International Journal of Computer Science and Engineering Open Access
Review Paper Volume-2, Issue-3 E-ISSN: 2347-2693

Overview of IPv6 Mobility Management Protocols and their Handover Performances

Fatema Tuz Zohra[1*], Samiul Azam[2] and Md. Mahbubur Rahman[3]

[1*,3] *Department of CSE, Bangladesh University of Business & Technology, Bangladesh*
[2] *CSE Department, United International University, Bangladesh*

www.ijcseonline.org

Received: 5 March 2014 Revised: 14 March 2014 Accepted: 26 March 2014 Published: 31 March 2014

***Abstract*—** IPv6 mobility management is one of the most challenging research topics for an efficient support of global roaming of mobile nodes (MNs) in next-generation wireless networks. The Internet Engineering Task Force (IETF) has developed Mobile IPv6 (MIPv6) and its proposed enhancements, i.e., Fast Handovers for Mobile IPv6 (FMIPv6) and Hierarchical Mobile IPv6 (HMIPv6) as host-based mobility management protocols. Recently IETF working group has standardized network-based mobility management protocols, such as, Proxy Mobile IPv6 (PMIPv6) and Fast Proxy Mobile IPv6 (FPMIPv6). Unlike host-based mobility management protocols PMIPv6 and FPMIPv6 have significant features and enable IP mobility for a host without requiring its participation in any mobility-related signaling. In this literature, host-based IPv6 mobility management protocols including the network-based PMIPv6 and FPMIPv6 are analyzed and compared. Each IPv6 mobility management protocol's characteristics and performance indicators are identified by examining handover operations in terms of handover latency, handover blocking probability and packet loss. The conducted analysis in this literature can be used to facilitate decision making in development for a new mobility management protocol.

Keywords—Fast mobile IPv6 (FMIPv6), fast proxy mobile IPv6 (FPMIPv6), handover, hierarchical mobile IPv6 (HMIPv6), latency, mobile IPv6 (MIPv6), proxy mobile IPv6 (PMIPv6)

I. INTRODUCTION

In a network, the IP addresses for each host are assigned in a topologically significant manner. For each subnet, the address prefixes are different. So, when a mobile node MN moves must be assigned a new address to retain the routing. But, changing the address causes IP session break with any correspondent node. Since a TCP connections are defined by [Source IP, Source Port, Destination IP, Destination Port], MN's address must be preserved regardless of its location to preserve the ongoing IP session. Fig. 1 shows such problems when a mobile node moves into different subnet.

Various mobility management protocols for enabling mobility support in the network layer have been being developed by the Internet Engineering Task Force (IETF). The IETF working group have designed protocol enhancements for IPv6, known as Mobile IPv6, that allow transparent routing of IPv6 packets to mobile nodes. But the standard Mobile IP protocol could result in a high signaling load, as well as, high handoff latency and packet losses for environments where the mobile nodes could change its point-of-attachment frequently. So various enhancements to the MIPv6 base protocol, such as, Fast Handovers for Mobile IPv6 (FMIPv6) and Hierarchical Mobile IPv6 (HMIPv6) have been proposed. But for such conventional solutions a mobile node (MN) is required to have mobility functionalities at its network protocol stack inside, and thus, modifications or upgrades of the MN are forced. As a result the operation expense and complexity are increased for the MN. Network-based mobility is another approach to solving the IP mobility challenge. It enables IP mobility for a host without requiring its participation in any mobility-related signaling. The network is responsible for managing IP mobility on behalf of the host. Proxy Mobile IPv6 (PMIPv6) and Fast Proxy Mobile IPv6 (FPMIPv6) are two network-based mobility management protocols that allows an MN to change its point of attachment without any mobility signaling processed at the MN. A comparative performance analysis for MIPv6, FMIPv6, HMIPv6, PMIPv6 and FPMIPv6 has been carried out in this literature.

The rest of the paper is organized as follows. In Section II, existing mobility management protocols for Mobile IPv6 are explained along with its protocol operation and timing diagram. Section III presents a comparative performance analysis of these protocols. Finally, we conclude the paper in Section IV.

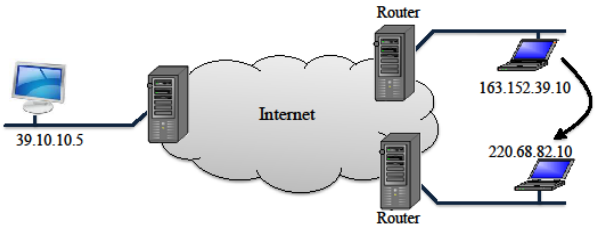

Fig.1. Mobility problem.

II. MOBILITY PROTOCOLS

In this section, existing mobility management protocols for Mobile IPv6 both host-based and network-based are

Corresponding Author: *F. T. Zohra*

explained along with its protocol operation and timing diagram.

A. *Mobile IPv6*

Mobile IPv6 allows nodes to remain reachable while moving around in the IPv6 Internet [1], [2]. There is no need to deploy special routers as "foreign agents". Mobile IPv6 operates in any location without any special support required from the local router. Thus, it avoids triangle routing problem of Mobile IP. Route Optimization is a fundamental part in MIPv6. Besides these, Bi-directional tunneling has become a part of the core protocol. MIPv6 uses Neighbor Discovery to find Link layer addresses of neighbors. In MIPv6, Mobile nodes can obtain Care-of Addresses via Stateless Address Auto-configuration.

