Chapter (1)
Introduction

1.1 Introduction:-

Wireless networks are in full development because of the flexibility of their interfaces, which allow users to be easily connected to the Internet. Among various technologies of wireless networks, IEEE 802.11/Wi-Fi technology is becoming better known and more used to construct high speed wireless networks in areas with high concentration of users, such as airports, campuses or industrial sites. The passion for wireless networks and in particular for Wi-Fi networks has given rise to new uses of the Internet, such as moving in wireless networks while still being connected.

In Wi-Fi networks, the user's movement may sometimes lead to a change of Access Points (APs) to the network. This fact is generally named the handover of layer 2 because this change involves only the first two layers of the OSI model. If the two APs are located in different networks, the change of AP would entail a change of network for the user. This situation is generally termed, the handover of layer 3 because the user should change his network and his IP address to maintain connection to the Internet. Therefore, this change intervenes on the network layer of the OSI model.

The process of the handover of layer 2 is handled by the IEEE 802.11 standard and that of layer 3 is controlled by the Mobile IP protocol. The Mobile IP protocol is a protocol standardized by IETF, which allows users to change network, while maintaining their actual connection to the Internet. Consequently, users can connect to the Internet, while keep moving in Wi-Fi networks in control of the IEEE 802.11 standard and the Mobile IP protocol. However, the delay induced by these procedures of handover is too long. As such, this generally leads to the cut-off of current communications, hence impacting adversely on the qualitative requirements of real-time applications, such as video conferencing or voice over IP.

Various proposals have been made to reduce the delay of handover procedures and to improve their performances. However, these proposals are either imperfect, or non-implementable because of their complexity.

Based on the premise that Wi-Fi networks and access routers are already massively implanted in academia and in industry, we propose to add a new functionality, called L-HCF (Lightweight Handover Control Function) in routers, without modifying other network equipments. A router equipped with this functionality is called an L-HCF router. To reduce the delay of handover procedures, the L-HCF

functionality allows a router to generate a topology of APs by using the neighborhood graph theory and to maintain a pool of available IP addresses in its database. When a Mobile Node (MN) needs to change its AP, the L-HCF router may propose to the latter a list of potentially usable APs. If the change of APs involves a change of network, the MN must change its IP address. In this case, the L-HCF router can assign a unique IP address to this MN. The MN can thus use this address without engaging in the process of Stateless Address Auto-configuration or the procedure of Duplicate Address Detection. With this new L-HCF functionality, we can reduce the delay of handover procedures from a few seconds to one hundred milliseconds.

To reduce packet loss, incurred due to handover procedures, The control function proposed to modify the Mobile IPv6 protocol. In general, the MN terminates the binding between its home address and its care-of address with its Home Agent (HA) and it's Correspondent Node (CN) before proceeding with the handover procedures. Consequently, it use the HA to intercept and redirect the packets of the CN or the MN respectively to the new care-of address of the MN or to the addresses of the CN during the complete binding process. With this method, it will limit packet loss and guarantee an acceptable delay.

To support this method, we used the OPNET simulator to simulate the handover procedures in Wi-Fi networks as defined by the L-HCF method and by the Mobile IPv6 protocol. The results obtained show that it guarantee an acceptable delay and limit packet loss with L-HCF method.

1.2 IPv6 and IPv4

Internet Protocol version 6 (IPv6) is the next generation of Internet Protocol (IP) which was released by Internet Engineering Task Force (IETF) in 1996. The motivation of the protocol is to resolve the problem of IPv4 address shortage in global Internet.

However, the adoption of IPv6 has been slowed by the introduction of network address translation (NAT). The NAT alleviates the address exhaustion by separating the local IPv4 address and the global IPv4 address, and reusing the global addresses locally. However, NAT also makes it difficult and sometimes impossible to use peer-to-peer applications, such as Voice over Internet Protocol (VoIP) and multi-user games. Recently, due to the increasing demand and requirement for the wireless Internet, the deployment of IPv6 has become an urgent issue for the future Internet.

In essence, IPv6 offers everything IPv4 does and better, with additional features that were not available with IPv4. The following section lists the specific strong point of IPv6 over IPv4:-

1. IPv6 increases the IP address size from 32 bits to 128 bits which can support 1028 times more devices in the global Internet. For this reason, it can also allow more levels of addressing hierarchy.
2. Instead of using broadcast, the usage of multicast and "any cast address" in IPv6 provides better scalability of multicast routing.
3. IPv6 has a simpler header format than IPv4 which reduces the processing cost and bandwidth cost.
4. The design of IPv6 is more flexible than IPv4. The header design in IPv6 supports future extensions and new options.
5. The Flow Labeling Capability (FLC) in IPv6 enables the labeling of packets which can be used to optimize QoS. This includes enabling premium pricing for guaranteed delivery, and prioritization of defense or other critical government Internet-based communications, even when network is congested.
6. Unlike IPv4, IPv6 has been designed together with security features. It has Authentication and Privacy Capabilities Extensions to support authentication and data integrity. Also, the IPSec is mandatory to the protocol.

1.3 Mobile IPv6:-

The Mobile IPv6 (MIPv6) is a standard proposed by the IETF. The official name of standard is "Mobility Support in IPv6", and the last update of the standard is in 2004.

As the successor of Mobile IP support in IPv4 (Mobile IPv4), MIPv6 is designed with more experience. It does not only shares many features with Mobile IPv4, but also offers many other improvements. The following list summarizes the major differences between Mobile IPv4 and Mobile IPv6:-

1. In MIPv6, the entity "foreign agent" is excluded which makes the implementation of routers become easier. There is no special support required from the access router any more.
2. MIPv6 has built-in route optimization which belongs to a nonstandard set of extensions in MIPv4.
3. Mobile IPv6 route optimization can operate securely even without prearranged security associations. It is expected that route optimization can be deployed on a global scale between all mobile nodes and correspondent nodes.
4. MIPv6 provides support on allowing the route optimization and "ingress filtering" to coexist efficiently on a router. The "ingress filtering" is a technique used to confirm that incoming packets are from the networks they claim to be from. The technique is to prevent denial of service attacks which employ IP source address spoofing.

5. The Neighbor Unreachability Detection which belongs to the IPv6 standard assures the reach-ability from the mobile node to its default router and vice versa.
6. In Mobile IPv6, when a mobile node is away from its home network, most of packets are sent to it by using an IPv6 routing header rather than IP encapsulation. In result, the amount of resulting overhead are reduced comparing to Mobile IPv4.
7. Mobile IPv6 is decoupled from any particular link layer, as it uses IPv6 Neighbor Discovery instead of ARP which improves the robustness of the protocol.
8. Mobile IPv6 is not required to manage the "tunnel soft state" information because of the usage of the IPv6 encapsulation and the routing header.
In a computer network, a tunnel is created by following the tunneling protocol which encapsulates packets at a peer level or below. It is used to transport multiple protocols over a common network as well as provide the capability for encrypted virtual private networks (VPNs). Inside of a tunnel, when one of the routers encounters an error while processing the datagram, it requires the router to return an ICMP error message to the source of the tunnel. Unfortunately, the size of the ICMP packet is greater than the IPv4 header; it is generally not possible for the router to immediately reflect an ICMP message. To resolve this problem, the source of tunnel requires to maintain extra information regard to the tunnel which is called "soft state" information.

1.4 Problem Statement

Mobile IP allows a mobile node to maintain a continuous connectivity to the Internet when moving from one access point to another. However, due to the link switching delay and to the Mobile IP handover operations, packets designated to mobile nodes can be delayed or lost during the handover period.

1.5 Aim and Objectives

A new control function called Lightweight Handover Control Function (L-HCF) in order to improve the handover performance in the context of Mobile IPv6 over wireless networks. This solution allows to provide low latency, low packet loss to the standard handover of Mobile IPv6.

Chapter (2)
Literature Review

1. Overview

A MIPv6 handover can cause delay and/or packet-loss for an ongoing traffic stream. Over last ten years, a number of research projects have aimed at shortening the handover process by improving different part of a MIPv6 handover.

2. Fast Handover MIPv6 (FMIPv6)

FMIPv6 is a protocol which has been standardized by IETF to improve the AC process in a MIPv6 handover. There are two operation modes:

1- The predictive mode
2- The reactive mode.

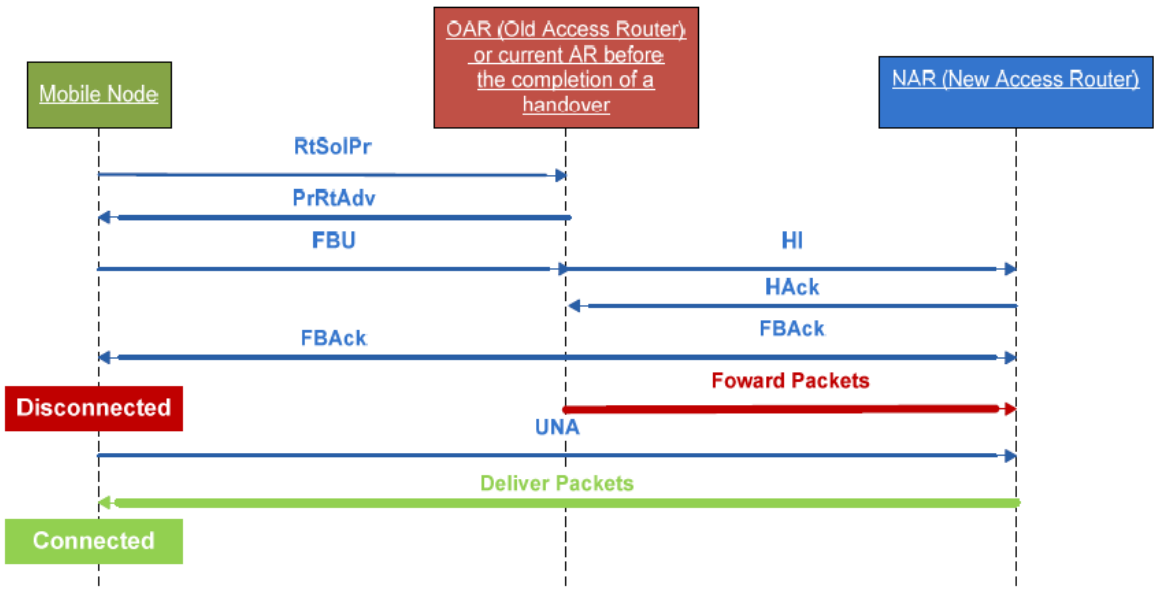

Figure 2.1 Predictive Mode

2.1. The predictive mode:-

The predictive mode shortens the AC process by performing the process before it is required. This means the handover process is started without the confirmation from a standard Movement Detection process. In addition, the packet loss is minimized by buffering packets at the Old AR (OAR) and forwarding them to the New AR (NAR).

Figure 2.1 illustrates the steps in this mode, and details and functionality of each step is described in the following paragraphs.

1. **Router Solicitation Proxy (RtSolPr) and Proxy Router Advertisement (PrRtAdv):** Router Solicitation Proxy (RtSolPr) and Proxy Router Advertisement (PrRtAdv) messages are transferred between an MN and its current AR in the beginning of an FMIPv6 handover. The RtSolPr message is sent from the MN to its current AR, and the message is used for requesting the information from a NAR. As Figure (1) shown, the current AR will be also referred as OAR (Old Access Router) after the MN has connected to the new AR. After receiving the message, the current AR will reply to the MN with a Proxy Router Advertisement (PrRtAdv) message which contains the AP-ID (Access Point ID) of the found AP, the IPv6 address and network prefix of the NAR (New Access Router) which the AP belongs to. After receiving the PrRtAdv message, the MN is able to form a new CoA that will be used in the new access network.

2. **Fast Binding Update (FBU):** The Fast Binding Update (FBU) message is sent from the MN to the OAR after receiving the PrRtAdv message. The FBU message contains the new CoA which is derived from the information that is contained inside of the PrRtAdv message. The OAR extracts the new CoA from the FBU message, and binds the new CoA with the current CoA for forwarding packets to the NAR.

3. **Handover Initiation (HI), Handover Acknowledge (HAck) and Fast Binding Acknowledge (FBack):** After the OAR receives the FBU message; the OAR sends the Handover Initiation (HI) message to the NAR. The HI message contains the current CoA, the layer 2 address and the proposed CoA of the MN. The NAR uses the information to execute the AC process which contains a DAD process, and may be a stateful address configuration process if the proposed CoA is duplicated in the network. This AC process is exactly same the standard MIPv6 AC process which has been described in previous sections. Then, the NAR replies to the OAR by a Handover Acknowledge (HAck) message. The message is used to inform the OAR that the AC process has been completed successfully. During the AC process, if the proposed CoA fails the DAD, the HAck message may also suggest a CoA. The suggested CoA is derived from the stateful address configuration process. The CoA will be forwarded by the Fast Binding Acknowledge (FBack) message from the OAR to the MN.

4. **Unsolicited Neighbor Advertisement (UNA):** The UNA message is the last message in an FMIPv6 handover which is shown in Figure (1). The MN breaks its connection with the OAR after receiving the FBack message. The OAR then will forward the buffered packets to the new CoA of the MN. The packets will be buffered at the NAR until a UNA message is sent from the MN. Once the UNA message is received by the NAR, the NAR will remove and update internal entries, and the buffered packets will be forwarded to the MN.

2.2. The reactive mode:-

If the overlap area between two APs from two different AR is relatively small, and the MN moves too fast, the MN may be able to receive the FBack message before the OAR becomes unreachable. In this case, the predictive mode will have never enough time to be performed complete, and the reactive mode is specially designed for this situation.

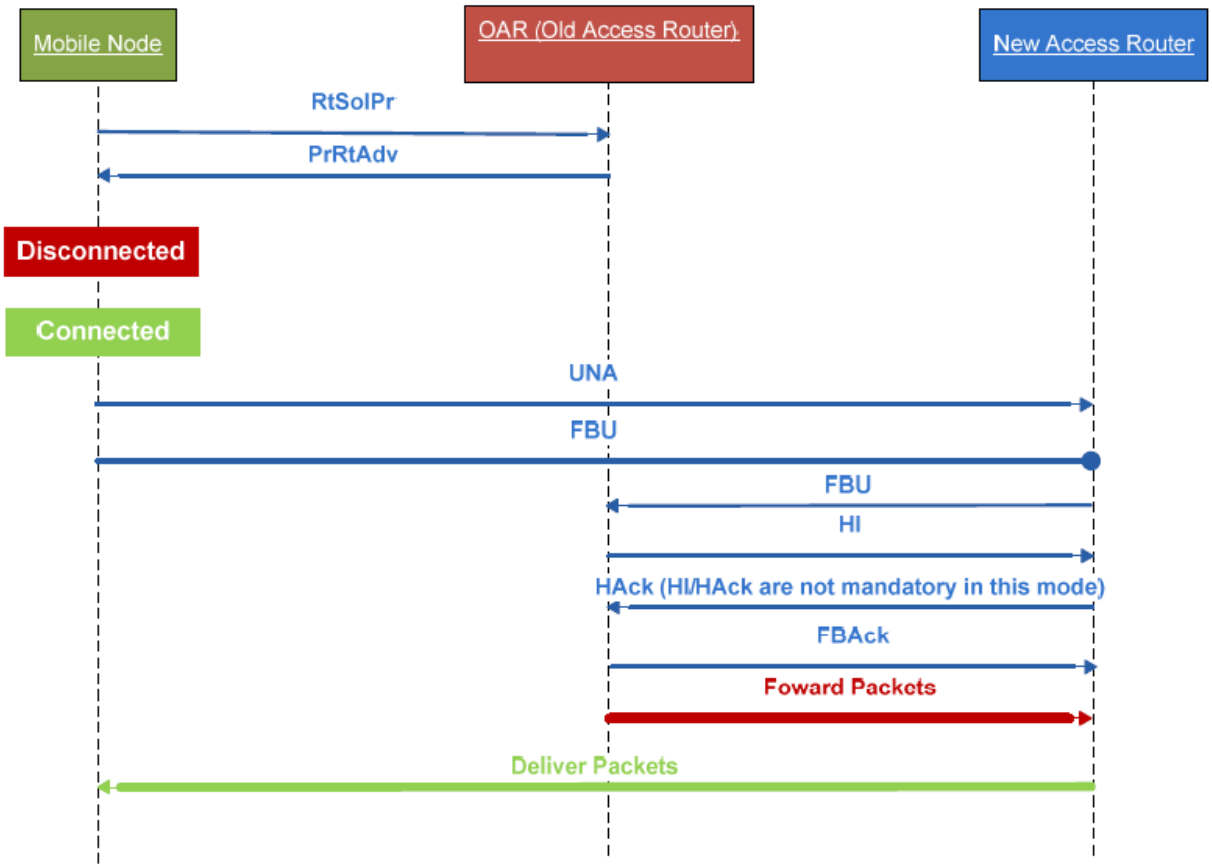

Figure 2.2 Reactive Mode

The unexpected disconnection of the OAR causes the FMIPv6 to reorder its sequence of messages. The biggest change is the order of the UNA message. The UNA message is no longer the last message sent in a fast handover, but the first message after the MN connects to the NAR which is shown in Figure 2.2. Following the UNA message, a FBU message is also sent to the NAR, and forwarded to the OAR. From this point, the message sequence becomes the same as in the predictive mode. According to the FMIPv6 standard, the HI/HAck message pair may not be required for quickening the process. At last, the OAR will send an FBack message to the NAR with the buffered packets, and the packets will be forwarded to the MN.

