Performance Study of Mobile IPv6 Using OPNET

Firas Abdullah Thweny Al-Saedi
Computer Engineering Department
Al-Nahrain University
Baghdad, Iraq

Muhanad Mustafa Asem
Computer Engineering Department
Al-Nahrain University
Baghdad, Iraq

***Abstract* -Mobile IP technology is one of the important supporting techniques in the construction of pervasive computing environment. This paper is a study of the Mobile IPv6 issues using OPNET IPv6 model. Mobile IPv6 (MIPv6) allows Mobile Node (MN) to remain reachable while moving around in the Internet. In MIPv6, each MN is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a MN is also associated with a Care-of Address (CoA), which provides information about the MN's current location. In this paper, the simulated topologies were MIPv6 handover with default direction, MIPv6 handover with changing direction of movement, MIPv6 handover with changing speed of movement, MIPv6 handover with ping pong movement. The effect of different parameters, loads, movement, multiple AP's were taking into consideration for the mentioned scenarios.**

***Keywords* –Mobile IPv6, Handover, Mobility, OPNET IPv6**

I. INTRODUCTION

IPv6 is considered to be the next generation Internet Protocol, the current version of the IP, IPv4, has been in use for almost 30 years and faces some challenges in supporting emerging demands for address space cardinality, high density mobility, multimedia, and strong security. IPv6 is an improved version of the IPv4 that is designed to coexist with IPv4 and eventually provide better internetworking capabilities than IPv4 [1].

The most persisting reason for deploying IPv6 is its vastly increased address space which offer 128-bits addresses compared with IPv4's 32-bit addresses. While most companies and institutions running Network Address Translation (NAT) to serve a large number of networked hosts behind a small pool of public IP addresses. Additional benefits of IPv6 include better support for MIPv6 and for plug and play networking through stateless auto configuration [2].

IPv6 also adds improvements in areas such as routing and network auto-configuration. Specifically, new devices that connect to Internet will be plug and play devices. With IPv6, it is not required to configure dynamic non published local IP address, the gateway address, the sub network mask, or any other parameters. The equipment, when plugged into the network, automatically obtains all requisite configuration data [3].

II. MOBILE IPV6 TECHNOLOGY

The MIPv6 specification [4] enables hosts to change their point of attachment to the Internet whilst not breaking existing application sessions. This is achieved primarily through the MN which is always being reachable at its Home Address (HoA) via its Home Agent (HA). The resulting inefficiency of triangular routing (routing that sends a packet to a proxy system before transmission to the intended destination) can be eliminated in MIPv6 with the use of route optimization. In route optimization, the MN issues a Binding Update (BU) to its Correspondent Node (CN) to inform the CN of its current location and it's Care-of-Address (CoA). Once the BU has been acknowledged by the CN, communication can continue on a direct path rather than a triangular one.

The term handoff or handover refers to the process of MN moving from one point of attachment to the Internet to a different point of attachment. There are different types of handover according to which layers of the communication stack are affected. In general, handovers that only affect the link Layer Two (L2) without resulting in a change of IP, Layer Three (L3) state are known as horizontal handovers. An example of this is when a MN moves between different Wireless Local Area Network (WLAN) Access Points (APs) that are served by the same IP Access Router (AR). In 802.11 terminologies, both APs belong to the same Extended Service Set (ESS). Handovers that affect both L2 and L3 (a new IP address is obtained by the MN) are known as vertical handovers.

A hard handover occurs when all the links in the MN are disconnected before the new links are established. Conversely, a soft handover refers to the case where the MN is always connected to the network via at least one link. In this way, there is an overlap of different link usage during the handover process.

All the mentioned types of handover may be either intra technology (Fig. 1-a) or inter technology (Fig. 1-b and Fig. 1-c) handovers. In inter-technology, handovers are the handover between different network technologies. Intra-technology handovers are handovers of the same network technologies [5].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 8, August - 2014

III. MOBILE IPV6 HANDOVER PROCESS

The demand for wireless access to the internet through mobile devices continues to grow. To meet this demand, internet and wireless networks have merged into a unified network, the wireless internet. Enabling the Internet requires several issues to be addressed. In a wired Internet, all nodes are always reachable during normal operation. In a wireless Internet, nodes constantly move and their addresses change in a corresponding manner.

When the MN moves, it must change its point of attachment to the network via a handover. A handover is complex process and involves several steps: L2 move detection occurs which marks when L2 detects a loss of connection with the old AP, L2 searches for a new AP, L2 switches to the new AP, after L2 is complete, L3 move detection occurs which marks L3 detection of a loss of connection with the old router, finally, the handover process ends with L3 handover execution which includes BU and Duplicate Address Detection (DAD) [6].

