GAZİ ÜNİVERSİTESİ

1926

COMPARISON OF PERFORMANCE EFFECTS OF FIXED AND ROAMING CORRESPONDENT NODE IN MOBILE IPv6 NETWORKS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
GAZI UNIVERSITY

BY
Papa DJASSI

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
THE DEPARTMENT OF COMPUTER ENGINEERING

NOVEMBER 2017

The thesis study titled "COMPARISON OF PERFORMANCE EFFECTS OF FIXED AND ROAMING CORRESPONDENT NODE IN MOBILE IPv6 NETWORKS " is submitted by Papa DJASSI in partial fulfillment of the requirements for the degree of Master of Science in the Department of Computer Engineering, Gazi University by the following committee.

Supervisor: Prof. Dr. Şeref SAĞIROĞLU

Department of Computer Engineering, Gazi University

I certify that this thesis is a graduate thesis in terms of quality and content. ..…………………

Chairman: Prof. Dr. Ebru AKÇAPINAR SEZER

Department of Computer Engineering, Hacettepe University

I certify that this thesis is a graduate thesis in terms of quality and content. …………………...

Member: Assoc. Prof. Dr. Suat ÖZDEMİR

Department of Computer Engineering, Gazi University

I don't certify that this thesis is a graduate thesis in terms of quality and content. …………………...

Date: 24/11/2017

I certify that this thesis, accepted by the committee, meets the requirements for being a Master of Science Thesis.

…………………….…….

Prof. Dr. Hadi GÖKÇEN

Dean of Graduate School of Natural and Applied Sciences

ETHICAL STATEMENT

I hereby declare that in this thesis study I prepared in accordance with thesis writing rules of Gazi University Graduate School of Natural and Applied Sciences;

- All data, information and documents presented in this thesis have been obtained within the scope of academic rules and ethical conduct,
- All information, documents, assessments and results have been presented in accordance with scientific ethical conduct and moral rules,
- All material used in this thesis that are not original to this work have been fully cited and referenced,
- No change has been made in the data used,
- The work presented in this thesis is original,

or else, I admit all loss of rights to be incurred against me.

Papa DJASSI
24/11/2017

MOBİL IPv6 AĞLARINDAKİ SABİT VE DOLAŞIM DÜĞÜMLERİN PERFORMANS ETKENLERİNİN KARŞILAŞTIRILMASI

(Yüksek Lisans Tezi)

Papa DJASSI

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Kasım 2017

ÖZET

Günümüzde iletişim ağlarının çoğu TCP/IP mimarisinden kaynaklanmaktadır. Mobil ortamdaki cihazların sayısı, IP ortamında taşınabilirliğin desteklenmesinden dolayı gün geçtikçe katlanan bir öneme sahip olmuştur. Mobil şebekedeki en büyük zorluklardan biri, hem Mobil Düğüm (MN) hem de Muhabir Düğüm (CN)' ün aynı zamanda dolaşımda olup olmadığı veya yalnızca Mobil Düğüm'ün (MN) dolaşımdayken belirgin bir performans sergileyip sergilemediğidir. Bu çalışmada, OPNET Simülatör kullanilarak rota optimizasyonu etkinleştirildiğinde ve etkinleştirilmediğinde sabit ve dolaşımdaki CN'nin MIPv6 ağlarındaki etkilerini değerlendirmiştir. Sonuçlarımız, rota optimizasyonunun etkinleştirildiği zaman Uçtan-uca gecikmenin haricinde, muhabir CN'nin, mobil şebeke performansı üzerinde olumsuz etkisi olduğunu göstermistir. MN ve CN'nin her birine yakın olduğu ve paketleri olmadan ev ajan iletildiği zaman, bir dolaşımlı CN ile uçtan-uca 0.55 saniyelik bir gecikme ortaya çıkmıştır. CN dolaşımdayken, özellikle aktarma işlemi sırasında Gecikme Varyasyonu, Alınan Paketler, Alınan Kontrol Trafiği, Tünel Oluşturma Tepesi ise artmiştir. Bununla birlikte, hem MN hem de CN'nin etkin olduğu deneyde rota optimizasyonu etkin durumdayken Yönlendirme Optimizasyonu yükü yüksektimiştir. Bunun sebebinin ise, iki düğüm'de her iki yönden RH2 bilgisi olan paket göndermişidir. CN'nin her türlü dağıtımı üzerinde çalışan araştırmacıların bu konulara odaklanılması faydalı olacaktır.

Bilim Kodu	:	92407
Anahtar Kelimeler	:	MIPv6, Sabit CN, Dolaşım CN, MN, HA and FA
Sayfa Adedi	:	51
Danışman	:	Prof. Dr. Şeref SAĞIROĞLU

COMPARISON OF PERFORMANCE EFFECTS OF FIXED AND ROAMING CORRESPONDENT NODE IN MOBILE IPv6 NETWORKS

(M.Sc. Thesis)

Papa DJASSI

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

November 2017

ABSTRACT

Nowadays, most types of communication networks were originated from TCP/IP architecture. The number of mobile devices increases exponentially that is why the support of mobility in an IP environment is very important. One of the big challenge in mobile network is whether both Mobile Node (MN) and Correspondent Node (CN) are roaming simultaneously or whether MN shows a distinctive performance while roaming alone. In this study using OPNET Simulator, we evaluated the effects of fixed and roaming CN in MIPv6 networks when route optimization is enabled and when it is not enabled. Our result showed that roaming CN has negative impact on the performance of Mobile Network, except in the end-to-end delay when route optimization is enabled. The end-to-end delay of 0.55 seconds was achieved with a roaming CN when MN and CN were near to each and directly communicating without packets forwarded to their Home Agents. The Delay Variation, Packets Received, Control Traffic Received, Tunneling overhead increased when CN was roaming especially during the handover process. However, route optimization overhead in enabled route optimization mode form was high when both MN and CN were roaming. This was because both nodes (MN and CN) were sending packets with RH2 information in both directions. In fact, these should be the main indicators that researchers should focus on while considering deployment of any kind of CN.

Science Code : 92407
Key Words : MIPv6, Fixed CN, Roaming CN, MN, HA and FA
Page Number : 51
Supervisor : Prof. Dr. Şeref SAĞIROĞLU

ACKNOWLEDGEMENTS

The accomplishment of any work in life involves the participation of a large number of people who directly or indirectly offer their contribution. The making of this thesis was no different. Several people have been and are involved with your love, your work and your support. I wish to express my sincere thanks:

To God for my life for giving me the force to overcome all barriers and to achieve this goal that I have always dreamed. Thank you for protecting me on this journey and for further this conquest.

To Prof. Dr. Şeref SAĞIROĞLU, my eternal gratitude for the excellent guidance, confidence, patience and encouragement during this thesis work. I world like extend my thanks sincere thanks to my beloved father, mother, brothers, sisters, all my family.

Also my thanks to Gazi University, and teachers and friends from Gazi University, mainly teachers of Faculty of Science, Department of Computer Engineering, for accepting me among thousands of other and for providing me the best quality of education.

Lastly, I thank the Republic of Guinea-Bissau and Republic of Turkey. I am thankful to the Turkish Republic for being my Motherland during all my stay.

TABLE OF CONTENTS

Page

LIST OF TABLES

Table **Page**

LIST OF FIGURES

SYMBOLS AND ABBREVIATIONS

The symbols and abbreviations used in this study are presented below along with explanations.

Symbols	**Explanations**
-	-

Abbreviations	**Explanations**
Aps	Access Points
AR	Access Router
BA	Binding Update
BC	Binding Cache
BU	Binding Acknowledgment
CN	Correspondent Node
CoA	Correspondent of Address
CoT	Care of Test
CoTi	Care of Test Initiate
DHCPv6	Dynamic Host Configuration Protocol version 6
FR	Foreign Router
FSMs	Finite State Machines
GUI	Graphical User Interface
HA	Home Agent
HoT	Home Test
HoTi	Home Test Initiate
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
Kbm	Binding Management Key
LR-PMIPv6	Localize Routing Proxy MIPv6

Abbreviations	Explanations
MAC	Media Access Control
MIPv4	Mobile Internet Protocol Version 4
MIPv6	Mobile Internet Protocol Version 6
MN	Mobile Node
MPLS	Multi-Protocol Label Switching
MR	Mobile Router
MTU	Maximum Transmission Unit
OMNET++	Objective Modular Network Testbed in C++
OPNET	Optimized Network Engineering Tools
OSPFv3	Open Shortest Path First Version 3
PMIPv6	Proxy Mobile IPv6
QoS	Quality of Service
RH2	Routing Header type 2
RRP	Return Routability Procedure
SN2	Network Simulator version 2
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol
WiMAX	Worldwide Interoperability for Microwave Access

1. INTRODUCTION

The impact of wireless networks is undeniable in the current technological era. Due to the market growth of mobile devices such as tablets or smartphones and the increasing use of real time applications and social media networks, efforts to provide uninterrupted Internet connectivity starting to forces the end users. Since Internet Protocol (IP) was primarily created for fixed networks, linking its IP address to a fixed network location will remain unchanged throughout an IP session. This will not allow a connection to a mobile user while moving from his home network to a foreign network. Due to this, the Internet Engineering Task Force (IETF) has proposed Mobile IP (MIP) to allow mobile users a transparent communication environment [1-3].

The main idea of MIP is to give the Mobile Node (MN) a temporary address while it is in foreign network that will be associated with the new connection point, and the original fixed IP address represents the MN home network where other network nodes think it is always situated. Thus allowing the mobility of nodes without losing their original IP addresses and the IP session continues without interruption. Version six of the IP protocol is a protocol with more capacity to grow and it is more feasible for the implementation of network mobility. Since the disadvantage of shortage of fixed addresses available in IPv4 was revealed, IPv6 was considered the solution for this problem. Given the greater availability inherent in this version of IPv6 protocol, it is much easier to obtain single fixed addresses [4]. In this regards, many works have been developed around IPv6 with special emphasis on MIPv6 that successfully implementation of mobility for end devices in a network will have great benefits.

As described above the IETF has developed MIPv6 to support end-user mobility.MIPv6, as it is known, enables a MN to move from one network to another without re-establishment of new sessions on the internet [5, 6]. Without using MIPv6, a session between a CN and MN will be interrupted and a new one will be created when a MN establishes a session with CN on its home network and moves to another network. MIPv6 supports a MN to configure Home Address (HoA) and acquire Care of Address (CoA) when in the foreign network [7]. A MN informs its Home Agent (HA) or previous Foreign Agent (FA) of the acquired new address when reaching to new foreign network in order maintain the session of their communications [6].

Currently the MIPv6 network communication architecture between CN and MN is considered as client-server model where CN is considered as a fixed server. A CN can be a server like youtube.com, serving streaming video to MN over the internet. In contrast, there are some scenarios in which the CN will need to move from one place to another, such as during disaster scenarios, military operations, etc. With the CN as a mobile server, a central mobile point can communicate with another point during disasters or military operations. Due to the increased rapid response in these scenarios, in the near future, the need for CN as a mobile server will be vital.

In this study, two models was analyzed, a mobile network which comprises of a CN with a fixed cable connected to router and a CN roaming in the network. These models were analyzed when the route optimization were enabled and when they were not. The results obtained from the route optimization model and no route optimization model were then compared. In each model, the following performance parameters Delay Variation, End-to-End delay, Packet Received, Control Traffic Received and Overhead were used to observe the effects of these models in the MIPv6 Networks.

Objective

The main objective of this thesis is to analyze and compare the performance effect of fixed and roaming CN in mobile network. The tested scenarios (fixed and roaming CN) are performed with Route Optimization activated and when it is not activated.

Related work

There are few studies carried in relation to the effect of roaming or fixed CN in MIPv6 networks. Most of these studies ware focused on route optimization and handover of MIPv6 networks in the last decade. With route optimization, a great performance improvement has been archived in [8, 9]. However, this is not conclusive either this improvement in performance can (only) be obtained if all end nodes (CN and MN) are roaming or MN is roaming and CN is fixed.

According the reference [10], mobility of CN causes degradation effect on performance in a MIPv6 environment because of frequent handoffs. For this reason, researchers have proposed a new scheme for Mobile IPv6 called Intelligent Mobile IPv6 (IMIPv6) that minimizes the handoff delay caused by the movement of MN and CN. In their study, they compared the existing MIPv6 with the proposed IMIPv6 in a simulation. The results indicate that, IMIPv6 significantly reduces overhead signaling costs and packet loss during handoffs.

In [4] proposes a mobility model that puts in consideration MN as well as the CN especially when MN and CN are in foreign networks. It is obvious that in real-time application such as video conferencing and voice need faster re-establishment of broken connections because of their frequent exchanging of network access points. The proposed model was efficient as the nodes are changing network access point frequently because of the high mobility and result in less packet loss and faster handoff. In addition, the model make best use of available bandwidth, which is a sensitive parameter in wireless networks.

Several studies have also considered the notions such as handover, route optimization, and mobility efficient. For instance, in [11] delivery mechanism was proposed to reduce the initiation time of handover, thus reducing the handover latency. In addition, the designed mechanism reduced the overlap of coverage between adjacent cells. Choi *et al* in [12] proposes an efficient network mobility support scheme with direct Home Network Prefix (HNP) assignment to reduce the location update cost and packet tunneling cost.

Schmidt and Wahlisch in [13] investigated the topological impacts of continuous support on efficient mobility in the MIPv6 hierarchical environment. In their model, during handoff MN does not depend on the roundtrip time of binding with HA or CN. They suggested MIPv6 improvements for a continuous handover for avoiding bidirectional multicast communication. Zohra *et al* in [14] conducted an analytical study on IPv6 mobility management and its Handover Performances. The results collected can be used to analyze and identify the characteristics and performance indicators of mobility proposed. This can facilitate decision-making in the development of a new mobility management protocol in the mobile network.

2. MOBILE NETWORKS

Mobile networks are sets of subnets or single nodes connected to the Internet through mobile routers (MRs) that change their anchor points (Access Router) over the Internet. A mobile network consists of the following nodes: Mobile Node (MN), Corresponding Node (CN), Home Agent (HA), Foreign Agent or Router (FA or FR) and Mobile Router (MR). The CN is a node that is in communication with a mobile node. The corresponding node can be mobile or stationary. Therefore, the terms MN and CN are used to refer to any end nodes located within the mobile network and any nodes communicating with one another. The home agent is a router in the Home network that is used for assigning HoA to MN and tunneling packets to deliver them to a new address of MN when found outside the Home network. FA represents the network where the MN is temporarily attached. It is configured and assigned as a CoA to a MN [15, 16].

2.1. Mobile Internet Protocols

Mobile IP is one of the best-known protocols that supports mobility. It is a network layer, which allows a mobile device to communicate with other devices (fixed or mobile) while traversing IP networks (i.e. it allows a device to move from one network to another without changing its permanent address).

