ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

Performance Analysis Of Mobile IPv6 Based On Opnet Model

Mutasim Abdel Gaffar Mohamed [1], Amin Babiker Abdel Nabi Mustafa [2]

1. MSc, Department of Computer Engineering, Faculty Of Engineering, Neelain, Khartoum, Sudan

2. Associate Professor, Department of Computer Engineering Faculty Of Engineering, Neelain, Khartoum, Sudan

Manuscript Info

Manuscript History:

Received: 25 September 2014
Final Accepted: 26 October 2014
Published Online: November 2014

Key words:

Mobile IPv6, MN,COA ,HA,CN, Opnet,

Corresponding Author

Mutasim AbdelGaffar Mohamed

Abstract

Internet Protocol IPv6 that provides a large number of addresses, and this protocol allow device roaming around the internet. Each mobile node is identified through a local address. During it's moving from home address there is care-of address that provides information about the Mobile node's current location. In this paper we analysis Mobile ipv6 performance through simulation software OPNET MODELER and we have to load a number of applications (E-mail, Telnet, Http, Ftp).and study effect light load and high load and found that the loss and delay and throughput,

Introduction

The protocol known as Mobile IPv6, allows a mobile node to move from one link to another without changing the mobile node's "home address". Packets may be routed to the mobile node using this address regardless of the mobile node's current point of attachment to the Internet. The mobile node may also continue to communicate with other nodes (stationary or mobile) after moving to a new link. The movement of a mobile node away from its home link is thus transparent to transport and higher-layer protocols and applications (1).

One can think of the Mobile IPv6 protocol as solving the network layer mobility management problem. Some mobility management applications -- for example, handover among wireless transceivers, each of which covers only a very small geographic area -- have been solved using link-layer techniques. For example, in many current wireless LAN products, link-layer mobility mechanisms allow a "handover" of a mobile node from one cell to another, re-establishing link-layer connectivity to the node in each new location (2).

I. OVERVIEW OF MOBILE IPV6

Mobile IPv6 is next generation protocol and in the near future, router are become more faster and new technology are going to reduce the internet delay (delay incurred in transmitting packets from on network to another) .Mobility support in IPv6 is particularly important ,as mobile computers are likely to account for a majority or at least a substantial fraction of the population of the internet during the life time of IPv6.The Mobile IPv6 protocol is just as suitable for mobility(3) across homogeneous media .For Example ,Mobile IPv6 facilitates node movement from one Ethernet segment to anther as well as it facilitates node movement from an Ethernet segment to a wireless LAN cell, with mobile nodes IP address remaining unchanged in spite of such movement.

II. MOBILE IPV6 COMPONENT

Mobile Node (MN): A host or router that changes its point of attachment from one network or subnet work to another. A mobile node may change its location without changing its IP address; it may continue to communicate with other Internet nodes at any location using its (constant) IP address, assuming link-layer connectivity to a point of attachment is available(4).

Correspondent Node (CN): Any node that communicates with the mobile node. Note that the terms "mobile" and "correspondent" nodes refer to certain functions within an IPv6 node. Therefore, a mobile node can also be a correspondent node, and vice versa, depending on the context. For instance, a host can be seen as a correspondent node by the mobile (moving) node it communicates with. At the same time, the correspondent node might also move, which makes it a mobile node (because it is moving) while being seen as a correspondent node by its mobile peer.

Home address: A stable address that belongs to the mobile node and is used by correspondent nodes to reach mobile nodes. Like all IPv6 addresses, the home address is based on the 64-bit prefix assigned to the ***home link*** combined with the mobile nodes interface identifier. A mobile node can have more than one home address. IP Packets addressed to the home address are routed to the home link using standard routing protocols.

Home link: A link to which the home address prefix is assigned(5).

Home Agent (HA): A router located on the home link that acts on behalf of the mobile node while away from the home link. The ***home agent*** redirects packets addressed to a mobile node's home address to its current location (care-of address) using IP in IP tunneling. **Foreign link(6):** Any link (other than the home link) visited by a mobile node. Care-of address: An address that is assigned to the mobile node when located in a foreign link. of the foreign link combined with the mobile node's interface identifier. There is no special format for a care-of address; it is a norm a unicast IPv6 address. This address identifies the current location of the mobile node. Binding: The association of the mobile node's home address with a care-of address for a certain period of time. That is, between the stable home address and the mobile node's current location. This allows the home agent (post office) to forward packets to the mobile node's current location. The binding is refreshed (if the timer expires) or updated when the mobile node gets a new care-of address (because it moved to a new link). Binding cache(7): A cache stored in volatile memory containing a number of bindings for one or more mobile nodes. A binding cache is maintained by both the correspondent node and the home agent. Each entry in the binding cache contains the mobile node's home address, care-of address, and the lifetime that indicates the validity of the entry. When the binding cache is maintained by correspondent nodes, Binding Update List (BUL): A list maintained by the mobile node in volatile memory. This list contains all bindings that were sent to the mobile node's home agent and correspondent nodes. This list is maintained in order for the mobile node to know when a binding needs to be refreshed and is also used for selecting the right care-of address when communicating directly with a correspondent node(8).

