants to behave like REGR, it should embed the REG_INFO parameter in all R1 packets which will be sent during all BE setups. But, for temporary failure cases, REG_INFO parameter of R1 packets should be sent by UPDATE packets to enable required services. When a REQR wants to register to an existing service, it creates a REG_REQUEST parameter in I2 packet. Thus, the number of packet sent to REGR will be minimized. A HIP connection can be closed by a REGR in R2 packet by using REG_REQUIRED parameter set as NOTIFY type. In this state, there will be no HIP connection establishment between hosts.

When registration procedure starts, the server identity on REQR I2 packet is checked by REGR. If identity is authenticated, REQR may reach to preferred services. Likewise, preferred service types should be defined in this reply packet and should not include REG_FAILED parameter that is used for registration failure. This reply packet may be a R2 packet of BE or an UPDATE packet. IF REGR can implement identity authentication procedure and REQR has an available identity, then HIP connection is established. REQR may try again to register. The message sequence chart of registration mechanism without active connections is shown in Figure 2.5 and without active connections in Figure 2.6.

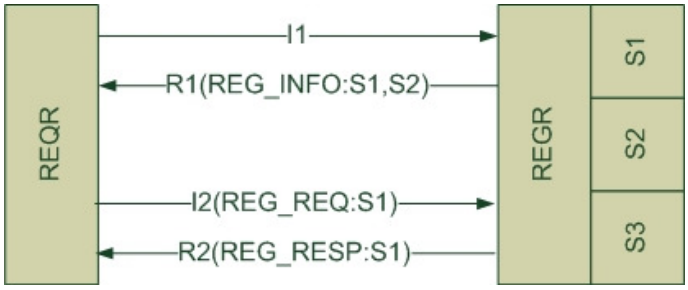


Figure 2.5: Registration mechanism without existing HIP connections

If REG_RESPONSE parameter is processed successfully, registration mechanism is created by REQR side. At the same time, this step shows the successful initialization of registration

mechanism on REGR side. Also the services become available. Both REQR and REGR may cancel their connections whenever they want but before completing the procedure.

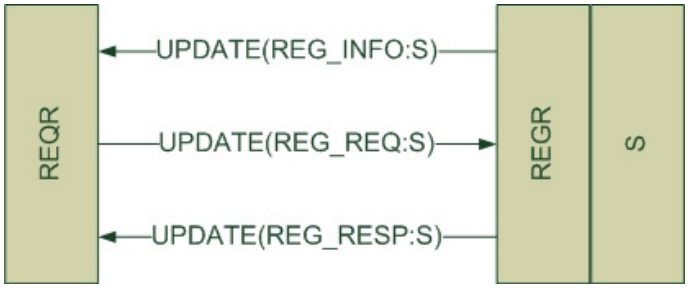


Figure 2.6: Registration mechanism with existing HIP connections

2.1.1.6 ESP Security Association Setup

ESP (Encapsulating Security Payload) protocol provides security association setup between HIP servers by message exchange like BE. During ESP communication HIP server requires information exchange. During this two-way communication, ESP parameters are sent inside I1, R1 and R2 messages as shown in Figure 2.7.

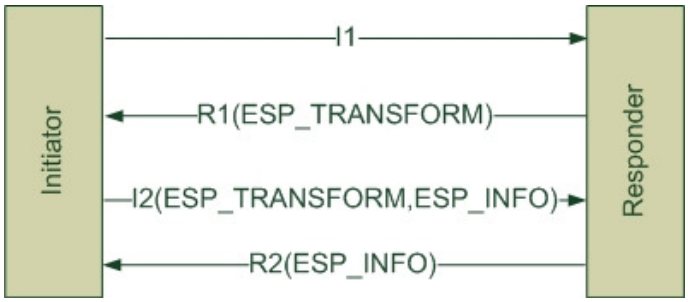


Figure 2.7: ESP Security Association Setup

R1 message includes ESP_TRANSFORM parameter. This parameter is an identifier of its demand to its peers to use ESP. I2 message replies related to this parameter from R1 message. Responder should have been chosen from one of the ESP_TRANSFORM parameters in R1 message and insert this parameter value inside I2 message. Besides, the responder host should also send SPI (Security Parameter Index) values of other connected hosts by ESP_INFO parameter. R2 message finalizes the ESP setup. This R2 message includes necessary SPI information for initiator host.

ESP update procedure use two types of messages. HIP UPDATE message is used for updating the parameters of active ESP security association (SA). UPDATE mechanism and messages are presented in the studies of (MOSKOWITZ, et al., 2008) and (JOKELA & MOSKOWITZ, 2008). Figure 2.8 summarizes this procedure.

Figure 2.8: ESP Update Procedure

A host creates an ESP SA (Security Association) update request and sends it within an UPDATE message. This message includes old SPI value, new SPI value and necessary information about the index value of the next step. If there is a need of creating an index, UPDATE message should include DIFFIE_HELLMAN parameter as in (MOSKOWITZ, et al., 2008). The other side replies by an again UPDATE message via existing active ESP SA as corresponding to this UPDATE message. This message should include new SPI value and ESP_INFO parameter. If incoming UPDATE message includes DIFFIE_HELLMAN parameter, the reply packet should also include DIFFIE_HELLMAN parameter.

2.1.1.7 Mobility and Multi-homing

When a mobile node changes its location in its current network or towards another one, its IP address changes and it should notify its corresponding peers about this change by LOCATOR parameter inside HIP UPDATE messages. In other word, LOCATOR parameter in this packet carries the new IP address to the corresponding nodes.

With this packet, two nodes may either decide to continue their communication with their current connection or decide to re-key their association and generate a new DIFFIE_HELLMAN key. After the first UPDATE message, the corresponding node requires an availability test by ECHO_REQUEST and update exchange procedure ends with mobile node's ECHO_RESPONSE in another UPDATE message. Figure 2.9 shows the basic updating scenario without any rekeying between two nodes. UPDATE messages may include more parameters but the basic parameters are shown in the figure.

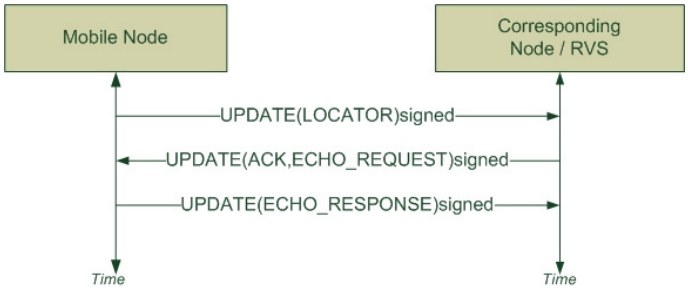


Figure 2.9: UPDATE procedure of HIP

If there is an existing ESP security association (SA), one of the corresponding host may require to setup the SA again and even generate a new DIFFIE_HELLMAN key. All these procedures are triggered by optional parameters inside UPDATE packet.

HIP also has multi-homing support in its nature. In HIP terminology, while the mobility means changing locators, the multi homing means adding new locators for a mobile node. A node with multi homing support might have multiplied the interfaces with multiple IP addresses. A mobile node may inform its corresponding peers about its IP addresses and default address for communication. Information exchange for multi homing issues is provided by UPDATE messages too. LOCATOR parameter of UPDATE packet is used for these actions. It may also specify preferred default address via this parameter. A host should check the availability of these addresses when it receives an UPDATE message in order to prevent wrong updates (NIKANDER, 2008a).

HIP has an architecture that separates network and transport layers by using private/public key pairs instead of IP addresses. When a host runs HIP, all layers identify this host with these identities and IP addresses are just used for packet forwarding. However, every host should know at least one IP address of corresponding hosts. These addresses are the ones used in Base Exchange. New solutions, which are devoted to network layer mobility and host multi homing, reveal according to this layer separation idea.

There are many situations that basic end-to-end addressing stands insufficient such as reachability of a host, location privacy, synchronous mobility of host and NAT (Network Address Translation) traversal issues. At this point, HIP RVS takes an important role for network functionality.

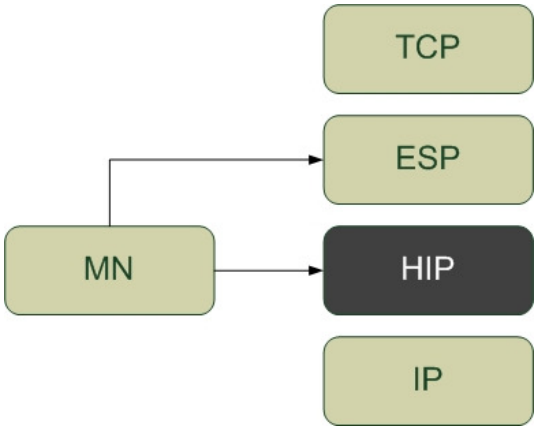


Figure 2.10: HIP protocol layer structure while using ESP

Figure 2.10 depicts the layered structure of HIP which inherits ESP transport format. Upper layers use HITs instead of IP addresses to identify a host. HIP layer functions this mapping between HITs and IP addresses. SPI is used for mapping the incoming packet with the right HIT.

***Locator* Parameter**

Locator parameter defines a point of attachment to a network and includes per-host multiplexing or end-to-end tunneling contexts in order to decide how packets are handled below HIP layer. HIP does not determine its behavior to lower layer packets not only by the effect of IP addresses. In some multi-homing scenarios, IP address-transport port mappings or SPI-IP address mapping might be needed. In these cases, LOCATOR parameters act like traditional network addresses.

Mobility

When a host moves to a different address, it should notify its CNs by a HIP UPDATE packet containing a Locator parameter. CN verifies this UPDATE packet. To provide security, when a packet gets lost, it may be sent again according to HIP. Data content may be checked by signature and hash to provide authentication.

Multi Homing

A host (mobile or fixed) may have more than one interface or global address. This host notifies the corresponding peers about his extra interface/address with LOCATOR parameter. ESP should establish different security associations for each of interface or address inside multi locators. This

allows for simultaneous packet transmission instead of sequential transmission. If more than one locator is sent to corresponding host, one of them should be set as "preferred" one.

In multi homing, the sender may have more than one available locator. In practice, in a multi homed structure, HIP connection may both have preferred host locator and preferred local locator.

2.1.1.8 Security

One of HIP's most important features compared to other mobility protocols is its inbuilt security. IPSec (KENT, 2005) is required for identity authentication to be used for connection setup. During this procedure, SA (Security Association) mechanisms should also continue for a secure ESP connection. Also, HIP identifier are public keys, so this identifier both protects against possible attacks and recognizes HIP packets. As last feature, the effects of DoS attacks are reduced. Besides all the features, HIP still has some security challenges.

Data carried over HIP packets are only reachable by hosts which share the same HIP connection. Thus, even there is no secure connection communication channel between two hosts, they can communicate with each other in a secure manner. Security in HIP protocol is provided by an agreeable collaboration of all these mechanisms. Any disruption in any of these mechanisms leads to security challenges.

2.1.2 Locator/Identifier Split Protocol (LISP)

Locator/Identifier Split Protocol (LISP) is network layer based protocol that is developed by IRTF and it inherits locator/identifier split approach. It is a type of "map and encap" protocol, namely IP-over-IP tunneling type protocol. LISP pledge to practice locator/Identifier split idea without modifying the TCP/IP protocol stack with additional layers. LISP and its fundamental functionalities are defined in RFC 6830 (FARINACCI, et al., 2013). LISP is mainly concentrated on routing scalability problem that arises due to dual role of IP addresses in the network. LISP offers its main functionalities on routers, not on stack layers or existing databases on Internet.

LISP propose to separate the IP addresses into two types of numbering context: Routing Locators (RLOC) and Endpoint Identifiers (EID). Routing Locators define network point of attachments (generally routers) that are used for routing of packets throughout the network. Endpoint Identifiers are used for numbering of devices independent from network topology and they are non-routable identifiers. Both RLOCs and EIDs are syntactically identical to IP addresses but they functions in different ways.

LISP is composed of two system planes as data plane and control plane. Data plane is responsible for map-and-encap operations whereas control plane is responsible for EID-RLOC mapping operations. Briefly, LISP is capable of managing a data traffic generated by devices with non-routable EIDs and forwarding and routing them inside the network based on RLOCs. Certainly, a mapping database is used for these operations.

In map-and-encap approach, "map" phase refers to the operation of any border router that maps the destination EID of a packet coming from a source inside its domain. Border router demands for a mapping of destination EID to a RLOC in the destination domain entry point from main mapping system service. Then, in "encap" phase, it encapsulates the packet and insert the returned

RLOC value as destination address. The destination border router encapsulates the packet and forwards to its main destination inside its domain.

Map-and-encap type schemes operate by appending a new header to packets in a way to include EIDs and RLOCs. These types of schemes generally do not require host based modification but require routing system modification on core network. (MEYER, 2008)

2.1.2.1 Routing Locators (RLOC) and Endpoint Identifiers (EID)

RLOC is an IPv4 or IPv6 address of an Egress Tunnel Router (ETR) (described in section 2.1.2.3). RLOC is obtained by querying the mapping database. EIDs may be mapped to one or more RLOCs. RLOCs are always IP addresses that are assigned to routers.

EID is a value of 32 bit length (such as IPv4 addresses) or 128 bit length (such as IPv6 addresses). The same length is used in order to provide identical structure with IP addresses. LISP use these values as source and destination address in LISP packets. A host may obtain the EID at the beginning by querying a DNS server (similar to DNS look up for HITs in HIP) or via a SIP (Session Initiation Protocol) establishment. EIDs should be globally unique in the network. EIDs are usually defined according to organizational structures. That also means that EID mappings may have hierarchical and localized structures inside a network. EIDs are always IP addresses that are assigned to hosts.

An EID-RLOC Database keeps all mappings of these two numbering spaces. This database should be a globally distributed database.

2.1.2.2 LISP Packets

LISP defined three main types of packets to be used especially in EID-RLOC mapping operation: Data Probe, Map Request and Map Reply. Data Probe is the packet type which an Ingress Tunnel Router (ITR) (described in section 2.1.2.3) sends to mapping system for query. When the related ETR receives this type of packet, it replies with a Map Reply packet.

Map Request is the packet type that an ITR send to mapping system to query for specific EID-RLOC mapping. ETR also replies to ITR with a Map Reply packet similar to Data Probe packet. Map Reply is the packet type that ETR send to ITR just after realizing the incoming LISP packet is Data Probe or MAP Request. It defines two types of packets according to some address values in LISP header.

2.1.2.3 LISP Network Elements

LISP defines two prominent network elements: Egress Tunnel Router (ETR) and Ingress Tunnel Router (ITR). Egress Tunnel Router is the router that accepts the IP packets that includes a RLOC that belongs to it in its header. It encapsulates and forwards the packet according to the value in LISP-encapsulated IP packets.

Ingress Tunnel Router is the router that takes a packet that does not contain a LISP header, performs EID-RLOC mapping from the EID inside this packet and then encapsulates the packet with its globally routable RLOC as source address and returned mapping value as destination

address. This RLOC should not be the real destination; it may refer to an intermediate device close to actual destination EID.

Any router that performs the roles of above two types of routers are also named as LISP Router as a general nomenclature. All LISP routers' functionalities are mostly related to RLOCs.

2.1.2.4 Data Plane and Control Plane

On the whole, map-and-encap operations are under the responsibility of Data Plane. As we explained above, in a LISP enabled domain, a host sends a packet with EIDs as source and destination addresses which are typically obtained from DNS. The ITR of its domain forwards that packet to ETR of the destination domain or any intermediate device/proxy by mapping the correct RLOC. ITR encapsulates the packet before sending to related ETR after obtaining the RLOC from mapping system. Then, ETR decapsulates arrived packet and sends to its real destination. In data plane three types of packets (described in 2.1.2.2) takes role for mapping system.

Since packets are sent by EIDs as destination addresses and EIDs are not globally routable on internet, RLOCs should have been obtained for destination EIDS, especially for packets moving among different domains through Internet. So, EID-RLOC mapping system has a very key role in LISP and even for other locator/identifier split approaches. Three important parameters while considering a mapping system design is update rate to database, state of mapping required and latency for database lookup (FARINACCI, et al., 2013).

LISP-Alternative Topology (LISP-ALT) (FULLER, et al., 2013) is an alternatively designed control plane scheme for managing EID-RLOC mapping system by using existing Border Gateway Protocol (BGP).

2.1.2.5 Mobility

LISP is concerned with several types of mobility as stated in (FARINACCI, et al., 2013). One of the most relevant one is Fast Endpoint Mobility. It is concerned with point of attachment changes while session continuation is also aimed. Mobile IP mechanisms (MIPv4 and MIPv6) are used with interaction with LISP, but this context is still under point of interest. When a mobile node moves, it need to update its EID-RLOC mappings for its new location. This overhead of procedure is added to one of regular Mobile IP updates. LISP EID-RLOC mapping updates are necessary for communication between the mobile node and home agent (HA) or foreign agent (FA).

2.1.2.6 Security

LISP security is mainly related to mapping schemes. The LISP-SEC study introduces the security mechanisms for LISP that provide authentication, integrity and anti-replay protection for LISP's EID-to-RLOC mapping data (MAINO, et al., 2011). LISP-SEC provides different mechanisms for different types of security threats. One of these security mechanism aim to prevent insertion of unauthorized mapping data. Due to the related former studies of LISP-SEC, it assumes that any kind of attack, such as Man in the Middle attacks can be captured in access network, out of LISP mapping systems. LISP-SEC also provides verification of authorization on EID prefix requests.

2.1.3 Mobile Oriented Future Internet (MOFI)

Mobile Oriented Future Internet (MOFI) is designed as an architecture to support future mobile internet needs based upon locator/identifier split idea. The overall architecture design aims to provide seamless mobility and also propose and design some architecture-specific protocols. MOFI presents three main fundamental blocks such as: Host Identifier and Local Locator (HILL), Query-First Data Delivery (QFDD) and Dynamic and Distributed Mapping System (DDMS).

In MOFI HILL, HID is attached to a host, not to an interface. This is a feature that differentiates MOFI from HIP and LISP. Also, LOC is assigned to a network that the host belongs to, not directly to the host. The HID space is the main contribution of MOFI architecture and it also introduces a new layer for communication like HIP. The modified network elements of routers are responsible for HID an LOC mappings, so MOFI appear like LISP with this feature.

There are also architecture specific protocols designed with this proposal. These are Access Network Protocol (ANP), Backbone Network Protocol (BNP), User Identifier Resolution Protocol (URP) and Mobility Control Protocol (MCP). All are presented in detail in (JUNG & KOH, 2009)

Host Identifier (HID) and Locator (LOC) are two main identifier types and spaces introduced by MOFI. HID is used for identifying a host within Internet. It also includes domain and ISP information. LOC defines the location of a host in the network and used for data delivery to this host. HID is a globally unique address whereas LOC represents a local routable address of the host.

The Access Router and designed mapping services comprise the other functional block of Dynamic Distributed Mapping System (DDMS). To find the location of a host before starting to send packets through network, Query-First Data Delivery (QFDD) takes an important role for especially mobile nodes. The Access Routers keeps all local mapping information between HID and A-LOCs, where A-LOCs (Access LOCs) are used for forwarding packet between host and ARs. They also function in case of multi-homing (JUNG & KOH, 2009) (CHOI, et al., 2013).

2.1.4 A brief comparison among HIP, LISP and MOFI

Although all these three proposals are based on locator/identifier split idea, there are some technical differences among them from different perspectives (YOU & JUNG, 2012).

MOFI is designed as a novel and from scratch approach, while HIP and LISP are compatible architectures with current Internet and TCP/IP stack. LISP was especially developed for routing scaling problems and HIP has security, mobility and multi homing feature in it nature.

MOFI and HIP are similar to each other in terms of introducing new namespaces as host identifiers. Besides, LISP and MOFI are similar to each other in terms of highlighting a router as a network element with new features. LISP introduced ETR and ITR (described in section 2.1.2.3) for map-and-encap features while MOFI introduce AR to use address rewriting, which is another approach regarding the locator/identifier separation techniques. The main difference between them is complexity and overhead issue. LISP Map-and-encap is an easy to use technique but brings additional overhead to system. On the other side, MOFI address rewriting is very simple without additional overhead and bring security challenges to the system.

Regarding the system mapping, each architecture has its own mapping system variations such as LISP-ALT for LISP, DDMS for MOFI. Conversely, HIP introduces a fixed and central mapping system of rendezvous servers in interaction with DNS feature. However, central RVS brings scalability problem for HIP.

2.2 Mobility Enhancements based on Host Identity Protocol

After the description of the location, identified split approach of LISP, MOFI and HIP, we concentrate in this part on HIP protocol and its mobility properties. As we know, Mobile IP is the IETF standard for mobility management since years. It requires little addition to classic IP architecture and fits especially macro mobility requirements very well. HIP is an alternative solution to MIP for macro mobility using the secure Locator/identifier approach. It also has some problems as Mobile IP in terms of micro mobility such as unnecessary signaling load, packet loss and handoff latency. End-Host Mobility and Multi homing procedures for HIP are defined in RFC 5206.

While some of related proposals introduce new network entities to cope with the micro mobility challenges, some of them define new additional messages for regular HIP procedures especially during handover process.

2.2.1 μHIP: Hierarchical HIP

μHIP extends the HIP with a gateway centric network component and paging extension. This new network component is called Local Rendezvous Server (LRVS), thus extends the properties of RVS. μHIP proposes to divide the network domain into various administrative domains; each one is managed by LRVS. In every domain, there is an access network and a LRVS. LRVS is responsible for managing the mobile nodes and connections of μHIP enabled access networks to the Internet. Mobile nodes register their local IP addresses to the LRVS. LRVS maps local and global IP addresses. This is very similar to Hierarchical Mobile IP (HMIP).. LRVS inherits the role of RVS and also acts as a gateway to the Internet.

2.2.1.1 Initiation Mechanism

When a MN enters into a new domain, it needs to start an initiation mechanism to communicate within this domain. After entering to the domain, MN connects to an Access Router (AR) in a regular way. After connection and getting a new local IP address, MN, either starts a HIP discovery procedure or wait for the service announcement of LRVS. After that, MN gets information about the HIT and IP address of the LRVS (BOKOR, et al., 2007) (NOVACZKI, et al., 2006).

2.2.1.2 Intra-Domain Handovers

If a MN (Mobile Node) moves to a different point of attachment within the same domain, it starts to receive service from a different AR in the same LRVS service domain. MN that realizes the change of its IP address updates its record at LRVS with its new IP address. CNs (Correspondent Node) or RVS of the MN are not informed about this movement and updates. LRVS is responsible

for the movements within the domain. Since network components out of the MN's domain are not informed about the movements, signaling overhead, packet loss and handover latency is reduced.

2.2.1.3 Inter-Domain Handovers

If a MN moves between different local domains inter-domain procedures of μHIP are invoked. When arriving at the new domain, MN receives a new local IP address and discovers information about the new LRVS. After MN learns its new HIT and IP address from LRVS, it starts a new registration procedure. Since MN changed its LRVS, it needs to update its RVS and all CNs to keep on communication. But, first thing that it has to do is to update its old LRVS in order to forward its incoming packets to MN's old globally routable IP address until the end of update procedures. After finishing all updates, MN disconnect from it old LRVS or this connection is closed automatically after a timeout value.

2.2.2 Micro-HIP (mHIP)

mHIP is designed as an extension of HIP in order to reduce the unnecessary signaling and control messages . It introduces new network components such as mHIP Agents. There are two types of mHIP agents. All mHIP enabled network components in mHIP network architecture are called mHIP agents. Their main role is during the intra-domain handovers (HON SO & WANG, 2008).

In mHIP, mHIP Gateway Component acts similarly to LRVS in μHIP especially during initiation mechanisms. mHIP routers are able to handle the intra-domain handoff and so load of mHIP gateways and signaling load of handoff is reduced. Multi homing scenario is also included in mHIP whereas there are no explanations about multi homing in μHIP.

2.2.2.1 mHIP Agents

There are two types of mHIP agents defined in this proposal: mHIP gateways and mHIP routers. A mHIP gateway serves as a root router and acts similar to LRVS in μHIP. mHIP gateway keeps the records of MNs within a domain. MN registers to a mHIP gateway. When mHIP gateway receives data or signaling packets, it redirects these packets to the correspondent MN. A mHIP router redirect the HIP based communication to the current location of MN. It also manages the intra-domain handover. With this role, they reduce the load of mHIP gateways and so handover latency is reduced.

2.2.2.2 Initiation Mechanism

When a MN enters into a new domain, it needs to start an initiation mechanism to register to the mHIP gateway. MN gets the HIP and IP information from the ICMP announcement messages and starts registration procedure with mHIP gateway. mHIP gateway and MN exchange their information about the signatures used in the system. All mHIP agents in the same domain get the information about the MN's HIT and new IP address. Finally, MN registers to its RVS with its new HIT.

2.2.2.3 Idle Intra-domain Handover

If there is no ongoing communication during MN's intra-domain handover, MN sends an UPDATE packet to mHIP gateway to inform about its new IP address. The nearest mHIP, which is located between the old location of the MN (NmHIPA in the related study) and mHIP gateway, captures the UPDATE packet and signs the packet with selected signature scheme. When MN receives and verifies the signed packet, intra-domain handover process is complete. The all mHIP agents learn the HIT and IP address of MN. The old location mHIP also notifies all neighbors to update the MN's record.

2.2.2.4 Handover with Active Connections

If there is ongoing communication, when CN wants to communicate with MN, it learns the RVS of MN from DNS server and starts the connection procedure with RVS. RVS forwards the I1 packet to mHIP gateway. Using the mapping information, I1 is forwarded to MN. The rest of BE (Base Exchange) occurs in the traditional way. For handover, the MN sends an UPDATE packet to CN. As in paging, NmHIPA captures this UPDATE message before CN and replies to it by signing the packet with the signature scheme of the domain. After MN replies to the address checking required by NmHIPA intra-domain handover procedure is complete. NmHIPA updates the mappings and notify the neighbors about the change of IP address of the MN.

2.2.2.5 Multi-homing

In case of multi-homing, MN sends the UPDATE packet of its new interface. NmHIPA captures it and forward to the new interface. Since mHIP handover is based on connections instead of interfaces, in case of multi homing, handover can be performed while moving from one interface to another by using mHIP agent in a mHIP domain.

2.2.3 DH-HIP (Dynamic Hierarchical HIP)

DH-HIP is a location management scheme and introduces three levels architecture of rendezvous servers as Rendezvous Server (RVS), Gateway RVS (GRVS) and Local RVS (LRVS) respectively. The mobile node according to the packet arrival rate and mobility status determines the size of administrative domain managed by a LRVS after selection of LRVS.

DH-HIP architecture network is divided into two types of domains: autonomous and administrative domains. While LRVS are responsible for managing administrative domains, GRVS are responsible for autonomous domains. Autonomous domains may consist of several administrative domains. GRVS is responsible for communication between LRVS and MNs.

In DH-HIP, size of administrative domains, which means the number of access routers managed by same LRVS, is set according to the packet arrival and mobility rate of MNs in order to minimize signaling cost. In DH-HIP scheme, all ARs inherit the roles of LRVS. When MN enters the network, it registers its HIT and IP address at LRVS, GRVS and RVS respectively. While MN registers at LRVS directly, during registration of GRVS and RVS, previous level rendezvous server intercepts the packets and replace the MN's IP address and HIT with themselves and forward them. If a CN wants to communicate with MN, after querying DNS; it obtains the IP address of the MN's RVS. The interception and forwarding of messages continue in some steps of Base

Exchange too. This work also includes a mathematical analysis about the signaling cost function of their scheme (YANG, et al., 2007).

The main difference of DH-HIP over μHIP concerns its three level hierarchy architecture. Also, number of AR is not constant as in μHIP, it is updated dynamically according to the packet arrival rate and MN's status.

2.2.4 HIP Based Micro Mobility Optimization

In this work, a new network component called Co-Agent (Co-A) for each domain is proposed to extend the micro mobility behavior of HIP. LRVS is also inherited from μHIP. The main role of Co-A is managing mobile nodes during intra and inter domain handovers by acting as both a mobile and a corresponding node. LRVS of each domain is normally responsible for mapping local-global addresses of mobile nodes. The HI and IP of Co-A are also mapped with MN and the Co-A can receive local IP addresses from another domains for MNs which it manages. Owing to Co-A can monitor the movement of MNs; it can prevent the packet loss by informing the related entities in the network and optimize handovers (MUSLAM, et al., 2009).

2.2.4.1 Initiation

When a MN enters a new domain, it registers itself to LRVS as usual. It does not need to register to RVS, but LRVS must be registered to DNS. In this approach, MNs ask for advertisement messages from access routers by sending Router Solicitation messages. So, MN determines its Co-A and registers itself and its Co-A to LRVS. After the LRVS's mapping procedures, a secure connection is established between Co-A of MN and Co-A and CN.

2.2.4.2 Intra-Domain Handovers

Access points periodically broadcast advertisement messages that contains HIT and IP of Co-A. If intra domain movement occurs, no operations are needed to do for MN; Co-A acts on behalf of them. Since LRVS and MN exchange information about their registration in their domain.

2.2.4.3 Inter-Domain Handovers

When a MN changes its domain and inter domain handover occurs, it realizes this again by Router Advertisement Messages, then it registers itself to new LRVS through one of Co-A. MN's old Co-A informs the CN's LRVS via MN's old LRVS about its new location. After some other message exchange between Co-As, CN's LRVS forwards data to MN through its new LRVS.

2.2.5 An Extension of HIP for Next Generation Wireless Networks

This study basically proposes to optimize the handover process by informing the related entities about the access technology in next generation wireless networks (TOLEDO, et al., 2009). The solution they propose is based on a scenario where both communicating hosts are mobile. Their main aim is handling mobility of two mobile communicating nodes when they change their access technologies, namely when vertical handover occurs.

The main concept of their proposal is introducing a new message for update procedure named as VHO_NOTIFY. This message informs the nodes about the technology that they will communicate next, in order to let the corresponding peer to know which interface to activate. This VHO_NOTIFY message also has a role for handover process that some parameters related to handover (IP addresses etc.) may be sent earlier to inform peers about handover. They also introduce a new type of UPDATE message named as NEW_UPDATE. The main difference between NEW_UPDATE and regular HIP UPDATE message is about the content of LOCATOR parameter. Unlike regular HIP, in NEW_UPDATE, LOCATOR parameter may not be the IP address of the owner of this message. This is done to delete the dependency of sending the packet via new configured address, and consequently allowing to send the new configured address from any existing interface. It is not necessary to set the LOCATOR parameter same as the source address. That is the main difference between the NEW_UPDATE packet and the original HIP UPDATE packet. Briefly, by allowing sending VHO_NOTIFY and NEW_UPDATE messages with old access technology, informing the corresponding peer about the next technology will be used. So, the necessary information about handover may be sent before handover starts.

2.2.6 Simultaneous End-Host Mobility Extension for HIP

This scheme's main idea is to enhance the role of RVS to support simultaneous mobility in HIP in which two communicating host change their locations at the same time (HOBAYA, et al., 2009). As these simultaneous movements occur, both nodes inform their RVS about their new addresses.

The basic idea of this solution is relaying UE-PEER messages. This enhances the role of RVS. To avoid the loss of UE-PEER messages, they offer the interception of UE-PEER messages from MNs by RVS. But, second UE-PEER message exchange occurs since first attempts of RVS to relay the UE-PEER messages are done toward their old addresses. After timeout, UE-PEER message exchange is done. This second attempt is not done through RVS, besides third UE-PEER exchange is again intercepted by RVS. After this third data exchange, data flow starts.

2.2.7 HIP-PMIPv6 Based Localized Mobility Management for Multihomed Nodes

In this study, the authors propose a global and localized mobility management scheme based on the integration of HIP and Proxy Mobile IPv6 (IAPICHINO & BONNET, 2009). This scheme brings a solution for inter technology handovers and multi homing in PMIPv6. While the macro mobility side is based on traditional HIP procedures, they define a combination of HIP and PMIPv6 regarding to micro mobility.

2.2.7.1 Initiation Procedure

The initiation procedure of HIP-PMIPv6 combination is mostly relying on the procedures of PMIPv6 and its network elements (i.e. Mobile Access Gateway-MAG). The regular RVS update process of HIP follows the message exchanges and settings based on PMIPv6 in order to set up the trusted connection. In case of ongoing communications, regular HIP update procedures occur in order to update the corresponding nodes. Due to the type of IP addresses used by PMIPv6, LRVS idea cannot be inherited as in mHIP and μHIP. The macro mobility procedure is inherited

from regular HIP whereas the micro mobility procedure is defined as a combination of HIP and PMIPv6.

2.2.7.2 Intra-Technology Handover

Since there is no change in locator of mobile node during movement, HIP does not sense the intra-technology handover. This procedure is completely based on PMIPv6. No updates to RVS and corresponding nodes (CNs) occur since the mobile node does not detect any change of its interface.

2.2.7.3 Inter-Technology Handover

Inter-technology handover means that a mobile node switches on to its second interface during an ongoing communication. If a MN switches on to its second interface, it again obtains the same Home Network Prefix if it is in the same domain. In this case, MN does not send an UPDATE to its RVS but sends to corresponding nodes to notify them about its new IP address of second interface. Mobile Access Gateway intercepts this UPDATE packet and does not forward it to CNs. It performs the necessary update operations on behalf of mobile node through other network elements.

2.2.8 Localized Mobility Management for HIP (L-HIP)

In L-HIP (HU, et al., 2010), a localized mobility management technique is presented by inheriting the idea of somehow proxy mobile IPv6. In their scheme, some entities in the network are responsible to track the mobile nodes' movements such as PMIPv6. They introduce a new entity called Local Mobility Management Server (LMMS) to cope with the intra-domain mobility especially. They also employ the usage of Mobile Access Gateways (MAGs) of PMIPv6 and present handover management scheme based on combination of PMIPv6 and HIP.

2.3 Chapter Summary

In this chapter, the locator/identifier split idea and the most popular protocols and architectures which are employing this approach, are reviewed with their advantages and limitations. The increase in heterogeneity and fast spread of Internet of Things concept, the need for good adaptation of different types of wireless networks in IP layer became important. While considering these challenges, locator/identifier split idea is a promising solution. Two main protocols HIP and LISP which are employing this approach has been introduced in detail. MOFI architecture is also a new and overall architectural solution that relies on locator/identifier split wave. A brief comparison among them also presented. Since we focus on improving the mobility management of Host Identity Protocol, related previous work has been presented. It is clear that in some of related proposals, new network entities such as local rendezvous servers are implicated in the network architecture. On the other side, some of them propose new message exchange procedures to support handover or introduce new network architectures. The strong and weak aspects of existing mobility mechanisms are reviewed.

