Factors Affecting the Handover Latency in MIPv6

Arun Kumar Tripathi
Krishna Institute of Engineering and Technology
Ghaziabad-U.P., India

R. Radhakrishnan
ABES Engineering College,
Ghaziabad-U.P., India

J.S. Lather
National Institute of Technology, Kurukshetra-Haryana, Indla

ABSTRACT

Mobility management for the next generation IPv6 networks is one of the recent research issues due to the growing demand for wireless services over internet. Mobile Internet Protocol version 6 (MIPv6) has been proposed to solve the problem of mobility in the next generation era of Internet. MIPv6 allows packets from source to destination and vice versa while mobile node has moved away from its home network. Handover latency is the primary cause of packet loss resulting in performance degradation of Mobile IPv6. This paper surveys various mobility management protocols, basic handover mechanisms for MIPv6 and delay components affecting the handover latency are identified and mathematically calculate the delay among these components.

Keywords: Handover Latency, MIPv6, DAD, Route Optimization.

1. INTRODUCTION

The remarkable advancements in the field of communication and information technology over the last decades have influenced our lives greatly. IP-based next-generation wireless networks are widely adopted for transporting media such as audio, voice, text, images etc. Initially mobility management based on IPv4 was proposed in 1993. At that time, there were no real "mobile" computers. There were very less computers in number called laptops, but they were still relatively large and very expensive as compared to desktop computers. Mobile phones were in use, but they were large and had poor computing resources. In Mobile IP, an MN is addressed by two addresses; a home address (HoA) [1] and a care-of address (CoA) [1]. The MN is identified by its fixed HoA within the home network. When it leaves its home network and attached to a new network, known as visited network, then it is take care by a temporary address known as CoA. This dual address mechanism allows continuous delivery of data packets to MN without knowing the point of attachment to the Internet. This mechanism provides transparency to transport and higher-layer protocols.

In November 1996, Internet Engineering Task Force (IETF) has proposed Mobile IPv6 (MIPv6) as the main protocol for mobility management at the IP layer. The IP based protocol, Mobile Internet Protocol version 6 (MIPv6) [1] has been proposed to solve the problem associated with mobility management in IPv6 network. This allows users to seamlessly movement from one location to another and stay connected to the Internet. As mobility increases across networks, handover process significantly impacts the quality of the connection and user application.

During the handover management Mobile node (MN) gets disconnected to old communication link and connected to new one. The decision for a new association may be initiated due to movement, if we are moving away from the old connection point and approaching a new one or due to low signal quality at the interference. The basic objective of handover management is to maintain the continuity and quality of service of communication.

Rest of the paper is organized as follows. Section II deals with introduction of mobility management protocol. Section III describes handover management and its type in MIPv6. Various factors affecting the handover latencies during the handover process are discussed in section IV. Conclusion is made in Section V.

2. MOBILE IPV6 PROTOCOL

In 2004, IETF standardized mobility management protocol known as host-based mobility protocol. In host-based mobility management protocol all the efforts such as detection of new network, request a Care-of Address (CoA), association with new CoA, send information about the CoA to the Home Agent (HA), etc. for handover over management are made by the Mobile Node (MN). This reflects high involvement of MN in the handover process and as a result handover latency is high. MIPv6 is an IP-layer mobility management protocol for the IPv6 Internet. It is designed to provide mobility services on top of the existing IP infrastructure, without requiring any modifications to the routers, the applications or the stationary hosts. MIPv6 protocol allows mobile nodes to stay connected during the roaming within IPv6 Internet. When MN moves from home network to a foreign network and wants to use services of foreign network. For this MN must be connected to foreign network. For this, MN sends a router solicitation massage and in response to that it get router advertisement message. MIPv6 provides transparent mobility to MN with the help of HoA and CoA. The MIPv6 architecture and flow of messages is shown in Figure 1.