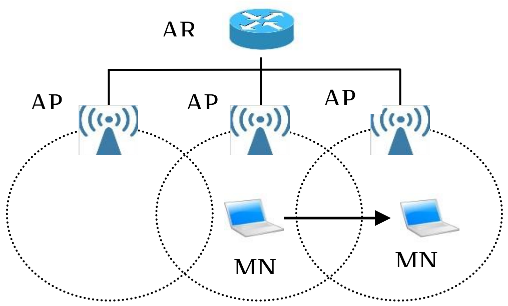
When a MN is far from its home network, packets can still be routed to it using the MN's HoA. In this way, the movement of a node between networks is completely invisible to transport and other higher-layer protocols. When a MN changes its point of attachment to the Internet from one IPv6 network to another IPv6 network, (also referred to as roaming), it will perform the MIPv6 handover procedure. The MIPv6 handover procedure is similar to the auto configuration procedure an IPv6 node booting up onto a network but has some important differences [5]:

- The MN must somehow detect that it has moved onto a new network.
- Once configured, the MN must inform it's HA and each CN of its new location.
- During the handover procedure, upper layer connections will still be active so the handover procedure should be performed as quickly as possible to minimize disruption from lost and severely delayed packets.

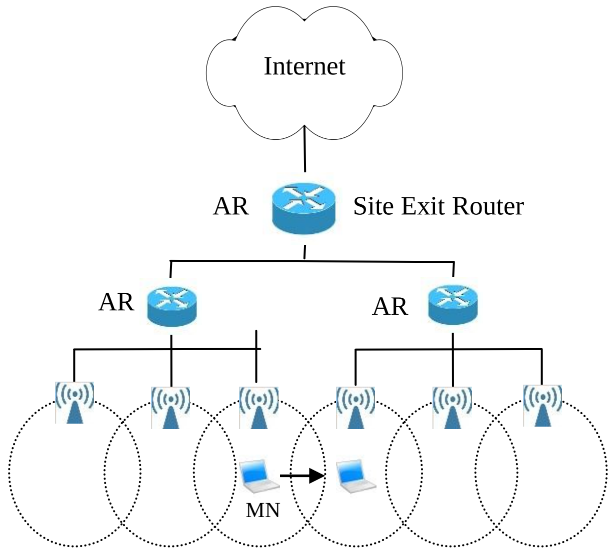
The MIPv6 handover procedure is illustrated in Fig. 2 and it will be described in more detail in the following sections [7]. In current IPv6 specifications, each stage of the procedure is mandatory with the exception of Authentication, Authorization and Accounting (AAA) protocol.

IV. ANALYSIS AND EVALUATION OF MIPV6 HANDOVER

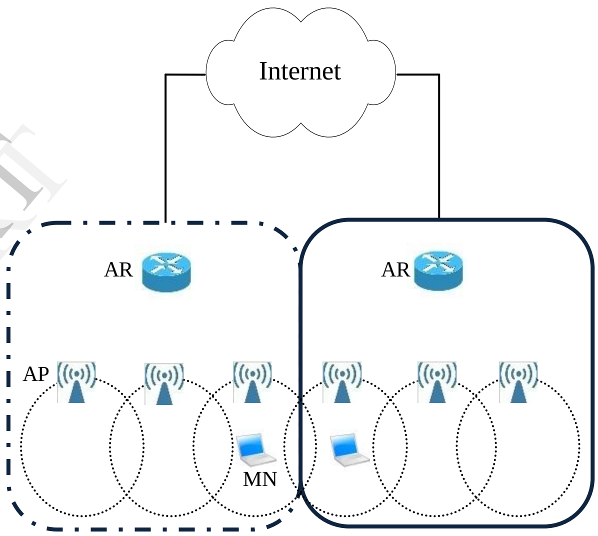
Analyzing the behavior of the MIPv6 standard over WLAN identifies the latency that can significantly affect handover delay during an IPv6 handover as shown in Fig. 3.



(a) MN moving with same Basic Service Set (BSS)



(b) MN Moving between ARs of the same provider



(c) MN Moving between ARs of different providers

Fig. 1 Types of handover

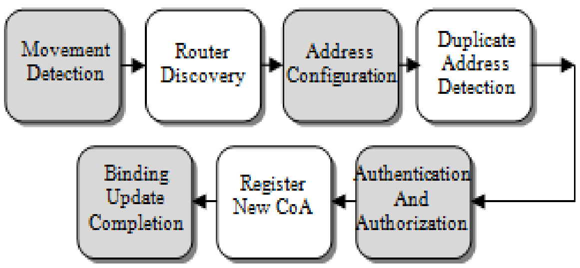


Fig. 2 MIPv6 Handover Procedure

The total IP handover delay defined as the sum of these components:

$$t_h = t_d + t_a + t_c + t_r + t_o \quad (1)$$

Where:

Movement Detection (MD) time (t_d): this is the time required by the MN to detect and establish that it has moved to a new point of attachment (the discovery of a new on-link router).

IP CoA configuration time (t_a): this is the time between the establishment of having moved and the time that a globally routable IPv6 address has been configured (this includes DAD).

Context establishment time (t_c): this is the time between the establishment of a globally routable CoA and the establishment of the appropriate context state.

