CHAPTER TWO

LITERATURE REVIEW

Chapter Two

Literature Review

2.1 Introduction:

Efficient GMIPv6 scenarios need to be simulated to provide the required QOS to a wide range of applications while allowing seamless roaming among a multitude of access network technology.in this chapter, a comprehensive survey of the handover decision, mobile generations and internet protocols to satisfy these requirements is presented.

2.2 Related works:

Jayaganesh.M and Aravinth.T.S based on Control/User (C/U) plane split heterogeneous networks can provide high quality broadband wireless service for passengers in high-speed rail, with the higher system capacity, better transmission reliability and less co-channel interference. The handover problem that the novel Vehicle communication system based on C/U plane split heterogeneous networks would encounter in high speed Vehicle. The analysis shows that, because of its special networks architecture, the handover problem, particularly the Inter-Macro cell handover problem, is more serious than that in traditional Long Term Evaluation (LTE) networks only covered by Macro eNB and directly impacts its applicability and availability in high-speed Vehicle scenario with the fundamental reason that Ultimate Ears (UE) must complete Macro-Macro and Phantom-Phantom handover twice in an Inter-Macro cell handover before the train leaves away from the overlap region of

Phantoms, more shortage than the available overlapping region in LTE handover [4].

Chung-Sheng Li, Yung-Chih Tseng and Han-Chieh Chao proposed the Neighbor Graph Cache (NGC) mechanism to reduce scanning latency while a mobile station tries to make a link-layer handover. The handoff latency can be greatly reduced through NGC algorithm. We use OPNET modeler as the simulation tool. The simulation results show that the handover delay by NGC is 2.614 ms. It is less than 50 ms and able to meet the criteria of VoIP application [5].

Hajer Abbas, Rashid A. Saeed presented a novel control function that is called Lightweight Handover Control Function (L-HCF). The purpose of this control function is to improve of the handover performance in the perspective of Mobile IPv6 over wireless networks. The L-HCF functionality allows a router to choose which AR/AP address that the mobile node is associated with when movement is needed, by using available IP addresses in its database if the movement operation in side domain or by exchange messages between other routers if the movement alter domain. Thus the MNs can use this address without engaging in the process of Stateless Address Auto-configuration or the procedure of Duplicate Address Detection (DAD). The result shows that, the control function offer minimum latency, less packet loss compared with the standard function of the mobile IPv6[6].

2.3 Fifth Generation Technology (5G):

5G Technology is a name which was announced to indicate the significant upcoming step in mobile and wireless communication after the previous serial 1G, 2G, 3G, 4G, LTE advanced. However, 5G technology is not deployed yet and whereas it faces some challenges. According to many researches, there will be no standard's implementation for 5G technology before 2020 [7].

5G promises to increase the aptitude to 1,000 fold and slightest 100 billion devices connected. It provides a low latency which allows the ability of individual experience to reach a 10 GB/s. The deployed existing technologies and a new Radio Access Technology (RAT) have a big influence on 5G radio access's structure [8].

The improvement of wireless network (Breakthroughs) which will be needed in 5G technology, will affect the growth of the social and economic in varies ways. Zero distance connectivity will be provided by 5G technologies between connected devices as well as the people. The 5th generation of wireless mobile communication is wireless internet network which is supported by OFDM, MC-CDMA, LAS-CDMA, UWB, Network-LMDS and IPv6. The basic protocol for running on both 4G and 5G is IPv6. The 5G is complete wireless communication system having no limitation and is called as Real World Wireless or Worldwide Wireless Web (WWWW) [9].

The 5G technology mobile phone shall maintain virtual multi-wireless network. For this, the network layer should be divided into two sub layers. For mobile terminal, the upper network layer and for interface, the lower network layer. This is an initial design for internet, where all the routing will be based on IP addresses which should be different in each IP network worldwide [10].