The following terminology and abbreviations are used in this protocol.

1) MN: Mobile Node, which can change its access point to the Internet while still being reachable under its Home Address.
2) HoA: Home Address, static IP Address of the Mobile Node valid at its home network.
3) CoA: Care of Address, temporary IP Address of the Mobile Node valid at the actually visited network of the Mobile Node (c/o = care-of).
4) CN: Correspondent Node, any node with which a mobile node is communicating
5) HA: Home Agent, router located at the Mobile Node's home network used by the mobile node for registering its c/o-Address.
6) FA: Foreign Agent, router located at the Mobile Node's visited network used by the mobile node for relaying data packets between MN and HA/CN

Protocol Overview:

a) Mobile nodes use Router Discovery to discover new routers and on-link network prefixes; a mobile node may send Router Solicitation messages, or may wait for unsolicited (periodic) Router Advertisement messages, as specified for Router Discovery. Based on received Router Advertisement messages, a mobile node maintains an entry in its Default Router List for each router, and an entry in its Prefix List for each network prefix, that it currently considers to be on-link. Each time the mobile node moves its point of attachment from one IP subnet to another; the mobile node will configure its care of address by stateless address auto-configuration, or alternatively by stateful address auto-configuration.

b) The association between a mobile node's home address and care-of address is known as a "binding" for the mobile node. While away from home, a mobile node registers its primary care-of address with a router on its home link, requesting this router to function as the "home agent" for the mobile node. The mobile node performs this binding registration by sending a "Binding Update" message to the home agent. The home agent replies to the mobile node by returning a "Binding Acknowledgement" message. Any node communicating with a mobile node is referred as a "correspondent node" of the mobile node, and may itself be either a stationary node or a mobile node. Mobile nodes can provide information about their current location to correspondent nodes by registration. As a part of this procedure, a return rout ability test is performed in order to authorize the establishment of the binding.

c) There are two possible modes for communications between the mobile node and a correspondent node. The first mode, bidirectional tunneling, does not require Mobile IPv6 support from the correspondent node and is available even if the mobile node has not registered its current binding with the correspondent node. Packets from the correspondent node are routed to the home agent and then tunneled to the mobile node. Packets to the correspondent node are tunneled from the mobile node to the home agent ("reverse tunneled") and then routed normally from the home network to the correspondent node. In this mode, the home agent uses proxy Neighbor Discovery to intercept any IPv6 packets addressed to the mobile node's home address (or home addresses) on the home link. Each intercepted packet is tunneled to the mobile node's primary care-of address. This tunneling is performed using IPv6 encapsulation.

d) The second mode, "route optimization", requires the mobile node to register its current binding at the correspondent node. Packets from the correspondent node can be routed directly to the care-of address of the mobile node. When sending a packet to any IPv6 destination, the correspondent node checks its cached bindings for an entry for the packet's destination address. If a cached binding for this destination address is found, the node uses a new type of IPv6 routing header to route the packet to the mobile node by way of the care-of address indicated in this binding. When routing packets directly to the mobile node, the correspondent node sets the Destination Address in the IPv6 header to the care-of address of the mobile node. A new type of IPv6 routing header is also added to the packet to carry the desired home address. Similarly, the mobile node sets the Source Address in the packet's IPv6 header to its current care-of addresses. The mobile node adds a new IPv6 "Home Address" destination option to carry its home address. The message flow diagram of MIPv6 has been shown in Fig. 2.

B. *Hierarchical Mobile IPv6*

Mobile IPv6 allows nodes to move within the Internet topology while maintaining reachability and on-going connections between mobile and correspondent nodes. To do this a mobile node sends Binding Updates to its Home Agent, every time it moves. These round trip delays will disrupt active connections every time a handoff to a new AR is performed. Eliminating this additional delay element from the time critical handover period will significantly improve the performance of Mobile IPv6. Hierarchical MIPv6 [3] addresses the limitations of MIPv6. A new Mobile IPv6

node, called the Mobility Anchor Point, is used in HMIPv6 and can be located at any level in a hierarchical network of routers, including the Access Router (AR). A MAP is essentially a local Home Agent. Movements within MAP are not informed to outer nodes of MAP. Only movements between MAPs are notified to home agent, which reduces mobile signaling message exchanges between inner MAP domain and outer network. The aim of introducing the hierarchical mobility management model in Mobile IPv6 is to enhance the performance of Mobile IPv6 while minimizing the impact on Mobile IPv6 or other IPv6 protocols.

The following terminologies and abbreviations are used:

1) AR: The Access Router AR is the Mobile Node's default router. The AR aggregates the outbound traffic of mobile nodes.
2) MAP: A Mobility Anchor Point is a router located in a network visited by the mobile node. The MAP is used by the MN as a local HA. One or more MAPs can exist within a visited network.