Binding registration time (t_r): past the establishment of context-specific state of the MN, this is the time between the dispatch of BU signal to the HA to the receipt of an acknowledged BU on the first packet from its communication peer.

Route optimization time (t_o): this is the time from registering the new CoA with the HA to completing route optimization with the current list of CNs. This includes the return route-ability procedure which, if used, must occur before a BU is sent by the MN to a CN.

A. *Movement Detection Time*

The MD time (t_d) is the sum of two individual latency components [5]:

Link switching delay (T_{l2}): this is the time delay pertaining to the re-association of the wireless station in an 802.11 wireless LAN with its Basic Service Set (BSS) AP.

Link-local IPv6 address configuration delay (T_{ll}): this is the time between the first time that the MN encounters a new link by receiving neighbor adverts over its all nodes or solicited nodes multicast address and configuration of a link-local address. Configuration of a link local address is affected as well as L2 information is exchanged with the new AR.

The MD time can thus be expressed as:

$$t_d = T_{l2} + T_{ll} \quad (2)$$

Where: T_{l2} is Link switching delay

$T_{ll}$is Link-local IPv6 address configuration delay

B. *IPv6 CoA Configuration Time*

CoA configuration time (t_a) was defined as the time commencing from the moment of the receipt of a RA to the moment that DAD and the update of the routing table has completed. Depending on the mechanism employed to configure an IPv6 CoA t_a may vary. For stateless IPv6 address auto-configuration t_a is comprised of the following delay components [5]:

$$t_a = T_{prefAdv} + T_{AddrConfig} + T_{DAD} + T_{RouteUpdate} \quad (3)$$

Where $T_{prefAdv}$is defined as:

T_{rtAdv}- T_{rtSol} (if the RA is solicited)

rtAdvInterval / 2 (if RA is periodic)

$T_{AddrConfig}$ is the time required by the MN to employ the address configuration rule, such as EUI64, to produce a unique globally routable IPv6 address. The latency component is dependent on the processor speed of the MN and as such may be negligible compared to the total of t_a.

T_{DAD} is the time required to resolve uniqueness of the configured IPv6 CoA. The mechanism to effect this is typically address resolution by transmitting a NS for this address to the all-nodes multicast address and then waiting for Retransmission Timer (RT) interval before transmitting up to DAD Transmits. If during or after RT interval there has been no NA on the particular tentative CoA, the address is assumed to be unique and is assigned to the interface.

In the event of stateful address auto-configuration, the time for CoA configuration becomes:

$$T_{AddrConfig} = T_{DHCPaddrReq} + T_{DHCPaddrResp} + T_{RouteUpdate} \quad (4)$$

$T_{DHCPaddrReq}$ and $T_{DHCPaddrResp}$ represent the transmission delay incurred by stateful configuration of a CoA via a Dynamic Host Configuration Protocol (DHCP) server.

C. *CoA Registration Time*

The CoA registration time (t_r) is defined as the transmission delay incurred during registration of MN's location [8].

$$t_r = RTT_{MN\text{-}HA} + BU_{proc} + BA_{proc} \quad (5)$$

Where:

BU is the time taken by BU packets to reach from MN to HA.

BA is the time taken by BA packets to reach from HA to MN.

D. *Route Optimization Time*

The route optimization time (t_o) is defined as the transmission delay incurred during registration of the MN bindings with the CN that is furthest away in two distinct cases depending on the mode of security affected in the BU registration process [5]:

(if BU is not authenticated):

$$t_o= RTT_{MN\text{-}CN} + BU_{proc} + BA_{proc} \quad (6)$$

(if BU authenticated):

$$t_o= T_{HoT\text{-}CoT}+ (RTT_{MN\text{-}CN} + BU_{proc} + BA_{proc}) \quad (7)$$

In the event of an unauthenticated BU, the route optimization time to be defined as the time period between a

BU dispatched to the CN and the first data packet received by the MN from the CN.

In the event of an unauthenticated using RR, The MN must first initiate the Home Test (HoT) and Care-of Test (CoT) before it can send a binding update. The RR procedure is illustrated in both Fig. 3 and Fig. 4.