In wireless radio interface the higher bit rate is a big loss; in 5G this loss is controlled by using open transport protocol (OTP). The transport layer and session layer in 5G network support this protocol. The application layer is for quality of service management over different type of networks. The important features of 5G technology includes bidirectional larger bandwidth, less traffic, equally availability of network across the world, 25Mbps connectivity speed, data bandwidth higher than 1Giga bit and low-cost [11].

2.4 IPv6 and IPv4:

Internet Protocol version 6 (IPv6) is the next generation of Internet Protocol (IP) which was released by 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 [12].

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 IP security (IPsec) is mandatory to the protocol [13].

Types of IPv6 addresses:

- Unique local Address (ULA):

Is an IPv6 address in the block fc00::/7 . It is the approximate IPv6 counterpart of the IPv4 private address. Unique local addresses are available for use in private networks, e.g. inside a single site or organization or spanning a limited number of sites or organizations. They are not routable in the GMIPv6 Internet [14].

- Link-local Address:

Is an IPv6 unicast address that can be automatically configured on any interface using the link-local prefix FE80::/10 (1111 1110 10) and the interface identifier in the modified EUI-64 format. Link-local addresses are not necessarily bound to the MAC address (configured in a EUI-64 format). Link-local addresses can also be manually configured in the FE80::/10 format using the IPv6 address link-local command [15].

- Global Unicast Address:

A global unicast address is simply what we call a public IP address in IPv4 that is, an IP address that is routed across the whole Internet. You can make out a global unicast address easily: The first three bits are set to 001. Thus, the address prefix of a GMIPv6 address is 2000::/3 because 0010000000000000 is 2000 in hex.

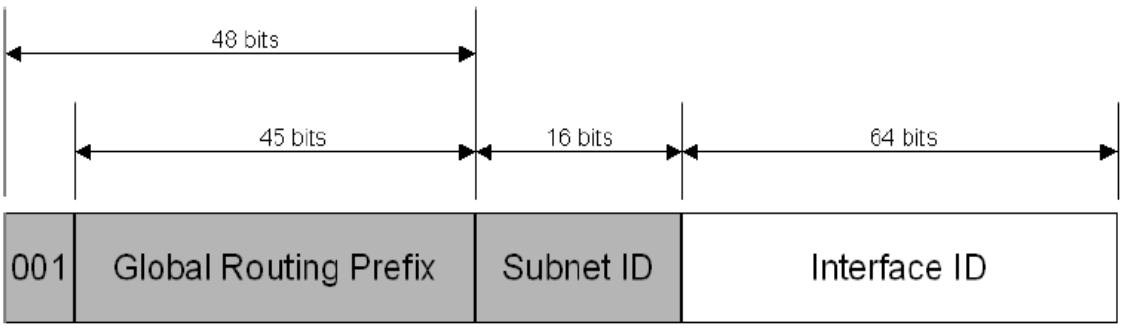

Figure (2.1): Global MIPv6 address

The next 45 bits are the so-called global routing prefix. This is the part that is assigned to organizations. The following 16 bits are for the subnet ID, which you can use for hierarchical addressing in your network. The last 64 bits indicate the interface ID, which is the part of the IPv6 address that must be unique within a subnet [16].

2.5 Mobile IPv6:-

The 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 Mobile IPv4 (MIPv4), 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 (FA) is exclude 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. MIPv6 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 (NUD) which belongs to the IPv6 standard assures the reach-ability from the mobile node to its default router and vice versa.

6. In MIPv6, when a MN 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 (ND) instead of Address Resolution Protocol (ARP) which improves the robustness of the protocol.

8. MIPv6 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 Internet Control Message Protocol (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 [17].

2.6 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. 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 [18].

Types of Handovers:

- 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 [19].

- 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 [20].

- 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 (2.2) depicts a MN moving from the access range of AP1 to AP2. As the figure demonstrated, both AP1 and AP2 are connected with the same AR. This means there is no topological change from the perspective of the MN.Therefore, it is a horizontal handover.

