Real-time Traffic Performance for WiFi Handovers over MIPv4 versus MIPv6

Ahmad H. Talaat
Electronics and Communications Dept., Ain Shams University
Cairo, Egypt

Nael A. Hussein
Dept. of Electrical and Communication Eng., British University in Egypt
Cairo, Egypt

Hussein A. Elsayed
Electronics and Communications Dept., Ain Shams University
Cairo, Egypt

Hadia Elhennawy
Electronics and Communications Dept., Ain Shams University
Cairo, Egypt

ABSTRACT
One of the major problems faced by different wireless networks nowadays, is the mobility. Inter-Radio Access Technologies handovers, roaming, and application continuity problems motivate the MIPv6 rather than MIPv4. This paper will cover the main benefits and drawbacks for the different mobile IPs via literal and simulation discussions. Using IPv4 tunnels to carry MIPv6 as a alternate will be discussed also, in case of not all-IPv6 network is used.

Keywords
MIPv4, MIPv6, IPv4 Tunnel, Wifi Handover, Route Optimization.

1. INTRODUCTION
Nowadays, Wireless networks are facing problems due to the most used network protocol IPv4, such as end of addresses capacity, and poor security and quality of service performances. In new wireless networks generations like Long Term Evolution (LTE) the fourth generation (4G), it needs an "always-on" connection for each user, because Circuit Switching (CS) is no longer used for Real-time connections (RT) such as Voice or Video applications, and it is alternated with the Packet Switching (PS) to handle the RT applications like Voice-over IP or Video-over IP technologies as a user plane protocol via the Session Initiation Protocol (SIP) as the control plane protocol; accordingly we have to dedicate a public IP for each single user. This approach is not possible with IPv4 because Network Address Translation (NAT) cannot handle these huge amounts of addresses.

Questions and challenges of the transition from IPv4 to IPv6 in all-IP 3G system is illustrated in [1], beside the main benefits and drawbacks of five different technologies including IPv4, IPv6, and IPv6 tunneled over IPv4.

Also, another major problem which is the mobility support for the network layer protocol; to handle the Inter Radio Access Technologies (Inter-RAT) handovers such as GSM, UMTS, LTE, WiMAX, and WiFi in such a seamless way.

We will cover the performance evaluation for different Mobile IP technologies; MIPv4, MIPv6 with Route Optimization, and MIPv6 over IPv4 tunnel on the handover process. Section 2 is the introduction for Mobile IP and IPv6 tunneling concepts. Section 3 will introduce the simulation model and test-benches used in comparison. Section 4 includes the different scenarios results, comparison and discussion as well.

2. MOBILE IP BACKGROUND

2.1 Mobile IP Need
In the past few years, the need network layer or Internet Protocol mobility is getting more important than before; the reasons behind that are illustrated in the following points below.

- Always on IP connectivity.

- Roaming between different RATs like; WiFi, WiMAX, UMTS, and LTE.

- Roaming between networks and sub-networks.

- Huge WLAN deployments mostly use different L3 subnets.

- Inter-network seamless handovers

- Application continuity (Session persistence).

- Static IP Addresses for mobile nodes.

- Mobile devices may act as servers.[2]

2.2 Mobile IP Concept
The mobile IP network consists of the following nodes as shown in
Figure 1.

Mobile Node (MN): an Internet-connected device whose location and point of attachment to the Internet may frequently be changed. It 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, as specified in [4].This kind of node is often a cellular telephone, handheld or laptop computer.

Home Agent (HA): A router on a mobile node's home network that maintains information about the device current location, as identified in its care-of address. The home agent uses tunneling mechanisms to forward Internet traffic so that the device's IP address doesn't have to be changed each time it connects from a different location.

Foreign Agent (FA): a router serving as a mobility agent for a mobile node. As specified in [4], a foreign agent works in conjunction with the home agent to support Internet traffic forwarding for a device connecting to the Internet from any location other than its home network.