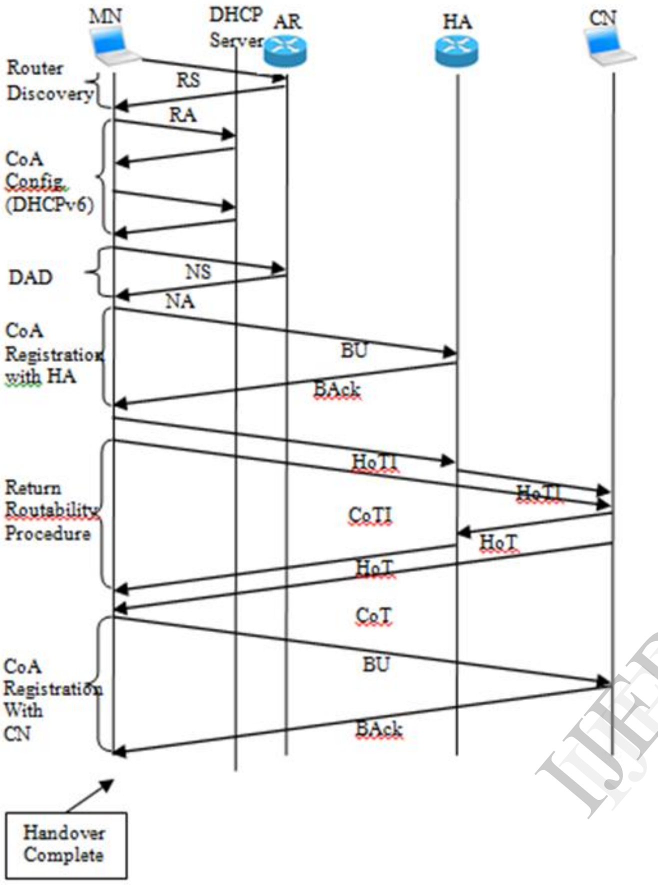


Fig. 3 Steps of IPv6 handover procedure

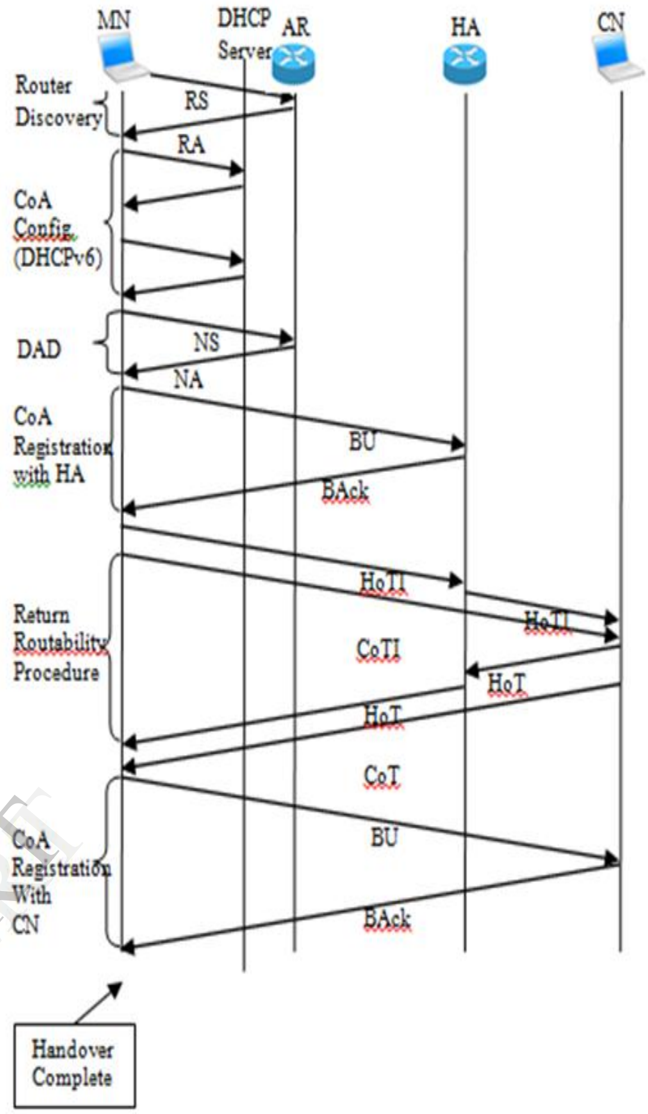


Fig. 4 Handover procedure using DHCPv6

When the HA has acknowledged the registration of the MN's new CoA, any new CN attempting communication with the MN will succeed due to the HA being able to tunnel packets destined for the MN to its new CoA. However, communication with any existing CN at the time of handover occurred and with whom route optimization was being used, cannot resume until the MN has successfully registered its new CoA with it by performing the route optimization procedure [5].

Fig. 4 illustrates the MIPv6 handover procedure where DHCPv6 is used for CoA configuration.

V. MIPv6 Model Overview

In order to perform mobility operations, the OPNET MIPv6 model has been designed and developed with many standard MIPv6 definitions and extensions such as Extension headers (including Mobility, Routing and Destination Extension headers), Neighbor Discovery (ND), Router Advertisements (RA) (including movement detection, stateless address auto-configuration and HA address detection) and DAD etc. OPNET also includes the MIPv6 entities models: MN, CN and HA. And The OPNET MIPv6 model supports two routing mechanisms for communication between the MN and the CN: bidirectional tunneling and route optimization. Therefore, researchers can observe and analyze the simulation results demonstrated in the MIPv6 model and compare with the real MIPv6 network environment. In the following subsections, the characteristics of the MIPv6 model are presented by configuring node models for MIPv6 [9, 10].

The main topologies were simulated (MIPv6 handover with default direction, MIPv6 handover with changing direction of movement, MIPv6 handover with changing speed of movement, MIPv6 handover with ping pong movement). The effect of different parameters, loads, movement, multiple AP's were taking into consideration for the mentioned scenarios. The simulation strategy was made to examine the possible topologies and configuration for the network. Figures (5-10) show the simulated scenarios.