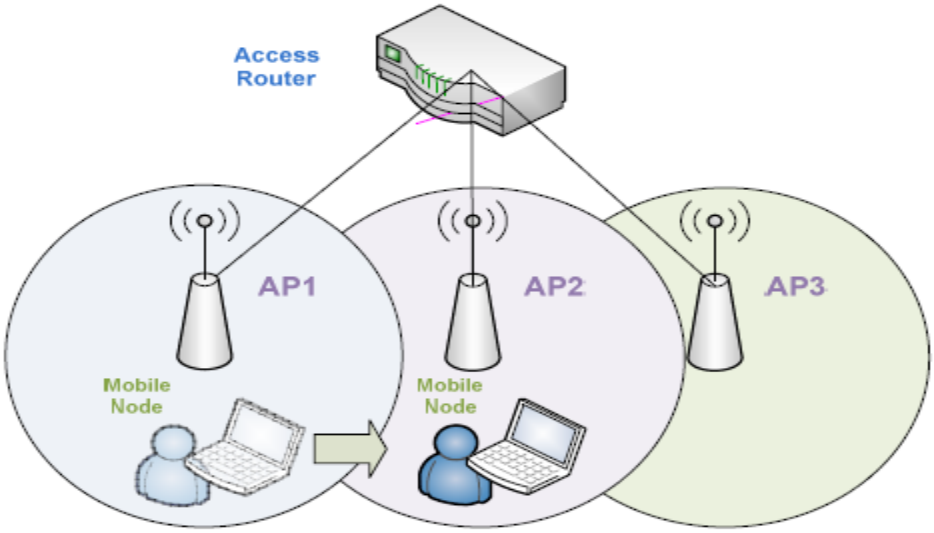

Figure (2.2): Horizontal Handover

Figure (2.3) demonstrates a scenario of a vertical handover. In this figure, the MN moves from the access range of AP3 to AP4. As the figure shown, AP3 and AP4 are connected with different AR. Since the AR of

the MN has changed, the access network topology is also changed. Therefore, it is a vertical handover [21].

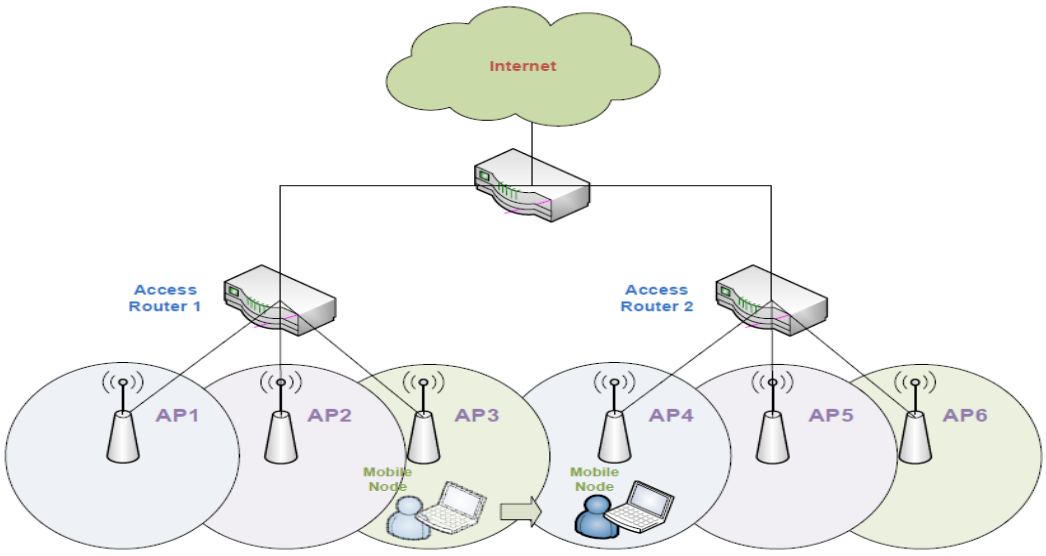

Figure (2.3): Vertical Handover 1

Vertical handover does not only happen within the network of one Internet Service Provider (ISP), it can also happen between ISPs. Figure (2.4) demonstrates such a vertical handover that happens between ISPs. In the figure, the MN moves from AP3 to AP4 where AP3 and AP4 are connected with different ARs which belong to different ISPs [22].