Correspondent Node (CN): The device that the mobile node is communicating with as an end user such as a web server.
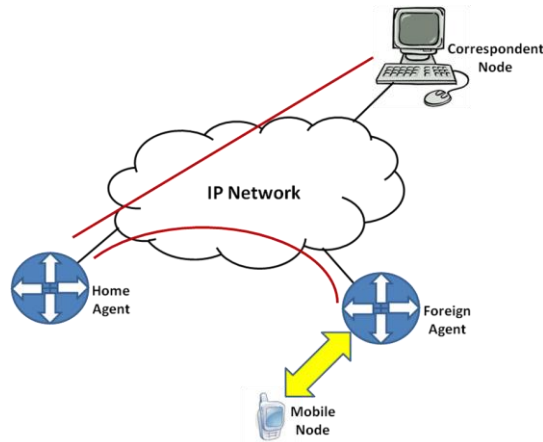
Figure 1 Mobile IP Network

To accomplish this, mobile IP established the visited network as a foreign node and the home network as the home node. Mobile IP uses a tunneling protocol to allow messages from the Packet Data Network (PDN) to be directed to the mobile node's IP address. This is accomplished by way of routing messages to the foreign node for delivery via tunneling the original IP address inside a packet destined for the temporary IP address assigned to the mobile node by the foreign node. The Home Agent and Foreign Agent continuously advertise their services on the network through an Agent Discovery process, enabling the Home Agent to recognize when a new Foreign Agent is acquired and allowing the Mobile Node to register a new Care of Address[3].

2.3 Mobile IPv4 versus Mobile IPv6

The major differences between Mobile IPv4 and Mobile IPv6 are:

- No special support is required from the local router in the case of Mobile IPv6. This allows it to operate in any location unlike the case of Mobile IPv4 which needs special routers known as "foreign agents"

- Instead of a nonstandard set of protocols, specific route optimization forms an essential part of the protocol.

- Pre-arranged security associations are not necessarily for the Mobile IPv6 route optimization to act securely. The route optimization is expected to be deployed on a global scale between all mobile nodes and correspondent nodes.

- Route optimization is allowed to coexist efficiently with routers that perform "ingress filtering". This could be achieved through the integrated support into the MIPv6. [8]

- The symmetric reach-ability between the mobile node and its default router in the current location could be assured through the IPv6 neighbor un-reach-ability detection.

- An IPv6 routing header is used for sending most packets to a mobile node being away from home in Mobile IPv6 rather than using IP encapsulation. This results in decreasing the amount of resulting overhead in comparison to Mobile IPv4.

- MIPv6 uses Neighbor Discovery as a substitute of ARP protocol which makes MIPv6 eliminates any linkage with any particular layer [7].[7]

- MIPv6 no more needs to manage tunneling due to the use of IPv6 encapsulation.

- The directed broadcast address discovery method used in MIPv4 returns separate responses from each router. The dynamic method in MIPv6 returns a single reply to the mobile node [4][5][6][7][8][9].

2.4 6to4 Tunneling

6to4 is a tunneling mechanism used to transfer IPv6 packets over an IPv4 infrastructure, typically the IPv4 Internet without the need to configure explicit tunnels. Special relay servers are also in place that allows 6to4 networks to communicate with native IPv6 networks.

6to4 is especially relevant during the initial phases of deployment to full, native IPv6 connectivity, since IPv6 is not required on nodes between the host and the destination. The 6to4 mechanism was created to support coexistence of both versions during the transition to IPv6, which is expected to take years.

6to4 may be used by an individual host, or by a local IPv6 network. When used by a host, it must have a global IPv4 address connected, and the host is responsible for encapsulation of outgoing IPv6 packets and de-capsulation of incoming 6to4 packets. If the host is configured to forward packets for other clients, often a local network, it is then a router.

6to4 performs three functions:

- Assigns a block of IPv6 address space to any host or network that has a global IPv4 address.

- Encapsulates IPv6 packets inside IPv4 packets for transmission over an IPv4 network.

- Routes traffic between 6to4 and "native" IPv6 networks [10][11].