III. MOBILE IPV6 BASIC OPERATION

In MIPv6, each Mobile Node (MN) is identified with a static IPv6 address called home address. The MN can always be reached using the fixed home address. When a MN is on its home link, it acts as a fixed host; When the MN is attached to a foreign link, it requires a new Care of Address (CoA). The CoA provides information about the MN's current location, so the HA or CN shall map the home address to its corresponding currently CoA by binding mechanism for location management and packets routing. The MN registers the CoA with the HA (i.e. home registration), and it may also inform the acquired CoA to CNs (i.e. correspondent registration). There are two possible routing mechanisms between the MN and the CN. The first is bidirectional tunneling, which does not require MIPv6 support from the CN. The second is route optimization, which requires the MN to register its current CoA binding at the CN. Therefore, packets from the CN can be routed directly to the CoA of MN. The basic sequences of communication and interactions between entities for the two routing mechanisms are depicted in figure 1(9).

The following subsections detail the major functional elements operation of MIPv6 that make use of MIPv6 features (9).

Movement Detection:-

When a MN moves, it must detect its current location. In MIPv6, a MN can determine its current location by listening to the router advertisements and comparing the network prefix of the source address within this advertisement with the network prefix of its home link. If the network prefix of the source address within the router advertisement equals the network prefix of the home address of MN, then the MN is on its home link. Otherwise the MN is on a foreign link(11).

Acquisition of the CoA:-

When a MN attaches to a foreign link, it will need to acquire a new CoA. To obtain a CoA, the MN can use either stateful or stateless address auto-configuration methods. In the first situation, the MN obtains a CoA from a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [6] server. In the latter situation, by using the Neighbour Discovery protocol [3], a MN is able to find the network prefix at any point of attachment that it might select and then adds a unique interface identifier to form a CoA for that point of attachment. After a CoA is obtained or formed, it must be checked whether this is a unique address or not by duplicate Address Detection (DAD) mechanism (12)