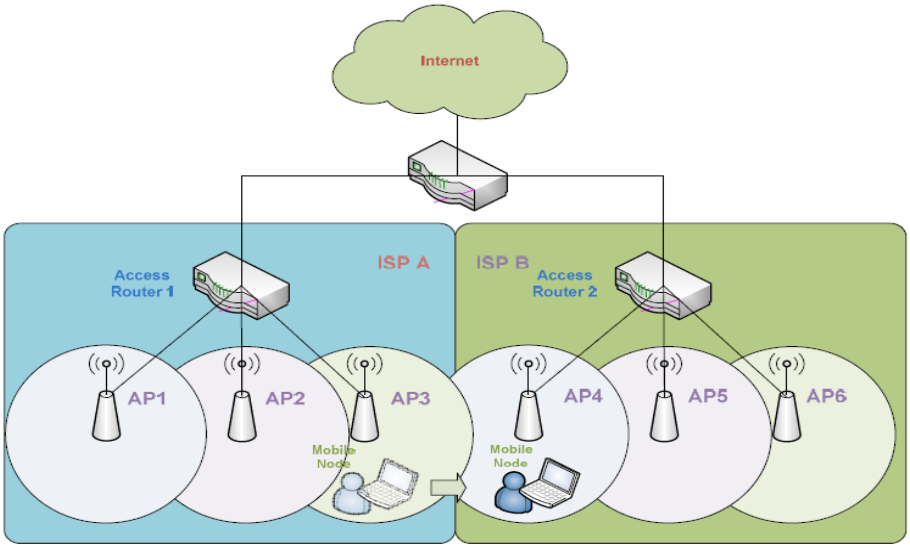

Figure (2.4): Vertical Handover 2

- 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 AP, 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 [23]. A handover in MIPv6 is a layer 3 handover which is the main focus of this project.

2.7 Handover in MIPv6:

The MIPv6 handover process has many terminologies 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 [24].

Figure (2.5) provides a graphical demonstration to all the terms mentioned above. In Figure (2.5), the MN is labeled with light green color. 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 to a FN, and range of these two networks are indicated by different color of circles. Inside of each circle, there are one AR and two APs. In the HN, the AR is

the HA of the MN. In the FN, the AR is referred as FAR. Below the MN's icon, it is the current IPv6 address of the MN.