The main difference of the predictive mode and the reactive mode are when the UNA message has been sent in an FMIPv6 handover and where the FBU message is sent.

The reactive mode almost does not shorten the handover latency comparing to the standard MIPv6, but minimizes the packet loss by using a tunnel to forward the packets from the OAR to the NAR.

In conclusion, the main difference between FMIPv6 handover and MIPv6 handover is when the AC process is initiated. The standard MIPv6 requires two conditions to confirm a layer 3 movement which leads to the initiation of the AC process. However, FMIPv6 starts the AC process once an AP from a new access router has been detected.

3. Hierarchical Mobile IPv6 (HMIPv6)

Hierarchical Mobile IPv6 (HMIPv6) is another standard for improving the MIPv6 handover process which has been published in early 2000s and updated by IETF in 2008. It is an extension of MIPv6 like FMIPv6, and it focuses on reducing the latency caused by the BU process in a MIPv6 handover.

After an MN changes its AR, the MN needs to update its new CoA to it's HA and CNs to maintain its reach-ability. The BU messages are specially designed for this purpose.

However, when the MN is geographically too far from the HA or the CNs, the BU process may add hundreds of milliseconds to the handover process because of the propagation delay. HMIPv6 is specifically designed to solve this problem.

Instead of sending the BU messages to the relatively far HA and CNs, in HMIPv6, the MNs send the BU messages to a closer proxy server. The mechanism is demonstrated in Figure 2.3 below.

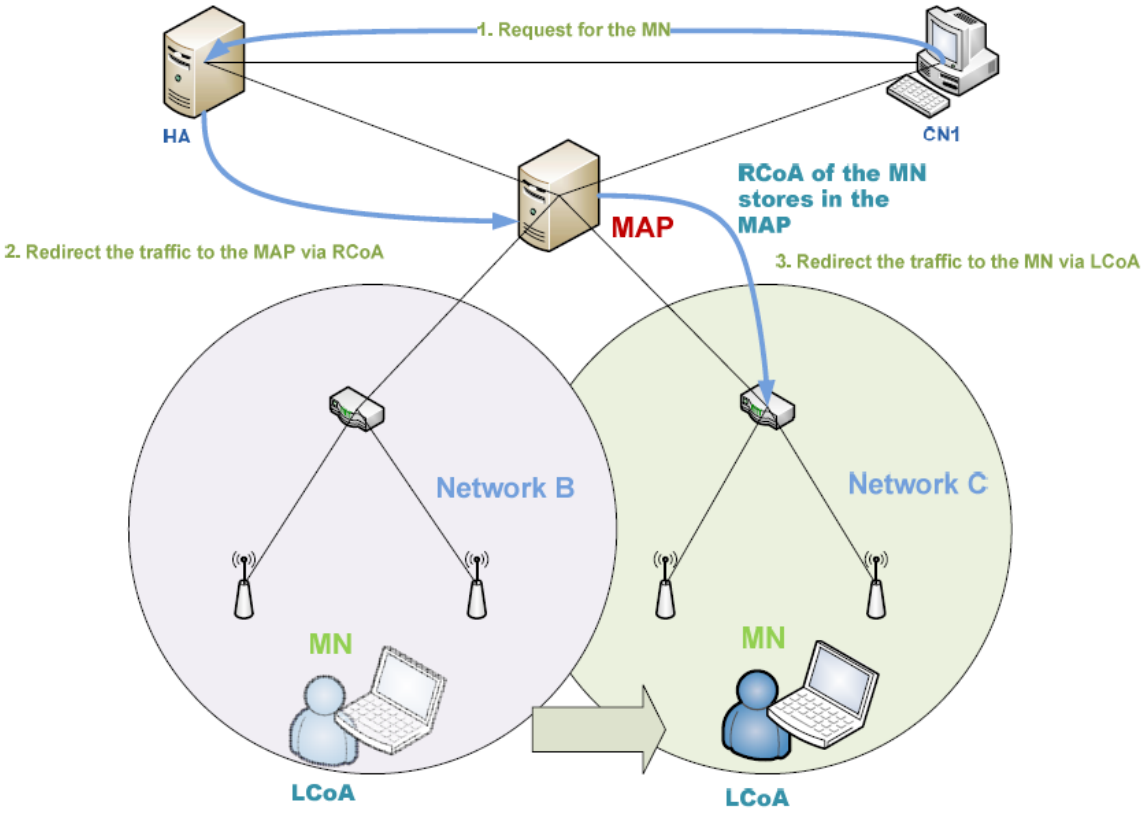

Figure 2.3 Hierarchical Mobile IPv6

In Figure (2.3), there are three new elements added to the standard MIPv6. They are MAP, Regional Care-of-Address (RCoA) and Local Care-of-Address (LCoA). MAP is the proxy server which stands for Mobility Anchor Point (MAP). It behaves like a HA which keeps tracking the location of an MN within its domain. The RCoA and the LCoA are used to allow an MAP to work with an MN's HA and the CNs seamlessly.

When an MN enters to a MAP's domain, an RCoA and an LCoA are both assigned to the MN. The RCoA is sent to the MN's HA instead of the normal CoA within a BU messages. From this point, as long as the MN moves within the domain of the MAP, the MN only needs to change its LCoA. The BU process only happens between the MN and the MAP, and the LCoA is stored inside of the MAP for updating the MN's location. The HA will not these BU processes until the MN leaves the domain, and changes its RCoA.

In MIPv6, from the perspective of a CN, every time when a CN intends to communicate with an MN, the node will send a packet to the MN's HoA, and the traffic will be directed to the MN's HA. If the MN is not within the HN, the HA

will search the binding entries to match the HoA and the CoA. In the HMIPv6, the CoA is substitute with an RCoA. Via the RCoA, the traffic will be directed to the MAP by the HA. After the traffic is received by the MAP, the MAP will search its binding entries to match the RCoA and the LCoA. At last, the traffic is sent to the MN according to the LCoA.

4. Fast Hierarchical Mobile IPv6(FHMIPv6)

FHMIPv6 is another proposed standard which was published by IETF in 2006. In order to allow the FMIPv6 and the HMIPv6 to work together, the original messages involved in a handover need to be modified to fit this purpose. Figure 2.4 below illustrates a handover process involved in FHMIPv6 in the predictive mode. Same as FMIPv6, the MN exchanges information with the OAR by the Router Solicitation Proxy (RtSolPr) and the Proxy Router Advertisement (PrRtAdv) messages.

Similar to FMIPv6, once the MN receives the hint for a handover, the Fast Binding Update (FBU) message is sent to the OAR. In addition, the FBU message is also sent from the OAR to the MAP. Comparing to FMIPv6, it is the MAP that communicates with the NAR by the HI/HAck pair messages instead of the OAR. At the same time, the OAR will buffer all the incoming packets for the MN while the MN is detached from the OAR. The MAP sends a Flush message to the OAR to indicate that the HI/HAck messages have been sent successfully between the MAP and the NAR, and the BCE will be updated in the MAP. Once the BCE is updated, the MAP will send the FBack message to the NAR with a new LCoA for the MN, and it will also forward all the packets to the new LCoA. Meanwhile, the OAR sends all the buffered packets to the NAR and end with a Flush message. Once the MN is connected to the NAR, the MN will send a FNA message. Then the NAR will forward all buffered packets and future incoming packets to the MN.

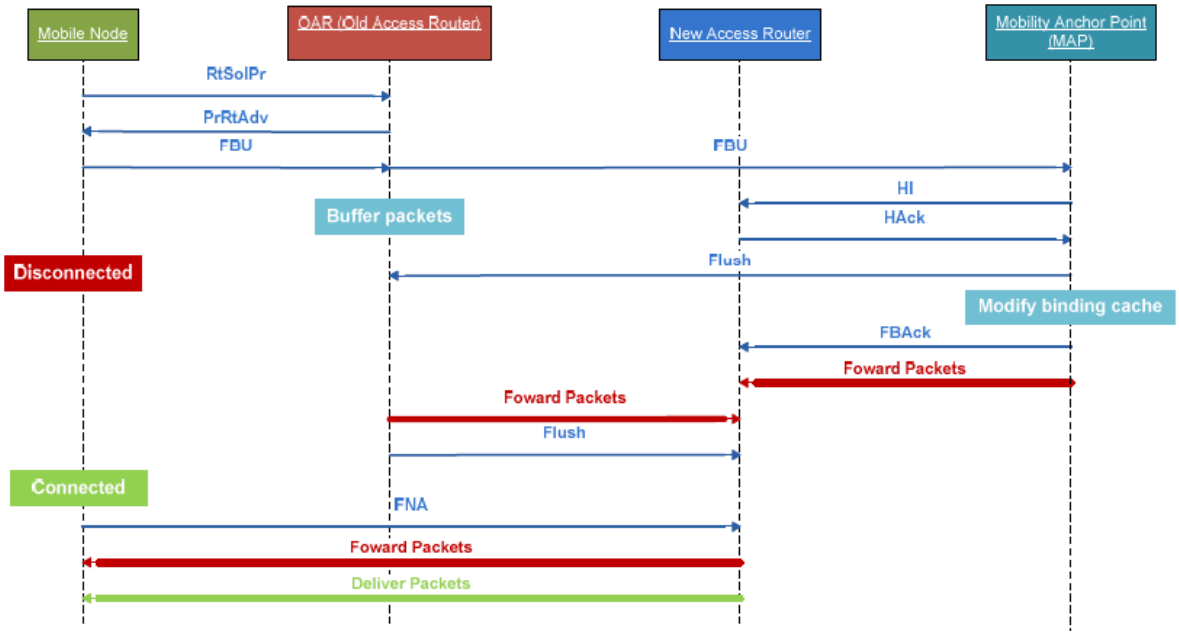

Figure 2.4 Predictive Mode of FHMIPv6

The reactive mode in the FHMIPv6 is activated when an MN has not been able to send a FBU message to the OAR to continue the predictive mode. This is mode is very similar to the FMIPv6 reactive mode. Once the MN attaches with the NAR, the MN will send a FNA message to the NAR with its information. It is the NAR's responsibility to inform the OAR that a fast handover is required. The NAR send a FBU message to the OAR, and the OAR will start to buffer the incoming packets for the MN. Since this point, the reactive mode has same message sequence as the predictive mode from the point that the OAR sends the FBU to the MAP.

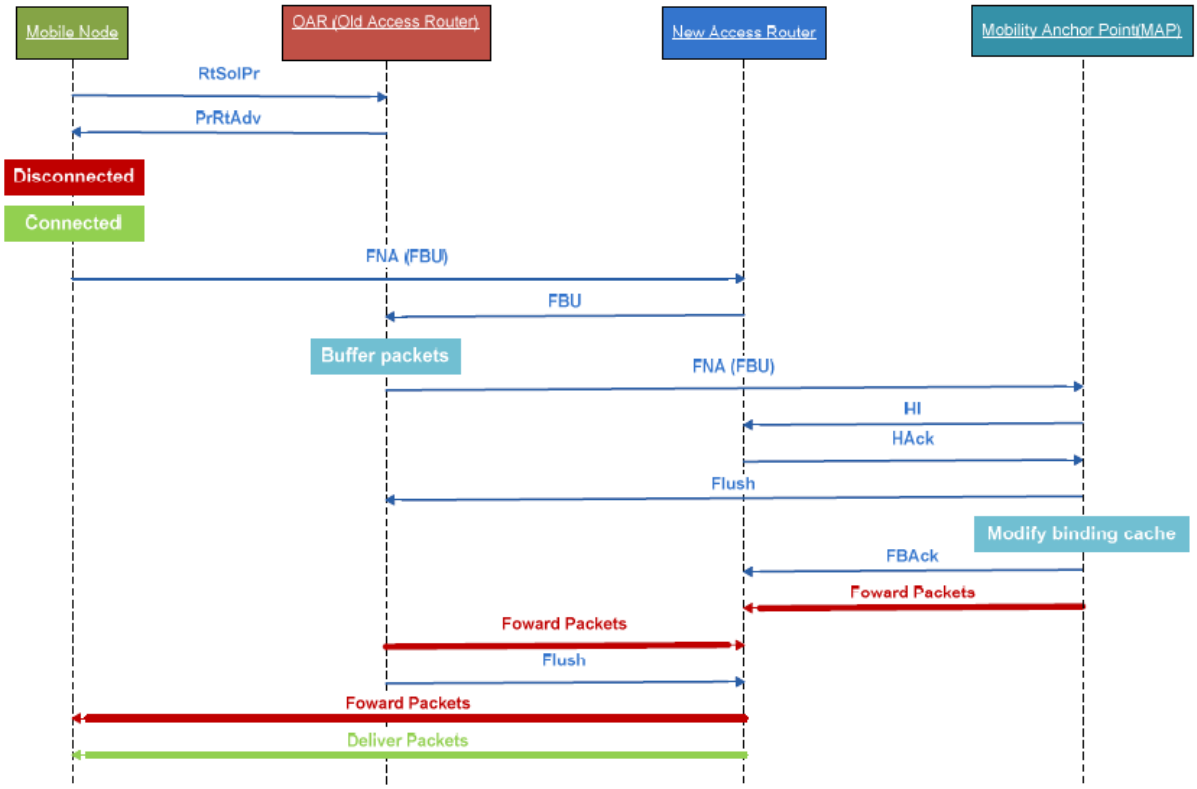

Figure 2.5 Reactive Mode of FHMIPv6

5. Seamless MIP (S-MIP)

Seamless MIP (S-MIP) was originally designed for the MIPv4 standard, and has been proposed to work with IPv6. S-MIP adopts the idea of combining the HMIP and the FMIP, and provides further improvements in two aspects. Firstly, SMIP includes the consideration of the Candidate Access Router Selection (CARS) process which is neglected by other proposals. This is achieved by using three routers to track the physical location of the MNs, and a server to determine the best Candidate Access Router respectively. Secondly, the mechanism intends to avoid the case which the forwarded packets may be out of order during a handover. This is achieved by separating the forwarded packets from the different sources, and sending them at different chunk of time.