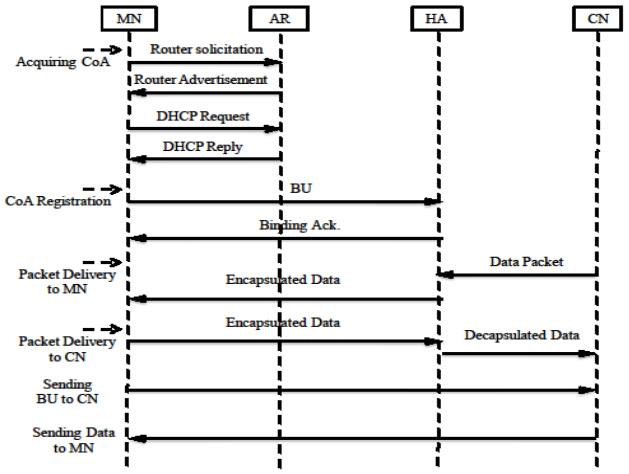

Fig.2. Message flow diagram of MIPv6

3) RCoA: Regional Care-of Address is an address obtained by the mobile node from the visited network. An RcoA is an address on the MAP's subnet. On-link Care-of Address, it is auto-configured by the mobile node when receiving the MAP option.
4) LCoA: The LCoA is the on-link CoA configured on a mobile node's interface based on the prefix advertised by its default router.
5) LBU: Local Binding Update. The MN sends a LBU to the MAP in order to establish a binding between the RCoA and LCoA.

Protocol Overview:

There are two types of handover in HMIPv6 [4]: macro-mobility and micro-mobility.

a) Macro Mobility: When a mobile node moves into a new MAP domain (i.e., its MAP changes), it needs to configure two CoAs: an RCoA on the MAP's link and an on-link CoA (LCoA). The RCoA is formed in a stateless manner. After forming the RCoA based on the prefix received in the MAP option, the mobile node sends a local BU to the MAP with the A and M flags set. The local BU is a BU defined in and includes the mobile node's RCoA in the Home Address Option. No alternate-CoA option is needed in this message. The LCoA is used as the source address of the BU. This BU will bind the mobile node's RCoA (similar to a Home Address) to its LCoA. The MAP (acting as a HA) will then perform DAD (when a new binding is being created) for the mobile node's RCoA on its link and return a Binding Acknowledgement to the MN. This acknowledgement identifies the binding as successful or contains the appropriate fault code. The mobile node must silently ignore binding acknowledgements that do not contain a routing header type 2, which includes the mobile node's RCoA.

After registering with the MAP, the mobile node must register its new RCoA with its HA by sending a BU that specifies the binding (RCoA, Home Address) as in Mobile IPv6. The mobile node's Home Address is used in the home address option and the RCoA is used as the care-of address in the source address field. The mobile node may also send a similar BU (i.e., that specifies the binding between the Home Address and the RCoA) to its current correspondent nodes.

b) Micro Mobility: In this case, MN moves locally between AR within the same MAP domain. MN only changes its LCoA but its RCoA remains unchanged and it does not have to send BU to CN/HA to inform it about its new address.

For the registration process MN sends BU to MAP through AR. MAP then performs duplicate address detection (DAD) check and sends Binding Ack. to MN through AR. If there is any packet addressed to MN's RCoA, MAP will encapsulate and tunnel the packets and sends to MN through the new AR based on MN's new LCoA. The MN de-capsulates the packets and then process the packets in the normal manner.

When the MN moves locally within MAP domain, MN does not have to send binding update to CN or HA since CN/HA sends packets based on MN's RCoA, and subsequently, MAP sends packets to the MN as described before. Unlike basic Mobile IPv6, where MN roaming in a small coverage area (micro-mobility) still needs to send BU to CN/HA that could be located far away from it.

c) Following a successful registration with the MAP, a bi-directional tunnel between the mobile node and the MAP is established. All packets sent by the mobile node are tunneled to the MAP. The outer header contains the mobile node's LCoA in the source address field and the MAP's address in the destination address field. The inner header contains the mobile node's RCoA in the source address field and the peer's address in the destination address field. Similarly, all packets addressed to the mobile node's RCoA are intercepted by the MAP and tunneled to the mobile node's LCoA. The

message flow diagram of HMIPv6 has been illustrated in Fig. 3.

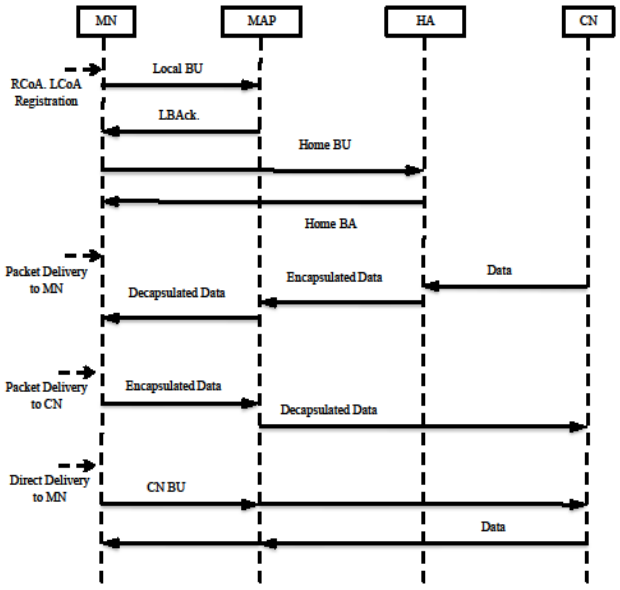

Fig.3. Message flow diagram for HMIPv6

C. *Fast Handovers for Mobile IPv6*

Mobile IPv6 describes the protocol operations for a mobile node to maintain connectivity to the Internet during its handover from one access router to another. These operations involve movement detection, IP address configuration, and location update. The combined handover latency is often sufficient to affect real-time applications. Throughput-sensitive applications can also benefit from reducing this latency. Fast Handover for Mobile IPv6 (FMIPv6) reduces the handover latency. FMIPv6 [5], [6] addresses the following problem: how to allow a mobile node to send packets as soon as it detects a new subnet link, and how to deliver packets to a mobile node as soon as its attachment is detected by the new access router. The protocol defines IP protocol messages necessary for its operation regardless of link technology. By definition, this specification considers handovers that interwork with Mobile IP: once attached to its new access router, an MN engages in Mobile IP operations including Return Routability. There are no special requirements for a mobile node to behave differently with respect to its standard Mobile IP operations.