3. SIMULATION MODEL

In this section we introduce our simulation model via different scenarios to compare the handover metrics (handover process directions, and duration) over different network layer techniques supporting mobility for IEEE 802.11b. The first subsection includes an overview on the logical process for Mobile IP for MIPv4, and MIPv6. The second subsection covers handover procedure over the three measurement scenarios MIPv4, MIPv6, and MIPv6 tunneled on IPv4 network. All simulations are done over OPNET 14.5. The used real-time application between MN and CN is voice codec G723.1 5.3 Kbps.

3.1 Mobile IP Handover over WiFi Networks

Firstly, we have to define the different technologies procedures and routes for Mobile IP Handover. The studied technologies are MIPv4, MIPv6 with route optimization, and MIPv6 tunneled over IPv4 network with route optimization. As shown in Figure 2 the simulation model used for coming results is based on a moving WiFi mobile traveling from its own home network whose HA is shown as HA_AP heading to a foreign network

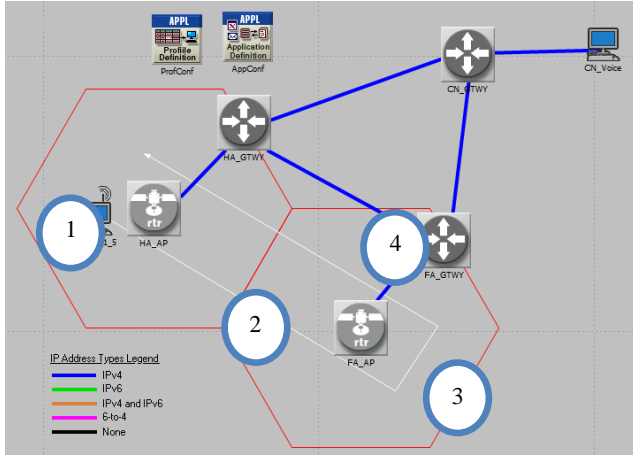whose FA is FA_AP, then the user travels back again to its home network.

Figure 2 Mobile Node movement test bench

The details for trajectories and the shown four steps in above figure used in simulation are shown in the following Table 1.

Table 1 Trajectories used in simulation

Step	Description
1.Before moving	Wait for 1 minute
2.While moving	Moving with 10 or 30 km/hr
3.Stop moving	Wait for 1 minute
4.Moving back	Moving with 10 or 30 km/hr

3.2 MIPv4

For MIPv4, it is expected that the route used in downlink case (user-wise) should pass by the HA in case of roaming is applied. On the other side, uplink direction is optimized that it is not passing through the HA in case of roaming.

While the mobile node is located at the home agent, it communicates with the correspondent node directly through the home agent gateway to correspondent node gateway connection in the uplink and the downlink. The routes directions in roaming case are shown in next network Figure 3.
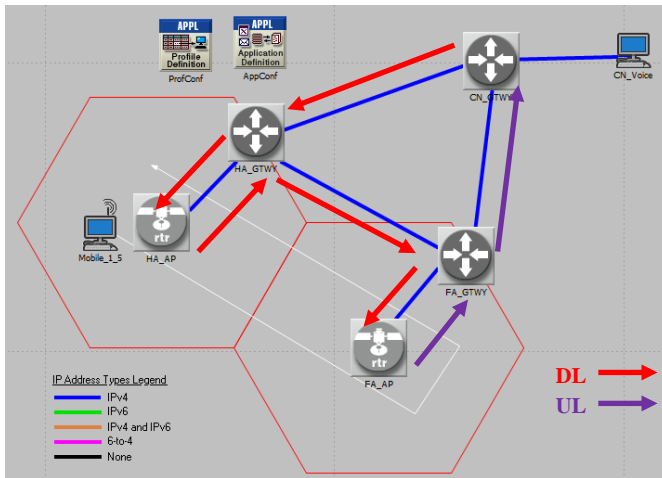