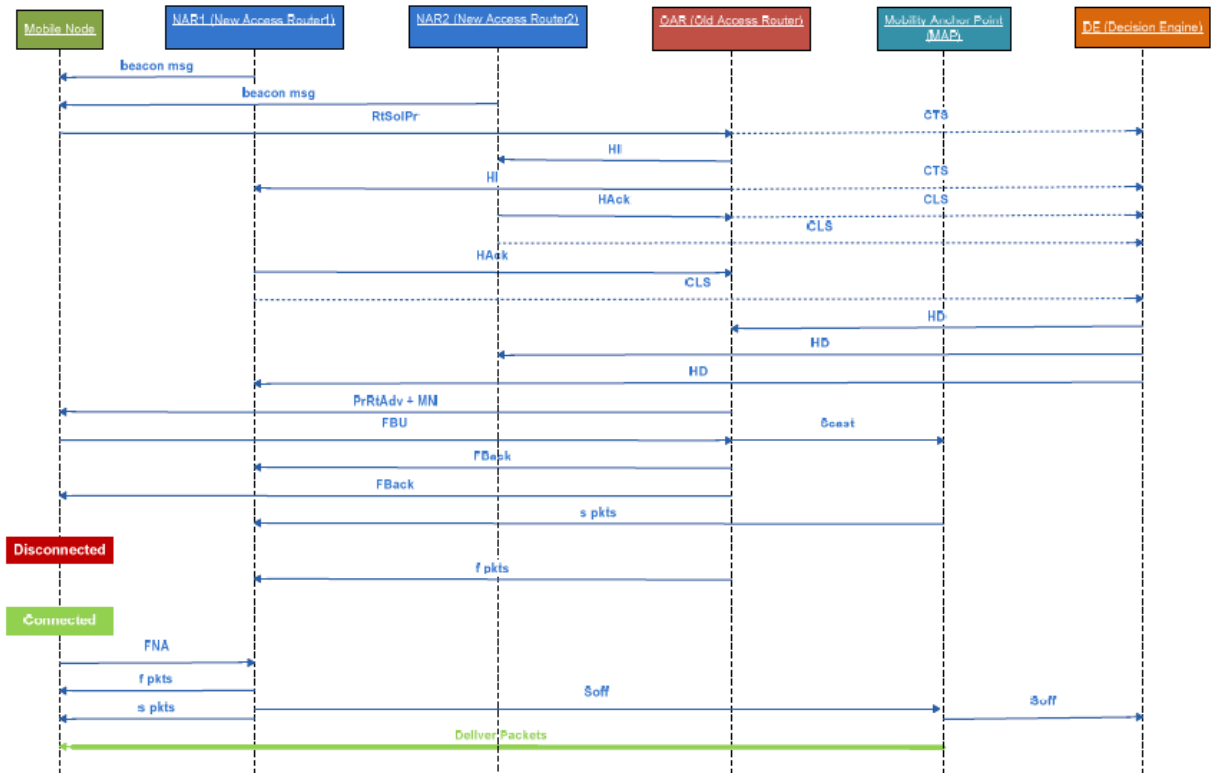

Figure 2.6 The message sequence of S-MIP

As Figure 2.6 shown, the S-MIP has one extra entity and multiple new messages compare to FHMIPv6. To make the concept more clearly, the names and the functionalities of the entity and the messages are listed below.

Current Tracking Status (CTS) message is used to track the physical location of the MN for DE.

Carrying Load Status (CLS) message contains the information regarding to the loading capacity of the AR.

Handoff Decision (HD) message contains the handover decision information from the DE. It informs the entire candidate ARs which AR has been chosen for the MN.

Handoff Notification (HN) message is sent from the OAR to the MN. It indicates which NAR the MN should connect to. The content of the message is derived from the HD message.

Simulcast (Scast) message is the message which starts the Synchronized-Packet-Simulcast (SPS) process. The SPS process is used for separating the packets from the OAR and the MAP. By doing this, there will be less possibility of massing the order of the packets.

Simulcast off (Soff) message terminates the SPS process.

Decision Engine (DE) is the entity which uses the information from the CTS and CLS messages to make the handover decision.

A handover process in the S-MIP starts with detecting the NARs from an MN. Once the MN receives beacon messages from the NARs, the MN will send an RtSolPr message to the OAR. The OAR will immediately sends the CTS message to the DE to update the location of the MN. Then the OAR sends HI message to all the NARs, and the NARs will send their own CTS message to the DE too. All the CTS messages will be used for the DE to work out the exactly physical location of the MN. In response to the HI message, all NARs will send back a HAck message back to the OAR, and the CLS messages are also sent to the DE for the handover decision. After the DE makes the decision basing on the capacity loading status of each NAR and the location of the MN, the DE sends the HD messages to the OAR and all the NARs for the result of the decision. HN and PrRtAdv messages will be returned to the MN by the OAR. The MN replies a FBU message to the OAR, and the OAR will send a Scast message to the MAP to start the SPS process. The OAR will also reply a FAck message to the selected NAR and the MN each. At the mean time, because of the SPS process, the buffered packets from the NAR and the MAP are labelled with "f" and "s" header respectively.

Once the MN completes the L3 handover with the NAR, the NAR will forward the "f" packets and "s" packets in sequence. Each forwarding process is terminated with the Soff message. At last, the MAP will be able to forward all incoming packets directly to the MN with the new CoA

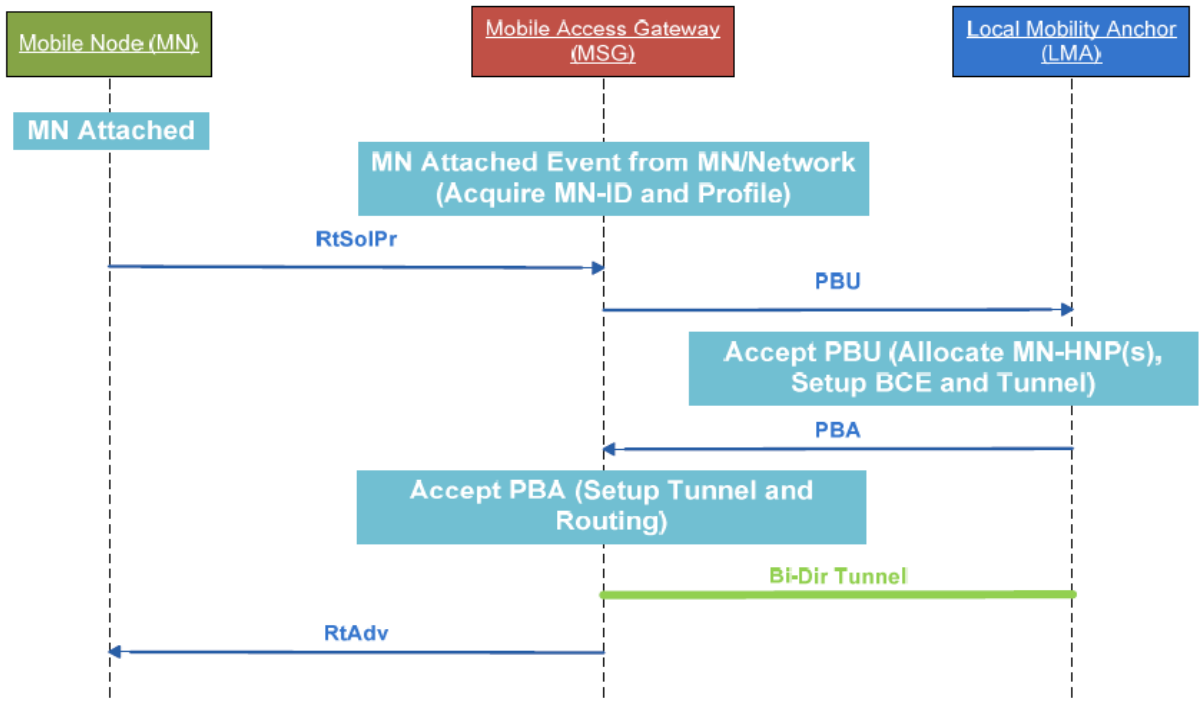

Figure 2.7 Processes occurring during MN Registration in a PMIPv6 Domain

Figure 2.7 illustrates the events and messages occurred during an MN registration to a PMIPv6 network. When an MN first time enters a PMIPv6 network, the MN will be notified an event "MN Attached". Meanwhile, the MAG detects the attached MN, and start to acquire MN-ID and profile information. Then the MN requests the MAG's information by sending a Router Solicitation (RtSol) message. Different from MIPv6, the MAG sends a Proxy Binding Update (PBU) to the LMA first instead of replying the Router Advertisement (RtAdv) message to the MN immediately. The LMA uses the information contained inside of the PBU message to update its Bind Cache Entries (BCE) for recording the location of the MN, and request for setting up a bi-directional tunnel. The request of the tunnel and the Home Network prefix(es) of the MN are sent back to the MAG by the Proxy Binding Acknowledge message. Once the PBA is accepted by the MAG, the bi-directional tunnel is set, and the MAG replies the MN with the Router Advertisement (RtAdv) message. The RtAdv contains the MN's Home Network prefix (es), and the MN will consider it is at the Home Network.

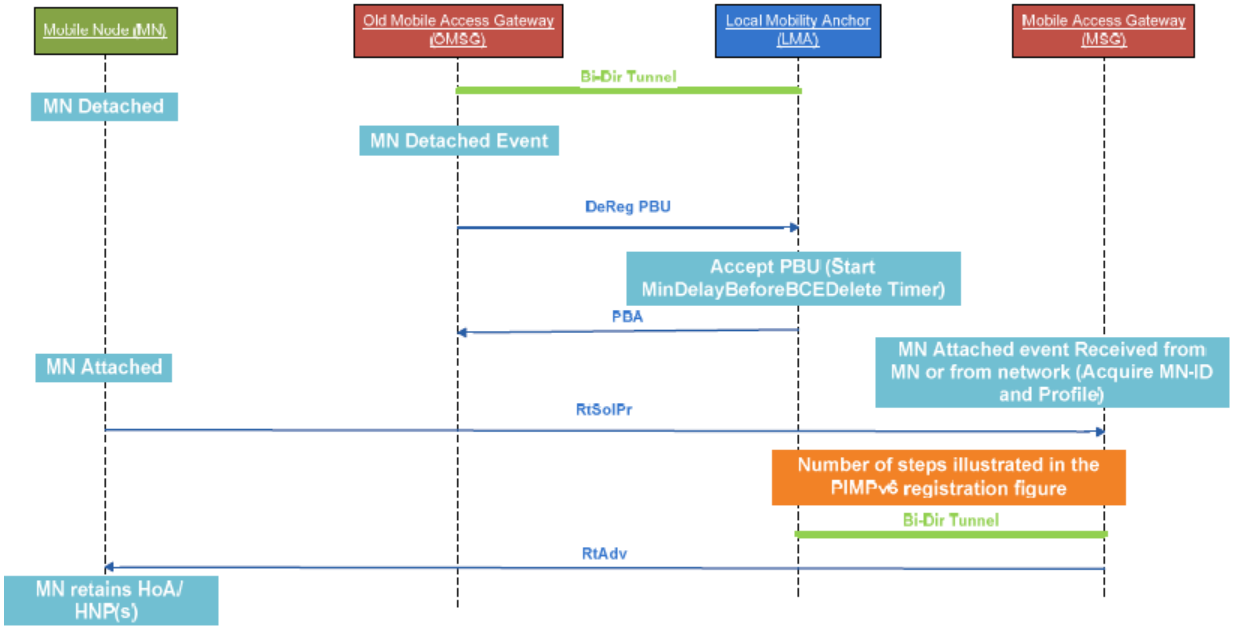

Figure 2.8 Processes of a handover in a PMIPv6 domain

When the MN changes the access network within a LMA domain, the handover procedure follows the above figure. Once the MN has been detached from the Old Mobile Access Gateway (OMAG), both the MN and the OMAG will be notified. The OMAG then sends a De-Registration Proxy Binding Update (DeReg PBU)

message to the LMA for updating the location of the MN and removing the bi-directional tunnel.

The LMA waits for the "MinDelayBeforeBCEDelete" amount of time for the New Mobile Access Gateway (NMAG) to updates the location of the MN. If the timer expires, the MN's location entry will be removed from the BCE. Then the LMA replies the OMAG with the PBA message. If a NMAG does reply to the LMA before the timer expires, the registration process has been described in the last paragraph will be repeated. However, it is not always true like the figure shown that the MN's attachment to the NMAG is after its detachment with the OMAG.

Therefore, the performance of these solutions is scenario-dependent which makes them hard to compare. For example, the HMIPv6 shortens the handover process by improving the Binding Update process, and the FMIPv6 shortens the handover by performing the Address Configuration process before it is required. Since the duration of the Binding Update process strongly relies on the propagation delay of the network, the HMIPv6 may have a better performance than FMIPv6 in some cases, but worse in others. Precise specification of applications which perform better under specific handover mechanism will be possible when their accurate simulation models become available. Currently, the only credible MIPv6 simulation models are those in OMNeT++ and probably in OPNET.

Chapter (3)
Overview about Handover

3.1. Handover:-

In the wireless network aspect, a handover is usually referred to transferring an ongoing call or data session from one subnet to another. The process can also be known as handoff. A handover process usually causes a transmission to be discontinued in a period of time, so the user may experience a long extra delay for the application he or she is using. During the period, a large amount of packets can be lost depending on the speed of the connection, and the QoS will drop dramatically.

3.2. Types of Handovers:-

Currently, there are many different types of handovers which can be categorized by the connection status, the technology used, the network topology or the layer where they occur in the OSI model.

1. **Soft Handover and Hard Handover**

When the handover process is categorized according to its connection status, a handover can be soft or hard. The difference between them is based on whether a mobile device maintains a connection with at least one access points during the handover process. In the handover period, if the mobile device keeps its connection with the old access point until it fully establishes its connection with a new access point, the handover is called a soft handover. In contrast, if the mobile device breaks its connection with the old access point before it is connected with a new access point, we deal with a hard handover.

2. **Inter-technology Handover and Intra-technology Handover**

In the wireless network area, there are many different types of wireless access technology have been developed. Each of the technology provides different connection range, network capability and so on attributes. In future, it is very likely to see all these technologies coexist and complement to each other. Therefore, it may be frequent to see a mobile device using different access technologies while moving. If a handover happens between two different technologies, we deal with an inter technology handover. Otherwise, it is an Intra-technology handover.

3. **Horizontal Handover and Vertical Handover**

Horizontal handover and vertical handover are distinguished by whether a mobile node has changed its access network or access router. The following figure illustrates a horizontal handover.

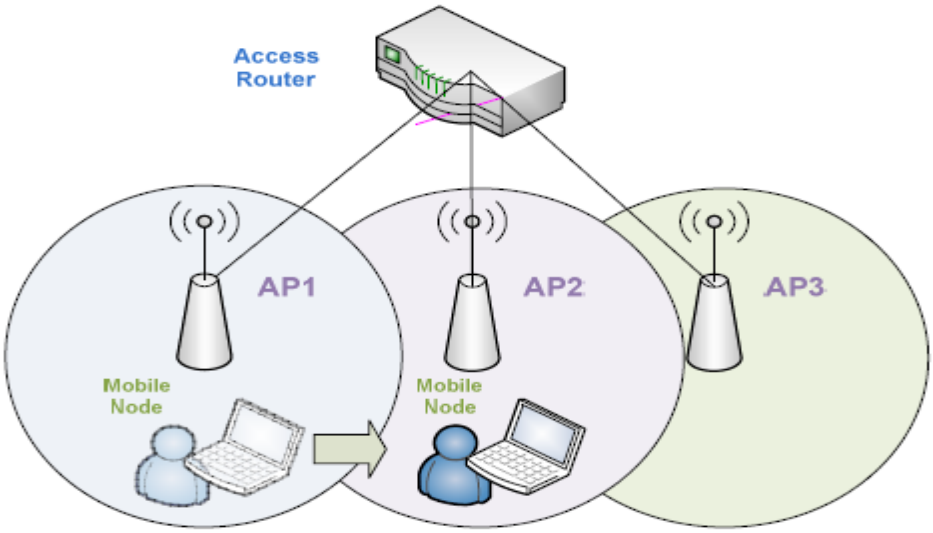

Figure 3.1 **Horizontal Handover**

Figure 3.1 depicts a mobile node moving from the access range of AP1 to AP2. As the figure demonstrated, both AP1 and AP2 are connected with the same access router. This means there is no topological change from the perspective of the mobile node.
Therefore, it is a horizontal handover.

