

An Evolution of Protocols in Mobile Networks

^{1,2}Sakshi Rajput

¹Dept. of Electronics and Communication, Maharaja Surajmal Institute of Tech.,
GGSIU, Janakpuri, New Delhi, India

²Dept. of Electronics and Communication, UTU, Prem Nagar Sudhowala,
Dehradun, Uttarakhand, India

Abstract

Internet Network contains different yet reliable Protocol for Internet Routing. Recently there has been a substantial increase in the number of Internet Routing Protocols. However, the performance of these different types of protocols is not up to the mark, from this survey paper different types of protocols have been investigated including MIPv6, FMIPv6, HMIPv6, FHMIPv6, PMIPv6, and DHMIPv6 are investigated in the DMM environment. The effective solution for mobility management mechanism is needed for the end users while changing their location. For supporting mobility, Mobility management protocols have been introduced was evolved from Host-based approach to Network based approach. In network-based protocols, host was shielded by transferring the mobility – related signaling to the network entities whereas host-based protocols the mobility-related signaling is involved with MN. The purpose of the mobility protocol is to enable network applications to operate continuously with the good quality of services for both wireless networks.

Keywords

IPv4, IPv6, MIPv4, MIPv6, FMIPv6, HMIPv6, PMIPv6, DHMIPv6, FHMIPv6, DHMIPv6, LTE and DMM

I. Introduction

The wireless connection technology is being increasingly utilized by the Internet users. Users are increasing day by day and connecting wireless devices to the internet, but increasing number of users are leading to disconnection and congestion. Hence, many researches have been conducted to resolve the disconnection and congestion over the wireless communication [2]. Therefore, The IETF working group on internet protocol had introduced several Internet protocols to reduce issues like latency and packet losses.

In 1993, Internet Engineering Task Force (IETF) introduced and released the MIPv4 (Mobile Internet Protocol Version 4) to provide mobility management. With the release of these protocols, IETF also introduced some of the terms such as home agent (HA), foreign agent (FA), mobile node (MN), visitor list (VL), care of address (CoA), mobility binding table (MBT) and corresponding node (CN). To ensure accessibility to mobile node HA is responsible to provide internet in the same domain and keep their mobility information in MBT. FA is placed in foreign domain to assign temporary address which is based on the current location of the mobile node and stores the information of mobile node in visitor list and also informs the home agent about the mobile nodes movement. Then home agent updates the information of MN in MBT. The corresponding node (CN) which is a mobile host either in static or mobile nodes communicates with MN. Therefore MIPv6 [21] is the next approach proposed by the IETF. MIPv6 offers efficient routing, neighbour discovery, auto-configuration service, built-in security efficient, extension headers and infinite address space which are not found in MIPv4. However, a MIPv6 protocol does not support critical real-time application due to

signalling overhead, handover latency and packet ratio loss.

Later several more protocol are designed and released by the IETF such as such as Fast Handover MIPv6 (FMIPv6 [22], Fast Handover for Hierarchical (FHMIPv6) [20] and Hierarchical MIPv6 (HMIPv6) [21] to overcome signalling overhead, handover latency and packet ratio loss problems. Access point (AP) and access router (AR) are used by MN to relieve any signalling during handover in order to minimize handover latency. Efficient mobility and communication support which is major issue in host-based protocols are improved with this approach.

Furthermore, a new protocol namely, PMIPv6 (proxy mobileIPv6) [14] was released. In this protocol two terms are introduced such as MAG (mobility access gateway) and LMA (local mobility anchor). LMA is used to make the mobile node reachable when it moves between sub-networks in local domain while MAG is used to registers LMA with mobile node and it authenticates MN with AAA (authentication, authorization, and accounting) signalling. This protocol ensures that signalling messages are exchanged between MN, CN and HA which produce very high level of tunnelling message. The main objective is to keep all mobile hosts in a network which can be accessible through their permanent internet protocol address. This protocol is a derivative of MIPv6 in terms of use of concept of home node functionality. However, it has same limitation as of MIPv6 which are packet loss, handover latency and signalling overhead.

Another protocol proposed by IETF is DHMIPv6 [18]. This protocol works on mono or two-layer MAP. It divides mobile node in two parts. The first one is micro mobility which is controlled by MIPv6 and another is micro mobility which is controlled by HMIPv6. By this approach, it resolves single point load failure which is very common in large traffic using its monolayer structure.

To surmount the limitations of the global mobility management, a new concept has been introduced known as distributed and dynamic mobility management system. It has three key concepts. The first concept is to place mobile anchors as close as possible to the MN (mobile nodes). According to second concept, the data and control planes are distributed among network entities which are situated on the edge of the network that needs to be accessed. And the last concept is based on the principle that, the mobile nodes are provided with the dynamic mobility support when it really needed to the services.

