COST AND HANDOVER PERFORMANCE ANALYSIS OF DMM PROTOCOLS FOR FUTURE MOBILE NETWORKS

A THESIS SUBMITTED TO

THE FACULTY OF ENGINEERING & TECHNOLOGY OF

JADAVPUR UNIVERSITY

IN PARTIAL FULFILMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

MASTER OF ENGINEERING

IN SOFTWARE ENGINEERING

SUBMITTED BY

MEGHNA MITRA

CLASS ROLL NO.: **001711002010**

EXAMINATION ROLL NO.: **M4SWE19014**

REGISTRATION NO.: **140969** OF **2017-2018**

UNDER THE SUPERVISION

OF

DR. BHASKAR SARDAR

ASSOCIATE PROFESSOR

DEPARTMENT OF INFORMATION TECHNOLOGY

JADAVPUR UNIVERSITY

2019

DEPARTMENT OF INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING & TECHNOLOGY

JADAVPUR UNIVERSITY

Certificate of Submission

I hereby recommend that the thesis entitled, ***"Cost and Handover Performance Analysis of DMM Protocols For Future Mobile Networks"****, submitted by* ***Meghna Mitra*** *(Registration No. 140969 of 2017-2018) under my supervision, be accepted in partial fulfilment of the requirements for the degree of* ***Master of Engineering in Software Engineering*** *from the* ***Department of Information Technology*** *under* ***Jadavpur University****.*

_____

(Signature of Supervisor)
DR. BHASKAR SARDAR

Countersigned by:

_____	_____
Head of Department **Department of Information Technology** **Jadavpur University**	**Dean** **Faculty of Engineering & Technology** **Jadavpur University**

DEPARTMENT OF INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING & TECHNOLOGY

JADAVPUR UNIVERSITY

CERTIFICATE OF APPROVAL

The thesis at instance is hereby approved as a creditable study of an engineering subject carried out and presented in a manner satisfactory to warrant its acceptance as a prerequisite to the degree for which it has been submitted. It is understood that by this approval the undersigned do not necessarily endorse or approve any statement made, opinion expressed or conclusion drawn therein, but approve this thesis for the purpose for which it is submitted.

Signature of External Examiner

(Signature of Supervisor)

Dr. Bhaskar Sardar

Associate Professor, Dept. of I.T.

Jadavpur University

DEPARTMENT OF INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING & TECHNOLOGY

JADAVPUR UNIVERSITY

DECLARATION OF ORIGINALITY AND COMPLIANCE OF ACADEMIC ETHICS

I hereby declare that this thesis contains literature survey and original research work done by me, as a part of my Master of Engineering in Software Engineering course.

All information in this document have been obtained and presented in accordance with academic rules and ethical conduct.

I also declare that, as required by these rules and conduct, I have fully cited and referenced all materials and results that are not original to this work.

Name	:	MEGHNA MITRA
Roll No.	:	M4SWE19014
Thesis Title	:	COST AND HANDOVER PERFORMANCE ANALYSIS OF DMM PROTOCOLS FOR FUTURE MOBILE NETWORKS

_____

Signature (with date)

ACKNOWLEDGEMENT

The satisfaction I have on successful completion of the thesis will be incomplete without mentioning the people who have helped me achieve success. I offer my sincere gratitude to the Department of Information Technology, Jadavpur University for giving me the opportunity to pursue this thesis, during the course of Master of Engineering in Software Engineering.

I take this opportunity to express my sincere appreciation and humble gratitude for my respected mentor, Dr. Bhaskar Sardar for his guidance and full support in completing my research work successfully. He has always motivated and inspired me to pursue and delve into the depths of the work I am doing. I thank him for his constant support and effort, without which I would not have been able to achieve success.

I will thank Prof. Palash Kundu for his guidance in my thesis work. I want to express my heartfelt gratitude for his diligent counsel every time I faced a problem.

In addition to this, I would like to acknowledge the helping hand extended by Ms. Debadreeta Das, Junior Research Fellow of the Information Technology department, especially for motivating me to explore new ideas and for her constant support whenever I needed it.

Lastly, I wish to thank my parents for their encouragement and blessings. There is little doubt that without their help this work would not have been possible.

_____

(MEGHNA MITRA)
M.E. in Software Engineering
Dept. of Information Technology
Jadavpur University

ABSTRACT

Mobile devices and the proportion of their connectivity to the internet is increasing exponentially with time. This has led to a monumental pressure on the network entities involved in transmission of data packets between mobile nodes, in terms of handover latency and cost. Currently used centralized mobility management schemes are grappling to handle this immense pressure. Distributed mobility management (DMM) protocols shift the focus from the present hierarchical network architecture to a flatter network structure. For this reason, it is quite apparent to study the various solution families of DMM. In this research work, I have compared and analysed four different DMM-based IP mobility solutions: MIPv6-based DMM, PMIPv6-based DMM, SDN-based DMM, and Routing-based DMM. With the help of an analytical model, I have formulated the total cost and handover latency of these four different DMM solutions. Based on the results I have got, I compared these four solutions with the help of graphical charts.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1

INTRODUCTION

The internet allows us to connect to the World Wide Web and perform various operations like searching, surfing, viewing images and videos, and many other diverse functions. There was a time when connection to the internet was static. People used to sit at one place and connect their computers to the internet through a LAN/WAN. These computer nodes, which used to connect to the internet at a fixed point of location or a fixed area, is known as *static nodes*. Static nodes are used still now, but with the advancement of technology, a new category of computers, called *mobile nodes* have come up. A mobile node is a device connected to the internet, whose location and point of attachment to the internet may change frequently. For example, mobile phones, laptops, tablets, and even a router. Thus, with these moving devices, the need for mobility management came up.