3 Proposed Early Update Enhancement for Host Identity Protocol

The most important spot of this chapter is enhancing the handoff quality of HIP during micro mobility. According to this extent, firstly we propose a hierarchical network architecture that provides inheriting the localized RVS as in μHIP, in order to improve the handoff delay. Secondly, an early update mechanism (eHIP) is proposed in order to meet the improved handoff requirements in our proposed architecture (GURKAS AYDIN, et al., 2009).

3.1 Proposed Network Architecture

Most of the HIP based mobility studies (such as mHIP, μHIP, DH-HIP) implements the update procedure just after either obtaining a new IP address or moving to the new location completely. These features remind us Mobile IP based solutions such as Hierarchical Mobile IP (SOLIMAN, et al., 2005) that promises proactive handoffs and Fast Handovers for Mobile IP (KOODLI, 2005) that enhances handoff delay. We can summarize FMIP as completing the registration procedures of a mobile node before arriving to its new location. In this section, our proposed network architecture is introduced intended for our early update mechanism for HIP.

Anticipation for handoff refers to triggering and realizing the handoff of a mobile node (MN) without disconnecting from its current location, by the help of topology information, signal strength, movement detection or network layer triggers. Most of the former studies based on anticipation use L2 (Layer 2) triggers, but only some technologies allow using L2 triggers. Actually, after getting some L2 triggers, L3 handoff cannot be decided exactly due to some conditions such as speed of mobile node or network topology. Speed of mobile node is a critical factor for anticipation of handoff. During the movement, decision for the exact time of L2 trigger is a vital point to start the L3 handoff as soon as anticipating the next cell of mobile node.

As a way to improve the micro mobility limitations and use in our studies, we consider a hierarchy of Local Rendezvous Servers (LRVS) named RVS_i to minimize delays of HIP registration process; *i* being the level of the hierarchy. RVS_i are directly connected to the global, main and only one RVS

named RVS_0. In first step we consider $i = 2$ as two level hierarchy (If $i = 2$, it is three level hierarchy, because there is level 0). The network is then divided into several sub-domains organized in two levels. We consider two levels of local rendezvous servers (RVS_1 and RVS_2).

3.1.1 Hierarchy Levels

The higher level H1 (Hierarchy Level 1) contains one or more RVS_1 that manages the outer level sub domains which includes several inner sub domains. RVS_1 is responsible of the eHIP registration in the larger area. The lower level H2 (Hierarchy Level 2) may contain one or more

RVS_2. RVS_2 is responsible of the eHIP registration of one or more MN hosted by one or more wireless AP. Figure 3.1show us a sample orientation of H1 and H2 level rendezvous servers on our network topology. Note that RVS_1 is connected to main and single RVS_0 on the network.

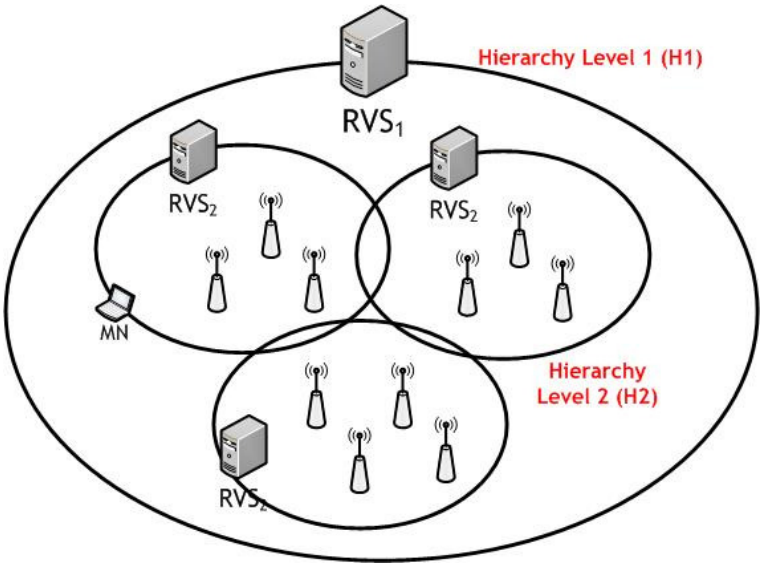


Figure 3.1: Hierarchy Levels of Proposed Architecture

Note that during the update process of a new RVS, it is necessary to be previously registered through a HIP Base Exchange, which is adding high latency for ongoing communication of the MN. All the hierarchy based proposals (mHIP, µHIP, DH-HIP) do not mention how the new RVS server deals with the update of the location of MNs that are not previously registered.

3.1.2 Pre-Registration Mechanism

We propose, to avoid additional latency and overhead during the update process of the handover to pre-register with all the lower level RVS of the same domain. In our scenario, a MN registers with all RVS_2 as soon as it enters the RVS_1 domain. Also we propose to add an active status flag indicating in which RVS_2 sub-domain that MN is located "actively" to the registration message. In other words, this flag is set as "passive" status while it is pre-registering to other RVS_2 in the same RVS_1 sub-domain. Obviously, after MN leaves the RVS_1 domain, all RVS_2 should remove the corresponding record for this mobile node.

Whenever a mobile node joins a RVS_1 sub-domain, as known as H1, starts it first registration procedure to the RVS_2 that currently serving access point belongs to. It is assumed that all

rendezvous servers have trusted connection between them and accept all messages and update messages from each other.

In DH-HIP architecture that employs the hierarchical network architecture idea, there is just one Gateway RVS as the second level component under the global RVS. Especially during the connection initiation, all new components in DH-HIP architecture intercept the packets, add some parameters to them and forward them to lower level component. In our architecture, we do not propose an essential modification for the Base Exchange procedure. We just propose to proceed with the registration with RVS that are in the same domain as the mobile node proactively. This is to avoid additional latency during the update process.

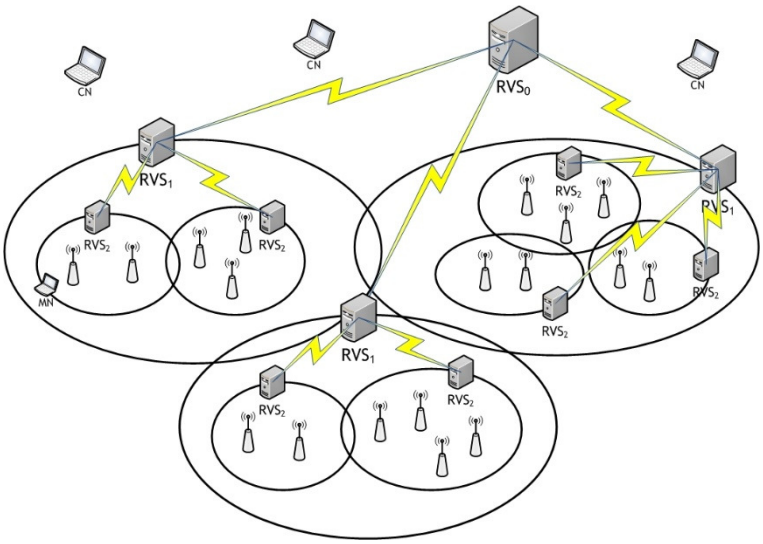


Figure 3.2: Proposed Hierarchical Network Structure

While considering micro mobility problem, traditional HIP requires too much and long signaling for updates and this brings packet loss, handover latency and overhead. It was well documented in some related micro mobility proposals of HIP (mHIP, μHIP, DH-HIP). The main role of LRVS is to keep the update process of MN in the local domain and minimize the signaling overhead. The global RVS does not sense the movement of MN but it is updated by the RVS_1. In fact, the lower level RVS (RVS_2) is responsible for the movement of mobile nodes inside H2 domain. The higher level RVS (RVS_0) is informed by RVS_1 in case a mobile node moves to a different H1 domain managed by another RVS_1. Advantage of this architecture is similar to HMIP proposal, which is to minimize the signaling overhead for frequent movements of MNs and to reduce handover latency.

If a MN moves to a different point of attachment within the same H2 domain, it starts to be served by a different AP in the same sub-domain. MN that realizes the change of its IP address updates its record at RVS_2 with its new IP address. CNs or RVS (global RVS) of the MN are not informed about this movement and updates. Since all components of the MN's sub domain are not updated about the movements; so signaling overhead is reduced, also packet loss and handover latency is slightly better than normal HIP and somehow handover latency is reduced.

3.2 Early Update Mechanism for HIP

In addition to the hierarchical approach, we introduce the early update mechanism as Early Update for HIP (eHIP). Early Update simply means that MNs obtain their new IP address from the network they want to move to and make their registration before the handover process. Early Update handoff can be triggered by different parameters applied to the handoff decision function of the MN. These parameters can be L2 triggers if the technology allows it or any other parameter just like FMIP. In order to cope with the drawbacks of L2 triggers anticipation process, early update approach was proposed in (KIM & KIM, 2006) to improve Mobile IP.

In our proposal, each AP does not act necessarily as a RVS like in (YANG, et al., 2007). If a MN wants to start the early update procedure, firstly discover the next RVS IP address covering the next AP. To discover the next AP and RVS's IP address, service discovery complements our architecture. The routing advertisement messages are the simplest way to announce the IP addresses. Note that MNs are pre-registered to all RVS inside their existing domains. The main role of Early Update procedure is during handoffs that MN moves to a domain served by a different RVS_2.

3.2.1 Message Types and Concepts

We introduce two new main types of messages called as EARLY UPDATE (EU) and FINISH UPDATE (FU) to be used in our early update procedure. EU message are sent when MN node is still in its current domain before movement after the service discovery. FU messages are sent when MN arrives its new domain meanly after movement. EU messages are also numbered differently for indication the purpose and source of messages. Table 3.1 summarize the terminology and message types used in eHIP.

Table 3.1: Terminology and Messages used in eHIP

oAP	Old AP that MN is currently connected to.
nAP	New/Next AP that MN will perform handoff
oRVS2	Old RVS2 that MN is currently connected to.
oRVS1	Old RVS1 that MN is currently connected to.
nRVS2	New/Next RVS2 that MN will perform handoff
nRVS1	New/Next RVS1 that MN will perform handoff
EU	First Early Update message that MN sends
EU1	Early Update message that oRVS2 sends to nRVS2
FU	Finish Update message
NEW_HOST_REG	New registration message among rendezvous servers
DELETE_HOST_REG	Delete registration message among rendezvous servers
EU2(OK)	Confirmation message that nRVS2 sends during handoff
EU2(ERROR)	Error message that nRVS2 sends during handoff
EU3(OK)	Confirmation message that oRVS2 sends to MN during handoff
EU3(ERROR)	Error message that oRVS2 sends to MN during handoff
FU1	Update messages that nRVS2 sends to corresponding nodes

Table 3.2 shows the detailed overview of messages defined for eHIP, message formats and contents of these messages.

Table 3.2: eHIP Messages, message formats and contents

Message Type	Format	Context
EU	srcHIT srcIP destHIT destIP nRVSHIT newHostIP	When MN receives a RA message including a different RVS information from than its current one, it sends an EU message to $oRVS_2$ including the $nRVS_2$ information and requested IP obtained from RA message of nAP
EU1	srcHIT srcIP destHIT destIP HostHIT HostResvIP	The message that forwards the EU request of MN to $nRVS_2$ from $oRVS_2$. It includes the MN's HIT and requested IP address.
EU2	srcHIT srcIP destHIT destIP AckHostHIT statusFlag	The response message from nRVS2 to oRVS2 for EU1 message. It includes the status flag that indicates whether the EU request is successful or not.
EU3	srcHIT srcIP destHIT destIP AckRvsHIT statusFlag	The message that indicates the status of early update request from $nRVS_2$ to $oRVS_2$. It includes the status flag and HIT of newly registered $nRVS_2$
FU	srcHIT srcIP destHIT destIP CnHITList CnIPList	The early update finalization message that is sent from MN to $nRVS_2$ to indicate its complete arrival to $nRVS_2$ domain. It includes the HIT and IP list of CNs if MN has ongoing connections.
FU1	srcHIT srcIP destHIT destIP MnHIT MnIP	The message that is sent from $nRVS_2$ to CNs which indicates the MN's IP information. It includes the MN's HIT and IP address.
NEW_HOST_REG	srcHIT srcIP destHIT	The message that RVS informs the upper level RVS in the hierarchy about the arrival of MNs. It includes the new host's HIT information. Upper level RVS

	destIP newHostHIT	maps the MN-RVS information according to this message.
DELETE_HOST_REG	srcHIT srcIP destHIT destIP oldHostHIT	The message that is sent from any upper level RVS (RVS_1 or RVS_0) when it receives NEW_HOST_REG message. If the MN is registered to any different RVS_2. Upper level RVS requests the deletion of MN's record. It includes the HIT's of MN.
RA	RvsHIT RvsIP	The modified version of IPv6's router advertisement as including the RVS information. It includes HIT and IP of RVS that manages related IPV6 router subdomain.

eHIP procedure can be summarized as follows: after the anticipation next AP and RVS2, discovering the candidate IP addresses during the MN's movement, MN send a EU message to its currently connected RVS_2 ($oRVS_2$) and then $oRVS_2$ forwards this request to $nRVS_2$ by other EU messages. After the necessary processes are completed by $nRVS_2$, the response messages are sent back to MN via $oRVS_2$. After these steps are completed, MN moves towards its new location and arrives to nAP's coverage. Here MN send the FU message directly to $nRVS_2$ and confirms its arrival to nAP. At this point, MN starts to be served by nAP. After the reception of FU message, $nRVS_2$ sends the FU1 messages to CNs if there are existing ongoing connections. Also NEW_HOST_REG message is sent to $nRVS_1$ to update the all hierarchy. While data communication from MN to CNs starts as soon the first FU message is sent, MN starts to receive data from CNs right after the FU1 message is received.

3.2.2 Connection Setup Procedure

As described in 3.1.2, pre-registration mechanism complements our proposed network architecture. A mobile node, as soon as it enters in a RVS_1 domain, registers to all sub level RVS_2. This process is somehow connection initiation procedure. Figure 3.3 depicts the message sequence chart of pre-registration schema and procedure when a MN enters inside a new H1 domain. MN sends first I1 message to $nRVS_2$ when arrives inside a H1 domain. While Base Exchange procedure continues between $nRVS_2$ and MN, after the recipient of I2, $nRVS_2$ sends the closure packet of BE (R2) and performs the registration of this new MN to upper level RVS_1, other RVS_2 in the same sub-domain and the main RVS_0 at the same time by NEW_HOST_REG messages.

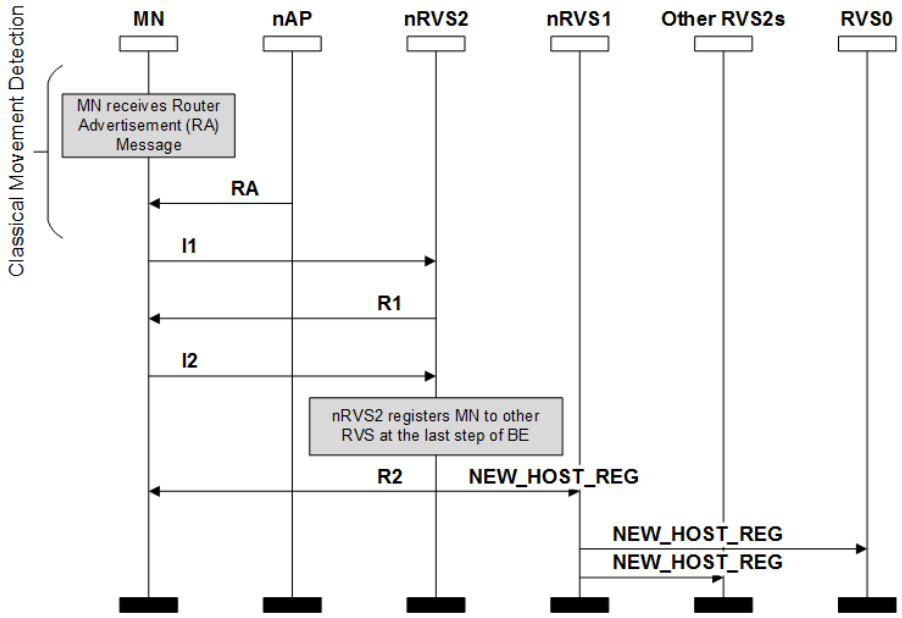


Figure 3.3: Connection Initiation / Pre-Registration Message Sequence Chart

When a MN wants to communicate with a CN, it should start the BE procedure. Depending on the level that CN located in, message flow is provided by benefits of hierarchical architecture. Figure 3.4 shows the connection initiation message sequence chart if MN and CN is under the same sub domain managed by same RVS_2. MN send the I1 message to its current RVS_2. If RVS_2 finds the CN inside its domain, forwards the I1 message and the rest of BE continues in its normal way between MN and CN.

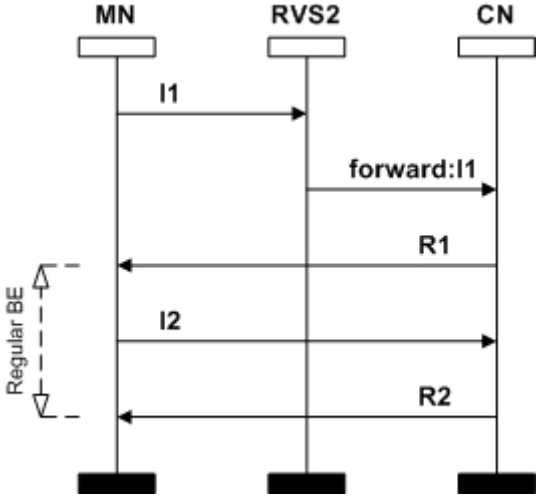


Figure 3.4: Connection Initiation where MN and CN are located in same H2

Figure 3.5 and Figure 3.6 depicts the connection initiation message flow charts where CN and MN are located in different H2 and H1 respectively. After MN send the I1 message to its RVS_2, if this RVS cannot find the CN inside its domain, forwards this I1 message to upper level RVS_1. If this RVS_1 detect the existence of CN in another RVS_2 inside its domain, it forwards the I1 message to

this RVS_2. Finally after forwarding of this message to CN by RVS_2, the rest of BE procedure continues in normal way between MN and CN.

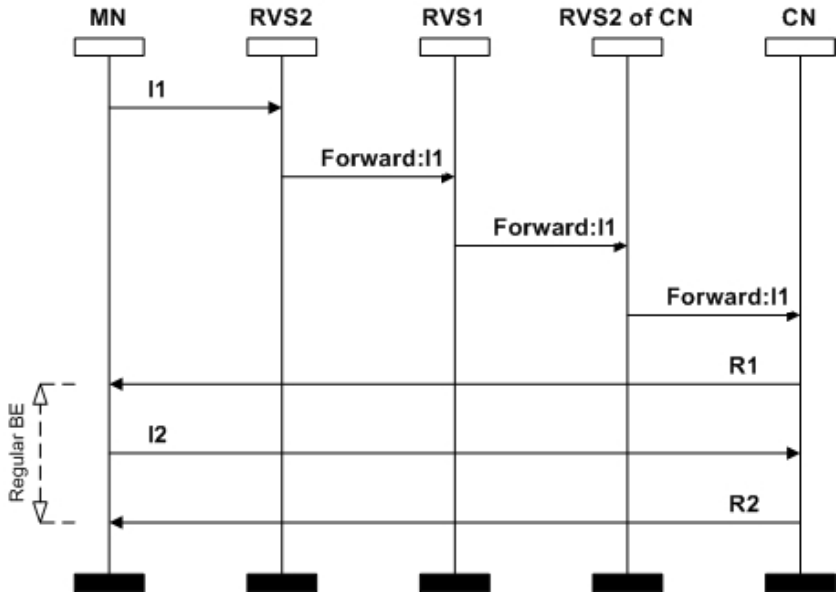


Figure 3.5: Connection Initiation where CN and MN are located in different H2

Besides, if CN is located inside a different H1, I1 message follows a way towards the top level of hierarchy with necessary controls. All RVS checks the status of CN respectively and if necessary they forward the message to upper level RVS. When I1 message reaches the main RVS_0, it once again follows the hierarchy of RVS through top to bottom and reaches to corresponding CN. The rest of BE procedure continues in normal way between MN and CN.

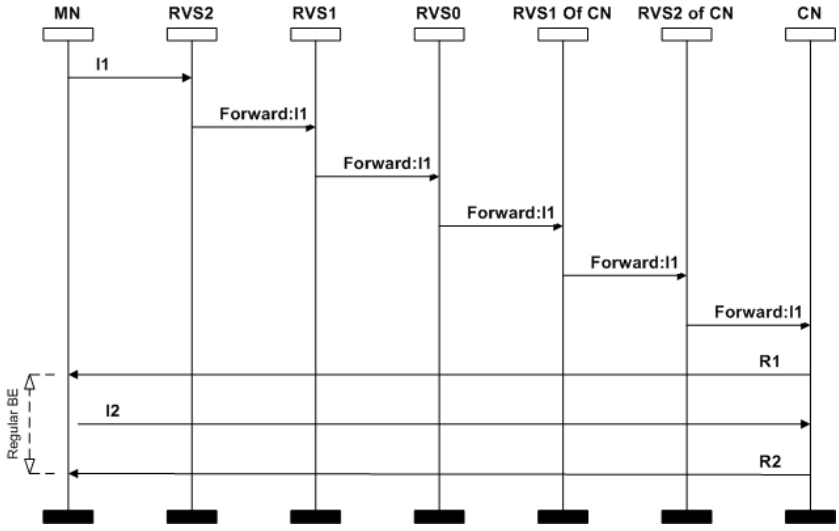


Figure 3.6: Connection Initiation where CN and MN are located in different H1

3.2.3 Hierarchy Level 1 Handoff Procedure (H1H)

HI handover (H1H) denotes the movement of a mobile node among two different H1 domains, meanly changing RVS_1. Figure 3.7 summarizes the H1 handover as a message sequence chart.

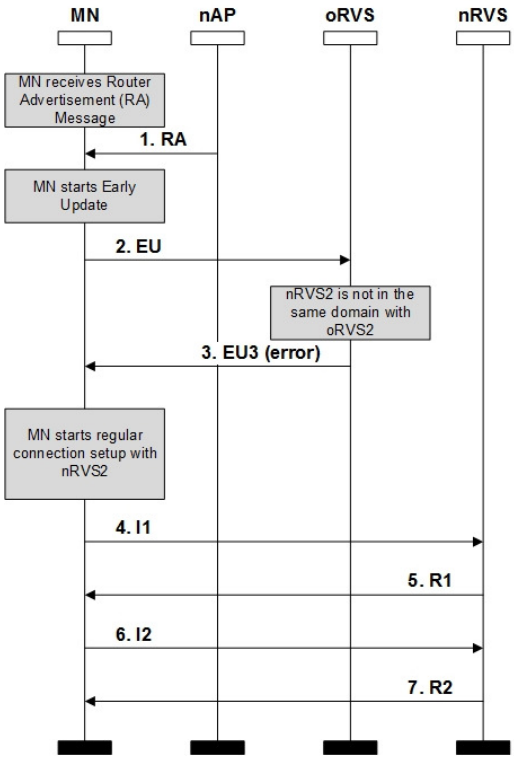


Figure 3.7: H1 Handover Message Sequence Chart

When the movement of MN starts and receives a router advertisement (RA) message broadcasted from a different AP, it sends first EU message directly to its current RVS_2 ($oRVS_2$). According to our architecture, all RVS_2 inside the same H1 are aware of each other. EU message contains the MN's HIT, new IP address (CoA) from new AP and $nRVS_2$ information that will be get involved inside its sub domain. Herein, whenever a RVS receives an EU message, firstly controls whether the requested $nRVS_2$ exists inside the same domain with itself. If the requested $nRVS_2$ belongs to a different H1 sub domain, $oRVS_2$ send the EU3 message to MN with error status. As soon as MN receives an error message, it starts a registration procedure from scratch with $nRVS_{2\ which}$ belongs to a different H1. This procedure is called H1 handover (H1H) in eHIP. After the registration of MN to nRVS2, nRVS2 updates the upper level $nRVS_1$ and other RVS_2 inside the same domain as stated before.

3.2.4 Hierarchy Level 2 Handoff Procedure (H2H)

H2 handover is defined as movement of MN among different H2 domains under the management of same H1 domain, in other words changing the RVS_2. Figure 3.8 depicts the message sequence of this process.

Whenever an oRVS2 receives an EU message from MN and requested nRVS2 is involved to the same H1 domain, it sends an EU1 message to nRVS2 in order to request a new registration or update process. If $nRVS_2$ replies to this message by EU2 message, it means that $nRVS_2$ has successfully completed the pre-settings and accepts this update about the arrival of MN to its coverage. $oRVS_2$ replies to this message by EU3 as an approval and acknowledgment. Finally, as soon as MN receives the EU3 message, becomes eligible for sending the FU message to $nRVS_2$.

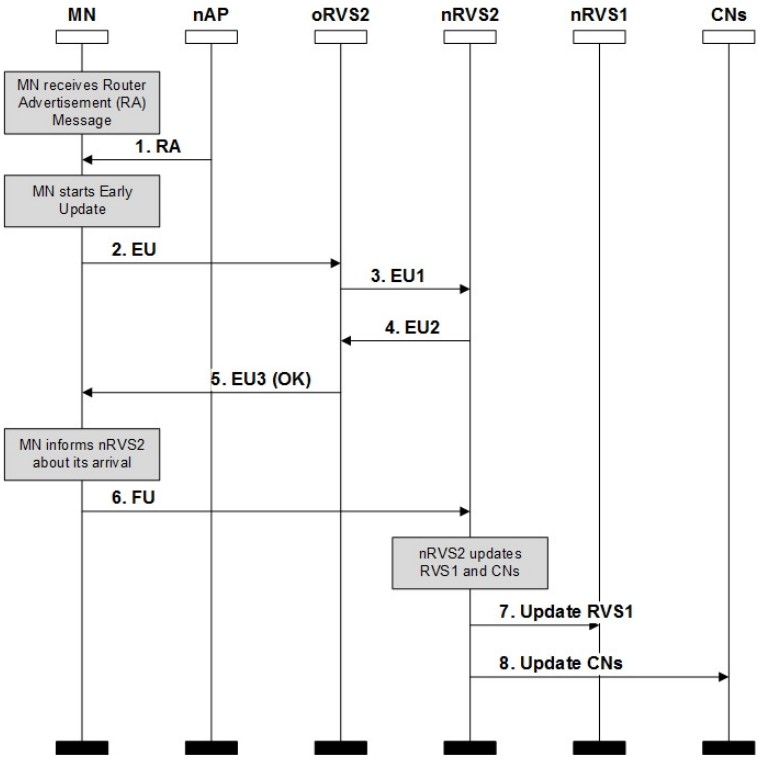


Figure 3.8: H2 Handover (H2H) message sequence chart for successful case

MN's ability to send messages directly to $nRVS_2$ depends on pre-registration feature to all RVS_2 in the same sub domain. At this point, if a MN does not receive the EU3 message before it completely leaves its current domain, it should start a registration from scratch with nRVS2.

By FU message, MN can inform its CNs if there are ongoing connections. $nRVS_2$ updates $nRVS_1$ and existing CNs just after receiving the FU. MN has no more responsibilities after sending FU message. When an early update event is triggered and the existence of requested nRVS2 in a different H1 domain is discovered, an EU3 (error) message is directly sent to MN to indicate this status. The message sequence chart of this case is presented on Figure 3.9. Later on MN realizes that it is about to make a H1 handover and starts a new registration procedure.

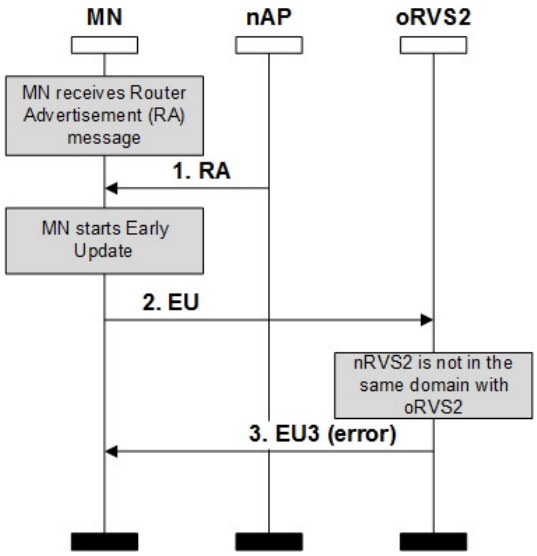


Figure 3.9: H2 Handover (H2H) message sequence chart when $nRVS_2$ belongs to another H1 domain

Another option that may occur regarding to H2H is that $nRVS_2$ may fail to complete the early update request of $oRVS_2$. In this case, if $nRVS_2$ is located inside the same H1 domain with $oRVS_2$ and even $oRVS_2$ receives the MN's new IP details with an EU1 message, it may not be able to complete the necessary pre-settings and updates successfully. In this case, $nRVS_2$ replies to $oRVS_2$ with an EU2 message to MN and later on $oRVS_2$ sends the EU3 (error) message to MN to indicate the status of its request as failed. Figure 3.10 depicts the message sequence chart for this case.

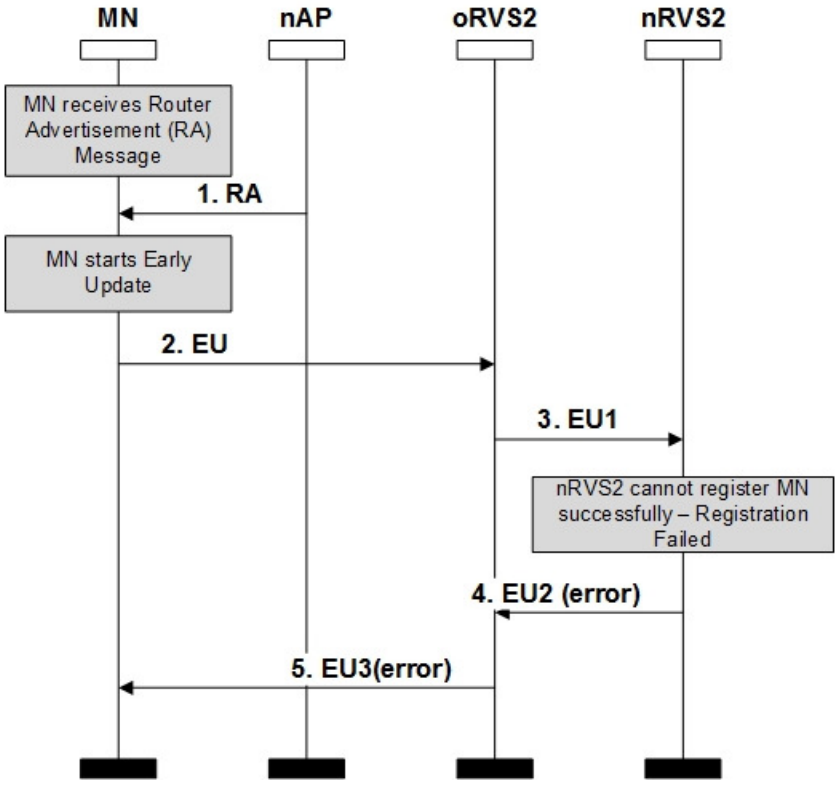


Figure 3.10: H2 Handover (H2H) message sequence chart when $nRVS_2$ fails to complete the early update request

3.2.5 Intra-H2 Handoff Procedure

When a MN starts to move and receives a router advertisement (RA) message from a different AP but in same H2 domain, it sends an EU message directly to its RVS_2 ($nRVS_2$). Thereby, oRVS2 becomes aware of new IP address of MN that already belongs to its sub-domain. It immediately replies to MN with EU3 confirmation message. Whenever MN completes the handover process, it sends FU message directly to its RVS_2 with necessary CN information if there are ongoing connections.

RVS_2 informs and updates all CNs with FU1 message about MN's handover. As a consequence, handover latency is reduced by replacing traditional three-way update procedure by eHIP intra H2 procedure through rendezvous serves.

Figure 3.11 shows the state transition diagram of MN for whole eHIP procedures.

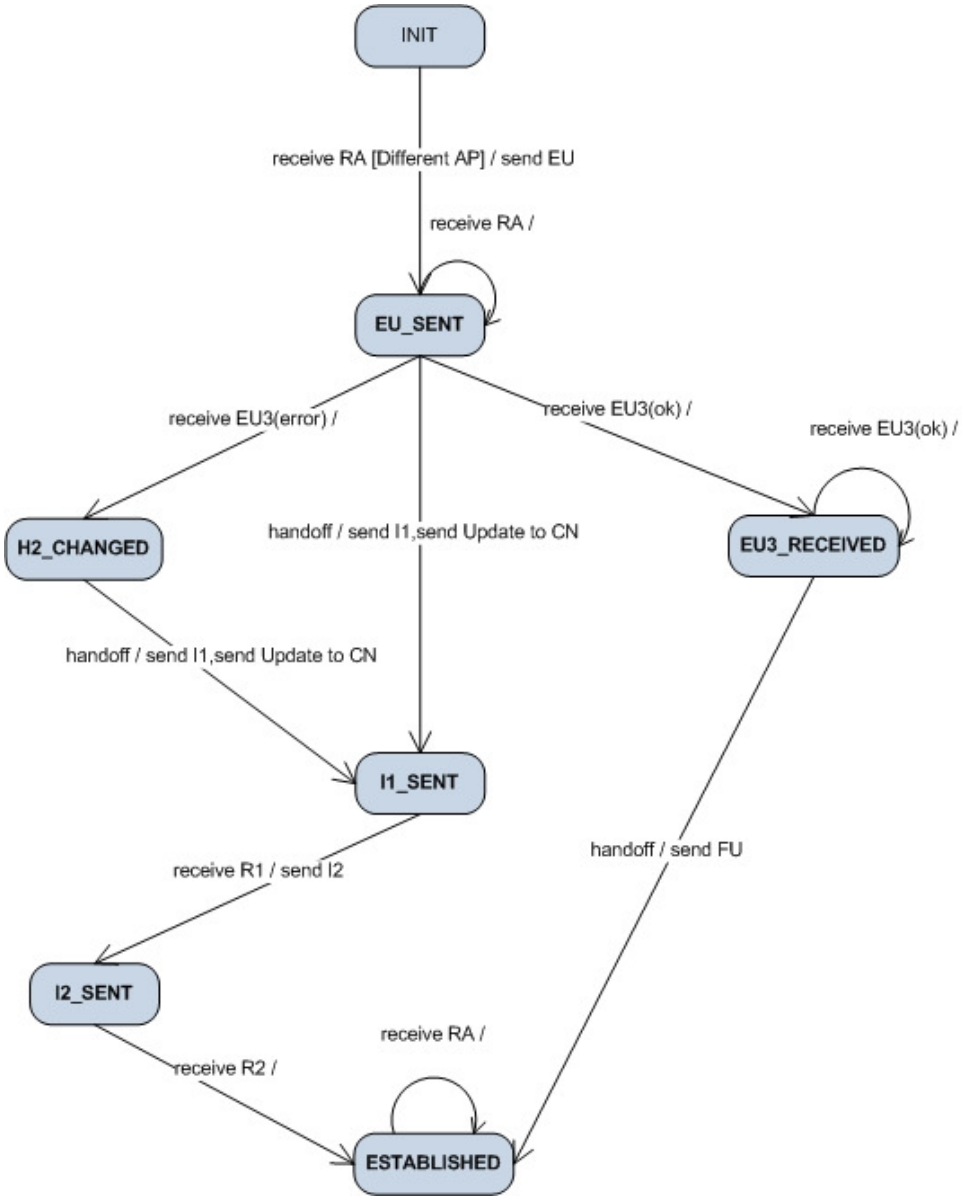


Figure 3.11: eHIP State Transition Diagram for MN

3.3 Performance Evaluation

3.3.1 Simulation Environment and Scenarios

OMNET++ is a discrete event based simulation environment for modeling communication networks, IT systems, queuing systems and hardware architecture (OMNET++, 2013). It is used for eHIP simulation in this thesis. OMNET++ is an open source, non-profit software. It acts as an intermediate solution between Network Simulator (NS-2, open source and research based (NS-2, 2013)) and OPNET (high cost and commercial (OPNET, 2013)).