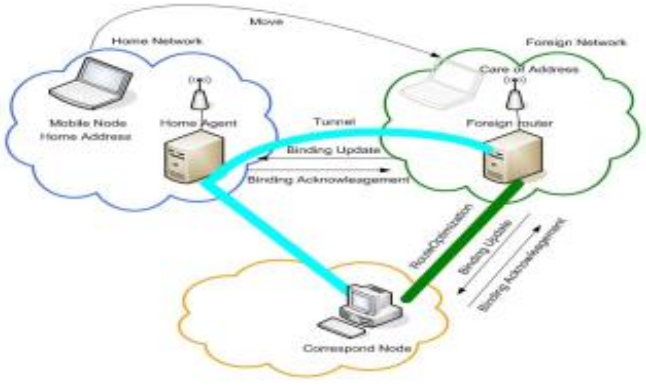

Fig. 1. MIPv6 Architecture

As MN reach to foreign network and get the CoA. This CoA must be configured with the HA via sending Binding Update (BU) message to Home Agent (HA). HA stores (HoA, CoA) pairs in binding cache. To keep this mapping up-to-date, MN

periodically informs it's HA about its new CoA via binding update messages. After successful registration to the foreign network, MN and CN can communicate in two ways. The first mode is known as "Bidirectional" mode. In this mode, Correspondent Node (CN) sends packets to MN's home address and then, the home agent intercepts the packets and forwards them to the MN Care-of-Address. In this process, home agent encapsulate the data packets and during encapsulation source address in the packet is home address and destination address as MN address. When the packet reached at MN, it de-capsulate the packet to retrieve the actual message send by CN. In second mode, CN can directly send data packets directly to MN to avoid triangle routing from CN to HA and then HA to MN. The triangular routing creates delay caused by a long trip time that affects real time traffic. The process of directly transfer of data between MN and CN is called route optimization. It needs to send Binding Update (BU) to its Home Agent (HA) to register its new location. After receiving the Binding Acknowledge (BA) from HA, it can use its home address to communicate with Internet. MN can also send BU to Corresponding Nodes (CN) to optimize the routing between them. The security is one of the important aspects in route optimization. It is not the part of this paper.

3. HANDOVER IN MIPV6

When a MN changes its point of attachment to the network and moves from one network to another new network. This process is known as handoff or handover. During this process, the MN usually has disconnected from the old network and connects to the new network. The handover can be categorized on the basis of connection status and the network technology.

On the basis of connection status, the handover can be categorized as soft handover and hard handover. A handover process is said to be hard handover if MN changes its point of attachment with interruption of service. For this MN releases radio link from old base station before establishing radio link to new base station. Hard handoff is mostly used in FDMA (Frequency Division Multiple Access) and TDMA (Time Division Multiple Access) channel access methods. This handover method is known as brake before make. On the other hand, handover process is said to be soft handover, when the MN is always connected to the network via at least one base station with the help of radio link. Hence, there must be an overlap of different link usage during the soft handover process. This implies either multiple interfaces or multiple radio modules on a single interface are available on the MN.

Now a days different types of wireless technologies are developed. Each of the technology provides different connection range, network capability and so on attributes. Therefore, and during the movement the mobile devices may use different access technologies. In case of intra-technology handover the handover occurs between access points within same access router using same technology. The example of intra-technology handover is horizontal handover. On the other hand, handover is said to be inter-technology handover, if a handover occurs between access router using two different technologies. The example of inter-technology handover is vertical handover.

Thus, horizontal handover and vertical handover depends on change of its access network or access router by mobile node. The horizontal and vertical handoffs [2] are categorized on the basis of link layer and IP layer.

A. Horizontal Handover

If during the handover process, the MN changes its point of attachment without affecting the IP layer (i.e. L_3) is known as horizontal handover. Thus the only link layer (i.e. L_2) participates in the horizontal handover process. In such type of handover mobile node changes only its access point (point of attachment) without changing the access router. The layer 2 handover processes a scan phase, authentication phase and association phase.

MN moves between different wireless accesses points that are served by the same IP access router. The mobile node initially connected to access point-1. After handover mobile get connected to access point-2 and disconnected to access point-2. As shown in Figure 2, during the handover process only link layer association is changed. The IP layer remains unaffected due to movement of mobile node.

