ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

A Review on Handover Processes in IPv6 Mobility Management Protocols

Ritika[1], Dinesh Kumar Verma[2]

Student, Electronics & Communication, PDM College of Engineering, Bahadurgarh, India [1]

Assistant Professor, Electronics & Communication, PDM College of Engineering, Bahadurgarh, India [2]

Abstract: Mobility over internet connection being one of the essential requirements of communication industry needs a thorough study. For this, Internet Engineering Task Force (IETF) is been continuously working towards the development of such protocols that help in maintaining a connection between end users during handoff. As a result of it Mobile IPv6 (MIPv6) and its extensions like Fast Mobile IPv6 (FMIPv6), Hierarchical Mobile IPv6 (HMIPv6) are standardized as host-based mobility management protocols. FMIPv6 is divided into predictive and reactive modes. Similarly HMIPv6 is explained in intra-MAP domain and inter-MAP domain. Further advancement results in network-based localized mobility management protocol i.e. Proxy Mobile IPv6 (PMIPv6) and Fast Proxy Mobile IPv6 (FPMIPv6). These protocols are also called as optimization techniques of MIPv6. This paper provides a constructive survey of these protocols by classifying, discussing the detailed signaling of protocols. This will lead to better understanding of current protocols and guide a way for further enhancements.

Keywords: Mobile IPv6 (MIPv6), Fast Mobile IPv6 (FMIPv6), Hierarchical Mobile IPv6 (HMIPv6), Proxy Mobile IPv6 (PMIPv6), Fast Proxy Mobile IPv6 (PMIPv6).

I. INTRODUCTION

With the advent of increasing number of internet users over mobile network, there is a great need of awareness about such protocols that can provide un-interrupted and reliable communication between two end-points. As we know that every device connected over internet has its own IP address. This address is required to provide communication between two end users. But when the mobile internet device moves outside of its home network then there is a great need of such protocols that route data packets to the same destination while maintaining original or temporary IP address. The whole process is known as Handover. More technically, a Handover or Handoff is a movement of an MN between two attachment points, i.e., the process of terminating existing connectivity and obtaining new connectivity [1]. In addition handovers are considered Link Layer (L2) if they are performed between connection points belonging to the same subnet, or Network Layer (L3) if they are performed between different subnets and require the configuration of a different IPv6 address. In particular, mobility support in the network layer has been developed by the Internet Engineering Task Force (IETF). The main goal of the mobility protocols is to enable network applications to operate continuously at the required quality of service for both wired and wireless networks [2]. The IETF is continuously working in creating and further advancing the existing mobility management protocols. Mobile IP consists of both MIPv4 and MIPv6, but MIPv4 has a couple of drawbacks, the main one being IP address exhaustion making MIPv6 the future option for mobility protocol in IP Networks [3]. MIPv6 uses the existing IPv6 protocol to enable seamless roaming between different access points [2], [4].

IETF classified mobility management protocols as: host-based and network-based. Some of the host-based mobility management protocol are Fast Mobile IPv6 (FMIPv6), Hierarchical Mobile IPv6 (HMIPv6) and combination of last two i.e. Fast Hierarchical Mobile IPv6 (FHMIPv6). Similarly standardized network-based localized mobility management protocols are Proxy Mobile IPv6 (PMIPv6) and Fast Proxy Mobile IPv6 (FPMIPv6).

II. MOBILITY MANAGEMENT PROTOCOLS

These are the protocols that basically manage the mobility of the devices connected over internet. Here mobility specifies the change of location of the device. Some of the mobility management protocols of IPv6 are explained below.

A. Mobile IPv6 (MIPv6)

MIPv6 uses the existing IPv6 protocol to enable seamless roaming between different access points. MIPv6 supports the mobility of IP hosts by allowing them to utilize two IP addresses: a Home Address (HoA), and a Care-of-Address (CoA).

MIPv6 Terminology [6]**:-**

Mobile Node (MN): The MN is a node that moves between different networks, namely the home network and foreign networks.

Home Network (HN): The MN is permanently connected to this network. The subnet of this network corresponds to the home address of the MN and home agent [3].