The above discussed concepts of DMM [3] are expected to be an effective solution in terms of Internet protocol mobility management. However, to handle vast number of data traffic and devices, the internet protocol multicast technique could be considered as a valuable solution from service point of view. In terms of overall resources consumption (like Bandwidth, network load, server load, deployment cost). The internet protocol multicast can provide significant benefits when compared to single cast to deliver the data traffic, particularly video and audio traffic [4] [5].

In this paper, we have first discussed the basics of IPv4 and IPv6 which is followed by operation, advantages and disadvantages of

mobility management protocols. The special focus is given on the comparison of mobility protocols.

1. IPV4

Internet Protocol Version 4 (IPv4) is the most-widely used network in the world. The Addressing space (Source and destination) of IPv4 is 4 bytes or 32 bits of length Size of address. The length of IP header is 20–60 bytes which depends on internet protocol options which are Self-Configuration, Manual or dynamic. These IP configurations Broadcast Technique are used to transfer the address to all nodes on its own networks. It works on the TTL (Time to live) mechanism which is used to determine the lifetime of datagram on the network. IPv4 is a wireless protocol used in switched-packet layer networks. Fragmentation is applied by host (destination) and router and use offset map addresses fields and flag for fragmentation ID. To work on node addresses recorded in Dynamic Network Services (DNS) for mapping node names securely an IP security (IPsec) header is used as an optionally service for protecting the packets. Furthermore, IPv4 does not support packet identification and use broadcast to transfer the IP address to all nodes on its networks which means it only cast one address at one time. To overcome these problems IPv6 had introduced.

2. IPV6

IPv6 is the successor of IPv4, which was developed by IETF (Internet Engineering Task Force). Despite of the fact that IPv4 is used Worldwide, IPv6 deals with the most important problem of all time – “Decreasing Address space”. IPv6 improved the declination in the address spaces which was there in IPv4 in the last decade. Features that attract the world are – Larger Address Space, Stateless and State-full Address Configuration, Built-in Integrated Security (IPsec), Modern Protocols, Extensibility, Quality of Service (QoS) for neighboring Node. This Internet Protocol has the ability to extend a system and the ability to make further growth in future with the easy implementation.

In IPv4, the datagram is used whereas in IPv6 it is known as Packets regardless of its meaning with different format. In IPv6, Host node will never forward the packets unless the packet is not addressed to the same (Host). In that case, the Router acts as a Node and forwards packets which are not called for it (Router). The demand for the address Spaces have been increased in last decade only which results into increase in the number of IP Hosts. Multicast Ad Technique is known as one to many communications over an IP infrastructure in a network. To map Node names, it uses accounting (AAA) in DNS (Domain Name System) and authentication authorization. The actual deployment is still a critical issue as it will take much time to implement this protocol in a proper manner. The 128 Bits are represented in 8 groups each of 16 Bit with 4 Hexadecimal digits separated by a colon.

3. MIPv4

The MIPv4 is a mobile internet protocol version 4. It was also designed and produced by IEFT for mobile users. This protocol is developed to connect the node to the network without any interruption. The functioning of the various entities involved in MIPv4 is depicted in Fig.1. The role of home agent (HA) is to ensure that local MN connects continuously to the correspondent node (CN) network even if the mobile node is moving from one point to another. It can be done by giving information of MN to CN from MN’s own mobility binding table (MBT). The CN, which is located on the global internet trying to communicate to

MN. Foreign agent (FA) is assigned to another network in which MN moves and FA assigns care of address (CoA) to MN, keeping information registered in its visitors list (VL). When datagrams arrive on HA, these are received by MN through routing protocol, then it will go under HA (fetched on MBT), to check if it’s in domain or not. If it is not in domain, then CoA is used by the HA to enclose the datagrams and send them directly to FA. Else, datagrams are received by MN directly through routing protocol. Moreover, FA fetches CoA to update it VL. Then foreign agent reveals and forwards the received packet to the mobile node. On other side, the FA forwards the datagram to the CN which is coming from the other CN using a tunnel between HA and FA.

Despite these benefits, MIPv4 suffers from some limitations such as triangular protocol or long communication routing protocol which occurs on HA by receiving and sending the data packets. So, it requires some extra time to send data packets to their desired destination. Triangular routing makes the network extra loaded. New visited network is restricted from informing about MN’s movement to old networks which results in loss of packets during handover process.