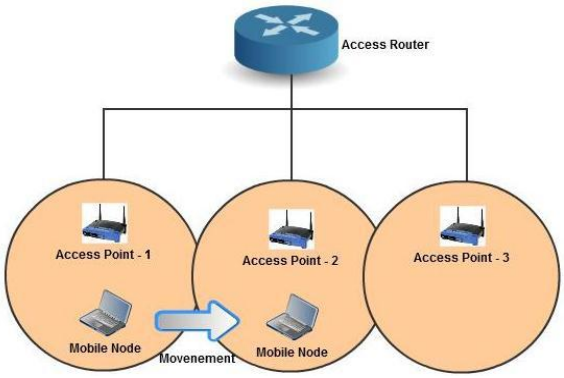

Fig. 2. Horizontal Handover

B. Vertical Handover

If during the handover process, the MN changes its point of attachment that affect the IP layer (i.e. L_3) is known as vertical handover. Thus in vertical handover link layer (i.e. L_2) as well as IP layer (i.e. L_3) participates. In such type of handover mobile node changes its access router and access point both.

The vertical handover is depicted in Figure 3. In this figure, the mobile node moves from the access point-1 under access router-1 to the access point-1 under access router-2. The IP-layer handover occurs during movement mobile node connected with different access router. Since the access router of the mobile node has changed, the access network topology is also changed.

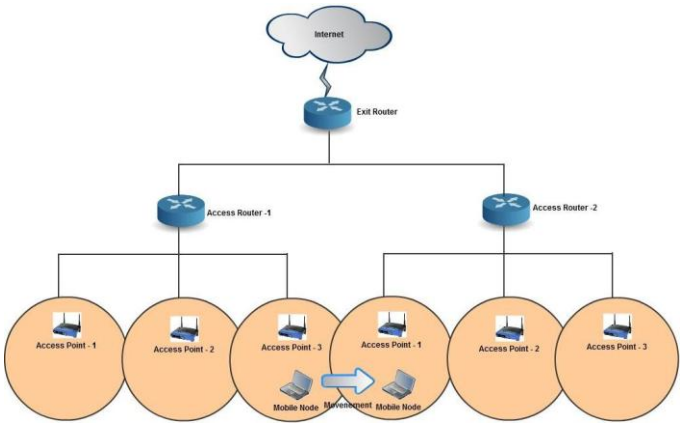

Fig. 3. Vertical Handover

4. FACTORS AFFECTING THE HANDOVER LATENCY

A handover in MIPv6 is sequence steps as shown in Figure 4. This sequence includes Movement Detection (MD), Candidate Access Router Discovery (CARD), Address Configuration (AC), Duplicate Address Detection (DAD), Authentication & Authorization (A&A), Care-of-address Registration, Binding Update (BU) and Binding Acknowledgement (BA) [2].

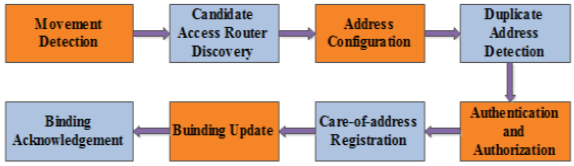

Fig. 4. Handover Process in MIPv6

A. Movement Detection (MD)

Movement detection is first step of handover process. It is critical in order to provide mobility, since delays in movement detection mechanisms will cause delays in obtaining a new CoA. This will again decrease the performance when moving between different networks. Movement detection can be described as the time taken for a mobile node to aware its movement into another new network area. In MIPv6 the movement detection is layer-3 process in which MN try connects a new network and breaks the connection from old network.

In MIPv6 enabled wireless networks, every wireless router multicasts a Router Advertisement (RA) message through its APs periodically. The multicasting of RA depends on minimum and maximum router advertisement interval. If the MN do not receive RA message from the connected access router and the time interval is larger than the maximum router advertisement interval. It is a hint [3] for MN that it is a new subnet. Then the MN will immediately multicasts a Router Solicitation (RS) message. If any router in the range of MN finds that message will immediately response back to MN via sending a RA message. The RA message includes access router MIPv6 address and link address of access point.