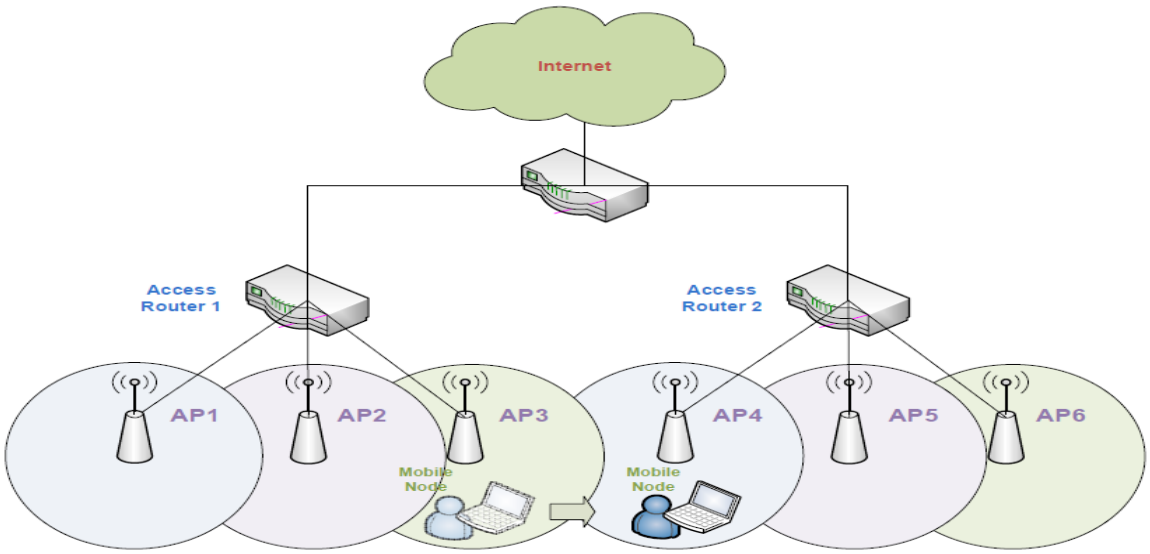

Figure 3.2 Vertical Handover 1

Figure 3.2 demonstrates a scenario of a vertical handover. In this figure, the mobile node moves from the access range of AP3 to AP4. As the figure shown, AP3 and AP4 are connected with different access router. Since the access router of the mobile node has changed, the access network topology is also changed. Therefore, it is a vertical handover.

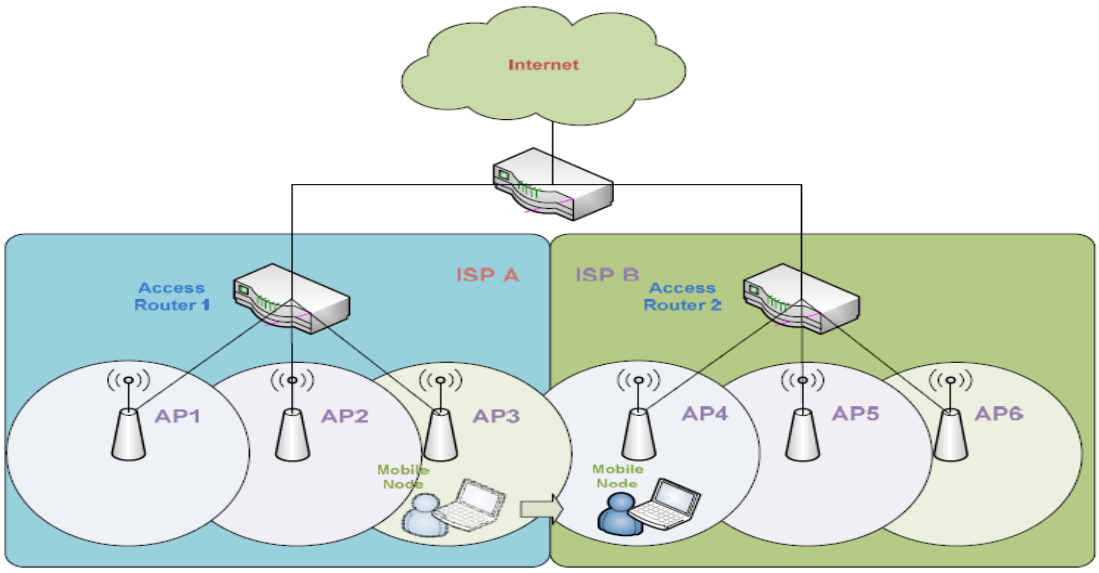

Figure 3.3 Vertical Handover 2

Vertical handover does not only happen within the network of one Internet Service Provider (ISP), it can also happen between ISPs. Figure 3.3 demonstrates such a vertical handover that happens between ISPs. In the figure, the mobile node moves from AP3 to AP4 where AP3 and AP4 are connected with different access routers which belong to different ISPs.

4. Layer 2 and Layer 3 Handover

A complete vertical handover consists of the processes occurring in layer 2 and layer 3. The processes occurring within layer 2 are known as layer 2 handover, and the processes occurring within layer 3 are called layer 3 handover. The layer 2 handover often indicates the changes of the access point, and the handover delay in this layer is often media or technology dependent. The layer 3 handover often indicates the change of the access route, and the length of the delay is related to the

network protocol. A handover in MIPv6 is a layer 3 handover which is the main focus of this project.

3.3. Handover in MIPv6

1. MIPv6 Terminology and Conditions

This section lists the terminologies which will be used to explain a MIPv6 handover in later sections.

Mobile Node (MN): MN is a terminal that moves between networks.

Access Point (AP): AP is the facility that provides the radio connectivity to MNs.

Access Router (AR): AR is the router that provides Internet connectivity to MNs.

Home Address (HoA): HoA is a unicast address which is permanently assigned to an MN. Usually the traffic will be delivered to the MN by this HoA directly.

Home Agent (HA): HA is the AR that assigns the HoA to an MN. The assigned HoA should have the same network prefix as the HA. The network prefix is a part of IPv6 address.

Home Network (HN): HN is the network where MN has acquired the HoA. It is the network where the HA belongs to.

Care-of-Address (CoA): CoA is a temporary address for an MN while it is not at the HN.

Foreign Access Router (FAR): FAR stands for Foreign Access Router which refers to any AR provides Internet connection to an MN except HA. Please note it is not a Foreign Agent as MIPv4, since there is no special router required in MIPv6.

Foreign Network (FN): FN is the network where the MN is currently connecting with but not HN.

Correspondent Node (CN): CN is the terminal that is currently communicating with the MN.

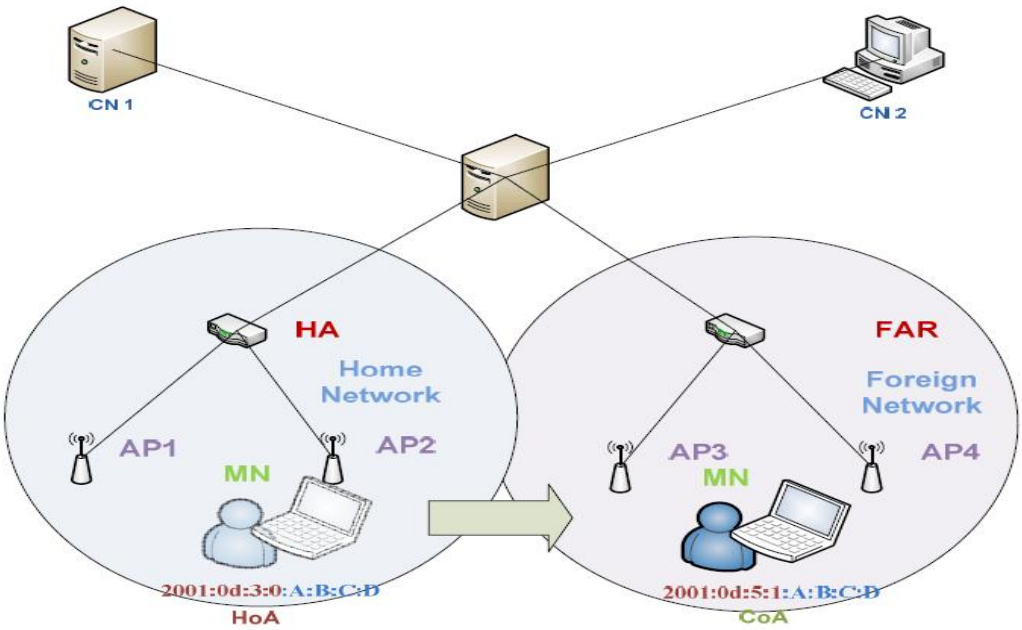

Figure 3.4 Graphical Explanations of the MIPv6 Terminology

Figure 3.4provides a graphical demonstration to all the terms mentioned above.

In Figure (3.4), the MN (Mobile Node) is labeled with light green colour. It is indicated by an icon which is a combination of a user icon and a laptop icon. In the figure, the MN travels from its HN (Home Network) to a FN (Foreign Network), and range of these two networks are indicated by different colour of circles. Inside of each circle, there are one access router and two access points. In the HN, the access router is the HA (Home Agent) of the MN. In the FN, the access router is referred as FAR (Foreign Access Router). Below the MN's icon, it is the current IPv6 address of the MN.

When the MN is at the HN, the MN uses its HoA (Home Address). When the MN is at FAR, the MN uses its CoA (Care-of-Address). The addresses are labeled with different color in the figure because they represent different parts of an IPv6 address. There are two desktop icons which indicate the CNs (Correspondent Node) of the MN. In this context, the CNs are the computers or servers which are currently communicating with the MN.

3.4. **The Processes of MIPv6 handover:-**

A MIPv6 handover can be divided into five different processes: Movement Detection (Movement Detection), Candidate Access Router Selection (CARS), Address Configuration (AC), Authentication & Authorization (A&A), and Binding Update (BU) which are demonstrated in Figure 3.5. Each of these sub-processes is described in detail in the following sections.

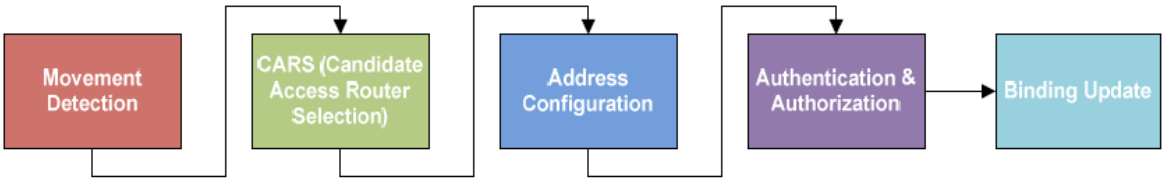

Figure 3.5 Basic Procedures of an MIPv6 Handover

1. Movement Detection

Movement Detection is a process that recognizes when a Mobile Node (MN) has moved away from its current access network. It is the first stage of a handover. When the movement of the MN is confirmed, a sequence of other handover sub processes shown in Figure 3.5 will be performed.

The movement of an MN is confirmed when the following two conditions are both satisfied:

1. A new AR has been detected by the MN.
2. The current AR has become bi-directional unreachable. It means that the MN is not able to reach the AR, and the AR is not able to detect the MN either.

These conditions guarantee a handover occurs only when it is necessary. In another words, it means the MN will not perform a handover unless it realizes that the current Internet connection is not available any more. This is one of the reasons why the QoS will drop dramatically during a handover. The Movement Detection process is defined this way to avoid packet loss and signaling overhead during the Binding Update which is the last stage of a handover.

The Movement Detection conditions are tested by the facilities of the IPv6 Neighbour Discovery (ND) which includes the Router Discovery (RD) and the Neighbor Unreachability Detection (NUD).

The Movement Detection process employs two messages from the IPv6 RD messages to confirm the first condition of a network movement. The employed

messages are the Router Solicitation (RS) and the Router Advertisement (RA) messages. The mechanism of detecting a new AR behaves as follow. In the MIPv6 wireless networks, every MIPv6 enabled wireless router multicasts a RA message through its APs periodically.

The duration of the period is defined by two configurable values MinRtrAdvInterval and MaxRtrAdvInterval in the router. If an MN has been waiting for a RA message from the current AR more than MaxRtrAdvInterval time, the MN will consider it as a movement hint. Then the MN will immediately multicasts a RS message. If any router receives the message, it will reply to the MN with a RA message. This message contains the global IPv6 address of the router and link address of the APs. Once the MN receives a RA which contains a new IP address of an AR (Access Router), the first condition of the Movement Detection is considered to be satisfied. If the MN receives a RA from a new AR without sending RS message, the first condition is also considered to be satisfied.
The Neighbour Unreachability Detection (NUD) in IPv6 is used to check for the second condition of a network movement. It verifies the current AR of the MN has become bi-directional unreachable. The behaviour of the NUD are specified by RFC 2461 [33], and depicted in Figure 3.6. According to RFC 2461, every IPv6 node can have five statuses: “Reachable”, “Stale”, “Delay”, “Probe” and “Unreachable”.

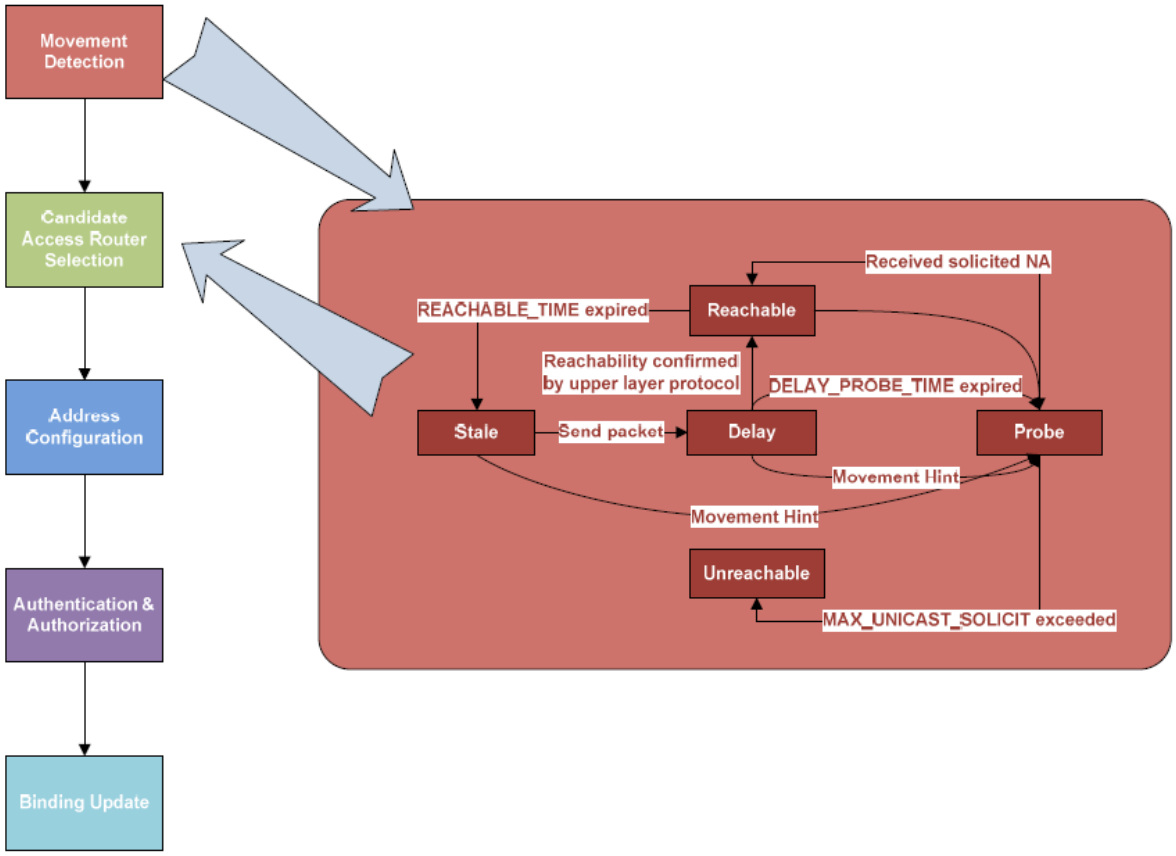

Figure 3.6 State transitions during the execution of the Neighbor Unreachability Detection Procedure

When an MN enters to a new network, it multicasts ND messages to find the possible neighbors. Once the MN receives a replied message from a neighbour, the state of the neighbour will be recorded as “Reachable”. After a fix time interval which is known as “REACHABLE_TIME”, the state of the neighbour will change to “Stale”.