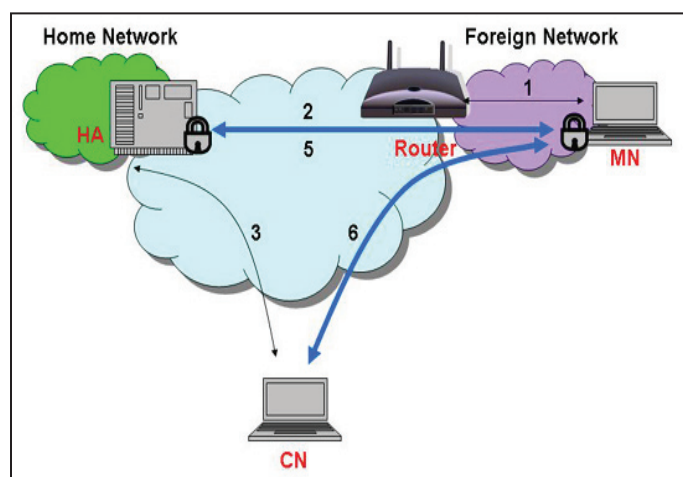


Fig.1: Operation of MIPv4

4. MIPv6

This protocol is an enhanced version of MIPv4. MIPv4 operates in the same address size while moving across the networks. In MIPv6, it doesn’t need any outside foreign agent to use MIPv6. In MIPv6, the nodes can be accessed without any system up gradation. The auto-configuration feature of MIPv6 removes the complexity in assigning address between MN and CN. It was developed to remove the issue found in MIPv4 protocol such as long routing protocol issue that arises because HA and FA are dependent on each other while transferring the datagram between mobile node and correspondent node. This is because of the fixed home of address (HoA) that is given by HA to MN in order to maintain the connection between MN and its CN. But, in MIPv6 protocol a MN is allowed to wander within its domain range without losing any connection with the CN. The MN moves to a newly visited network that enables MN access to care of address (CoA) and MN will no longer be accessible by the HoA. The Operation of MIPv6 is explained with the help of Fig.2. In MIPv6, all the flying packets are interrupted by the home agent to MN’s HoA and redirected to the care of address of the current mobile node. The MIPv6 solves various limitations such as, message query response can be exchanged between MN and CN, direct and secure connection can be established, long routing issue can be minimised and performance of the network can be enhanced. All

this is done by the route optimization scheme introduced in MIPv6 [6]. This scheme provides reliability, security and minimization of the network load to the network. Along with these benefits, MIPv6 protocol lacks of some factors too which, includes intense signalling, packet loss and long handover latency. These factors may occur due to the movement of MN to a new sub-domain because its CoA is updated to it's HA and MN's CN. Moreover, IPv6 tunnel cause extra overhead, which requires an additional IPv6 header [7]. To overcome these weaknesses, more enhanced protocol like HMIPv6 [10] and FMIPv6 [9] are introduced.

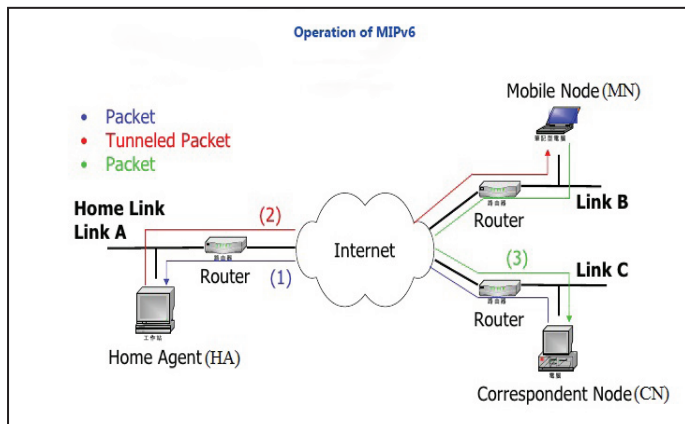


Fig. 2: Operation of MIPv6

5. FMIPv6

This is fast handover, for MIPv6. Its main objective is to support the adaptability of the Mobile Network. The access router (AR), keeps the MN in the mobile network to make it continually attainable even when they are in movement. FMIPv6 [9] provides uninterrupted services when MN is in motion. It also minimizes the time required for MN to roam among sub-entities through the handover affiliated with MIPv6. In FMIPv6, there are three signaling messages. These messages involve anticipation phases which are RtSolPr (Router Solicitation for Proxy Advertisement), PrRtAdv (Proxy Router Advertisement) and FBU (fast binding update). The RtSolPr and PrRtAdv messages are used when mobile node can capture NCoA (New care of address) without closing the session to current link and discover NAP. This process eliminates connectivity latency. Packet losses due to handover process and latency are minimized using these signaling methods. Furthermore, FMIPv6 carry out the handover signalling burden through network entities, alleviation of the MN signal is carried out in mobile signalling. These entities consist of HA, NAR (New Access Point/Router) and PAR (Previous Access Point/Router) which help in performing two types of handover operations called as Predictive Fast Handover and Reactive Fast Handover. Reactive fast handover allows MN (mobile node) to send fast binding update (FBU) after it is attached to new access point. Predictive fast handover allows MN to send FBU before it is attached to NAR. The mobile node (MN) sets up a predictive handover with NAR whereas the NAR sets up the reactive handover with Previous Access Router (PAR). This leads the formation of a bidirectional tunnel between NAR and PAR, resulting into reduction of noteworthy time in handover process. Finally, a bidirectional tunnel has been developed in the middle of NAR and PAR after the handover resolution between NAR and MN. The architecture of FMIPv6 is depicted in Fig.3. The operation of FMIPv6 begins when MN sends RtSolPr to previous access router (PAR) which request for potential handover. The RtSolPr message is scanned through network subnet by PAR containing access point and send it back to mobile node. Then