The arrangement of objects in these scenarios contains multiple objects which it explained below:

- MN: a node was moved from specific location through three AP's (HA – AR 1 – AR 2) to implementing handover in the network.
- HA, AR1 and AR2: Multiple AP's connected with different routers, placed respectively on the way of MN with coverage area a radius of 100 meters.
- Central Router 1 (CR1) and Central Router 2 (CR2): two wired routers connected to multiple AP's and founded to separate from two networks.
- Switch: a device that channels incoming data from any of multiple input ports to the specific output port that will take the data toward its intended destination (Servers).
- Servers: three servers are used in the designed network with different supported Profile (Engineer, Multimedia, Researcher).
- Application Definition: to define multiple application configurations.

Profile Definition: to define multiple profile configurations.

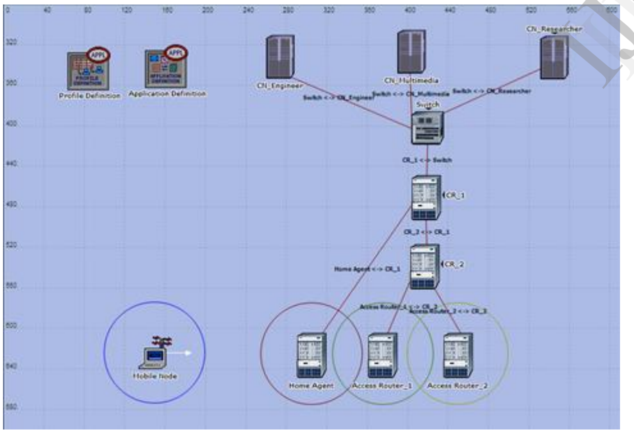


Fig. 5 MIPv6 handover with default direction of movement

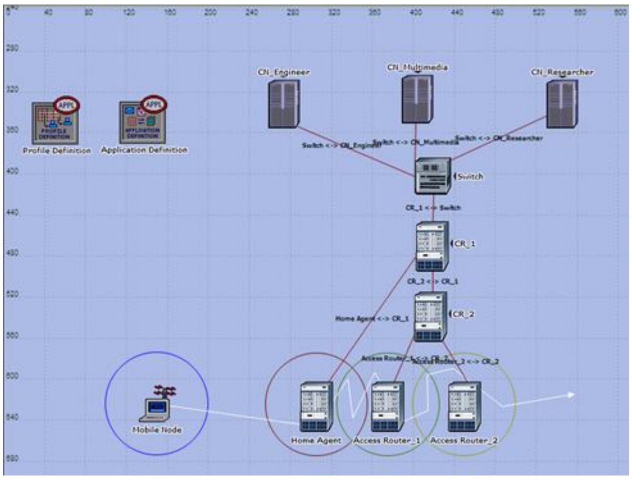


Fig. 6 MIPv6 handover with random direction of movement

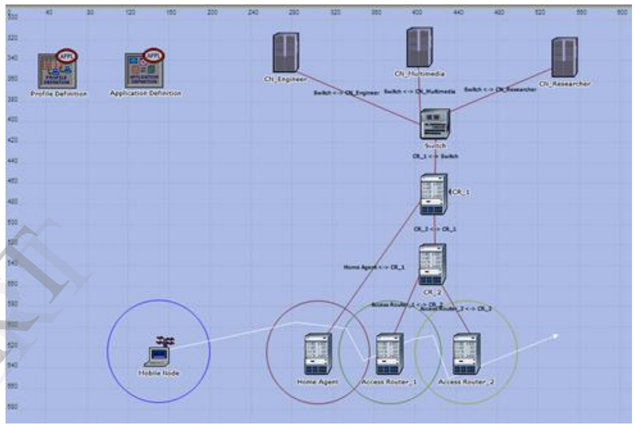


Fig. 7 MIPv6 handover with random speed of movement

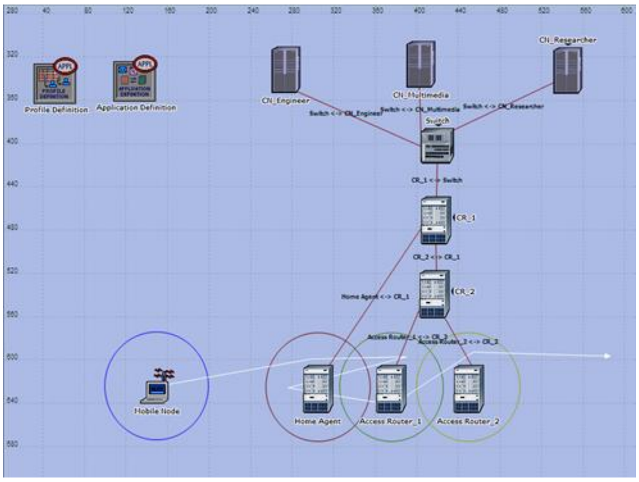


Fig. 8 MIPv6 handover with ping pong movement

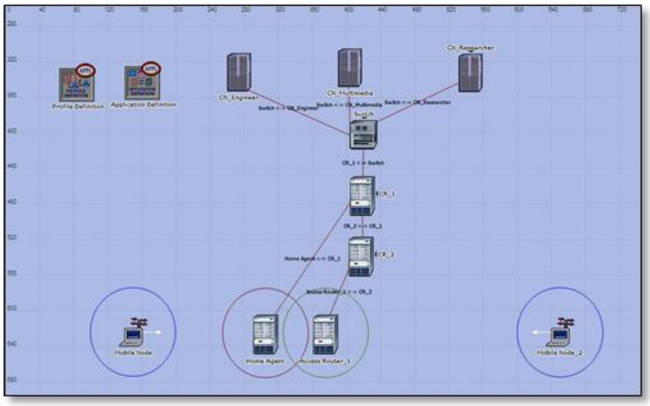


Fig. 9 MIPv6 handover with two MN's movement

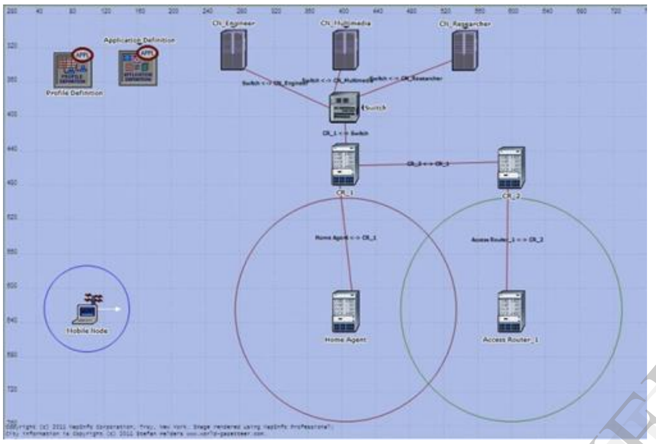


Fig. 10 MIPv6 handover with 10m/sec speed

A. Mobile Node Configuration

In OPNET MIPv6 model, the node models of (wlan_wkstn_adv) can be configured as MNs by setting the Node Type attribute in the attributes dialog box: IP->Mobile IP Host Node Parameters->Mobile IPv6 Parameters. The IP address of HA can be learned from the HA's router advertisements when the MN is at home network. However, if the MN is initially away from the home network and more than one access routers exists, the IP address of HA need to specify in the HA Address attribute. The number of lost router advertisements that constitutes a network layer handover indication can be set by specifying the Mobility Detection Factor attribute. In MN, the global IP address should use the same network prefix as the IP address of HA. Table 1 shows the example of MN configuration with (wlan_wkstn_adv) model.