There will be no further state change until the MN sends a packet to the neighbor. Once a new packet is sent by the MN, the state of the neighbor will be labeled as “Delay”. During the “Delay” cycle, the MN waits for reply from the neighbour for another time interval called “DELAY_FIRST_PROBE”. If the MN does not receive replies from the neighbour within the time limit, the state of the neighbour will change to “Probe”. In this stage, the MN waits a time interval which may take as long as multiple times of the interval between the periodic Neighbour Solicitation (NS) messages. If the MN still does not receive any reply from the neighbor, the state of the neighbour will be changed to “Unreachable”. The waiting interval is exactly specified by MAX_UNICAST_SOLICIT variable times the time interval between the periodic NS messages. The time interval

between the periodic NS messages is specified by RETRANS_TIMER variable which can be customized as well as MAX_UNICAST_SOLICIT variable.
In conclusion, the duration of the Movement Detection process essentially depends on the value of MaxRtrAdvInterval, MAX_UNICAST_SOLICIT and RETRANS_ TIMER.

2. Candidate Access Router Selection (CARS)

After a layer 3 movement has been detected by an MN, the MN needs to connect to a new AR to maintain its network connection. The process of selecting a CAR consists of two parts: the Candidate Access Router Discovery process and the Target Access Router Selection (TARS) process.

2.1 Candidate Access Router Discovery

CARD is an IETF experimental protocol which has been published one year after the standardization of MIPv6.The major functions of CARD are acquiring the IP addresses of the Candidate Access Routers (CARs), and discovering the ARs' capabilities.

2.2 Target Access Router Selection (TARS)

TARS can be performed by either the MN or the current AR. The capability information of the CARs which are obtained from the CARD process is fed into the TARS process. The TARS process uses specific algorithm to choose the most appropriate Access Router (AR). The capacity information includes information about such properties of the CARs as: bandwidth, available channels and so on. Since there is no standard algorithm for this process.

3. Address Configuration

After the new AR has been selected, the MN will need a new temporary IPv6 address according the RFC 3775. The process of acquiring of the address is called Address Configuration (AC). The temporary address is usually known as Care-of-Address (CoA).
There are two approaches to obtain a CoA for an MN. One is the stateless address configuration, and the other is the stateful address configuration.
The stateful address configuration is usually performed by DHCPv6 which behaves in a similar way as DHCPv4. The method in general appears to be too time consuming for a handover. Therefore, the stateless address configuration is usually preferred.

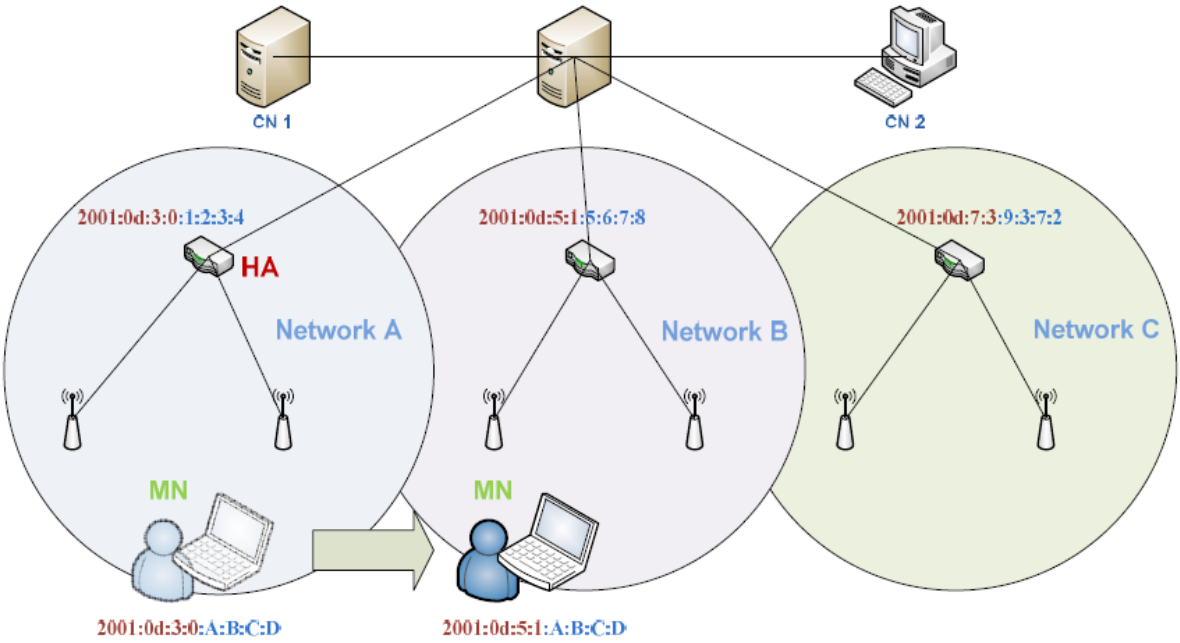

Figure 3.7 Example of an Address Configuration Process

In a wireless IPv6 network, every MN and sub network has an interface identifier. The stateless address configuration forms the CoA by combining the prefix of the network and the prefix of the MN. This is demonstrated in Figure 3.7. In this figure, the red part of IP addresses is the network prefix, and the blue part is the MN prefix.

After the MN has moved from network A to network B, the IP address of MN has changed its network prefix only, but keeps using the MN's prefix which is the second part of the CoA.

A CoA can be used only after it has passed the Duplicate Address Detection (DAD), and this process has been standardized by IETF. The standard only defines how to detect whether a CoA is unique, but it does not mention the procedures after a duplicated address is found. "A tentative address that is determined to be a duplicate as described above, MUST NOT be assigned to an interface and the node SHOULD log a system management error. If the address is a link-local address formed from an interface identifier, the interface SHOULD be disabled". Disabling an MN, when it fails the DAD is not a desirable solution in practice. For most of the Wireless Internet Service Providers (WISPs), it is more logical to use stateful address configuration as a backup procedure.

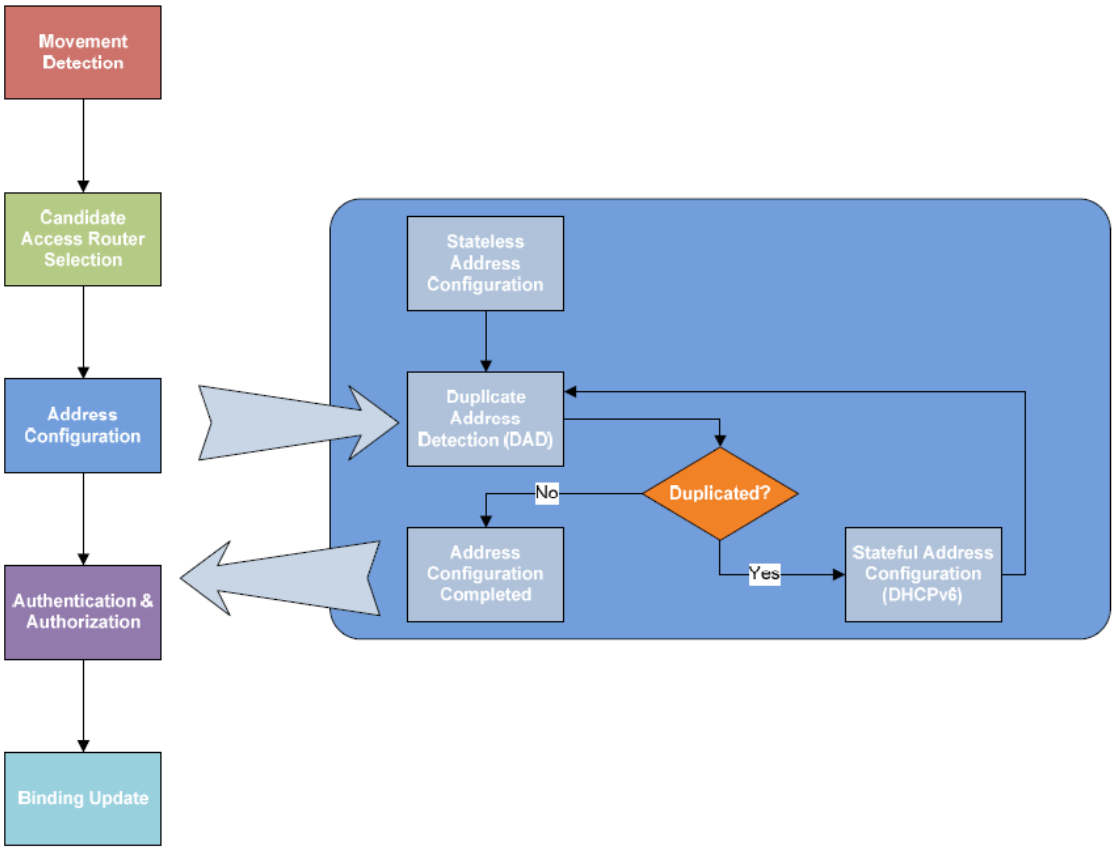

Figure 3.8 **Sub-processes of the Address Configuration**

Figure 3.8 demonstrates all the states in an address configuration process. The process starts with a stateless address configuration which is used to form a CoA. The newly formed CoA will be tested by the DAD, and if the address is duplicated, a stateful address configuration will be performed. The stateful address configuration will assign a new CoA to the MN, and address will be tested by the DAD again. This cycle repeats until the assigned address passes the DAD. Once the address has been confirmed to be unique, the handover will shift to another stage which is Authentication and Authorization.

4. **Authentication and Authorization (A&A)**

The A&A process is used for checking whether an MN has the authority to use the connection from an AR.

5. **Binding Update**

Bind Update (BU) is the last stage in a handover process. The purpose of the BU is to keep tacking the network location of an MN for its Home Agent (HA) and the

Correspondent Nodes (CN). The BU process is completed with assist of two messages which are a BU message and a Binding Acknowledge (BACK) message.

5.1 Binding Update message to HA

Inside of every HA, there is a Binding Cache Entries (BCE) table where records both the HoA and CoA of MNs. The BCE allows the MNs to be reachable in Internet, and it is frequently updated by BU messages.

5.2 Binding Update to CN

The BU is sent to CNs only when the "route optimization" mode is used in IPv6. In the MIPv6 standard there are two communication modes between MN and CN. One is "bi-directional tunnel" mode, and the other one is "route optimization" mode.

In the "bi-directional tunnel" mode, MNs are not required to register on its CNs. HA is the only node that keep tracking the location of MNs. When a CN intends to send a packet to an MN, the packet will have to be delivered to the HA of the MN first. The HA then will redirect the packet to the MN. Conversely, if the MN tries to send a packet back to the CN, the packet will need to be sent to the HA first. The HA then will redirect the packet to the CN.

In the "route optimization" mode, the HA is excluded from the packet delivery. The CN keeps a BCE itself for tracking the location of the MNs. In this case, any packets between CNs and MNs are transmitted directly. The "router optimization" mode obviously saves more network resource and reducing the round trip time between the MN and the CNs. Therefore, in general, for a MIPv6 handover, the "router optimization" mode is used, and the BU messages are sent to both HA and CNs.

c. Binding Acknowledgement (BACK)

If a BU message has been successfully received by an MN's HA or a CN, the HA or the CN will reply a BACK message to the M.

Till here, we have finished describing all the stages in a standard MIPv6 handover. Then we will be able to understand how the existing solutions can shorten the duration of a MIPv6 handover.

Chapter (4)

Methodology and Simulation

1. Methodology:-

A handover consists of a Link Layer handover and of a Network Layer handover. The Link Layer handover includes a Discovery phase (scanning the channels to discover an available Access Point), an Authentication phase, and a Re-association phase, whereas the Network Layer handover is concerned by a Router Discovery phase, a Detection Address Duplication (DAD) phase, a Binding Update phase and a Binding Acknowledgement phase respectively. The standard MIPv6 handover latency has been estimated to a maximum value of 1290 ms. This long latency is not acceptable for real time applications such as video and audio. If analyze each phase during the Network Layer handover in figure(1) (Router Discovery, DAD, Binding Update and Binding Acknowledgement), Can note that the DAD latency costs almost 1000 ms and has a heavy weight on the global handover latency. As a result, in order to reduce the total handover latency, now a new procedure is developed to avoid any DAD operation during handover procedure. A new local intelligent entity is introduced called Lightweight Handover Control Function (L-HCF) which should be capable of controlling its attached Access Routers (ARs), Access Points (APs) and Mobile Nodes (MNs). Linked directly with its ARs, each L-HCF router reserves beforehand a list of all available IP local addresses. The L-HCF router also generates and updates periodically a second list which records the used ARs/APs/IP addresses. By comparing these two lists, the L-HCF router can find a potential duplicate IP address (collision) in its domain. Then, this L-HCF router can withdraw this potential duplicate IP address or can ask a concerned sub-node to change its IP address. In this way, the L-HCF router enables to insure an unique IP address to a MN without DAD. Furthermore, an L-HCF router could exchange both some local information with its ARs/APs/MNs and some external information with other L-HCF routers.

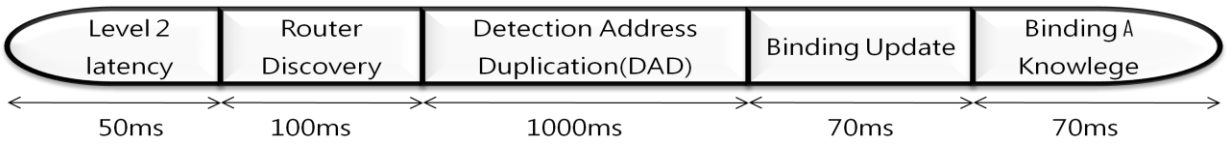

Figure 4.1 Handover standard delay time

To realize L-HCF method six new messages proposed: MN Request (MNReq), MN Reply (MNRep), HCF Request (HCFReq), HCF Reply (HCFRep), Connection Established Information (CEInf) and Handover Finished Confirmation (HFCon) messages.

- ✓ LEHCF: Total handover latency with the L-HCF approach.
- ✓ Lscan: Latency due to the MN's original scanning of its neighbour AR/AP's information.
- ✓ LMNReq: Latency for a MN to send a MNReq message to its L-HCF original router.
- ✓ Ldec: Latency necessary to an L-HCF router to decide which AR/AP the MN should be attached (including the short delays to send an HCFReq message and to receive an HCFRep message).
- ✓ LMNRep: Latency for an L-HCF router to send a MNRep message to the MN.
- ✓ LCNinf: Latency necessary for a MN to auto-configure its new CoA.
- ✓ Lconf: Latency due to the fact that an L-HCF router sends buffered packets and a HFCon message.
- ✓ LBU=BA: Binding Update/Binding Acknowledgement latency.