OMNET++ is composed of components and functions in a modular manner. A simulation model is composed of interacting modules in OMNET++. These modules are named as simple modules. They are written by C++ programming language and inherits OMNET++'s simulation libraries. Besides, these simples modules are combined in or der to compose compound modules. The network topologies are defined by using NED (NEtwork Definition) definition language. NED files includes simple module, compound modules and network topology definitions. With these behaviors of OMNET++, model topology definitions and model behaviors differ from each other. While model behaviors are written by C++, network topology and all related settings are done by NED language. Simulation parameters are defined in separate INI files apart from C++ and NED files.

Plenty of simulation models for OMNET++ are developed by research groups or communities. The most relevant model framework for communication networks is INET Framework (INET, 2013). INET Framework support many protocols such as IPv4, IPv6, TCP, UDP, MPLS, RSVP etc., many applications such as telnet, video streaming etc. and many link layer models such as PPP, Ethernet, 802.11b/g etc.

3.3.2 HIPSIM++

HIPSIM++ is the model developed under INET Framework of OMNET++ and provides basic extensions and functionalities of HIP (HIPSIM++, 2013). The basic functions of HIPSIM++ are modeling the core functions, mobility support and wireless behaviors of HIP. Therefore, it lacks IPSec and all related algorithms. Also, all cryptographic methods such as Diffie–Hellman, RSA etc. are not involved (BOKOR, et al., 2009a) (BOKOR, et al., 2009b).

3.3.2.1 Basic Modules of HIPSIM++

a) HIP Module

HIP module is the core module of HIPSIM++ that models the HIP layer. It creates a HIPSM daemon for each HIP session. This daemon is responsible for all functions (BE and mobility) of HIP state machine (HIPSM)

b) HIPSM Module

It is the module that functions fundamentals of HIP state machine. HIPSM assume that a packet is authenticated and processed correctly. A HIPSM represents a single HIP connection and HIP

security association (SA). HIPSIM++ implements BE, RVS registration, UPDATE procedures and generates necessary HIP messages during state transitions.

c) RVSHIP Module

It is the module that implements RVS functions. All registration messages are processed in this modular and related I messages are forwarded to appropriate HIP-Responder.

d) DNSBase Module

This module is a simple UDP application that implements the basic DNS server functions such as HIP host resolution and new resource registration. This module converts domain names to HIT's and IP addresses.

3.3.2.2 HIP Nodes

a) Wired HIP I/R Node (HipHost6)

This node is derived from INET's StandardHost6 compound module and defines functions of Initiator and Responder nodes on HIP. HIP Layer is integrated between network and transport layers. It represents a basic HIP node and mechanisms, HIP based UDP/TCP applications without mobility support.

b) Wireless HIP I/R Node (WirelessHipHost6)

This node is a version of basic HIP host with a WALAN physical interface. It also supports HIP mobility operations.

c) Wireless Multi Homed HIP I/R Node (WirelessMultihomeHipHost6)

This is a HIP host type that has many physical interfaces to support multi homing feature of HIP.

d) DNS Server (StandardHost6 with DNSServer)

A DNS server node is responsible for name resolution of HIP hosts. In HIPSIM++, at least one DNS server is required in each simulations scenario.

e) HIP Rendezvous Server

This node implements the rendezvous server function of HIP. It forwards I1 messages to related and registered Responder nodes from wired or wireless Initiator nodes. Wireless nodes always should inform their RVS about their movement.

3.3.3 eHIP Simulation

All modules and nodes defined for our eHIP simulation are based on HIPSIM++ framework and described in this section.

3.3.3.1 eHIP Modules

a) HIPEU Module

HIPEU is the extended version of HIP module of HIPSIM++ to support functions and hierarchical architecture. In addition to functionality of HIP module, this module is responsible for getting RVS information from router advertisement messages, extra functions for processing EU or FU type messages and state transitions.

b) HIPEUFSM Module

This is the module that implements the eHIP state machine functions. In addition to HIPSM, is responsible for status changes for early update and processing update messages of CN from RVS_2 at the end of EU procedure.

c) HIPEURVS Module

This module supports RVS functions in hierarchical manner as proposed in eHIP. Unlike traditional HIP, hierarchy level information is kept. In this module, lowest level rendezvous servers are responsible for communication among HIP hosts, whereas upper level rendezvous servers only communicate with other rendezvous servers that belongs to whole hierarchy. The lowest level RVS register a HIP host and also forwards I1 messages sent by HIP hosts to upper (parent) levels of RVS if necessary. In addition, lowest level RVS informs the parent RVS by NEW_HOST_REG message about new host registration by lowest level RVS.

Upper level rendezvous servers forward the host generated I1 messages from same level rendezvous server or in traversal way forwards to the RVS of corresponding HIP-Responder. IF a RVS switch occurs for a host and there is any record of this host in another H1 domain, they both update this host's status and also delete the registration of old H1 domain with DELETE_HOST_REG message.

3.3.3.2 eHIP Nodes

a) Wired eHIP I/R Node (EUHipHost6)

This module is derived from INET's StandardHost6 to define I and R host functions. It represents a basic eHIP enabled nodes and mechanisms, HIP based UDP/TCP applications without mobility support. Figure 3.12 shows the NED representation of a wired eHIP node (EUHipHost6).

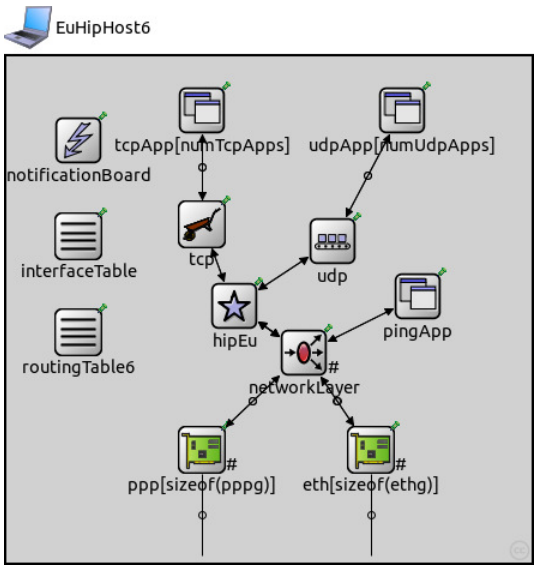


Figure 3.12: NED representation of a EUHipHost6 node

b) Wireless HIP I/R Node (EUWirelessHipHost6)

This node is derived from INET's WirelessHost6 compound module. It represents a basic eHIP enabled nodes and mechanisms, HIP based UDP/TCP applications with mobility support. It is a kind of normal HIP host with a WLAN physical interface. Figure 3.12 shows the NED representation of a wired eHIP node (EUHipHost6).

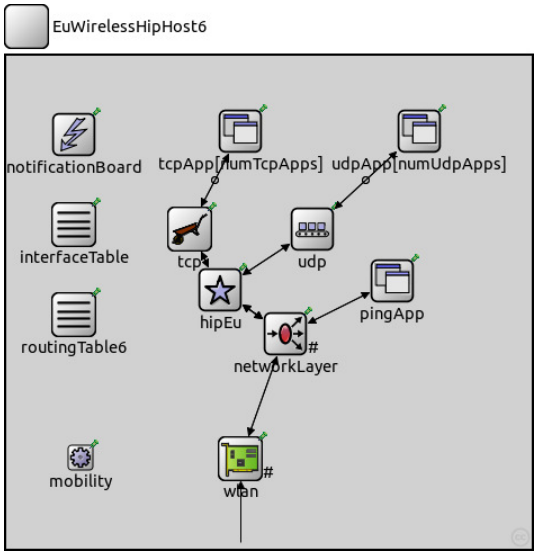


Figure 3.13: NED representation of a EUWirelessHipHost6 node

c) HIP Rendezvous Server (EURvsHost6)

This module implements rendezvous functions according to eHIP's hierarchical architecture. All level RVS can be defined as a type of this node and behaves as regards to their level functionalities. Figure 3.14 shows the NED representation of an eHIP enables rendezvous server node (EURvsHost6).

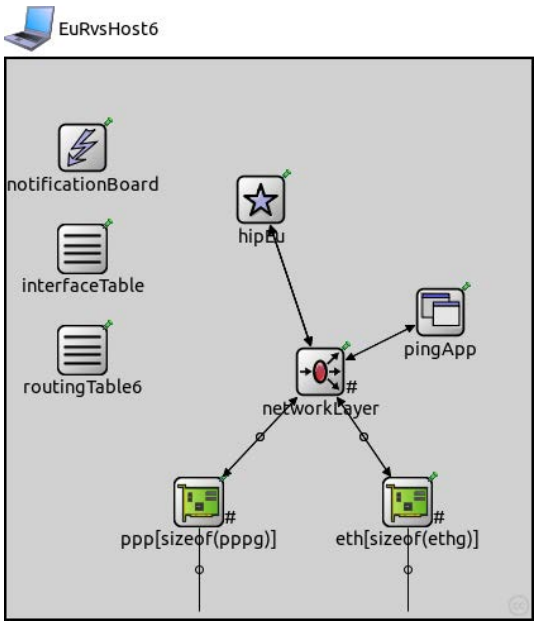


Figure 3.14: NED representation of a EURvsHost6 node

3.3.3.3 Topology

Figure 3.15 illustrates our simulation environment. The hierarchical design for eHIP support *N* level hierarchy. As to use in our simulations, three-level hierarchy is selected as simulation topology in order to obtain sufficient and similar results to compare with existing related work. The hierarchical scenario of level 1 and level 2 RVS are located on the networks with several AP connected to them. All APs are identical. There are also other network elements located in the scenario such as IPv6 routers and switches.

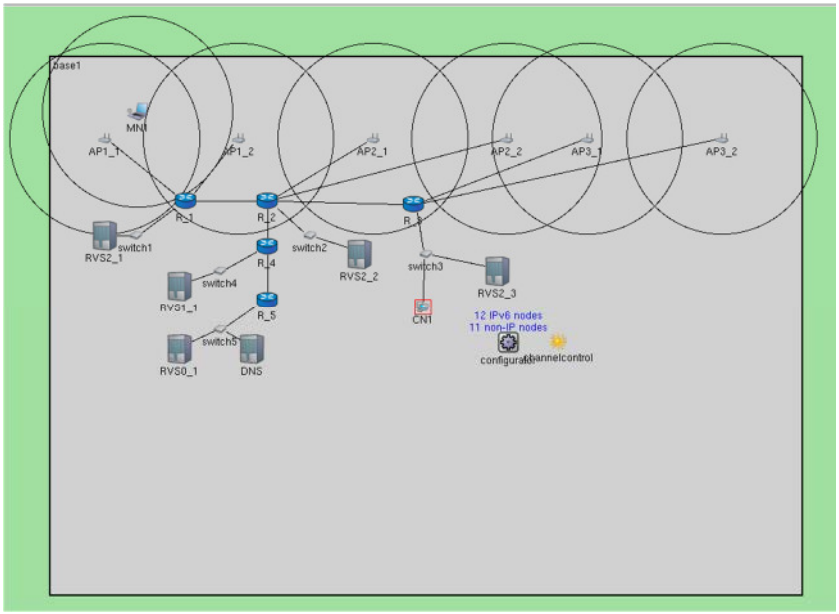


Figure 3.15: Network topology used in simulations

Simulation results are evaluated from three different scenarios to be compared. These are traditional HIP architecture, hierarchical HIP architecture without early update (Hierarchical HIP)

and HIP with early update mechanism (eHIP). In traditional HIP scenario, there are only one single main RVS on the network.

3.3.4 Simulation Parameters

In OMNET++, simulation parameters can be defined in INI files. In these files, HITs of all RVS, MNs and CNs are defined. In traditional HIP scenario, there is only single and main RVS, whereas in Hierarchical HIP and eHIP scenarios, all RVS in the network is defined by their HITs as simulation parameters.

Mobile nodes' mobility model is assumed as "Rectangle Mobility" model and employed in all types of scenarios in order to provide similar behaviors of different scenarios. In this model, a mobile node chooses a path in a rectangular shape among the selected network topology. The MN repeats its movement via this model through the simulation time. Apart from this, all MAC addresses and physical interface properties of access points are also defined.

Simulations are experimented under three different network loads and five different speed of mobile node. Load 1 is defined as a total 2.5 MBps, Load2 is defined as 5 MBps and Load 3 is defined as 10 MBps as network load to experiment the scenarios under different possible cases of a network. Total simulation time is 10000 s, and several runs of all simulation scenarios and configurations are reviewed by 95% confidence interval to obtain average results.

Mobile nodes are able to generate both TCP and UDP traffic in the network. For TCP, TCPSessionApp was used on MN and TCPSinkApp is used on CN. The packet size is variable on TCP applications. For UDP, UDPEchoStream is used on MN and UDPEchoApp is used on CN. Packet size is 256 B on UDPEchoStream app.

Several parameters are examined with these simulations. We present a set of results of four important parameters. Total number of HIP messages; it represents the number of messages generated by only HIP protocol, not related to eHIP procedure. The effects of hierarchy on total number of HIP messages are analyzed for mobile node, corresponding nodes and rendezvous servers separately. Besides, even the definitions of handoff times are also given before the related results; it can be briefly summarized as the period of completing the handoff to obtain the new address for mobile node. Also as enlightener parameters of a communication network simulation, jitter and RTT are also examined to discuss the effects of eHIP procedures.

3.4 Results

3.4.1 Total Number of HIP Messages

The advantages of Hierarchical HIP and eHIP over traditional HIP in terms of total HIP messages handled in the network are firstly examined. The difference between the Hierarchical HIP and eHIP methods reveals during the message exchange among lowest level RVS and corresponding nodes (CN). Since there is no early update mechanism in Hierarchical HIP, for every movement to a new RVS, a base exchange (BE) procedure occurs which provides the initial connection setup

between a node and the new RVS. This BE procedure, both increase the elapsed handoff time to RVS and also inherently increase the number of HIP messages in the whole procedure.

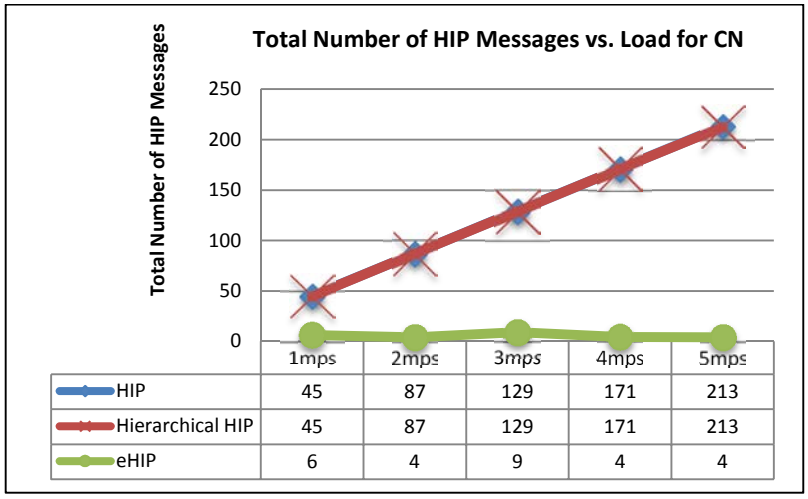


Figure 3.16: Total number of HIP messages generated at CN

Figure 3.16 presents the total number of HIP messages generated at CN for all three scenarios. Since CN performs the traditional UPDATE procedure of HIP in its every movement, so the total number of messages for CN is the same for traditional HIP and Hierarchical HIP scenarios. In eHIP, due to the advantage of early update decision triggered by MN, CN does not generate HIP messages. Updating the new location information of MN is the responsibility of new RVS_2 by sending a finish update type message to the CN. We can say that there are up to maximum 95% improvements in total number of HIP messages for CN in average for eHIP.

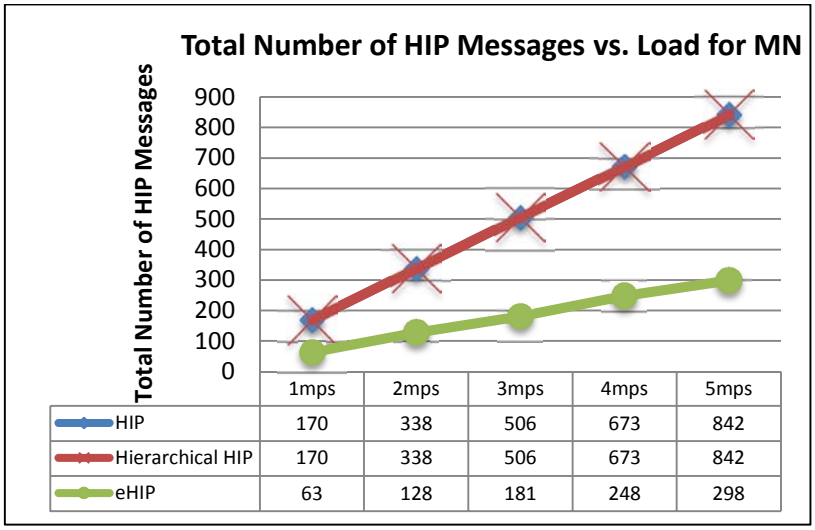


Figure 3.17: Total number of HIP messages generated at MN

Figure 3.17 presents the total number of HIP messages generated at MN for all three scenarios. In traditional HIP and hierarchical HIP, total number of messages is the same for MN in these two scenarios also. While moving, MN sends UPDATE messages to its current RVS_2 and CNs in traditional HIP. In Hierarchical HIP, UPDATE message is only sent while the MN moves inside the same H2 domain, from one AP to another. If it moves between H2 domains, classical UPDATE procedure with CNs and BE procedure with new RVS is performed. In both cases,

MN send two HIP messages to the destination, so the number of messages for these cases remains same.

In Hierarchical HIP, if the mobile node moves to one AP's coverage to another within the same H2 domain, RVS_2, initiates the traditional update procedure to update the MN's new information about its movement. In eHIP, this location update procedure is performed earlier by EU messages. Consequently, HIP messaging is reduced and updating the CNs are transferred to the RVS.. In eHIP, MN only sends EU messages while moving among the same H2 domain access points and receives a confirmation message (EU3) from RVS_2. Other eHIP messages are not used since there is no communication over other RVS_2. While considering MN has several ongoing connections with CNs, total number of messages will be a small amount in eHIP, since MN should do all updates to CNs separately in traditional and Hierarchical HIP scenarios. This increase in messaging load of MN also causes MN not to continue the active connection as fast as possible. In eHIP, the responsibility of updating CN's is transferred to powerful RVS. We can say that there are up to maximum 65% improvements in total number of HIP messages for MN in average for eHIP.

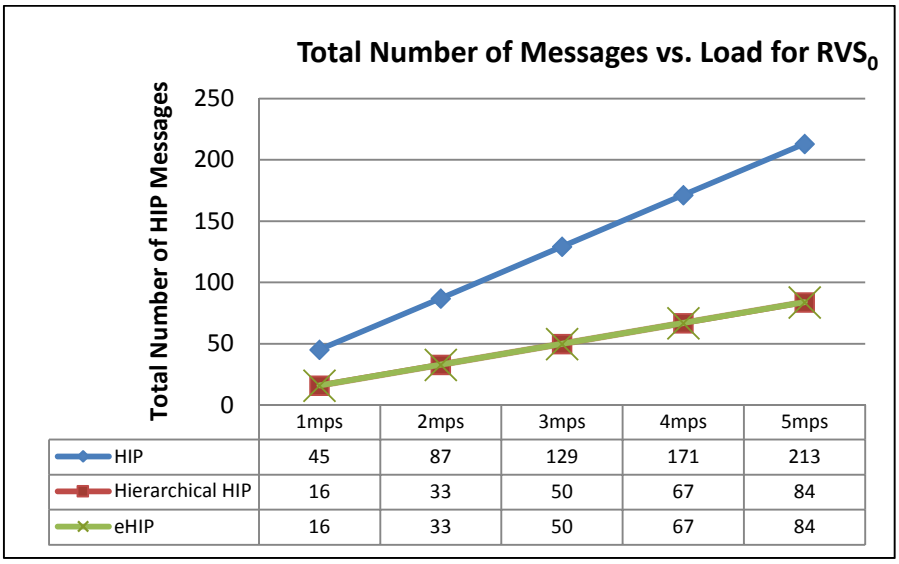
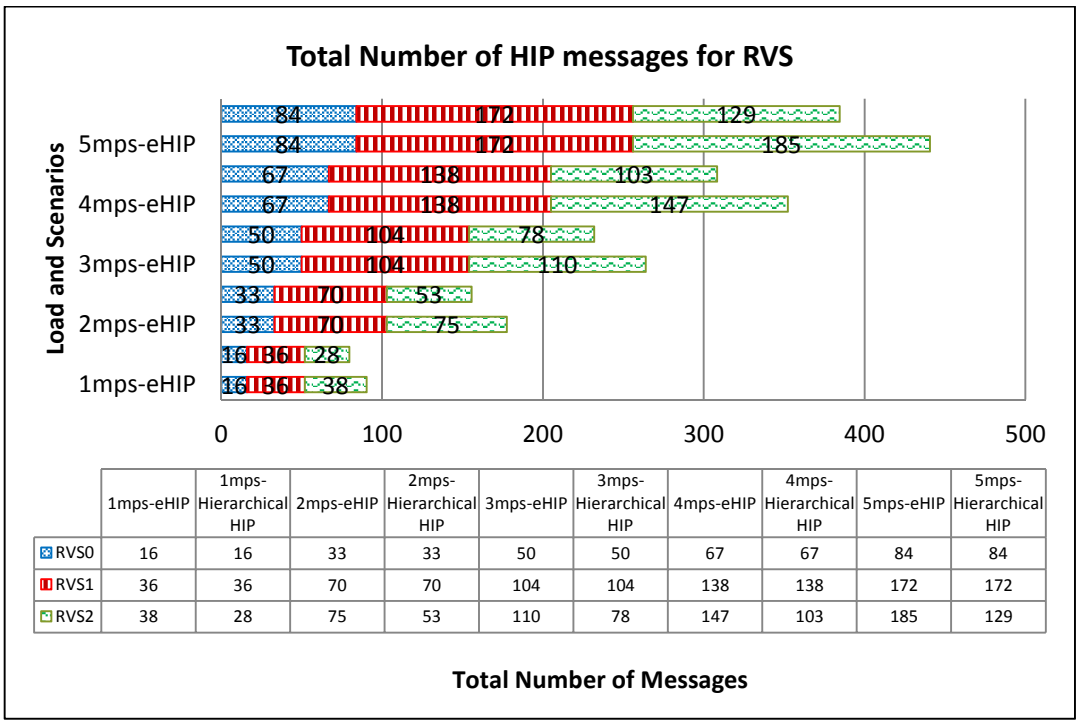


Figure 3.18: Total number of HIP messages generated at RVS_0

Figure 3.18 presents the total number of HIP messages generated at top-level main RVS_0. Due to the hierarchical approach nature, eHIP and Hierarchical HIP has significantly lower overload on main RVS in terms of total HIP messaging. Whereas there is only one RVS on traditional HIP and it is responsible for all RVS communication, the processing overload is divided into several RVS through all hierarchical levels in other two architectures. The results show us that there are up to maximum 60% improvements in average in total number of HIP messages on RVS_0 in traditional HIP and Hierarchical HIP.

In Figure 3.19, total number of HIP messages for all level RVS in Hierarchical HIP and eHIP is shown by numerical samples. Since the responsibility of updating the CNs is on lowest level RVS on eHIP, message overload differences occur between Hierarchical HIP and eHIP in term of the number of messages sent by RVS_2. In other methods, since this process is under the responsibility of MN, the number of RVS_2 level messages in eHIP is higher than other methods about 30% more.



	1mps-eHIP	1mps-Hierarchical HIP	2mps-eHIP	2mps-Hierarchical HIP	3mps-eHIP	3mps-Hierarchical HIP	4mps-eHIP	4mps-Hierarchical HIP	5mps-eHIP	5mps-Hierarchical HIP
RVS0	16	16	33	33	50	50	67	67	84	84
RVS1	36	36	70	70	104	104	138	138	172	172
RVS2	38	28	75	53	110	78	147	103	185	129

Figure 3.19: Total number of HIP messages generated at all levels of RVS

3.4.2 Handoff Time

Handoff time may be defined shortly, as the process of MN's to obtain a new IP address after its movement among the network. The IP address changes while a MN changes the AP, which it is currently served. In traditional HIP, three-way update procedure is completed with CN and RVS after MN completes its movement and start to be served by the new AP. Handoff process ends with the last message of update procedure. In hierarchical HIP, update procedure is done for inside domain H2 handoff (only changing AP inside the same domain) while update procedure with CNs and BE procedure with RVS is done for H2 level handoff.

Handoff time in eHIP can be defined as the time elapsed between starting to be served by new AP and the time of sending the FU (finish update) message. This is because the EU message that starts the early update procedure is triggered by the receipt of router advertisement (RA) message from new AP while still being connected to the old one. Figure 3.20 summarizes the performance of eHIP over other methods in terms of the handoff over time. It shows us that up to maximum 40% improvement in Hierarchical HIP according to HIP and an average 90% improvement in Hierarchical HIP according to HIP. The picks on the eHIP lines show the handoff time between two different H2 domains, namely changing the RVS_2. The larger period of time is expected on H2 handovers due to extra procedures explained before.

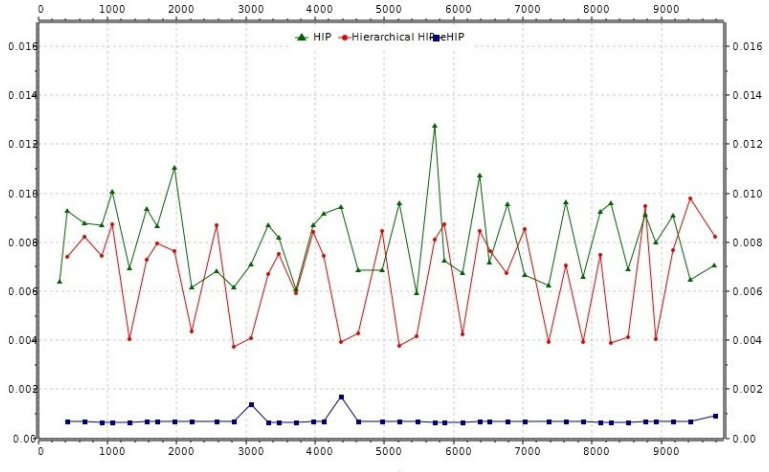


Figure 3.20: Handoff over Time for all scenarios

Figure 3.21 presents a group graphic for handoff times of all scenarios under different network loads. They let us to see an up to 40% time gain on Hierarchical HIP and also significantly up to maximum 90% time gain for eHIP in terms of handoff time.

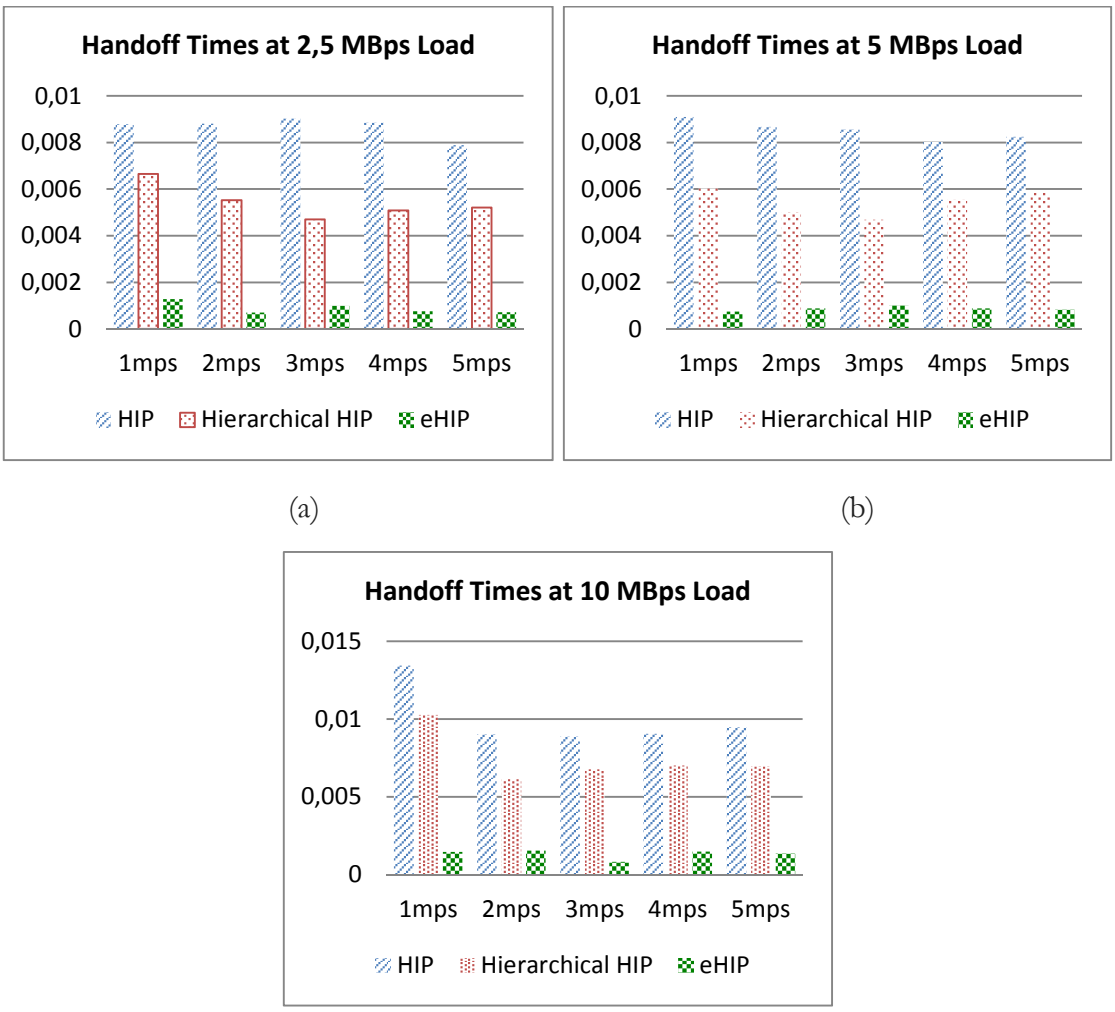


Figure 3.21: Handoff times at 2.5 MBps (a), 5 MBps (b) and 10 MBps (c) network loads respectively for different speeds of mobile node

In eHIP, the time elapsed between the first EU message and the EU3 message is very small. Whenever a MN receives the EU3 message, it can finalize the registration procedure to its new RVS_2 using the new location information obtained from RA messages. The next step is sending the FU message to complete the handoff procedure when it just finishes its physical movement towards its way. MN finalizes its role on eHIP's handoff procedure by sending the FU message. If there are ongoing connections with a single CN or many CNs, as soon as it arrives at its new location it sends their information to its RVS_2 by FU1 messages. Updating the CNs is done by this RVS.

Figure 3.22 show the handoff time for rendezvous servers. RVS handoff time is defined as the total time that RVS need to complete the updating MN's new location information. eHIP's improvement over Hierarchical HIP is shown for each second level RVS. Due to the single RVS in the system and thus there is no change of RVS, traditional HIP scenario is not included in these results.

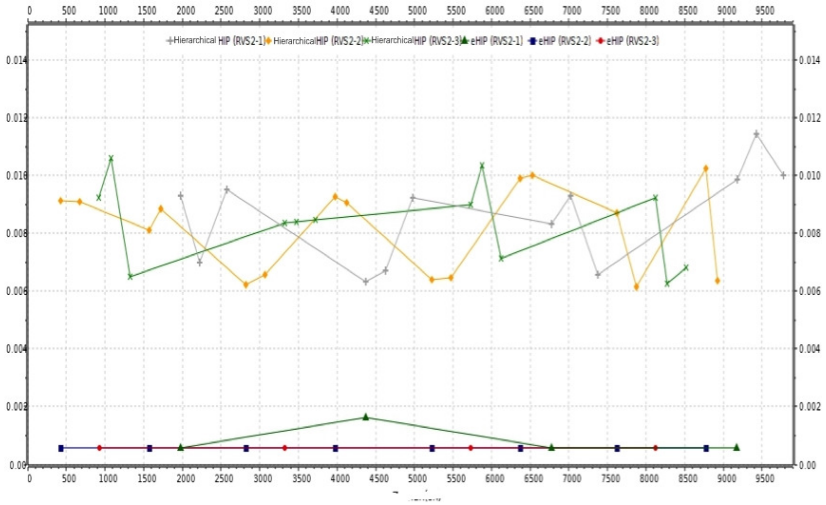


Figure 3.22: RVS handoff over time for Hierarchical HIP and eHIP

3.4.3 Jitter

Jitter of eHIP for different traffic loads calculated as variation of delay of packet from source to destination. Especially for delay sensitive applications such as VoIP, low jitter has of importance. Figure 3.23 express the jitter for our simulations under three different scenarios. Although the method has an extra message flow, due to the gain on handoff times, jitter is slightly lower than the other mechanisms compared. The rushes on the graphic indicate the handoffs.