The Mobile Internet Protocol is a protocol solution proposed by the IETF [17, 18]. Mobile IP is the standard technology for node mobility on the Internet. To provide support for node mobility, MIP defines two entities: A Home Agent (HA) and a Foreign Agent (FA). HA is a router in the home network of a MN that forwards datagrams for delivery to the mobile node when it is away from home and maintains current location information for the MN. FA is a router in the visited network of a MN that provides routing services to MN when it is registered. The HA encapsulates, decapsulates and delivers datagrams to and from MN and forward them to CN. For datagrams sent for MN, the HA can serve as the proxy for MNs.

2.2. Mobile IPv6

Mobile Internet Protocols Version 6 or the Mobility Support in IP version 6 protocol, also known as MIPv6, is a protocol supporting the mobility of nodes in IPv6 networks, where each MN can be identified by its HoA regardless of its current connection point on the Internet [19]. It was designed due to experience gained from MIPv4 [2] and also specified in-[20], where terminology and components that are involved in mobility are defined. The main advantage of this protocol is that MNs can change their IPv6 Internet connection point without changing their IP address. A node that does not support the mobility, when moves from one network to another, loses the existing connections. When an IPv6 address is assigned to a node within the base prefix of a network, if node moves from one network to another, the assigned address is ceases to be valid for the use to another node. Therefore, to meet the necessity for mobility, connections with MIPv6 nodes are made (without user interaction) with a specific address that is always attributed to the MN, and through which the MN is always accessible.

The main idea for MIPv6 development was based on the fact that a mobile node should be able to communicate with other nodes after changing its internet connection point, even if is configured a second IPv6 address as an identifier which is normally the one which is different from home network. This process consists for every MN to have a fixed address from its home network, known as HoA. When MN self-configures on foreign network, the MN sends a message to notify it is HA of a new address on the network is visiting. In this way, all the packages destined to its original address will be routed to its visitor address, thus allowing the reception of packages in a transparent way.

On the other hand, new messages (BU and BA) were added to the protocol that allow to inform the CNs of the CoA of the MN when a route optimization is enabled, thus avoiding the dependence of the HA in the routing of the traffic between the CN and the MN, reducing the overhead caused by the triangular connection between CNs, HA and MNs [13, 14]. Before the route optimization, the first few packets during communication sessions of CN and an MN is sent through the HA. After the route, optimization packets exchanged between MN and CN the communication is proceeding directly between these two nodes. These are characteristics that make MIPv6 more scalable because it would be difficult for the HA to have bandwidth required to serve as an intermediary during all sessions established among multiple MNs with multiple CNs.

2.2.1. Mobile IPv6 operations

When MNs are outside of home network, at least two IPv6 addresses will be used to identify them to define their identity and location. One of the address is HoA, which is a permanent address of the MN as well as any IP node. The second address known as CoA, which is associated with MN only when it visits a different network (Foreign Agent or Foreign Link).

The HoA is assigned automatically or manually to the MN upon initialization, based on the prefix of the home Network. While the CoA is assigned whenever the MN attached to a new foreign network. The prefix used is that of the network visited by MN, the packets addressed to this CoA will normally be routed over the internet through HA or directly to MN visiting network.

Each time the MN changes from one network to another, it maintains the HoA and receives CoA. The CoA consisting of a valid prefix in visited network. This address can be assigne to MN in the following ways:

1. Stateless address configuration: The IPv6 stateless auto-configuration engine does not require host configuration, minimal or no configuration of the routers, and the server is not used. This 'non-state' mechanism allows the host to generate its own address by combining the information about the locally available addresses and the information disclosed by the routers [21].

2. State-full address auto-configuration: Is the mechanisms of such Dynamic Host Configuration Protocol version 6 (DHCPv6) or Point-to-Point Protocol version 6 (PPPv6), where hosts get parameters and addresses or configuration information on the configuration directly from a server [22].

The CoA will be used for binding operations to forward the packets destined to the MN by sending them through HoA using bidirectional tunnel [21, 22] established between the MN CoA network and the HA if route optimization was not activated., For the optimized communication between the MN and its CN will be used by MN and CN to exchange packets directly after the binding process is complete.

After MN assigned CoA in a foreign network, the MN must register its new address to HA in home network. This operation is called binding. The MN starts by sending a BU packet to the router requiring it to behave like proxy and then forwarding all the packets destined to MN through bidirectional tunneling process. The router must respond with a BA to confirm the registration if needed to do so by MN. From this point, all packets destined to the home address will be intercepted by the HA and encapsulated in the bidirectional tunnel bound to the CoA. The response to be sent by the MN must follow the inverse path, using the same bidirectional tunnel. Security issues related to these operations have been extensively studied in [23-27].

Once a MN receives packets from CN in bidirectional tunneling, MN initialize the route optimization procedure, thus avoiding that the traffic is to pass through a MN home network. This can avoid overloading of HA and packet fragmentation if exceed Maximum Transmission Unit (MTU).

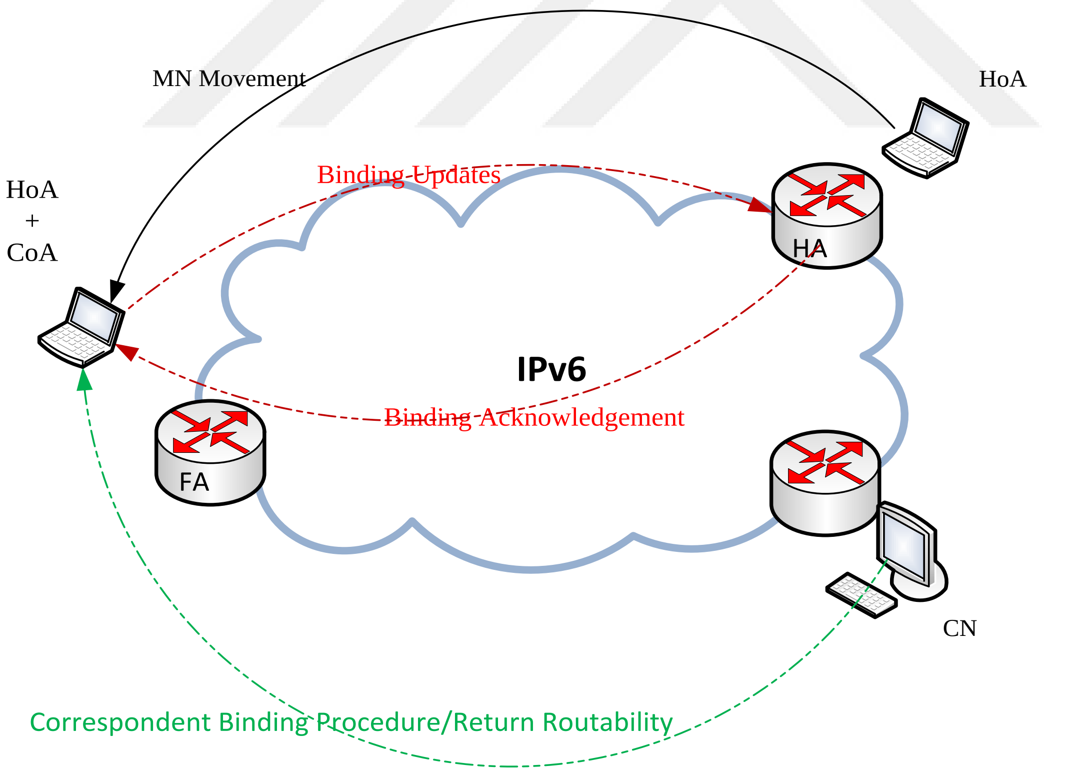

Figure 2.1. Mobile IPv6 operations

Figure 2.1 shows MIPv6 communication operation where at first a MN send BU to it is HA and HA reply this packet using BA. If route optimization method (in this context RRP was used) is used, also MN send BU to CN, also CN reply this message with BU to MN. From this point, onward packets from MN and CN will be exchange directly among them without passing to HA.

Routing optimization

Routing of packets by HA to MN is simple to implement and very safe since the communication between HA and MN is secured by IPsec [28-30]. On the other hand, it is particularly inefficient in terms of routing. Indeed, if MN is moving away from its home network, is communicating with server, and are close to each other, it is more efficient to communicate directly than to go through HA. This saves resources in the Internet and at the HA level, which may face difficulties on forwarding/tunneling every packets if the communications of all MNs pass through it. Therefore, routing optimization, which was an option in MIPv4, was integrated in MIPv6 [28, 31].

Routing optimization involves the routing of packets between MN and a CN, using the shortest path (as is usually done between two relay nodes retransmitted in normal routing). When MN wishes to send a packet to a CN, it checks whether a route optimization has been initialized. In not, MN initialize route optimization method using RRP method or any other method. Otherwise, start to send packet directly to the CN from its CoA network without passing to HA.

If a CN supports routing optimization, like HA maintains an association table for all the MNs using the routing optimization with which it is in communication. The MN updates the association by sending a BU association update message to the correspondent immediately after it has informed HA of its new location. For this purpose, MN must maintain a binding table of updates of associations containing all the binding list entries with the CNs and HA. This process is carried out at each time when binding update entry expire.

In addition, if CN uses route optimization and want to sends a packet to an MN CoA network, look on its binding table entry if there is any association with MN's CoA. It then replaces the destination address with the CoA and put MN's HoA in IPv6 extension header called routing header type 2 as the final destination address[32]. When MN receives this packet, remove extension header that contain MN's HoA and replaces the destination address of the packet with the HoA found in routing header type 2. Then delivers the packet to the upper layers, which consider MN's in home network. This allows the reduction of packet loss due to the lack of knowledge of the MN location. In this way, MIPv6 route optimization transparently hide the MN location to the upper layer, which sees the Communication between CN with the MN's HoA [33, 34].

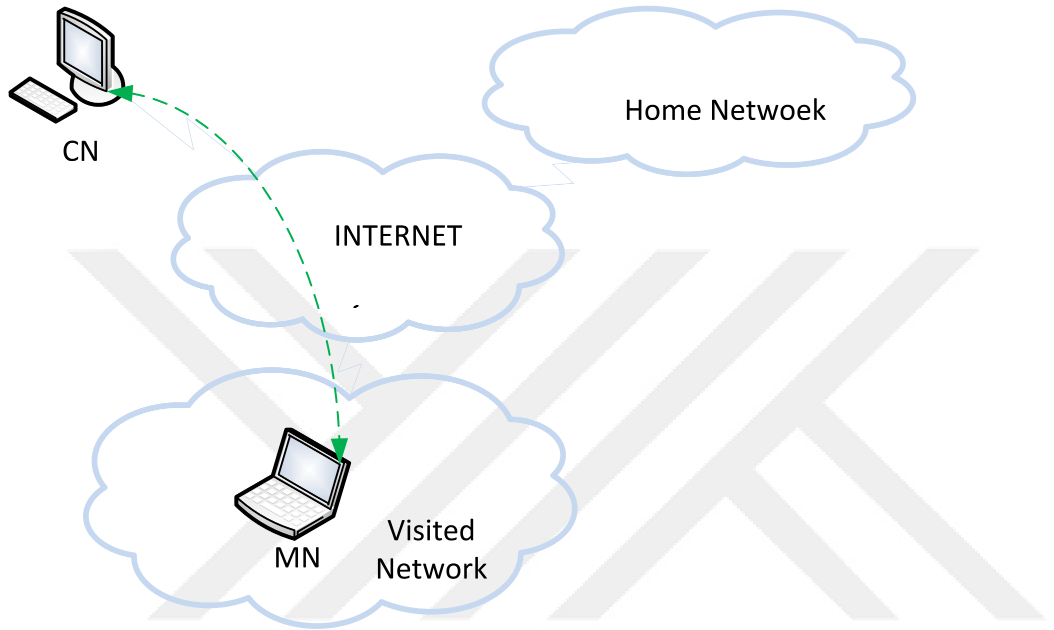

Figure 2.2. Optimized communication between MN and CN

Binding update

The BU is an extension header already incorporated into MIPv6 that consists of sending special messages that inform other nodes of the current location of the MN so that they communicate without using the HA [35, 36]. The BU utilizes the MH Type value 5. When this value is shown in the Binding update field, the format of the Message Data field in the Mobility Header is shown in figure 2.3:

					Sequence #
A	H	L	K	Reserved	Lifetime
Mobility options					

Figure 2.3. Binding update message format

- *Sequence #:* A 16-bit unsigned integer used by the receiver to sequence BU and by the sender to fit a returned BA with this BU.
- *Acknowledge (A):* The Acknowledge (A) bit is set by the sending MN to request a BA be returned upon BU receipt.
- *Home Registration (H):* the sending MN to demand that the receiving node should operate as this node's HA configures the Home Registration (H) bit. The packet destination taking this message should be that of a router having the same subnet prefix as the HoA of the MN in the binding.
- *Link-Local Address Compatibility (L):* The Link-Local Address Compatibility (L) bit is configured when the HoA reported the MN has the same interface identifier as the MNs link-local address.
- *Key Management Mobility Capability (K):* If this bit is cleared, the protocol utilized for constructing the IPsec security associations between the MN and the HA does not survive movements. It may then have to be rerun. If manual IPsec configuration is used, the bit has to be deleted.

This bit is applicable only in BU sent to the home agent, and has to be cleared in other BU. CNs have to skip this bit.

- *Reserved:* These fields are not used. They have to be initialized to zero by the sender and have to be skipped by the receiver.
- *Lifetime:* 16-bit unsigned integer. It is the time staying before the binding seen as expired. A value of zero shows that the BC entry for the MN has to be deleted. One time unit equal to 4 seconds.
- *Mobility Options:* It is a field of variable-length of such length that the total Mobility Header is an integer of 8 times of octets long. This field has zero or more TLV-encoded

options of mobility. The receiver jump any incomprehensible options. The following options are valid in a BU:

- Binding Authorization Data option (this option is mandatory in BU sent to a CN)
- Nonce Indices option.
- Alternante CoA option

If there is no options in this message, there is a necessity of 4 octets of padding and the Header Len field will be set to 1.

The CoA is defined by the field of Source Address either in the IPv6 header or by the Alternate Care-of Address option, if existent. The CoA has to be a unicast routable address. IPv6 Source Address has to be a topologically right source address. BU for a CoA, which is not a unicast routable address, has to be deleted. In a similar way, the BU has to be silently deleted if the CoA is a HoA in a current BC entry, with its actual location making a circular reference back to the HoA defined in the BU.

When the binding is deleted, it can be shown by configuring the Lifetime field to zero and by configuring the CoA similar to the HoA. Note that while the senders are required to set both the Lifetime field to 0 and the CoA equal to the HoA.