For the mobile IPv6 protocol and IEEE 802.11/802.16 networks context, a MN surveys periodically the received signal strength. When the signal strength drops below a predefined threshold, the MN must discover and connect itself to a new available AP for granting its communication with its correspondence. It reports to its L-HCF router (via its attached AR/AP) some AP's Basic Service Set IDentifier (BSSID) and signal strengths that it was probed. Based upon the reported information, the AR/AP's loading and the MN's Quality of Service (QoS) requirements, the L-HCF router decides which AP, the MN shall associate with and notifies the MN about the new AR/AP information, such as a new AP's BSSID, an AR interface address, a sub-network prefix and an IP address.

Consequently, the MN can configure its new Care-of-Address (CoA) and can take care of the Binding Update process even if it is still attached with its previous AR/AP. An L-HCF router can guarantee that the new IP address is unique thanks to the knowledge of its lists. If a MN moves to another domain, the L-HCF original router guarantees the new IP address by exchanging some data with the new L-HCF router. Moreover, in order to minimize the packet loss during a handover, an EHCF router stores packets into a buffer until the MN is really attached to the new IP address.

2. L-HCF Procedure:

Each *L-HCF* router must record and update its database periodically. This database helps to decide an unique new IP configuration in order to adapt for *MN* movements without the *DAD* phase during a handover. The *L-HCF* procedure is composed of the following steps:

- ✓ Moving in the network, if the threshold of the received signal strength is overstepped, the *MN* begins to probe the neighbor *AR/A*P's information, including the signal strength, some IP addresses, *AP*'s *BSSIDs*, *AR* interface addresses and the sub-network prefix. Then the *MN* sends a *MNReq* message to its *L-HCF* original router (via its *AR/AP*) to report this information.
- ✓ Receiving the *MNReq* message, the *AR* stops to forward all the packets sent to the *MN* and forwards them to its *L-HCF* original router in order to avoid the packet loss during the handover procedure.
- ✓ Receiving the *MNReq* message, the *L-HCF* original router decides to which *AR/AP* the *MN* will be associated. The choice of the *AR/AP* is mostly based on database obtained with periodic exchange messages from an *EHCF* router to another (*HCFReq* and *HCFRep* messages) or with periodic exchange messages from *ARs/APs/MNs*. For example, if the number of registered *MN*s in one *AR* or *AP* has reached a limit, the *L-HCF* original router will not attach the *MN* to this saturated *AR* or *AP*. After making the previous decision, the *L-HCF* original router sends to the *MN* a *MNRep* message which consists of a new *AP*'s *BSSID*, an *AR* interface address, a sub-network prefix and a new IP address.
- ✓ With the *MNRep* message, the *MN* can obtain its new *CoA* and configure it automatically.
- ✓ The *MN* sends a *CEInf* message to its *L-HCF* original router to confirm its new attachment.
- ✓ After receiving the *CEInf* message, the *L-HCF* original router transfers the buffered packets to the *MN*'s new *CoA*. Then, the *L-HCF* original router sends an *HFCon* message to end the handover procedure.
- ✓ The *MN* can then exchange Binding Update (*BU*) and Binding Acknowledgement (*BA*) messages with its home agent and its correspondent node. As shown in the *L-HCF* procedure, a *MN* can obtain its new *CoA* before it really attaches to its next *AR/AP*. Moreover, any *DAD* latency (about 1000 ms) is avoided. Thus, the *L-*

HCF approach allows the reduction of both the traditional handover latency and the packet loss. The handover performance is thus optimized compared to a traditional approach.

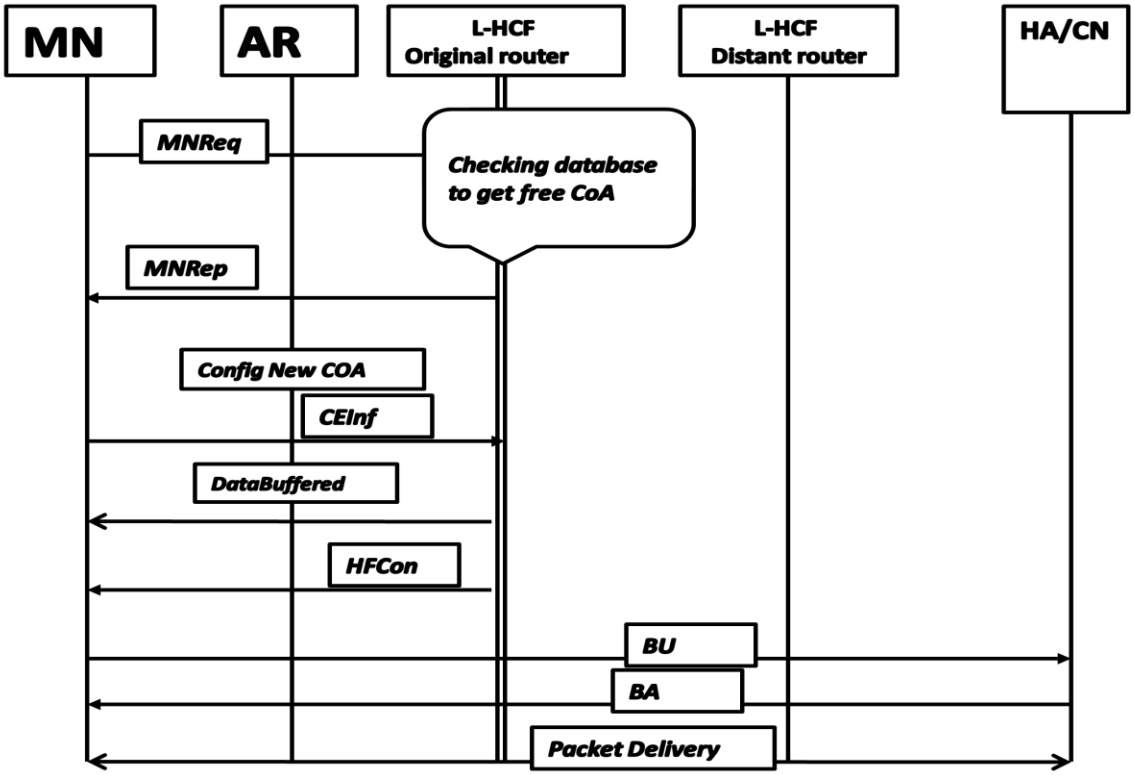

Figure 4.2 **entire handover procedure**

3. Evaluation:

The L-HCF performance estimation has been evaluated in terms of the total handover latency and of the packet loss with an analytical model in figure 4.3 using Opnet simulation. This model compare L-HCF handover with the standard handover of the MIPv6 protocol.

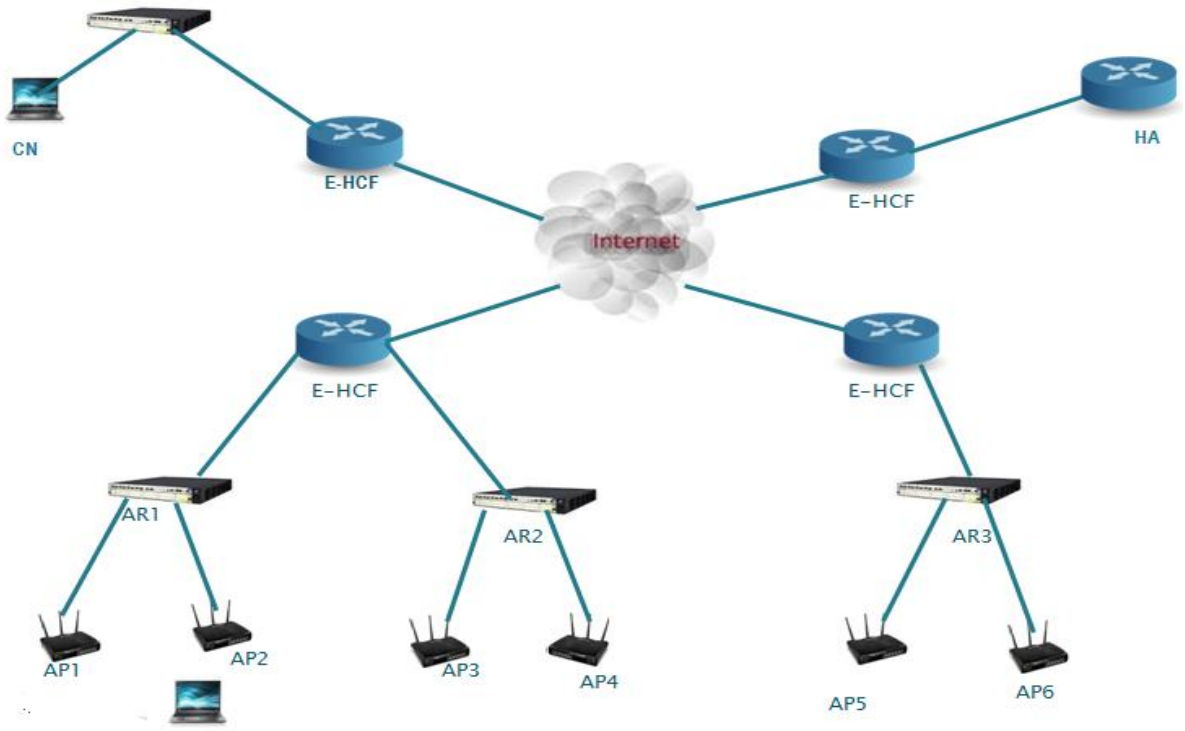

Figure 4.3 Network Model

L-HCF Latency Analysis According to the handover procedure on Figure 4.2.
The overall L-HCF handover latency LEHCF can be summed as following:
LEHCF =Lscan + LMNReq + Ldec + LMNRep +LCNinf + Lconf + LBU=BA(1)
A comparison between the standard handover latency and the EHCF latency according to equation (1), The average of the L-HCF handover latency is about 200 ms, this value of 200 ms will validated by our simulation results on OPNET.
Although the latency will reduction from 1290 ms to 200 ms is significant, the value of 200 ms is still too long to support a real time application in wireless networks. This is due to the number of channel scans.
In terms of packet loss with the L-HCF approach, packets can be stored into a buffer during the handover this can reduce packets that can be lossed.

4. Simulation

In this section L-HCF method that aims to improve the performance of handover using OPNET simulation to simulate handover procedures in Wi-Fi networks.

OPNET is a tool for modeling and simulation of networks is developed and marketed by OPNET Technologies Inc. It is now a standard reference in the field of network simulation.

There are other simulation tools similar networks, such as NS-2 OMNET + +. We chose OPNET as the simulation tool networks because that OPNET which is developed in C + + uses a graphical environment and runs under UNIX and Windows. These features allow us to design, study, modify and simulate networks and communication protocols with flexibility. In addition, OPNET also allows us to simulate many kinds of hardware, such as routers, switches that are manufactured by Cisco, Nortel or Lucent.... Thanks to this, existing networks wholes become easy to be modeled and simulated.

4.1. Characteristics of applications:

We use applications that generate a stream of constant flow to observe the interruption of receiving the data stream of MN and packet loss due to handover in wireless network applications that we have chosen are classified according to their mode of transport:

1. The reliable mode with TCP (Transmission Control Protocol).
2. An unreliable mode with UDP (user Datagram Protocol).

TCP and UDP are the two main protocols of the transport layer. The transport layer is between the session layer and the network layer of the OSI model. The primary role of the transport layer is to take messages from the session layer of the segment if necessary into smaller units and pass them to the network layer, while ensuring that the pieces arrive correctly the other side. Therefore, this layer also performs the reassembly of message reception pieces.

- ✓ TCP protocol is a connection-oriented and reliable mode. It controls the flow of data through sliding windows and uses sequence numbers and acknowledgments to ensure proper routing segments. It transmits all non-received segments. This protocol has the advantage of ensuring the transmission of data.
- ✓ UDP protocol is an unreliable connectionless mode. Although the charge of transmission of messages, it does not perform any verification software routing segments at this layer. The advantage of this protocol is its speed. As it does not provide acknowledgments, the network traffic is lower, resulting in faster transfers.

4.2. Applications using TCP:

Applications that require reliable transfer of data streams generally use the TCP protocol, in the case of Email, instant messaging, SSH (Secure Shell), the Web application, FTP (File Transfer Protocol), etc...

FTP:

The FTP protocol is a communication protocol dedicated to the exchange of computer files over a TCP / IP network. It allows for a computer to copy files to or from another computer on the network, manage a website, or delete or modify files on this computer. It uses the client-server mode, that is to say, a computer that acts as the client sends commands, and the other plays the role of the server is waiting for requests to perform actions. During an FTP connection, the TCP protocol is used to create two virtual connections: one is used to transfer commands, and the other is used to transfer data.

We define a model of FTP. The MN sends the command with an interval of one second to download the file server. The file size is constant, it is 50,000 bytes. With this model, we can receive a flow of a constant rate of 50 Kbytes/s at the transport layer in the TCP packet format with a frequency of 9 TCP packets /s and a flow of a constant rate of 435 Kbits/s to the MAC layer of MN See Figure 4.4.

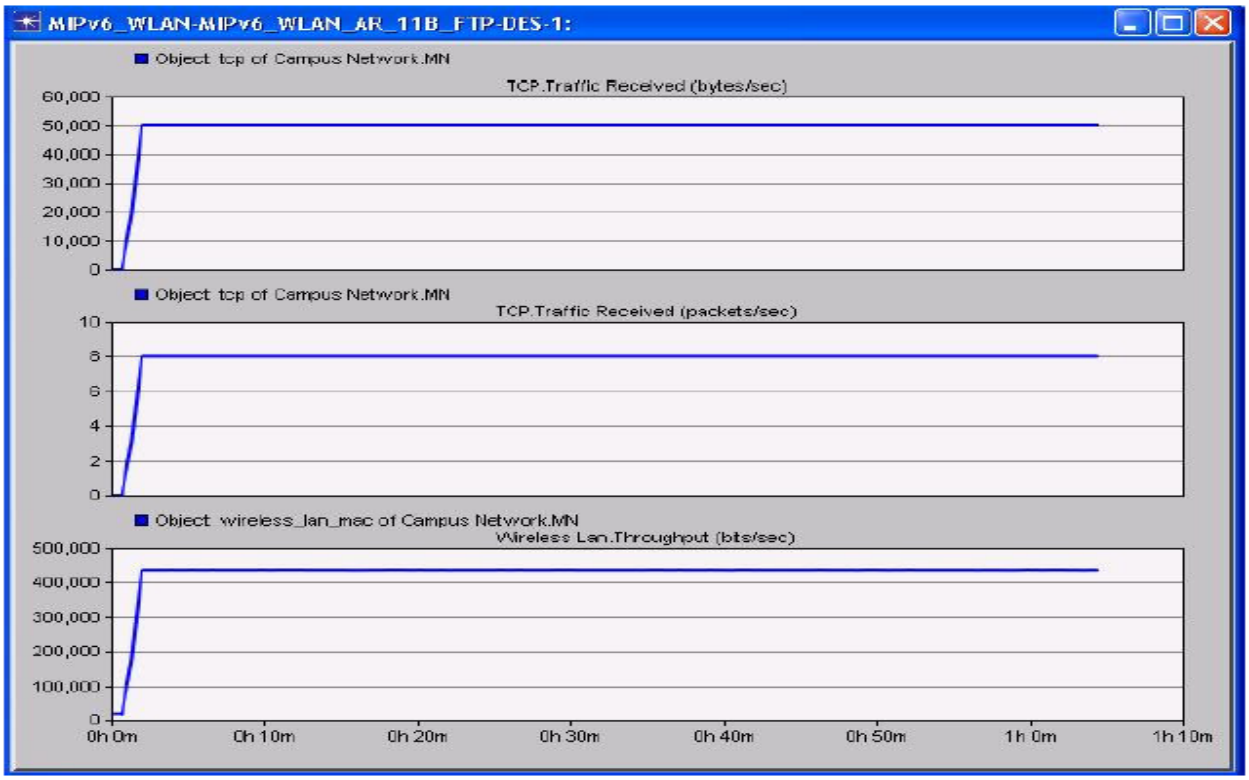

Figure 4.4 TCP Data sent

4.3. Applications using UDP

With UDP, applications can simply encapsulate IP datagrams and send without connecting. So UDP is suitable for real-time applications such as VoIP, video conferencing, etc ...