Figure 3 MIPv4 network

3.3 MIPv6

In MIPv6 case as shown in Figure 4, the route used in downlink and uplink should not pass through the HA in case of roaming is applied (Route optimization is working). Therefore, the direct connection between MN and CN in both directions is directly from FA_GTWY to CN_GTWY (Uplink) and from CN_GTWY to FA_GTWY in the opposite direction (Downlink).
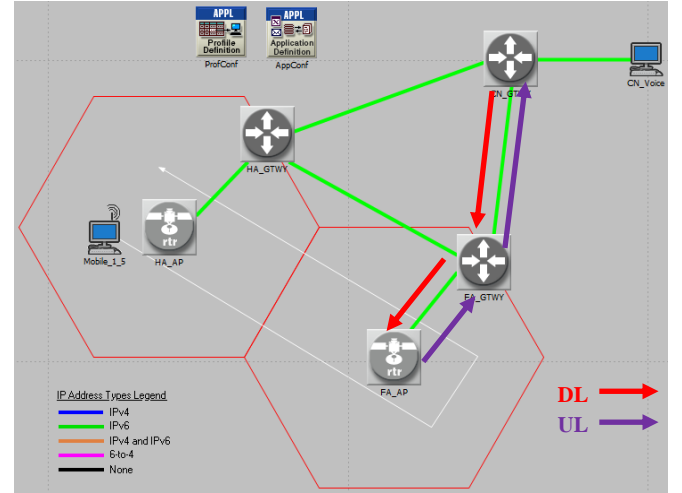

Figure 4 MIPv6 Network

3.4 MIPv6 over IPv4 Tunnel

Similar to MIPv6 as in 3.3, the route is optimized between MN via FA and CN as shown in Figure 5.
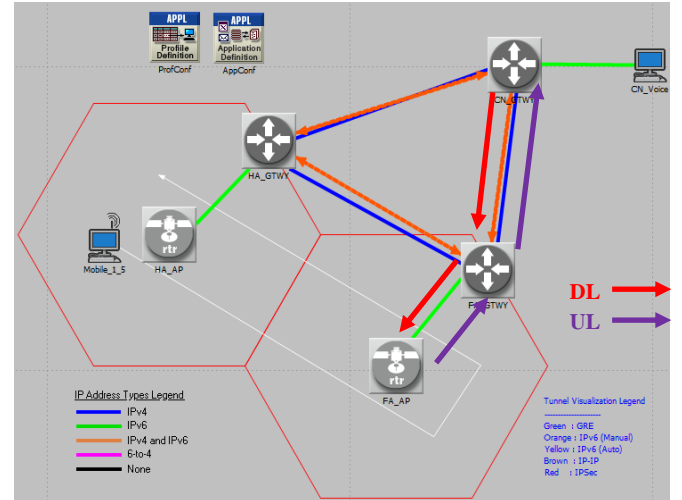

Figure 5 MIPv6 over IPv4 tunnel network

4. SIMULATION RESULTS

In this section, this document will explicitly concern the handover process directions, excess data, and time issues of the model discussed in the previous sections.

As investigated in WiFi networks, handover procedure is performed on two stages; uplink handover followed by downlink handover. Under the same simulation conditions for section 3, the following subsections results will be illustrated and analyzed.

4.1 MIPv4

As expected from section 3.2, the route used in downlink passes through the HA while roaming to FA_AP. On the other side, uplink direction is directly connected to CN it is not passing through the HA. This is illustrated in the traffic through core network (HA_GTWY, FA_GTWY, and CN_GTWY) is shown in Figure 6. It is found that during roaming period (between the two handovers) HA which is HA_AP is forwarding downlink data to MN with extra 5334 bps (20 byte) which are the mobility header according [4] used to allocate MN at FA. But in uplink direction, MN is sending data without these extra 5334 bps; because data are directly headed to CN without mobility headers.
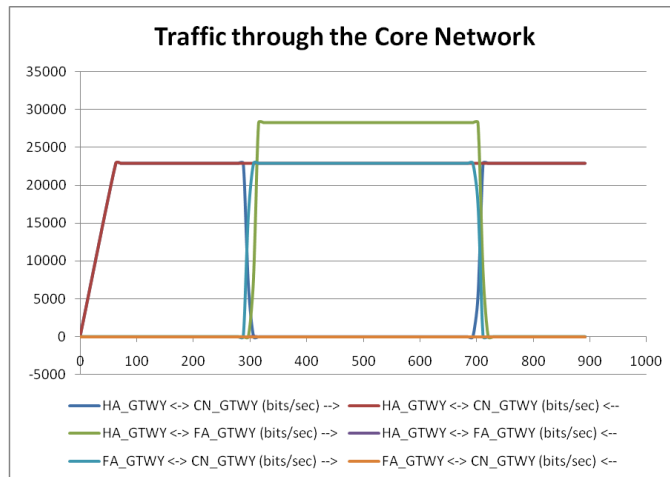
Figure 6 Traffic through Core Network in MIPv4 case