CNs must not discard the entry of BC before the lifetime ends, if any application hosted by the CN is still likely to demand communication with the MN. A BC entry that is assigned prematurely can cause subsequent packets to be discarded from the MN, if they have the HoA destination option. This situation recoverable, since a Binding Error message is sent to the MN. However, it occasions useless communication delay [37-41].

Binding acknowledgement

Binding Acknowledgment is a message used to validate the data received via a BU if the BU requests a confirmation [42, 43]. When MN visits a network, then detects the movement and configures its CoA, it sends BU to the HA or CN so that it can associate its HoA and CoA. This information is stored in a local HA or CN cache. The HA and CN in turn returns BA as a response message.

BA is also encoded in MH Type value 6 in IPv6 extension header. When this value is shown in the MH Type field, the format of the Message Data field in the Mobility Header is shown in figure 2.4:

<table>
<tr><td>Status</td><td>K</td><td>Reserved</td></tr>
<tr><td colspan="2">Sequence #</td><td>Lifetime</td></tr>
<tr><td colspan="3">Mobility options</td></tr>
</table>

Figure 2.4. Binding acknowledgement message format

Key Management Mobility Capability (K), Reserved, Status, Sequence #, Lifetime was previously described on section 3.2.1.2. Mobility Options in BA the receiver skips all incomprehensible options. The following options are valid in a BA:

1. Binding Authorization Data option is a required option in BUs sent to a CN. Also valid for BA, it contains a cryptographic value that can be used to determine that the message in question comes from the right authority.
2. Binding Refresh Advice option.

If there is no option in this message, 4 octets of padding are needed and the Header Len field will be put to 1 [39, 44, 45].

<u>Binding cache</u>

Binding Cache (BC) is a volatile memory that hold the Bindings of other nodes. It is maintained by the CN and the HA and contains the current links of MN. Each entry in the BC contains a HoA, CoA of MN, and the lifetime that indicates the validity of the entry. When the BC is held by CN, it also contains some security parameters [46].

As mention earlier, BC also has a useful information such as lifetime, which is set in the BU message where the nodes binds each other. If the lifetime expires, it is deleted in the lists of the cache table [47]. In addition, a node cache may use some reasonable strategy to manage the space within the memory cache as described in [48].

Binding update list

A Binding Update List is a list held by a MN to record the BU that the MN has or is trying to establish binding with a certain node. The list has an item for every binding that the mobile node has or is trying to establish with a specific other node. Both correspondent and home registrations are included in this list. Entries from the list are deleted as the lifetime of the binding expires.

The binding update list is maintained by each MN to record the most recent link updates sent to the HA and the CNs.

2.2. Route Optimization Methods

Various Route Optimization methods have been introduced into the literature to resolve the issues in rectangular routing in MIPv6 networks [33, 49, 50]. To mention the few, based on approach used, the Route Optimization method that have been introduced can be generally classified as:

i. Stateless (e.g. RRP, TOTP-RO etc.)
ii. Proxy Mobile IPv6 (PMIPv6) (e.g. LR-PMIPv6)

Stateless based Route Optimization methods includes Return Routability Procedure (RRP), Time-based One-Time Password Route Optimization (TOTP-RO) etc. In Proxy, based Route Optimization methods, several schemes has been introduce, to mention the few such as Localize Routing Proxy MIPv6 (LR-PMIPv6) etc. In this study, Return Routability Procedure (RRP) was used in our study when performing simulation scenario with Route Optimization enabled [31, 32, 51]. This method is explained in section 2.1.

2.2.1. Return Routability procedure

MIPv6 Route Optimization certifies the authenticity of MN through a routing property [52]. Return Routability Procedure (RRP) is the Routing Optimization method in which MN proves to CN that it has moved to foreign network and simultaneously holds two addresses (i.e. HoA and a CoA) [53]. As shown in figure 2.5, this is done by sending Home address Test Init (HoTi) and Care-Of address Test Init (CoTi). This procedure allows the CN to obtain reasonable assurance that the MN is actually addressable via CoA as well as via its HoA. Then the CN makes two Tokens that only the CN can make (i.e. the CN encrypts with a secret key Kcm that is known only by CN) it sends a Token to HoA in two messages separately, these messages are Home Test (HoT) and Care-Of Test (CoT).

Both tokens are utilized by the MN to make a key (Kbm) that can be used to authenticate a BU message to the CN. Since the CN knows all the information required to regenerate the key, it can regenerate it when the BU is received, and thus authenticate the message. The same key is used for authentication of the BA. The HoTi message is sent by the MN to request a HoA test. The source address used in the IPv6 header is the HoA of the MN and the destination is the CN address. Therefore, this message is tunneled to the HA (since HoA is not topologically correct in the visited network), which decapsulates the message and resend it to the CN. The HoTi message is transported using type 1 mobility header. CoTi and HoTi messages are sent by the MN almost simultaneously. The CoTi message is sent from the CoA network of the MN straightly to the CN.

When the CN receives the HoTi message, it generates a 64-bits source key token (the token produced is based on HoA). The source keygen token is generated by having the first 64 bits of the output of a message authentication code function using Kcn and then computed in the concatenation of the home address and a Nonce. The keygen is computed by the CN as follows:

Home keygen token = First (64, HMAC_SHA1 (Kcn, HoA|nonce|0))

Where

(n, j) = represents the first n bits in j.

HMAC_SHA1 (Kcn, info) = means a hash message authentication code (hash with key) based on the SHA1 hash algorithm, also utilizes Kcn to verify the function, which performs the information.

The CN then builds a HoT message and sends it to the MN. The message will be intercepted by the HA and tunneled to the MN CoA. A similar operation is performed when the CN receives the CoTi message where keygen is computed as follow:-

Care-of keygen token = First (64, MAC (Kcn, CoA|nonce|1))

This message ends the RR procedure. At this point, the CN has not yet kept information that it possessed at the beginning of this procedure: Kcn and an indexed list of nonces. The CN keeps neither the keygen nor the keygen-token. When necessary, these tokens can be reproduced, given the nonce indices originally used to produce them.

After getting the HoT (tunneled from HA) and the CoT message, the MN is in a position to produce the binding management key, Kbm. This is done as follows:

Kbm = SHA1 (home keygen token/care-of keygen token)

Now MN can make the mobility header used for the BU message. The mobility header comprises of the BU, the nonce indices option, and a binding authorization data option. Mobility header data covers the contents of the mobility header except only the authorization data option. The final destination is the destination address of the packet (i.e. address of the CN). If the CN is also an MN, the packet will include a routing header type 2 (containing the HoA). Once the routing header is treated before the mobility header, the final destination field must have the HoA of the CN [30, 54-56].

Since the CN does not keep state for any MN during the RRP, the MN requires to include its HoA and CoA in the BU. The HoA is put in a HoA option, which predates the mobility header. If the CoA were different from the source address of the packet, it should be put in the alternate CoA option; otherwise, the source address of the packet is undertook to be the CoA. In any case, the CoA must always be the one utilized in the source address CoTi message field; otherwise, the wrong care-of keygen token will be utilized to produce Kbm when the BU is got at the CN. After BU message construction, the MN sends it to the CN. At the time the CN gets the BU, it checks in the nonce indices option and finds the corresponding nonces. If a confirmation is requested, the CN must send a BA.

The RR procedure is advantageous because it is lightweight and does not need pre-shared authentication material. It also does not need any status in the CN. On the other side, the two accessibility tests can bring to unacceptable download delay for many interactive or real-time applications such as video conferencing and Voice over IP (VoIP). In addition, RRassured security is not enough for security-sensitive applications. Finally, periodic updating of registration in a CN involves an overhead of hidden signaling that may prevent MNs from being hibernated during periods of inactivity [14, 41, 57, 58].

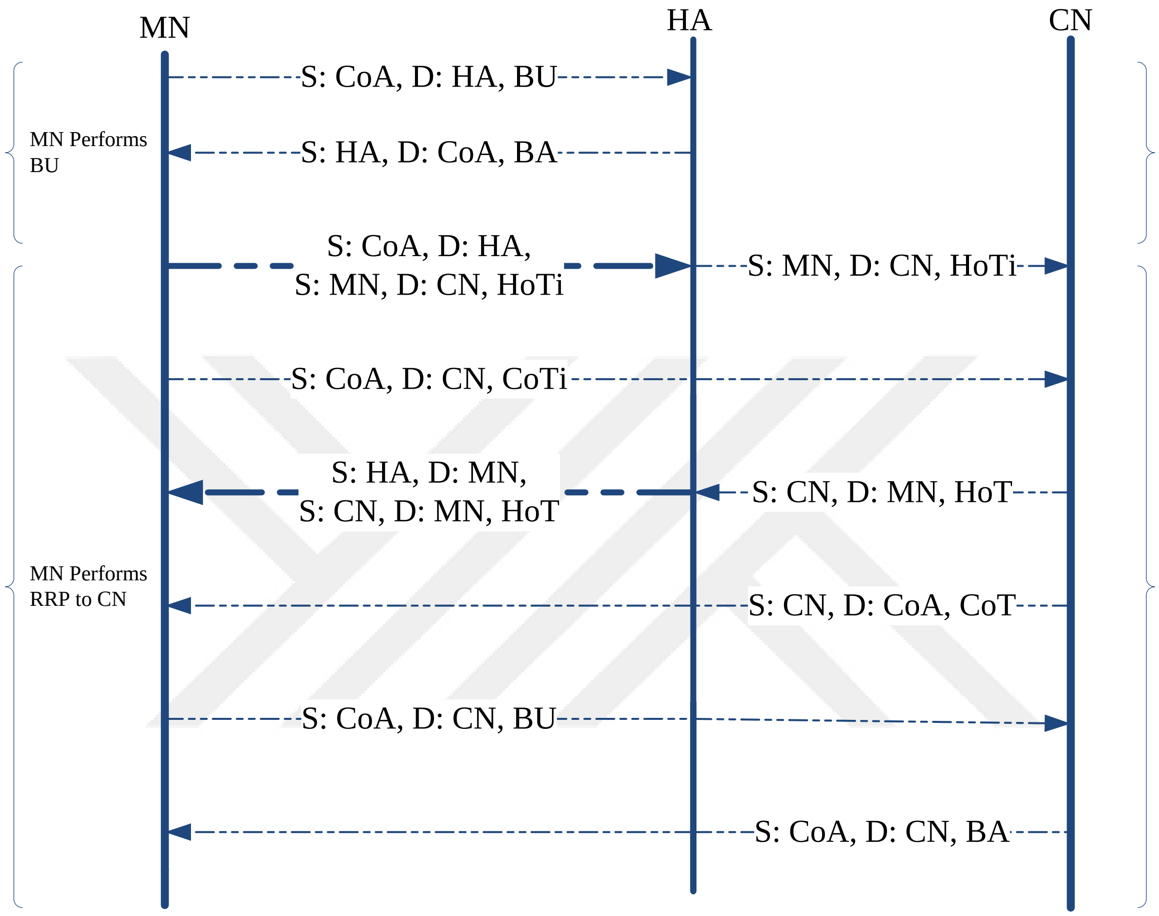

Figure 2.5. Return Routability procedure steps.

2.3. Roaming and Fixed Correspondent Node Model

The CN is a node that is in communication with MN. The CN may be mobile or stationary. Every node of an IPv6 network is a potential candidate to exercise, for some period, the role of CN. Therefore, every IPv6 node must be able to process BU received, send BA and maintain Binding Cache. Nodes receiving BU or BA should verify the authenticity of the packet.

Fixed CN may be any normal server connected in the network through a cable and in communication with MN. In this model, the communication between MN and CN occurs exclusively through the exchange of messages. This model works as the client-server model where the CN is considered as a fixed server serving video streaming to the MN through the internet. In order to obtain a service, the MN sends a request to the CN. This, in turn, performs the operations associated with the service and sends a response to the MN. We created the communication mechanisms scenario that allow the exchange of messages between act as a MN and the other one as a fixed CN.

In the second case Roaming CN is an autonomous node, equipped with wireless network access interfaces, which is part of a network, but which can also change from one network to another and continue to belong to the original network. Therefore, the flow steps of the messages will change, according to the movement of the CN. In this case, the packets destined for the CN are forwarded by their HA in the case of scenario where the route optimization is not activated.

3. SIMULATION STUDIES

3.1. Simulation Tools

This chapter gives a description of simulator used in our study. In addition, it contains explanation of the model simulator that used by OPNET Modeler. Lastly, the scenario network models to simulate Effect of fixed and roaming CN in MIPv6 Networks was presented.

3.1.1. OPNET simulator

The OPNET simulator is a modeling and simulation tool of all kinds of networks, with native mobility support; it was developed and marketed by OPNET Technologies Inc. Currently OPNET is a great reference in the field of network simulation.

There are other similar simulation tools, such as:

1. NS-2 (Network Simulator version 2), is a simulator that has been used frequently by researchers in computer networks. It simulates an IP network and protocols such as TCP and UDP. In addition, SN2 can be used to implement Multicasting and some of the MAC layer protocols for simulation of LANs. After simulation, the NS2 produces detailed simulation data that can be studied and analyzed. Generally, NS2 bears a lot of resemblance to OPNET Modeler. The complete set of OPNET Modeler offers more features than Ns2 and therefore is more attractive to network researchers [59, 60]. For example when we perform the "finetuning" of the parameters, it is verified that OPNET Modeler is a more precise simulator for this particular case. The advantage of NS2 over OPNET Modeler is that, NS2 simulator is open source simulation tool. However, open source simulators are disadvantageous in the aspects of upgrades, full documentation and cannot be maintained by any specialized team in that company.

2. OMNET++ (Objective Modular Network Testbed in C++), is an object-oriented sequential discrete simulation system developed in the academic field with the aim of being an alternative to the high prices of commercial products in the simulation domain. It was developed to simulate mainly computer networks, multiprocessors, and other distributed

systems etc. In OPNET probably has the largest selection of ready-made protocol models (including IPv6, MIPv6, WiMAX, QoS, Ethernet, MPLS, OSPFv3 and many others) compared to OMNET++. In general, OPNET and OMNET++ both have rich simulation libraries of approximately comparable functionalities. In addition, OMNET++ architecture is similar to OPNET because it allows hierarchical models, but OMNET++ has some constraints such as at the "node" level cannot be hierarchical. The big difference between OMNET++ and OPNET is that OPNET models are always fixed topologies, while OMNET++ NED, the graphical editor of OMNET++ allows parametric topologies. In OPNET, the preferred way to define the network topology is to use the graphical editor [61].

We compare OPNET Modeler and other simulators focusing on the usability and scalability capabilities of simulator characteristics. We observe that each has some advantages and disadvantages and each may be appropriate in different situations. We chose the OPNET Modeler simulator based on the reason for our study. In choosing the simulator, we consider the pros and cons of different time for developing our simulation model, simple ability to archive our goal, component-based or object-oriented architecture, simulator complexity level, resources for inclusion and exclusion among other design options. NS2 and OMNET++ in terms of open source should be the best choices. However, Ns2 for example is a very popular simulator for academic research, but its architecture is very complicated. While OMNET++ is gaining popularity in the educational and industrial area, but OPNET has a library of larger protocol models compared to them. In terms of commercial simulator, OPNET Modeler satisfies almost the important features of our study [62, 63].