Recent years have seen an explosive growth in the number of mobile devices that connect to the internet. Also, the amount of time that these devices remain connected to the internet has increased. Coupling the fact that mobile devices roam around freely with that of increased amount of internet connection time, it is quite clear that the connection needs to be maintained intact, even if the mobile node moves from one network to another. This is the main work of mobility management- mobile wireless devices needs to be remain attached to the internet even as they move from one place to another, establishing new links on the way and moving away from the previously established links.

Mobile IP is an Internet Engineering Task Force (IETF) standard communications protocol and it is designed to allow mobile device users move from one network to another while maintaining a permanent IP address. Mobile IP allows location independent routing of IP datagrams on the internet. Each mobile node is identified by its home address irrespective of its current location in internet. If the node is away from its home network, it can communicate with the internet through its care-of-address (in a foreign network). Mobile IP hence specifies how a mobile node registers with its home network, and how home agent routes the datagram packets to the mobile node through the tunnel (between the home network and the foreign network).

There are two ways to handle the mobility of nodes, namely, centralized mobility management and distributed mobility management. In the centralized schemes, as the name suggests, there is a central entity that handles all the mobility related signaling alone. This seems to be an attractive choice because of the ease of operation. But the major problem in these schemes is the single point of failure, along with many other security and network entity issues. To overcome these hassles, distributed schemes came into view [1].

D-MIP represents distributed MIPv6, which has been modified from its centralized counterpart [2]. It can be followed either with route optimization or without it. But it is a type of protocol that involves the host, that is, the mobile node (MN) itself. This type of involvement is not at all accepted in today's world. It is almost obsolete. That is why this protocol gave way to other variants of distributed schemes, which do not involve the MN in any handover operation. All operations take place at the network level. D-PMIP represents distributed PMIPv6. It is a partially distributed scheme. Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG) are the two main entities. LMA is the topological anchor point for the MN's home network prefixes. MAG performs the mobility management on behalf of MN. The MAG acts

as a proxy to the MN, and runs MIPv6 on behalf of the MN. LMA acts as the home agent (HA) in PMIPv6. D-SDN represents distributed Software-defined Networking scheme, which is also partially distributed. A driving factor of SDN is DP (data plane)-CP (control plane) separation. CP is separated from the hardware and implemented as a software, and runs on a standard server in a centralized location. SDN has transformed the networks from a tightly coupled architecture to a distributed architecture. Thus lies its application in DMM. Location and handover management is done at the centralized SDN controller, while packet forwarding is fully distributed at access routers. In the control plane, a centralized controller maintains a global view on the network and computes the optimal path from CN to the new AR. The computed optimal path is established in the DP and the packets are routed to the new AR without any tunnelling overhead. Thus, SDN-based DMM can achieve path optimization and provide significant benefits in terms of network and traffic management [3]. D-Routing represents distributed routing-based scheme, and this one is fully distributed. Routing-based solutions follow a totally different approach. In this case, when MN attaches to a new mobility access router (MAR), it requests for node information from other routers in the network. The old router forwards the information about the MN to all the routers at the same level and cluster. In this way, information about the MN gets propagated by broadcasting. Finally, all routers update their routing tables and know the next hop of the MN [4]. In this way, the reachability of the node is ensured while moving within the domain. This approach has some limitations in terms of handover and scalability.

The significance of network layer mobility management is that when a packet is sent to a mobile node, a risk of breaking the TCP connection cannot be taken, which is connection-oriented. Changing the IP address while still having a TCP connection open means breaking the connection. A TCP connection is identified by the tuple (source IP address, source port, destination IP address, destination port), also known as a socket pair. Therefore, a TCP connection cannot survive any address change.

Mobile IP can be thought of as the cooperation of three processes. First, there is a discovery mechanism defined so that mobile computers can determine their new attachment points (new IP addresses) as they move from place to place within the internet. Second, once the mobile node knows the IP address at its new attachment point, it registers with an agent representing it at its home network. Lastly, mobile IP defines simple mechanisms to deliver datagrams to the mobile node when it is away from its home network.

At first, the concept of *centralized mobility management (CMM)* is there and the various protocols that come under this category. Here, there is a central mobility anchor that handles all the work on behalf of the mobile node and the network. A network layer mobility management protocol is typically based on the principle of distinguishing between a session identifier and a *forwarding address*; and, maintaining a mapping between the two. In mobile IP, the new IP address of the mobile node after the node has moved is the forwarding address, whereas the original IP address before the mobile node moves is known as the *session identifier*. The location management (LM) information is kept by associating the forwarding address with the session identifier. Packets addressed to the session identifier will first route to the original network, which redirects them using the forwarding address and then delivers them.

Redirecting packets this way can result in long routes. An existing optimization routes directly, using the forwarding address of the host, and as such is a host-based solution.

In centralized mobility management, the location information in terms of a mapping between the session identifier and the forwarding address is kept at a single mobility anchor, and packets destined to the session identifier are forwarded via this anchor. In other words, such mobility management systems are centralized in both the control plane and the data plane. Here, there is a hierarchical network architecture.