Home Agent (HA): The home agent is a router in the HN responsible to forward packets destined for the MN when the MN has moved to a foreign network.

Access Router (AR): The AR is the end point of wired network and provides services to MN via wireless radio links. It is directly connected to HA via direct tunnel.

Foreign Network (FN): This is the network to which the MN moves and attaches when not in the HN.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

Foreign Agent (FA): The foreign agent is a router in the FN to which a MN attaches when not in the HN. The FA assigns a care-of-address to the MN and is used to forward and receive packets destined for the MN.
Home Address (HoA): This address represents the address of MN in home network.
Care-of-Address (CoA): This address is a IPv6 address assigned to the MN via the foreign agent and can be a agent care-of-address, or a co-located care-of-address. The MN uses this address to communicate when not in its home network.
Correspondent Node (CN): The CN is a node located somewhere in any network and communicates with the MN.

Signal flow steps in MIPv6: The sequence of signal flow during handover process in MIPv6 is shown in Fig. 1.

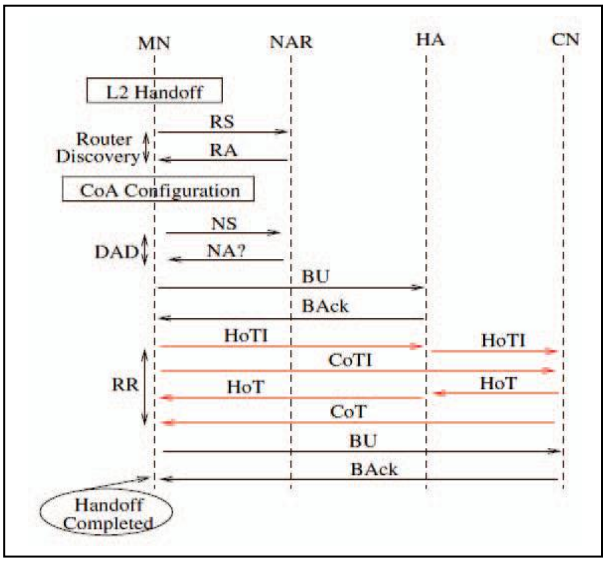

Fig. 1 Signaling messages sequence: MIPv6 [5]

Step l: Discovery of New Access Router (NAR) is performed through Router Solicitation (RS)/ router Advertisement (RA) messages exchange. MN scans the available networks by capturing RA message or MN can send RS messages to trigger the process.
Step 2: Address configuration and Duplicate Address Detection (DAD) is start by sending Network Solicitation (NS) message.
Step 3: After completing DAD, an address is assigned to MN in Foreign Network (FN) which is known as Care-of-Address (CoA). After assigning the CoA the MN receives Network Advertisement (NA) from AR.
Step 4: Once the CoA is assigned in foreign network, the MN informs to Home Agent (HA) about binding update by sending Binding Update (BU) message.
Step 5: In response to BU the HA creates a Binding Cache Entry (BCE) and stores as pair of Home Address (HoA) and Care-of-Address (CoA).
Step 6: After completing the BCE, the HA informs back to MN about updating by sending Binding Acknowledgement (BAck) message.

Now the communication between MN and CN starts but suffers from triangular routing that causes delay in packet delivery. To overcome from triangular routing the Route Optimization (RO) is called with the help of Return Routability procedure (RR).
Step 7: In RO, two messages one from MN is forwarded to CN via HA. This message is known as Home Test Init (HoTI). Another message Care-of Test Init (CoTI) is also forwarded from MN to CN directly. The CN verifies both the messages.
Step 8: If the verification of HoTI and CoTI is successful at CN, then it reply back MN via two messages Home-test (HoT) and Care-of -Test (CoT). The HoT is forwarded via HA and CoT directly to MN. Again at MN both messages are compared.
Step 9: If the match occurs then MN binds its address to CN address and sends Binding Update (BU) message to CN. After receiving BU, the CN also update its BCE and binds with MN address.
Step l0: After successful binding the CN reply back to MN via Binding Acknowledgement (BAck) message.
Step 11: Now the MN starts directly communication with CN without participation of HA and vice-versa.