In fact, multimedia applications consist of multiple streams: audio, video, text and possibly other streams. To transport the media stream over IP networks, it is necessary to use not only the UDP protocol, but also RTP (Real- Time Transport Protocol - Protocol for Real-Time Transmission). RTP is a transport protocol implemented in the application layer. As UDP, RTP receives no flow control or error control or acknowledgment, or retransmission request mechanism, but it can multiplex multiple data streams in real time by a UDP packet stream which is then sent via the UDP protocol.

VoIP:

VoIP uses the IP network to provide telephone voice communications. The sounds are first scanned and then they are transmitted in IP networks as packets and are converted into sound at the destination. The audio codes are used to convert sounds as digital data. The different types of audio codes are selected by the user according to the voice quality, throughput and delay. The voice quality is very often denoted by Score (MOS Mean Option Score – MOS).

For a flow of a constant rate, we have chosen not to use the compression technique of silence in our simulation. We use the G.711 codec to generate a flow of a constant rate of 10 Kbytes / s at the transport layer in the format of the UDP packet with a frequency of 100 UDP packets /s and a constant flow rate of 128 Kbits/s average MAC layer MN See Figure 4.5.

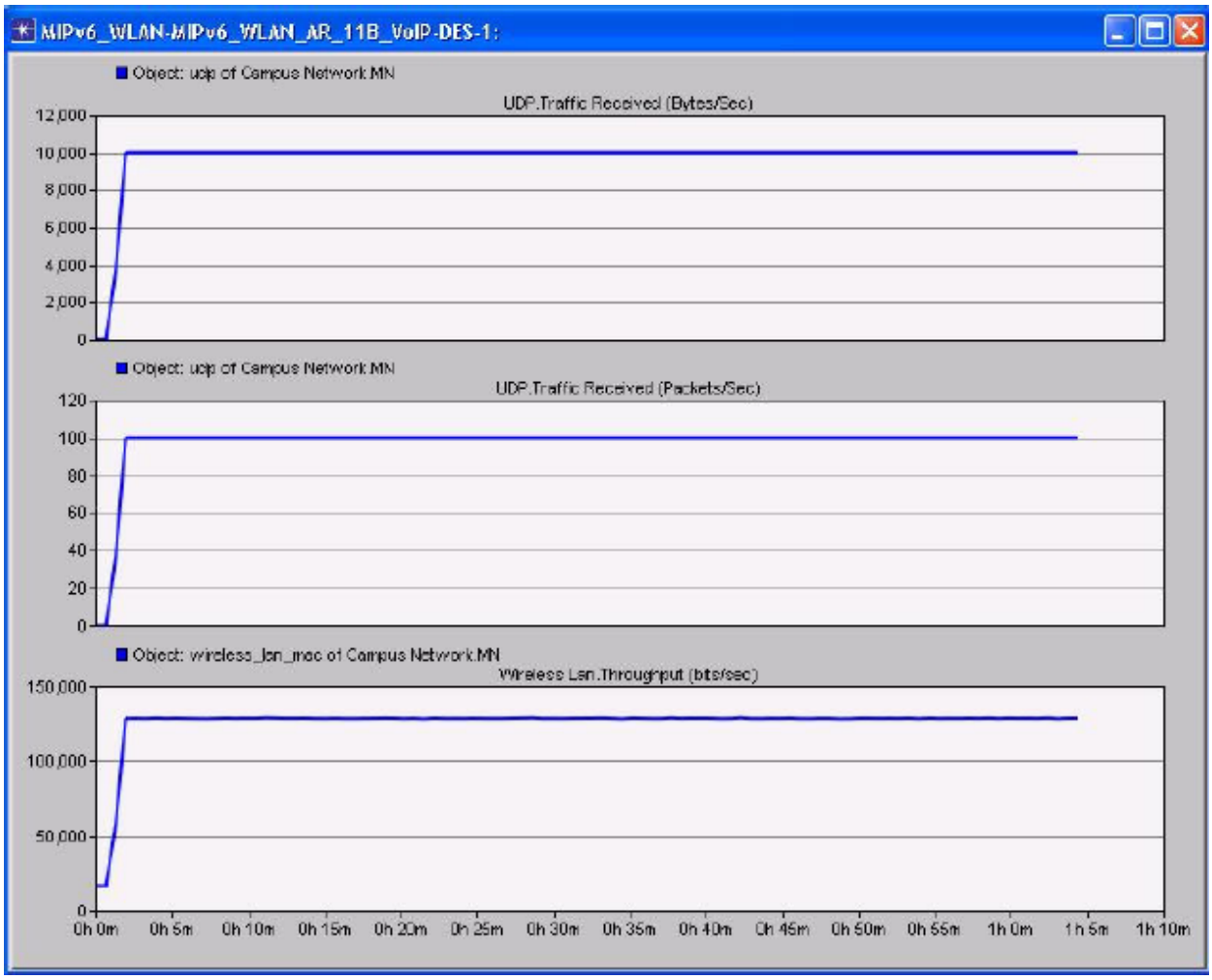

Figure 4.5 UDP Data sent

Chapter (5)
Result and Discussion

1. Results and Performance Analysis of L-HCF by simulations:

We simulate the handover procedures using a scenario with two different types of applications – FTP and VoIP. The scenario is given in Figure 5.1.

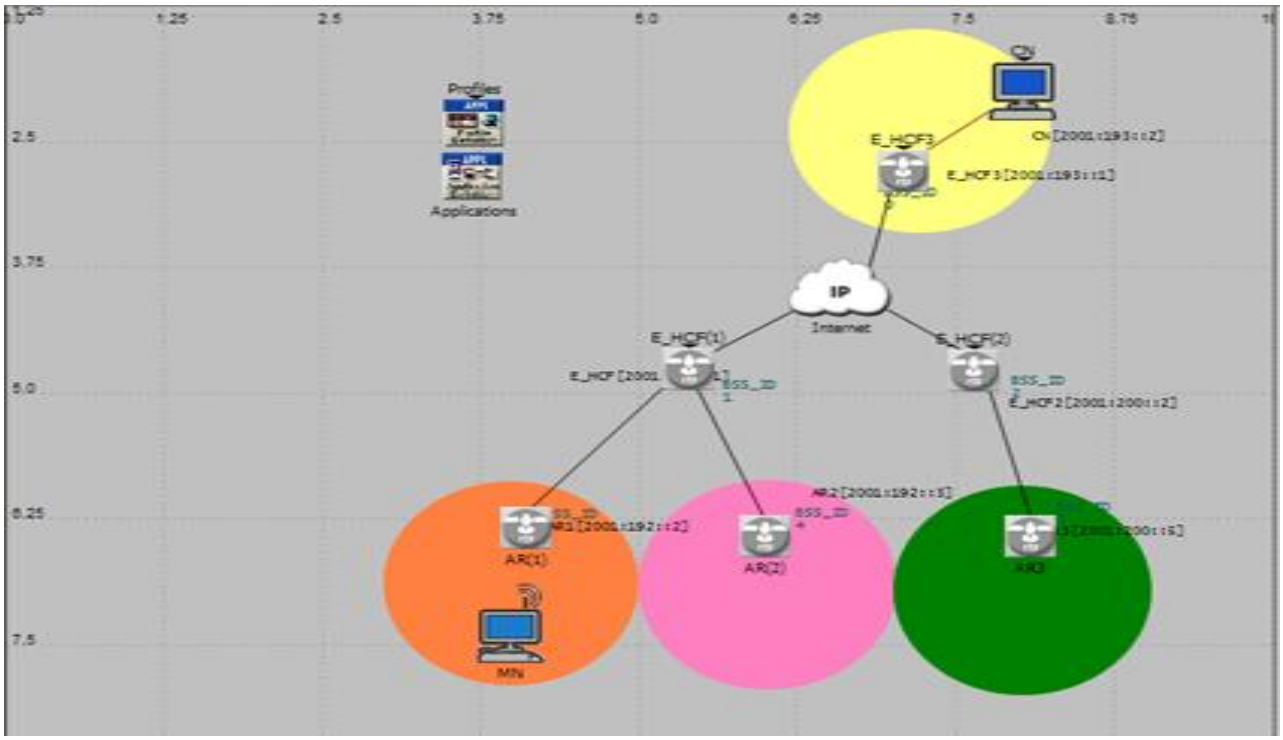

Figure 5.1 Simulation Network

MN moves through access routers. The distance between two access routers is 500 meters. When the MN changes the AR, this implies a change in the network. In our simulation, the speed of movement of the MN is 3 km / hour. This is an average speed of walking. We may also increase the speed of movement; it does not produce an effect on the duration of the handover. MN starts to launch an application between (100, 110) seconds, it first connects to it's HA and remains in its home network without stirring for 5 minutes. Then, it moves at a speed of 3 km/h and passes through 3 ARs, it loses connection with the AR after a 6 hour ride. we observe handovers that occurred during the simulation, the first handover is one of the home networks to the visited network, and the others are visited network.

We can choose the number of values collected for each statistic during the simulation. Because that OPNET generates a value of statistical data collected from a period measurement. More the number of values, the greater the measurement period for data collection is shorter and the simulation time increases. The following figures show the results of simulations. The top graph shows the results of simulations using the L-HCF method and the bottom shows the results of simulations using the standard method. We compare and explain the results of simulations in the following paragraphs.

1.1. Results and analysis of simulations for applications using UDP:-

When the MN and CN launch an application that uses UDP, MN and CN send UDP packets hoping that the other side is able to receive, there is no guarantee that UDP packets are delivered to the destination. If the network connection is interrupted, the packets are lost.
We present the results of simulations using the VoIP application in the following paragraphs.

Figure 5.2 shows Comparison between Standard and L-HCF method for the application reception (number of packets received per second) packet to the MN during simulation. The Figure shows a comparison between the standard method and the L-HCF method for packets received by the MN 600 and 610 seconds. The procedure of handover occurred at 605.8 seconds. We can see in this figure a power reception of the data stream in the standard method and a low flow received by the MN in the method L-HCF. In fact, the VoIP application sends 10 packets for 100 ms, OPNET measure for a period of 100 ms and generates a statistic value during the simulation. Since the duration of handover procedures managed by the L-HCF method is only about 140 ms, that is to say that the handover is often begins and ends in the middle of a measurement period, therefore we can see a drop in flow received, but we do not see a break in the receipt of data flow in the L-HCF method.

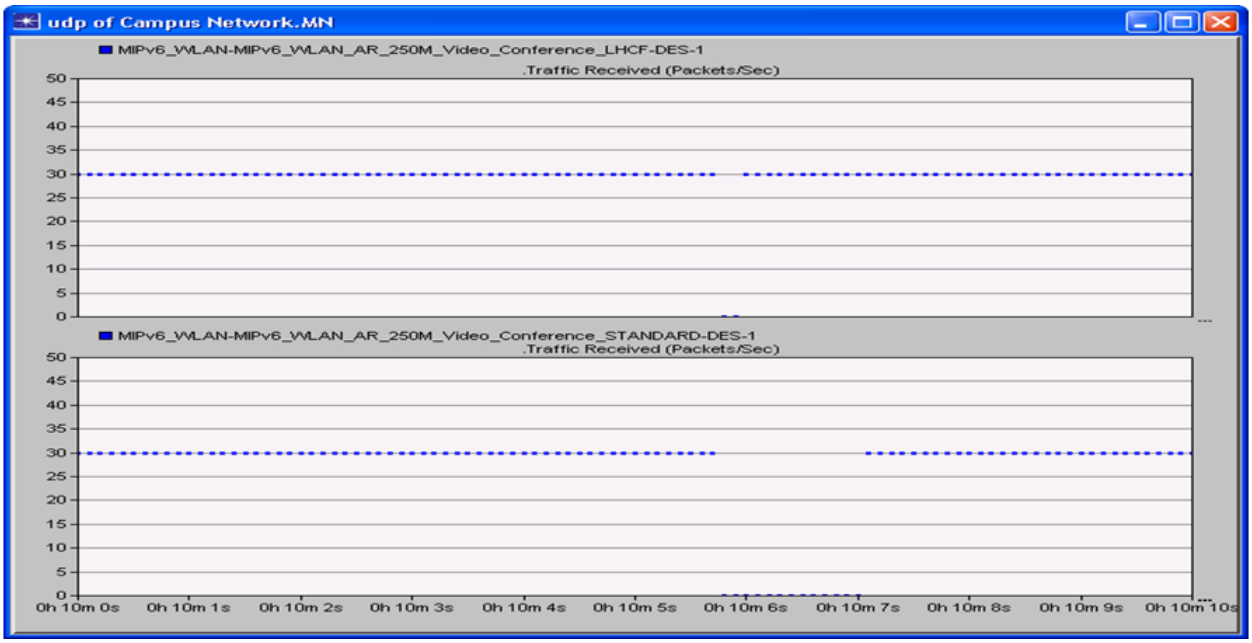

Figure 5.2 Comparison of Standard Method and L-HCF for receipt of UDP packets

1.2. Results and analysis of simulations for applications using TCP:-

TCP stream managed by the principle of "sliding window". So after sending the packet, a MN expects an acknowledgment CN before sending the next packet. This flow causes the management number of received packets with respect to the variable UDP applications.

We present the simulation results for the FTP application in Figures 5.3.