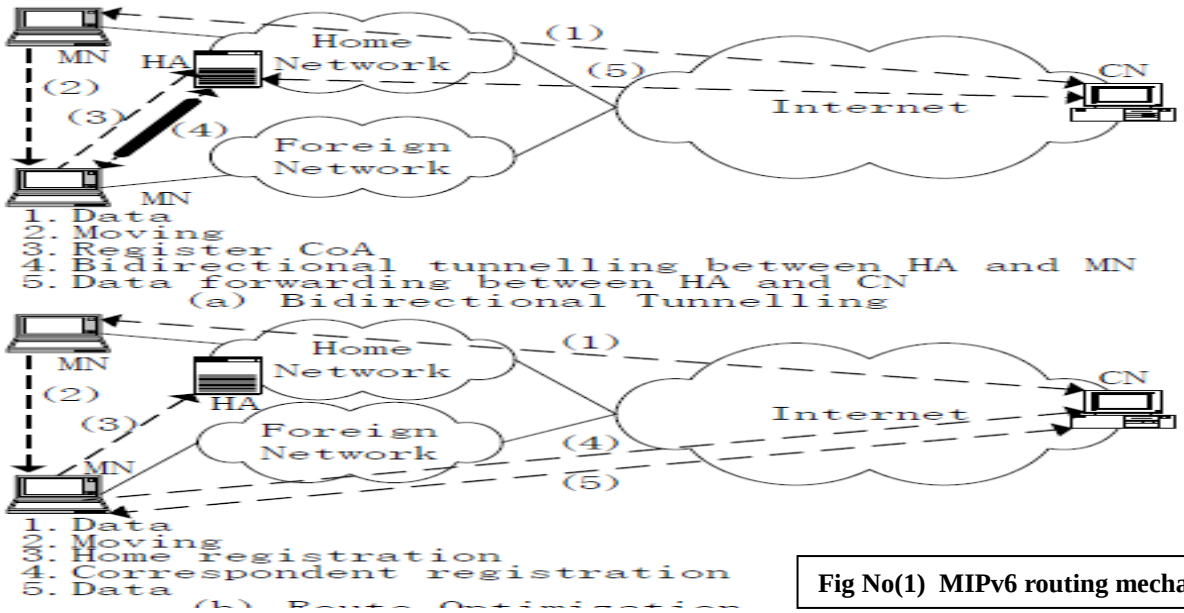


Fig No(1) MIPv6 routing mechanisms

Registration and Binding Management:-

When a MN moves to a foreign link and acquires a CoA, it then registers to the HA or CNs in its list to inform them of its current location by using the IPv6 Mobility header [2]. Mobility header messages related to the management of bindings include Binding Update message(, Binding Acknowledgement message, Binding Refresh Request message etc. The MN performs the binding registration by sending a Binding Update message to the HA or CNs. The HA or CNs reply to the MN by returning a Binding Acknowledgement message. In the correspondent registration, as a part of this procedure, a return rout ability test is performed in order to authorize the establishment of the binding. The Binding Refresh Request message is mainly used to refresh binding when nearing the end of the current binding lifetime.

(4) Location Tracing and Packets Routing(13)

Finally, after registering and binding, the CN can trace the MN and route packets to it continuatively. In bidirectional tunnelling mechanism, Packets from the CN to the MN are routed to the home address of MN, the HA shall uses proxy Neighbour Discovery [3] to intercept any IPv6 packets addressed to the MN's home address on the home link. Each intercepted packet is tunnelled to the MN's current CoA. Packets to the CN are tunnelled from the MN to the HA, which is called reverse tunnelling, and then routed normally from the home network to the CN (see figure 1, a)(14).

In route optimization, the HA no longer exclusively deals with the address mapping, but each CN can have its own binding cache. In the direction from the MN to the CN, packets sent by the MN are delivered to the CN with the Home Address option in the Destination Option Extension header when the MN is away from its home network. In this case, the MN sets the IPv6 header's source address as its CoA and adds a Home Address option with the MN's home address to IPv6 header. When the CN receives the packet from the MN, it replaces the MN's home address to be the IPv6 header's source address before delivering the packet to the upper layer. This way, the MN not only keeps mobility transparent to its upper software, but also passes the packet through any router implementing ingress filtering [8]. In the opposite direction, when sending packets to the MN, the CN checks its cached bindings for an entry for the packets' destination address. If a cached binding for this destination address is found, the CN uses Type

2 Routing header to route packets to the MN by specifying the CoA as the destination address in IPv6 header and the MN's home address as the final destination in the Routing header. When the MN receives packets , the MN processes this Routing header and delivers packets to the upper layer using the MN's home address as if the MN was at home (see figure 1, b). If a cached binding for this destination address is not found, for examples the binding is timeout or the CN originates a communication with the MN etc., the CN does not know the current location of MN. In this case, it shall send packets using the MN's home address as destination address. The MN's HA will intercept the packets and tunnels them to the current location of MN (see figure 1, a). When the MN receives packets from its HA, it knows that the CN is not aware of its current CoA and will inform the CN of the current CoA by sending a Binding Update message to the CN, so that the CN later can send packets to the MN directly (15).

IV. ARCHITECTURE OF MIPv6 AND EXPERIMENTAL RESULTS :-

Objective:-

To show the traffic overhead produced by Mobile IPv6 mechanisms in a network with 37 mobile nodes that are randomly moving across various access points.

* Configuration *

All nodes run four applications simultaneously: HTTP, Email, Telnet and FTP.

Nine access points are placed across the network. Initially each access point serves 4 mobile nodes, for which the initial access point will be their Home Agent.

Four wireless domains define the area of mobility for the mobile nodes. Each mobile node is restricted to move across four access points, maximum.

Two mobiles (MN_0A and MN_6B), have been set to follow fixed trajectories across all nine access points. These two run a heavier loaded version of the applications mentioned above.

* Results *

The statistics show three main aspects of the dynamics of the simulation:

1) Application traffic.

-Performance of the applications can be observed.

2) Mobile IPv6 traffic.