B. Fast Mobile IPv6 (FMIPv6)

Fast Handovers for Mobile IPv6 (FMIPv6) [2] is implemented based on the MIPv6. Its goal is to reduce the handover latency. The principle is to let the mobile node establish a new temporary address with the new access router before breaking connection with the previous access router. FMIPv6 operates in two modes: Predictive and Reactive. In both modes the link layer information (L2 trigger) is used either to predict or rapidly respond to handover events.

FMIPv6 Terminology [6]**:-**
Access Router (AR): This router refers to the MN's default router.
Access Point (AP): The AP refers to the device that enable wireless connection to the MN and is a Layer 2 device connected to a IP subnet.
Previous Access Router (PAR): This router refers to the MN's default router prior to its handover.
New Access Router (NAR): This router refers to the MN's new router subsequent to its handover.
Previous Care-of-Address (PCoA): The valid IP address on the PAR's subnet.
New Care-of-Address (NCoA): The valid IP address on the NAR's subnet.

1) FMIPv6 (Predictive Mode):

Signal flow steps in FMIPv6 (In Predictive Mode): The sequence of signal flow in Predictive Fast handover Mode is shown in Fig. 2(a).
Step 1: When an MN detects its movement toward NAR, by using L2 trigger, it exchanges Router Solicitation for Proxy (RtSolPr) and Proxy Router Advertisement (PrRtAdv) messages with the PAR to obtain information about NAR and to configure a new CoA (NCoA).
Step 2: MN sends a Fast Binding Update (FBU) to PAR in order to associate previous CoA (PCoA) with NCoA.

DOI 10.17148/IJARCCE.2015.45102

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

Step 3: Handover Initiate (HI) and Handover Acknowledgment (HAck) message are exchanged to form a bi-directional tunnel between PAR and NAR.

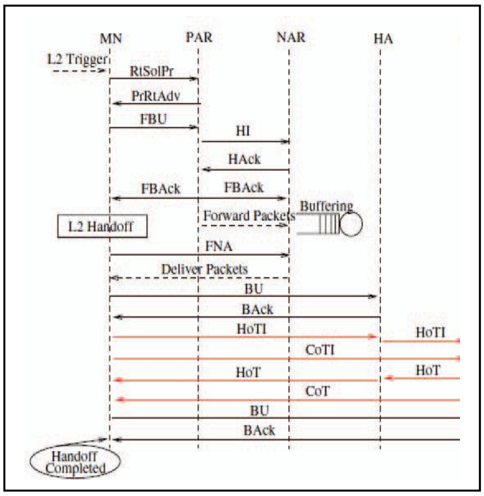

Fig. 2(a) Signaling messages sequence: Predictive FMIPv6 [5]

Step 4: The Fast Binding Acknowledgment (FBAck) message is used to report status about validation of preconfigured NCoA and tunnel establishment to MN.
PAR establishes a binding between PCoA and NCoA so that any packets addressed to PCoA can be forwarded towards NCoA through NAR's link.
Step 5: The NAR buffers forwarded packets from PAR until the MN attaches to NAR's link.
Step 6: Then, NAR delivers the buffered packets to the MN after it receives Fast Neighbor Advertisement (FNA) from MN.

2) FMIPv6 (Reactive Mode):

A counterpart to predictive mode of FMIPv6 is reactive mode which refers to the case where the MN does not receive the FBack on the previous link since either the MN did not send the FBU or the MN has left the link after sending the FBU (which itself may be lost), but before receiving an FBack.

Signal flow steps in Reactive FMIPv6: The sequence of signal flow in Reactive Fast handover Mode is shown in Figure 2(b).