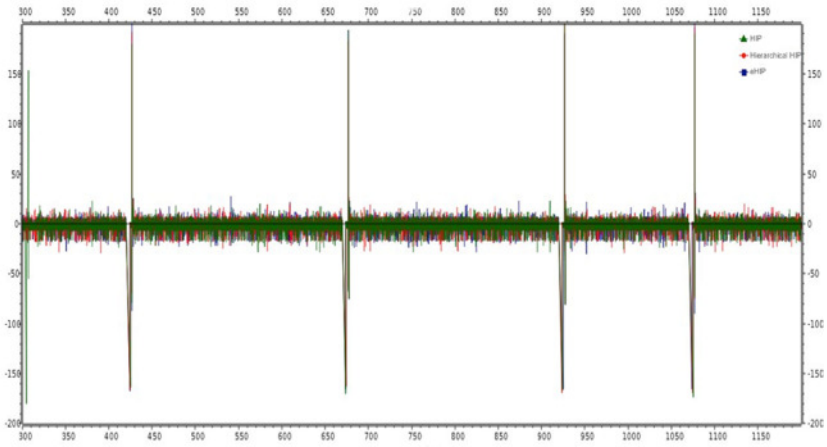
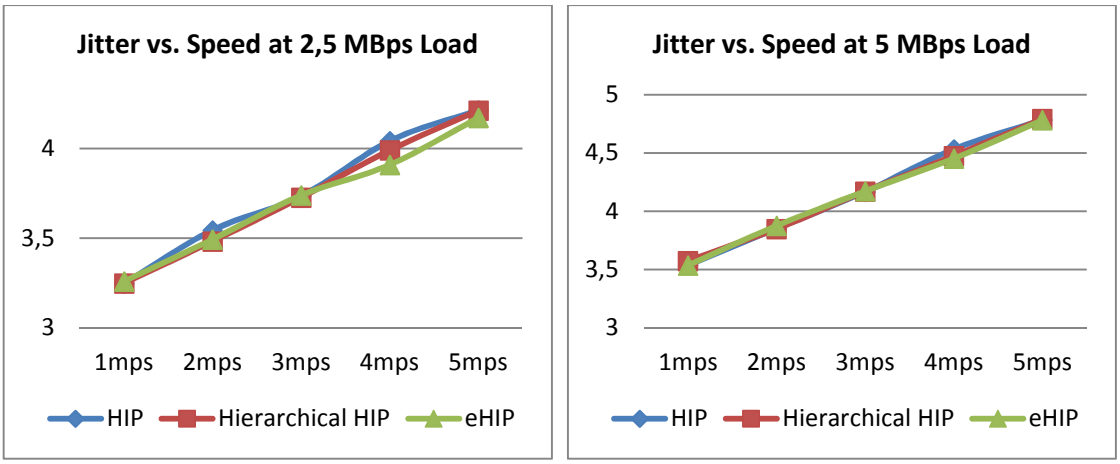
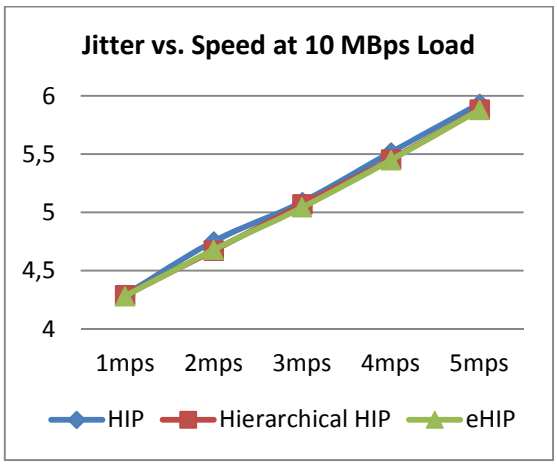


Figure 3.23: Jitter over Time for all architectures

Figure 3.24 presents a group graphic for jitter of all scenarios for different speed of mobile node. The numerical values are given as standard deviation of the jitter values. For each different network load, eHIP has is even slightly lower jitter than other methods. Although the extra message processing and exchanging procedures of eHIP, jitter does not increase significantly because of the positive gain on handoff time. The increasing number of handoffs for faster mobile nodes causes the increase on jitter in the network.



(a) (b)



(c)

Figure 3.24: Jitter vs. Speed results at 2.5 MBps (a), 5 MBps (b) and 10 MBps (c) traffic load respectively for different speeds of mobile node

3.4.4 Round Trip Time (RTT)

RTT is calculated as the time of arrival of packet from source TCP and UDP applications and arrival of reply from destination to source. Figure 3.25 presents the RTT values over time for all scenarios. The rushes show the packet losses during the simulation. The speed of mobile nodes may be determined as a neutral factor on RTT. RTT varies depends on the packet queue length, packet delays and loss. MN'S moving speed or handoff time doesn't have prominent effect on RTT.

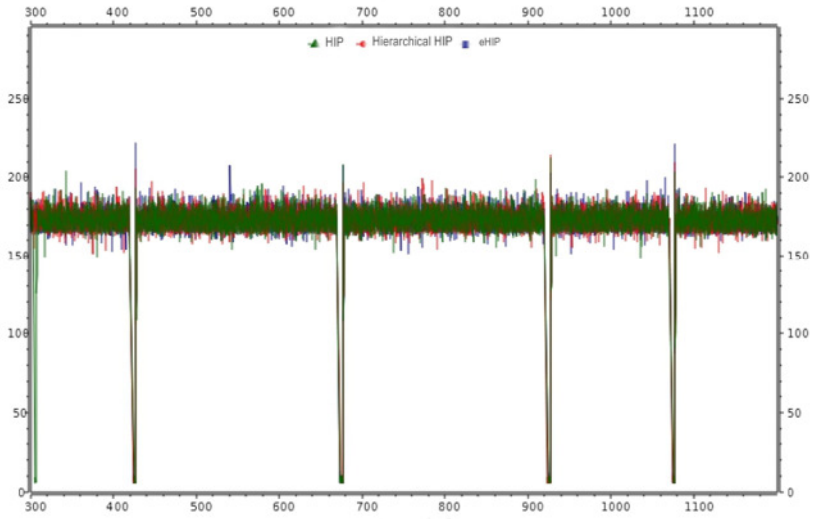


Figure 3.25: RTT over Time for all architecture

Figure 3.26 presents a group graphic for RTT of all scenarios for different speed of mobile node. In eHIP, although the extra messaging overload of multi rendezvous servers located on hierarchical HIP and eHIP architectures, RTT is not affected in negative manner.

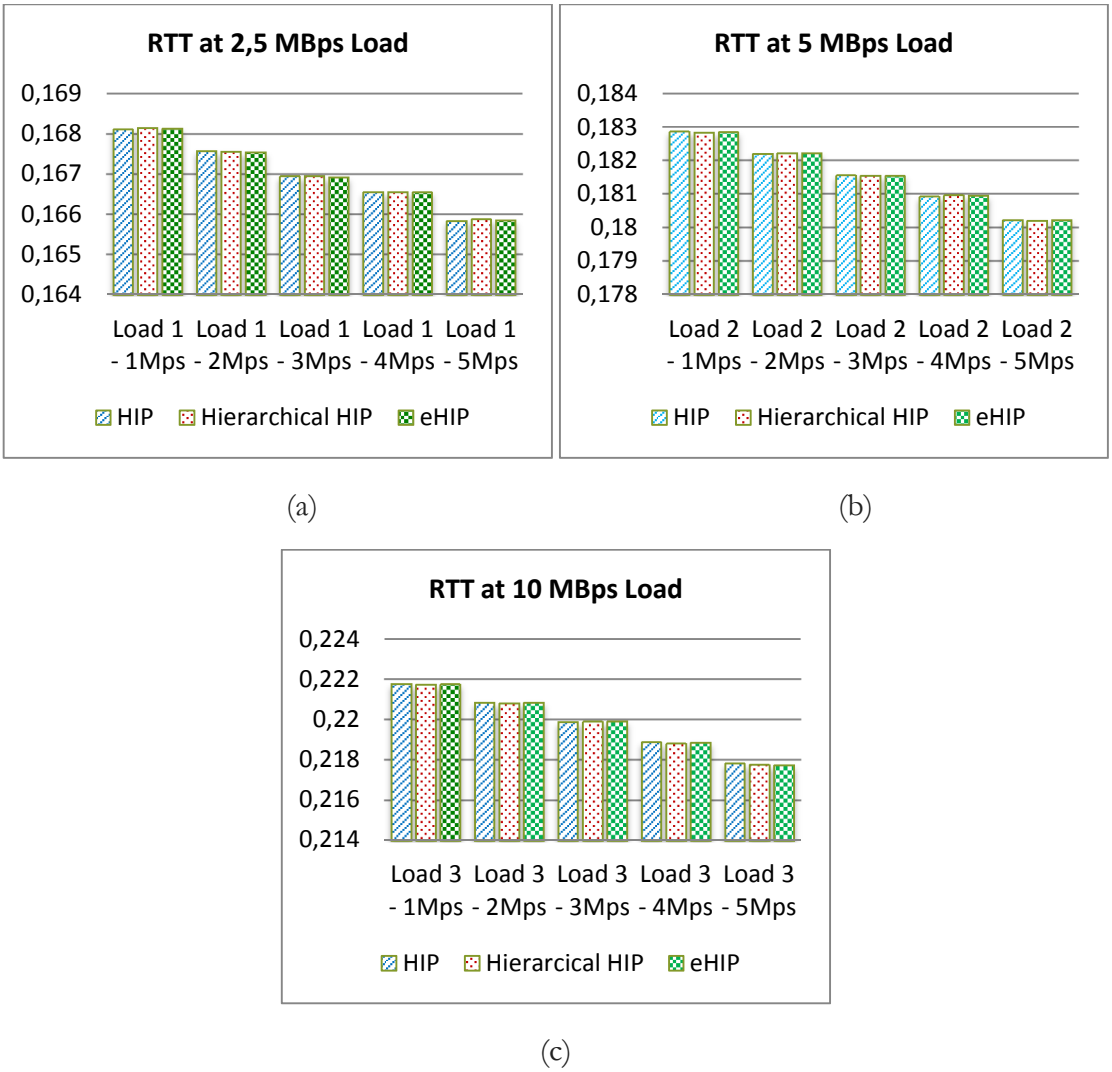


Figure 3.26: RTT results at 2.5 MBps (a), 5 MBps (b) and 10 MBps (c) traffic load respectively for different speeds of mobile node

3.5 Chapter Summary

HIP is the dominant and promising protocol that supports locator/identifier approach and provides many other features such as multihoming and security. In this chapter, we have proposed a handoff management mechanism for existing imperfections of HIP's classical mobility (UPDATE) process. While classical HIP offers to follow the classical handoff approach where L3 handoff operations initiate after L2 handoff completion.

For our proposed mechanism, we first introduce a hierarchical network architecture for HIP and our novel handoff mechanism. This new proposal is called "early update for HIP (eHIP)". eHIP aims to start the update process of mobile node's location changes earlier than classical HIP's process. The main difference of eHIP from former proposals is inheriting the idea of starting movement detection for mobile node and attempt to finish the location update dependent from L2 handoff completion. The idea of updating the new location of a MN is primarily feeds from

FMIPv6's fast handoff and anticipation methods. Due to our hierarchical network structure and early update process, we have evaluated the advantage of our proposal over classical HIP approach.

eHIP's movement detection and handoff decision function rely on router advertisement messages which may reveal extra bandwidth consumption and message exchange density in the network. Therefore, while keeping this fundamental eHIP version, we also propose to enhance eHIP by employing predictive approach of mobile node's movement in the network.

4 A Prediction Extension for eHIP

In this chapter, a simple and architecture-compatible prediction extension is proposed for eHIP in order to improve the update mechanism. This extension, aims to trigger the early update of a mobile node by investigating the path during its mobility somehow earlier than triggering point of eHIP. The success of this method has been examined with integration of this extension to eHIP method and successful decisions made both with and without taking into account the mobile node's speed.

In eHIP, the update need for a MN is based on a decision before completely leaving from its current domain. EU procedure is triggered by recipient a router advertisement message from its candidate AP. This new extension runs as a new operating mode for eHIP that aims to trigger early update before receiving a signal from a candidate. Some new assumptions are made for network architectures due to the prediction feature of eHIP.

4.1 p-eHIP Network Architecture

In order to run p-eHIP mode in an eHIP architecture, we assume that rendezvous servers (RVS) have the network topology information considering all other rendezvous servers and access points in the network.

According to this new design, actually two modes of eHIP can operate together according to the success of our decision and early update. Note that the operating responsibility of this new mode is on rendezvous servers. If a RVS match the conditions for prediction then it completes a decision based early update (p-EU) for the mobile node. Figure 4.1 shows a sample network topology and scheme for predictions and p-EU decisions on mobile node's path.

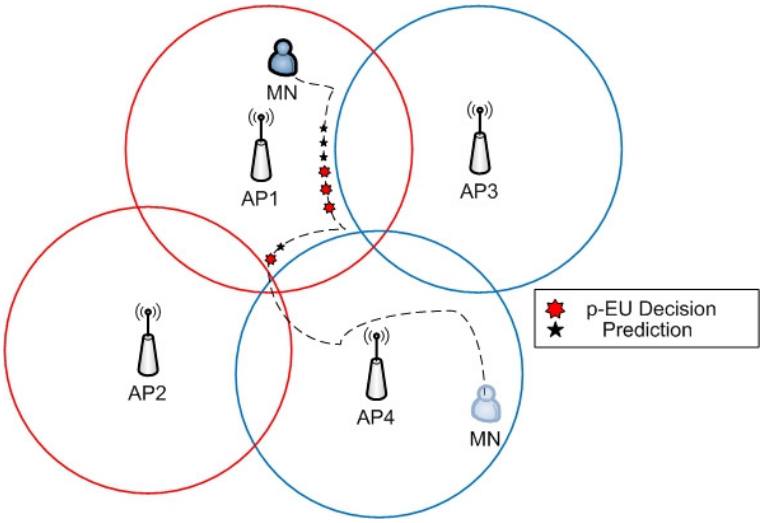


Figure 4.1: Predictions and p-EU decisions on mobile node's path

When a mobile node continues its movement and requests the regular early update initiation from its current RVS, then RVS replies it with the information that it has been successfully updated before its request base on movement prediction. If there is no prediction based update or if the prediction is not successful, then RVS switches on to regular early update mode and continues early update for the mobile node. Figure 4.2 represents the general process flowchart of p-eHIP extension.

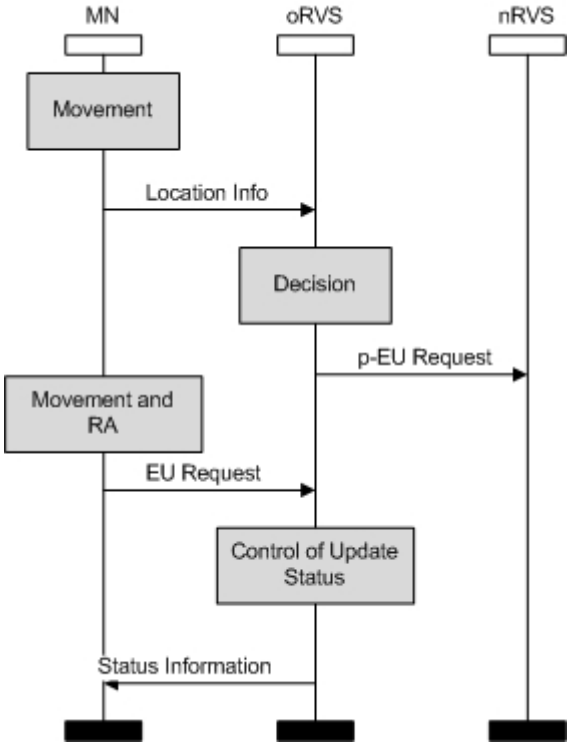


Figure 4.2: p-eHIP General Process Flowchart

We also propose that mobile nodes are responsible for sending their location information in the network to their current RVS periodically. RVS keep these location information tables for each mobile node to track the changes in its movement.

4.2 Prediction based Decision for p-eHIP

In order to apply this method, a decision method is needed. According to this prediction method, two main functionalities are needed.

1. Mobile nodes send their location information periodically to their current RVS_2
2. RVS keep these records as tables in order to track movement of mobile nodes.

Whenever a movement is detected due to the records that RVS keep for mobile nodes' location, our prediction calculation method is invoked. The movement of mobile node is simply detected by any change on the location information of the mobile node. Figure 4.3 shows the prediction method for p-EU decision in p-eHIP. L1… L5 show the location information of mobile node and Prediction 1… Prediction 3 show the prediction made for the mobile node's next AP which is calculated according to network topology information.

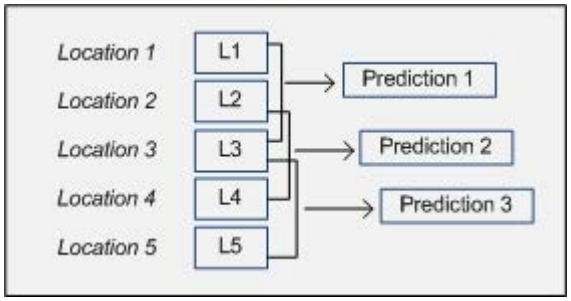


Figure 4.3: Prediction method according to location information

Since the RVS know the topological information of the network, a prediction for the next access point and RVS can be calculated based on the location information and other parameters such as velocity, distance etc. A prediction for next AP and RVS can be made after each location information. However, the decision of triggering an early update for this mobile node is made after iterative three identical results in order to avoid unnecessary false updates for the mobile node.

These early updates are made for each prediction that satisfies the conditions and can be cancelled due to false predictions or any timeout condition. The flowchart of classic mode of p-eHIP is presented in Figure 4.4.

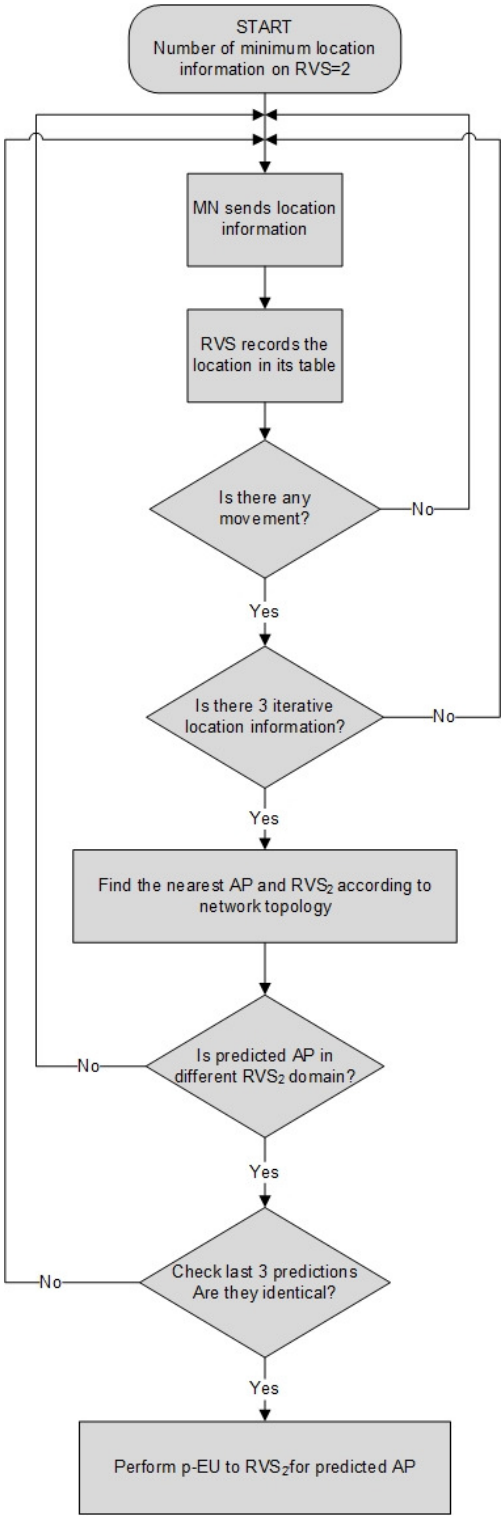


Figure 4.4: p-eHIP flowchart of classic mode

4.3 An improvement on p-eHIP considering Velocity Factor

In order to improve the prediction based p-EU decisions, a method for considering the velocity of a mobile node has been also figured on for p-eHIP. The aim of this variation is to minimize the false or too early update decisions for a MN that has a regular direction and movement towards same AP and to minimize the false p-EU decisions that can be changed for another AP and RVS for a mobile node later.

Each prediction in p-eHIP is related to the distances calculated by depending on fixed locations of APs and their coverage areas in the network architecture. Normally, in eHIP scenario, when a mobile node enters new AP's coverage area, which is managed by different RVS_2 from the current one, early update (EU) is triggered according to the information received from router advertisement messages. For a mobile node moving regularly towards the same AP and in the same direction, iterative p-EU decisions can be made.

The proposed control mechanism in this variation is based on calculating the average velocity of a mobile node from the beginning of its movement (path) records and taking into account this average velocity and its distance to nearest predicted AP. The distance between the mobile node's location and the predicted AP is taken into consideration in this variation. The displacement of mobile node with its current average velocity for its next movement is compared with the calculated distance to the predicted AP. If mobile node can get over this distance within unit time with its next step, then p-EU decision can be made, otherwise, p-EU decision is not made. The flowchart of p-eHIP including the velocity factor is presented in Figure 4.5.

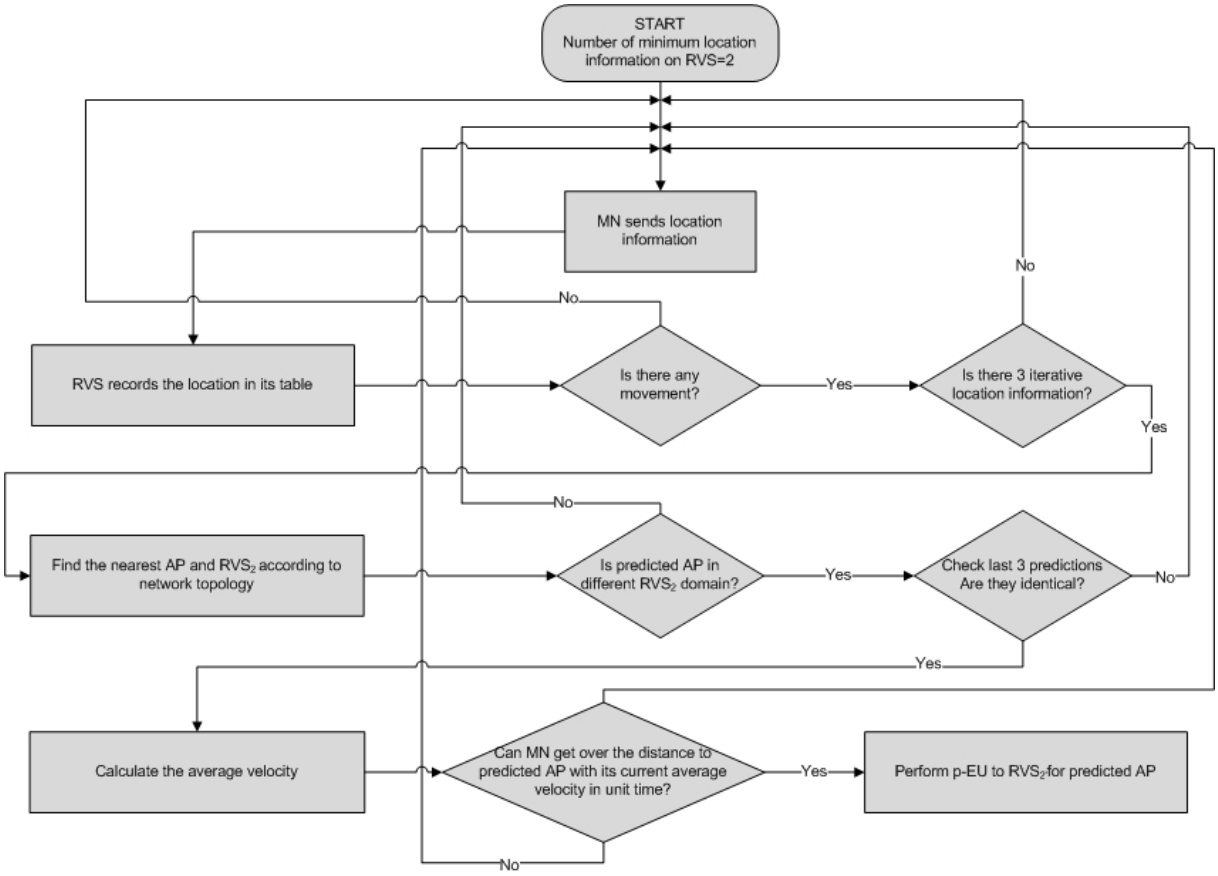


Figure 4.5: p-eHIP flowchart of velocity based mode

4.4 Simulation Environment and Scenarios

The methods for p-eHIP are developed on MATLAB (MATLAB, 2013) environment and numerical results are obtained and analyzed. The results presented in this section are related to the mobile node's path and the networks topology chosen.

In the simulation, the path of mobile node can be drawn by the user with random step intervals or by the simulation randomly. We assume that each step of the path is in one unit time of the simulation. If random path mode is used, some rules are applied due to our assumptions. In other words, the path is drawn according to the probabilities set for movement through x-axis, y-axis or not moving. The algorithm determines the direction of the step according to the possibilities given by the user. For example, the movement of mobile node through x-axis in positive and negative way or staying in its location is determined by 40%, 20% and 40% probabilities in order to implement a circular shape for the mobile node's entire movement in the network. Same parameters are used for y-axis movement also. In the network, the number of RVS_2, APs for each of them, the coverage area (as diameter) of APs are determined as user parameters. The environment is set as 500x500 units^2 for user-drawn scenarios, whereas it is set automatically for random path scenarios due to the number of steps.

The prediction and p-EU decisions are done while considering that MN is sending its location information on its each step/movement during its path as period (p). Scenarios can also be examined under different periods such as p=2 or p=3. In this section, some scenarios are presented and analyzed for p-eHIP method.

4.4.1 Handoff (HO)

The main parameter used for testing our method is handoff time for normal and prediction mode. The handoff time based on prediction is named as p-EU. This p-EU time is defined as the unit time interval between last successful prediction for the new AP that MN moves towards and the first step of mobile node inside the new AP's coverage area. The reason for choosing the first step inside the new AP's coverage is that early updates concludes in advance without any necessity of remaining procedures of normal EU request of MN because of pre- and early registration mechanisms. n-EU duration is defined as the time interval between first EU request message as soon as the MN moves inside a new AP's coverage and the disconnection time from this AP.

4.4.2 Period (p)

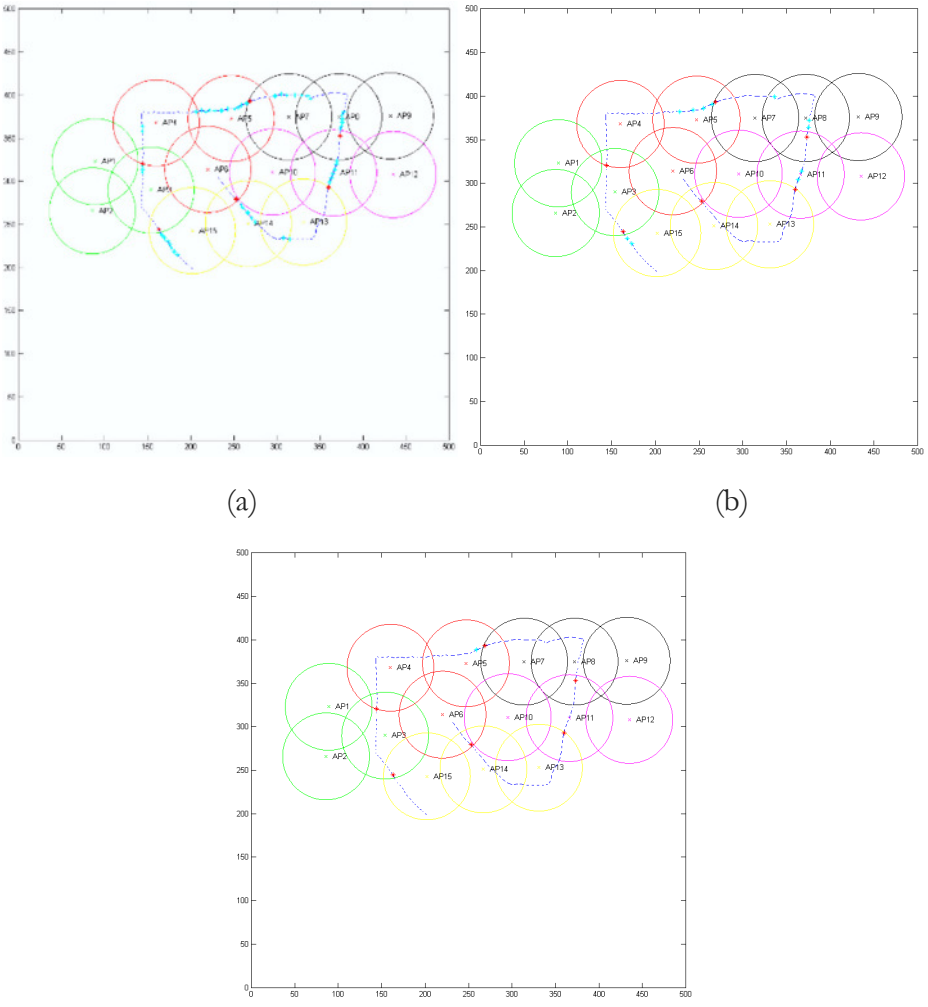
The first assumption for location updates that MN performs to RVS is determined as triggering them at each step. Later different scenarios are settled by using different period values in order to examine the negative or positive effects and their reasons are considered. Period values are determined as a set of p= {1, 2, 3}. P=2 and p=3 means that MN updates its location information to RVS at each two or three steps while moving on its path, while p=1 means updating information is sent at each step as we described above.

4.5 Results

4.5.1 Topology and Scenario 1

In the first network topology and scenario, five different RVS_2 and three APs connected to each of them are located. MN's path was drawn by user and started from AP15's area and ended in AP6's area. Different colors of APs represents that they are under the management of different RVS. RVS are not located in the network topology in the figures.

Figure 4.6 illustrates the p-EU decisions and EU requests for mobile node due to periods 1, 2 and 3 respectively. Blue marks show the p-EU decisions where red marks show the EU requests of mobile node according to eHIP protocol.



(a) (b)

(c)

Figure 4.6: Topology 1 of p-eHIP for p=1(a), p=2 (b) and p=3(c)

As the period increases, the number of p-EU decisions is reduced due to the process of p-eHIP. The number of true or false predictions is determined by comparing the decisions to the requested AP by mobile in EU message (red marks). Some numerical results of this scenario for both methods of p-eHIP (classic and velocity mode) are presented in Table 4.1.

Table 4.1: Numerical results of total predicted p-EU decisions for Topology 1

Mode	Period	Total p-EU Decisions	False	True	Number of Handoffs	Number of Handoffs without p-EU decision
Classic	1	50	7	43	6	0
Classic	2	11	0	11	6	2
Classic	3	1	0	1	6	5
Velocity	1	9	3	6	6	0
Velocity	2	5	0	5	6	2
Velocity	3	1	0	1	6	5

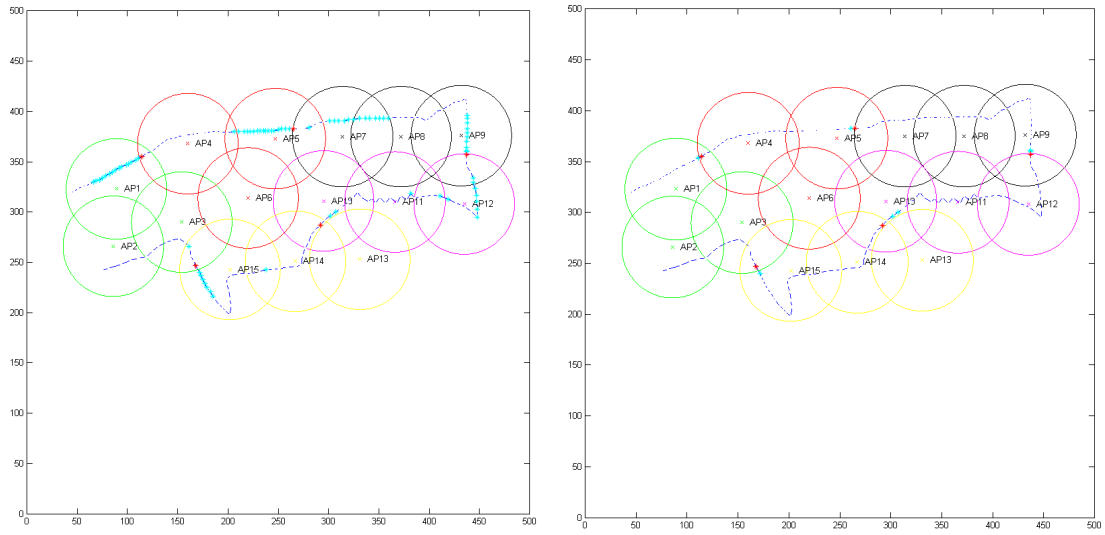
The numerical results depend of the mobile node's path and its average velocity during this path. When the path of mobile node is drawn manually as in this scenario, the velocity is not constant. It changes according to the mobile node's step interval, so mobile node can get over different distances for each unit time in the simulation.

According to the results in Table 4.1 and figures shown above, for p=1, p-EU decisions are made before all EU requests in both modes. An 86% true decision rate is obtained for this period. As expected, number of total decisions reduced in p=2 and p=3. The increase in the period means, the prediction for mobile node cannot be done for each location information, so p-EU decisions' interval is increased and RVS cannot satisfy the conditions for p-EU decision before the EU request. However, p-EU decisions for all handoffs (EU requests) could not be made for p=2 and p=3. Nevertheless, true decision rate is 100%, which means all predictions and decisions are true. Especially for velocity mode, number of unnecessary updates and false decisions significantly reduced as intended. It is clear that 80% enhancement for total number of decisions (updates) and 70% enhancement in number of false decisions are obtained.

4.5.2 Topology and Scenario 2

In the second network topology and scenario, five different RVS_2 and three APs connected to each are located. MN's path, which is drawn by user manually, started from AP1's area and ended in AP2's area as in Figure 4.7

Figure 4.7 show the p-EU decisions and EU requests for mobile node due to p=1 and p=2 and for classic and velocity based mode respectively. Some numerical results of this scenario for both methods of p-eHIP (classic and velocity based) are presented in Table 4.2.