The terminologies are:

1) PAR: Previous Access Router. The MN's default router prior to its handover.
2) NAR: New Access Router. The MN's default router subsequent to its handover.
3) PCoA: Previous CoA. The MN's Care of Address valid on PAR's subnet.
4) NCoA: New CoA. The MN's Care of Address valid on NAR's subnet.
5) RtSolPr: Router Solicitation for Proxy Advertisement. A message from the MN to the PAR requesting information for a potential handover.
6) PrRtAdv: Proxy Router Advertisement. A message from the PAR to the MN that provides information about neighboring links facilitating expedited movement detection. The message also acts as a trigger for network initiated handover.
7) FBU: Fast Binding Update. A message from the MN instructing its PAR to redirect its traffic (toward NAR).
8) FBack: Fast Binding Acknowledgment. A message from the PAR in response to an FBU.
9) FNA: Fast Neighbor Advertisement. A message from the MN to the NAR to announce attachment, and to confirm the use of NCoA when the MN has not received an FBACK.
10) HI: Handover Initiate. A message from the PAR to the NAR regarding an MN's handover.
11) HAck: Handover Acknowledge. A message from the NAR to the PAR as a response to HI.

Protocol Overview:

a) The protocol begins when a MN sends an RtSolPr to its access router to resolve one or more Access Point Identifiers to subnet-specific information. In response, the access router (e.g., PAR) sends a PrRtAdv message containing one or more [AP-ID, AR-Info] tuples. With the information provided in the PrRtAdv message, the MN formulates a prospective NCoA and sends an FBU message when a link-specific handover event occurs. The purpose of the FBU is to authorize PAR to bind PCoA to NCoA, so that arriving packets can be tunneled to the new location of the MN. Whenever feasible, the FBU should be sent from PAR's link. For instance, an internal link specific trigger could enable FBU transmission from the previous link. When it is not feasible, the FBU is sent from the new link. Care must be taken to ensure that the NCoA used in FBU does not conflict with an address already in use by some other node on the link. For this, FBU encapsulation within FNA must be implemented and should be used when the FBU is sent from NAR's link. Depending on whether an FBack is received on the previous link (which clearly depends on whether the FBU was sent in the first place), there are two modes of operation.

b) Predictive mode of operation: The MN sends an FBU and receives an FBack on the previous link. This means that packet tunneling is already in progress by the time the MN handovers to NAR. The MN should send FNA immediately after attaching to NAR, so that arriving and buffered packets can be forwarded to the MN right away. Before sending an FBack to an MN, PAR can determine whether the NCoA is acceptable to the NAR through the exchange of HI and Hack messages. When assigned addressing (i.e., addresses are assigned by the router) is used, the proposed NCoA in the FBU is carried in HI, and the NAR may assign the proposed NCoA. Such an assigned NCoA must be returned in

HAck, and the PAR must in turn provide the assigned NCoA in the FBack. If there is an assigned NCoA returned in the FBack, the MN must use the assigned address (and not the proposed address in the FBU) upon attaching to NAR. Fig. 4 shows the message flow diagram of such protocol.

c) Reactive mode of operation: The MN sends an FBU from NAR's link. The MN does not receive the FBack

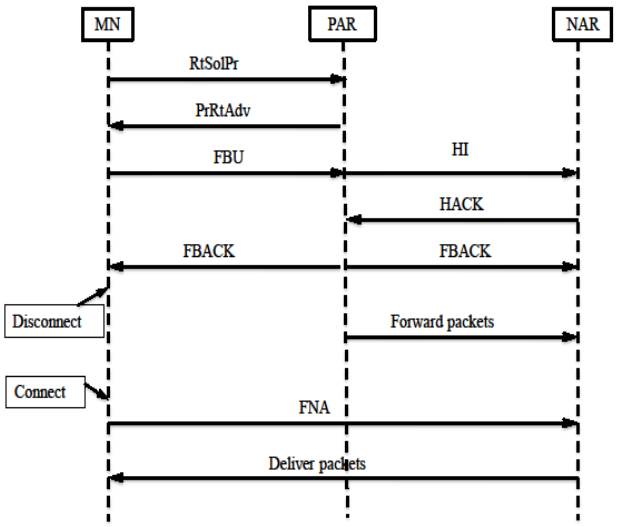

Fig.4. Message flow diagram in predictive FMIPv6.

on the previous link because the MN has not sent the FBU or the MN has left the link after sending the FBU (which itself may be lost), but before receiving an FBack. Without receiving an FBack in the latter case, the MN cannot ascertain whether PAR has successfully processed the FBU. Hence, it (re)sends an FBU as soon as it attaches to NAR. To enable NAR to forward packets immediately (when FBU has been processed) and to allow NAR to verify whether NCoA is acceptable, the MN should encapsulate the FBU in the FNA. If NAR detects that NCoA is in use when processing the FNA, for instance while creating a neighbor entry, it must discard the inner FBU packet and send a Router Advertisement with the "Neighbor Advertisement Acknowledge (NAACK)" option in which NAR may include an alternate IP address for the MN to use. This discarding avoids the rare and undesirable outcome that results from address collision. Fig. 5 shows the message flow diagram of such protocol.