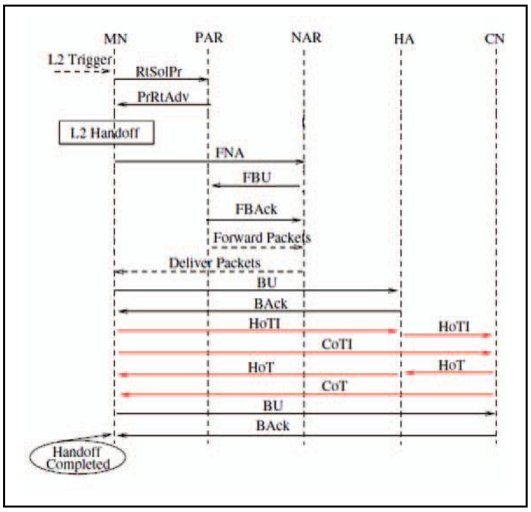

Fig. 2(b) Signaling messages sequence: Reactive FMIPv6 [5]

Step 1: In this case, since an MN is not sure whether PAR has successfully processed the FBU, it forwards FNA encapsulated with FBU, as soon as it attaches to NAR.
Step 2: If NAR detects that NCoA is in use (duplicate address) when processing the FNA, it must send a Router Advertisement (RA) message, discarding the inner FBU, with the Neighbor Advertisement Acknowledge (NAACK) option including an alternate IP address for the MN to use.
Step 3: Otherwise, NAR forwards FBU to PAR which responds with FBack.
Step 4: At this time, PAR tunnels any packets addressed to PCoA to NCoA at NAR which delivers these packets to the MN.

C. *Hierarchical Mobile IPv6 (HMIPv6)*

With MIPv6, an MN performs binding update to HA/CNs regardless of its movements to other subnets. This induces unnecessary signaling overhead and latency. To address this problem, HMIPv6 was proposed to handle handoff locally through a special node called Mobility Anchor Point (MAP). MAP allows for local handoff. It is a router located in a network visited by the MN and used as a local HA.
HMIPv6 operates in two scenarios: Intra-MAP domain i.e. within MAP domain and Inter-MAP domain i.e. between two different MAP's.
Whenever MN moves within MAP's domain (Fig. 3(a)) or access network (AN) it does not need to transmit BU messages to HA/CNs, but only to MAP when its LCoA changes. Hence, the movement of an MN within MAP domain is hidden from HA/CNs.

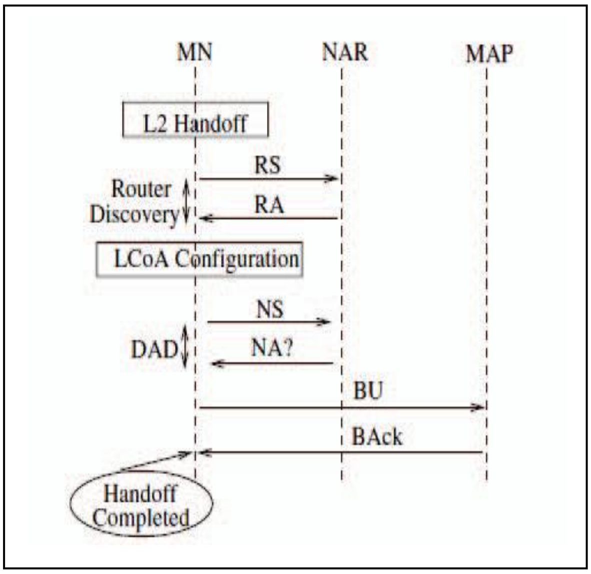

Fig. 3(a) Signaling messages sequence: Intra-MAP HMIPv6 [5]

For inter-MAP domain roaming (Figure 3(b)), MIPv6 is used rather than HMIPv6. Whenever an MN crosses a new MAP's domain, it has to registered with new MAP. Also BU messages need to be sent by the MN to its HA/CNs to inform them of its new location.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

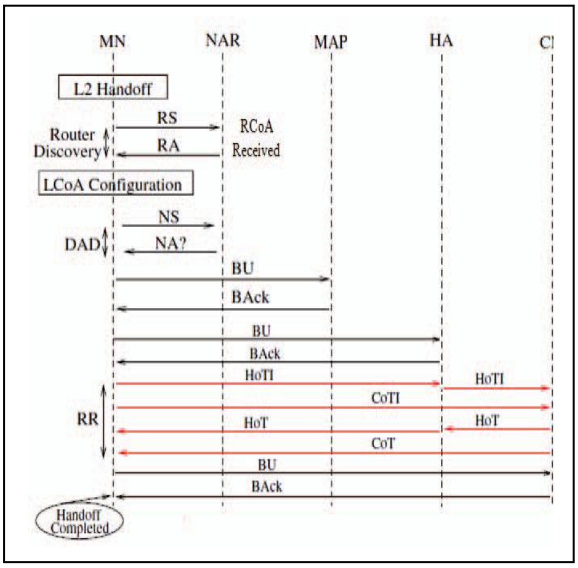

Fig. 3(b) Signaling messages sequence: Inter-MAP HMIPv6 [5]