mobile node requests PAR to send HI (handover initiate) to new access router which obtains NCoA the arriving packet to PCoA (previous care of address) can be tunneled to (NCoA). Duplicate address detection (DAD) is performed by NAR to return the HACK (Handover Acknowledgement) back to NAR to MN. In the final step, fast neighbor advertisement (FNA) is sent by mobile node to the NAR. This step is to ensure that MN is in NAR subnet and MN receives the FNA-ACK (Fast Neighbor Advertisement Acknowledgement). In addition, a buffering technique is used in NAR and PAR just to minimize the packet/data loss throughout the handover operation, and then these packets are redirected to MN. Regardless of all these benefits of FMIPv6 over MIPv6, the FMIPv6 has some limitations such as recognition of the packets is caused by redirecting the packets using multipath. The two techniques, buffering and packet tunnelling reduce the packet/data loss throughout MN's movement, especially for constant bitrate 'CBR' services. Hence, during operations, some extra processing is needed which eventually increase the overall load on network in between PAR and NAR, which actually arises by the successive tunnelling and de-tunnelling of the packets. The availability of the trigger and appropriate decision making are two key characteristics, which determines the reliability and accuracy in tunnelling operations between PAR and NAR. The main limitations of the FMIPv6 are High handover latency and overload signalling [11].

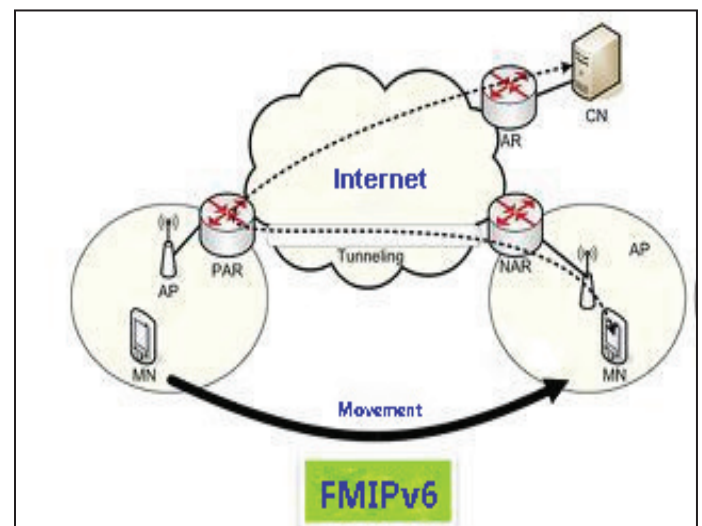


Fig. 3: Architecture of FMIPv6

F. HMIPv6

This is a hierarchical mobile IPv6 protocol proposed by [10]. This protocol ensures the mobility signalling message exchange between HA, MN and CN which causes high level of tunnelling. The objective is to make mobile network available to the host. It also maintains the ongoing session within the MIPv6 domain. It is an extension of MIPv6 protocol which introduces new mobile node known as Mobility Anchor Point (MAP). It is employed to reduce the Handover latency. HMIPv6 implicates 3 phases such as MAP Discovery, MAP Registration and Packet Forwarding. A Bidirectional tunnel is built between mobility anchor point and mobile node, the Packets are sent by the mobile node to the MAP via the tunnel. These packets are sent from the MN's RCoA to the MN's LCoA which in between intercepted by MAP. The Packet Loss per handoff decreases as the Inter Packet Arrival Time (ms) increases. The Number of Corresponding Nodes (CN) gradually increases with signalling load. For the host-based protocol, devices are highly limited in terms of memory size,

power and processors. For this reason, new entity name mobility anchor point (MAP) is added in the Protocol's architecture. There are two CoA associated with MN which are On-Link Care-of-Address (LCoA) and Regional Care-of-Address (RCoA). The RCoA is used for making the MNs accessible in which MAP roams with MN whereas in LCoA, MNs are accessible when MAP is inside the visited network. The RCoA is assigned by MAP to MN whereas (LCoA) is configured on MN interface, the Local Binding Update (LBU) is sent via MN to the MAP in order to bind RCoA with LCoA. This MAP is addressed by RCoA which can support access routers (AR). These ARs are supported to determine the coverage area of MAP which can announce itself using broadcast mechanism. The Architecture of HMIPv6 is shown in Fig. 4.

The handover process is performed by the MN to disconnect from PAR and connect to NAR. MN has to send a BU message through CN and HA to connect them with new CoA. This message goes through MAP and reaches to CN or HA. Then, this message is sent to the MN via CN. In case, the MAP is located far away then there will be a time delay to deliver the BU message in both directions HA or CN to MAP. Due to this limitation, it is logical to have provisional HA with MAP. So, when MN roams in same area with MAP domain, then MN's address is in LCoA. The MN can employ multiple MAPs and use RCoA as Source Address for momentary communication. By employing the RCoA MN can conceal itself. If MAP is topologically far then the inter-map handover may take longer time than expected. This protocol also suffers from signalling overload, high packet loss, and high handover delay, which leads to degradation of (Qos) Quality of service. To overcome these limitations a new protocol has been introduced which is explained in the next section.