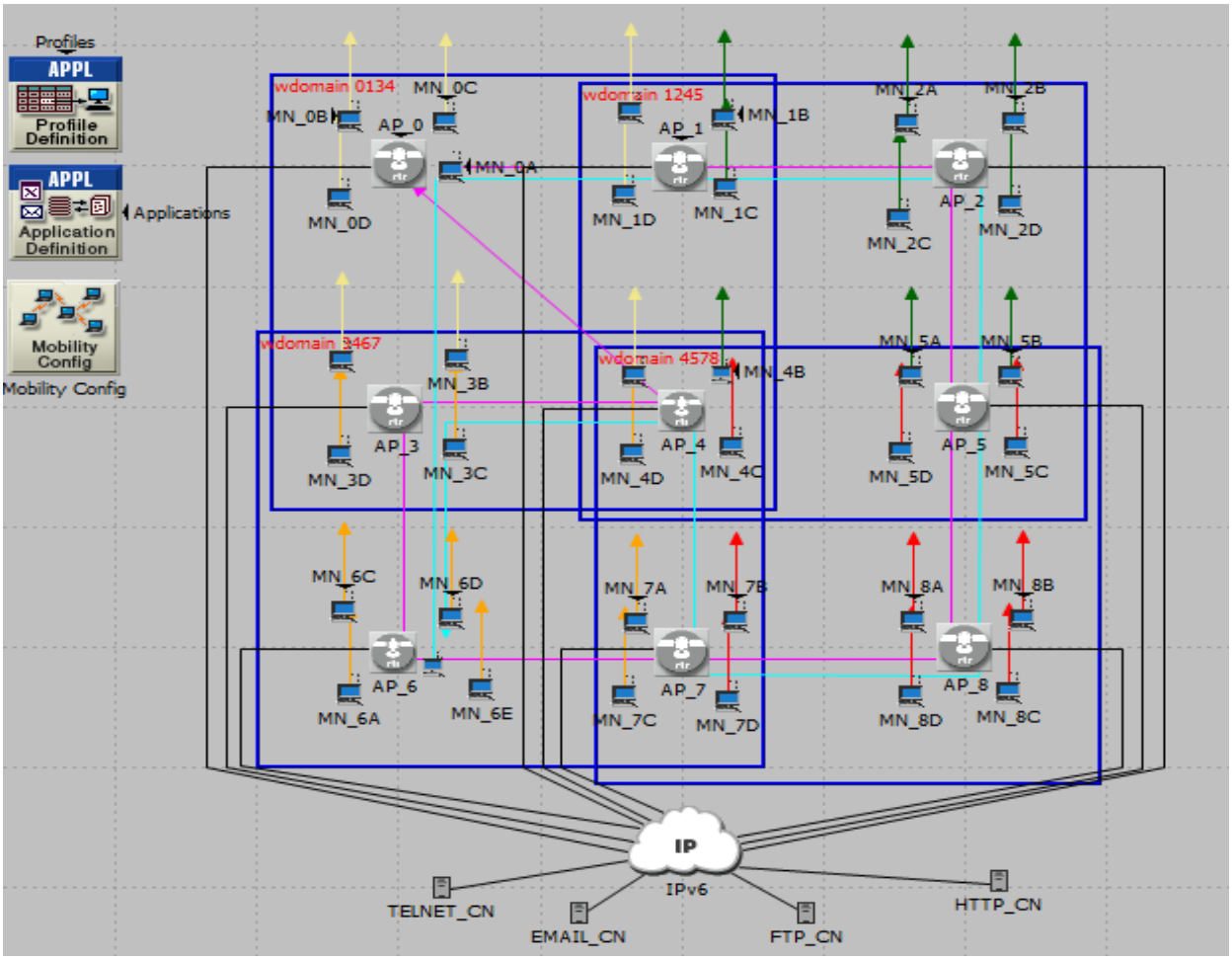
-Control traffic generated by MIPv6 (mobile IPv6 mobility messages)

-The time that takes to a mobile to bind with its Home Agent is measured.

-Overhead due to MIPv6 mechanisms also shown: route optimization and tunneled traffic.

3) Visited access points.