4.1.1 Home Network to Foreign Network Handover

The uplink and downlink handovers take 18 seconds each to complete as shown in Figure 7, but an increase in speed will increase the time for the whole handover process. For a MN moves with 10km/hr as in Figure 7 with 28 seconds of overall handover time. While in 30km/hr case as in Figure 8, overall handover time is 54 seconds.
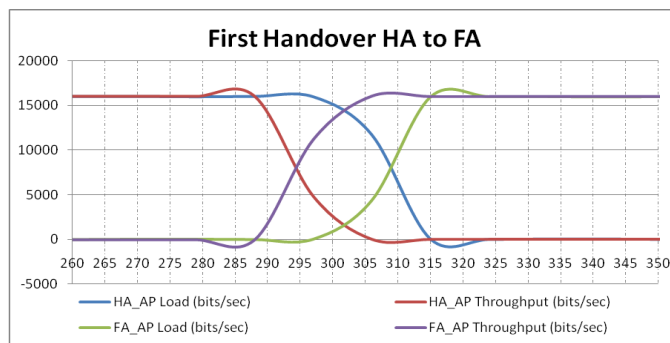

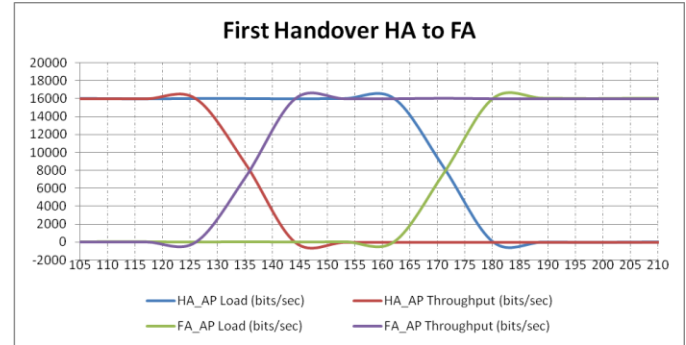**Figure 7 MIPv4 First Handover at 10km/hr**

Figure 8 MIPv4 First Handover at 30km/hr

4.1.2 Foreign Network to Home Network Handover

Referring to Figure 9 and Figure 10, it has been analyzed that the speed of MN does not alter the handover time while returning back to its home network. This time has been discovered to be 27 seconds, from the start of uplink handover till downlink handover end, at different speeds 10 or 30 km/hr.
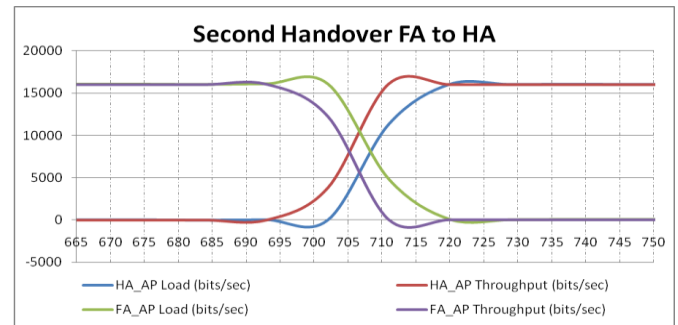

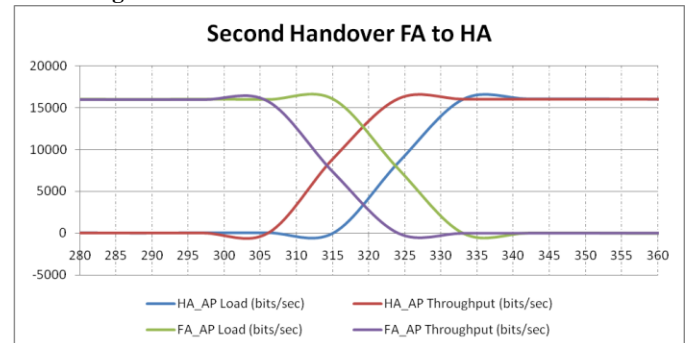**Figure 9 MIPv4 Second Handover at 10km/hr**