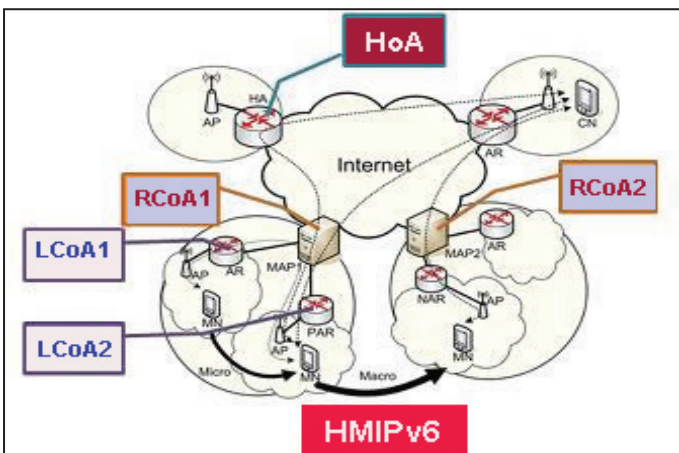


Fig. 4: Fast Handover in HMIPv6

6. DHMIPv6

Dynamic Hierarchical Mobile Internet protocol version 6 is proposed by [18]. In this protocol, different hierarchies are set up dynamically to minimize total cost of mobile nodes according to their movement characteristics. At the time of handover monolayer or two-layer MAP (mobility anchor point) is selected by the mobile nodes. DHMIPv6 separates the MN (mobile node) into two parts micro mobility and micro -mobility. In the case of macro-mobility MN moves out of the new domain and mobility is controlled by MIPv6 management. In micro -mobility, mobile node moves in a particular hierarchical domain and mobility is controlled by HMIPv6 to reduce the number of signals which are generated by HA and CN. The MAP is a substitute of HA in which each domain of network hides from the outer domain of the user mobility. In the next step, MAP receives BU (binding updates) directly from the

mobile node in a specific region instead of CN or HA but only when Mobile node stays in some specific region. The signaling overhead is reduced because mobile mode's exact position is hidden from the outer region. When MN moves out of this specific region then it has to register its position to CN and HA.

As shown in fig.5. MAP1 domain is occupied by the MN1 domain and then passes through MN2 domain and flowed by MN3 domain and finally reach MN4 domain. When MAP1 is occupied by MN1 it performs home registration and obtains (RCoA) and (LCoA). Packet routing and location management is performed by the MN1 with HMIPv6. When MN1 enters the MAP2, it performs registration to MAP1 and not to HA which in return reduces the registration cost. It registers to MAP1 instead. With RCoA collected in MAP as online-CoA domain. In DHMIPv6, it reduces the total home registrations, and also resolves single point and load of failure problems. It performs very well in large traffic using its monolayer structure. The packet delivering cost is reduced for data forwarding operation between more than one MAPs.

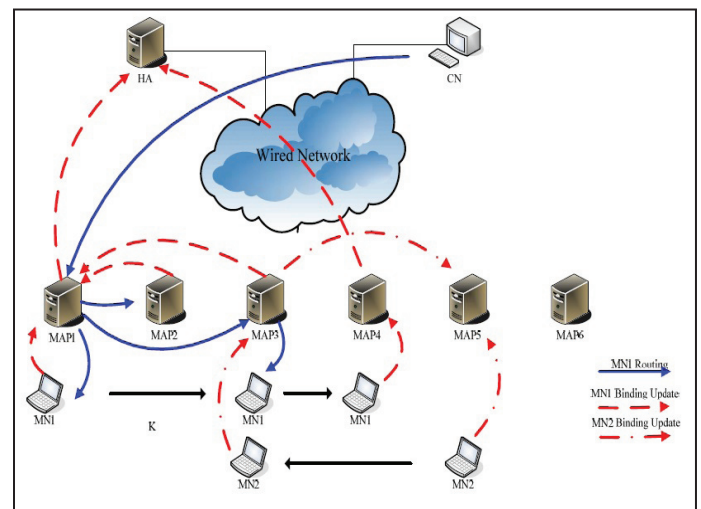


Fig. 5: Packet Routing in DHMIPv6

7. FHMIPv6

This protocol is a combination of Fast Hierarchical Mobile Internet Protocol version 6 (FMIPv6) and Hierarchical Mobile Internet Protocol version 6 (HMIPv6). This combination gives combine advantages of both protocols (FMIP and HMIP) which results in the Enhanced Mobile Internet Protocol (MIP). This Protocol offers reduced packet losses, decreases handover delays and better throughput.