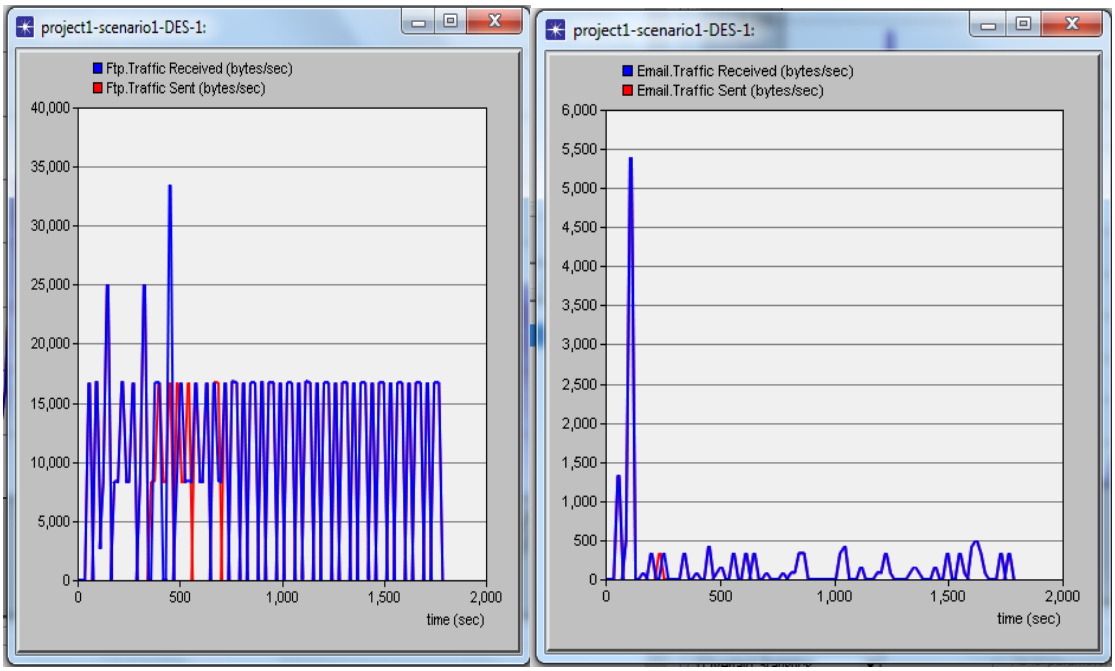
-The different networks (access points) visited by the mobile nodes can be observed (MN_0A and MN_6B visited access points shown).