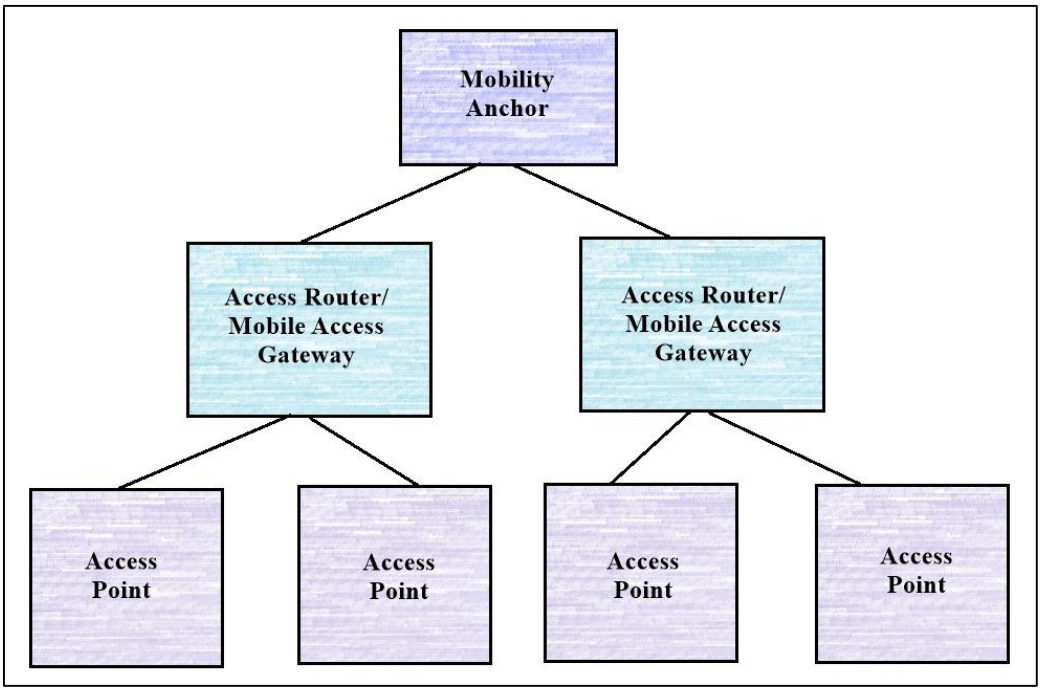


Fig.1. Hierarchical Architecture in Centralized Mobility Management

Then, *distributed mobility management (DMM)* comes up which is an alternative to centralized deployment. A distributed mobility management scheme has a flat network architecture. It has many advantages over the currently operating centralized mobility management schemes, and can be the next big turnover in the coming years. This is because DMM opts for a flatter network, which has fewer hierarchical levels compared to a hierarchical mobile network. DMM is distributed in the data plane, whereas the control plane may be either centralized or distributed.

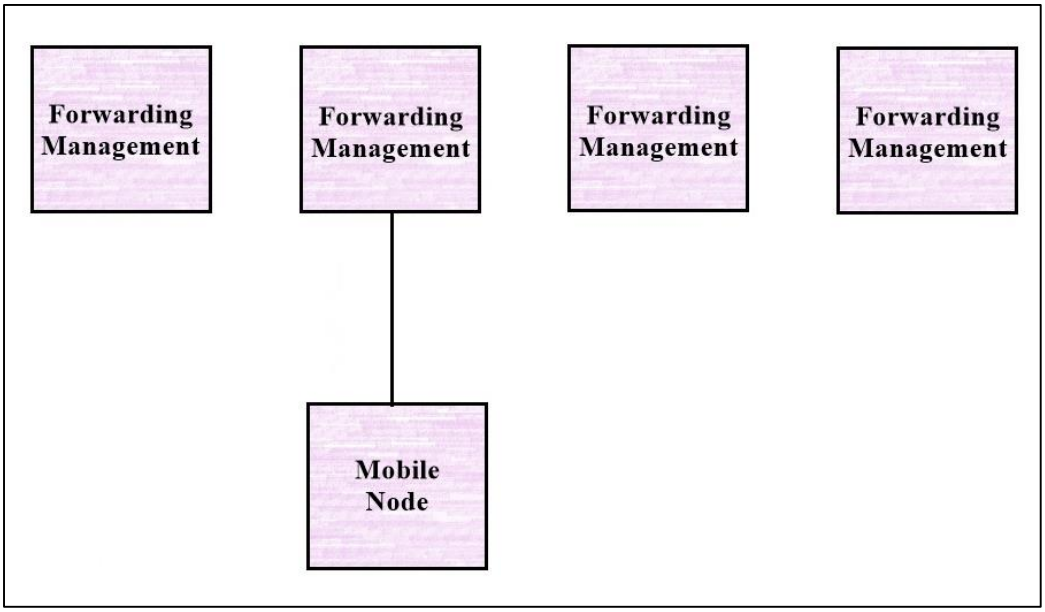


Fig.2. Flat Architecture in Distributed Mobility Management

There are some issues that need to be tackled with the increase in mobility:

i. The focus should be on using less number of network resources to reduce cost of physical devices.
ii. The focus should be on lesser handoff latency, and it is one of the main concerns in mobility.
iii. There should not be any delay in packet transmission.
iv. Flatter network so that mobile nodes could get closer to the main access network device.

All these requirements prod us to move towards a more effective and robust architecture, and that is DMM. Advantages of DMM over CMM are seen, and the reasons behind the fact that DMM will hugely propagate future 5G networks.

Chapter 2

CENTRALIZED MOBILITY MANAGEMENT

Traditional networks have a centrally deployed mobility anchor, for managing mobility of nodes. This is more due to the fact that in the past decade, a good number of network layer mobility protocols have been standardized like mobility in IPv4 (MIPv4), mobility in IPv6 (MIPv6), hierarchical mobile IPv6 (HMIPv6), proxy mobile IPv6 (PMIPv6) and fast handovers in MIPv6 (FMIPv6). All these protocols are different from each other in terms of functionality and associated message formats. But they all employ a centralized mobility anchor to allow a mobile node to remain reachable after it has moved to a different network. Among other tasks that the anchor point performs, the anchor point ensures connectivity by forwarding packets destined to, or sent from, the mobile node. It is a centrally deployed mobility anchor in the sense that the deployed architectures today have a small number of these anchors and the traffic of millions of mobile nodes in an operator network is typically managed by the same anchor.

Mobility management is needed because the IP address of a mobile node may change as the node moves. Mobility management functions may be implemented at different layers of the protocol stack. At the IP (network) layer, mobility management can be *host-based* or *network-based*. Host-based mobility means that mobile nodes must signal themselves to the network when their location changes and must update routing states in the home agent. This leads to many security concerns. Thus, advancement to network-based mobility management protocols were made. Contrary to host-based approach, network-based functionality is implemented by the network itself, which is responsible for tracking the movements of the host and initiating the required mobility signalling on its behalf. All the previous discussed protocols are host-based protocols except only one protocol, that is, PMIPv6. Network-based Localized Mobility Management (NetLMM) enables IP mobility for a host without requiring its participation in any mobility-related signalling. The network infrastructure is responsible for managing IP mobility on behalf of the host. PMIPv6 is one such standard NetLMM IP mobility solution.