In Table 1, the Node Type attribute is set as MN, and Route Optimization attribute is enabled. The IP address of HA is 2005:0:0:1:0:0:0:1 with network prefix 64, and the global IPv6 address of MN is 2005:0:0:1:0:0:0:2 with the same network prefix as the HA. And other parameters are set to default. When a node is configured as the MN, it has the ability to support MIPv6 applications.

Table 1 IPv6 configuration for MN in MIPv6 handover design

Parameters	Value
IP	
IP Host Parameters	(…)
Interface information	(…)
Name	IF0
Subnet Mask	Auto assigned
IPv6 Parameters	(…)
Link Local address	Default EUI-64
Global address(es)	(…)
Number of Rows	1
2005:0:0:1:0:0:02	
Address	2005:0:0:1:0:0:0 :2
Prefix Length (bits)	64
IPv6 Default Route	2005:0:0:1:0:0:0 :1
Mobile IPv4 Parameters	Disabled
Mobile IPv6 Parameters	(…)
Node Type	Mobile Node
Route optimization	Enabled
Home Agent Address	2005:0:0:1:0:0:0 :1
Binding Parameters	Default
Return Routability	Default
Mobility Detection factor	3

There are other parameters for MN configuration which are explained in Table 2.

Table 2 MN parameters in MIPv6 handover design

Parameters	Value
BSS Identifier	1 (to start with HA coverage)
Access Point Functionality	Disabled
Data Rate (bps)	1 Mbps
Packet Reception Power Threshold	-69 dB
RTS Threshold (bytes)	None
Fragmentation Threshold	None
Large Packet Processing	Drop
Roaming Capability	Enabled

B. Correspondent Node Configuration

In MIPv6 model, the CN functionality is included in the MN functionality. To configure a node as the CN, the Node Type attribute can be set to MN or CN.

C. Home Agent and Access Points Configuration

The home agent interface can be a wireless interface or wired interface. An interface is configured as a home agent through the IP->Mobile IP Router Parameters->Mobile IPv6 Parameters attribute in the attributes dialog box of router node and set the interface type to HA. Also BSS Identifier must be set for HA, AP1 and AP2 as explained in Table 3.