The table below presents a summary of comparative analysis of different network simulators.

Table 3.1 Comparison of different network simulators

MAIN FEATURES	OMNET++	NS2	OPNET
Language supported	C++	C++ and OTCL	Proto-C, C, C++
License	Open Source	Open Source	Commercial
GUI support	Good	Poor	Excellent
Time taken to learn	Moderate	Long	Long

Table 3.1. (continuation) Comparison of different network simulators

Platform	Linux, Mac-Os, Unix	Microsoft Window, Mac-Os, Unix, Cygwin	C, C++, Opnet Modeler software
Network visualization tool	✓	✓	✓
Possibility to design and modify scenarios	✓	✓	✓

We chose OPNET to perform our experiment in this work due to the following reasons:

- Simplification in the process modeling of the system through graphical interfaces by divided into hierarchical levels that allow the expansion of the models in subnetworks.
- There are a large number of pre-defined network equipment in standard libraries as well as in manufacturer libraries that allows users to simulate various types of hardware such as routers, switches that are manufactured by Cisco, Nortel and Lucent, Dell, Novell, 3COM etc.;
- Equipment already evaluated and validated by its manufacturers, which allows the obtained results to be very close to those obtained in real environments;
- Possibility to change and create any equipment and other components such as protocol, CPU, queues etc.;
- Source code available for all devices in C language, facilitating changes and new implementations;
- Inclusion easy of algorithms in the different levels of the model, concrete case of scheduling algorithms in the routers;
- Availability of technical support in the use of resources;
- Fast discrete event simulation engine
- Lot of component library with source code
- Object-oriented modeling
- 32-bit and 64-bit graphical user interface
- Customizable wireless modeling
- Discrete Event, Hybrid, and Analytical simulation

- Grid computing support
- Integrated, GUI-based debugging and analysis
- Open interface for integrating external component libraries

3.1.2. OPNET modeler relevant structure in simulation

The network simulation process in the OPNET Modeler simulator is organized in four steps, which are generally used by computer network researchers to create a network model. These steps are:

1. Create Network Model
2. Choose Statistics
3. Run Simulations
4. View and Collect Results

The first step is to create a network environment that will include network structure and network devices. The second step is to choose the statistics that we want to analyze. Then to run the simulations. Finally is to collect and analyze the results obtained after simulating your network model. In addition, OPNET Modeler has a set of hierarchical editors that parallel executes networking equipment and protocols[64, 65]. These editors are:

- Project Editor
- Node Editor
- Process Editor

Project editor

Figure 3.1 represents project editor used to specify the physical topology of a communication network. In this editor, a network model/scenario can be constructed using the available models from the object palette. Also in this editor, one choose individual statistics; run a simulation, and collecting results. The project editor is made up of network objects such as subnetworks, network devices/nodes and network links. Nodes and links have a set of parameters that can be configured through the dialog boxes. A node can be fixed, mobile or even a satellite. All functions available in the editor are accessible through the menu bar.

The bar with action buttons contains frequently used functions. The message area, located in the lower left corner, provides information about the status of the tool.

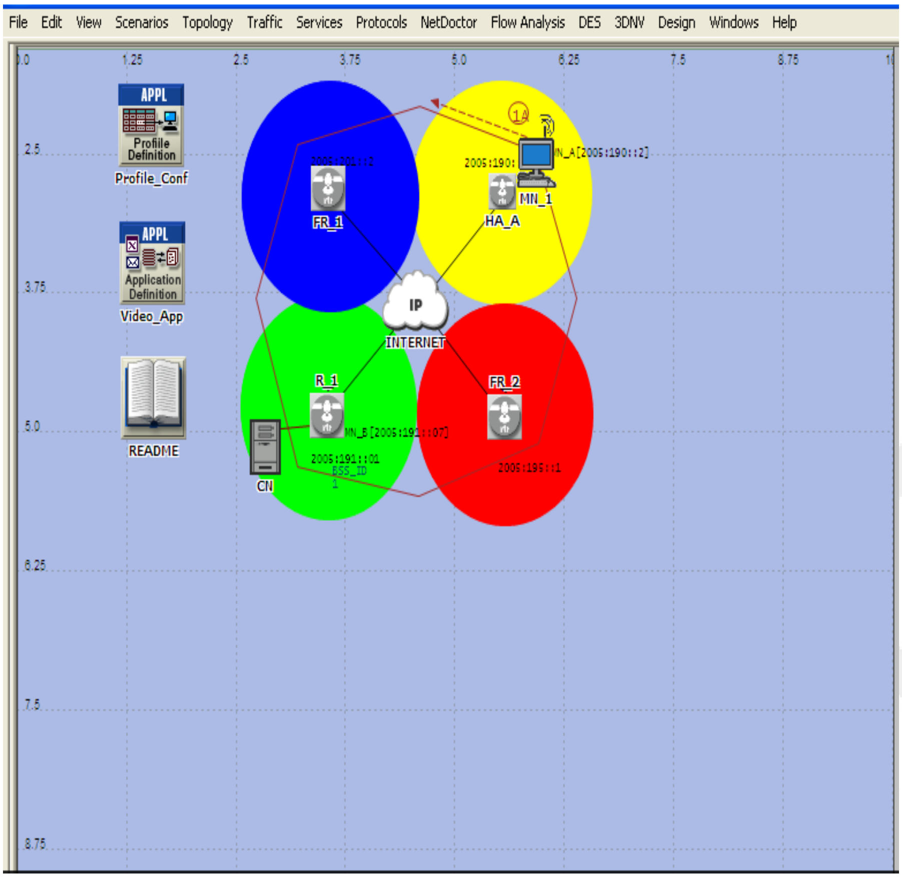

Figure 3.2. Project editor

Node editor

Figure 3.3 represents node editor that is a flow diagram of data between functional elements, called modules, where you can define the behavior of each network object. The modules can be grouped into two different categories:

- The first category consists of modules that predefine characteristics and their respective internal parameters. For example, a data generator, a transmitter, a receiver or an antenna.
- The second category consists of modules that can be programmed. For example, protocols, algorithms, rows, etc.

Modules are interconnected by static wires and communicate via packet streams. Modules can generate, send or receive packets from other modules, to perform their function within the node. Each programmable module in a node model has its functionality defined by a model process.

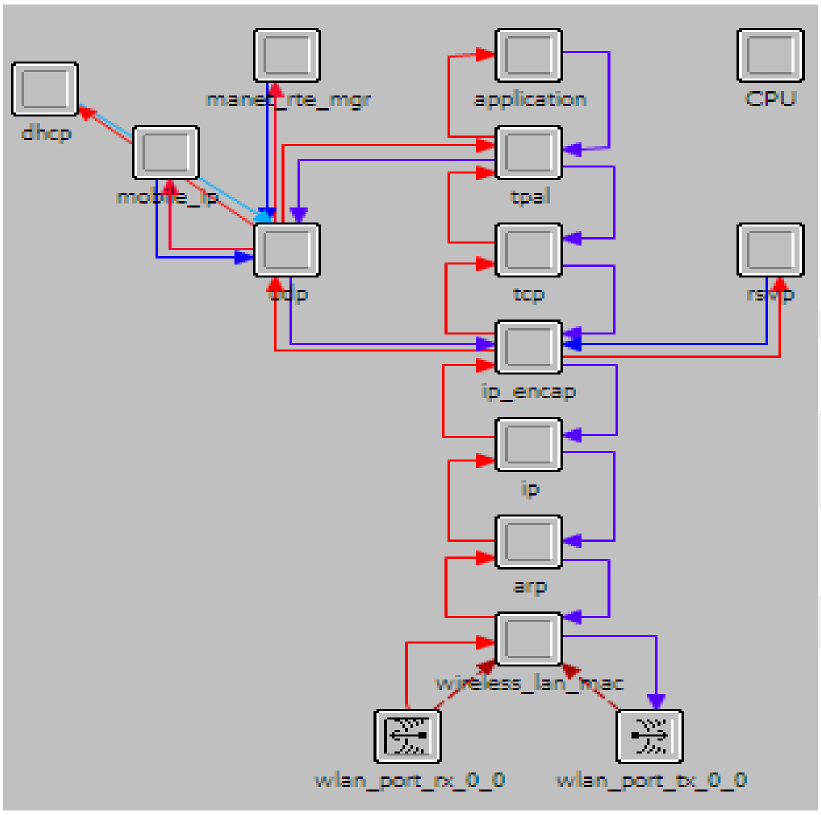

Figure 3.4.Node editor of MN

Process editor

Figure 3.3 represents process editor is a process used to create process models that control the functionality of the layers of the node models created in NODE EDITOR. A finite number of state machines (FSMs) and lines representing transitions between states of process model. State-related operations or transitions are described in blocks using the C or C++ programming language.

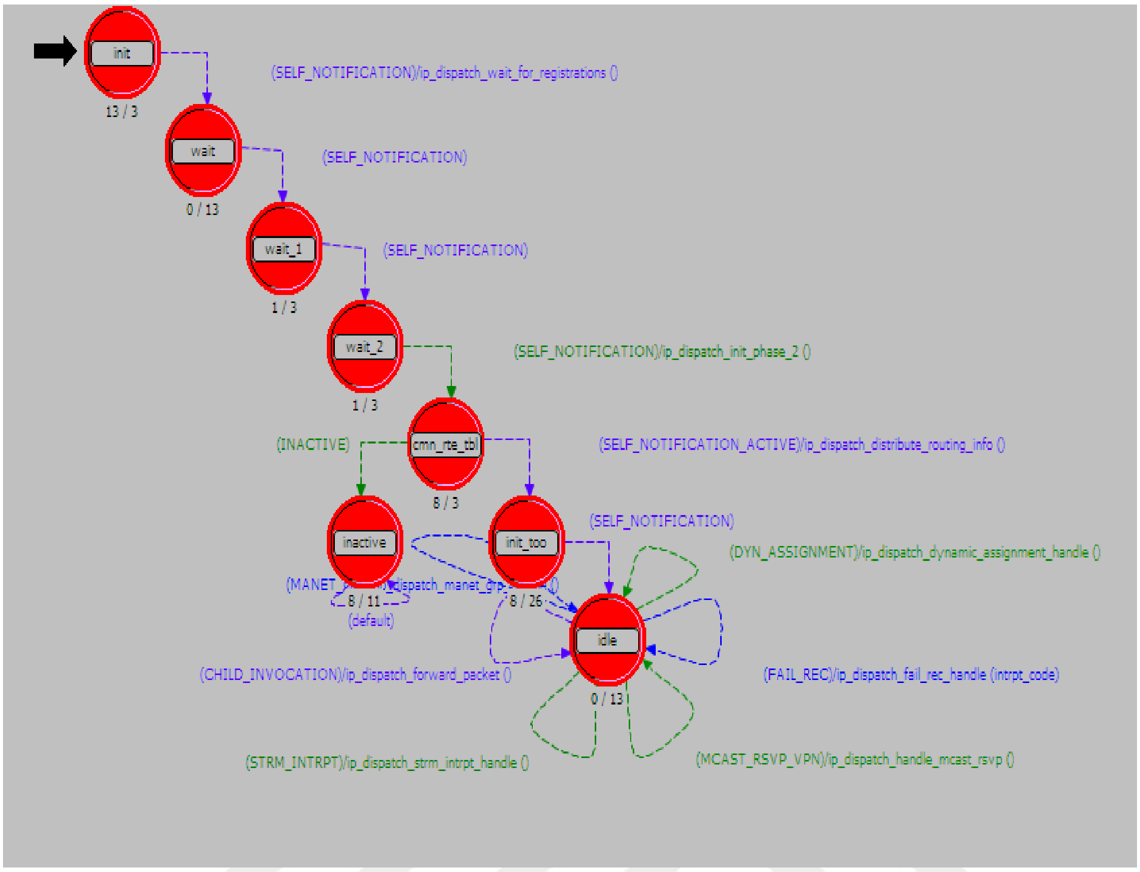

Figure 3.5. Process editor of IP_disparch

4. TEST SCENARIOS

In our study, two scenarios were studied. The first scenario is the one in which a CN is roaming as well as the MN, while the second scenario is the fixed CN and only MN is roaming. These topological scenarios are shown in Figure 4.1 and Figure 4.2 for roaming and fixed CN respectively. Each topology consists of six nodes, IPv6 Internet cloud, four Access Points and the mobile trajectory. These two topological scenarios are depicted in section 3.2.1 and 3.2.2 below:

4.1. Roaming Correspondent Node

In this model with mobile CN, we present a network scenario with a roaming CN and MN.

Figure 4.1 shows topology of the network model used to simulation scenarios of the roaming CN.

This topology consists of two mobile nodes; CN and MN, all of these nodes are roaming in their define trajectory. In this topology, we simulate a network when route optimization is enabled and route optimization is not enabled.

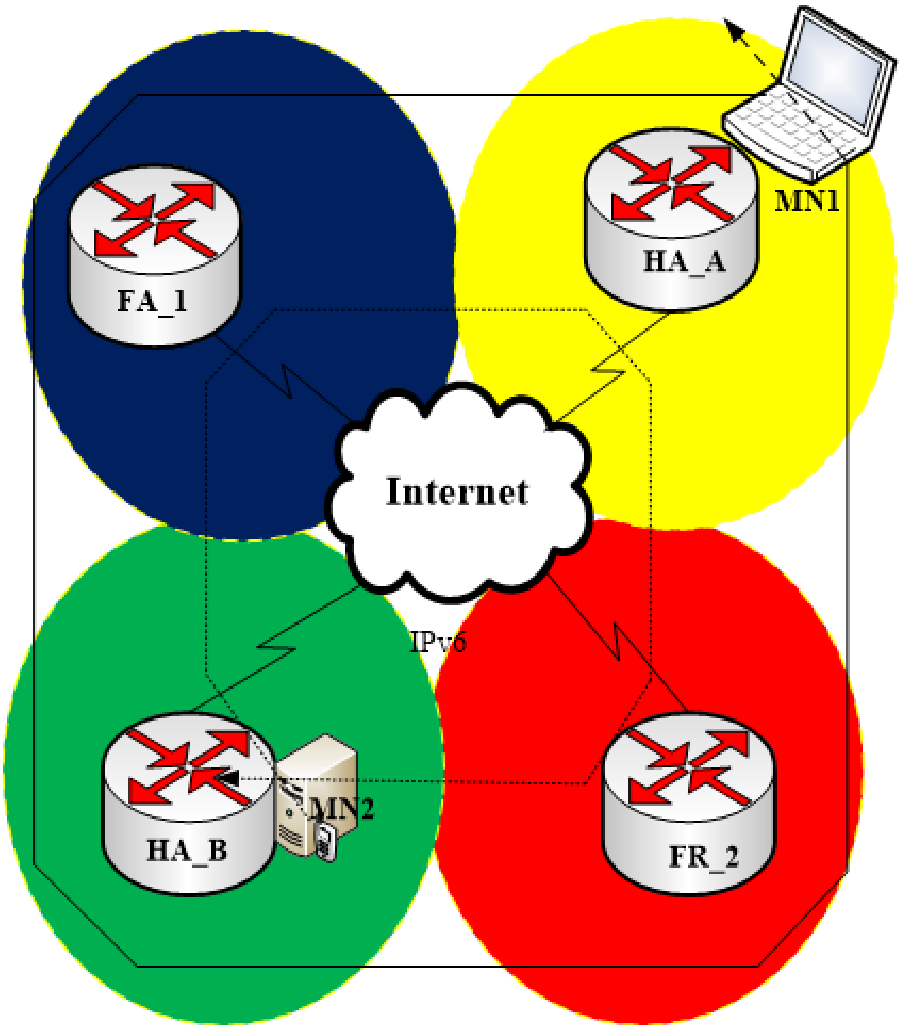

Figure 4.1.Network model with roaming CN

In addition, this network model consists of two foreign routers (FA_1) and (FR_2) and two home agents (HA_A and HA_B). This network model also have MN_2 which is considered as a roaming CN with it is HA as HA_B and MN_1 which is considered as MN and it's HA as HA_A. These mobile nodes (MN_1 and MN_2) pass through the four APs using defined trajectory and a fixed speed.