2.1. MIPv6

In MIPv6, mobile nodes can roam around various networks, and still maintain an active connection to the internet. A care-of address (CoA) is an IP address of a mobile node that is currently in some foreign network, and is assigned the subnet prefix of that foreign network. During the handoff, a new IP address is allocated to the mobile node (MN), known as the CoA. Before the handoff, correspondent node (CN) transfers packets directly to the home agent (HA); and after the handoff, CN transfers packets through the tunnel set up between the home network's agent and the foreign network.

Binding means the relation between MN's home address and CoA. When MN is in a foreign network, it registers its CoA with a HA (like a router). This binding registration is done by the MN by sending a binding update to the HA. HA replies with a binding acknowledgement message. The routing of packets directly to the mobile node's CoA ensures the shortest communication path. It also eliminates congestion at the MN's home link.

Some limitations of MIPv6 stand out due to which other protocols were enhanced. In MIPv6, there is high packet loss rate and the handoff latency is also very high. There is a huge load on the home agent since it has to keep track of all its mobile nodes in a faraway network.

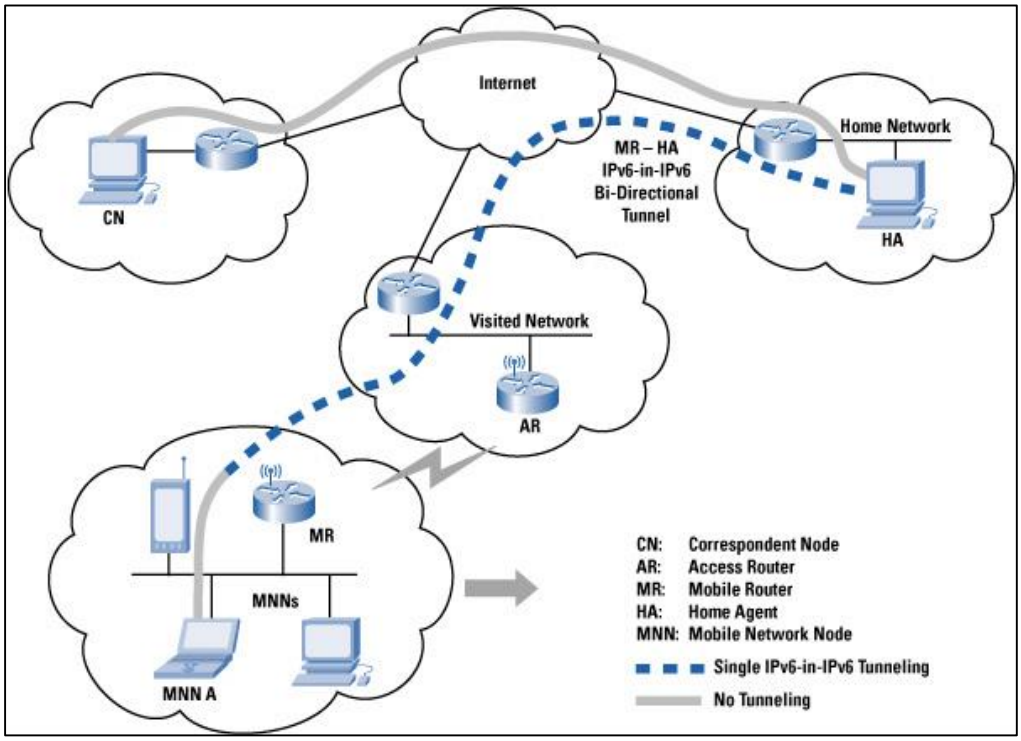


Fig.3. MIPv6 Architecture

2.2. HMIPv6

Micro mobility means the mobile node's movements inside a network. In contrast, macro mobility means movement between different networks. The mobile nodes may change their point of connection to the internet very frequently. The change of an access point during active data transmission or reception is called a *handoff* or *handover*. The IETF published several standards for supporting mobility in IP networks. The standards are divided into two categories, those supporting macro-mobility and those supporting micro-mobility. The IETF's macro-mobility protocol is the Mobile IPv6 (MIPv6) protocol. Micro-mobility protocols aim to improve localized mobility by reducing the handover overheads. Fast Handover and Hierarchical MIPv6 (FMIPv6 and HMIPv6) are two micro-mobility protocols standardized by the IETF.
A large number of MNs change networks frequently. This puts a huge pressure on both the HA and the network due to the exchange of registration and binding update messages. Thus, the above mentioned micro-mobility protocols have come up.

HMIPv6 provides micro-mobility support by installing a mobility anchor point (MAP), which is responsible for a certain domain and acts as a local HA within this domain for visiting MNs. The MAP receives all packets on behalf of the MN, encapsulates and forwards them directly

to the MN's current address (link COA or LCOA). As long as an MN stays within the domain of a MAP, the globally visible COA (regional COA or RCOA) does not change. A MAP domain's boundaries are defined by the access routers (AR) advertising the MAP information to the attached MNs. A MAP assists with local handovers and maps RCOA to LCOA. MNs register their RCOA with the HA using a binding update. When a MN moves locally it must only register its new LCOA with its MAP. The RCOA stays unchanged. To support smooth handovers between MAP domains, an MN can send a binding update to its former MAP.