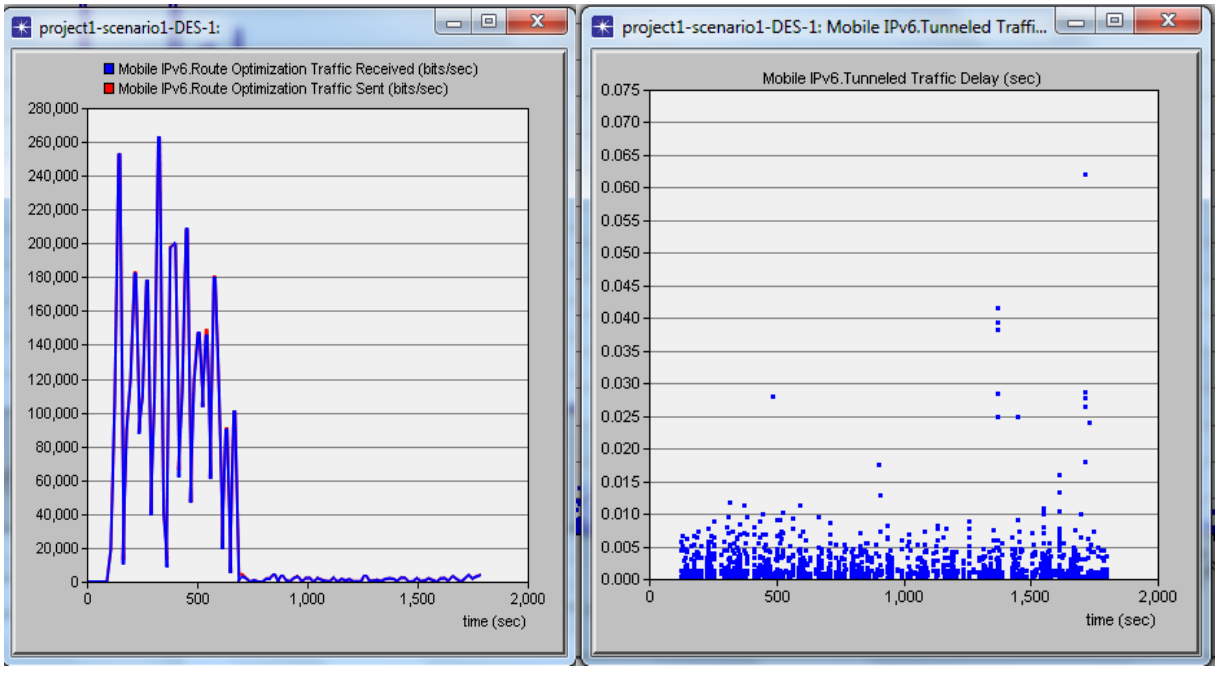
a. **Architecture of MIPv6 in opnet**

Fig. 2. :- **Architecture of MIPv6**

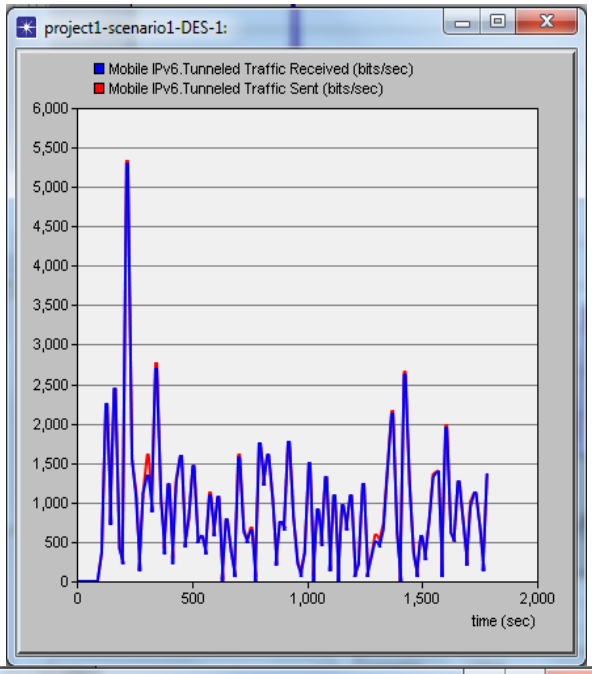
Results and analysis:-

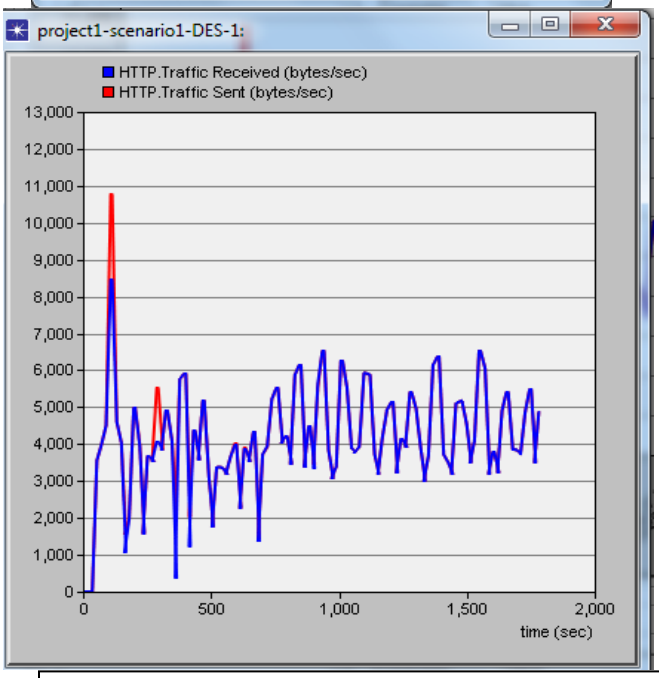

project1-scenario1-DES-1:
Ftp.Traffic Received (bytes/sec)
Ftp.Traffic Sent (bytes/sec)
40,000
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
0
500
1,000
1,500
2,000
time (sec)
project1-scenario1-DES-1:
Email.Traffic Received (bytes/sec)
Email.Traffic Sent (bytes/sec)
6,000
5,500
5,000
4,500
4,000
3,500
3,000
2,500
2,000
1,500
1,000
500
0
0
500
1,000
1,500
2,000
time (sec)