The operation of FHMIPv6 starts with L2 (Layer 2) handover in which Mobile Network sends Router Solicitation for Proxy Advertisement (RtSolPr) message to MAP which contains information of NAR. After that MAP forwards Proxy Router Advertisement (PrRtAdv) message to MN, MN has the information about the New Link Care of Address (LCoA) which is going to be used in NAR region. Fast Binding Update is sent out from MN, after FBU is received, Handover Initiate (HI) is out from MAP which results in enclosing IP address of NAR. The NAR sets up the host route and reply with handover Acknowledge (HACK). A Bi-Directional tunnel is established. The Fast Binding Acknowledgement (FBA) is sent towards MN, the established tunnel will have to forward data/packets which is tunnelled through MAP to MN which directly send out Fast Neighbour Advertisement (FNA). FNA-ACK is returned by NAR to MN. The MAP receives Local Binding Update (LBU) from MN Duplicate

Address Detection (DAD) is performed on HA and updates binding cache. In return the MAP forwards a Binding Acknowledgement to MN. The BU is sent to HA via MN which activates CN. Then CN acts as a destination address, when it is linked with NCoA as source address. By creating such a hybrid connection, the data can reach in less time at particular direction. The network diagram of FHMIPv6 is shown in Fig. 6.

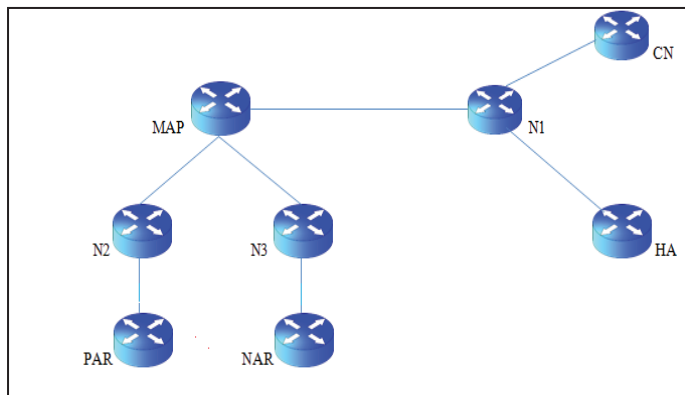


Fig. 6: Flow diagram of FHMIPv6

8. PMIPv6

Host-based protocols have their limitations and drawbacks, which are overcome by proxy-based protocols. PMIPv6 [14], SMIPv6 [23-25] and CSMIPv6 [26], are proxy-based protocols introduced by IETF.

In an ongoing handoff process of proxy-based protocols, mobility management relieves sensor nodes which results in reduction of handoff registration, signalling costs, signalling overhead etc. PMIPv6 performs in the network layer [14] to fix the network management related mobility challenges. In proxy-based protocols, MNs are independent of any mobility associated signalling and proxy mobility functions take the responsibility of all signals related to mobility, whereas in MIPv6, MN takes the entire burden.

PMIPv6 is an enhanced version of MIPv6 with improved signalling. The MN runs the standard protocol stack. The objective of PMIPv6 is to propose mobility to IP devices without their participation. As discussed earlier, MN is independent and does not take part in mobility related signalling, this is because PMIPv6 protocol has added local mobility anchor (LMA) and mobile access gateway (MAG) [14]. The main role of the LMA is to behave as a home agent of MN to keep in touch with ongoing sessions even if it roams between the sub-domains. MAG is used to support connectivity of networks in the PMIPv6. Whenever MN connects the MAG and PMIPv6 network, the MN assigns a home network prefix (HNP) to every mobile node with the help of MN prefix address nodes as referred in [14].

In a PMIPv6 operation, when MN enters in PMIPv6 domain, MAG provides an access link to connect to node. The MAG performs a security check on MN to identify if it is authorised to use the mobility management related services. Then MAG performs all the MN's mobility signalling and sends a proxy update to LMA with MN's authorization confirmation and its own address. After acknowledging this request, LMA assigns a prefix address to the MN. The LMA sends back a proxy acknowledgement to the MAG containing the MN's prefix address. And it creates a bidirectional tunnel between MAG and LMA. LMA receives the traffic associated with the home network prefix. The MAG has a special policy configured for data traffic that sent from one access link and sent to another access link of MAG, which operates the

traffic locally and avoid traffic forwarding by LMA. Prefix addresses are used for mobile nodes to make it feel that network domain is in the home network and then it gets HoA to access the network. The operation of PMIPv6 is shown in Fig.7.

PMIPv6 proposes two advantages in its performance as compared to its earlier version (MIPv6). The LMA being a local entity of the network takes lesser time to receive the signalling than home agent. Moreover, in MIPv6 the tunnel is terminated at MN, but to manage the traffic the tunnel is required to halt in the MAG. Despite all of the benefits like reduction in time required for signalling and decreasing the handover delay, it has its drawbacks due to long communication routing protocol between CN, LMA and MN. This reduces the QoS. Furthermore, there could be a problem for Internet of Things (IoT) equipment, which uses driver's application [16-17].