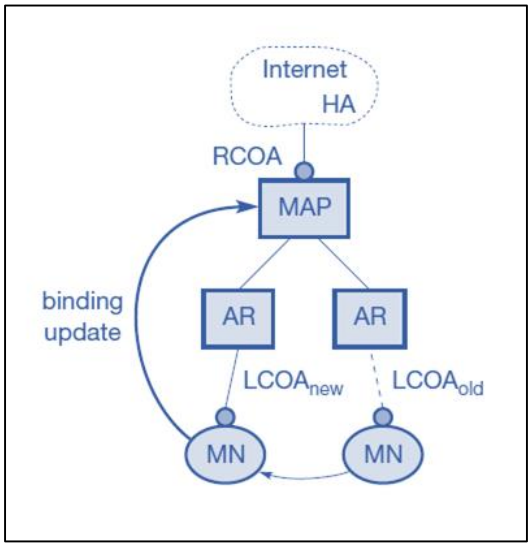


Fig.4. HMIPv6 Architecture

Advantages

- MNs can use their RCOA as source address.
- MNs can have limited location privacy because LCOAs on lower levels of the mobility hierarchy can be hidden (only in same domain).
- Direct routing between CNs sharing the same link is possible. MNs location is revealed but there is a better packet flow optimization (direct routing without involving MAP).

Disadvantages

- Additional infrastructure component (MAP).
- Routing tables are changed based on messages sent by mobile nodes. Additional security functions might be necessary in MAPs.

2.3. FMIPv6

Fast Handover for Mobile IPv6 (FMIPv6) is a solution for long handover latency and high packet loss in MIPv6. The MN can quickly detect that it has moved to a new subnet as the protocol lets MN know the new access point (AP) and prefix when the MN is still connected to its current subnet, which will be Previous Access Router (PAR) in near future.

MN discovers APs and requests subnet information. The result is [AP-ID, AR-Info] tuple. For this purpose, some additional messages are introduced such as Router Solicitation for Proxy (RtSolPr) - message from MN to PAR before a potential handover, Proxy Router Advertisement (PrRtAdv) - message from PAR to MN giving information about neighbouring links, Fast Binding Update (FBU) - MN tells PAR that it will move to a New Access Router (NAR). MN formulates a new CoA (NCoA) when it is still on PAR. Thus, latency due to new prefix discovery is eliminated. This NCoA can be used immediately after the MN attaches to the NAR, only if it had received Fast Binding Acknowledgment (FBack) before it moved. In case MN moved without receiving FBack, it can still start using NCoA after announcing its attachment through an unsolicited Neighbor Advertisement message (FNA). So the latency due to NCoA configuration is reduced. Handover Initiate (HI) is a message from the PAR to the NAR regarding MN's handover. Handover Acknowledge (HAck) is a message from the NAR to the PAR as a response to HI.

Depending on whether an FBack is received on PAR, there are two modes of operation.

1. MN sends FBU when it is still on PAR, which then establishes traffic forwarding. The scenario in which MN sends an FBU and receives an FBack on PAR's link is characterized as the *predictive* mode of operation.

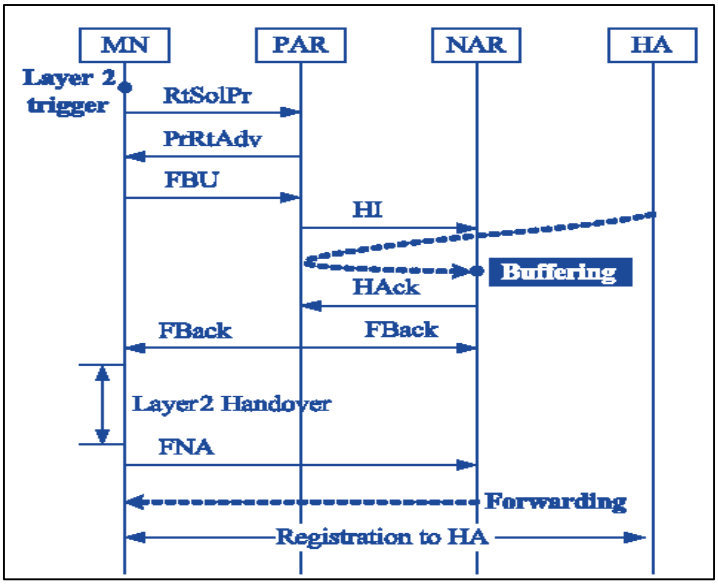


Fig.5. Predictive Fast Handover in FMIPv6

2. MN sends FBU only after attaching to NAR. The scenario in which the MN sends an FBU from the NAR's link is characterized as the *reactive* mode of operation.

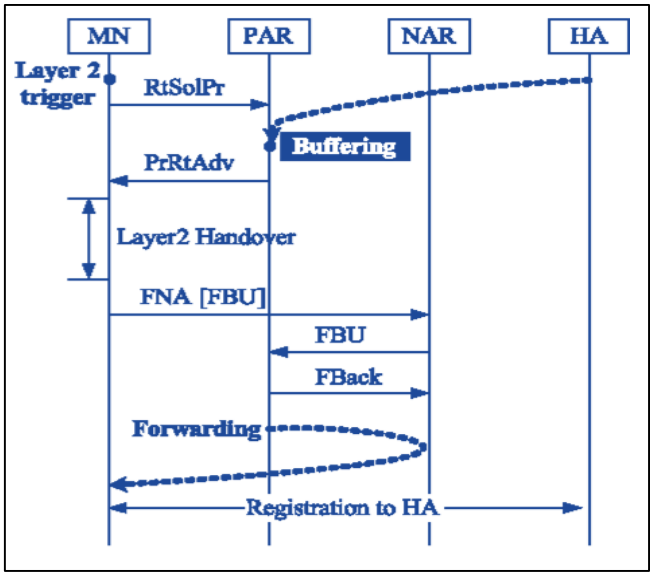


Fig.6. Reactive Fast Handover in FMIPv6

2.4. PMIPv6

Network-based mobility is another approach to support mobility for IPv6 nodes without host involvement. This approach does not require the MN to be involved in the exchange of signalling messages between itself and the HA. A *proxy* mobility agent in the network performs the signalling with the HA and does the mobility management on behalf of the MN. Because of the use and extension of MIPv6 signalling and HA functionality, this protocol is referred to as Proxy Mobile IPv6 (PMIPv6).

Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG) are the two main entities. LMA is the topological anchor point for the MN's home network prefixes. MAG performs the mobility management on behalf of MN. In PMIPv6, the MN is not at all involved in the handoff process. The MAG acts as a proxy to the MN, and runs MIPv6 on behalf of the MN. LMA acts as the HA in PMIPv6. The MAG is given a proxy-CoA (not the MN). CN transfers packets to the LMA, which in turn forwards the packets to the respective MAG's network in which the MN is currently residing. The MAG accepts the packets and forwards them to the MN, in the same way both before and after handoff.

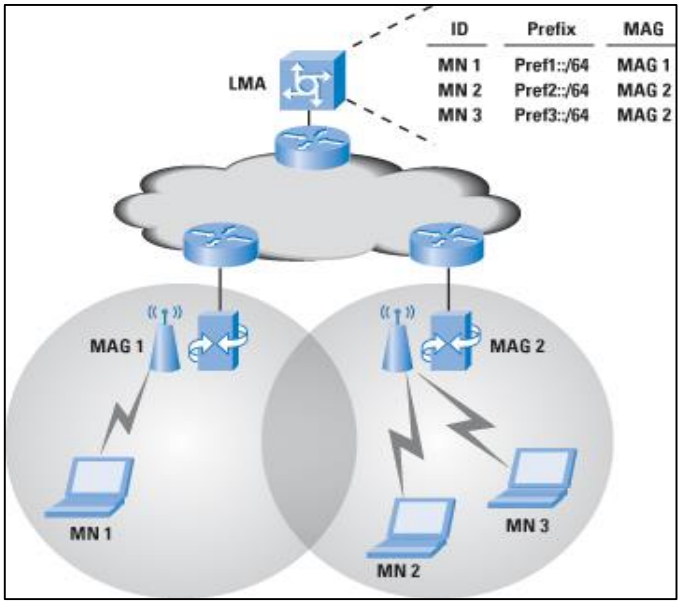


Fig.7. PMIPv6 Architecture

The process for MN attachment in PMIPv6 is as follows:

1. Attaching: MN attaches to the MAG.

2. Identification: MAG authenticates MN based on its link layer address (e.g. MAC address) and authorizes MN.

3. Router solicitation: MN sends a router solicitation to obtain an IPv6 prefix.

4. Proxy binding update (PBU): MAG sends a PBU to the LMA. This PBU associates the MAG address with the identity of the MN.

5. Allocate prefix, update BC: The LMA allocates a prefix for MN (Home Network Prefix). The LMA creates an entry in its BC. The entry contains the MN ID (MN-ID-1), the address MAG of the proxy MAG (proxy-CoA) as well as the prefix assigned to MN.

6. Proxy binding acknowledgement (PBA): The LMA sends a PBA back to MAG. The PBA contains the information of the BPC entry created in step 5.

7. Tunnel setup: The LMA and MAG establish a bidirectional IPv6-in-IPv6 tunnel that is used for tunneling packets to and from MN.

8. Router advertisement: MAG sends a router advertisement with the assigned prefix to MN. MN creates a routing table entry for the prefix.

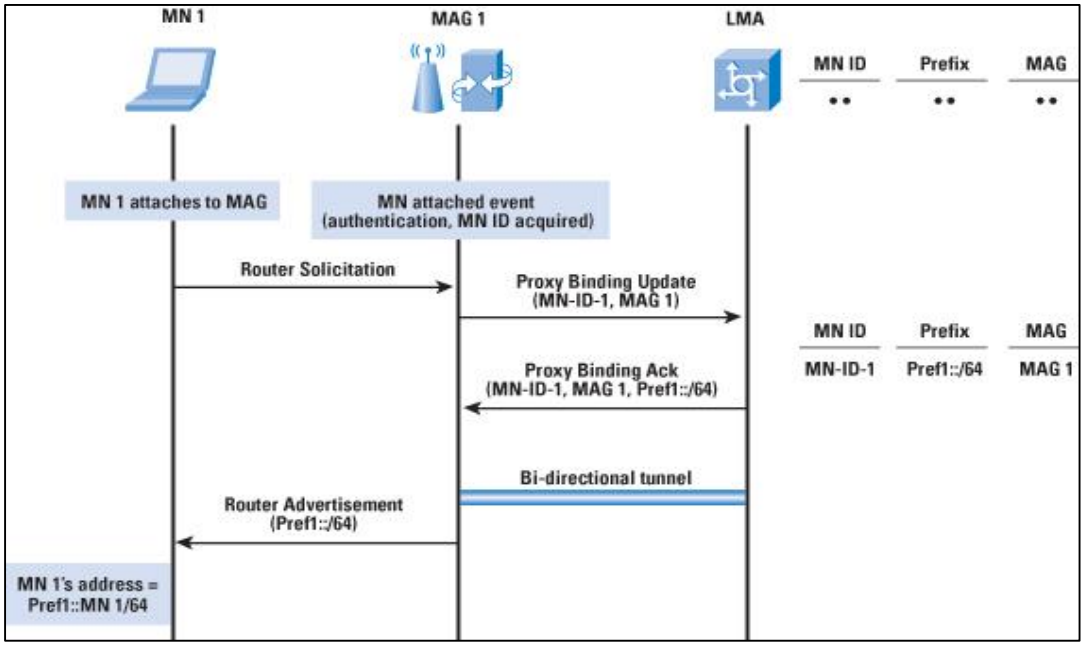


Fig.8. Signal Flow for MN Attachment in PMIPv6

The process for MN handoff in PMIPv6 is as follows:

1. Detaching: MN detaches from p-MAG (PMAG – Previous MAG) or MAG1.

2. Deregistration: p-MAG sends a PBU with a de-registration request for MN (MN-ID-1).

3. Start timer: LMA starts a timer for the MN proxy binding cache entry. During the timer period the LMA drops any packets received for MN.