B. Candidate Access Router Discovery (CARD)

Once the IP-layer movement is detected by MN. It is necessary to MN to find out new access router for further communication. The candidate router selection is a complicated process in which firstly make the list of all available candidate routers the can provide services to MN via APs and then after selection of most appropriate router for communication. There are two methods for selecting the candidate routers [4] (a) Mobile Node Orchestrated Mode (b) Network Assisted Mode.

1) Mobile Node Orchestrated Mode: In this mode the MN discovers a new AP by periodic L_2 scan [5] of the non-IP-connected interfaces. After this MN requests for the capabilities of the newly discovered CAR by sending MN-AR CARD Request ICMP options. In reply the capabilities to the MN by sending AR-MN CARD Reply ICMP options. The MN orchestrated CARD mechanism is shown in Figure 5.

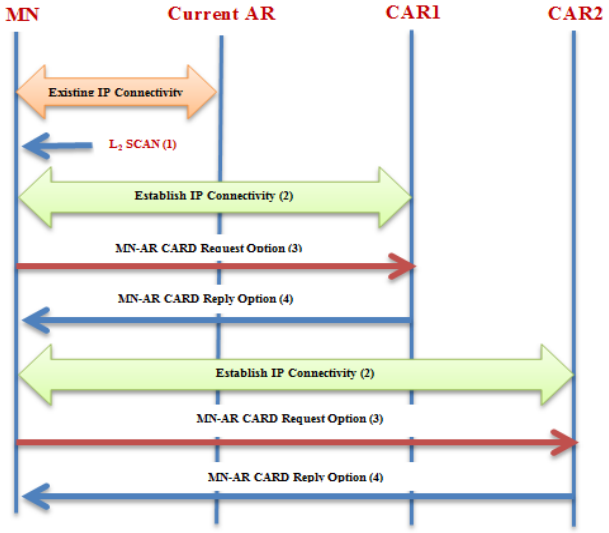

Fig. 5. MN orchestrated CARD

MN orchestrated mode is less used due increases in cost and complexity of hardware design. Because generally one network interface can only allow the MN to connect with one CAR. But in above mode, MN must have multiple network interfaces to maintain connections with different CARs.

2) Network Assisted Mode: In this mode all candidate access routers must be registered with the candidate access routers server. The CARD [6] process is initiated when MN receives a beacon message from a new AP during periodic L2 scan process as shown in Figure 6. Then MN sends an MN-AR CARD request to obtain the identity and the capabilities of the associated CAR, which passed the Layer-2 ID of the new AP to the current AR. If information is not available in local cache, the current AR subsequently sends AR-Server CARD Request message to the CARD server to resolve the IP address of the serving AR of the newly discovered AP. The CARD server then resolves the link layer ID to the IP address of the CAR and returns the identity of the CAR as well as available static capabilities to the requesting AR in the Server-AR CARD Reply message. Upon receipt of the Server-AR CARD Reply message, the current AR extracts the IP address of the CAR and in turn requests remaining capabilities by sending AR-AR CARD request message to the CAR. The CAR subsequently conveys its capabilities to the requesting AR in AR-AR CARD reply message. Upon receipt of the AR-AR CARD reply message, the current AR caches the CAR's capabilities as well as the L2-L3 mapping information in local cache and encodes the capabilities as the sub-options of the AR-MN CARD Reply ICMP options. The AR-MN CARD reply ICMP options are conveyed to the Mobile Node either as piggybacked options of an outgoing MIP Proxy Router Advertisement message or the options of the new AR-MN CARD ICMP message.