Figure 10 MIPv4 Second Handover at 30km/hr

4.2 MIPv6

In MIPv6 case, the route expected as in section 3.3 from FA_GTWY to CN_GTWY in both directions as MIPv6 feature "Route Optimization" is shown in Figure 11.

Referring to Figure 11, While MN is located at the home network; an extra overhead compared to the MIPv4 network is found due to the larger header for IPv6 which is 20 byte overhead according to [12]. After handover, a direct connection is established between MN via FA and CN, then data is sent with an additional 6400 bps IPv6 mobility header to the FA according to [9].
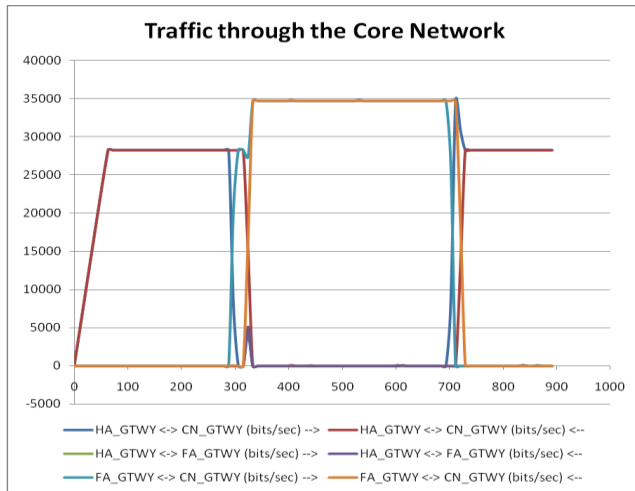
Figure 11 Traffic through Core Network in MIPv6 case

In MIPv6, the uplink handover followed by the start of the downlink handover end by the successful completion of the full handover as shown in Figure 12.
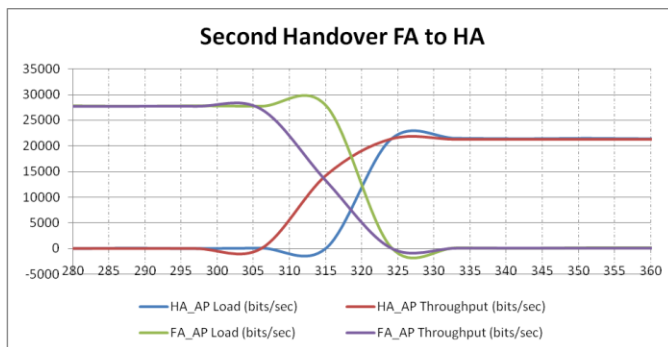

Figure 12 MIPv6 Second Handover at 30km/hr

4.3 MIPv6 over IPv4 Tunnel

As investigated in the traffic passing through the core network as in Figure 13, gateways add 20 byte of IPv4 header to be transmitted through the network to designated destination encapsulated through gateways links in the core network.
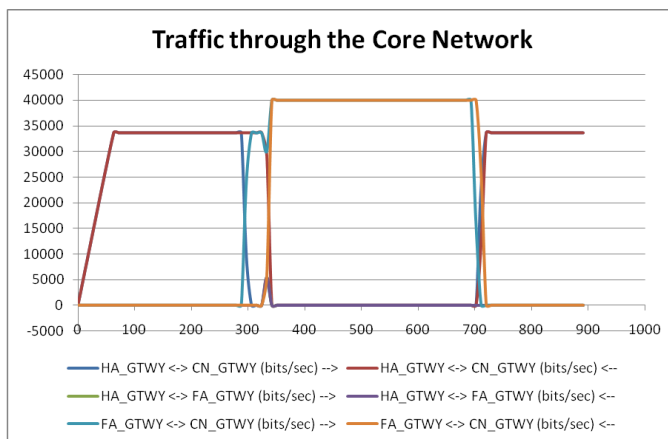