4. Proxy binding acknowledgement (PBA): The LMA sends a PBA back to p-MAG. The PBA contains the information of the BPC entry created in the MN attachment phase.

5. Attaching to n-MAG (NMAG – New MAG): MN now attaches to n-MAG or MAG2 the same way as it did to p-MAG in the MN attachment phase.

6. Router solicitation: MN sends a router solicitation to obtain an IPv6 prefix.

7. Proxy binding update (PBU): n-MAG sends a proxy binding update to the LMA. This PBU associates the n-MAG address with the identity of the MN.

8. Update of the binding cache entry (BCE): The LMA detects that MN already has an entry in the binding cache and therefore updates the entry for MN. MN is now associated with n-MAG. The prefix for MN remains the same (address transparency for MN).

9. Proxy binding acknowledgement (PBA): The LMA sends a PBA back to n-MAG. The PBA contains the information of the BPC entry updated in step 8.

10. Tunnel setup: The LMA and n-MAG establish a bidirectional IPv6-in-IPv6 tunnel that is used for tunneling packets to and from MN.

11. Router advertisement: n-MAG sends a router advertisement with the same prefix assigned to MN. MN will not see an address change and thus all open transport connections (TCP, UDP) remain open.

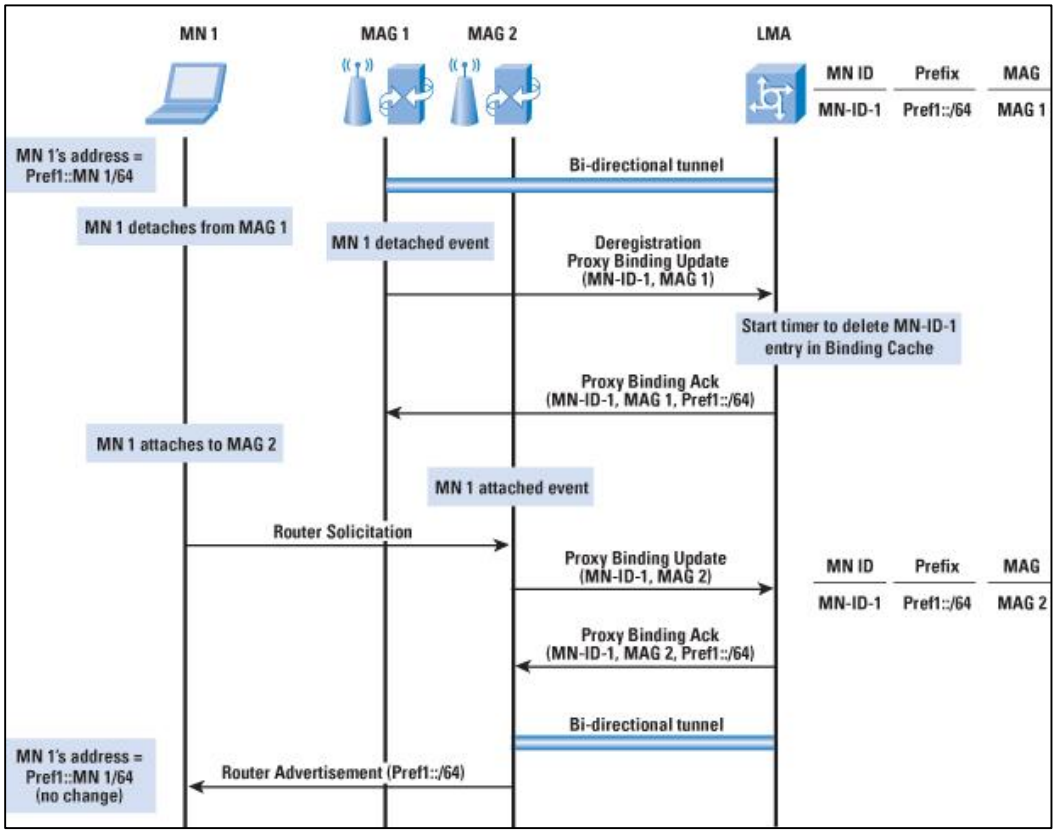


Fig.9. Signal Flow for MN Handoff in PMIPv6

2.5. Limitations of CMM

- The network traffic needs to traverse the centrally deployed mobility anchor, and it is not always the optimal route.
- Since the whole path of the packet is dependent on the central anchor, there is high chance of single point failure.
- There are some nodes which does not need mobility support in the network. But still, in CMM, resources are wasted to support these nodes.
- Maintenance is high.

Thus, there is a need to move on to DMM, and explore it in depth. There is a need to see its future applications in upcoming 5g networks.

Chapter 3

DISTRIBUTED MOBILITY MANAGEMENT

A *distributed mobility management (DMM) environment* means a scenario in which network traffic is distributed in an optimal way, without relying on a central anchor. The centralized deployment of mobility anchors gives rise to several problems. In order to address these problems, a DMM architecture has been proposed by IETF. For this reason, DMM architecture is needed.

A distributed mobility management (DMM) scheme has a flat network architecture [5]. By a flatter architecture, it means that the anchors (access routers) are placed topologically closer to the user (mobile node); distributing the control and data plane functions among the various entities located in the network. It has many advantages over centralized mobility management schemes, and can be the next big turnover in the coming years. This is because distributed schemes opt for a flatter network, which has fewer hierarchical levels compared to a hierarchical mobile network in centralized schemes. DMM is distributed in the data plane, whereas the control plane may be either centralized or distributed. Distributed mobility management protocols can be further divided into sub-categories [6], as shown in Fig. 10.