A scenario is also composed of an IPv6 internet cloud which connect so four routers, FA_1, HA_A, HA_B and FR_2.

Table 4.1. Motion parameters of network model with roaming CN

Parameters	Value
Simulation softwere	Opnet Modeler 14.0
Network topology	10 x 10 km
Routing protocol	RIPng
Simulatio time	1200 seconds
Routers	HA_A, HA_B, FR_1, and FR_2
Nodes	MN_1, MN_2
Number of Trajectory	MN1_Traj and CN_Traj
Route Optimization Method	RRP
Mobility model	Random movement at maximum speed
Initial x position	5.93 for MN_1, 3.91 for MN_2
Inintial y position	2.49 for MN_1, 4.51 for MN_2

4.2. Fixed Correspondent Node

In this part, a network model with fixed CN is shown in Figure 4.2.

This topology consists of fixed CN and a roaming MN. A MN is roaming from it is HA and passing through FA_1, R_1, FA_2 and way back to it is HA.

In addition, this network topology simulates the scenario when route optimization is enabled and when is not enabled.

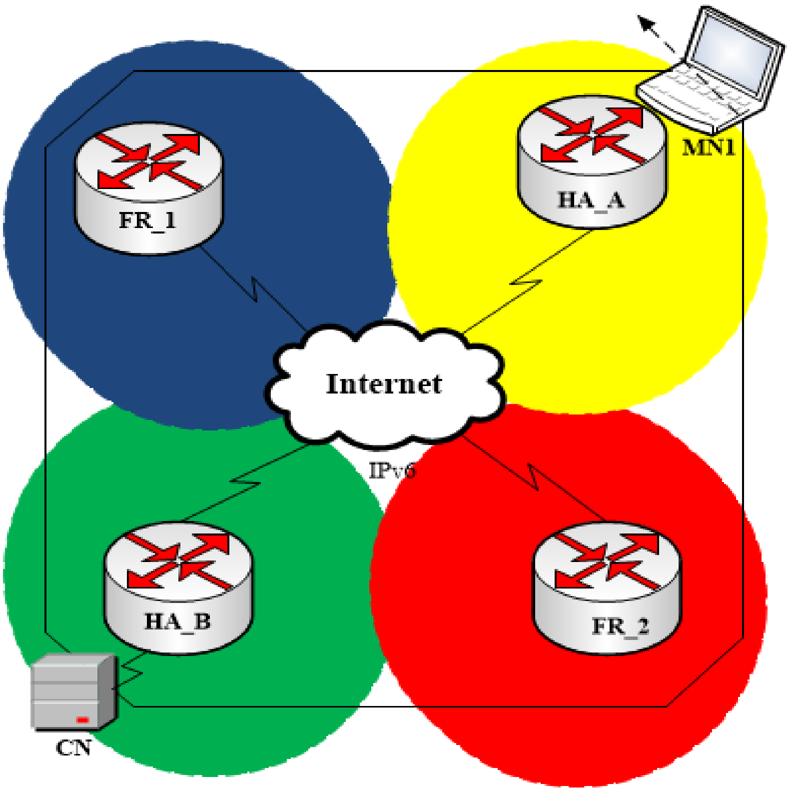

Figure 4.2. Network model with fixed CN

In this network model where we have a fixed CN, the network model consists of two foreign routers (FR_1 and FR_2), one HA (HA_A for MN_1) and one router (FR_1) which connects CN using fixed cable. In addition, in this scenario, it is composes of an IPv6 internet cloud which connects four routers (FR_1, HA_A, HA_B, and FR_2).

Table 4.2 Motion parameters of network model with fixed CN

Parameters	Value
Simulation softwere	Opnet Modeler 14.0
Network topology	10 x 10 km
Routing protocol	RIPng
Simulatio time	1200 secods
Routers	HA_A, HA_B, FA_1, and FR_2
Nodes	MN_1, CN
Number of Trajectory	MN1_Traj
Route Optimization Method	RRP
Mobility model	Random movement at maximum speed
Initial x position	5.93
Inintial y position	2.49

5. RESULTS AND ANALYSIS

Computer Networks can be measured according to some comparison criteria. The most important criteria are the performance, reliability and security.

The performance of a network can be measured in different ways such as transit time and response time, packet delivery, packet loss ratio, overhead etc. Transit time is the time interval required for a message to travel from one device to another. Response time is the time elapsed between a request and a response. The performance of a network depends on a number of other factors, such as the number of users, the medium of transmission, the capacity of the networked hardware, and the efficiency of the software running on the network.

In addition to the delivery guarantee, the reliability of a network is measured by the frequency of failures, the time to reconfigure the link after a failure, and the robustness of the network in a catastrophe.

Network security is a criterion whose purpose is to ensure the protection of data and information that travels in the network from unauthorized access.

In this study, a simulation was performed in OPNET Modeler version 14.0. Performance parameters such as Delay Variation, End-to-End Delay, Traffic Received, Control Traffic Received, Route Optimization Overhead, and Tunneling Overhead were selected for Video Conference application (Lightweight Video Conference). The performance of the Fixed and Roaming CN topological scenario was compared for each above parameter when a route optimization was enabled and when it was not. The following parts explain each of the results.

5.1. Comparison for Scenarios in Route Optimization

5.1.1. Delay variation

The difference in end-to-end delay in one-way direction of the video conference are represented here. Figure 5.1 shows a delay variation of a video conference application in the network with fixed and roaming CN when the route optimization was enabled. Within

300 seconds of simulation time, delay variation with a fixed CN was equal to zero while the roaming CN with slightly increased value to 0.003s. Within 300 to 600 seconds of simulation time, the delay variation was approximately the same for all scenarios. However, after 660 seconds of simulation time, a delay variation started to jump up to high value with a fixed CN scenario showing a small value of delay variation compared to a roaming CN scenario. This also show that, if a route optimization is enabled, there is a huge difference in delay variation when a CN is roaming and when is fixed.

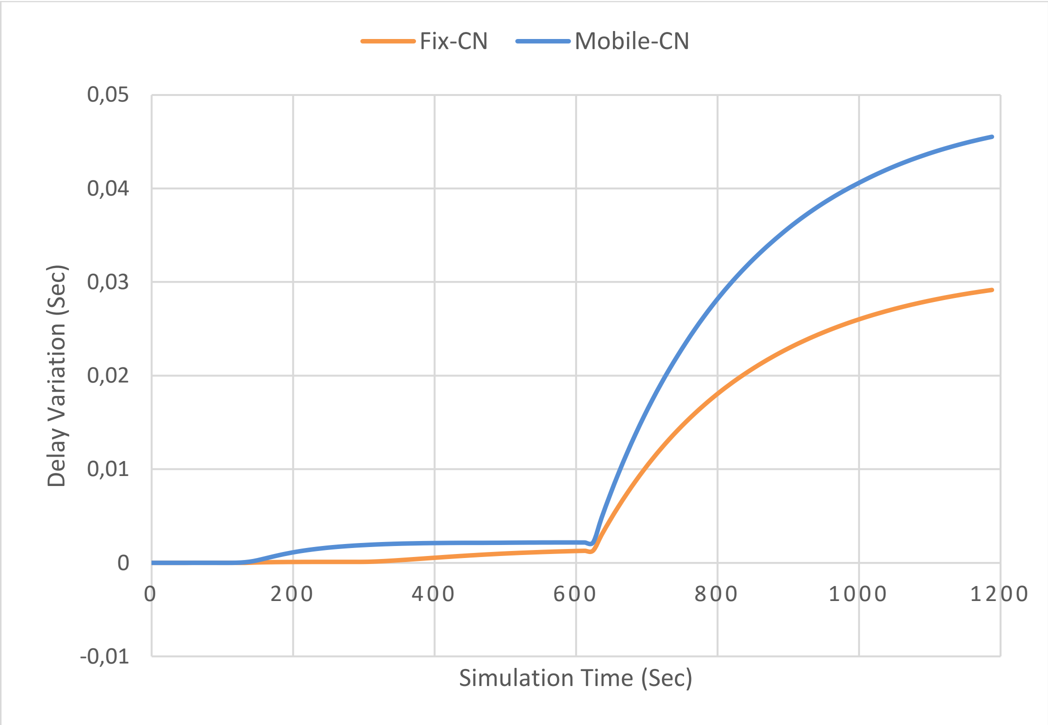

Figure 5.1. Delay variation for video conference when route optimization enabled

5.1.2. End-to-End delay

In this part, the end-to-end delay for the video conference application in fixed and roaming CN is shown. The time take for a packet from the sender to the receiver is referred as end-to-end delay. Figure 5.2 shows an end-to-end delay for fixed CN and roaming CN when route optimization was enabled. MN and CN all together roaming, the end-to-end delay was better due to the fact that at some point the CN and MN closer to each other. With a route optimization enabled the packet are sent directly to each other without passing to HA which make end-to-end delay to become approximately to zero in some cases. With a fixed CN, an end-to-end delay is approximately to zero at one time during the simulation time when the

MN is passing near the fixed CN. The roaming CN has advantage of reducing end-to-end delay when roaming near the MN when route optimization is enabled.

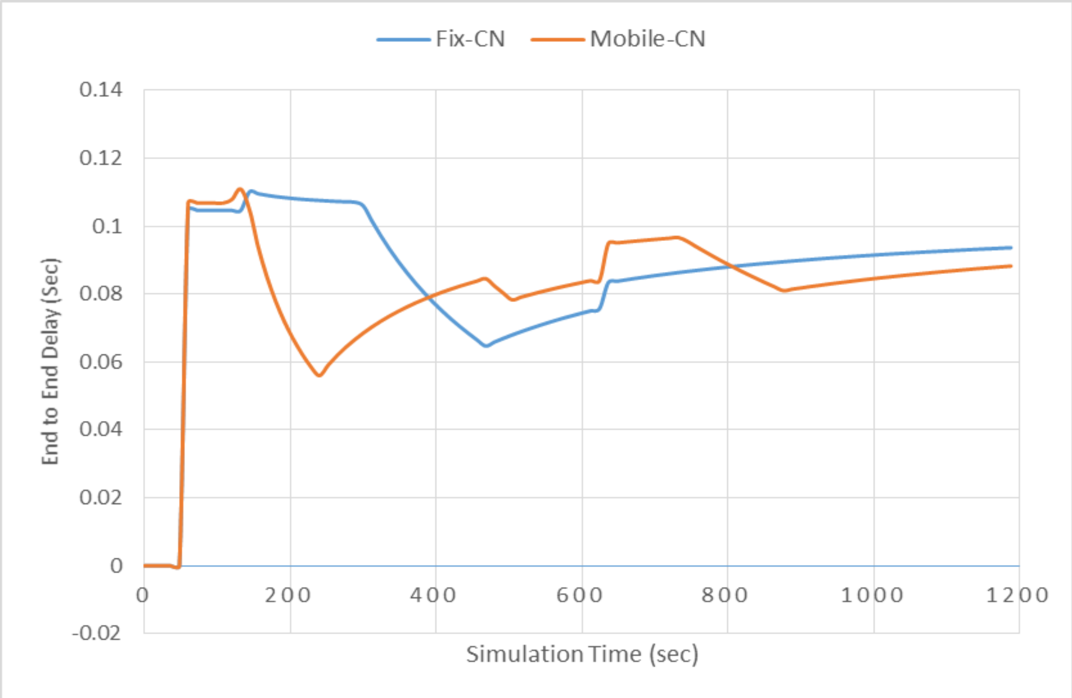

Figure 5.2. End-to-End delay for video conference when route optimization enabled

5.1.3. Traffic received

The number of packets received for video conference application is discussed in this part. In Figure 5.3 packets received when route optimization enabled for fixed and roaming CN scenarios was compared. From the results, no packet drops during the communication of MN and CN except when MN or CN has to do handover process. It is clear that, if the two nodes where roaming packets drops during handover process is more, compared to a fixed CN scenario, packets during handover process is occurred only in the MN side. However, when all two nodes perform handover process, no packets received in either side of the nodes (the packet drop is severe). This phenomenon is shown around 600 seconds of simulation time in Figure 5.3.