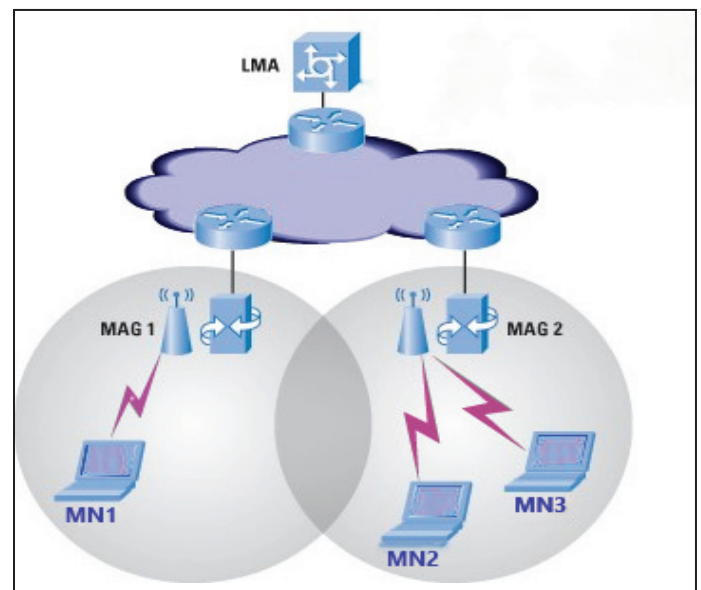


Fig. 7: Operation of PMIPv6

II. Research Gap

These protocols discussed in above section are compared in Table 1 on the basis of certain characteristics which are as follows:

A. Handover latency

The time from the last receiving packet from PAR to first receiving packet from NAR is handover latency. The upcoming protocols aim to reduce latency.

B. Scope of Mobility

Protocols are classified into two categories; local mobility and global mobility as per scope of operations. The MN moves within different sub domains in global mobility, and in local mobility the MN moves in its domain.

C. Mobility Class

Mobility management is classified as host based and network based categories. In host based, some modification is needed in IP stack protocol but network based mobility does not require such modification as it is network oriented mobility.

D. Power Consumption

The power consumed for performing mobility related functions. Many techniques are introduced to reduce the power consumption or emission of carbon dioxide such as green mobile techniques.

III. Conclusion

In this paper, mobility management protocols including; MIPv4, MIPv6, FMIPv6, HMIPv6, PMIPv6, FHMIPv6 and DMM are discussed in detail. The aim of this paper is to compare all the above protocols in respect of handover & throughput to reduce the delay in wireless communication. By decreasing the delay and increasing the throughput, these protocols can provide better service quality to the wireless Internet users. It may be concluded by this research that partially DMM protocol may be proved to be an efficient solution for issues related to handover in wireless communication.