(a) (b)

Figure 4.7: Topology 2 of p-eHIP for p=1(a) and p-eHIP with Velocity Factor and p=1 (b)

Table 4.2: Numerical results of total predicted p-EU decisions for Topology 2

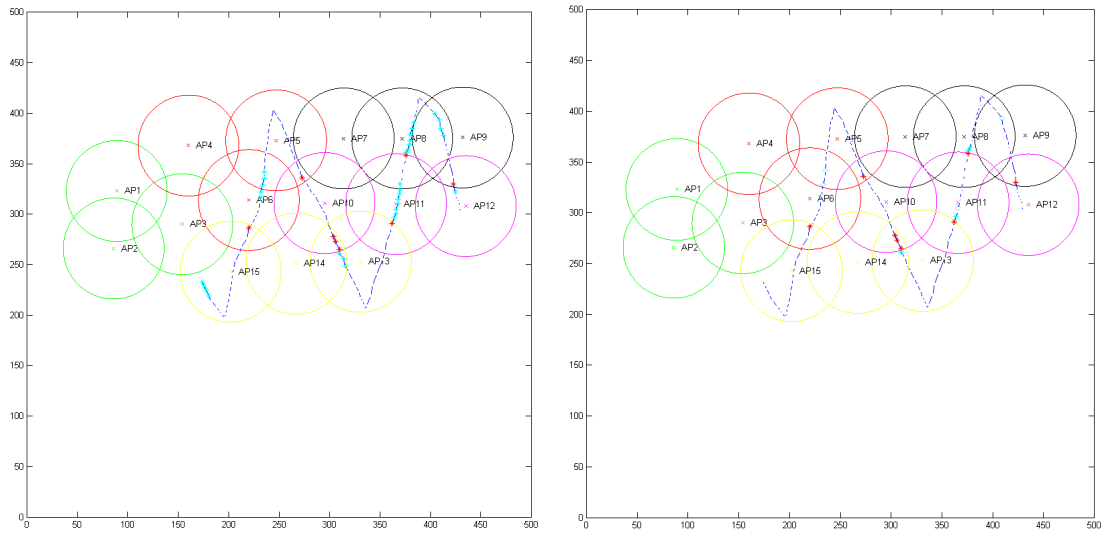
Mode	Period	Total p-EU Decisions	False	True	Number of Handoffs	Number of Handoffs without p-EU decision
Classic	1	77	28	49	5	0
Classic	2	24	7	17	5	0
Velocity	1	7	2	5	5	0
Velocity	2	5	1	4	5	0

In this scenario, the path of mobile node has been chosen in a rectangular structure and mostly toward the same direction regularly. Total five handoff and EU requests happened in this scenario and for p=1, true decision rate is about 64%. In velocity based mode, although the number of decisions reduced, 71% enhancement in true decision rate is observed. This enhancement is observed both by reducing the total number of decisions and total number of false decisions significantly when comparing to classic mode.

Due to the consistency in the direction of mobile node's path, high true decision rates are obtained for p=2 also. Both total number of decisions and total number of false decisions reduced but true decision rates are observed as 71% and 80% respectively for two modes.

4.5.3 Topology and Scenario 3

In the third network topology and scenario, five different RVS_2 and three APs connected to each are located. MN's path, which is drawn by user manually, started from AP12's area and ended in AP15's area as in Figure 4.8. Figure 4.8 also show the p-EU decisions and EU requests for mobile node at p=1 for classic and velocity based mode respectively.



(a) (b)

Figure 4.8: Topology 3 of p-eHIP for p=1(a) and p-eHIP with Velocity Factor and p=1 (b)

In this third scenario, network topology was kept same with Topology 2 whereas path was drawn as to handoff frequently among APs that belongs to different RVS. The effect of these frequent changes on total number of predictions and true decisions are shown on Table 4.3.

Table 4.3: Numerical results of total predicted p-EU decisions for Topology 3

Mode	Period	Total p-EU Decisions	False	True	Number of Handoffs	Number of Handoffs without p-EU decision
Classic	1	32	13	19	8	3
Classic	2	7	4	3	8	5
Classic	3	1	0	1	8	7
Velocity	1	4	0	4	8	5
Velocity	2	2	0	2	8	6
Velocity	3	1	0	1	8	7

For p=1, true prediction decision rate is about 59% while no p-EU decision could have been made for three of total eight handoff during the whole movement. Number of unpredicted handoff increases while the period increases and as a consequence true predictions are decreased. On the

other side, on velocity mode, it is observed that number of predictions are significantly low but also true. This proves us the effect of velocity mode even the mobility pattern is not very steady.

4.5.4 Topology and Scenario 4

In the fourth network topology and scenario, three different RVS_2 and two APs connected to each are located. MN's path, which is drawn by user manually, started from AP2's area and ended in AP1's area as in Figure 4.9 and also show the p-EU decisions and EU requests for mobile node at p=1 for classic and velocity based mode respectively. The low number of network elements are chosen for this topology in order to observe the effect of velocity based predictions. Figure 4.9 shows this observation clearly for p=1.

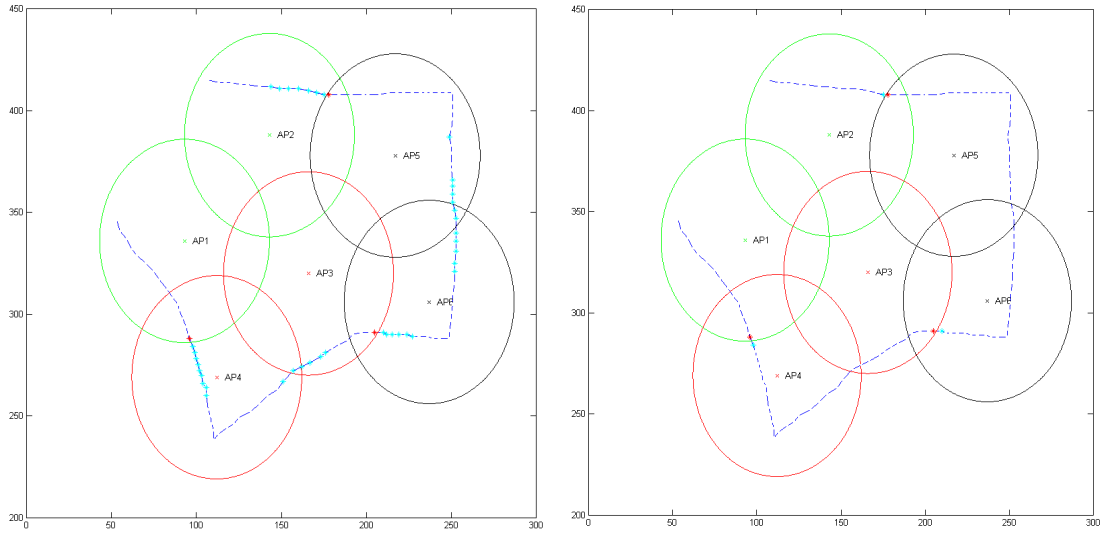


Figure 4.9: Topology 4 of p-eHIP for p=1(a) and p-eHIP with Velocity Factor and p=1 (b)

Three handoff occurs in this network scenario. In classic mode, total number of predictions is 40. True decision rate is observed as 98% for these handoff. But, this situation triggers unnecessary extra update overhead in the network. Regarding to velocity mode, number of predictions regress by 92.5% but all handoffs are predicted and p-EU is decided. Table 4.4 shows all results for both modes of this scenario.

Table 4.4: Numerical results of total predicted p-EU decisions for Topology 4

Mode	Period	Total p-EU Decisions	False	True	Number of Handoffs	Number of Handoffs without p-EU decision
Classic	1	40	1	39	3	0
Classic	2	8	0	8	3	0
Classic	3	2	0	2	3	2
Velocity	1	3	0	3	3	0

Velocity	2	3	0	3	3	0
Velocity	3	0	0	0	3	3

For p=2 and p=3, total number of prediction regress significantly and also not even observed for velocity mode. The reason of that is the MN's path characteristics such as moving in a fast manner. While Mn is moving fast and period is chosen as a larger value, sufficient number of steps for p-eHIP predictions and EU decisions are not supplied effectively.

4.5.5 Topology and Scenario 5

In the fourth network topology and scenario, six different RVS_2 and three APs connected to each are located. MN's path, which is drawn by automatically, started from AP1's area and ended in AP18's area. Figure 4.10 show the p-EU decisions and EU requests for mobile node at p=1.

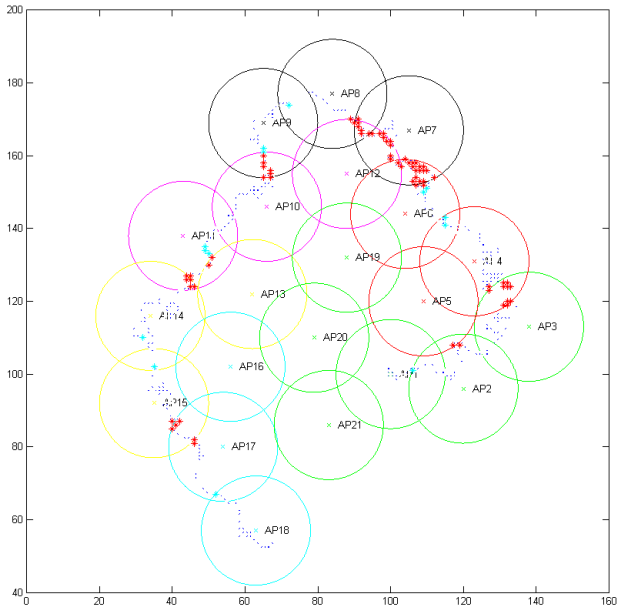


Figure 4.10: Topology 5 of p-eHIP for p=1

Figure 4.11 shows us the inconsistencies on mobile node's drawn path. As we stated before, path is created automatically as one unit or √2 units per step right/left and upwards/downwards.

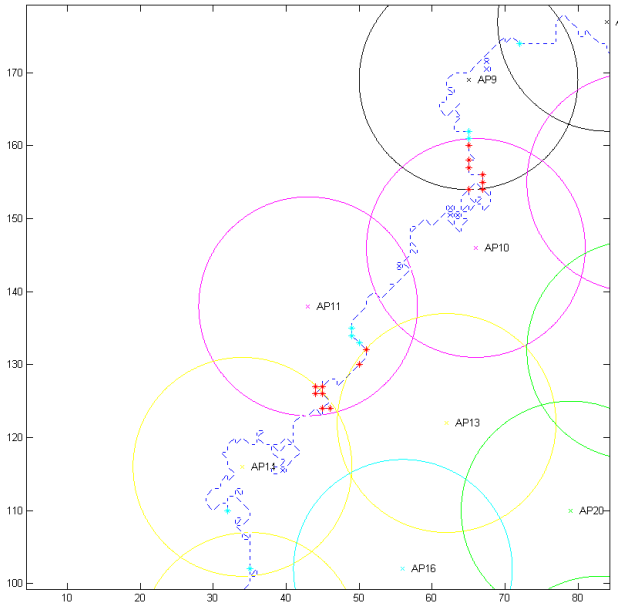


Figure 4.11: A detail of MN's automatically drawn path for Topology 5 of p-eHIP

When the path is drawn automatically, mobile node makes frequent handoffs due to the randomness of its movement. Thus, too many p-EU decisions are not done. But, true decision rate for existing predictions are obtained as 80%.

4.5.6 Time of n-EU and p-EU

While considering and comparing n-EU and p-EU time, for all topologies, p-EU is shorter than n-EU. This time gain varies according to MN's path and network topology as can be expected. The time gain reach up to 50%-60% percent for fast mobile nodes while for slower mobile nodes this gain reach up to 80%-85% percent. For similar scenarios to Topology 5, this gain may increase up to higher values.

4.6 Chapter Summary

In this chapter, we introduced the idea of prediction based eHIP to improve the handoff mechanism by removing dependency to router advertisement messages. We firstly proposed a simple prediction mechanism that relies on capability of mobile node's location awareness by using a generic location system. RVS is responsible for analyzing the mobile node's location updates and make the handoff decision on predictive mode. The main aim was to form a basis for more advanced enhancement for triggering eHIP mechanism. This enhancement aim requires to become dependent from RA messages but use the topological information for movement detection. This chapter shows us that several parameters and factor can be considered from network topology for helping movement detection.

To improve this idea, in next chapter, we consider a grid deployment of wireless sensor nodes that will help to calculate the position of the mobile node. But also mobile node will not need to know its real position by any generic system, neighboring information on the network will be used for location estimation with different techniques and specific new network elements.

5 Sensor Based Location Estimation and Handoff Improvement on eHIP

As described in Chapter 3, eHIP mainly propose to improve the layer 3 handoff procedure that we defined in conjunction with changing RVS_2 domain in our hierarchical architecture. eHIP aims to achieve the early update of a mobile node's location update just before the physical point of attachment change (layer 2 handoff) occurs and as soon as it is completed, MN just finalizes the eHIP procedure, thus experiencing minimum delay disruption as shown in the evaluation of our eHIP protocol.

In this chapter, we propose to improve the current eHIP's movement detection mechanism to trigger the early update initiation regardless of using router advertisement messages broadcasted from HIP enabled and RVS aware access points. As in 802.11 and Mobile IP generic principals, the network-level movement of a MN trigger the need of layer 3 handoff in order to continue its ongoing connections, this generates delay between the link layer handover and the network layer handover. In our hierarchical architecture and eHIP schemes, the network level movement detection procedure is also network based using Router Advertisement messages.. The eHIP procedure is triggered and takes place in focus when a H2 and H1 domain handoffs occur. While changing an AP inside the same domain, only regular RVS update procedures take place (described in section 3.2).

In order to develop an improvement for movement detection phase of eHIP and proceed with a proactive registration of the moving node,, we propose to deploy a sensor node assisted mechanism. As, Internet of Things is emerging with different enabling technologies such as sensors and RFIDs, the basic idea of this proposal is to use sensor nodes based extra topology information from network and use for movement detection phase by obtaining location information from these sensor nodes. We follow the approach introduced in (PAPAPOSTOLOU & CHAUCHI, 2010)]applied to Mobile IP movement detection improvement for better handover quality. Since sensor nodes are small, lightweight and portable detection station, it is a kind of preferable type of technology for recent years especially for wireless localization techniques. Some related work can be found on (WAHARTE, et al., 2008) and (BAHETY & PENDSE, 2004). Waherte's study

introduce sensor based architecture to limit the number of channels to scan for next AP decision to connect. In Bahety's study, sensor networks are employed to enhance the sensing of L3 handoff decision and manage the AP registration.

There are also many other location sensing technologies that can be used for positioning mechanism such as infrared, ultrasound, wireless local area networks, cellular networks, Bluetooth, RFID, ultra wideband etc. (PAPAPOSTOLOU & CHAOUCHI, 2009).

5.1 System Design

In our proposed hierarchical network architecture, a deployment of sensor nodes on the network is considered to help for location estimation of a mobile node during its real time mobility. Each sensor node has a unique identifier (ID). This identifier might be its absolute position. The active side of our proposed architecture is named as H2 domains, which are composed of access points and managed by lowest level RVS_2 in eHIP network architecture. RVS_2 is responsible for administrating of early update mechanism. The main purpose of this mechanism is based on collecting ID information from nearby sensors of a mobile node and uses them in order to evaluate a location estimation assisted by a new network component named Network Location Server (NLS). This location estimation is considered to be used for early update (EU) decision of mobile node according to eHIP mechanism. Simply, it is considered to make an EU decision apart from waiting router advertisement message broadcast in the network for next AP decision.

5.1.1 Message Types

A few types of new messages are introduced to be used in this mechanism. Three types of messages are introduced for our improved movement detection function as ID_REQUEST, ID_REPLY and SENSOR_ID_LIST. ID_REQUEST is the broadcast message from MN to all sensors inside its coverage area to receive their IDs. ID_REPLY is the type of messages generated by sensors for each request from mobile nodes including their ID information. SENSOR_ID_LIST is the list of detected messages that MN retrieves and used for sending this information to NLS.

Location Estimation function is primarily dependent on geometric calculations of positioning algorithm and distance calculation. NLS replies to MN with LOC_EST_POA message to inform about the estimated best appropriate PoA.

5.1.2 Grid of Sensor Nodes

We consider a set of sensor nodes located throughout the network environment; at this stage of our work we consider them static sensors. We assume that their locations are stored on Location Server in order to use for location estimation. RVS_2 are responsible of number of APs in H2 domain and the equally spaced grid of sensor nodes are deployed as serving for these domains. Mobile nodes periodically request these sensors to obtain their ID information and create a list as SENSOR_ID_LIST and send to the NLS.

Sensor nodes only keep their ID information in order to reply to the MN when it is requested. When a MN sends an ID_REQUEST message to query its nearby sensors, these nodes reply to

MN by ID_REPLY message with their IDs. The coordinates of these sensor nodes are stored in the NLS.

Ones again, as stated before, at this stage of our work, the sensors are considered to be static. Also, the deployment of the sensor nodes are considered both steady and organized manner or distributed randomly, however their positions are well known by the NLS server. The other case to be taken into consideration is involving dynamic and mobile sensor enabled nodes to movement detection phase. In our proposal, we assume and examine the deployment of a static and passive grid of sensor nodes throughout network topology for enhancing movement detection of a mobile node. An illustrative figure can be seen on Figure 5.1.

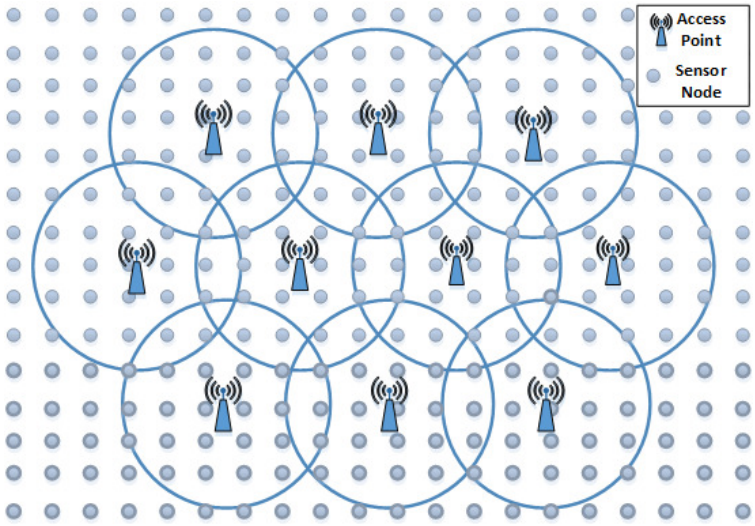


Figure 5.1: An illustrative sample for sensor grid deployment and Access Points

5.1.3 Network Location Server (NLS)

The location information of all sensor nodes, access points (APs) and necessary information for IP address configuration is stored in a database. This information is needed to be used for the location estimation of a mobile node. NLS is responsible for most important system function of location estimation and decision of most appropriate next and new point of attachment for the mobile node.

NLS store actual *(x,y)* coordinates of sensor nodes and access points of the subdomains. The topologically nearest AP to each sensor is also stored. It maintains location of sensor nodes and access points in separate tables. New network address configuration information for access points is also stored in its table. Table 5.1 summaries the table that is storing sensors' topology information.

Table 5.1: Storing Sensor ID, location information and nearest AP on NLS

Sensor_ID	***x*-coordinate**	***y*-coordinate**	**Nearest_AP**
001	3	3	AP_1
002	3	2	AP_2
003	2	3	AP_2
…	…	…	…

NLS retrieves the detected sensor list from mobile nodes and estimates their location inside the network for each SENSOR_ID_LIST and returns the most appropriate AP and its address configuration details. The details of this functions are described in 5.2.2. Initial construction of this database is under consideration of system designer manually.

5.2 System Functions

There are three main system functions as Sensing, Location Estimation and Handoff Decision. Table 5.2 summarizes the symbols used in system functions.

Table 5.2: Symbols used in system functions

Symbol	Definition
S_d	Set of detected sensor nodes
x_n, y_n	Position of a detected sensor node *n*
x_m, y_m	Estimated location for MN *m*
N	Number of detected sensors
x_r, y_r	Position of reference APs *r*
d_{mr}	Distance between estimated location of MN and reference AP
PoA_{est}	Estimated best appropriate AP for MN

5.2.1 Sensing

During the real time movement of MN, it periodically queries nearby sensor nodes to detect a network topology based ID list. This ID-retrieving scheme employs ping-pong phenomenon for message exchange between them. MN periodically broadcast ID_REQUEST messages. The sensor nodes which receive that message, without any other consideration or extra functions, reply to the mobile node with their ID information within ID_REPLY message.

Subsequently, MN receives the ID_REPLY messages, it constitutes a SENSOR_ID_LIST from set of detected sensor nodes S_d. MN sends this SENSOR_ID_LIST to NLS and waits for its reply. Figure 5.2 shows the sensor detection phase as message sequence chart block for MN.

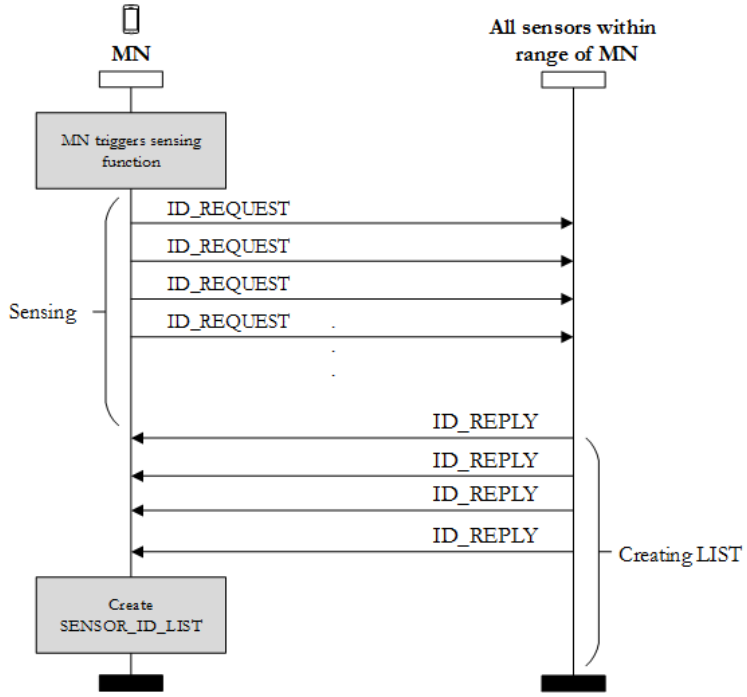


Figure 5.2: Message sequence chart for sensing function

Before sending the SENSOR_ID list to NLS, MN also maintains a control function for similarity of the current detected list with the former SENSOR_ID list. If the detected sensors are same with the former ones, it downs not send the list to NLS, since it will receive the same location estimation with the previous reply of NLS. This control is to avoid extra processing overhead regarding to distance calculation function described in section 0. Time intervals between periodic sensing messages and sending SENSOR_ID_LIST to NLS depends on network system design issues.

5.2.2 Location Estimation

This is the core function of our proposed mechanism that is implemented on NLS side. Whenever NLS retrieves list of detected sensor from mobile nodes, it triggers database lookup procedures to obtain the position $(x_{n,}y_n)$ information of sensor nodes on SENSOR_ID_LIST. MN also includes its identity in this message in order to receive the reply message from NLS. Figure 5.3 depicts the general message sequence chart of sensor enhancement in case of H2 handoff for eHIP. The main system's functions are described below that are positioning techniques and distance calculation on NLS.

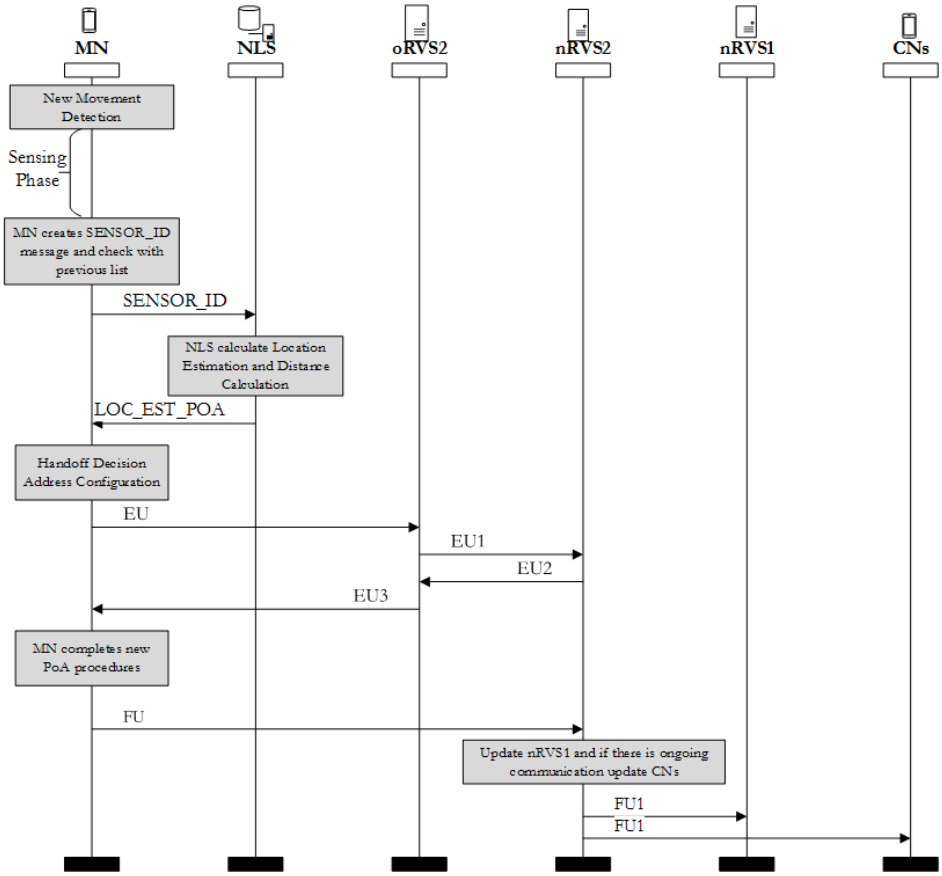


Figure 5.3: Message sequence chart for sensor-enhanced eHIP for H2 handoff

5.2.2.1 Positioning Techniques

The first and foremost part of location estimation phase is analyzing the SENSOR_ID_LIST and calculating the best approximate location for mobile node that requests an estimation for its best candidate PoA. With SENSOR_ID_LIST message, NLS obtains a list of N sensor IDs, which is also denoted as S_d.

A simple and least complex algorithm *Simple Average is* first used for positioning the mobile node from given set S_d. For all detected sensor coordinates of (x_n, y_n) where $n \in S_d$ and (x_m, y_m) is the estimated location of mobile node, estimated location can be expressed as:

$$Estimated\ Location_{Simple} = (x_m, y_m) = \left(\frac{\sum_{n \in S_d} x_n}{|S_d|}, \frac{\sum_{n \in S_d} y_n}{|S_d|}\right)$$

(Equation 5.1)

As another mode for positioning technique, a more complex algorithm *Weighted Average* is used by employing the received power strength of all sensors in S_d. Estimated location can be expressed as:

$$Estimated\ Location_{Weighted} = (x_m, y_m) = \left(\frac{\sum_{n \in S_d} w_n x_n}{\sum_{n \in S_d} w_n}, \frac{\sum_{n \in S_d} w_n y_n}{\sum_{n \in S_d} w_n}\right)$$

(Equation 5.2)

Where w_n is $1/RP_n^{sensor}$, RP_n^{sensor} is received power from each sensor n where $n \in S_d$. In this algorithm, these received power estimation is also sent to NLS by MN after sensing phase in accordance with SENSOR_ID list message.

5.2.2.2 Distance Calculation

After calculating the estimated location of mobile node based on simple geometric approach, the rest of the NLS procedure mostly relies on basic distance calculation techniques between two different points.

For given two points (x_m, y_m) and (x_r, y_r) the distance between these points is given by the equation below where x_r, y_r refers to reference locations of access points on the network topology and d_{mr} denotes the calculated distance between mobile node and reference locations of APs:

$$Distance\ Calculation = d_{mr} = \sqrt{(x_r - x_m)^2 + (y_r - y_m)^2}$$

(Equation 5.3)

NLS calculates the distance between estimated MN location and set of nearest access points to the sensors in S_d. In order to avoid extra processing overhead of distance calculation for all APs in the network, it selects the AP that has the shortest distance to estimated location of MN as the best appropriate PoA for MN. NLS constitutes a LOC_EST_POA message as to include the next candidate AP and its address configuration information related to its subnet. NLS sends this message to MN immediately in order to inform it about its estimation.

$$PoA_{est} = AP_{\min_{mr \in S_d} d_{mr}}$$

(Equation 5.4)

This phase is only based on positioning estimation and principle distance calculation. No other parameters are taken into consideration such as velocity or direction. Handoff decision to trigger early update due to this estimation of NLS is in charge of the mobile node. Algorithm 1 shows the pseudo code for Location Estimation system function.

Algorithm 1 : Positioning and Distance Calculation

1: If NLS receive SENSOR_ID list message **then**
2: For all sensor_id in SENSOR_ID list message
3: Find (x,y) coordinates of all detected sensors from database
4: Find Nearest_AP of all detected sensors from database
5: Calculate $Estimated\ Location$ for MN using simple average algorithm
6: For all AP in Nearest_AP set
7: Calculate $Distance\ Calculation$ equation
8: Choose the AP which has $\min d_{mr}$ as PoA_{est}
9: Send to MN in LOC_EST_POA message

5.2.3 Handoff Decision

Regarding to our proposal, the definition of handoff decision function is selecting the next point of attachment for a MN during its real time mobility based on network topology information. Considering our two system functions, it is clear that the handoff decision depends on the LOC_EST_POA message from NLS. When MN receives this reply message from NLS and the estimated PoA is different from the current one, then MN may decide to trigger the eHIP early update procedure. This decision moment is independent from any L2 technology specific handoff triggers such as WiFi 802.11 based RSS scanning data. Even, router advertisements are ignored to trigger early update of eHIP as we decided to use our sensor based movement detection procedure instead of the classical router advertisement procedure. After handoff decision of MN, it sends the first EU message to its nRVS2 and the remaining procedure of eHIP early updates advances as described in section 3.2 in detail.

Algorithm 2 : Handoff Decision

1: If MN receive LOC_EST_POA message **then**
2: Compare the estimated next AP with the current one
3: if $PoA_{est} \neq AP_{current}$ then
4: MN performs new address configuration
5: and send EU message to its current RVS_2

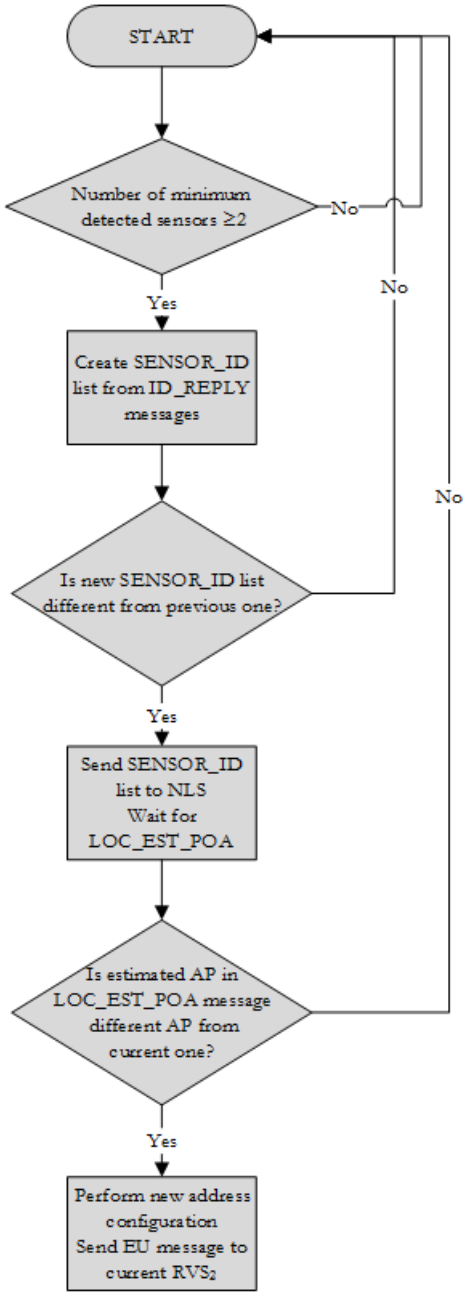


Figure 5.4: Basic flowchart for system functions of MN

5.3 Theoretical Analysis

In this section, a general theoretical analysis is presented for sensor assisted scheme in terms of total *elapsed time* and *energy consumption* due to involving sensor detecting phase for a mobile node.

5.3.1 Total Elapsed Time

5.3.1.1 HIP Handoff

According to basic specification of most of communication mobility protocols, Layer 3 handoff is initiated after L2 handoff is completed. In traditional HIP, UPDATE process (described in section 2.1.1.7) is initiated when L2 handoff is completed. L2 handoff time is technology related such as in the standard IEEE 802.11 or LTE handoff process and it can be defined as total elapsed time of discovery, authentication and association steps of this handoff process:

$$T_{L2} = T_D + T_{AUT} + T_{AS}$$

(Equation 5.5)

where T_D is discovery delay, T_{AUT} is authentication delay and T_{AS} is association delay of L2 handoff. Discovery delay includes channel switching and transmission and probe delay. Probe delay depends on scanning mode used. Scanning mode may be passive or active. In passive mode, total probe delay depends on number of scanned channels and beacon frame transmission rate from APs. It is calculated as regular multiplication of them. Besides, in active mode, total probe delay depends on *MinChannelTime* and *MaxChannelTime* values. These values may be different for different types of devices. The probe delay for active mode can be expressed by equation below:

$$T_{probe} = C\ x\ \frac{MaxChannelTime - MinChannelTime}{2}$$

(Equation 5.6)

The UPDATE process of HIP, which replaces the Mobile IP handoff process, is a three-way handshake process (described in 2.1.1.7). The new point of attachment information is sent inside LOCATOR parameter of UPDATE packets. The average elapsed time for HIP's update procedures are examined experimentally in two different test bed scenarios in section 7.3.4. This average delay also depends on whether ESP association occurs or not between HIP initiator and responder. The basic HIP UPDATE procedure contains three messages. So total delay of this update process is defined as T_{HIP} and expressed as below. The average time for generating, sending and processing the first UPDATE packet is around minimum 20 ms (ARREZ, et al., 2011) for a small device such as tablet computer. This value changes according to device capabilities.

$$T_{HIP} = T_{UF} + T_{U2} + T_{U3}$$

(Equation 5.7)

Where T_{UF} is average delay for generating the first UPDATE packet, T_{U2} is average delay on responder side 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 and T_{U3} is average delay on initiator to respond to the echo request of the responder node

with an UPDATE message which includes the data requested. The total handoff delay for HIP protocol can be expressed as:

$$T_{HIP}^{HO} = T_{L2+}\, T_{HIP}$$

(Equation 5.8)

5.3.1.2 Location Estimation Time

We define the metric of Location Estimation Time (T_{LE}) as the total elapsed time for all functions and message exchange delays during three main phases of our proposed sensor based location estimation mechanism. The elapsed time definition of each part are summarized in Table 5.3.