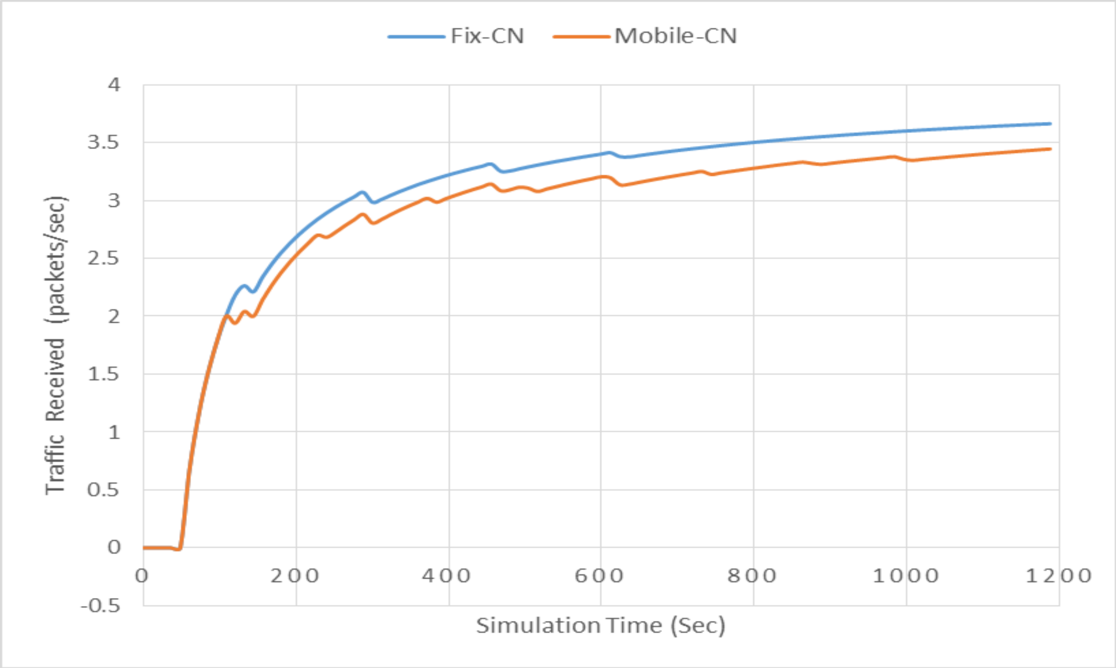

Figure 5.3. Packet received for video conference when route optimization enabled

5.1.4. Control traffic received

According to [34] network traffic control are the MIPv6 signaling messages sent and received by the participating node such as MN, CN, or HA. Traffic control message can be BU, BA, HoTi, CoTi, HoT and CoT. Figure 5.4 shows the control traffic due to the MIPv6 mobility messages measured packets per second. Within the first 120 seconds of the simulation time, the traffic control with a fixed and roaming CN was equal to zero. Starting at 144 seconds to the end of simulation time a traffic control for roaming CN was approximately 0.02 packet/second more higher compared to a fixed CN.

Generally shown in Figure 5.4, control traffic for roaming CN when route optimization was enabled is higher compared to fixed CN. This is because when MN increases in the network more control messages are triggered. This shows that if we enable route optimization, there is a difference in traffic control when a CN is roaming and when it is fixed.

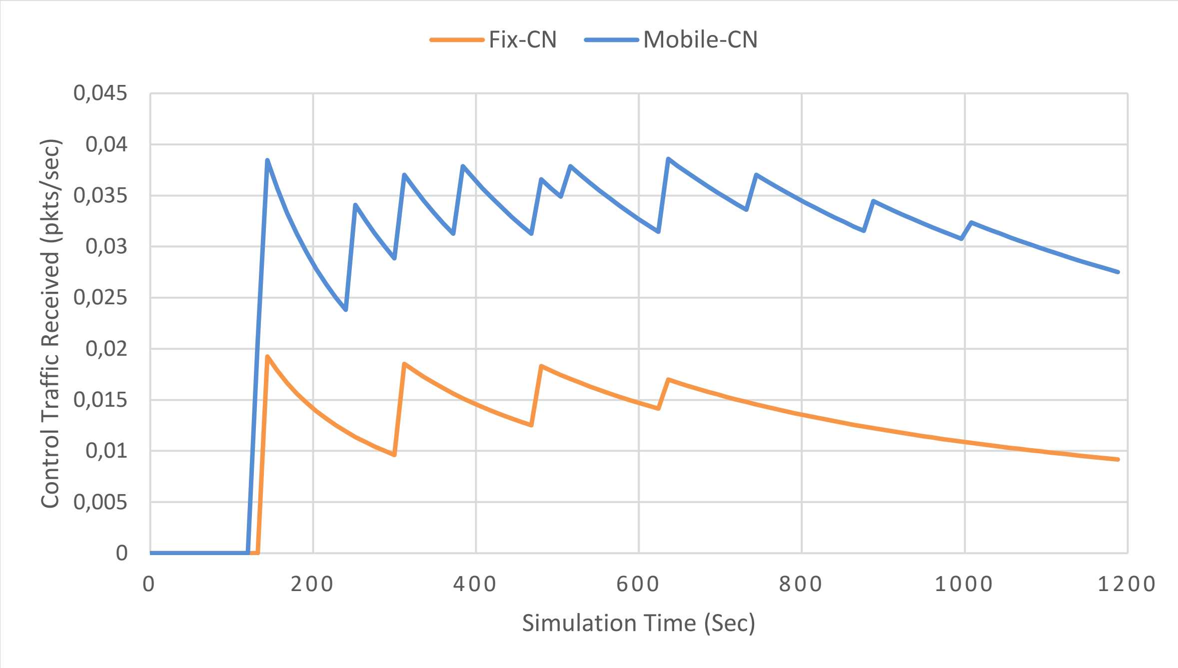

Figure 5.4. Control traffic received for video conference when route optimization enabled

5.1.4. Overhead

Tunneling overhead

Overhead is a combination of excessive computing time, memory, bandwidth especially in wireless network environments so that are required to perform a specific task. Tunneling Overhead represents the traffic overhead ratio due to IPv6 header encapsulation when sending data traffic through MIPv6 tunneling [34]. If Route Optimization was enabled, packet encapsulation is happening only when MN is bond to HA but not to CN. Figure 5.5 shows tunneling overhead in percentage with fixed CN and roaming CN when route optimization is enabled.

It is shown from Figure 5.5 with roaming CN scenario more tunneling overhead were encountered compared to fixed CN scenario when route optimization is enabled. For this case, with roaming CN packet encapsulation is done in HA_A and HA_B, while with fixed CN packet encapsulation is done only in HA_A. The tunneling overhead are ranging from 0.1% to 0.26% when both communicating nodes are begin to go out of their respective networks compare to tunneling overhead ranging from 0.1% to 0.2% when fixed CN was used.

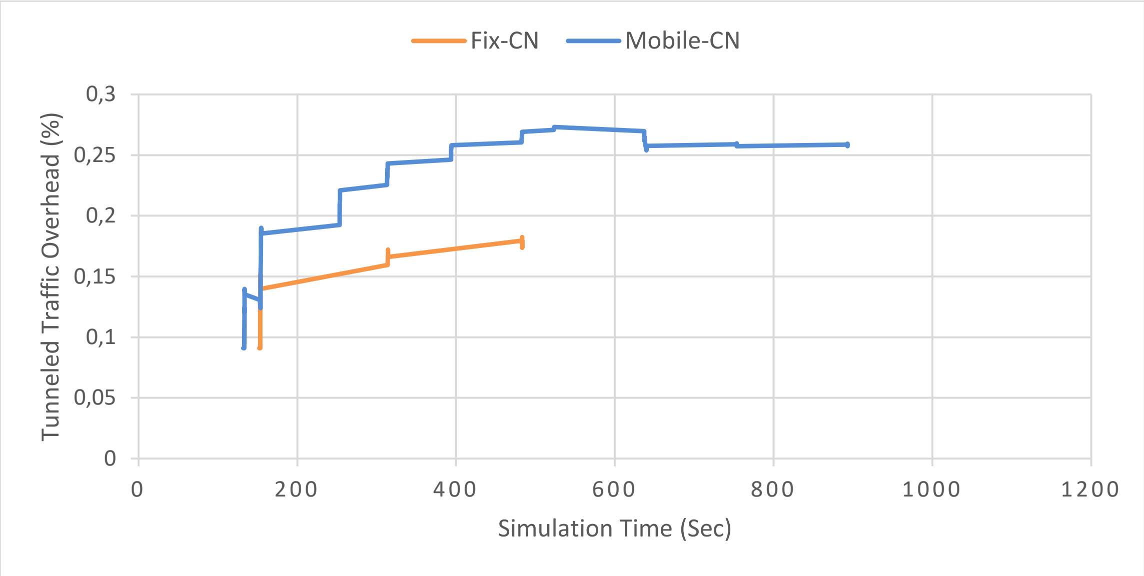

Figure 5.5. Tunneling overhead for video conference when route optimization enabled

<u>Route optimization overhead</u>

Route Optimization Overhead represents the traffic overhead ratio due to addition of IPv6 extension headers, when sending data traffic using MIPv6 RRP route optimization mechanism [34]. Figure 5.6 shows a Route Optimization Overhead in percentage. From the result shown within the first 153 seconds of simulation, the Route Optimization Overhead ware increasing in the approximate same value for all fixed and roaming CN scenarios. This is because only single node ware active as a MN. But from 153 seconds to the end of simulation time the Route Optimization Overhead of a roaming CN was high compared to fixed CN. This is due to fact that, two nodes ware in mobility and were in foreign network while in fixed CN scenario only single node was mobile, hence RH2 messages for Route Optimization were sent in both directions of MNs.

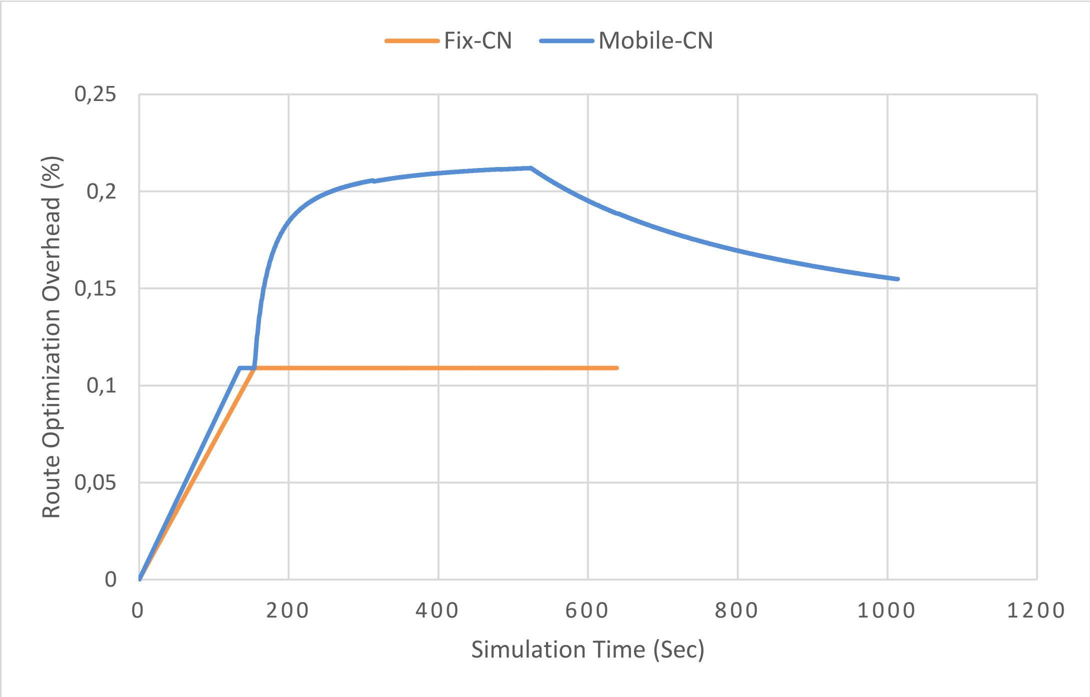

Figure 5.6. Route optimization overhead for video conference when route optimization enabled

5.2. Comparison of Scenarios in Non-Route Optimization

5.2.1. Delay variation

Figure 5.7 shows a delay variation of video conference application when no route optimization is enabled. It is clear that after 150 seconds of simulation time, the delay variation for these two scenarios was different. Even though there is a difference in delay variation, but this difference has a slight and approximately the same delay value for the entire simulations.

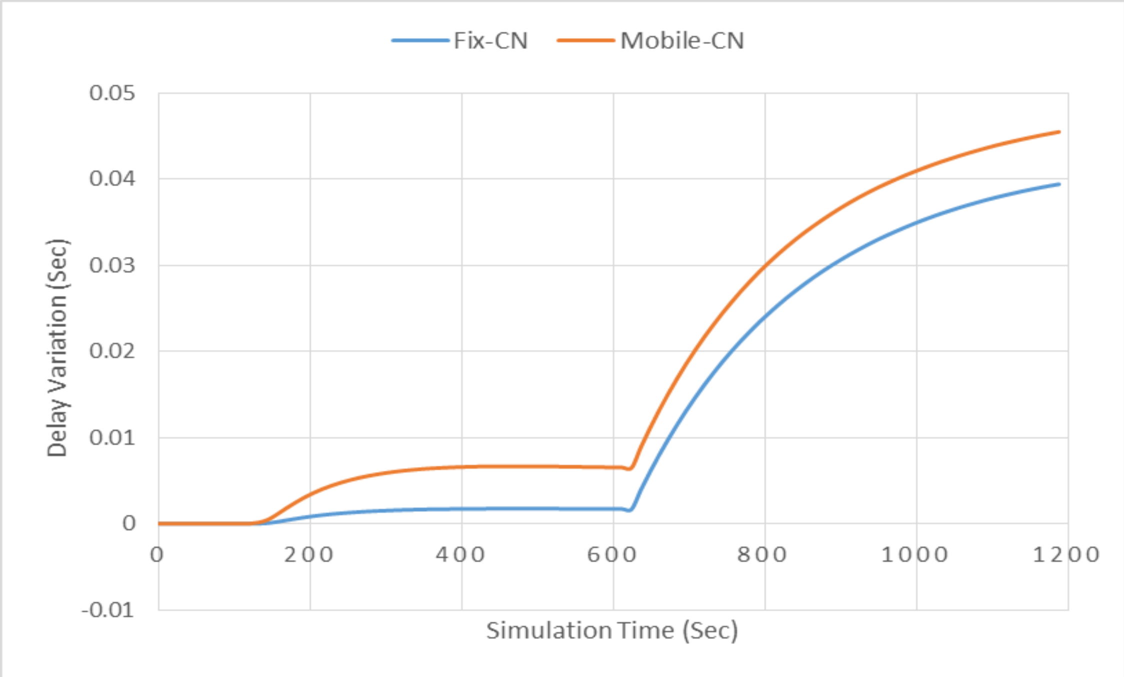

Figure 5.7. Delay variation for video conference when no route optimization enabled

5.2.2. End-to-End delay

Figure 5.8 shows end-to-end delay for roaming and fixed CN scenarios when no route optimization enabled. End to end delay for roaming is higher compared to fixed CN scenario. The end-to-end delay is higher even if the MN and CN are near to each other because a packet first have to pass HA then tunneled to MN and CN. With a scenario of fixed CN, only packet tunneled are in the MN node side. This feature reduces end-to-end delay in some desirable amounts.