D. Proxy Mobile IPv6

Network-based mobility is another approach to solving the IP mobility challenge. It is possible to support mobility for IPv6 nodes without host involvement by extending Mobile IPv6 signaling messages between a network node and a home agent. This approach to support mobility does not require the mobile node to be involved in the exchange of signaling messages between itself and the home agent. A proxy mobility agent in the network performs the signaling with the home agent and does the mobility management on behalf of the mobile node attached to the network. Because of the use and extension of Mobile IPv6 signaling and home agent functionality, this protocol is referred to as Proxy Mobile IPv6 (PMIPv6) [7]. PMIPv6 allows less signaling in each handoff because there is no Duplicate Address Detection (DAD) in each handoff and no return routability.

The core Entities in PMIPv6:

1) Local Mobility Anchor (LMA)

LMA maintains reachability to the MN's address while it moves around within a PMIPv6 domain. It keeps a binding cache entry for each currently registered MN: a) more extended than the binding cache entry of the HA in MIPv6 b) additional fields include, such as, MN-Identifier, MN's home network prefix, a flag indicating a proxy registration and the interface identifier of the bidirectional tunnel between the LMA and MAG

2) Mobile Access Gateway (MAG)

MAG detects the MN's movements. It initiates mobility-related signaling with the MN's LMA on behalf of the MN. MAG also establishes a tunnel with the LMA for enabling the MN to use an address from its home network prefix. It emulates the MN's home network on the access network for each MN.

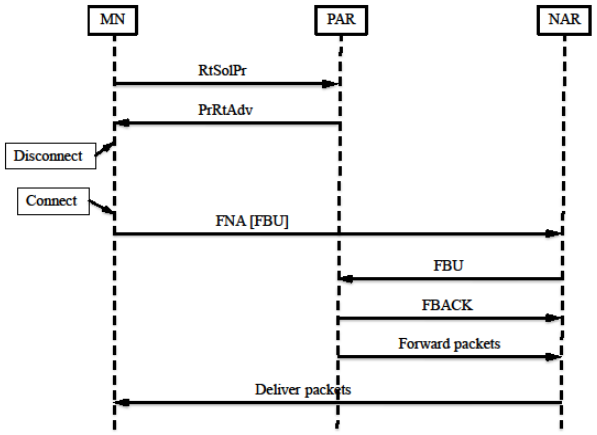

Fig.5. Message flow diagram of reactive FMIPv6

Protocol Overview:

The signaling call flow for PMIPv6 is described as follows:

a) The signaling call flow starts when the mobile node enters the Proxy Mobile IPv6 domain. The Router Solicitation message from the mobile node may arrive at any time after the mobile node's attachment and has no strict ordering relation with the other messages in the call flow. For updating the local mobility anchor about the current location of the mobile node, the mobile access gateway sends a Proxy Binding Update message to the mobile node's local mobility anchor. Upon accepting this Proxy Binding Update message, the local mobility anchor sends a Proxy Binding Acknowledgement message including the mobile node's home network prefix(es). It also creates the Binding

Cache entry and sets up its endpoint of the bi-directional tunnel to the mobile access gateway.

The mobile access gateway on receiving the Proxy Binding Acknowledgement message sets up its endpoint of the bi-directional tunnel to the local mobility anchor and also sets up the forwarding for the mobile node's traffic. At this point, the mobile access gateway has all the required information for emulating the mobile node's home link. It sends Router Advertisement messages to the mobile node on the access link advertising the mobile node's home network prefix(es) as the hosted on-link prefix(es). The timing diagram is shown in Fig. 6. The mobile node, on receiving these Router Advertisement messages on the access link, attempts to configure its interface using either stateful or stateless address configuration modes, based on the modes that are permitted on that access link as indicated in Router Advertisement messages. At the end of a successful address configuration procedure, the mobile node has one or more addresses from its home network prefix(es).