In our mechanism, T_{LE} is expressed as:

$$T_{LE} = T_{SP} + T_{MN-NLS} + T_{est} + T_{NLS-MN}$$

(Equation 5.9)

Table 5.3: Elapsed time for each step of sensor based location estimation mechanism

T_{SP}	Elapsed time for sensing all sensors within coverage and creating the SENSOR_ID
T_{MN-NLS}	Elapsed time for sending this list to NLS
T_{est}	Elapsed time for location estimation on NLS
T_{NLS-MN}	Elapsed time for sending the EST_LOC_POA to MN

T_{SP} is related to the sensing interval of MN and waiting time for responses from sensor nodes before creating the SENSOR_ID list for sending to NLS. While sensing interval has been considered as a system design parameter, waiting time depends on necessary time to collect reply messages from sensors within range of MN. The messages sent from MN to sensors are 64 bytes messages. The considered waiting time before creating the SENSOR_ID list depends on necessary and sufficient time to collect replies from sensors. In our method, this waiting time is assumed as a constant time interval, and so SENSOR_ID list is created with number of sensor information obtained during this interval, the collided replies are ignored. Also, there is a random small delay between transmissions from sensors as simulation parameter in order to provide a base delay.

After creating the SENSOR_ID list based on replies from sensor nodes, time needed to send this message to NLS (T_{MN-NLS}) and time needed to receive EST_LOC_POA from NLS (T_{NLS-MN}) is related to mainly message size and supported data rate of wireless medium. Due to high data rates of current 802.11 protocols, these values are considered as negligible. T_{est} depends on various components such as device properties of NLS and complexity of positioning algorithm chosen.

Note that handoff time regarding eHIP mechanism is considered as the time between completion of L2 handoff and transmission of eHIP FU message to its new local RVS of new point of attachment. The elapsed time for EU-EU3 message sequence is very low and considered as negligible.

Finally, the total handoff time for our sensor assisted eHIP mechanism is given as:

$$T_{s-eHIP} = T_{LE} + T_{L2-FU}$$

(Equation 5.10)

5.3.2 Mobile Node Energy Consumption

Energy consumption has been a crucial issue since number of mobile devices became as many as fixed devices in the network. Mobile devices operate based on their battery power and so energy consumption of these devices

It is clear to state that an extra mechanism brings overhead to the system in terms of whether number of messages or delay. This extra overhead consequently causes more energy consumption on mobile nodes. In this study, we concerns on mobile nodes' energy issues, however energy status of the sensors in the grid deployment is out of scope for simplicity.

In regular 802.11 protocol, energy consumption is mostly based on Received Signal Strength (RSS) scanning to start the physical handoff. RSS refers to power (or energy) of signal in transmission between two nodes. The distance between these two nodes affect the signal attenuation and propagation loss subject to it. In our proposal, we also have extra consumption for periodical sensing of sensor nodes and collecting replies from them.

5.3.2.1 Energy consumption during classical L2 Handoff

Layer 2 handoff of IEEE 802.11 standard depends on a decision based on received signal strength values obtained by channel scanning. A wireless/mobile device scans the available transmission channels by its interface card periodically. With this periodic scanning, both mobile nodes consumes significant amount of energy and also obtain the RSS measurements from all neighboring APs. The interval of this scanning operations is called as scanning period (T_{scint}) and affects the power consumption directly. Another parameter that influence this consumption is T_{probe}, which has been given in (Equation 5.6). The total consumed energy during IEEE 802.11 scanning can be expressed as:

$$E_{scan} = \frac{T_{total}^{MN}}{T_{scint}} . T_{probe} . P_{scan}$$

(Equation 5.11)

where T_{total}^{MN} is total duration of mobile node's movement and P_{scan} denotes power consumed during scanning phase.

5.3.2.2 Energy consumption during Sensing Phase

The sensing function on mobile node brings extra power consumption due to periodic sensing of sensors in the network for movement detection phase of handoff. While MN is moving among the network, it periodically sends ID_REQUEST messages and waits for a fixed waiting time for their responses. The interval of sensing (T_{spint}) and waiting time (T_{wt}) depend on system setup configuration. In our proposed mechanism, we consider to create SENSOR_ID list to be sent to

NLS for location estimation by using detected sensor within this T_{wt} period. T_{wt} can also be expressed as the response time for a sensor node with ID_REPLY message to MN. For simplicity, we ignore the collided or late replies.

If we define the P_{sense}^{MN} as power consumption during T_{spint} and $P_{recSensor}^{MN}$ as power consumption during T_{wt}, then the total consumed energy during the sensing phase can be expressed as:

$$E_{SP} = \frac{T_{total}^{MN}}{T_{spint}} \left[T_{spint} \, P_{sense}^{MN} + T_{wt} \, P_{recSensor}^{MN} \right]$$

(Equation 5.12)

5.4 Performance Evaluation

5.4.1 Simulation Environment and Parameters

Figure 5.5 illustrates our simulation environment which is a square shape area of *1000m×1000m* . There are 4 RVS_2 and 4 access points for each RVS (total 16 APs). All AP's are located in asymmetric way and has the identical distance between two neighbor APs of *200m*. A scenario which is a single RVS_1 domain is examined, since the main aim of this simulations is analyzing the performance of location estimation enhancement of the L3 movement detection. The communication details among MN and APs depends on HIPMSIM++ framework that eHIP has been developed and simulated in OMNET++ (details are described in section 3.3.2 and section 3.3.3). The inter spacing among sensor nodes is considered as the system parameter. Random WayPoint ("RandomWPMobility) model has been chosen as mobility model of MN inside the simulation environment.

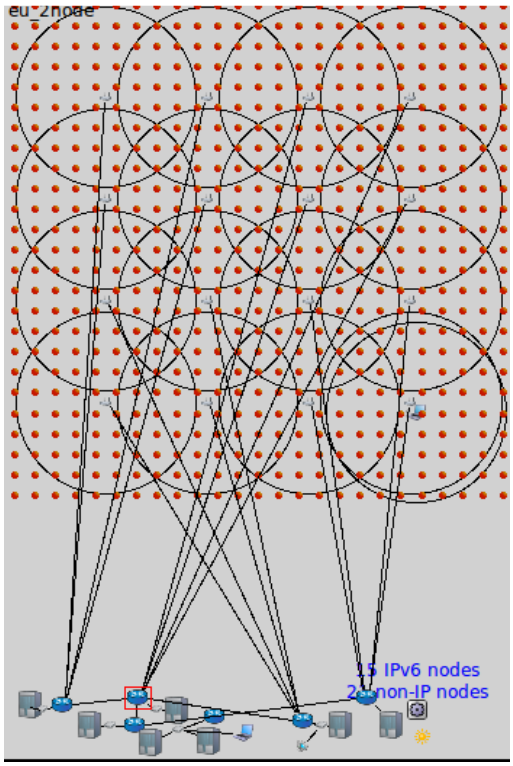


Figure 5.5: Simulation Environment

The most related and important parameters of the simulation design are given in Table 5.4.

Table 5.4: Simulation Setup Parameters

Parameter	Values
Environment	1000m x 1000m
Number of AP	16
Distance between two adjacent AP	200 m
Sensor spacing	{15,20,30,40,50} m
Sensing Interval (T_{spint})	{1,2,3,4,5,6,7,8,9,10}s
Waiting Period (T_{wt}) for sensor reply	50 ms
Speed of MN	{0,5,1,2}m/s
Sensing Range of MN	{30,40,50}m
Simulation Time	10000s

The number of detected sensors depends on the sensor deployment characteristics (inter spacing) and the coverage are of APs. The battery status of sensors are out of scope for this simulation. The list generated after sensing phase depends on the received reply messages from available sensors on the network.

5.4.2 Performance Metrics and Results

The definitions of performance metrics that we examined from simulations are explained in this section.

5.4.2.1 Mean Location Error (MLE)

As a performance metric, Mean Location Error (MLE) has been measured. It has been calculated as the Euclidean distance between the actual and the estimated positions mobile nodes during location estimation phase on NLS.

$$d_{mm'} = \frac{1}{N}\sum_{m=1}^{N}\sqrt{(x'_m - x_m)^2 + (y'_m - y_m)^2}$$

(Equation 5.13)

By measuring this metric, we examine the effect of topology characteristics on estimated location and consequently on the new designed movement detection.

Figure 5.6 and Figure 5.7 show the effect of sensor spacing on location error while using both Simple Average (SA) and Weighted Average (WA) positioning algorithms. It is clear that more intense deployment of sensors occurs greater number of detected sensors and therefore more accurate location estimation can be performed by NLS for both positioning algorithms. Regarding to Weighted Average algorithm, the received power coefficient used as weight values and helps for efficiency of location estimation when using arithmetical average operations. They increase the impact of nearer sensor locations on position estimation. While considering the effect of mobile node's speed, three different speeds have been shown on the figures. The main consideration is, when the mobile node is moving in faster case (V=2m/s) and as the inter sensor spacing increases, MLE also increase. This is because of the MN's changing location and less number of detected

sensors due to higher inter spacing value. All these results have been analyzed as an average of different reader ranges of MN, as stated on Table 5.4.

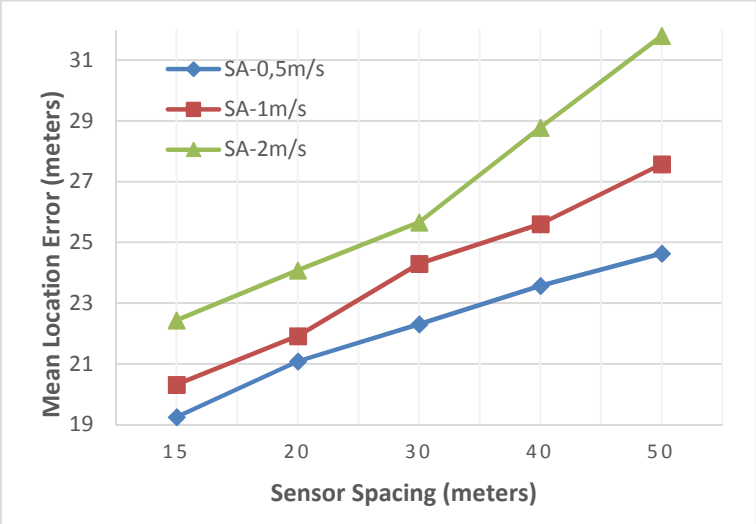


Figure 5.6: MLE vs. Sensor Spacing for Simple Average Algorithm

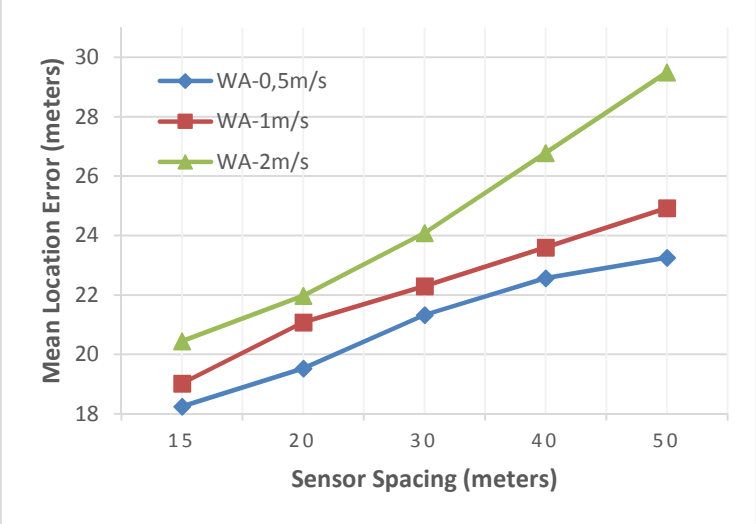


Figure 5.7: MLE vs. Sensor Spacing for Weighted Average Algorithm

In Figure 5.8 and Figure 5.9, we show the impact of sensing interval on mean location error. We have chosen linearly increasing sensing intervals for MN to observe the differentiations on MLE in accordance with MN's speed during its trajectory. The main observation for all cases is that, increase in both sensing interval and MN's speed increase the MLE. As expected, the WA algorithm also performs better due to the effect of weights of detected sensor nodes.

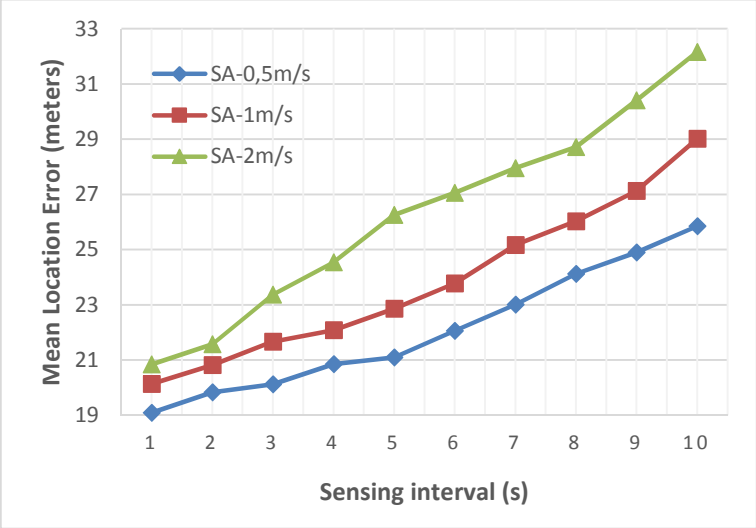


Figure 5.8: MLE vs. Sensor Interval for Simple Average Algorithm

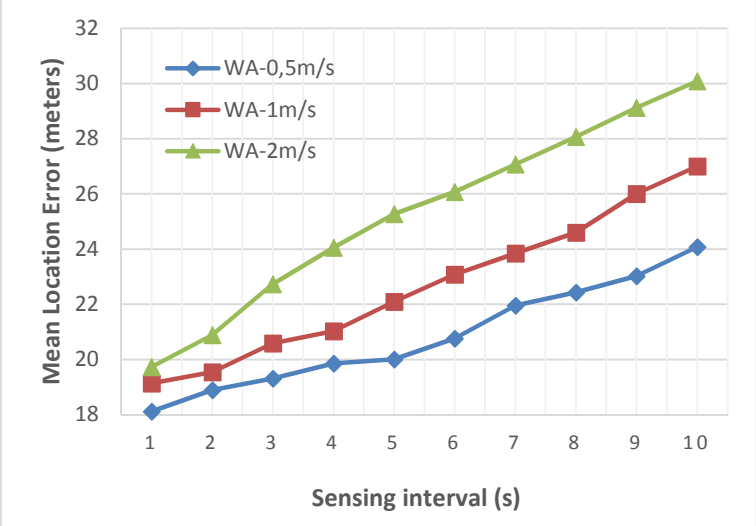


Figure 5.9: MLE vs. Sensor Interval for Weighted Average Algorithm

Figure 5.10 presents the MLE values depending on sensing interval during its movement by four different scenarios that has been analyzed to investigate the effect of mobile node's speed. For MN's speed of V=0,5m/s and V=2m/s, the MLE performance of both SA and WA have been given by considering the average of all different inter-space values of sensor deployment.

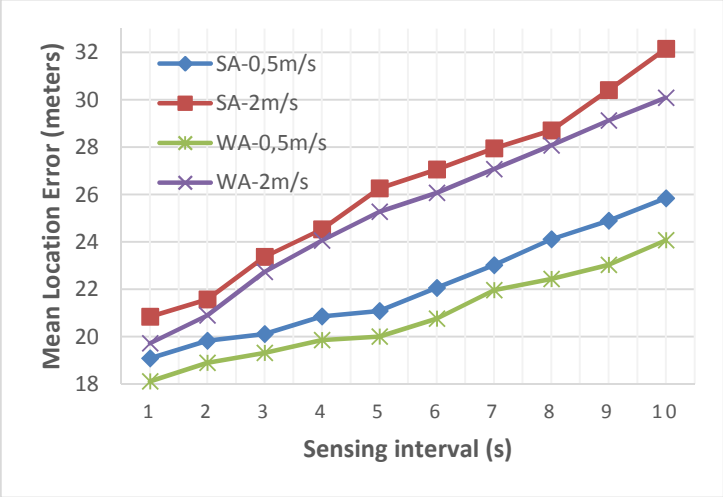


Figure 5.10: MLE vs. Sensor Interval for two positioning algorithms

5.4.2.2 Estimation Accuracy

The estimation of next PoA is the last step on location estimation function of NLS. NLS sends next appropriate PoA estimation to MN and MN performs the handoff decision. We consider the Estimation Accuracy metric as the ratio of correct PoA estimation for MN. When this estimation is identical to the AP which MN receives the highest RSS, we decide the estimation accuracy as correct. High estimation accuracy is main objective of this proposal. This accuracy is mainly related to sensor spacing on the environment and sensor reading period of MN. Estimation accuracy is calculated as the ratio of correct next PoA decisions over total number of decisions made by NLS during MN's movement.

In Figure 5.11 and Figure 5.12, estimation accuracy of two positioning algorithms has been presented as the sensor spacing increases. For both algorithms, larger sensor spacing decrease the estimation accuracy due to low number of detected sensors. For faster mobile nodes, the effect of less number of detected sensors is clearly observed. Especially for slower movement of MN (V=0,5m/s and 1m/s), after spacing values larger than 30m, the decrease on accuracy is noticed.

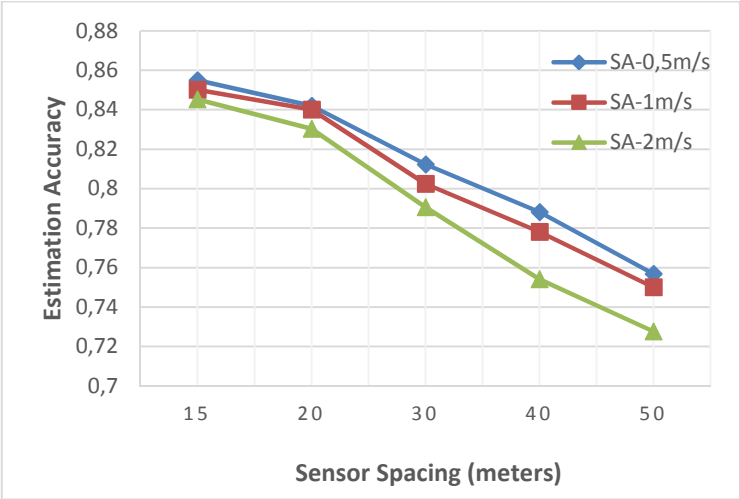


Figure 5.11: Estimation Accuracy vs. Sensor Spacing for Simple Average Algorithm

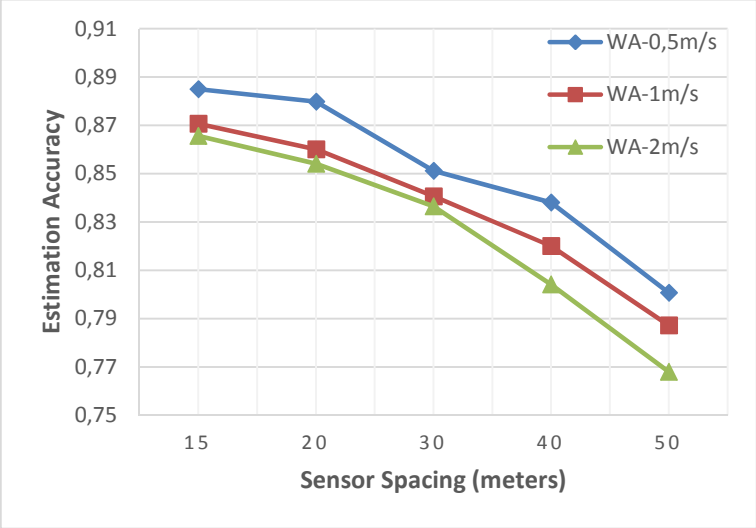


Figure 5.12: Estimation Accuracy vs. Sensor Spacing for Weighted Average Algorithm

In Figure 5.13 and Figure 5.14, the estimation accuracy while employing Simple Average and Weighted Average algorithms is evaluated as the sensing interval increases, for all speed values. For all cases, decreasing the frequency of demanding location and PoA estimation from NLS, degrades the accuracy performance. For larger sensing interval values, when MN moves faster, its sensor detecting capabilities also gets suffered in terms of changing the real location more rapidly. This will cause the difference between real best PoA and estimated PoA for mobile node, and rightfully decrease the accuracy performance.

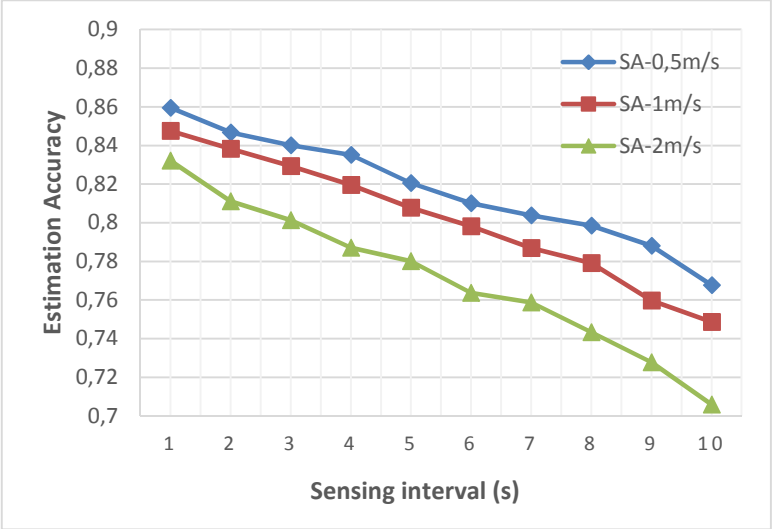


Figure 5.13: Estimation Accuracy vs. Sensing Interval for Simple Average Algorithm

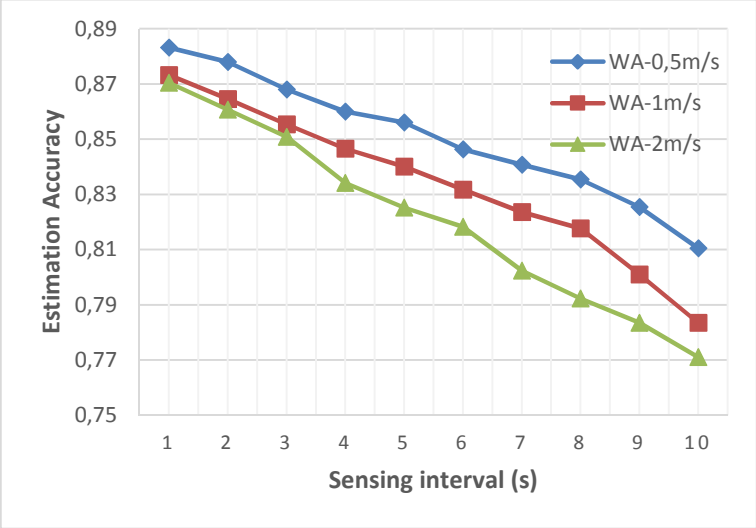


Figure 5.14: Estimation Accuracy vs. Sensing Interval for Weighted Average Algorithm

In Figure 5.15 the estimation accuracy of two different positioning algorithms as the sensing period increases and for different speeds of mobile node is evaluated for average of all reader ranges and sensing intervals. The superiority of WA algorithm on SA can be observed in accordance with sensor spacing, and as an average for all sensor intervals.

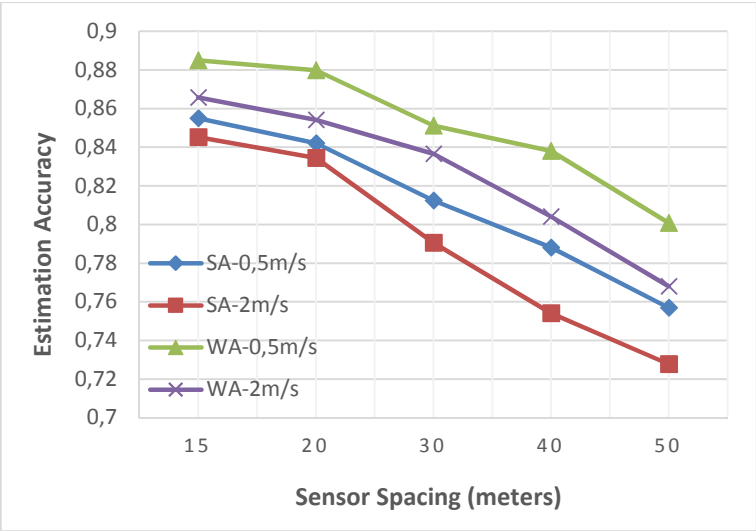


Figure 5.15: Estimation Accuracy vs. Sensor Spacing for two positioning algorithms

This extension relies on the sensor node deployment over any eHIP network to support eHIP handoff process by proactively estimating a next PoA for MN and triggering the eHIP procedure. The main benefit is by-passing the router advertisement broadcast throughout the network and transferring the decision control completely to MN by the help of topology information. This scheme can also help to trigger the L2 handoff in order to gain from energy consumption of mobile devices, after optimization and well deployment of proposed architecture. Either with L2 handoff triggering or just L3 movement detection enhancement, this proposal can support mobility inside heterogeneous network by its technology independence property.

5.5 Chapter Summary

In this chapter we introduced a sensor node deployment assisted extension for eHIP in order to provide a location estimation system for mobile node. This extension introduce a new network element named as Network Location Server (NLS) to provide location estimation function. Mobile nodes obtain a next appropriate PoA estimation related to their trajectory inside the network. This can provide proactive association with next AP by using eHIP's regular version. The mobile node's newly added sensor node detection capability offer to detect the neighboring sensor nodes identity information due to its reading range. The number of detected sensor nodes mainly depends on architectural design of sensor deployment in the network. Several parameters have been examined by extensive simulations. Moreover, the new network element (NLS), employed positioning techniques and new system functions are introduced. A simple but descriptive theoretical analyses are also done for total elapsed time needed for sensor assisted movement detection phase and energy consumption of mobile node during this extra features. This proposal show us that it is possible to benefice from network topology and environment to improve the mobility management of mobile node especially in heterogeneous networks.

Further performance analysis also can be done such as packet loss for different network loads or effect of different mobility patterns.

6 QoS-Aware Mobility Algorithm

In this chapter, we propose an algorithm in order to minimize radio resource utilization (RRU) for our architecture while considering MNs' quality of service needs and real time application delays. In this method, we assume our network architecture as a wireless mesh network version of our proposed architecture for eHIP. The proposed algorithm yields in terms of RRU for MN's ongoing and active real time applications (GURKAS AYDIN, et al., 2010a).

6.1 System Modeling and Problem Statement

We represent our proposed network architecture by a directed graph as $G(V, E)$. It is called a connectivity graph. Each node $u \in V = \{1, \ldots, N\}$ can represent an AP, RVS_2, RVS_1, RVS_0 and all routers connecting them to the Internet. A bidirectional wireless link exists between u and every neighbor v and is represented by the directed edges $(u, v) \in E$. We represent the graph connectivity by a connectivity matrix. The connectivity matrix of $G(V, E)$ is a matrix with rows and columns labeled by the graph vertices V, with a 1 or 0 in position (v, u) according to whether u and v are directly connected or not.

During the mobility, each time when the MN moves through one domain to another, it updates the system with its new location by sending registration update message to the RVS_0through the $RVS_1$of the visited domain. Regarding the data packets, an incoming packet from the backbone to the MN (i.e., downlink traffic) is first intercepted by the RVS_0 then the packet is forwarded to the current MN's RVS_1 which relays the data packet to the corresponding AP for delivery. Hence, the Radio Resource Utilization (RRU) of a MN involves two terms, i.e., the first one regarding the data packets' resource utilization and the second term is related to the resource utilization of the signaling messages used to manage the user mobility. We refer to the first term as the data delivery cost and to the second term as the registration updates cost.

We formulate the problem as follows: Given the RVS_0 scenario of N nodes, find the disjoint nodes that minimize the total radio resource utilization subject to the QoS constraints of the current application during the handover.

The QoS constraint in our case stands for the delay of the ongoing session -- Voice over IP (VoIP) application (LANGAR, et al., 2009).

Thus, the RRU cost can be expressed as

$$\text{RRU\_Cost} = \alpha \text{ xReg\_Update\_Cost} + \beta \text{ xData\_Delivery\_Cost} \quad \text{(Equation 6.1)}$$

where

$$\alpha = \frac{2\mu\ m_{sig}}{2\mu\, m_{sig} + \lambda m_{data}} \quad \text{(Equation 6.2)}$$

$$\beta = \frac{2\mu\ m_{data}}{2\mu\, m_{sig} + \lambda\, m_{data}} \quad \text{(Equation 6.3)}$$

α and β represent the proportion of the amount of signaling messages and the proportion of data packets among the total traffic generated by a MN. m_{sig} and m_{data} represent the average size of signaling messages and the average size of data packets used for registration updates, respectively. μ represents the mean sojourn time of a MN in a subnet (i.e., AP), and λ is the downlink packet transmission rate (in terms of packets/s). A summary of used symbols and parameters shown by Table 6.1 summarizes the symbols and parameters used in system modeling.

Table 6.1: Symbols and parameters used in system modeling

α	The proportion of the amount of signaling messages generated by MN
β	The proportion of data packets among the total traffic generated by MN
m_{sig}	The average size of signaling messages used for registration updates
m_{data}	The average size of data packets used for registration updates
$1/\mu$	The mean sojourn time of a MN in a subnet
λ	Downlink packet transmission rate (packets/s)
Π_i	The probability that the MN is located at the subnet AP_i
N_l	The total number of directional links in the whole network
D_{max}	The maximum tolerable delay for the VoIP application when handing over from one domain to another
T_{start}	The time when the MN starts to send the first packet of registration
T_{end}	The time when the CN starts to receive the first packet of data.

The Reg_Update_Cost can be written as:

$$\text{Reg\_Update\_Cost} = \frac{1}{N_l} \text{x} \sum_{i=1}^{N} \Pi_i \text{ xUpdate\_Cost}(i)$$

(Equation 6.4)

where Π_i is the probability that the MN is located at the subnet AP_i, N_l is the total number of directional links in the whole network and the Update_Cost is given by:

$$\text{Update\_Cost}(i) = \sum_{j=1}^{N}(P(i,j) \text{ x} \sum_{k=1}^{N} \min(d(j,k) \text{ x } d(k, RVS_0))) \quad \text{(Equation 6.5)}$$

where $(P(i,j) = P(AP_i, AP_j)$ denotes transition probability from AP_i to AP_j and where $d(x,y)$ denotes the distance (in terms of number of hops) between x and y.

Likewise, the Data_Delivery_Cost is the data delivery cost of downlink traffic when the MN is connected to the AP_i. It is given by:

$$\text{Data\_Delivery\_Cost} = \frac{1}{N_l} \text{x} \sum_{i=1}^{N} \Pi_i \text{ x Delivery\_Cost } (i)$$

(Equation 6.6)

where the Delivery_Cost(i) is the data delivery cost of downlink traffic when the MN is connected to the AP_i. It is given by:

$$\text{Delivery\_Cost } (i) = \sum_{j=1}^{N}(P(i,j) \text{ x} \sum_{k=1}^{N} \min(d(j,k) \text{ x } d(k, RVS_0)))$$

(Equation 6.7)

Hence we can formulate the problem as the following objective function:

$$\min RRU_{Cost}$$

(Equation 6.8)

subject to :

$$d(AP_i, AP_j) + d(AP_j, RVS_0) < D_{max}$$

(Equation 6.9)

where D_{max} is the maximum tolerable delay for the VoIP application when handing over from one domain to another and it is expressed as $D_{max} = T_{end} - T_{start}$. Where the T_{start} is the time when the MN starts to send the first packet of registration and the T_{end} is the time when the CN starts to receive the first packet of data.

6.2 Proposed QoS-Aware Mobility Algorithm

Our algorithm which takes into account the mobility of MNs with respect to their QoS constraints, starts each time when the MN moves to a new AP. It first compares the registration cost of its indirect path to the RVS_0 through the current RVS_i with a certain threshold *Thresh*. If this cost is equal or less *Thresh,* the MN will choose this path of registration to the RVS_0. After the procedure of registration, the data delivery procedure will take place by start searching the IP address of the RVS_0 in the new AP.

If it is found, then the AP looks for the shortest path to the RVS_0 that satisfy the conditions

$$d(AP_i, RVS_i) + d(RVS_i, RVS_0)\text{X} \leq D_{max}$$

(Equation 6.10)

and

$$Data\_Delivery\_Cost \leq Thresh\_data$$

(Equation 6.11)

If this condition is true then the data delivery to the new AP from the RVS_0will start, otherwise, the AP will search another shortest path that satisfies the previous condition.

An illustrative algorithm is found below:

Algorithm 3 : QoS-Aware Mobility Algorithm

1: if (MN enters a new domain) **then**
2: Calculate the Reg_Update_Cost to the RVS_i
3: Send a registration request containing the RVS_i IP address and the registration cost between the RVS_i and the RVS_0
4: **if** $Data\_Delivery\_Cost \leq Thresh_{Reg}$ **then**
5: Perform RVS_0 registration
6: **end if**
7: New AP checks the existence of the current RVS_0 IP address in its routing table
8: **if** (the address exists) **then**
9: New AP finds shortest path to the RVS_0
10: Calculate the $Data\_Delivery\_Cost$ to the RVS_0
11: **if** $d(AP_i, RVS_i) + d(RVS_i, RVS_0)\text{X} \leq D_{max}$ and $Data\_Delivery\_Cost \leq Thresh\_data$ **then**
12: Select this path as the path of Data Delivery
13: Perform the Data Delivery Procedure
14: **end if**
15: **else**
16: Search a path with lower Cost
17: **end if**
18: end if

6.3 Performance Evaluation and Results

We conducted extensive simulations to evaluate the performance of our algorithm using OPNET Tool (OPNET, 2013). In this set of experiments, we studied the performance of our proposed algorithm in terms of packet loss rate, latency and data delivery cost for the network. In our simulations, a MN has a VoIP connection when handing over from on ASN to another. We compared our algorithm with two other algorithms: Dynamic Hierarchical (DH) (YANG, et al., 2007) and Optimized Hierarchical (OH) method for finding RRU_Cost (MISRA, et al., 2006).

Figure 6.1 shows the average packet loss rate during the session as a function of number of hops for all algorithms. We remark that our proposed algorithm reduces the packet loss during a session compared to other algorithms. This is due to the cost based algorithm which tries to optimize the resources in term of data and signaling messages. We also compared the median delivery probability for our algorithm which is 0.77, 0.7 for the dynamic hierarchical and 0.49 for the optimized hierarchical algorithm. This means that our algorithm, Dynamic hierarchical and Optimized Hierarchical algorithms often use links with loss rates of 22% or more, 31% or more, and 53% or more, respectively.