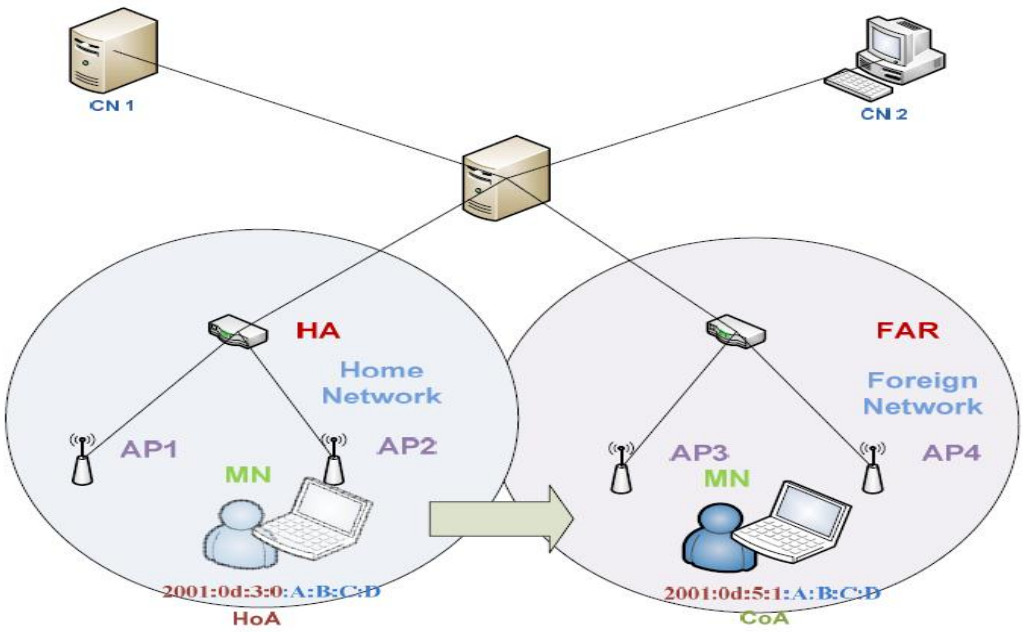

Figure (2.5): Graphical Explanations of the MIPv6 Terminology

When the MN is at the HN, the MN uses its HoA. When the MN is at FAR, the MN uses its CoA. 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 of the MN. In this context, the CNs are the computers or servers which are currently communicating with the MN [25].

2.7.1 The Processes of MIPv6 handover:-

A MIPv6 handover can be divided into five different processes: Movement Detection (MD), Candidate Access Router Selection (CARS), Address Configuration (AC), Authentication & Authorization (A&A),

and Binding Update (BU) which are demonstrated in Figure (2.6). Each of these sub-processes is described in detail in the following sections.

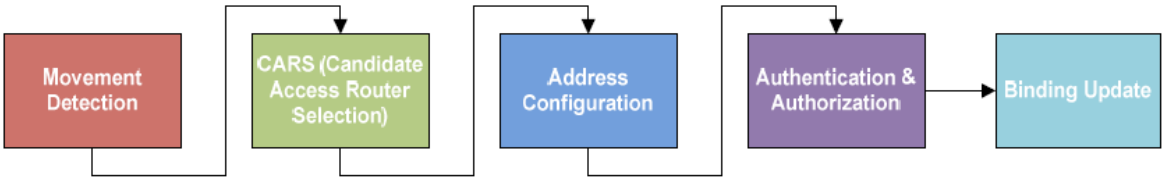

Figure (2.6): Basic Procedures of a MIPv6 Handover

2.7.1.1 Movement Detection:

MD is a process that recognizes when a 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 (2.6) 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 Neighbor Discovery (ND) which includes the Router Discovery (RD) and the 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 Minimum RA interval and Maximum RA interval in the router. If an MN has been waiting for a RA message from the current AR more than Maximum RA interval 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, 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 Neighbor 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 behavior of the NUD are specified by RFC 2461 [33], and depicted in Figure (2.7). According to Request For Comment (RFC 2461), every IPv6 node can have five statuses: “Reachable”, “Stale”, “Delay”, “Probe” and “Unreachable”.