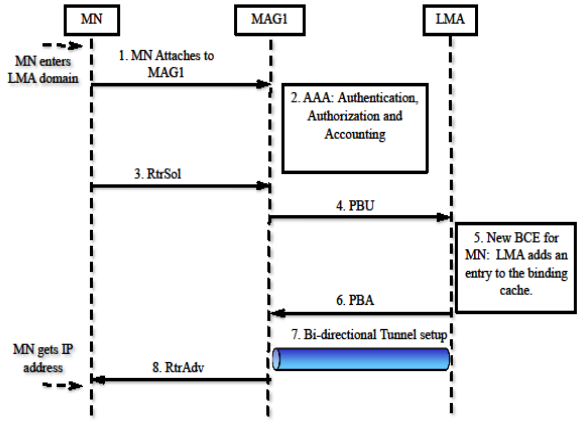

Fig.6. MN attachment: signal flow in Proxy MIPv6

b) After obtaining the initial address configuration in the Proxy Mobile IPv6 domain, if the mobile node changes its point of attachment, the mobile access gateway on the previous link will detect the mobile node's detachment from the link. It will signal the local mobility anchor and will remove the binding and routing state for that mobile node. The local mobility anchor, upon receiving this request, will identify the corresponding mobility session for which the request was received, and accepts the request after which it waits for a certain amount of time to allow the mobile access gateway on the new link to update the binding. However, if it does not receive any Proxy Binding Update message within the given amount of time, it will delete the binding cache entry. The mobile access gateway on the new access link, upon detecting the mobile node on its access link, will signal the local mobility anchor to update the binding state. After completion of the signaling, the serving mobile access gateway will send the Router Advertisements containing the mobile node's home network prefix(es), and this will ensure the mobile node will not detect any change with respect to the layer-3 attachment of its interface. The timing diagram for PMIPv6 handover is shown in Fig. 7.

E. Fast Handovers for Proxy Mobile IPv6

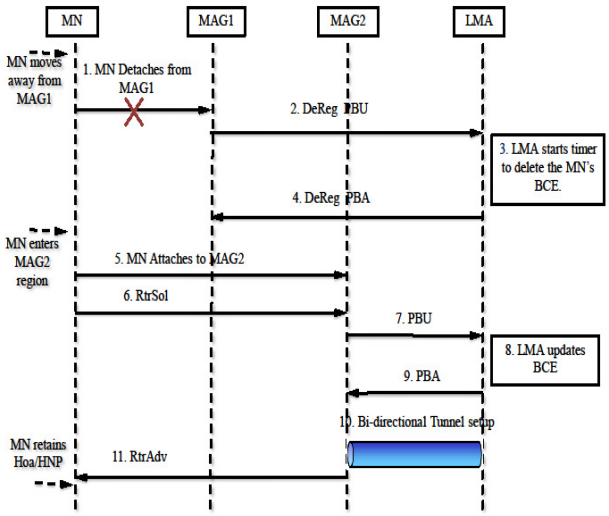

Fig.7. MN handoff: signal flow in Proxy MIPv6

The handover sequence defined by PMIPv6 is not optimized for fast handovers. Packets cannot be delivered to and from the mobile node during handover and the handover delay essentially leads to packet loss thus degrading the quality of service. In PMIPv6 the MAG is responsible for detecting the mobile node's movements to and from the access link and for initiating binding registrations to the mobile node's local mobility anchor. If the MAGs can be informed of the detachment and/or attachment of the mobile node in a timely manner via, e.g., lower-layer signaling, it will become possible to optimize the handover procedure, which involves establishing a connection on the new link and signaling between mobility agents, compared to the baseline specification of PMIPv6. In order to further improve the performance during the handover, Proxy-Based FMIPv6 specifies a bidirectional tunnel between the Previous MAG (PMAG) and the New MAG (NMAG) to tunnel packets meant for the mobile node which is referred to as Fast Handovers for Proxy Mobile IPv6 (FPMIPv6) [8], [9].

The Terminologies used in FPMIPv6 are:

1) AN: Access Network. A network composed of link-layer access devices, such as, access points or base stations providing access to a Mobile Access Gateway (MAG) connected to it.
2) P-AN: Previous Access Network. The access network to which the Mobile Node (MN) is attached before handover.
3) N-AN: New Access Network. The access network to which the Mobile Node (MN) is attached after handover.

4) PMAG: Previous Mobile Access Gateway. The MAG that manages mobility-related signaling for the mobile node before handover.
5) NMAG: New Mobile Access Gateway. The MAG that manages mobility-related signaling for the mobile node after handover.

Protocol Overview:
FPMIPv6 defines a fast handover to be used in PMIPv6. It defines two modes:

1) Predictive PMIPv6:
(PMAG initiates handover before MN establishes connectivity with the new access network) A bidirectional tunnel between the PMAG (PAR) and NMAG (NAR) is established prior to the mobile node's attachment to the NMAG.
The sequence of events for the predictive fast handover is illustrated in Fig. 8. The detailed descriptions are as follows:

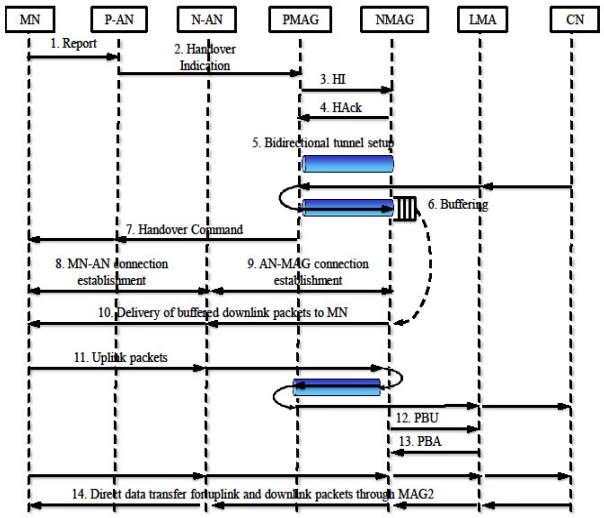

Fig.8. Signal flow in predictive FPMIPv6

a) The mobile node detects that a handover is imminent and reports its identifier (MN ID) and the New Access Point Identifier (New AP ID) to which the mobile node is most likely to move. In some cases, the previous access network (P-AN) will determine the New AP ID for the mobile node. The previous access network, to which the mobile node is currently attached, indicates the handover of the mobile node to the previous mobile access gateway (PMAG), with the MN ID and New AP ID. The PMAG derives the new mobile access gateway (NMAG) from the New AP ID. The PMAG then sends the Handover Initiate (HI) message to the NMAG. The NMAG sends the Handover Acknowledge (HAck) message back to the PMAG with the 'P' flag set.
b) If the 'F' flag is set in the HI message, a bidirectional tunnel is established between the PMAG and NMAG, and packets destined for the mobile node are forwarded from the PMAG to the NMAG over this tunnel. After decapsulation, those packets may be buffered at the NMAG. If the connection between the new access network and NMAG has already been established, those packets may be forwarded towards the new access network, which then becomes responsible for them. When handover is ready on the network side, the mobile node is triggered to perform handover to the new access network.
c) The mobile node establishes connection with the new access network. The NMAG starts to forward packets destined for the mobile node via the new access network. The uplink packets from the mobile node are sent to the NMAG via the new access network, and the NMAG forwards them to the PMAG. The PMAG then sends the packets to the local mobility anchor that is currently serving the mobile node. The NMAG sends the Proxy Binding Update (PBU) to the local mobility anchor. The local mobility anchor sends back the Proxy Binding Acknowledgment (PBA) to the NMAG. From this time on, the packets to/from the mobile node go through the NMAG instead of the PMAG.

2) Reactive PMIPv6:
(NMAG initiates handover after MN has established connectivity with the new access network) The tunnel establishment takes place after the mobile node attaches to the NMAG. In order to alleviate the packet loss during a mobile node's handover, the downlink packets for the mobile node need to be buffered either at the PMAG or NMAG, depending on when the packet forwarding is performed. It is hence required that all MAGs have the capability and enough resources to buffer packets for the mobile nodes accommodated by them.
The detailed signal flow is shown in Fig. 9 and descriptions are as follows:

a) The mobile node undergoes handover from the previous access network to the new access network. The mobile node establishes a connection with the new access network, which triggers the establishment of the connection between the new access network and NMAG. The MN ID is transferred to the NMAG at this step. The AP-ID on the old link, which will be provided by either the mobile node or the new access network, is also transferred to the NMAG to help identify the PMAG on the new link. The NMAG sends the HI message to the PMAG. The PMAG sends the Hack message back to the NMAG.
b) If the 'F' flag in the HI message is set, a bidirectional tunnel is established between the PMAG and NMAG, and packets destined for the mobile node are forwarded from the PMAG to the NMAG over this tunnel. After decapsulation, those packets are delivered to the mobile node via the new access network. The uplink packets from the mobile node are sent to the NMAG via the new access network, and the NMAG forwards them to the PMAG. The previous MAG then sends the packets to the local mobility anchor that is currently serving the mobile node. The NMAG sends the Proxy Binding Update (PBU) to the local mobility anchor. The local mobility anchor sends back the Proxy Binding

Acknowledgment (PBA) to the NMAG. From this time on, the packets to/from the mobile node go through the NMAG instead of the PMAG.

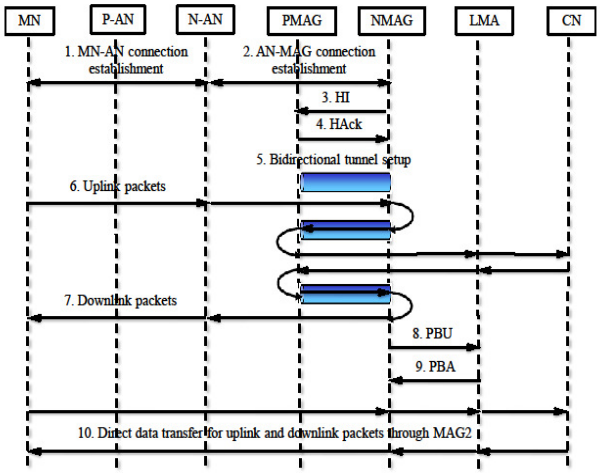

Fig.9. Signal flow in reactive FPMIPv6

III. PERFORMANCE ANALYSIS

The following performance metrics are used to evaluate the performance of Mobile IPv6 protocols [10], [11], [12].

1) Handover latency: It is the time interval during which an MN cannot send or receive any packets while it performs its handover between different access networks.
2) Handover blocking probability: It is the probability which an MN cannot complete its handover when the network residence time is less than the handover latency.
3) Packet loss: It is the sum of all lost packets destined for an MN during the MN's handover.

1) Handover latency:

a) Wireless link condition: The wireless link condition, i.e., FER over the wireless link, largely affects the handover performance of all mobility management protocols. With this point in view, the network-based mobility management protocols, such as, PMIPv6 and FPMIPv6 have an advantage owing to removed mobility signaling from the MN.

b) DAD latency: MIPv6 and HMIPv6 show poor handover performance. This phenomenon is caused by the DAD process, which counts for a large portion of handover latency. Since the DAD process is performed over a wireless link, in a poor wireless link condition, it badly influences the handover performance of MIPv6 and HMIPv6.

c) Network topology: As mobility signaling, i.e., BU/BAck, LBU/LBAck, PBU/PBAck, HI/HAck, etc., is sent along the network topology, the handover performance is affected by the network topology configuration. For instance, the handover performance of fast handover protocols, such as, FMIPv6 and FPMIPv6 is largely affected by the number of hops between the relevant ARs/MAGs.