(a) **(b)**

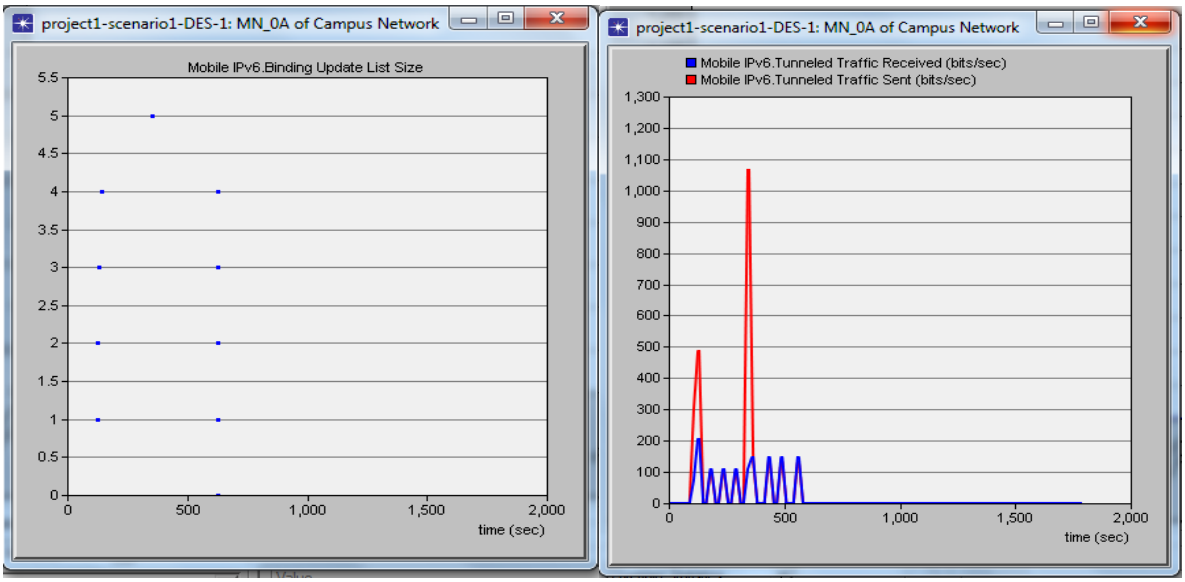

project1-scenario1-DES-1:
Mobile IPv6.Route Optimization Traffic Received (bits/sec)
Mobile IPv6.Route Optimization Traffic Sent (bits/sec)
280,000
260,000
240,000
220,000
200,000
180,000
160,000
140,000
120,000
100,000
80,000
60,000
40,000
20,000
0
0
500
1,000
1,500
2,000
time (sec)
project1-scenario1-DES-1: Mobile IPv6.Tunneled Traffi...
Mobile IPv6.Tunneled Traffic Delay (sec)
0.075
0.070
0.065
0.060
0.055
0.050
0.045
0.040
0.035
0.030
0.025
0.020
0.015
0.010
0.005
0.000
0
500
1,000
1,500
2,000
time (sec)

(c) (d)

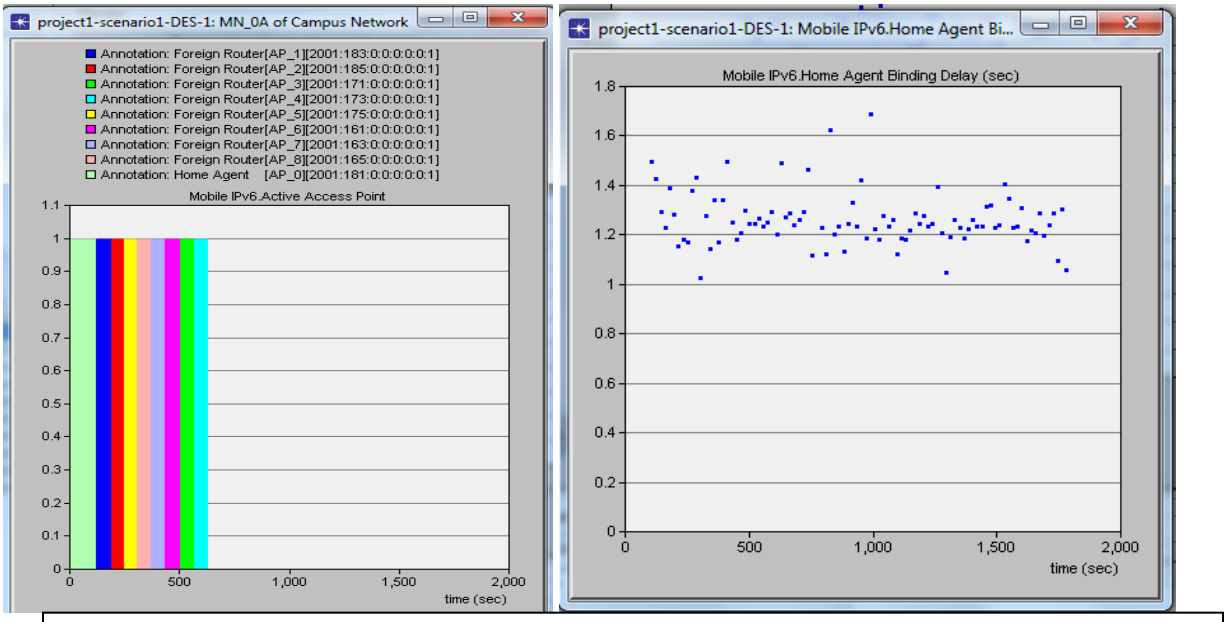

project1-scenario1-DES-1:
Mobile IPv6.Tunneled Traffic Received (bits/sec)
Mobile IPv6.Tunneled Traffic Sent (bits/sec)
6,000
5,500
5,000
4,500
4,000
3,500
3,000
2,500
2,000
1,500
1,000
500
0
0
500
1,000
1,500
2,000
time (sec)