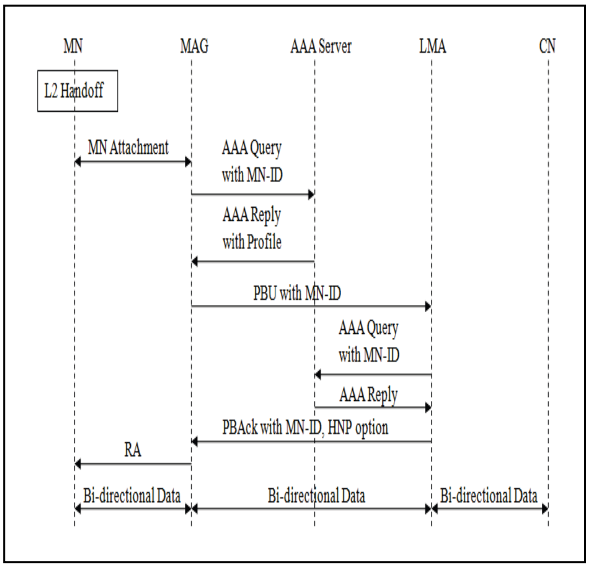

Fig. 4 Signaling messages sequence: PMIPv6 [5]

D. Proxy Mobile IPv6 (PMIPv6)

Proxy Mobile IPv6 (PMIPv6) is a network-based mobility management protocol that allows an MN to change its point of attachment without any mobility signaling processed at the MN.

PMIPv6 Terminology: The entities in this protocol are: MAG, LMA, AAA Server.

Mobile Access Gateway(MAG) [8]: It is responsible for detecting the movement of MNs and deals with mobility-related signaling. It establishes a tunnel with the MN's LMA.

Local Mobility Anchor (LMA) [8]: It is responsible for maintaining the MN location and forwarding data packets from/to MNs. Its functions are similar to those of HA in MIPv6.

Authentication, Authorization & Accounting (AAA) Server [9]: It manages MN's authentication and maintains MN's profile which is a set of parameters configured for a given MN.

Signal flow steps in PMIPv6 [7]: The sequence of signal flow in PMIPv6 is shown in Figure 4.

Step 1: When MAG detects the attachment of MN, it obtains MN's profile by using MN-ID after successful access authentication from AAA Server.

Step 2: MAG sends a Proxy Binding Update (PBU) message to MN's LMA on behalf of the MN to update the LMA about the current location of the MN.

Step 3: When LMA receives a PBU message for the same MN from the MAG, it queries AAA Server for received MN-ID.

Step 4: On receiving reply from AAA Server, the Binding Cache Entry (BCE) is updated with a new address of MAG (Proxy-CoA). Otherwise the LMA deletes the MN's binding cache entry and removes the routing state for the MN-HNP (Home Network Prefix).

Step 5: Then LMA sends a Proxy Binding Acknowledgment (PBA) to MAG, MAG then sends RA messages to the MN with its MN-HNP.

A tunnel is established between the LMA and the MAG, after which all traffic sent from the MN gets routed to its LMA through the tunnel.

E. Fast Proxy Mobile IPv6 (FPMIPv6)

Fast Handover for Proxy Mobile IPv6 (FPMIPv6) is an another network-based mobility management protocol. It describes the protocol to reduce the handover latency for PMIPv6.

FMIPv6 Terminology:-

Previous Access Network (P-AN): The network to which MN is attached before handover process.

New access Network (N-AN): The network to which MN is attached after handover process.