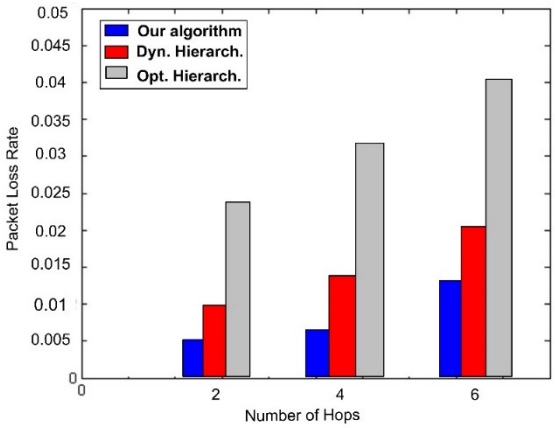


Figure 6.1: Packet Loss vs. Number of Hops

Figure 6.2 shows the results gained from handover latency measurements. One can observe that our proposed algorithm performs very well which proves that our proposal reduces the latency during the handover. This result comes from the fact that the policy by which we select the path optimizes the delay of transfer for messages especially when taking into account the minimization of the cost of data message regarding the total traffic.

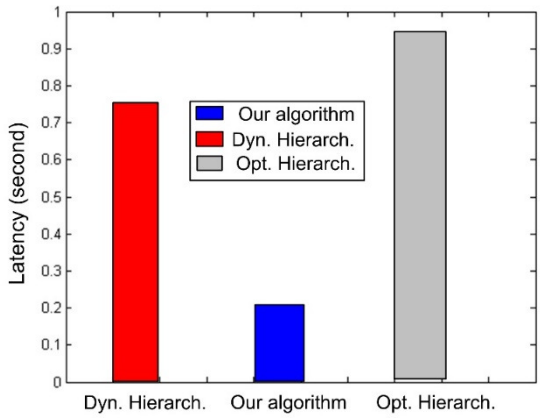


Figure 6.2: Handover Latency

We can also observe from that our approach always performs the best by offering a minimal RRU cost. This result is expected since the returned data delivery overhead and registration updates overhead are often minimal. The tradeoff between these two overheads is achieved through the objective function of our formulation.

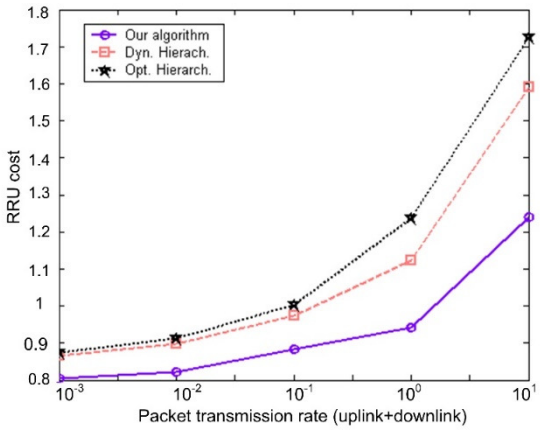


Figure 6.3: Radio Resource Utilization (RRU) cost vs. traffic

6.4 Chapter Summary

In this chapter, a sample mesh network case that is suitable for our proposed architecture of eHIP is taken into consideration. Also, a path selection algorithm is proposed that is compatible with this architecture. This algorithm consider the QoS constraints in terms of delay and packet loss for their ongoing VoIP session. The proposed algorithm has been compared with similar hierarchical path selection algorithms. Based on our simulations, the proposed scheme proved significant gains in terms of radio resource utilization cost.

7 HIP Testbed and Implementation

The objective of this part of our study (ARREZ, et al., 2011) 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.

7.1 Testbed

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 7.1 illustrates the distribution of the different elements of the test-bench while the technical specifications of each element of the test-bench are listed in Table 7.1.

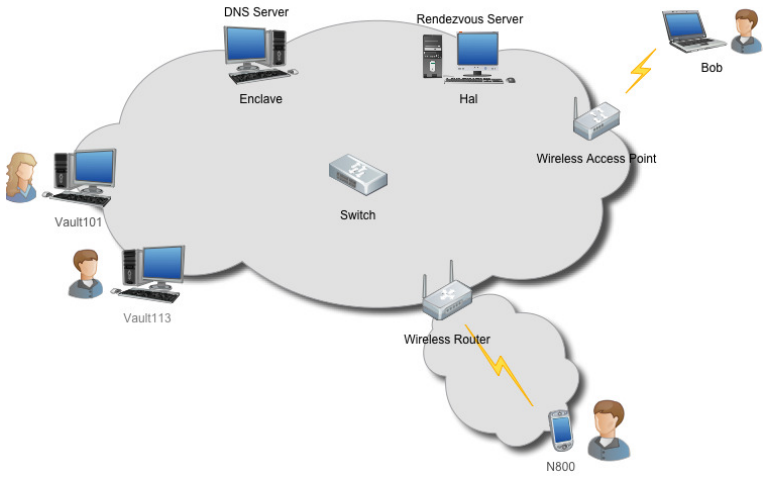


Figure 7.1: HIP Test bench

Table 7.1: Devices used in the HIP Testbed

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

7.2 Parameters and Scenarios

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 (INFRAHIP, 2013). 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, the openHIP project as an open source project from the IETF and the IRTF, and a freeBSD implementation from the Ericsson Nomadic Labs in Finland. 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.

7.3 Results

7.3.1 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 Figure 7.2 and Figure 7.3. The test focused on verifying the correct flow of the I1, R1, I2 and R2 messages involved in the process.

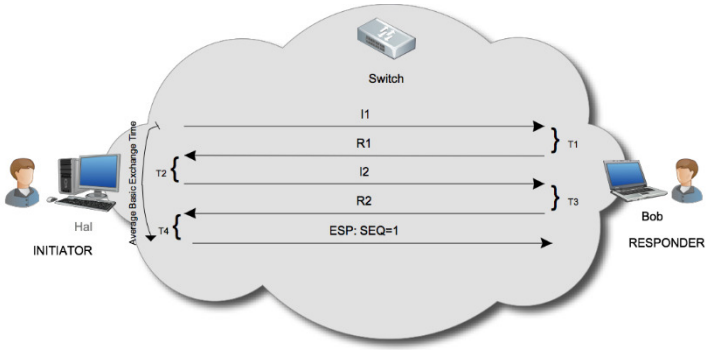


Figure 7.2: HIP Basic Exchange Test Scenario 1 (Laptop connected through Ethernet)

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.

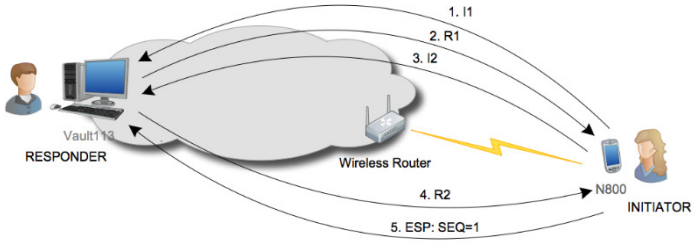


Figure 7.3: HIP Basic Exchange Test Scenario 2 (N800 connected through WiFi 802.11g)

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.

Figure 7.4 and Figure 7.5 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 (NIKANDER, et al., 2008b). 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.

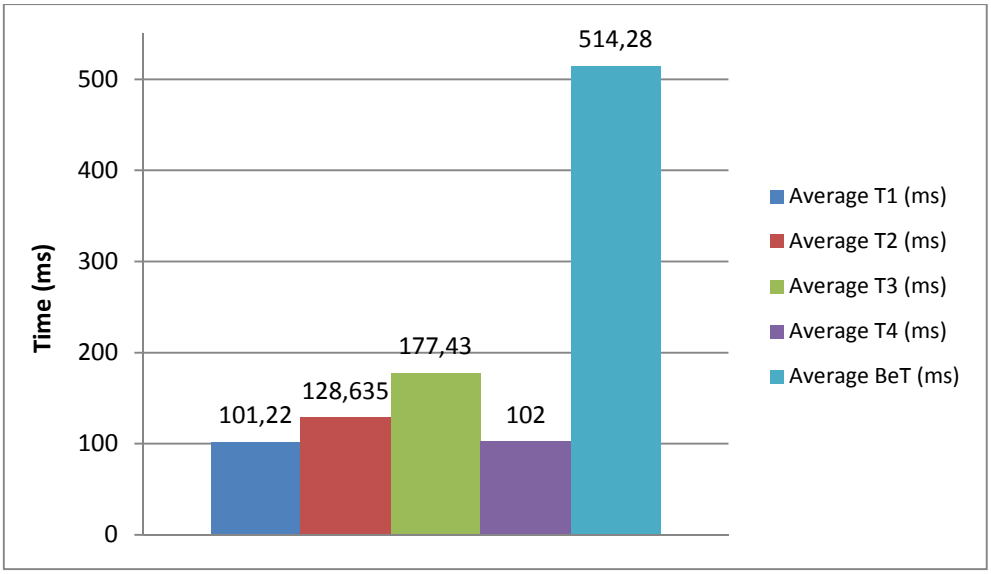


Figure 7.4: Average Times for HIP Basic Exchange (Scenario 1)

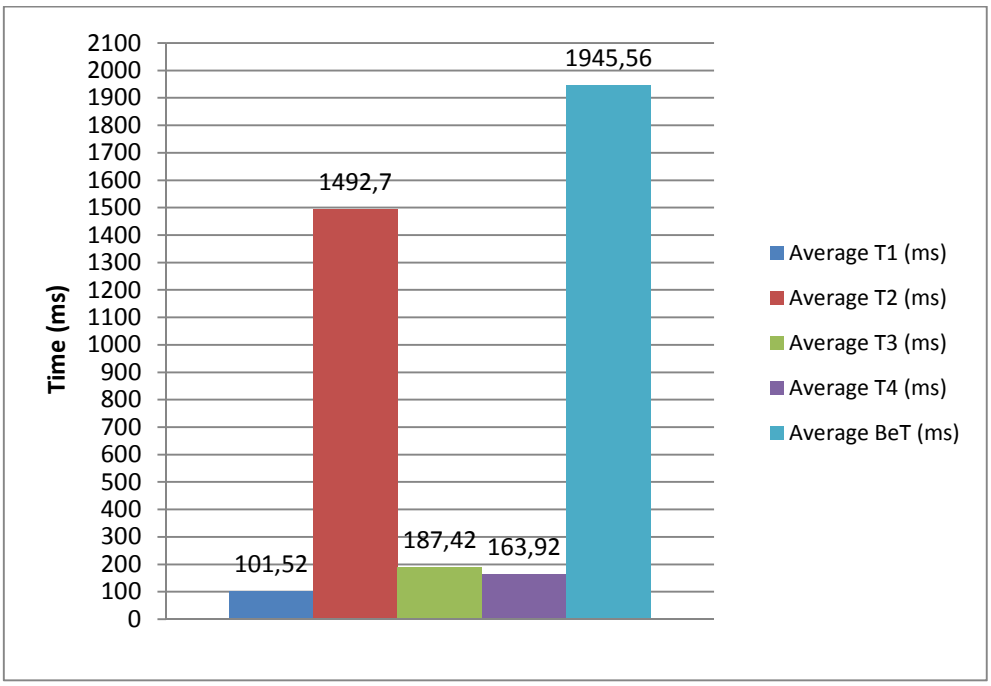
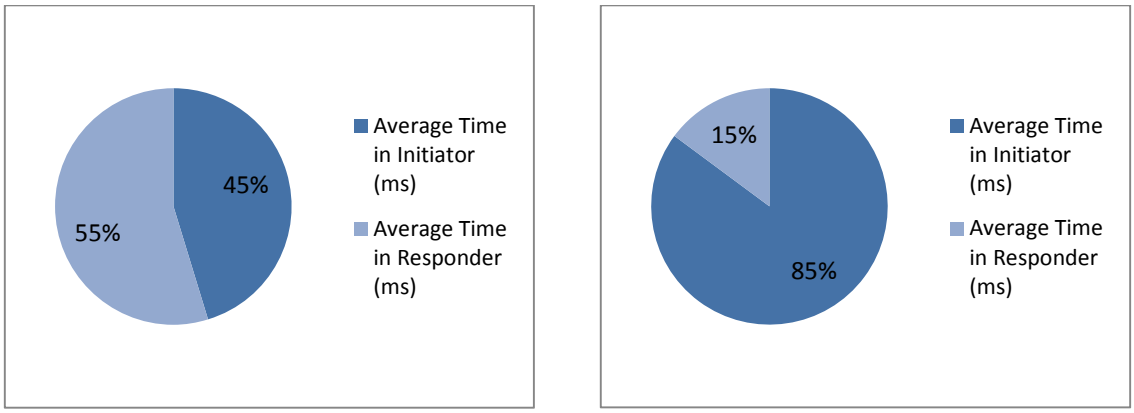


Figure 7.5: Average Times for HIP Basic Exchange (Scenario 2)

As it can be seen from Figure 7.6 the average percentage of time consumed during a basic exchange registration depends mostly on the hardware capabilities of the nodes. In the test case scenario 1, although the largest metric should be T2 (processing time of the cryptographic challenge), the responder node HAL took most of the consumed time (55% vs 45%) mainly due to the difference in the processors between nodes and the noticeable difference in RAM between the nodes. Meanwhile, the initiator node took most of the processing time (85%) during the exchange registration for the same reasons as explained before.



(a) (b)

Figure 7.6: Average percentages of time consumption of Initiator and Responder during HIP Basic Exchange Registration Test Scenario 1 (a) and Test Scenario 2 (b)

7.3.2 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.

Figure 7.7 and Figure 7.8 illustrate the results obtained from the RTT estimates tests. The difference between the values for RTT of an ICMP message sent over regular IP encapsulation and RTT of an ICMP message sent over a secured ESP/HIP encapsulation in both test case scenarios are clear. The 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 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.

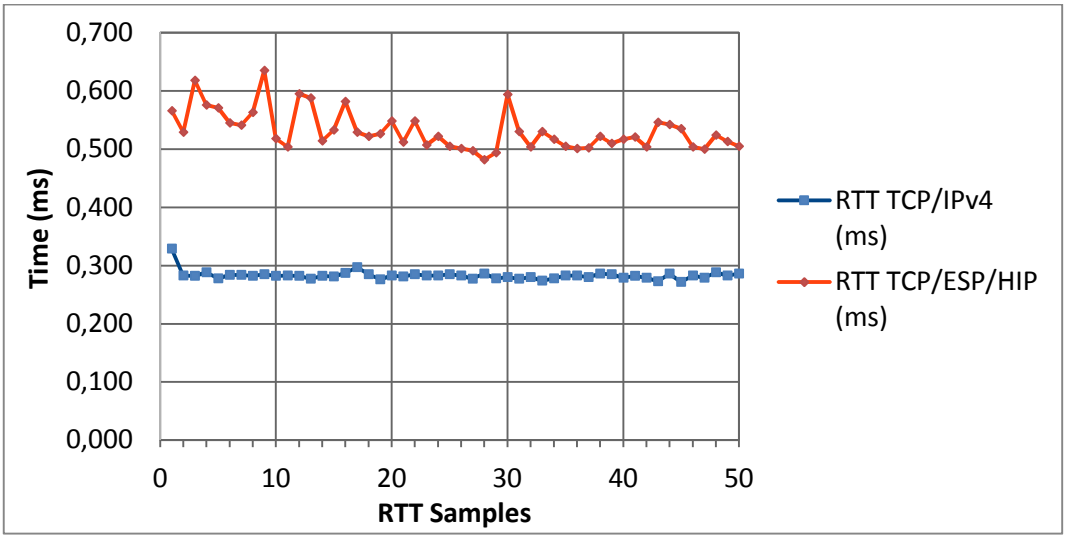


Figure 7.7: HIP round-trip (RTT) performed under Test Scenario 1

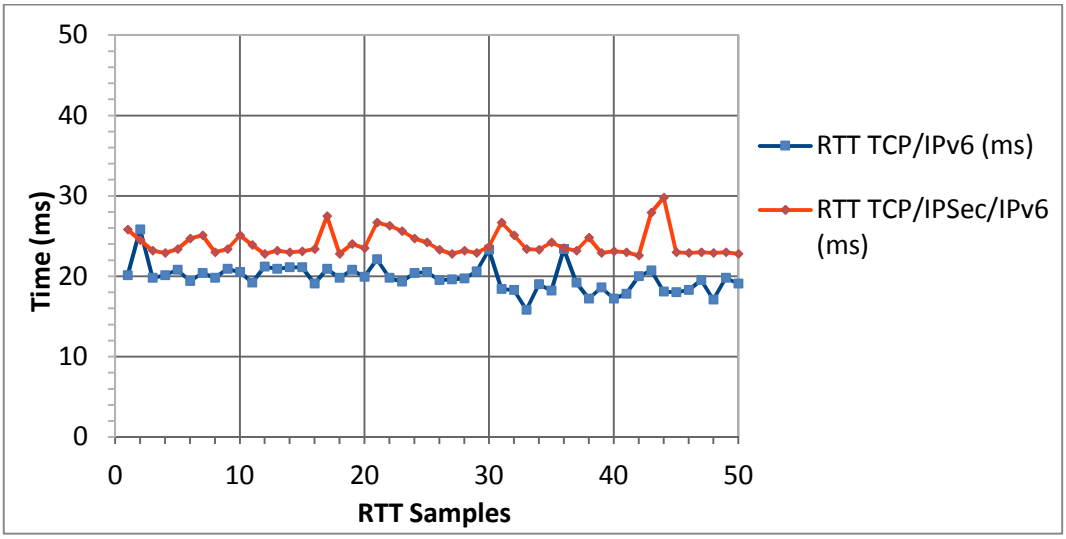


Figure 7.8: HIP round-trip (RTT) performed under Test Scenario 2

7.3.3 Throughput

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 (Figure 7.9 - Figure 7.12) 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 corresponds 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.

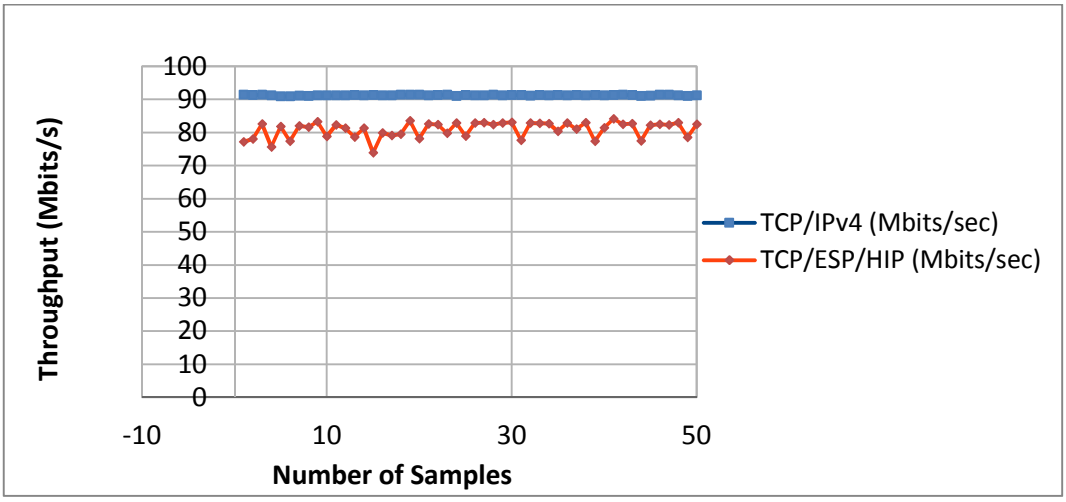


Figure 7.9: HIP-TCP Throughput Test Scenario 1 (Fixed Node)

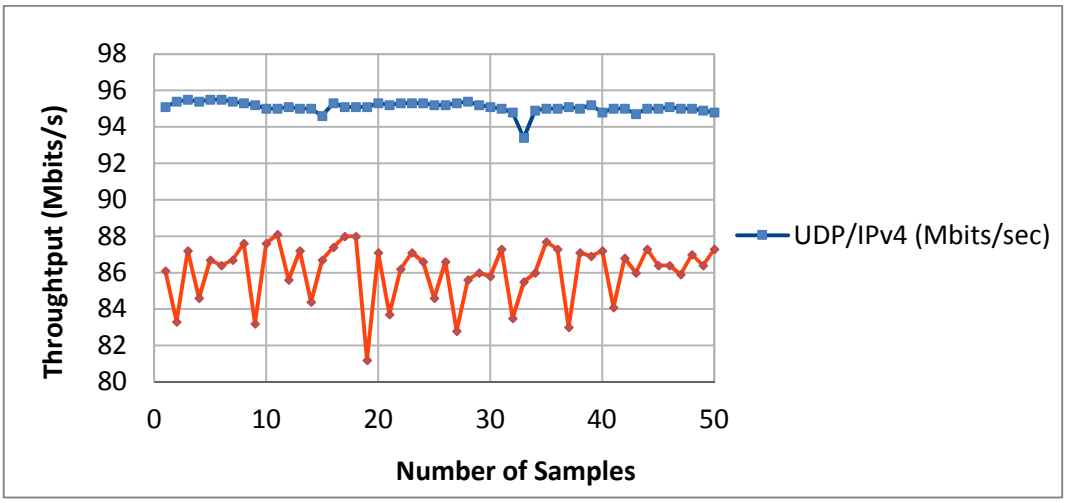


Figure 7.10: HIP-UDP Throughput Test Scenario 1 (Fixed Node)

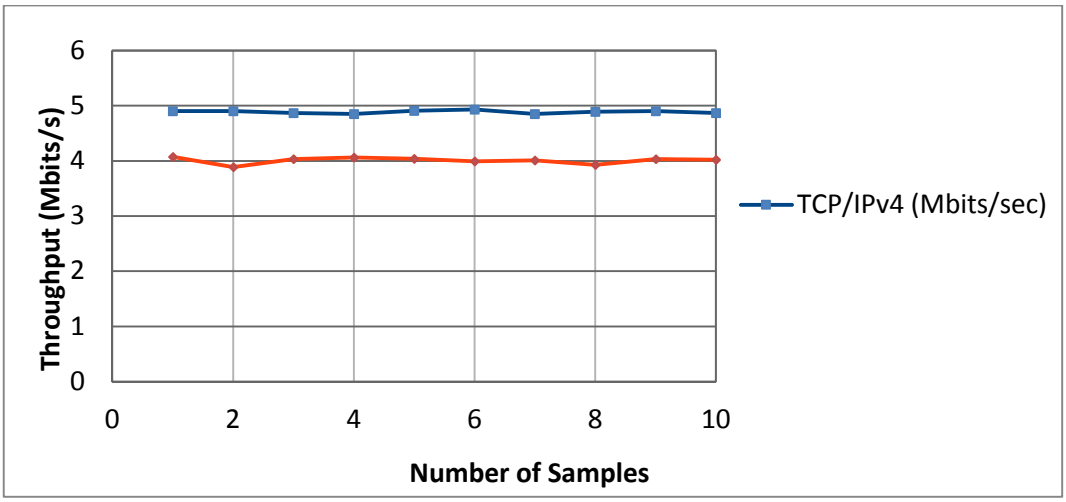


Figure 7.11: HIP TCP Throughput Test Scenario 2 (N800 connected through WiFi 802.11g)

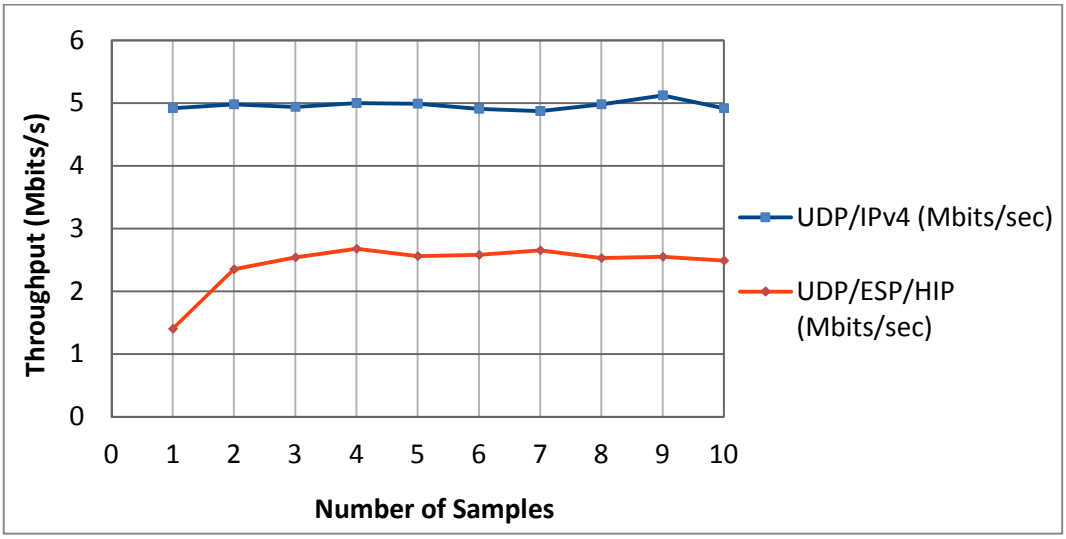


Figure 7.12: HIP UDP Throughput Test Scenario 2 (N800 connected through WiFi 802.11g)

7.3.4 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 (NIKANDER, et al., 2008b) . 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 Figure 7.13 and Figure 7.14 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.

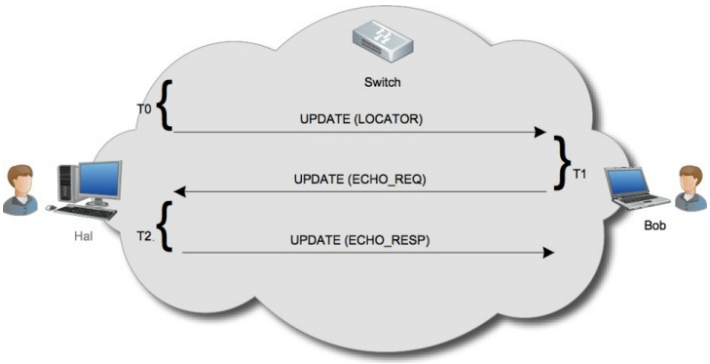


Figure 7.13: HIP Mobility Event Test Scenario 1

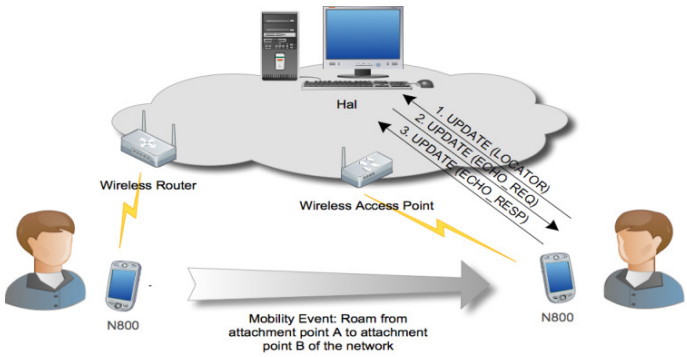


Figure 7.14: HIP Mobility Event Test Scenario 2

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 5206, 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.

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 and the mobility and multihoming extensions defined in (NIKANDER, 2008a). Figure 7.15 and Figure 7.16 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.

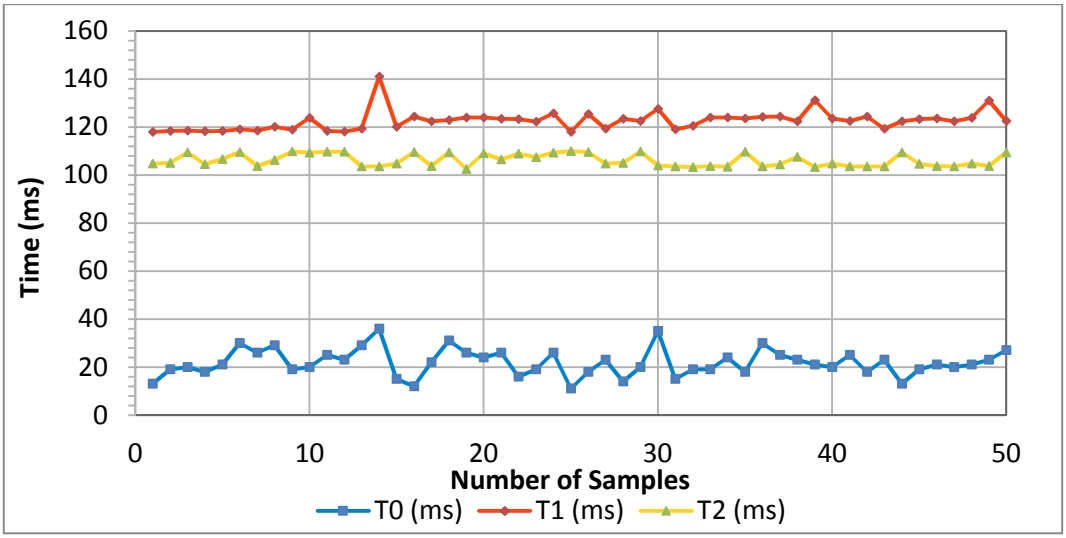


Figure 7.15: HIP Time results for Mobility Event Test Scenario 1

Figure 7.15 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.

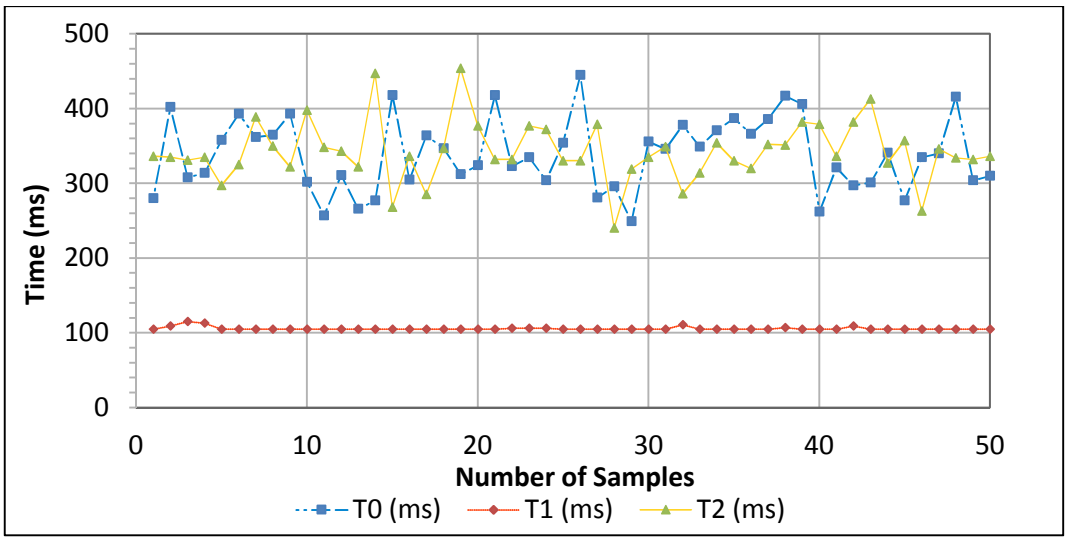
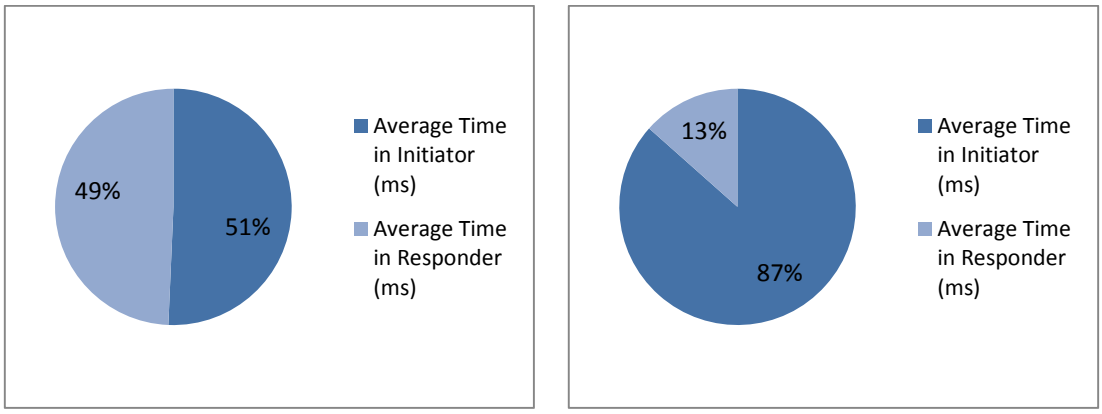


Figure 7.16: HIP Time results for Mobility Event Test Scenario 2

Figure 7.17 also show graphical results and percentages results of average time consumption for scenario 1 and scenario 2 respectively.



(a) (b)

Figure 7.17: Average percentages of time consumption of Initiator and Responder during a HIP Mobility Events for Test Scenario 1 (a) and Test Scenario 2 (b)

7.4 Chapter Summary

In this chapter, we reviewed 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 and provided us very valuable reference data for our both simulation analyses and theoretical analysis.

8 Conclusions

The new and pervasive evolution of heterogeneous networks in recent years reveals challenging issues regarding to session continuity and mobility. One of the emerging approaches relying on this challenge is the mobile host locator/identifier split idea. Especially, tremendous evolution of mobile and wireless networks, ubiquitous connectivity for hosts spread widely. Frequent user mobility context yields application layer and IP layer suffering. Mobility management suffered from location updates that have always been a focused challenge. IP addresses have dual role on legacy Internet architecture both as locators and host identifiers. The main aim of locator/identifier split idea as separating these roles to provide seamless communication sessions. In this approach, sessions are established by new host identifiers whereas network layer sessions still bound to IP addresses. This approach prohibits suffering of application layer sessions from frequent IP address changes. There are many prominent protocols and architecture proposals about this paradigm.

The main objective of this thesis is to concentrate on mobility management issues for Host Identity Protocol (HIP). HIP is a comprehensive protocol design by IETF and IRTF and take the lead for host locator/identifier split wave. While HIP has a mobility management procedure defined in its protocol design, it primarily focuses on macro mobility issues, not considering much on micro mobility challenges. The main focus of this thesis is to design and evaluate a novel micro mobility mechanism for HIP based on early update idea and called as early update for HIP (eHIP).

8.1 Contributions

Since handoff management is a challenging issue while the heterogeneity increase in network environments, we focused on enhancing the handoff behaviors of HIP. eHIP is based on the idea of anticipating a mobile node's next point of attachment inside the network during its real time mobility. From this context it differs from all former proposals related to HIP in terms of handoff management contributions. eHIP is the first method that embraced the idea of early update.