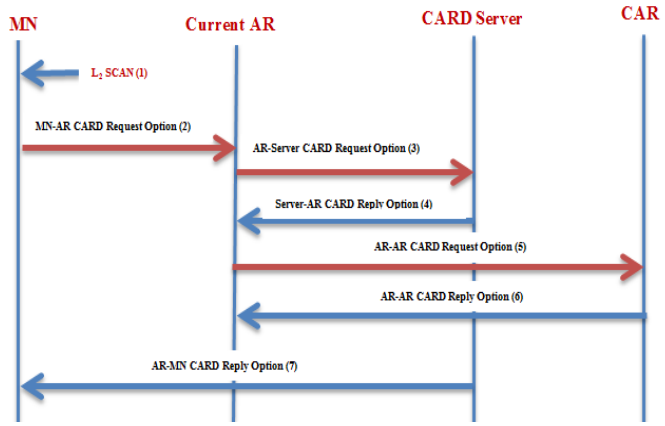

Fig. 6. Network Assisted Mode

C. Address Configuration (AC)

Once we have a list of candidate access routers. Now we have to select target access router. Selection procedure of access router is based on specific properties such as bandwidth, available channels and so on.

D. Duplicate Address Detection (DAD)

Once the candidate access router is selected. Now a new IP addresses has to configure for MN. Access Router generates a 64-bits prefix and sent it to MN. Now MN generates a 64-bit suffix randomly or based on interface and combines with the prefix obtained from the router to get the 128-bit IPv6 address. This new address is referred to as a Tentative Address. The uniqueness of this tentative address must be checked before using this address as CoA. This process is referred to as the Duplicate Address Detection (DAD) [7]. For this MN broadcast a Neighbour Solicitation (NS) message local link asking if anyone is using its Tentative Address. If tentative address is already used by another node, that node must send a Neighbour Advertisement (NA) message to defend its address. Then MN has to generate a new tentative address and repeat the DAD process until tentative address is not unique in the network.

E. Authentication and Authorization (AA)

The Authentication and Authorization process is used for checking whether an MN has the authority to use the connection from an AR.

F. Care-of Address Registration

When a MN leaves its home network and gets connected to a foreign network or changes its location from one foreign network to another, in both case it gets a new care-of-address. During the time from when the MN lost connectivity with its previous access router until it informs its HA of its new location, all packets that have been sent to it will have been lost and it will not have been able to send packets to any of its correspondent node (CN). Every HA maintains a Binding Cache Entries (BCE) [8] table that contains biding of home address (HoA) with care-of-address of MN. The BCE has to update by sending binding update (BU) message, which includes, new care-of-address, to HA.

G. Binding Update (BU)

Binding update messages are transmitted In two cases: (a) During CoA registrations the Binding Update (BU) take place only in between MN and HA (b) During Route Optimization (RO) BU take place in between MN and CN.

(a) As seen in CoA, the BU take place only in between MN and HA. In this case all packet transmission between MN and CN take place via HA. It is known as bidirectional tunning mode and increases round trip time (RTT).

(b) To overcome from large RTT problem Route Optimization (RO) mode is used. In RO mode packets are directly transmitted between MN and CN besides transmitting through HA that makes triangular routing. In this mode CN and MN maintain Binding Cache Enter (BCE). To keep (HoA, CoA) pair mapping up-to-date, the MN also has to periodically inform its CN about its new CoA via Binding Update (BU) message. However, if the CN is communicating for the first time with the MN, then the packet has to go through the Home Agent first before being routed to the MN Care-of-Address.

Route optimization is the implementation of the Return Routability (RR) [1] procedure. The RR protocol consists of two checks, a home address check and a care-of address check. Basically, it means that a node verifies that there is a node that can respond to packets sent to a given address. It is assumed that a successful reply indicates that there is indeed a node at the given address, and that the node is willing to reply to the probes sent to it. The message flow is depicted in Figure 7.There are four messages used to perform the return routability procedure between MN, HA and CN. These messages are:

- Home Test Init (HoTI)
- Home Test (HoT)
- Care-of Test Init (CoTI)
- Care-of -Test (CoT)

In brief, for authentication during RO, MN generates two messages HoTI sent to CN via HA while CoTI directly to CN. In response to these messages CN sent two messages to MN HoT via HA and CoT directly to MN. Once the nodes are authenticated, now communication to MN and CN directly take place.