2) Handover Blocking Probability:

Utilizing Layer 2 information: In order to improve the handover performance, Layer 2 information should be utilized. Predictive FMIPv6 and FPMIPv6 outperform the other mobility management protocols because those protocols allow an MN to prepare its handover before the MN performs its actual handover to the new access network. The reduced handover latency also results in the reduced handover blocking probability.

3) Packet Loss:

Employing buffering management: In order to prevent packet loss during the handover, any buffering mechanism should be employed. Only fast handover protocols, such as, FMIPv6 and FPMIPv6 prevent the loss the loss of data packets sent from the CN.

IV. CONCLUSION

In this literature, the existing IPv6 mobility management protocols developed by the IETF have been analyzed and compared in terms of handover latency, handover blocking probability, and packet loss. Security issues are not discussed in this comparative performance analysis of Mobile IP and MIPv6 protocols. We can also evaluate the performance of these mobility protocols in terms of other performance parameters, such as, the delay between MN and CN, movement detection delay, throughput of TCP connection, user-perceived video stream quality delay, etc. Besides we can combine different protocols and evaluate their performance. The conducted analysis results in this literature can be used to identify each mobility management protocol's characteristics and performance indicators which will greatly facilitate decision making in development for a new mobility management protocol. The IETF has recently opened the distributed mobility management (DMM) working group aiming at distributing mobile Internet traffic in an optimal way while not relying on centrally deployed mobility anchors, such as, HA, MAP, and LMA.

REFERENCES

[1] D. Johnson, C. Perkins, and J. Arkko, "Mobility support in IPv6," IETF RFC **3775**, Jun **2004**.
[2] V. Vassiliou, Z. Zinonos, "An Analysis of the Handover Latency Components in Mobile IPv6", Journal of Internet Engineering, vol. **3**, no**. 1**, Dec **2009**.
[3] Soliman, C. Castelluccia, K. ElMalki, and L. Bellier, "Hierarchical mobile ipv6 mobility management HMIPv6," IETF RFC **4140**, Aug **2005**.
[4] M.H. Habaebi, "Macro/micro-mobility fast handover in hierarchical mobile IPv6", Computer Communications, Volume **29**, Issue **11**, **26** July **2006**, Page **2168.**
[5] R. Koodli, "Fast handovers for mobile IPv6," IETF RFC 4068, Jun **2009**.
[6] M.Torrent-Moreno. "A Performance Study of Fast Handovers for Mobile IPv6", IEEE International Conference on Local Computer Networks, **2003**.

[7] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy mobile IPv6," IETF RFC 5213, Aug **2008**.
[8] H. Yokota, K. Chowdhury, R. Koodli, B. Patil, and F. Xia, "Fast handovers for proxy mobile IPv6," IETF RFC 5949, Sep **2010**.
[9] G. Heijenk, M.S. Bargh, J. Laganier, and A.R. Prasad "Reducing Handover Latency in Future IP-based Wireless Networks: Fast Proxy Mobile IPv6," In Second ERCIM workshop on eMobility, **30** May **2008**.
[10] C. Makaya and S. Pierre, "An Analytical Framework for Performance Evaluation of IPv6-Based Mobility Management Protocols," *IEEE Trans. Wireless Comm.,* vol. **7**, no. **3**, pp. **972-983**, Mar. **2008**.
[11] K. S. Kong, W. Lee, Y. H. Han, and M. K. Shin, "Handover Latency Analysis of a Network-Based Localized Mobility Management Protocol," IEEE International Conference on Communication, Beijing, China, pp. **5838-5843, 2008**.
[12] J. Lee, J. Bonnin, I. You, and T. Chung, "Comparative handover performance analysis of IPv6 mobility management protocols," IEEE Transactions on Industrial Electronics, vol. **60**, no**. 3**, pp. **1077–1088**, Mar **2013.**

AUTHORS PROFILE

Fatema Tuz Zohra received her B.Sc. degree in Computer Science and Engineering (CSE) from Military Institute of Science and Technology (MIST), Dhaka, Bangladesh, in 2010. At present, she is conducting her M.Sc. program in CSE at Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh. She is currently a faculty member of CSE department, Bangladesh University of Business and Technology (BUBT), Dhaka, Bangladesh.

Samiul Azam received his B.Sc. degree in Computer Science and Engineering (CSE) from Military Institute of Science and Technology (MIST), Dhaka, Bangladesh, in 2010. At present, he is conducting his M.Sc. program in CSE at Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh. He is currently a faculty member of CSE department, United International University (UIU), Dhaka, Bangladesh.

Md. Mahbubur Rahman received his B.Sc. engineering degree in Computer Science and Engineering (CSE) from Patuakhali Science and Technology University (PSTU), Bangladesh, in 2011. He is now working toward his M.Sc. engineering degree in CSE at Bangladesh University of Engineering and Technology (BUET), Bangladesh and working as a lecturer in CSE at one of the top most private universities in Bangladesh named Bangladesh University of Business and Technology (BUBT). His research interests are data mining, search engine optimization, biometric system, network Security.