Table 3 HA and AP's identifier

Parameters	Value
BSS Identifier	1 (for HA) 2 (for AP1) 3 (for AP2)
Access Point Functionality	Enabled

The route advertisement functionality can be configured in the Router Advertisement Parameters attribute: IP->IPv6 Parameters->Interface Information->Router Advertisement Parameters as shown in Table 4.

Table 4 Router Advertisement Configuration

	Parameters	Value
-	Router Advertisement Parameters	(…)
	Router Advertisement	Enabled
	Router Advertise Interval (sec)	Uniform (0.5,1)
	Current Hop Limits (hops)	32
	Advertised Lifetime (sec)	Half Hour
	Advertise Reachable Time (msec)	Unspecified
+	Advertise Prefix List	All

Trajectory Configuration

Trajectory was configured to control the MN movement and it can be configured with different ways such as vector movement, MN movement and speed can be changed during the simulation and the important parameters are shown in Table 5.

Table 5 MN parameters in MIPv6 handover design

Parameters	Value
Trajectory	Vector
Color	White
Bearing	90 (to move from left to right)
Ground speed	1 meter / sec for all scenario except the scenario displayed in Fig.7 which the speed of MN changed (1 meter /sec – 2 meter / sec – 3 meter / sec) and also Fig. 10 which the speed of MN is 10m/sec
Ascent Rate	0 meter /sec
X Position	150
Y position	625

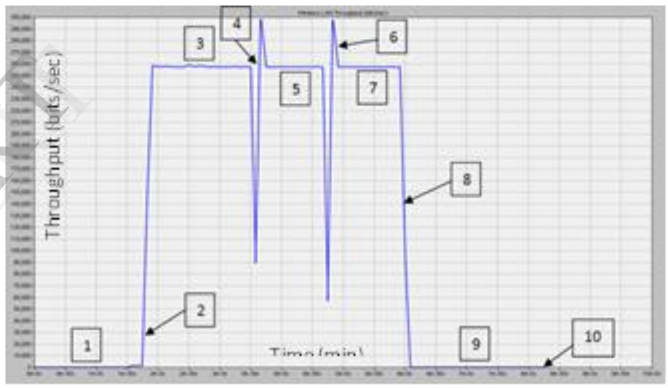
VI. RESULTS ANALYSIS

First, the application and profile configuration between MN and CN was set in order to run real time application between them.

Application Parameters: Set the applications to be supported by the nodes and servers. These parameters were configured to apply low load, medium load and heavy load traffic on the network.

Profile Parameters: Each profile contains a specific set of application which in turn generate different amount of traffic. In these scenarios many profile were used for the simulated model and these profile are (Engineer profile, Multimedia user's profile and Researcher profile) and all of them are representing either low load, medium load or heavy load.

Full study for the MIPv6 handover that happen in this scenario were displayed in Fig.11 which is displayed throughput for MN and the handover that happen under high load condition and with default direction of movement with a detailed explanation for each events in the result. Table.6 shows the throughput result of the MIPv6 handover with default direction movement.



Fig, 11 MN throughput curve in bits/sec for default movement

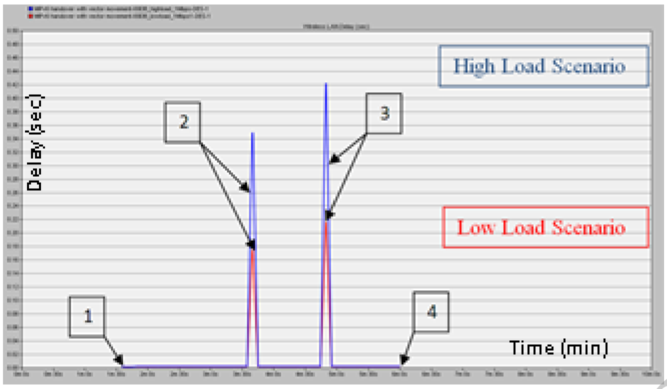
Where the points attached in Fig. 11 represent:

1. 100m without coverage area before the MN entering HA coverage.
2. Starting the coverage for HA.
3. 70m coverage area for HA.
4. Handover starting between HA and AP1.
5. 55m coverage area for AP1.
6. Handover starting between AP1 and AP2
7. 60m coverage area for AP2.
8. Coverage area for AP2 was ended.
9. 130m without coverage area after going out from all AP's.
10. 500 sec Simulation time was ended at this point.

Table 6 Throughput for MIPv6 handover with default movement (bps)

Data Rate	Without Fragmentation Without RTS		
	Low Load	Medium Load	High Load
1Mbps	83,836 bps	153,375 bps	232,762 bps

The delays that happen during the simulation are explained in Fig. 12 with brief description about each effect in simulation, Table 7 shows the delay for the default direction and speed of movement scenario (sec).



Fig, 12 Delay curves in (sec) for default movement

Where the points attached in Fig. 12 represent:

1. The delay started with the coverage area and not with the beginning of simulation.
2. Delay increase clearly between HA and AP1.
3. Delay increase clearly between AP1 and AP2.
4. Delay stopped with the ending of coverage area.