To be more precise and compare eHIP to other former proposals, the proposed combination of hierarchical architecture and early handoff decision process come to forefront. eHIP propose a network architectu re that is inheriting hierarchical deployment of rendezvous servers. Some proposals (mHIP) introduce new network elements that can intercept packets during handoffs or gateways which act like new root elements for routers. These gateways requires to be registered to themselves like RVS of traditional HIP. In eHIP, all hierarchical RVS elements (RVS_i) can act like a RVS and perform all of their roles. Also, eHIP does not bring any structural changes to BE (Base Exchange) procedure.

eHIP network architecture is similar to DH-HIP rather than other proposals that employs hierarchical approach. DH-HIP also divides the whole network into subdomains of which are managed by local RVS. But, eHIP does not change size of its administrative domains dynamically. Optimization of RVS_i domain size is a tractable problem for eHIP in terms of scalability. One of the important differences of eHIP from other hierarchical based proposals is registering to all RVS proactively for all visited subdomains. This registration occurs in passive or active mode.

Main contribution of this thesis is about handoff procedure for HIP. The idea of updating the new location of a MN is primarily feeds from FMIPv6's fast handoff and anticipation methods. In FMIPv6, handoff initiation is triggered by L2 triggers and these triggers are also used for anticipated handoff. In FMIPv6, MN sends a solicitation type messages to its old access router and informs it about its movement and location. In eHIP, we assume that MN learns about new RVS_2 and new AP address configurations from advertisement messages to implement eHIP procedures. Proactive registration to all RVS complements our proposal to avoid update and registration delays. MN is able to send first EU message to its current RVS2 and starts the early update procedure for new candidate RVS_2 which MN is registered in passive mode. Recipient of router advertisement messages trigger MN to send EU message. By receiving one of the periodically broadcasted RAs and realizing that it is broadcasted from a different AP from currently connected one, MN's handoff function decides to start L3 handoff procedures. EHIP primarily aims to end L3 handoff just after and as soon as L2 handoff completes and leaving the intersecting coverage area of two neighbor APs in order to minimize handoff delay. Note that eHIP sends it last message FU after completion of L2 HO, meanly after physical AP migration.

We also proposed two other improvements on eHIP. First one is a simple prediction idea based (p-eHIP) MN's capability of knowing its topological location and make prediction based decision for EU. The second one depends on the idea of using sensor nodes in network deployments for improving movement detect. Both of these improvements aims to improve movement detection phase of L3 handoffs to gain from handoff latency.

eHIP was analyzed by extensive OMNET++ simulation and compared with traditional HIP and Hierarchical HIP scenarios in order to interpret the effects of hierarchy on handoff in terms of latency. eHIP also reduce message overhead of HIP messages for MN and CN since active roles off lowest level RVS_2 in eHIP subdomains. eHIP outpace HIP and Hierarchical HIP in terms of exchange of HIP messages between RVS and mobile nodes. The message and processing overhead on only and main RVS of HIP is shared among other lower level RVS_i in the network. In the sense of handoff time, eHIP outstands its performance by significantly reducing update delay of HIP and hierarchical HIP. This reduction clearly depends on eHIP's proactive operations that starts in

parallel and even before L2 handoff. MN does not wait need to wait for completion of L2 handoff start location update procedures with new RVS_2.

Regarding to prediction extension based on MN's path characteristics, we obtained some numerical results on sample topologies as a basis for location based handoff improvement idea. An average of up to 60%-80% enhancement on EU time has been obtained from our sample topologies. Correct and false handoff decisions are also examined.

In our proposed sensor assisted extension for eHIP, the network was deployed with sensor nodes for estimating the mobile node's location. The mobile devices, which equipped by sensor reading capability, has an extra feature of periodic sensing and sending updates to NLS to obtain a next PoA estimation for handoff decision. This kind of extension proved us that in a heterogeneous environment, it is possible to benefice from network environment for L3 handoff decision following the L2 handoff. As a further option, this approach can also be used for L2 handoff decision and triggering in order to obtain energy saving. Energy saving is one of the most critical issues on future wireless networks which the domination of small and power constrained devices are getting bigger.

We also proposed an algorithm in order to minimize radio resource utilization (RRU) for our network architecture while considering MNs' quality of service needs and real time application delays. A system model to meet these requirements has been designed. This simple algorithm takes into account the mobility of MNs with respect to their QoS constraints. Our approach considers the QoS constraints in terms of delay and packet loss for their ongoing VoIP session. Based on our simulations, the proposed scheme proved significant gains in terms of RRU cost.

With our testbed implementation and experiments, it had been possible to review the basic architecture of HIP 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 testbed was assembled and configured using one of the best implementations of HIP currently available, the HIPL implementation from the infraHIP project. 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.

8.2 Future Directions

Although we focused on handoff management issues on HIP, there are still challenging issues regarding HIP and all other protocols and architectures which are embracing locator/identifier split idea. With the huge evolvements of Internet of Things wave and all heterogeneous networks, this idea will continue to grow. Some future directions for further studies based on this thesis may be:

- Enhancing eHIP by extra multi-homing features and studying on varieties of multi-homing scenarios.

- Scalability problem of RVS_i domains in the network hierarchy to prevent the network from unnecessary processing overhead due to frequent message exchanges among RVS and mobile nodes, meanly adjusting size and number of subdomains in the network.
- A new version of sensor assisted improvement by using dynamic sensor deployment instead of static deployment. The case of which reference points for location estimation in the network may be changing their locations during time.

9 Résumé de la thèse en français

En raison de la complexité des environnements sans fil, il est difficile de fournir une qualité de service efficace et une continuité de service surtout avec un réseau à commutation par paquet comme le réseau IP. En effet, de fournir à tout moment et n'importe où la connectivité pour les utilisateurs mobiles est une nécessité de plus en plus courante dans l'Internet. En outre, des environnements hétérogènes qui rassemblent jusqu'à plusieurs technologies d'accès radio comme le WiFi, GSM, GPRS, WiMax et plus récemment le LTE (Long Term Evolution), révèle plusieurs questions telles que la mobilité, le multi homing, la sécurité, la qualité de service (QoS) et un transfert transparent (Handover). Sous l'influence de toutes ces avancées des technologies de communication, les utilisateurs exigent également la connectivité partout et à tout moment pour différents types d'applications sans souffrir de l'hétérogénéité des environnements sous-jacents.

L'un des défis les plus attrayants des réseaux de prochaine génération a été le développement des techniques de gestion de la mobilité. Dans l'architecture traditionnelle TCP/IP, un hôte est identifié par les adresses IP qui en même temps définissent leurs localisations dans le réseau. Avec la prolifération des appareils mobiles connectés IP qui changent leurs adresses IP en raison des déplacements entre les différents réseaux, le besoin de maintien de la session au niveau applicatif est indispensable De plus, il est nécessaire de garantir une identification sécurisée des nœuds mobiles pour éviter toute usurpation d'identité lors des procédures d'enregistrements utilisées en mobilité. La gestion de la mobilité réseau implique deux processus qui sont le handover (transfert) et la gestion de l'attachement au réseau (Location). La gestion de l'emplacement définit les procédures de la mise à jour par le nœud mobile des éléments du système, tandis que la gestion de handover définit l'ensemble des opérations liées au déplacement entre deux points d'accès dans un réseau, même pendant des communications actives. Des solutions de gestion de transfert (handover) essayent de synchroniser autant que possible le handover au niveau de la couche et de

la couche réseau. L'objectif principal des techniques de gestion de la mobilité est tout simplement de fournir une connectivité transparente tout en se déplaçant à travers différents points d'accès. En plus de la gestion de transfert intercellulaire et l'identification des hôtes sont strictement liées, d'ailleurs toutes les solutions actuelles de transfert intercellulaire sont affectés par la méthode d'identification de nœud mobile dans l'architecture TCP / IP en cours (TUNCER, et al., 2012). La gestion de la mobilité peut également être classée de façon hiérarchique comme macro-mobilité et micro-mobilité. La macro mobilité se réfère au mouvement à travers différents domaines de réseaux administratifs, alors que la micro mobilité est liée au mouvement entre les différents points d'accès dans les mêmes domaines administratifs réseau (ZEKRI, et al., 2012).

Mobile IP est le protocole de la standardisation IETF pour gérer la mobilité IP. Alors que certains d'entre eux peuvent être classés comme des solutions de mobilité basées sur le nœud tel que Hierarchical Mobile IP (HMIPv6) et Fast Mobile IP (FMIPv6), certains d'entre eux peuvent être classés comme des solutions basées sur le réseau tel que Proxy Mobile IP (PMIPv6) et Network based Mobility (NEMO). Cependant, tous les protocoles basés sur IP mobile utilisent encore des adresses IP pour identifier les nœuds mobiles et essayer d'améliorer les capacités de mobilité dans tous les réseaux IP.

Basé sur les défis actuels d'amélioration de la gestion de mobilité, le besoin d'un nouveau cadre de support de la mobilité est avéré où le support du côté du nœud est du réseau est encouragé pour atteindre de bonnes performances (KAFLE & INOUE, 2010).

L'émergence de la connectivité ubiquitaire à travers le paradigme de l'Internet des objets (IoT : Internet of Things) fait également ressortir la nécessité de l'identification des nœuds à travers l'Internet à l'échelle mondiale et la réalisation réussie des opérations de localisation. L'idée de séparation du Locator / identifiant a attiré l'attention en particulier pour l'IoT. Rappelons que dans l'architecture de l'Internet d'aujourd'hui, deux espaces de noms sont utilisés: Domain Name Service (DNS) et les adresses IP. Ces deux espaces de noms jouent un rôle important pour les technologies basées sur Internet depuis des années. Adresses IP ont deux principales fonctionnalités de l'hôte. Ils sont utilisés à la fois comme localisateurs et les identifiants d'un nœud dans le réseau.

Récemment, les groupes de travail de l'IETF (IETF, 2013) et l'IRTF (IRTF, 2013) ont conduisent de profondes discussions sur la séparation du localisateur et identifiant séparation idée. Ils proposent essentiellement d'utiliser deux espaces de noms différents comme des identificateurs des nœuds terminaux (host identité) et localisateurs de routage (adresse IP). Outre les principaux avantages mentionnés précédemment, d'autres avantages comme la réduction de la taille des tables

de routage dans le réseau de base et l'amélioration des fonctionnalités d'ingénierie de trafic sont attendus.

Les solutions les plus développées aujourd'hui dans cette approche sont Host Identity Protocol (HIP) (MOSKOWITZ, et al., 2008) et Locator Indetifier Seperation Protocol (LISP) (FARINACCI, et al., 2013) de deux points de vue différents. Le protocole HIP est concentré sur l'hôte càd terminal d'accès au réseau et le support de bout en bout de la mobilité sécurisée et le support du multi homing. LISP est concentré sur l'optimisation de nouvelles fonctionnalités sur le plan routage dans le réseau.

9.1 Les Objectives de la thèse

L'objectif principal de cette thèse est l'amélioration de la gestion de la mobilité en se basant sur l'approche de séparation du localisateur et de l'identifiant des nœuds et plus particulièrement l'approche Host Identity Protocol (HIP), qui est l'approche dominante et la plus complète dans ce sens. L'approche HIP permet un support naturel de la macro de mobilité, cependant souffre du support de la micro mobilité. Le transfert sans couture (smooth Handover) a toujours été une question difficile pour les réseaux IP et elle est d'autant plus difficile avec le développement de l'hétérogénéité à l'accès.

Dans le cadre de cette thèse, nous proposons d'étudier le problème de la mobilité micro mobilité sous HIP, et nous proposons une amélioration du mécanisme de Handover qui puisse satisfaire les exigences de qualité de service des nouds. Notre premier objectif est de concevoir une architecture de réseau appropriée qui adopte l'approche hiérarchique et utilise de nouvelles technique d'amélioration de la gestion du handover.

9.2 L'Organisation de la thèse

Cette thèse est organisée comme suit. Chapitre 2 présente l'état de l'art de paradigme localisateur / identifiant séparation et les protocoles connexes.

Dans le chapitre 3, une version hiérarchisée pour le protocole HIP et un nouveau mécanisme de gestion de transfert (Handover) ont été présentés sous l'appellation eHIP. Dans le chapitre 4, une extension de la prise en charge proactive du Handover a été représentée pour la méthode eHIP qui vise à déclencher le début de la mise à jour d'un nœud mobile dès que possible et avant sa déconnection au cours de sa mobilité. Chapitre 5 introduit également une nouvelle amélioration du protocole eHIP pour faire avancer la phase de détection de mouvement de eHIP par le

déploiement de nœuds de capteurs dans le réseau et en utilisant des techniques de positionnement et des algorithmes d'estimation emplacement . Dans les chapitres 6 et 7 une évaluation du protocole eHIP avec modèle de simulation et aussi des tests d'expérimentation est proposée pour mieux observer les comportements de HIP sur les environnements de réseau réels. Enfin le chapitre 8 conclut et résume nos contributions et souligne certaines orientations futures de notre travail.

9.3 Contributions

Comme la gestion de transfert (Handover) est une des questions difficiles alors que l'augmentation de l'hétérogénéité dans les environnements réseau est inévitable, nous nous sommes concentrés sur l'amélioration des comportements de transfert intercellulaire de l'approche HIP. eHIP est basé sur l'idée d'anticiper le prochain point d'accès d'un nœud mobile à l'intérieur du réseau lors de sa mobilité en temps réel. De ce contexte, il se distingue des propositions relatives à HIP en termes de contributions de gestion de transfert ; eHIP est la première méthode qui a embrassé l'idée de la mise à jour proactive. eHIP propose une architecture de réseau qui hérite du déploiement hiérarchique de serveurs de rendez-vous (RVS) introduisent dans l'approche HIP pour gérer l'enregistrement de l'identificateur HIP. Certaines propositions comme (mHIP) introduisent de nouveaux éléments de réseau qui peuvent intercepter des paquets pendant des transferts (Handover) ou des passerelles qui agissent comme de nouveaux éléments pour les routeurs. Ces passerelles nécessite d'être enregistré en tant que RVS de HIP traditionnelle. Dans notre solution eHIP, tous les éléments de RVS hiérarchiques (RVS_i) peuvent agir comme un RVS et s'acquitter de toutes leurs fonctions. Aussi, eHIP n'apporte pas de modifications structurelles à la procédure de base HIP.

L'architecture eHIP est similaire à DH-HIP dans l'approche hiérarchique. DH-HIP divise aussi l'ensemble du réseau en sous-domaines qui sont gérés par des RVS locaux. Mais, eHIP ne change pas la taille de ses domaines administratifs (réseaux) dynamiquement comme DH-HIP. L'optimisation des RVS_i ainsi que la détermination de la taille des domaines est un problème d'optimisation de l'architecture. Une des différences importantes d'eHIP avec les autres propositions de base est l'enregistrement hiérarchique de tous les RVS de manière proactive pour tous les sous-domaines visités (r réseaux visités lors de la mobilité du nœud). Cet enregistrement se produit en mode passif ou actif.

La principale contribution de cette thèse est bien l'amélioration de la procédure de transfert de HIP. L'idée de mettre à jour le nouvel emplacement d'un nœud mobile (MN) est nourrit principalement de transfert intercellulaire rapide et d'anticipation des méthodes de FMIPv6. Dans

FMIPv6, l'initiation du transfert est déclenchée par le niveau 2 (L2 based triggers) et ces déclencheurs sont également utilisés pour le handover. En FMIPv6, le nœud mobile MN envoie un message de type sollicitation à son ancien routeur d'accès et l'informe de son mouvement et son emplacement. Dans notre solution eHIP, nous supposons que le nœud mobile MN apprend la présence du nouveau RVS_2 et récupère les nouvelles configurations d'adresses des points d'accès sur son chemin (AP) à travers les messages (Router Advertisement : AR) pour mettre en œuvre les procédures d'enregistrement de la nouvelle adresse avec eHIP. L'enregistrement proactive à tous les RVS complète notre proposition pour éviter la mise à jour et inscription retardés qui justement impacte le délai de reconnexion après handover. Le nœud mobile MN est capable d'envoyer le premier message de mise à jour à son RVS_2 en cours et démarrer la procédure de mise à jour au début d'une nouvelle RVS_2 candidat avec qui le nœud mobile MN est inscrit en mode passif. En recevant l'un des messages d'annonce de routeur AR diffusés périodiquement par les point d'accès visitées, le nœud mobile se rend compte qu'il est diffusé à partir d'un autre AP que celui auquel il est actuellement connecté, ainsi la fonction de transfert (handover) du MN décide de commencer les procédures de transfert intercellulaire de niveau 3 (L3 handover). eHIP vise principalement à démarrer dès que possible le handover de niveau 3 (L3 handover), juste après le handover de niveau 2 (L2 handover) et ce juste avant de quitter la zone la zone de couverture d'intersection de deux points d'accès voisin afin de minimiser les délais de transfert. Notez qu'eHIP envoie le dernier message de mise à jour de son emplacement juste après l'achèvement du handover de niveau 2 (L2 HO).

Deux autres améliorations au protocole eHIP ont été aussi présentées dans cette thèse. La première est une idée simple d'anticipation du déclenchement du handover avec la capacité du nœud mobile MN de connaître son emplacement topologique. La seconde dépend de l'idée d'utiliser des nœuds de capteurs dans les déploiements de réseaux pour améliorer la détection de la localisation du nœud mobile MN et d'aider à l'anticipation du déclenchement du Handover. Ces deux propositions visent à améliorer la phase de détection de mouvement du handover de niveau 3et ainsi diminuer la latence liée au handover.

eHIP a été analysé par simulation avec OMNET + +, il a été comparé au protocole de base HIP et HIP hiérarchiques pour interpréter les effets de la hiérarchie sur un transfert en termes de temps de latence. On montre que eHIP permet de réduire également le volume de messages d'enregistrement comparé à HIP pour le nœud mobile MN et le nœud correspondant CN. Concernant le temps du handover, eHIP montre de très bonnes performances en réduisant de manière significative la mise à jour HIP et HIP et hiérarchique. Cette réduction dépend clairement des opérations proactives de l'eHIP qui commence en parallèle et même avant L2 handover. Le

MN n'attend pas la fin de L2 handover pour démarrer les procédures de mise à jour avec le nouveau rendez-vous server responsable du nouveau point d'accès RVS_2.

En ce qui concerne la prolongation de la prédiction basée sur les caractéristiques du trajet du nœud mobile MN, nous avons obtenu quelques résultats numériques sur certaines topologies de base et pour l'amélioration de la localisation pour mieux anticiper le déclenchement du handover.

Dans notre capteur prolongation assistée proposé pour eHIP, le réseau a été déployé avec des nœuds de capteurs pour estimer l'emplacement du nœud mobile. Les appareils mobiles, qui équipés de capacité de lecture du capteur, a une fonction supplémentaire de détection périodique et l'envoi de mises à jour de NLS pour obtenir une prochaine estimation du PoA pour la prise de transfert. Ce type d'extension nous a montré que dans un environnement hétérogène, il est possible de bénéfice de l'environnement de réseau pour L3 décision de transfert intercellulaire après le transfert L2. Comme option supplémentaire, cette approche peut également être utilisée pour L2 décision de transfert intercellulaire et de déclenchement en vue d'obtenir des économies d'énergie. L'économie d'énergie est l'un des problèmes les plus critiques sur les réseaux sans fil de demain qui la domination des petites et puissance dispositifs contraintes sont de plus.

Nous avons également proposé un algorithme afin d'optimiser l'utilisation des ressources radio (RRU) pour notre architecture réseau tout en tenant compte de la qualité des besoins en services et les délais d'application en temps réel de MN. Un modèle de système pour répondre à ces exigences a été conçu. Ce simple algorithme prend en compte la mobilité des MN par rapport à leurs contraintes de QoS. Notre approche considère les contraintes de QoS en termes de délai et de perte de paquets pour leur session de VoIP en cours. Sur la base de nos simulations, le schéma proposé prouve bien le gain significatif en termes de coût RRU.

Enfin, grâce à notre mise en œuvre et expériences , il a été possible de revoir l'architecture de base de HIP et parvenir à une compréhension profonde et la compréhension des caractéristiques et des avantages prévus pour résoudre le paradigme actuel de l'emplacement , de l'identité et de la sécurité sur les communications d'un nœud mobile. Une plateforme a été mise en place et configuré avec l'une des meilleures implémentations de HIP actuellement disponibles, la mise en œuvre de HIPL du projet de infraHIP. Les tests effectués pour vérifier et valider les fonctionnalités et les caractéristiques principales du protocole telles que le processus d'échange de base, les temps d'aller-retour pour un message de HIP, le débit moyen et du processus en charge de la mise à jour du paramètre LOCATOR utilisé par nœuds mobiles pour mettre à jour l'information de leur attachement au réseau.

9.4 Orientations futures

Bien que nous nous sommes concentrés sur les questions de gestion de transfert dans HIP, il ya encore des questions difficiles concernant HIP et tous les autres protocoles et l'architecture qui adoptent l'approche de séparation localisateur / identifiant. Certaines orientations futures pour d'autres études fondées sur cette thèse peuvent être:

• Améliorer eHIP par des caractéristiques multi-homing supplémentaires et l'étude sur les variétés de scénarios multi-homing.

• problème de l'évolutivité des domaines RVS_i dans la hiérarchie du réseau pour empêcher le réseau de charge de traitement inutile en raison de fréquents échanges des messages entre les RVS et les nœuds mobiles.

• un déploiement de réseau de capteurs dynamique et non statique comme c'est proposé dans notre approche pour aider à la localisation du nœud mobile et au déclenchement anticipé de son handover. Ceci pour embrasser un scénario réel avec des capteurs mobiles.

List of Publications

INTERNATIONAL JOURNALS

1. Leonardo ARRAEZ, Hakima CHAOUCHI, Zeynep GURKAS AYDIN, "Performance Evaluation and Experiments for Host Identity Protocol", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011

2. Zeynep GURKAS AYDIN, Hakima CHAOUCHI, A. Halim ZAIM, "A Survey On Micro Mobility Management Of Host Identity Protocol", Journal of Electrical & Electronics Engineering (IU – JEEE), Vol. 10(2), (2010), 1279-1285

INTERNATIONAL CONFERENCES

1. Zeynep GURKAS AYDIN, Hakima CHAOUCHI, A. Halim ZAIM, Tulin ATMACA, "Performance Evaluation of an Enhanced Handoff Mechanism for Host Identity Protocol", submitted to IEEE WCNC 2014

2. Zeynep GURKAS AYDIN, A. Halim ZAIM, Hakima CHAOUCHI, Tulin ATMACA, "A Prediction based Mobility Extension for eHIP Protocol", ISCIS 2011, London

3. Zeynep GURKAS AYDIN, A. Halim ZAIM, Hakima CHAOUCHI, Tulin ATMACA, "Extending Early Update For Host Identity Protocol With Movement Prediction", International Conference on Networking and Future Internet 2011, Paris, Extended Abstract

4. Zeynep GURKAS AYDIN, Tara Ali-YAHIYA, Hakima CHAOUCHI, A.Halim ZAIM, 'QoS Mobility-Aware Algorithm using Early Update for Host Identity Protocol', The 21st Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2010) ,İstanbul, Türkiye

5. Zeynep GURKAS AYDIN, Hakima CHAOUCHI, A.Halim ZAIM, "eHIP:Early Update for Host Identity Protocol", ACM Mobility Conference 2009, Nice, France

References

AKYILDIZ, I. F. et al., 1999. Mobility Management for Next Generation Wireless Systems. *Proceedings of IEEE,* August, 87(84), pp. 1347-1384.

AKYILDIZ, I., XIE, J. & MOHANTY, S., 2004. A Survey Of Mobility Management In Next-Generation All-IP-Based Wireless Systems. *IEEE Wireless Communications,* 11(4), pp. 16-28.

ARREZ, L., CHAOUCHI, H. & GURKAS AYDIN, Z., 2011. Performance Evaluation and Experiments for Host Identity Protocol. *International Journal of Computer Science Issues,* 8(2).

BAHETY, V. & PENDSE, R., 2004. *Scalable qos provisioning for mobile networks using wireless sensors.* 1528-1533, IEEE Wireless Communications and Networking Conference.

BOKOR, L., NOVACZKI, S. & IMRE, S., 2007. *A Complete HIP Based Framework For Secure Micromobility.* Jakarta, Indonesia, MoMM 2007, pp. 111-122.

BOKOR, L., NOVACZKI, S., TAMASL, L. & JENEY, G., 2009a. *Design and Evaluation of Host Identity Protocol (HIP) Simulation Framework for INET/OMNeT++.* Tenerife, Canary Islands, MSWIM 2009, pp. 124-133.

BOKOR, L., TAMAS, L., NOVACZKI, S. & JENEY, G., 2009b. *Protocol Design and Analysis of a HIP-based Per-Application Mobility Management Platform.* Tenerife, Canary Islands, MobiWAC 2009, pp. 7-16.

CAMPBELL, A. et al., 2002. Comparison of IP Micro-Mobility Protocols. *IEEE Wireless Communciation,* 9(1), pp. 72-82.

CHOI, N., KIM, J. & KOH, S., 2013. *Host Identifier and Local Locator for mobile oriented future internet: Implementation perspective.* PyeongChang, s.n., pp. 463-468.

FARINACCI, D., FULLER, V., MEYER, D. & LEWIS, D., 2013. *RFC 6830 : The Locator/ID Separation Protocol (LISP),* s.l.: s.n.

FULLER, V., FARINACCI, D., MEYER, D. & LEWIS, D., 2013. *RFC 6836 : Locator/ID Separation Protocol Alternative Logical Topology (LISP+ALT),* s.l.: s.n.

GURKAS AYDIN, Z., CHAOUCHI, H., YAHIYA, T. & ZAIM, H., 2010a. *QoS Mobility-Aware Algorithm using Early Update for Host Identity Protocol.* Istanbul, Turkey, IEEE PIMRC 2010.

GURKAS AYDIN, Z., CHAOUCHI, H. & ZAIM, H., 2009. *eHIP : Early Update for Host Identity Protocol.* Nice France, ACM Mobility Conference.

GURKAS AYDIN, Z., CHAOUCHI, H. & ZAIM, H., 2010b. A Survey On Micro Mobility Management Of Host Identity Protocol. *IU-Journal of Electrical & Electronical Engineering,* 10(2), pp. 1279-1285.

GURTOV, A., 2008. *Host Identity Protocol (HIP)-Towards the Secure Mobile Internet.* s.l.:Wiley Publications.

GURTOV, A., KOMU, M. & MOSKOWITZ, R., 2009. Host Identity Protocol: Indetifier/Locator Split for Host Mobility and Multihoming. *The Internet Protocol Journal,* 12(1), pp. 27-32.

HIPSIM++, 2013. *HIPSim++: A Host Identity Protocol (HIP) Simulation Framework for INET/OMNET++.* [Online]
Available at: http://www.ict-optimix.eu/index.php/HIPSim
[Accessed 2013].

HOBAYA, F., GAY, V. & ROBERT, E., 2009. *Host Identity Protocol Extension Supporting Simultaneous End-host Mobility.* Cannes, La Bocca, IWCMC 2009, pp. 261-266.

HON SO, J. & WANG, J., 2008. *Micro-HIP : A HIP-based Micro-Mobility Solution.* Beijing, Proceedings of ICC 2008, pp. 430-435.

HU, B., YUAN, T., HU, Z. & CHEN, S., 2010. *L-HIP : A Localized Mobility Management Extension for Host Identity Protocol.* Chengdu, WiCOM 2010, pp. 1-4.

IAPICHINO, G. & BONNET, C., 2009. *Host Identity Protocol and Proxy Mobile IPv6: A Secure Global and Localized Mobility Management Scheme for Multihomed Mobile Nodes.* Honolulu, GLOBECOM 2009.

IETF, 2013. *Internet Engineering Task Force.* [Online]
Available at: http://www.ietf.org/
[Accessed 2013].

INET, 2013. *The INET Framework for OMNeT++.* [Online]
Available at: http://www.omnetpp.org/doc/INET/neddoc/index.html
[Accessed 2013].

INFRAHIP, 2013. *Infrastructure for HIP Implementation.* [Online]
Available at: http://infrahip.hiit.fi
[Accessed 2013].

IRTF, 2013. *Internet Research Task Force.* [Online]
Available at: http://www.irtf.org
[Accessed 2013].

JOKELA, P. & MOSKOWITZ, R., 2008. *RFC 5202 : Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP),* s.l.: s.n.

JOKELA, P. et al., 2004. *Handover performance with HIP and MIPv6.* Mauritius, Wireless Communciations Systems 2004, pp. 324-328.

JUNG, H. & KOH, S., 2009. *Mobile Optimized Future Internet (MOFI):Architecture and Protocols,* s.l.: s.n.

KAFLE, V. & INOUE, M., 2010. Locator ID Seperation for Mobility Management in the New Generation Network. *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications,* 1(2/3), pp. 3-15.

KENT, S., 2005. *RFC 4303 : IP Encapsulating Security Payload (ESP),* s.l.: s.n.

KHURRI, A., VOROBYEVA, E. & GURTOV, A., 2007. *Performance of Host Identity Protocol on Lightweight Hardware.* New York, USA, ACM/IEEE MobiArch'207.

KIM, H. & KIM, Y., 2006. *An Early Binding Fast Handover for High-Speed Mobile Nodes on MIPv6 over Connectionless Packet Radio Link.* Las Vegas, NV, SNPD'06.

KOODLI, R., 2005. *RFC 4068 : Fast Handovers for Mobile IPv6,* s.l.: s.n.

LAGANIER, J. & EGGERT, L., 2008b. *RFC 5204 : Host Identity Protocol (HIP) Rendezvous Extension,* s.l.: s.n.

LAGANIER, J. & KOPONEN, T., 2008a. *RFC 5203 : Host Identity Protocol (HIP) Registration Extension,* s.l.: s.n.

LANGAR, R., NIZAR, B. & BOUTABAA, R., 2009. Mobility-Aware Clustering Algorithms with Interference Constraints in Wireless Mesh Networks. *Computer Networks,* 53(1), pp. 25-44.

MAINO, F. et al., 2011. *LISP-Security (LISP-SEC) (draft-maino-lisp-sec-00.txt),* s.l.: s.n.

MATLAB, 2013. *MATLAB: The Language of Technical Computing.* [Online]
Available at: http://matrhworks.com/products/matlab
[Accessed 2013].

MEYER, D., 2008. The Locator Identifier Separation Protocol (LISP). *The Internet Protocol Journal,* 11(1), pp. 23-36.

MISRA, I., CHAKRABORTY, M., SAHA, D. & MUKHERJEEE, A., 2006. *An Approach for Optimal Hierarchical Mobility Management Network Architecture.* Melbourne, Vic, VTC 2006, pp. 481-485.

MOSKOWITZ, R. & NIKANDER, P., 2006. *RFC 4423 : Host Identity Protocol (HIP) Architecture,* s.l.: s.n.

MOSKOWITZ, R., NIKANDER, P. & HENDERSON, T., 2008. *RFC 5201 : Host Identity Protocol,* s.l.: s.n.

MUSLAM, M., ANTHONY CHAN, H. & VENTURA, N., 2009. *HIP Based Micro-Mobility Management Optimization.* Cannes, La Bocca, IWCMC 2009, pp. 291-295.

NIKANDER, P., 2008a. *RFC 5205 : Host Identity Protocol (HIP) Domain Name System (DNS) Extension,* s.l.: s.n.

NIKANDER, P., HENDERSON, T., VOGT, C. & ARKKO, J., 2008b. *RFC 5206 : End-Host Mobility and Multihoming with the Host Identity Protocol,* s.l.: s.n.

NOVACZKI, S., BOKOR, L. & IMRE, S., 2006. *Micromobility Support in HIP: a survey and extension of host identity protocol.* Benalmadena (Malaga), Spain, IEEE MELECON, pp. 651-654.

NS-2, 2013. *The Network Simulator – ns-2.* [Online]
Available at: http://nsnam.isi.edu/nsnam/index.php/Main_Page
[Accessed 2013].

OMNET++, 2013. *OMNeT++: Network Simulation Platform.* [Online]
Available at: http://omnetpp.org
[Accessed 2013].

OPNET, 2013. *OPNET Technologies, Inc. Simulation Platform.* [Online]
Available at: http://www.opnet.com
[Accessed 2013].

PAPAPOSTOLOU, A. & CHAOUCHI, H., 2009. *Considerations for RFID-based Indoor Simultaneous Tracking.* Gdansk, Polland, Proceedings of the 2nd Joint IFIP Wireless and Mobile Networking Conference.

PAPAPOSTOLOU, A. & CHAUCHI, H., 2010. *Deploying Wireless Sensor/Actuator Networks and RFID for Handoff Enhancement.* Paris,France, Proceeding of the International Conference on Ambient Systems, Networks and Technologies (ACM ANT).

PERKINS, C., 2002. *RFC 3220 : IP Mobility Support for IPv4,* s.l.: s.n.

QUOITIN, B., LAUNOIS, C. & BONAVENTURE, O., 2007. *Evaluating the Benefits of the Locator/Identidier Seperation.* Kyoto/Japon, MobiArch 2007.

REINBOLD, P. & BONAVATURE, O., 2003. IP micro-mobility protocols. *IEEE Communications Surveys & Tutorials,* Volume 5, pp. 40-57.

SO-IN, C., JAIN, R., PAUL, S. & PAN, J., 2012. Future Wireless Networks: key issues and a survey (ID/locator split perspective). *Int.J. Communication Networks and Distributed Systems,* 8(1/2), pp. 24-52.

SOLIMAN, H., CASTELLUCCIA, C., EL MALKI, K. & BELLIER, L., 2005. *RFC 4140 : Hierarchical Mobile IPv6 Mobility Management (HMIPv6),* s.l.: s.n.

TOLEDO, N., HIGUERO, M., JACOB, E. & MATIAS, J., 2009. *Extending the Host Identity Protocol for Next Generation Wireless Networks.* Cairo, Egypt, IFIP WCON 2009, pp. 1-5.

TUNCER, H., MISHRA, S. & SHENOY, N., 2012. A survey of identity and handoff management approaches for future Internet. *Computer Communications,* Volume 36, pp. 63-79.

WAHARTE, S., XIAO, J. & BOUTABA, R., 2008. Sensor-based architecture for qos provisioning and fast handoff management in wlans. *Annals of Telecommunications,* Volume 63, pp. 137-148.

YANG, S., QIN, Y. & YANG, D., 2007. *Dynamic Hierarchical Location Management Scheme for Host Identity Protocol.* Beijing,China, Lecture Notes in Computer Science, Mobile Ad-Hoc and Sensor Networks, Springer Berlin/Hiedelberg.

YOU, T. & JUNG, H., 2012. *A qualitative analysis of MOFI, LISP, and HIP*. Jeju Island, s.n., pp. 772-774.

ZEKRI, M., JOUABER, B. & ZEGHLACHE, D., 2012. A review on mobility management and vertical handover solutions over heteregenous wireless networks. *Computer Communcations,* Volume 35, pp. 2055-2068.