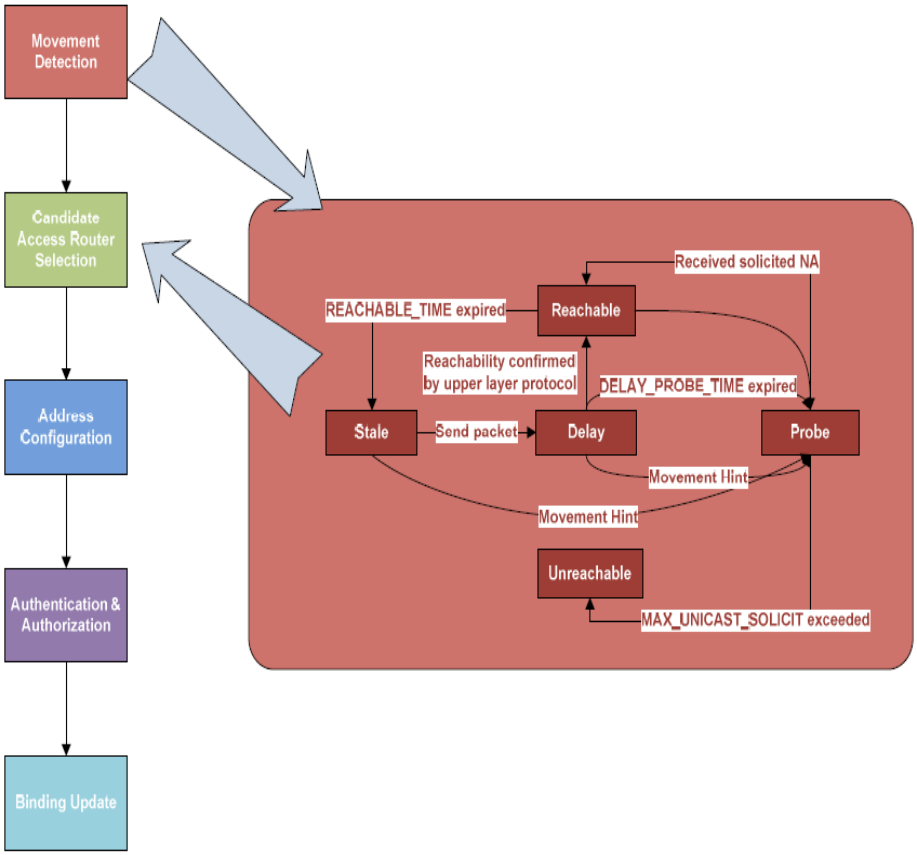

Figure (2.7): State transitions during the execution of the Neighbor Unreachability Detection Procedure

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 neighbor, the state of the neighbor will be recorded as "Reachable". After a fix time interval which is known as "REACHABLE_TIME", the state of the neighbor 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 neighbor for another time interval called "DELAY_FIRST_PROBE". If the MN does not receive replies from the neighbor within the time limit, the state of the neighbor 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 Neighbor Solicitation (NS) messages. If the MN still does not receive any reply from the neighbor, the state of the neighbor 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 Maximum RA interval, MAX_UNICAST_SOLICIT and RETRANS_ TIMER [15].

2.7.1.2 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.

- Candidate Access Router Discovery(CARD):

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.

- 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 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.

2.7.1.3 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 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 Dynamic Host Configuration Protocol version 6 (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 .

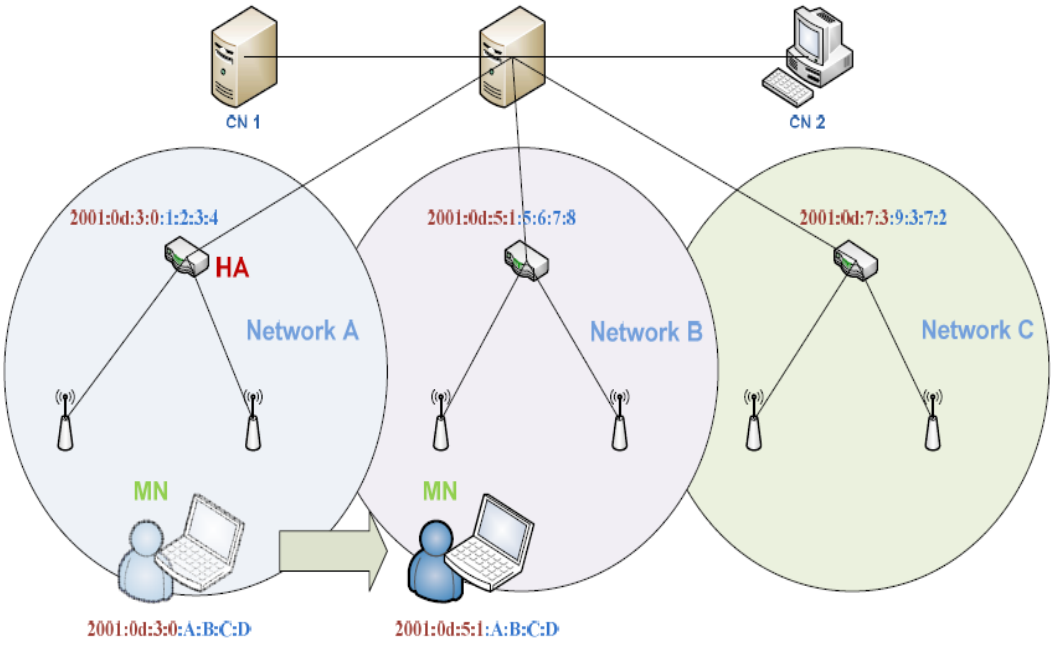

Figure (2.8): Example of an Address Configuration Process

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 (2.8). 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 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 (DA) 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 (2.9) 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.