Table 7 Delay in default direction of movement scenario (sec)

Data Rate	Without Fragmentation Without RTS		
	Low Load	Medium Load	High Load
1Mbps	0.008 sec	0.016 sec	0.016 sec

Figure 13 shows the data dropped (retry threshold exceeded) result of the MIPv6 handover with 2 MN movements comparing with the throughput for high load scenario.

Where the points attached in Fig. 13 represent:

1. MN1 entered the coverage area of HA.
2. Handover starting between HA and AP1 for MN1, MN2 entered the coverage of AP1.
3. MN1 went away from the coverage area of AP1.
4. Handover starting between AP1 and HA for MN2.
5. MN2 get out from HA coverage area.
6. These points represented the data dropped that appear clearly through handover process

Fig. 13 Comparison between throughput and data dropped (bits/sec)

Figure 14 shows a comparison between throughput and data dropped for 10m/sec MN Speed.

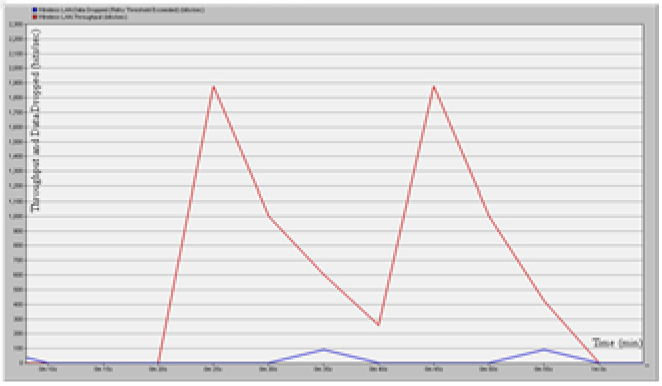


Fig. 14 Comparison between throughput and data dropped for 10m/sec MN speed (bits/sec)

The maximum speed allowed for MN with this design is (6m/sec) so that the dropped in throughput can be seen clearly in this scenario. Any handover happened with speed larger or equal than (6m/sec) will not give the best results. The maximum throughput that gets from this scenario is about (1,900 bits/sec), which is lower than throughput results for other scenarios (with speed less than 6m/sec).

VII. CONCLISIONS

- MN communicates with correspondent servers through its movement and the send / receive data did not disconnect when MN moved from AP to another.
- At the point where MN changed its location (handover), there were some data dropped, happened without making disconnection for data from MN to servers and vice versa.
- Mobility in IPv6 network applied with different movement and speed of MN, the handover occurred without disconnection.
- The average delay and binding update delay were almost the same in all simulated scenario.
- High load scenario gave the best throughput result with best delay comparing with other scenarios, because of high transmission and received data between MN and CN's.
- According to the results, Maximum allowed speed for MN was (6m/sec). For a speed greater than (6m/sec), they need special configuration changing some parameters such as (type of modulation, fragmentation, RTS and coverage area).
- Packet reception power threshold affects AP coverage area. Increasing power threshold would decrease the cell size of the AP. This technique is useful in maximizing the number of clients per specific area.

REFERENCES

[1] IPv6 Vendors Test Voice, Wireless and Firewalls on Moonv6 IPv6 Forum Driving IPv6 Deployment: http://www.ipv6forum.com/modules.php?op=modload&name=News&file=article&sid=15&mode=thread&order=0&thold=0

[2] JANET Service Desk, Lumen House, Library Avenue, Harwell Science & Innovation Campus, Oxfordshire, "Internet Protocol Version Six (IPv6)", Factsheet, The JNT Association 2007.

[3] http://www.ipv6tf.org/index.php?page=meet/faqs.

[4] David B. Johnson, Charles Perkins, J. Arkko, “Mobility Support in IPv6”, IETF Internet Draft, 2004.

[5] Martin Dunmore and Theo Pagtzis, "Mobile IPv6 Handovers: Performance Analysis and Evaluation", 6NET, 2005.

[6] May Siksik, Hussein Alnuweiri and Saif Zahir, "A DETAILED CHARACTERIZATION OF THE HANDOVER PROCESS USING MOBILE IPV6 IN 802.11 NETWORKS", Dept of Electrical Engineering University of British Columbia, IEEE 2005.

[7] Xinyi WU, Xinyi WU, “Performance Analysis and Evaluation of handover in Mobile IPv6”, College of Computer Science, Wuhan University of Science & Engineer, IEEE 2009.

[8] Irfan Ahmed, Usman Tariq, Shoaib Mukhtar, Kyung-suk Lhee , S.W. Yoo, Piao Yanji and ManPyo Hong, "Binding Update Authentication Scheme for Mobile IPv6", Graduate School of Information and Communication, Ajou University, Korea, IEEE 2007.

[9] OPNET Modeler 14, Modeler Help and Documentation.

[10] Deguang Le, Xiaoming Fu and Dieter Hogrefe, “Evaluation of Mobile IPv6 Based on an OPNET Model”, Telematics Group, University of Göttingen 37083, Germany.