Previous Mobile Access Gateway (PMAG): The MAG that manages mobility-related signaling for MN before handover.

New Mobile Access Gateway (NMAG): The MAG that manages mobility-related signaling for MN before handover.

FPMIPv6 operates in two modes: Predictive Mode and Reactive Mode. In the predictive mode, a bi-directional tunnel is established before the MN attaches to the nAN. In the reactive mode, the bi-directional tunnel is established after the MN attaches to the nAN.

1) FPMIPv6 (Predictive Mode):

Signal flow steps in FPMIPv6 (In Predictive Mode): The sequence of signal flow in Predictive Fast handover Proxy Mode is shown in Figure 5(a).

Step 1: When MN detects that handover is about to happen then reports its identifier (MN ID) and New Access Point Identifier (New AP ID) to which the MN most likely to move.

Step 2: The P-AN to which the MN is currently attached indicates the handover of MN to the PMAG with MN ID and New AP ID.

Step 3: The PMAG derives the NMAG from the New AP ID. The PMAG then sends Handover Initiate (HO) message to NMAG and then receives Handover Acknowledgement (HAck) back from NMAG.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

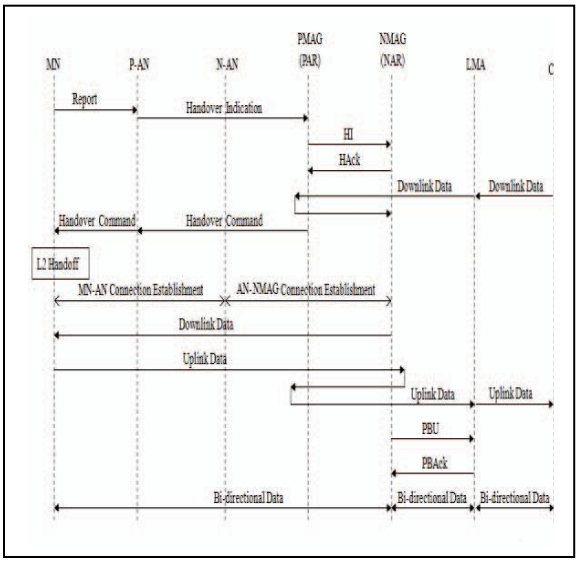

Fig. 5(a) Signaling messages sequence: Predictive FPMIPv6 [5]

Step 4: A bidirectional tunnel is established between the PMAG and NMAG, and packets destined for the MN are forwarded from the PMAG to the NMAG over this tunnel.
Step 5: After decapsulation, these packets are buffered at the NMAG. If connection between the N-AN and NMAG has already been established, those buffered packets are forwarded towards the N-AN.
Step 6: Once handover is ready on the network side, the MN is triggered to perform handover to the N-AN.
The MN establishes a physical-layer connection with the N-which in turn triggers the establishment of the link-layer connection between N-AN and NMAG if not yet established.
Step 7: The NMAG then starts to forward packets destined for MN via N-AN.
The uplink packets from MN are sent to NMAG via N-AN, and the NMAG forwards them to PMAG. Then PMAG sends packet to LMA that is currently serving the MN.
Step 8: The NMAG then sends Proxy Binding Update (PBU) to the LMA and then LMA sends back the Proxy Binding Acknowledgement (PBAck) to the NMAG. Now the packets to/from MN goes to the NMAG instead of PMAG.

2) FPMIPv6 (Reactive Mode):

Signal flow steps in FPMIPv6 (In Reactive Mode): The sequence of signal flow in Reactive Fast handover Proxy Mode is shown in Figure 5(b).
Step 1: The MN establishes a connection with N-AN, which triggers the establishment of connection between N-AN and NMAG.
Step 2: The NMAG sends HI message to PMAG that includes the MN ID. Then PMAG sends HAck message back to NMAG that includes HNP and address of LMA currently serving the MN.
Step 3: A bidirectional tunnel is established between the PMAG and NMAG through which packets destined for the mobile node are forwarded from the PMAG to the NMAG. After decapsulation, those packets are tunneled to the mobile node via the new access network.