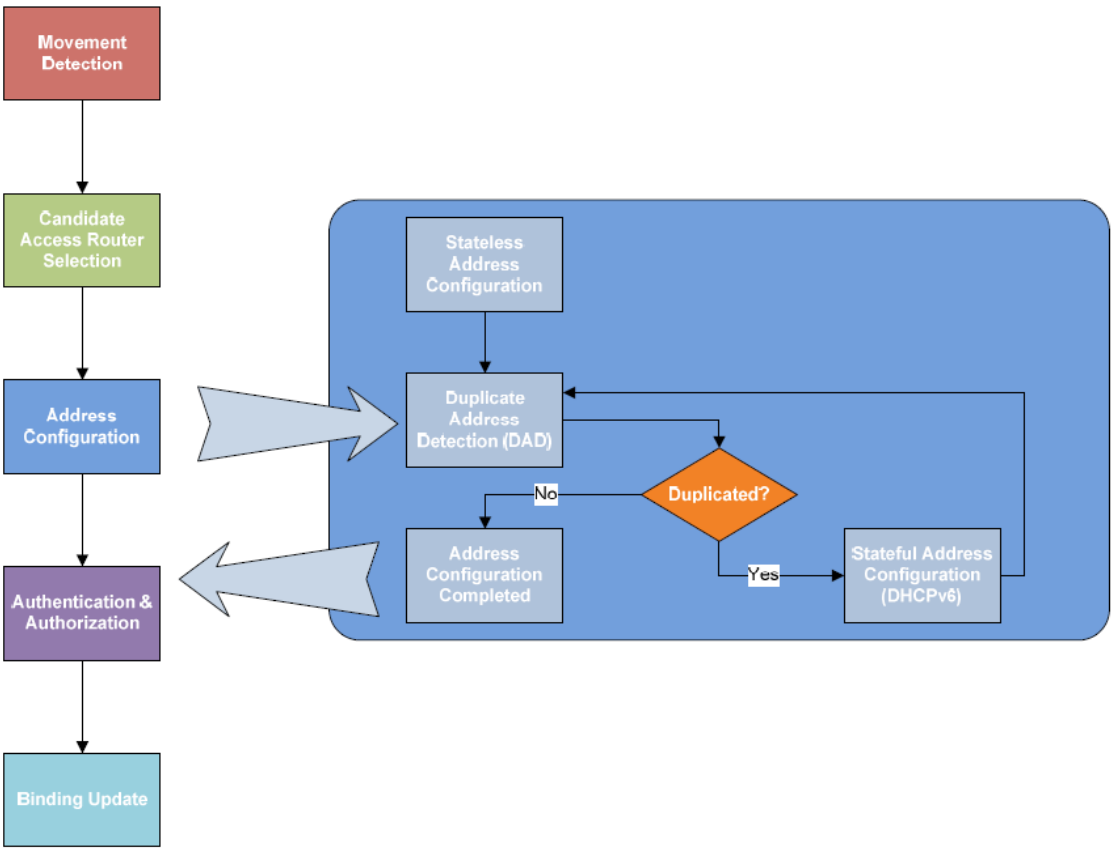

Figure (2.9): Sub-processes of the Address Configuration

2.7.1.4 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.

2.7.1.5 Binding Update:

Bind Update (BU) is the last stage in a handover process. The purpose of the BU is to keep tracking 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.

- 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.

- 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.

- 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 [26].