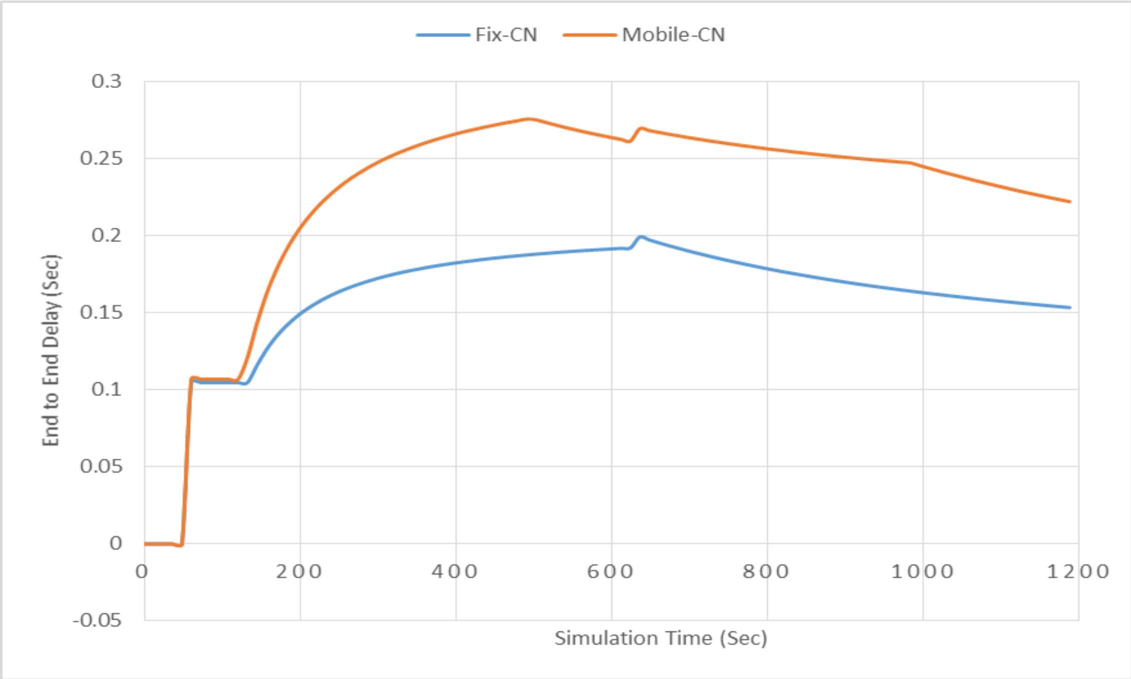

Figure 5.8. End-to-End delay for video conference when no route optimization enabled

5.2.3. Traffic received

Figure 5.9 shows packets received for video conference when no route optimization enable for roaming and fixed CN scenarios. As explained above, with roaming CN, the packet drops is more during the handover process. Since the hosts are not communicating directly as with route optimization enable, the packet has to pass first to HAs, which in some cases increases delay. However, the packet drop when all hosts perform handover process does not reach to maximum as in case of route optimization enabled.

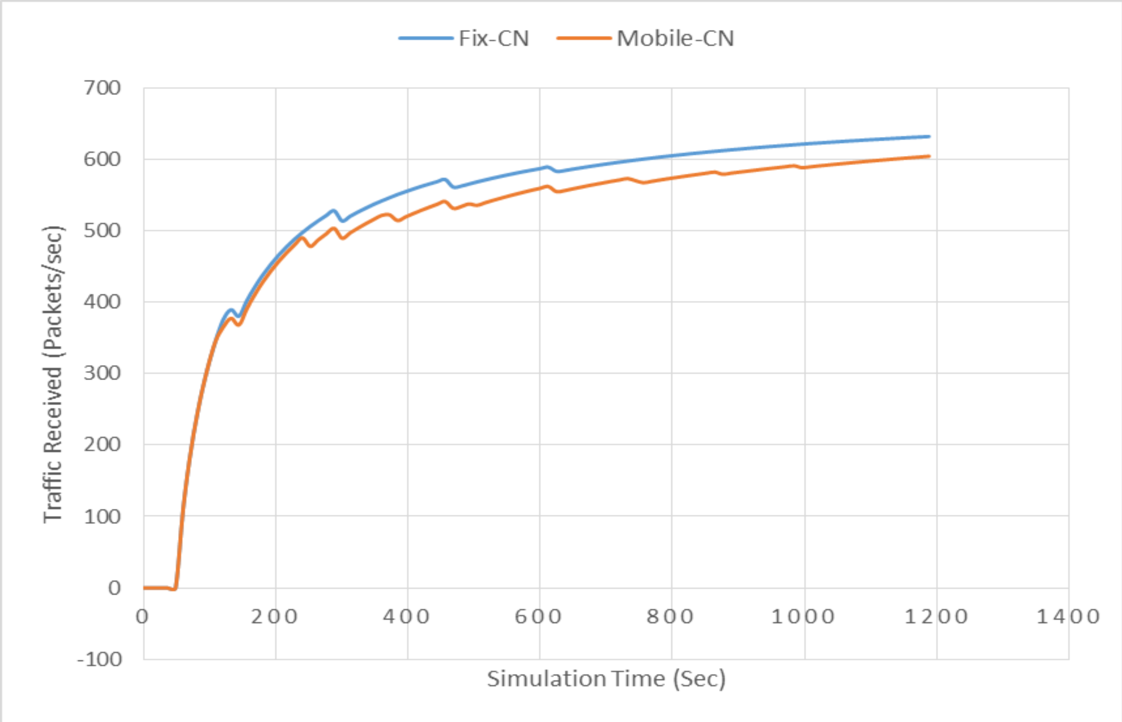

Figure 5.9. Packet received for video conference when no route optimization enabled

5.2.4. Control traffic received

Figure 5.10 shows control traffic received by MNs when no route optimization is enabled. As we can see in the first 160 seconds of simulation time, traffic control received was zero for all two-simulation scenarios. At this time all, the mobile nodes were at their home network. Thereafter, the traffic control of the two raised to 0.006 packets/second once after all handoff and fall to 0.003, 0.004, 0.005 and 0.003 packets/second in first, second, third and fourth handoff respectively for fixed CN while for roaming CN raises to 0.013 and fall back to 0.008 packets/sec. However, the value of control traffic received ranging between these values to the end of simulation time. During the decrease of control traffic, the control traffic decreased because the MNs was out of their home networks, but did not performing control signaling with their HA. This indicates that the handover performed by MNs does not influence control traffic in the mobile network especially when route optimization is not used.

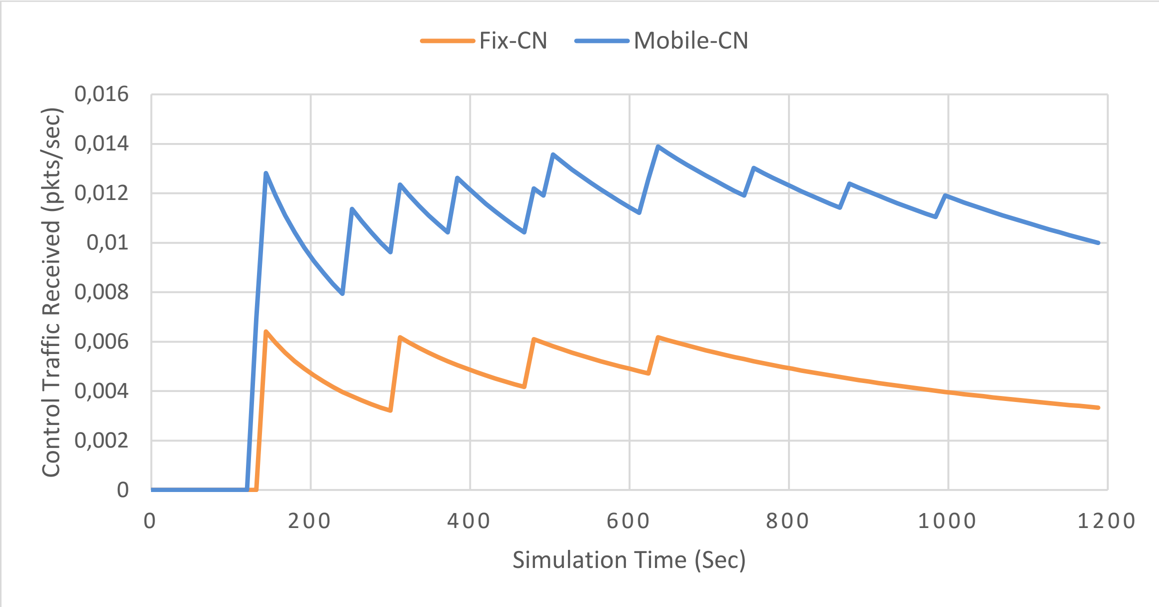

Figure 5.10. Control traffic received for video conference when no route optimization enabled

5.2.5. Tunneling overhead

Figure 5.11 shows a tunneling overhead in percentage when no route optimization is not active. As route optimization has not been activated then the MNs of both scenarios require the bidirectional tunneling method, in which they show an overload of inefficient packets when MN and CN are in movement. This is because, the packets of CNs had to be tunneled from HAs to MNs and are replied in the same tunnel from MNs to HAs. Since each tunneled packet used 40 bytes to route the packet to the other side of the tunnel. As a packet is tunneled twice to reach the destination, 80 bytes are consumed in two different communications if both MN and CN are roaming compared to 40 bytes when single node is roaming. Therefore, the overhead of roaming CN scenario becomes 0.09 higher for 375 seconds of simulation compared to fixed CN. The overhead of roaming CN become equal to 0.09% of fixed CN because MN1 was back to its home network, in this time only single node (CN) were roaming like in fixed CN scenario.

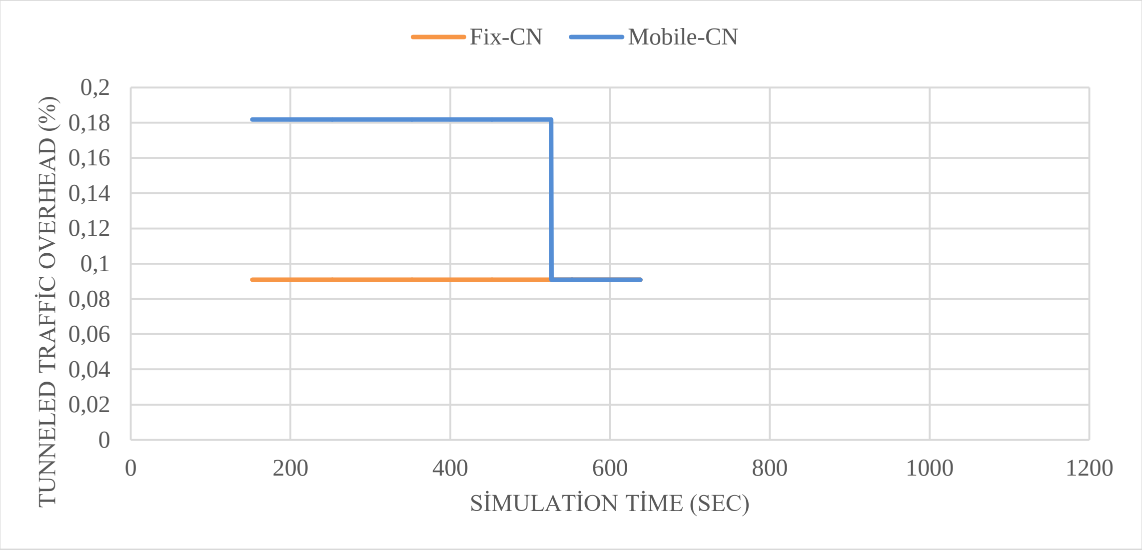

Figure 5.11. Tunneling overhead for video conference when no route optimization enabled

6. CONCLUSION

The current IPv6 mobility allows a mobile device to change its connection point to the Internet without losing sessions of the transport layer and higher layers. MN is always accessible by its HoA, which is an IPv6 address assigned to it on its home network. Even though MN is away from its home network, packets can still be forwarded to attached foreign network using the HoA. Therefore, the movement of a MN between networks is totally invisible through transport layer protocols and other higher layer protocols.

In this study, through simulation in OPNET Modeler 14.0, we evaluated the effects of fixed and roaming CN in MIPv6 networks when route optimization is enabled and when it is not enabled. Our result showed that, roaming CN has negative impact on the performance of Mobile Network, except in the end-to-end delay when route optimization is enabled. The good performance of end-to-end delay was achieved with a roaming CN because MN and CN were directly communicating to each other because they were near to each other. In this duration, the end-to-end delay was reduced significantly. The Delay Variation, Traffic Received, Control Traffic Received and Overhead especially during the handover process were due to mobility of CN and MN.

In analyzing our simulation study, we realize that MIPv6 communication network of a MN with a roaming CN incurred a negative impact in the network performance. To make this study more realistic, these effects might be studied, analyzed in real MIPv6 network environments. However, doing an in-depth analysis of different types of scenarios with sensitive application such as VoIP, video conferencing would be of great importance for the implementation of MIPv6 protocols. In fact, the results obtained in this study should be indicators for researchers to consider when considering mobility deployment of CN.

REFERENCES

1. Baddi, Y. and El Kettani, M. (2014, October). *Multiple active cores-based shared multicast tree for mobile IPv6 environment.* Paper presented at the Information Science and Technology (CIST), 2014 Third IEEE International Colloquium, Rabat, Morocco.

2. Faria, B. and Souto, E. (2014, November). *Performance analysis of Mobile IPv6 support for Dual Stack hosts.* Paper presented at the Computer Systems and Applications (AICCSA), 2014 IEEE/ACS 11th International Conference, Doha, Qatar.

3. Wiharti, W., Rimra, I. L., and Novid, I. (2015, October). *A comparative analysis and survey of handoff for VoIP applications in mobile IPv6 protocols.* Paper presented at the Information Technology, Computer, and Electrical Engineering (ICITACEE), 2015 2nd International Conference, Tembalang Semarang, Indonesia.

4. Kumar, M. and Jaffery, Z.A. (2012). A New Mobility Model for Multimedia Networks. *International Journal of Computer Science and Network Security*, 12(9), 107.

5. Tripathi, A.K., Radhakrishanan, R. and Lather, J.S. (2014, February). *Impact of wireless link delay on handover latency in Mobile IPv6 environment.* Paper presented at the Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference, Ghaziabad, India.

6. Internet: Arkko, J., Johnson, D.B. and Perkins, C.E. (2004). Mobility support in IPv6. URL: http://www.webcitation.org/query?url=https%3A%2F%2Ftools.ietf. org%2Fhtml%2Frfc6275&date=2017-09-28, Last Access Date: 21.08.2017.

7. Adibi, S., Naserian, M. and Erfani, S. (2005, May). *Mobile-IP MPLS-based networks.* Paper presented at the Electrical and Computer Engineering, 2005, Canadian Conference, Saskatoon, Canada.

8. Toshniwal, S.V. and Barbudhe, V.K. (2016). Mobile IPV6 route optimization. *International Journal of Engineering Science*, 6(12), 3575- 3577.