Figure 13 Traffic through Core Network in MIPv6 tunneled over IPv4 case

MIPv6 with IPv4 tunneling operates similarly in terms of handover to native MIPv6 as shown in Figure 14.
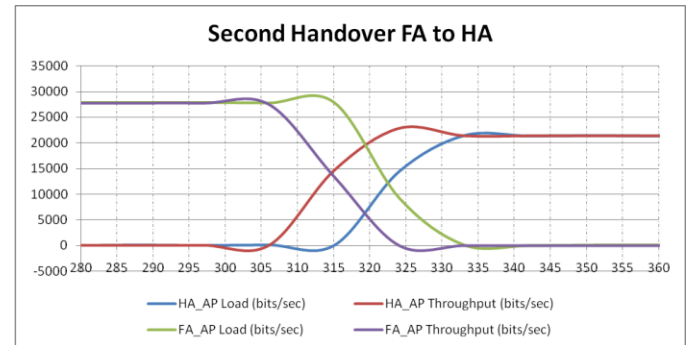

Figure 14 MIPv6 over IPv4 tunnel Second Handover at 30km/hr

5. CONCLUSION

In this paper, ways of supporting MIPv6 are proposed for IPv4 backbone network; which is the 6to4 tunneling approach. As a benefit, this approach helps using MIPv6 to couple many IPv6-capable end networks through central IPv4 backbones. On the other hand, it adds additional overhead of 20 byte for every transmitted packet more than the native MIPv6 solution; this additional overhead is due to encapsulating IPv6 packet inside an IPv4 packet which consists of IPv4 header of 20 byte (5334 bits). Also we covered the difference in roaming routed between MIPv6 and MIPv6, and it is noticed that MIPv4 is adding while roaming 20 bytes (5334 bits) per each packet for IPv4 mobility header [4]. For MIPv6 case 20 bytes are added more than MIPv4 case due to IPv6 header [12], beside adding another 24 bytes (6400 bits) due to mobility header for IPv6 [9]. According to these differences, MIPv6 over IPv4 tunnel adds the highest overhead for the transmitted data between MN and CN.

Handover process and its timing are also covered in the paper, and it is found that the handover process consists of two separate handovers: firstly occurred the uplink handover, then the downlink handover. In different type of mobile IP, each of two handovers, uplink or downlink, accomplished in 18 seconds but the time difference between them is depending on the speed of the MN in case of leaving home network in handover process. In the other direction heading back to its home network, handover process time is not depending on speed and it is 27 seconds. So it speed is considered while leaving the home network.

Our future plan will target the end-to-end delay and its variation while roaming to FA and the effect of changing the mobile IP technologies as in this paper.

6. REFERENCES

[1] L. Bokor, Z. Kanizsai, G. Jeney, "Performance Evaluation of Key IMS Operations over IPv6-capable 3G UMTS Networks", 2010 Ninth International Conference on Networks

[2] Mobile IPv6 -- A short introduction by Holger Zuleger (http://www.hznet.de/ipv6/mipv6-intro.pdf)

[3] IPv6 Coexistence and Integration, Salman Asadullah, Technical Advisor, IPv6 Forum, Cisco Systems

[4] Perkins, C., Ed., "IP Mobility Support for IPv4", RFC 3344, August 2002.

[5] Perkins, C., "IP Encapsulation within IP", RFC 2003, October 1996.

[6] Perkins, C., "Minimal Encapsulation within IP", RFC 2004, 1996.

[7] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[8] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, May 2000.

[9] RFC 3775: http://www.ietf.org/rfc/rfc3775.txt

[10] Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds". RFC 3056, February 2001. http://tools.ietf.org/html/rfc3056

[11] Gilligan, R. and E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers". RFC 2893, August 2000.http://tools.ietf.org/html/rfc2893

[12] http://www.cisco.com/web/about/ac123/ac147/images/ipj/ipj_9-3/93_ipv6_fig1_lg.jpg captured from http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-3/ipv6_internals.htm, The Internet Protocol Journal - Volume 9, Number 3