project1-scenario1-DES-1:
HTTP.Traffic Received (bytes/sec)
HTTP.Traffic Sent (bytes/sec)
13,000
12,000
11,000
10,000
9,000
8,000
7,000
6,000
5,000
4,000
3,000
2,000
1,000
0
0
500
1,000
1,500
2,000
time (sec)

(e) (f)



(g) (h)



(i) (j)

Fig. 3 OPNET simulation result (a) ftp (send & receive) (b)E-mail sent and receive (c)Mobile IPv6 route optimization(sent &receive) (d)mobile IPv6.tunneled traffic. Delay (e)Mobile IPv6 tunnelled (sent & receive) (f)HTTP traffic (sent & receive) (g)Mobile IPv6 binding update size (h)MobileIPv6 tunnelled (sent & receive)(MN-0A) (i) Mobile IPv6 Active Access point (MA-0A)(j) Mobile Home Agent Binding Delay

In fig.3 (a) the video conferencing traffic received statistics, from which some gaps in the communication can be observed. Each gap is produced every time the MN changes its current AR triggering MIPv6 registration/binding procedures to notify its HA and its CN of the new CoA. While the registration/binding procedures update the HA and the CN, all application traffic directed to the MN will be interrupted.

In fig.3 (g) this refers to size of binding update for all MIPv6 network

In fig.3 (j) this is delay for MN when communicated with CN .it need binding to complete handover

In fig.3 (I) we observe the different networks (ARs) visited by the MN during moving. The bar in the graph represents an AR visited by the MN, the bar width represents the time the MN used the AR until it moves to a different one. We can see that the data traffic switch inter the different ARs when the MN moves with ongoing communication.

In fig.3 (c) the Route Optimization Overhead (%) represents the traffic overhead ratio due to addition of IPv6 Extension headers, when sending data traffic using MIPv6 route optimization mechanism.
-all the results indicate that there is progress in mobile networks is better in MIPV6 than MIPv4
-has confirmed that all of the studies and the results show that the new protocol despite delays that gets to where he is able to satisfy every user

V. CONCLUSION

This paper described the MIPv6 technology and presented the MIPv6 model of OPNET simulator. Besides, using the simulator, we assessed the MIPv6 test bed. We observed the application traffic and visited ARs of MN during moving, the application responses time was measured in different routing mechanisms, and we demonstrated the adverse effect of handover procedure of MIPv6 on the congestion control in the transport layer. We also evaluate the impact of MIPv6 signalling in different routing mechanisms. The simulation and results of our test bed have been performed and demonstrated to show how to model real networks and provide some insights in the influence of the protocols on application traffic. Therefore, we will focus on the protocol enhancement including smooth handover, improvement of congestion control and signalling optimization etc. in the further work.

REFERENCES.

[1] Deering, S., and B. Zill, “Redundant Address Deletion when Encapsulating IPv6 in IPv6,” draft-deering-ipv6-encap-addr-deletion-00, work in progress, November 2001.
[2] Draves, R., “Default Address Selection for Internet Protocol version 6 (IPv6),” RFC 3484, February 2002.
[3] Eastlake, D., “Domain Name System Security Extensions,” RFC 2535, March 1999.
[4] Johnson, D., C. Perkins, and J. Arkko, “Mobility Support in IPv6,” draft- mobile ip- ipv6-24, work in progress, June 2003.
[5] Knight, S., et al., “Virtual Router Redundancy Protocol,” RFC 2338, April 1998.
[6] Nordmark, E., “MIPv6: From Hindsight to Foresight?” draft-nor mark-mobile ip-
[7] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.
[8] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.
[9] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.
[10] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.
[11] Maughan, D., Schertler, M., Schneider, M. and J. Turner,"Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.
[12] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.
[13] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.
[12] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.
[13] Thomson, S. and T. Narten, "IPv6 Stateless Address Auto configuration", RFC 2462, December 1998.
[14] Conta, A. and S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 2463, December 1998.
[15] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.