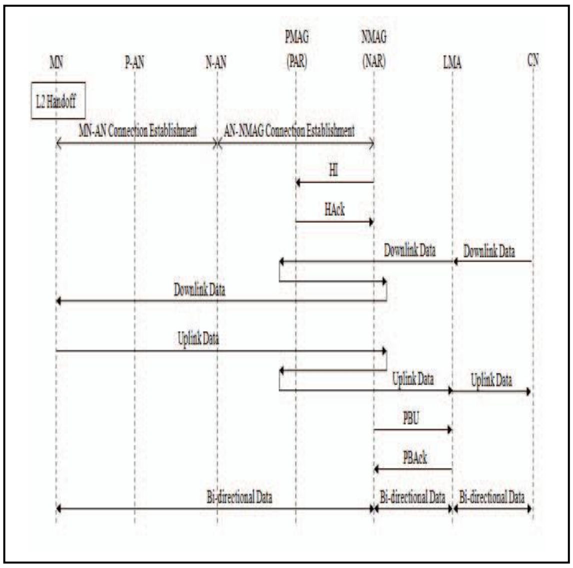

Fig. 5(b) Signaling messages sequence: Reactive FPMIPv6 [5]

Step 4: The uplink packets from the MN are sent to the NMAG via the N-AN, and NMAG forwards them to the PMAG. The PMAG then tunnels the packets to the LMA.
Step 5: The NMAG sends the PBU to the LMA. The LMA sends back the PBA to the NMAG after which packets to/from the MN go through the NMAG instead of the PMAG.

III. CONCLUSION

The IETF has proposed MIPv6 as basic host-based mobility management protocol. In this paper we have classified and discussed some host-based (MIPv6, FMIPv6, HMIPv6) as well as some network-based localized mobility management protocol (PMIPv6, FPMIPv6). A detailed review on signaling message sequence during handoff is studied. The basic signaling messages exchanged are somehow similar but the entities involved are bit different in different protocol. Host-based protocols involve more participation of MN during signal exchange as compared to network-based protocols.

REFERENCES

[1] C. Makaya and S. Pierre, "An Analytical Framework for Performance Evaluation of IPv6-Based mobility Management Protocols", IEEE Transactions on Wireless Communications, vol. 7, no. 3, pp. 972–983, March 2008.
[2] G. Xie, J. Chen, H. Zheng, J. Yang, and Y. Zhang, "Handover latency of mipv6 implementation in linux", Global Telecommunications Conference,2007. GLOBECOM '07. IEEE.
[3] R. Prasad and S. Dixit, Eds., "Wireless IP and Building the Internet," ser. The Artech House Universal Personal Communications Series. Artech House, 2003.
[4] J. Chandrasekaran, "Mobile IP: Issues, Challenges and Solutions," Master's thesis, Department of Electrical and Computer Engineering Rutgers University, 2009.
[5] C. Makaya and S. Pierre, "An Analytical Framework for Performance Evaluation of IPv6-Based mobility Management Protocols", IEEE Transactions on Wireless Communications, vol. 7, no. 3, pp. 972–983, March 2008.
[6] Johan Pieterse, Riaan Wolhuter "Investigation of Handover Techniques in a IPv6 Mobile Network," IEEE-APWC Topical

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

Conference on Antennas and Propagation in Wireless Communications, September 2012.

[7] Khatib Noaman Ashraf, Vidhate Amarsinh, Devane Satish, "Survey and Analysis of Mobility Management Protocols for Handover in Wireless Network," 2013 3rd IEEE International Advance Computing Conference (IACC).

[8] Jorge Dias, Andr´e Cardote, Filipe Neves, Susana Sargento, Arnaldo Oliveira, "Seamless Horizontal and Vertical Mobility in VANET," 2012 IEEE Vehicular Networking Conference (VNC).

[9] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6," Internet Soc., Reston, VA, IETF RFC 5213, Aug. 2008.

[10] H. Yokota, K. Chowdhury, R. Koodli, B. Patil, and F. Xia, "Fast Handovers for Proxy Mobile IPv6", IETF RFC 5949, September 2010.

 DOI 10.17148/IJARCCE.2015.45102