References

- [1] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, "Proxy Mobile IPv6", RFC 5213, 2008.
- [2] H. Chan, H. Yokota, J. Xie, P. Seite, D. Liu, "Distributed and Dynamic Mobility Management in Mobile Internet: Current Approaches and Issues", *Journal of Communications*, Vol. 6, No. 1, pp. 4-15, 2011.
- [3] H. Chan, D. Liu, P. Seite, H. Yokota, J. Korhonen, "Requirements for DMM", IETF Draft (work-in-progress), 2014.
- [4] B. Williamson, "Developing IP Multicast Networks", Cisco Press, 1999.
- [5] Ericsson white paper, "LTE Broadcast: A Revenue Enabler in the Mobile Media Era", 2013.
- [6] C Perkins, D Johnson, J Arkko, Mobility Support in IPv6. Technical report, RFC 6275, 2011. [Online] Available: <http://www.rfc-editor.org/info/rfc6275>.
- [7] AJ Jara, L Ladid, A Skarmeta, "The Internet of everything through IPv6: An analysis of challenges, solutions and opportunities", *J. Wirel. Mob. Netw. Ubiqu. Comput. Dependable Appl.* 4, pp. 97–118, 2013.
- [8] C Makaya, S Pierre, "An analytical framework for performance evaluation of IPv6-based mobility management protocols", *Wirel Commun. IEEE Transac.* 7(3), pp. 972–983, 2008.
- [9] R Koodli, "Mobile IPv6 fast handovers", IETF, RFC 5568, 2009. RFC 5568, [Online] Available: <http://www.rfc-editor.org/info/rfc5568>.
- [10] H Soliman, L Bellier, KE Malki, "Hierarchical mobile IPv6 mobility management (HMIPv6)", IETF, RFC 4140 (2005). RFC 4140, [Online] Available: <http://www.rfc-editor.org/info/rfc4140>.
- [11] A Petrescu, R Wakikawa, P Thubert, V Devarapalli, "Network Mobility (NEMO) Basic Support Protocol", IETF RFC. 4063 (2005). RFC 3963, [Online] Available: <http://www.rfc-editor.org/info/rfc3963>.
- [12] JH Kim, CS Hong, T Shon, "A lightweight NEMO protocol to support 6LoWPAN", *ETRI J.* 30(5), pp. 685–695, 2008.
- [13] M Shin, T Camilo, J Silva, D Kaspar, "Mobility support in 6LoWPAN", draft-shin-6lowpan-mobility-01 (2007). (work in progress, May 29 2007, Network Working Group, Internet-Draft ETRI) [Online] Available: <https://tools.ietf.org/html/draft-shin-6lowpan-mobility-00>.
- [14] V Devarapalli, K Chowdhury, S Gundavelli, B Patil, K Leung, Proxy Mobile IPv6. IETF, RFC 5213 (2008). RFC 5213, doi 10.17487/RFC5213, <http://www.rfc-editor.org/info/rfc5213>. Accessed 12 Oct 2015.
- [15] AJ Jabir, S Shamala, Z Zuriati, N Hamid, A comprehensive survey of the current trends and extensions for the proxy mobile IPv6 protocol. *IEEE Syst. J.* pp. (99), pp. 1–17, 2015.
- [16] JH Kim, R Haw, CS Hong, in Consumer Electronics (ICCE), 2010 Digest of Technical Papers International Conference On. Development of a framework to support network-based mobility of 6LoWPAN sensor device for mobile healthcare system, pp. 359–360, 2010.
- [17] J Kim, R Haw, EJ Cho, CS Hong, S Lee, A 6LoWPAN sensor node mobility scheme based on proxy mobile IPv6. *IEEE Transac. Mob. Comput.* 11(12), pp. 2060–2072, 2012.
- [18] H. Soliman, C. Castelluccia, K.E. Malki, L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)," IETF RFC 4140, 2005.
- [19] C. Perkins, "IP Mobility Support in IPv4," IETF RFC 3344, Aug. 2002.
- [20] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6," IETF RFC 3775, 2003.
- [21] C. Perkins, D. Johnson, J. Arkko, "Mobility Support in IPv6," RFC 6275 (Proposed Standard), Internet Engineering
- [22] H. Soliman, "Mobile IPv6 Support for Dual Stack Hosts and Routers," RFC 5555 (Proposed Standard), Internet Engineering Task Force, 2009.
- [23] MM Islam, E-N Huh, Sensor proxy mobile IPv6 (SPMIPv6)-A novel scheme for mobility supported IP-WSNs. *Sensors.* 11(2), pp. 1865–1887, 2011.
- [24] MM Islam, S-H Na, S-J Lee, E-N Huh, in Future Generation Information Technology: Second International Conference, FGIT 2010, Jeju Island, Korea, December 13–15, 2010. Proceedings, ed. by T-h Kim, Y-h Lee, B-H Kang, and D 'Slęzak. A Novel Scheme for PMIPv6 Based Wireless Sensor Network (Springer, Berlin, Heidelberg, 2010), pp. 429–438.
- [25] MM Islam, TD Nguyen, AA Al Saffar, S-H Na, E-N Huh, in Computational Collective Intelligence. Technologies and Applications: Second International Conference, ICCCI 2010, Kaohsiung, Taiwan, November 10–12, 2010. Proceedings, Part III, ed. by J-S Pan, S-M Chen, and NT Nguyen. Energy Efficient Framework for Mobility Supported Smart IP-WSN (Springer, Berlin, Heidelberg, 2010), pp. 282–291.
- [26] AJ Jabir, SK Subramaniam, ZZ Ahmad, NAWA Hamid, A cluster-based proxy mobile IPv6 for IP-WSNs. *EURASIP J. Wirel. Commun. netw.* 2012(1), 1–17 (2012).
- [27] C Perkins, IP mobility support for IPv4, revised (2010). [Online] Available: <http://www.rfceditor.org/info/rfc5944>.
- [28] M-C Chuang, J-F Lee, in Consumer Electronics, Communications and Networks (CECNet), 2011 International Conference On. FH-PMIPv6: A fast handoff scheme in Proxy Mobile IPv6 networks, pp. 1297-1300, 2011.
- [29] H. Chan, "Proxy Mobile IP with Distributed Mobility Anchors," *GlobeCom 2010 Workshop on Seamless Wireless Mobility*, Miami, USA, 6-10 December 2010.
- [30] P. Bertin, S. Bonjour, and J-M Bonnin, "A Distributed Dynamic Mobility Management Scheme Designed for Flat IP Architectures," *Proceedings of 3rd International Conference on New Technologies, Mobility and Security, (NTMS 2008)*
- [31] P. Seite, P. Bertin, "Dynamic Mobility Anchoring," IETF draft-seite-netext-dma-00.txt, May 2010, work in Progress.
- [32] R. Wakikawa, G. Valadon, J. Murai, "Migrating Home Agents Towards Internet-scale Mobility Deployments," *Proceedings of the ACM 2nd CoNEXT Conference on Future Networking Technologies*, Lisboa, Portugal. 4-7 December 2006.