9. Lee, K., Park, J. and Kim, H. (2003, October). R*oute optimization for mobile nodes in mobile network based on prefix delegation*. Paper presented at the Vehicular Technology Conference, 2003. VTC 2003-Fall, Orlando, United States.

10. Papadimitratos, P., De La Fortelle, A., Evenssen, K., Brignolo, R. and Cosenza, S. (2009). Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation. *The Institute of Electrical and Electronics Engineers Communications Magazine*, 47(11), 737-751.

11. An, Y.Y., Yae, B. H., Lee, K.W., Cho, Y.Z. and Jung, W.Y. (2006, April). *Reduction of handover latency using MIH services in MIPv6.* Paper presented at the Advanced Information Networking and Applications, 2006. AINA 2006. 20th International Conference, Vienna, Austria.

12. Choi, J. I., Seo, W. K. and Cho, Y. Z. (2015). Efficient network mobility support scheme for proxy mobile IPv6. *The European Association for Signal Processing Journal on Wireless Communications and Networking*, 2015(1), 210.

13. Internet: Schmidt, T.C. and Wählisch, M. (2004). Roaming Real-Time Applications-Mobility Services in IPv6 Networks. URL: http://www.webcitation.org/query?url=https%3A%2F%2Farxiv.org%2Fftp%2Fcs%2Fpapers%2F0408%2F0408002.pdf&date=2017-11-30, Last Access Date: 11.09.2017.

14. Zohra, F.T., Azam, S. and Rahman, M.M. (2014). Overview of IPv6 mobility management protocols and their handover performances. *International Journal of Computer Science International Journal of Computer Science and Engine and Engineering*, 2(3), 125-133.

15. Bernardos-Cano,C. J., Soto-Campos, I., Calderón-Pastor, M., von Hugo, D. and Riou, E. (2005). Nemo: Network mobility in ipv6. *IPv6 More than A Protocol*, 6(2), 36.

16. Montavont, N., Noel, T. and Ernst, T. (2004, January). *Multihoming in nested mobile networking*. Paper presented at the Applications and the Internet Workshops, 2004. SAINT 2004 Workshops. 2004 International Symposium, Tokyo, Japan.

17. Liu, C.Y., Leu, F.Y. and Liu, J.C. (2014, November). *S-PMIPv6: Efficient handover of proxy mobile IPv6 by using SCTP*. Paper presented at the Broadband and Wireless Computing, Communication and Applications (BWCCA), 2014 Ninth International Conference, Guangzhou, China.

18. Lee, J.H., Bonnin, J.M., You, I. and Chung, T.M. (2013). Comparative handover performance analysis of IPv6 mobility management protocols. *The Institute of Electrical and Electronics Engineers Transactions on Industrial Electronics*, 60(3), 1077-1088.

19. Dong, P., Zhang, H., Luo, H., Chi, T.Y. and Kuo, S.Y. (2010). A network-based mobility management scheme for future Internet. *Computers and Electrical Engineering*, 36(2), 291-302.

20. Internet: Arkko, J., Johnson, D. B. and Perkins, C. E. (2011). Mobility support in IPv6. URL: http://www.webcitation.org/query?url=https%3A%2F%2Ftools.ietf.org%2Fhtml%2Frfc6275&date=2017-09-28, Last Access Date: 18.09.2017.

21. Internet: Narten, T., Thomson, S. and Jinmei, T. (2007). *IPv6 stateless address autoconfiguration.* URL: http://www.webcitation.org/query?url=https%3A%2F%2Fbuildbot.tools.ietf.org%2Fhtml%2Frfc4862&date=2017-09-28 S, Last Access Date: 11.09.2017.

22. Internet: Thomson, S. (2007). *IPv6 stateless address autoconfiguration*. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fbuildbot.tools.ietf.org%2Fhtml%2Frfc4862&date=2017-08-28, Last Access Date: 11.09.2017.

23. Senie, D. and Ferguson, P. (2000). *Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing.* United States: Association for Computing Machinery Digital Library

24. Internet: Aura, T. and Arkko, J. (2002). MIPv6 BU attacks and defenses," *Work in Progress.* URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.arkko.com%2Fpublications%2Fdraft-aura-mipv6-bu-attacks-01.txt&date=2017-09-15, Last Access Date: 11.09.2017.

25. Roe, M., Aura, T., O'Shea, G. and Arkko, J. (2002). *Authentication of mobile IPv6 binding updates and acknowledgments.* Fremont: Internet Engineering Task Force.

26. Savola, P. (2002). Security of IPv6 routing header and home address options. *Work in Progress*, 5, 1-13.

27. Internet: Arkko, J., Aura, T., Montenegro, G., Nordmark, E., and Nikander, P. (2005). *Mobile IP version 6 route optimization security design background*. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.ietf.org%2Frfc%2Frfc4225.txt&date=2017-10-28 Son Erişim Tarihi: 15.09.2017, Last Access Date: 11.09.2017.

28. Sulander, M., Hamalainen, T., Viinikainen, A. and Puttonen, J. (2004, May). *Flow-based fast handover method for mobile IPv6 network.* Paper presented at the Vehicular Technology Conference, 2004. VTC 2004-Spring. Milan, Italy.

29. Ren, K., Lou, W., Zeng, K., Bao, F., Zhou, J. and Deng, R.H. (2006). Routing optimization security in mobile IPv6. *Computer Networks*, 50(13), 2401-2419.

30. Chen, Y.C. and Yang, F.C. (2009). An efficient MIPv6 return routability scheme based on geometric computing. *Proceedings of World Academy of Science, Engineering and Technology*, 39, 238-243.

31. Chiba, T., Yokota, H., Dutta, A., Chee, D. and Schulzrinne, H. (2008, December). *Route optimization for proxy mobile IPv6 in IMS network.* Paper presented at the Signal Processing and Communication Systems, 2008. ICSPCS 2008, 2nd International Conference, Gold Coast, Australia.

32. Shah, P.A., Hasbullah, H.B., Lawal, I.A., Aminu Mu'azu, A. and Tang Jung, L. (2014). A TOTP-based enhanced route optimization procedure for mobile IPv6 to reduce handover delay and signalling overhead. *The Scientific World Journal*, 2014, 16.

33. Prakash, A., Verma, R., Tripathi, R. and Naik, K. (2009, December). *A mobile IPv6 based route optimization scheme for mobile networks.* Paper presented at the 2009 Annual IEEE India Conference (INDICON), Ahmedabad, India.

34. Internet: Le, D., Fu, X. and Hogrefe, D. (n.d.). Evaluation of Mobile IPv6 Based on an OPNET Model. *Network*, *1*, 2. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fpdfs.semanticscholar.org%2F2b3f%2F315cd2b66ac8c069794d344f10cc576de523.pdf&date=2017-09-15, Last Access Date: 10.10.2017.

35. Barbudhe, A.K., Barbudhe, V.K. and Dhawale, C. (2014, October). *Comparative analysis of security mechanism of mobile IPv6 threats against binding update, Route Optimization and Tunneling.* Paper presented at the Adaptive Science & Technology (ICAST), 2014 IEEE 6th International Conference, Ota (Near Lagos), Nigeria.

36. Modares, H., Moravejosharieh, A., Keshavarz, H. and Salleh, R. (2012, November). *Protection of binding update message in Mobile IPv6.* Paper presented at the Computer Modeling and Simulation (EMS), 2012 Sixth UKSim/AMSS European Symposium, Valletta, Malta..

37. Lee, D. C. and Kim, K.J. (2014, October). *Improved Authentication Scheme of Binding Update Protocol in Mobile IPv6 Networks*. Paper presented at the IT Convergence and Security (ICITCS), 2014 International Conference, Beijing, China.

38. Qiu, Y., Bao, F. (2010, July). *Authenticated binding update in Mobile IPv6 networks.* Paper presented at the Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference, Chengdu, China.

39. Internet: Arkko, J., Johnson, D. B. and Perkins, C. E. (2004). *Mobility support in IPv6.* URL: http://www.webcitation.org/query?url=https%3A%2F%2Ftools.ietf.org%2Fhtml%2Frfc6275&date=2017-06-28, Last Access Date: 10.10.2017.

40. Gu, Z., Yang, D. and Kim, C. (2004). *Mobile IPv6 extensions to support nested mobile networks.* Paper presented at the Advanced Information Networking and Applications, 2004. AINA 2004. 18th International Conference, Fukuoka, Japan.

41. Muthut, S., Ong, B.L., Zahri, N. and Ahmad, R.B. (2015). An overview of performance enhancement of FHMIPv6 on wireless mesh network. *International Journal of Future Computer and Communication*, 4(3), 160-164.

42. Ho, C.K., Oostveen, J. and Linnartz, J.P. (2008, November). *Rate adaptation using acknowledgement feedback: Throughput upper bounds.* Paper presented at the Global Telecommunications GLOBECOM 2008 - 2008 IEEE Global Communications Conference New Orleans, USA.

43. Wang, S., Cui, Y., Das, S. and Xu, M. (2008, May). *Optimized Mobile MPLS*. Paper presented at the Communications Workshops, 2008. ICC Workshops' 08. IEEE International Conference, Beijing, China.

44. Cabellos-Aparicio, A. and Domingo-Pascual, J. (2007, September). *Mobility Agents: Avoiding the Signaling of Route Optimization on Large Servers.* Paper presented at the Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium, Athens, Greece.

45. Tran-Trong, S., Tursunova, S. and Kim, Y. T. (2008). *Enhanced vertical handover in Mobile IPv6 with media independent handover services and advance duplicate address detection.* Paper presented at the KNOM Conference, Kyeongbuk, Korea.

46. Costa, X.P. and Hartenstein, H. (2002). A simulation study on the performance of Mobile IPv6 in a WLAN-based cellular network. *Computer Networks*, 40(1), 191-204.

47. Choi, J. S., Jung, B. G. and Kim, T.I. (2009). LMA initiated route optimization protocol for improving PMIP handover performance. *The Institute of Electrical and Electronics Engineers Communications Letters*, 13(11), 871–873.

48. Internet: Arkko, J., Haddad, W. and Vogt, C. (2007). Enhanced route optimization for mobile IPv6. URL: http://www.webcitation.org/query?url=https%3A%2F%2Ftools.ietf.org%2Fhtml%2Frfc4866&date=2017-06-17, Last Access Date: 10.10.2017.

49. Zolfagharnasab, H. (2012). Reducing packet overhead in mobile IPv6. *International Journal of Distributed and Parallel Systems,* 3(3), 1-8.

50. Le, D., Chang, J. (2010, June). *Tunnelling-based route optimization for mobile IPv6*. Paper presented at the Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference, Beijing, China.

51. Guan, J., You, I., Xu, C., Zhou, H. and Zhang, H. (2012, July). S*urvey on route optimization schemes for proxy mobile IPv6.* Paper presented at the Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference, Washington, United States.

52. Al Hawi, F., Yeun, C. Y. and Salah, K. (2013, August). *Secure framework for the return routability procedure in MIPv6.* Paper presented at the Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, Beijing, China.

53. Jia, W.K. (2014). A unified MIPv6 and PMIPv6 route optimization scheme for heterogeneous mobility management domains. *Computer Networks*, 75, 160-176.

54. Li, F. (2005, October). *A novel haleness and efficiency method for return routability procedure in mobile IPv6.* Paper presented at the Communications and Information Technology, 2005. ISCIT 2005. IEEE International Symposium, Beijing, China.

55. Rossi, A., Pierre, S. and Krishnan, S. (2013). Secure route optimization for MIPv6 using enhanced CGA and DNSSEC. *The Institute of Electrical and Electronics Engineers Systems Journal*, 7(3), 351-362.

56. Susanto, H. and Kim, B. G. (2009, August). *Per-connection return routability test in mobile IPv6.* Paper presented at the Network-Based Information Systems, 2009. NBIS'09. International Conference, Indiana, United States.

57. Internet: Ismail, M.D. and Mohamad, M.M. (2010). *An enhancement on mobile IPv6: A review.* URL: http://www.webcitation.org/query?url=http%3A%2F%2Fdinus.ac.id%2Frepository%2Fdocs%2Fjurin%2F15008.pdf&date=2017-06-17, Last Access Date: 10.10.2017.

58. Gohar, M., Koh, S. J., Um, T. W. and Lee, H. W. (2010, February). *Seamless multicast handover in PMIPv6-based wireless networks.* Paper presented at the Advanced Communication Technology (ICACT), 2010 The 12th International Conference, Gangwon-Do, Korea.

59. Lucio, G. F., Paredes-Farrera, M., Jammeh, E., Fleury, M. and Reed, M. J. (2003). Opnet modeler and ns-2: Comparing the accuracy of network simulators for packet-level analysis using a network testbed. *World Scientific and Engineering Academy and Society Transactions on Computers*, 2(3), 700-707.

60. Garrido, P.P., Malumbres, M.P. and Calafate, C.T. (2008, March). *ns-2 vs. OPNET: a comparative study of the IEEE 802.11 e technology on MANET environments.* Paper presented at the Proceedings of the 1st International Conference, Marseille, France.

61. Varga, A., Hornig, R. (2008, March). *An overview of the OMNeT++ simulation environment.* Paper presented at the Proceedings of the 1st International Conference, Marseille, France.

62. Pan, J. and Jain, R. (2008). A survey of network simulation tools: Current status and future developments. *Technical Report*, Washington, 45.

63. Di Caro, G. A. (2003). Analysis of simulation environments for mobile ad hoc networks. *Technical Report*, Manno, 26.

64. Li, H. and Lin, X. (2005, October). *An OPNET-based 3-tier network simulation architecture*. Paper presented at the Communications and Information Technology, 2005. ISCIT 2005. IEEE International Symposium, Beijing, China.

65. Mekkanen, M., Antila, E., Virrankoski, R. and Elmusrati, M. (2014). Using OPNET to model and evaluate the MU performance based on IEC 61850-9-2LE. *Procedia Computer Science*, 36, 72-79.

CURRICULUM VITAE

Personal Information

Surname, name	: DJASSI, Papa
Nationality	: Guinea-Bissau
Birth date and place	: 14.04.1988 Mansabá
Marital status	: Single
Tel	: 0553 587 7577
E-mail	: djassi.papa@gazi.edu.tr

Education

Degree	**Graduate School**	**Graduation date**
Master	Gazi University Computer Engineering, Engineering Faculty	Continuing
Bachelor's	Dakar Bourguiba University Computer Engineering, Faculty of Science and Technology	2013
High School	Liceu Dr. Rui Barcelos da Cunha	2008

Work Experience

Year	**Place**	**Work**
None	None	None

Foreign Languages

Portuguese, French, Turkish and English

International Conferences

1. Djassi, P. (2017). *Effect of fixed and roaming CN in MIPv6 networks.* 4th World Conference on Computer Engineering (COMENG-2017), İstanbul, Türkiye.

Hobbies

Reading, computer technologies, running, football and tennis.

GAZİ GELECEKTİR...