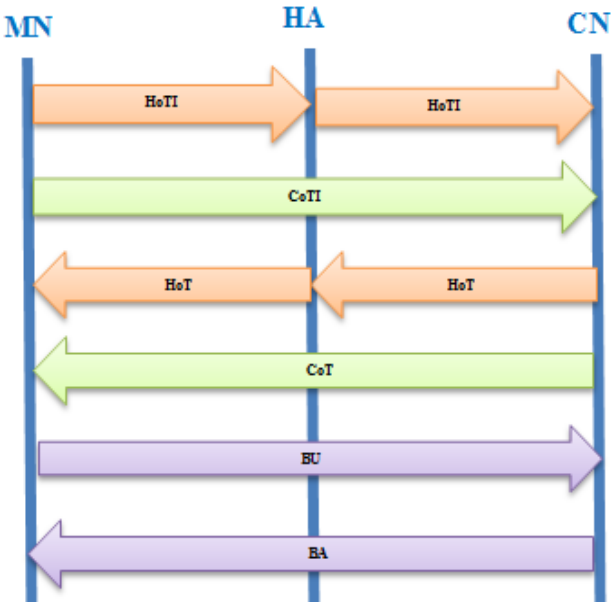

Fig. 7. Messages in Route Optimization

Route Optimization (RO) [1] reduces network utilization, load on the home agent and round trip time for application endpoints. Once the security credentials successfully done, MW sent a binding update message to CN.

H. Binding Acknowledgement (BA)

MN can enforce the receiver to acknowledge the receipt of a binding update by responding a Binding Acknowledgement. Until receipt of the Acknowledgement the MN continues retransmittinghe binding update message periodically. Once the MN has received BA's from its CNs, the handover process can be considered completed.

The total IP handover delay is sum of the above-mentioned latency components. If total handover delay, movement detection, candidate access router discovery, address configuration, duplicate address detection, authentication and authorization, care-of-address registration, route optimization, binding update, binding acknowledgement are represented by THD, TMD, TCARD, TAC, TDAD, TAA, TCoAR, TRO, TBU, TBA respectively. Then total handover delay described by

$$T_{HD} = T_{MD}+T_{CARD}+T_{AC}+T_{DAD}+ T_{AA}+T_{CoAR}+T_{RO}+T_{BU}+T_{BA}$$

5. CONCLUSION

MIPv6 is the next generation mobility management protocol. In MIPv6 the handover management is a critical issue. Layer-2 and Layer-3 are involved in handover management process and responsible for handover latency. Generally, handover is classified as horizontal and vertical handover. Layer-2 is responsible for horizontal handover and Layer-3 is for vertical handover. For MIPv6 eight sub processes are responsible for handover latency. These are movement detection, candidate access router Discovery, address configuration, duplicate address detection, authentication & authorization, care-of-address registration, Binding Update and binding acknowledgement. In this paper we have identified the components responsible for handover latency. As a future work, these components can be numerically analysed with the help of simulators.

[9]

6. REFERENCES

[1] Perkins, D. Johnson, and J. Arkko, "Mobility Support in IPv6", Internet Engineering Task Force, Request for Comment 3775, Jun 2004.

[2] Yu-xuan Hong, "DAD-Less MIPv6 for Reduced Handover Latency", IEEE IMSI international conference, ISBN: 978-0-7695-4372-7, 2011, Page(s): 353 – 360.

[3] Greg Daley, Samsung AIT, "Movement Detection Optimization in Mobile IPv6" Internet Engineering Task Force, 2003.

[4] M. Liebsch," Candidate Access Router Discovery" Internet Engineering Task Force, Request for Comment 4066, Jun 2005.

[5] Youngsong Mun etc., "Enhanced Fast Handover for Mobile IPv6 based on IEEE 802.11 Network", http://tools.ietf.org/html/draft-mun-mipshop-efh-fast-mipv6-06, 2012.

[6] D. Di Sorte, "Target access router selection in advanced mobility scenarios", Computer Communications Volume 29, Issue 3, 2006, Pages 337–357.

[7] N. Moore: Optimistic Duplicate Address Detection (DAD) for IPv6 Network Working Group, Request for Comment 4429, 2006.

[8] Muhanna etc., "Binding Revocation for IPv6 Mobility", Internet Engineering Task Force, Request for Comment 5846, 2010.