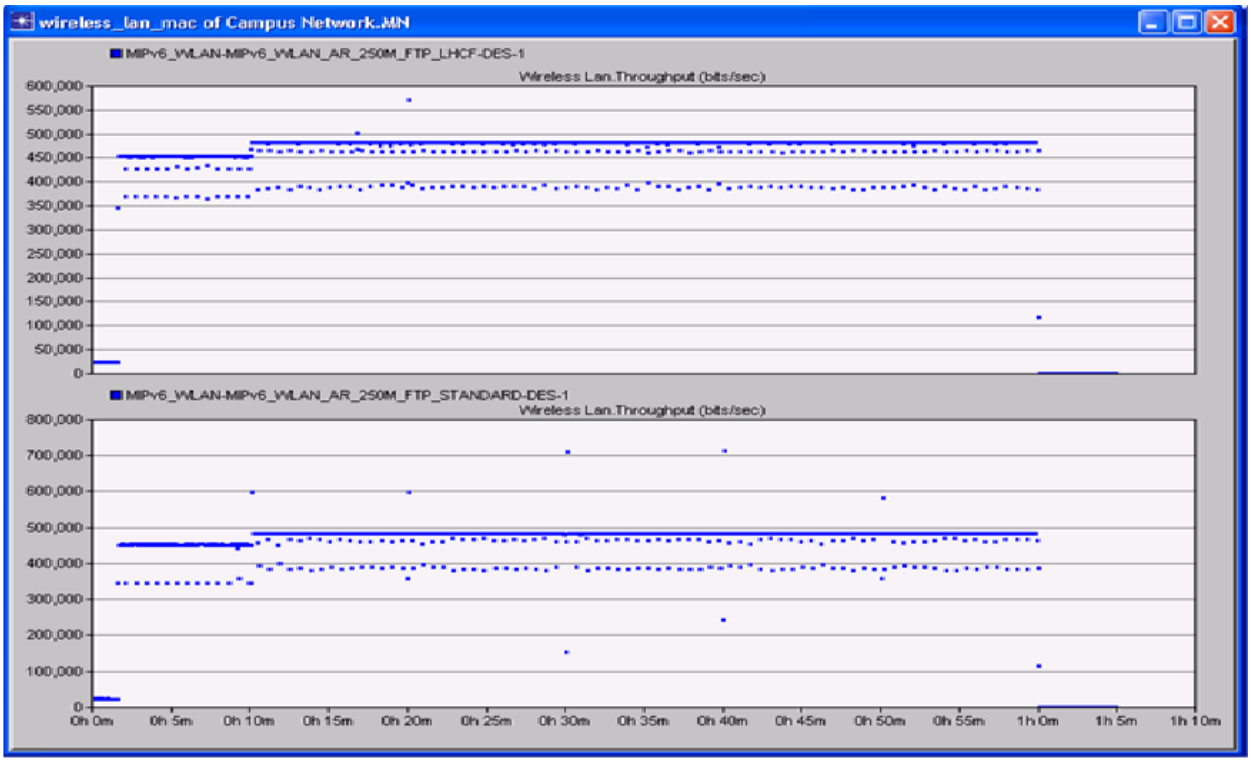

Figure 5.3 Comparison between Standard Method and L-HCF for receipt of TCP packets

2. Numerical Result:-

The table below contains the parameter used in the simulation network

Table 5.1 Network model Parameters

Parameter	Value	Comment
Channel scan time	50 ms	MIPv6 standard
BU/BA latency	140 ms	MIPv6 standard
Wireless link bandwidth	5.5 Mb/s	IEEE 802.11b
Wireless link bandwidth	9 kb/s	GSM
AR computation capacity	20 Mb/s	general router
MN computation capacity	10 Mb/s	PC computation capacity
MNReq message size	72 byte	E-HCF approach
MNRep message size	45 byte	E-HCF approach
HCFReq message size	45 byte	E-HCF approach
HCFReq message size	45 byte	E-HCF approach
CEInf message size	45 byte	E-HCF approach
HFCon message size	24 byte	E-HCF approach

To generate MNReq message by MN:
MN computation capacity= 10Mb/s
10×10^{6}bit ⟷ 1s
72× 8 bit ⟷ X s
X=0.0576ms
For Access Router:
AR computation capacity= 20Mb/s
Y= 0.0288ms
To put on Wi-fi Network:
Wireless link bandwidth =5.5 Mb
Z=0.1047ms
Latency=o.1914ms
LMNReq=0.1914ms
As a method above we can calculate times that AR, network and L-HCF routers need to process each message. Table 2 explain time for each message.

Table 5.2. messages latency in wi-fi network

Messages	Latency (ms)
MNReq	0.1914
MNRep	0.119
HCFReq	0.083
HCFRep	0.083
CEInf	0.119
HCFon	0.0638
Total Latency for messages	0.6588
Total Latency for handover process	190.7312

Total latency for handover process according to the equation 1.
LEHCF =Lscan + LMNReq + LHCFReq + LHCFReq+ LMNRep + LCNinf +Lconf + L(BU+BA) ⟶ Equation 1.

When we use Wi-fi network the total latency =190.7312 ms
When we use UMTS network the total latency =191.4352 ms
When we use GSM network the total latency =435.6645 ms

By comparing the latency in Wi-Fi network, UMTS network and GSM network using mat lab simulation code we get this result showing in figure bellow

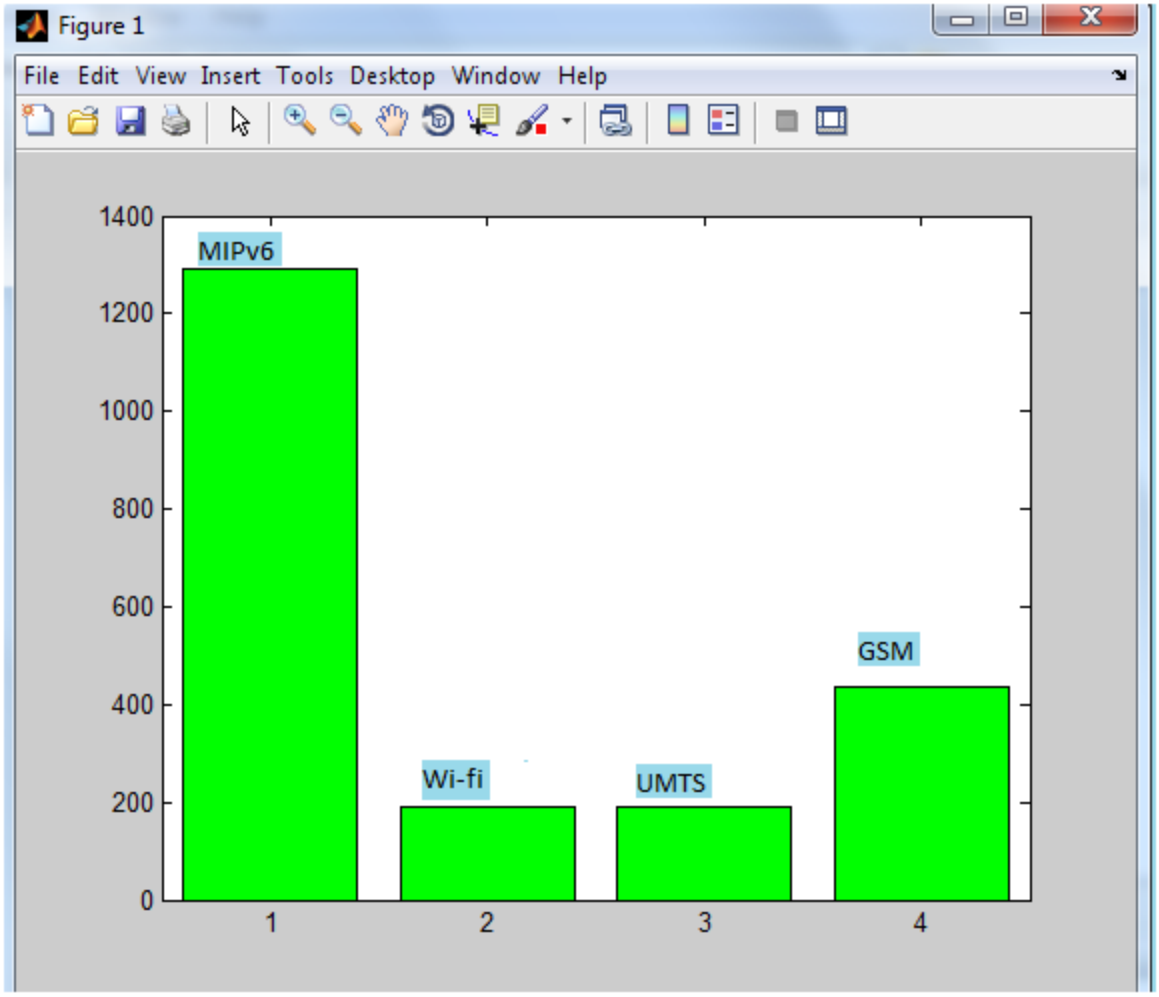

Figure 5.4 Compression Between network's handover delay

On Figure 5.4, the standard MIPv6 handover latency (1290 ms) is the first figure displayed on the left. The rest of the figures are the L-HCF handover latencies based on WiFi, UMTS and GSM link bandwidths. We note that the various L-HCF latencies are not really different when link bit rates vary from 150 kb/s to 5.5 Mb/s. If the link bit rate drops to 9 kb/s (GSM), the L-HCF handover latency raises up to 435ms. As a result, the wireless link bandwidth has an important influence over the overall handover procedure. Let us focus on the L-HCF latency with the IEEE 802.11b wireless networks.

Chapter (6)
Conclusion and Recommended Work

6.1. Conclusion

In order to improve the handover performance for the Mobile IPv6, this project proposes an *L-HCF* approach which allows collecting and storing some link and networking data. The main problems of the handover of level 2 and level 3 handover from the fact that the time of handover procedures is too important for many applications , especially for real-time applications. The delay causes both communication interruptions and loss of packets visible to users. Regarding the classical Mobile IPv6 handover performance, our numerical results validated by simulations show that the *L-HCF* approach enables to decrease the total handover latency significantly. As we have described, our method reduces the handover delay of 272 ms. To reduce packet loss due to handover procedures, we propose to amend the Mobile IPv6 protocol. The Mobile Node terminates the association between its home address and its care-of address with the home agent and Matching Nodes before the handover procedure. Therefore, we can use the home agent to intercept and redirect packets Matching Nodes or Mobile Node to the new address of the Mobile Node or to the addresses of nodes Correspondents respectively during phase Updating association. With this method, we can reduce packet loss and ensure an acceptable timeframe.

Also, we find that the interruption of the reception stream is much smaller in the L-HCF method than the Standard method. We get a visible result for applications that use TCP and UDP.

6.2. Recommended work

For future work we recommend to improve the handover performance in link layer and network layer by decrease router discovery time and mechanism to decrease Binding Update and binding Acknowledgement times.

Appendix 1

List of Figure:-

Appendix 2
Matlab Code:

```
clc
clear,close all
stan=1290;
gsm=9*10^3; %Wireless link bandwidth(for gsm)
umts=2*10^6; %Wireless link bandwidth(for umts)
wifi=5.5*10^6; %Wireless link bandwidth(for WIFI)
AR=20*10^6;%10mb/s AR computation capacity
MN=10*10^6;%MN computation capacity
MN_RQ=72; %MNReq message size
MN_RP=45; %MNRep message size
HCF_RQ=45; % HCFReq message size
HCF_RP=45; %HCFReq message size
CEInf=45; %CEInf message size
HFCon=24; %HFCon message size
MN_RQb=MN_RQ*8;
MN_RPb=MN_RP*8;
HCF_RQb=HCF_RQ*8;
HCF_RPb=HCF_RP*8;
CEInfb=CEInf*8;
HFConb=HFCon*8;
%Wifi network calculation
Lmn_q=((MN_RQb/MN)+(MN_RQb/AR)+(MN_RQb/wifi))*1000;
disp(Lmn_q);
Lmn_p=((MN_RPb/MN)+(MN_RPb/AR)+(MN_RPb/wifi))*1000;
disp(Lmn_p);
LHCF_RQ=((HCF_RQb/MN)+(HCF_RQb/AR)+(HCF_RQb/wifi))*1000;
disp(LHCF_RQ);
LHCF_RP=((HCF_RPb/MN)+(HCF_RPb/AR)+(HCF_RPb/wifi))*1000;
disp(LHCF_RP);
LCEInf=((CEInfb/MN)+(CEInfb/AR)+(CEInfb/wifi))*1000;
disp(LCEInf);
LHFCon=((HFConb/MN)+(HFConb/AR)+(HFConb/wifi))*1000;
disp(LHFCon);
latency_wifi=50+Lmn_q+Lmn_p+LHCF_RQ+LHCF_RP+LCEInf+LHFCon+70+
70;
%UMTS network calculation
Lmn_q_umts=((MN_RQb/MN)+(MN_RQb/AR)+(MN_RQb/umts))*1000;
```

```
disp(Lmn_q_umts);
Lmn_p_umts=((MN_RPb/MN)+(MN_RPb/AR)+(MN_RPb/umts))*1000;
disp(Lmn_p_umts);
LHCF_RQ_umts=((HCF_RQb/MN)+(HCF_RQb/AR)+(HCF_RQb/umts))*1000;
disp(LHCF_RQ_umts);
LHCF_RP_umts=((HCF_RPb/MN)+(HCF_RPb/AR)+(HCF_RPb/umts))*1000;
disp(LHCF_RP_umts);
LCEInf_umts=((CEInfb/MN)+(CEInfb/AR)+(CEInfb/umts))*1000;
disp(LCEInf_umts);
LHFCon_umts=((HFConb/MN)+(HFConb/AR)+(HFConb/umts))*1000;
disp(LHFCon_umts);
latency_umts=50+Lmn_q_umts+Lmn_p_umts+LHCF_RQ_umts+LHCF_RP_umt
s+LCEInf_umts+LHFCon_umts+70+70;
%GSM network calculation
Lmn_q_gsm=((MN_RQb/MN)+(MN_RQb/AR)+(MN_RQb/gsm))*1000;
disp(Lmn_q_gsm);
Lmn_p_gsm=((MN_RPb/MN)+(MN_RPb/AR)+(MN_RPb/gsm))*1000;
disp(Lmn_p_gsm);
LHCF_RQ_gsm=((HCF_RQb/MN)+(HCF_RQb/AR)+(HCF_RQb/gsm))*1000;
disp(LHCF_RQ_gsm);
LHCF_RP_gsm=((HCF_RPb/MN)+(HCF_RPb/AR)+(HCF_RPb/gsm))*1000;
disp(LHCF_RP_gsm);
LCEInf_gsm=((CEInfb/MN)+(CEInfb/AR)+(CEInfb/gsm))*1000;
disp(LCEInf_gsm);
LHFCon_gsm=((HFConb/MN)+(HFConb/AR)+(HFConb/gsm))*1000;
disp(LHFCon_gsm);
latency_gsm=50+Lmn_q_gsm + Lmn_p_gsm + LHCF_RQ_gsm +
LHCF_RP_gsm + LCEInf_gsm + LHFCon_gsm + 70+70;
disp(latency_wifi);
disp(latency_umts);
disp(latency_gsm);
x=[stan,latency,latency_umts,latency_gsm];
figure
bar(x,'group','g');
```

References:-

[1]. Salim M. Zaki1c and Shukor Abd Razak Mitigating Packet Loss in Mobile IPv6 Using Two-Tier Buffer Scheme.

[2]. Moore, N.S., Choi, J., Pentland, B. Tunnel Buffering for Mobile IPv6.

[3]. Hyon G. Kang and Chae Y. Lee Fast Handover Based on Mobile IPv6 for Wireless LAN.

[4]. Wei Kuang Lai and Jung Chia Chiu, ”Improving Handoff Performance in Wireless Overlay Networks by Switching between Two-Layer IPv6 and One-Layer IPv6 Addressing,” IEEE Journal on Selected Areas in Communications, vol. 23, No. 11, pp. 2129-2137, November 2005.

[5]. html, January 2003 ”IEEE 802.11f: Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Access Distribution Systems Supporting IEEE 802.11 Operation”, IEEE Standard 802.11, January 2003

[6]. Guozhi Wei1, Anne Wei1, Ke Xu2, and Hui Deng3 "Handover Control Function Based Handover for Mobile IPv6" Springer-Verlag Berlin Heidelberg 2006

[7]. Xavier P´erez-Costa and Marc Torrent-Moreno "A Performance Study of Hierarchical Mobile IPv6 from a System Perspective"

[8]. Matthew B. Shoemake "Wi-Fi (IEEE 802.11b) and Bluetooth Coexistence Issues and Solutions for the 2.4 GHz ISM Band" February 2001, Version 1.1

[9]. Hooshiar Zolfagharnasab "REDUCING PACKET OVERHEAD IN MOBILE IPV6" DOI 10.5121 /ijdps .2012.3301

[10]. Anne Weiy, GouZhi Weiand Benoit Geller "Improving Mobile IPv6 Handover in Wireless Network with L-HCF" This work was supported in part by the international project PRA-SIP under Grant SIP04-03.
[11]. Dr. Dimitrios Kalogeras "Introduction to Mobile IPv6"
[12]. Xavier P´erez-Costa and Marc Torrent-Moreno "A Performance Study of Hierarchical Mobile IPv6
from a System Perspective"
[13]. www.opnet.com

[14]. www.omnet.org

[15]. D.Johnson, C.Perkins, and J.Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.