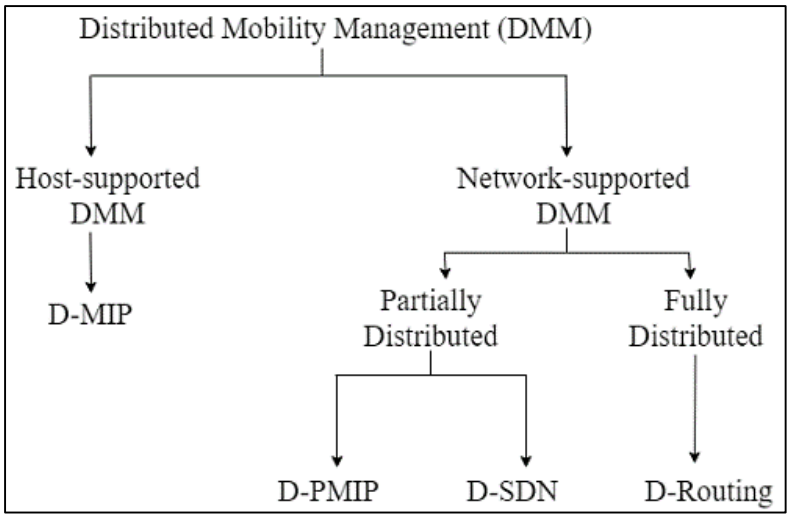


Fig. 10. DMM protocols

Host-supported DMM like D-MIP requires the MN to provide its current location, active prefixes and anchoring points to the mobility management system. Network-supported DMM can further be divided into two schemes: partially distributed and fully distributed. D-PMIP and D-SDN are partial DMM schemes, whereas D-Routing is fully distributed. Network-supported solutions retrieve all the information of the MN without involving it. MN is not aware of the operations going on in its handover process. Partial distribution means that there is at least one central entity (LMA in D-PMIP and SDN controller in D-SDN) that takes part in the handover process. Full distribution means there is no presence of a central entity. Though we are striving for full distribution, we will see that it has some shortcomings. All the protocols have some advantages on one hand, and weigh down with some issues on the other hand. Our goal is to measure these protocols based on their pros and cons.

The problems that can be addressed with DMM are as follows:

a) **Non-optimal routes**
Increase in delay due to forwarding via a centralized anchor.

b) **Divergence from other evolutionary trends in network architectures such as distribution of content delivery**
Mobile networks have generally been evolving towards a flatter network, which CMM does not support.

c) **Lack of scalability of centralized tunnel management and mobility maintenance**
Tunnel setup in CMM requires more resources and reduces scalability.

d) **Single point of failure and attack**
CMM is vulnerable to a devastating single source attack. The impact of a successful attack on CMM can be far greater as well.

e) **Unnecessary mobility support to clients that do not need it**
IP mobility support is usually provided to all MNs, which is not always needed.

f) **Mobility signalling overhead with peer-to-peer communication**
Resources may be wasted when mobility signalling is not turned off for peer-to-peer communication.

g) **Deployment with multiple mobility solutions**
There are already many variants and extensions of MIP. Deployment of new solutions can be risky when they work with solutions already deployed in the field.

h) **Duplicate multicast traffic**
Multicast subscriptions can exist in both upstream and downstream entities. This problem may also exist or be more severe in DMM.

3.1. DMM Requirements

The requirements of DMM, and the way in which these requirements can solve the above mentioned problems related to CMM are as follows:

1. **Distributed deployment**
Traffic should be routed in an optimal manner without having to traverse a central anchor point. For this, IP mobility, network access and routing solutions provided by DMM must enable a distributed deployment of mobility.

The motivation behind this requirement is to match with current trend in network evolution: more cost and resource effective, improve scalability, avoid single point of failure, mitigate threats being focused on a centrally deployed anchor (HA or LMA).

This requirement addresses problem numbers a), b), c) and d).

2. **Transparency to upper layers**
   The DMM solutions must provide transparency above the IP layer when needed.

   The motivation of this requirement is to enable more efficient use of network resources and more efficient routing by not maintaining a stable home IP address when there is no such need.

   This requirement addresses problem numbers e) and f).

3. **IPv6 deployment**
   The DMM solutions should target IPv6 as primary deployment and should not be tailored specifically to support IPv4.

   The motivation for this requirement is that IETF's general orientation is towards IPv6. Also, DMM deployment is tailored for IPv6 in a greater manner, since it is dependent on some IPv6-specific features.

4. **Compatibility**
   The DMM solution should be able to work between trusted administrative domains when allowed by the security measures deployed between these domains. Depending on the environment in which DMM is deployed, the DMM solutions may need to be compatible with other existing mobility protocols that are deployed in that environment.

   The motivation of this requirement is to allow inter-domain operation and to preserve backwards compatibility so that the existing networks and hosts are not affected by DMM.

   This requirement addresses problem number g).

5. **Existing mobility protocols**
   A DMM solution should first consider reusing and extending the existing mobility protocols before specifying new protocols.

6. **Security considerations**
   Signalling messages are subject to attacks over the internet and require end-to-end security. Thus, authentication and authorization mechanisms are required.

   The motivation behind this is that mutual authentication and authorization between a host and a router providing DMM support is needed to prevent attacks. Otherwise, various attacks such as impersonation, denial of service, man-in-the-middle attacks, etc. can collapse the DMM service.

3.2. DMM Solutions

Existing IP mobility protocols can be configured to work in a DMM environment. But before moving on to DMM specifics, there is a need to know about all the important planes. The control plane and data plane is the heart of today's networking hardware to move IP packets. These planes of operation are the building blocks of the layered architecture that networks have evolved to today. The *data plane (DP)* is the collection of resources across all network devices responsible for forwarding traffic. The DP is the unit that actually forwards traffic to the next hop along the selected path according to control plane logic. Data plane packets go through the router. The *operational plane (OP)* is the collection of resources responsible for managing the overall operation of individual network devices. The *control plane (CP)* is the collection of functions responsible for controlling one or more network devices. CP instructs network devices with respect to how to process and forward packets. The control plane interacts primarily with the data plane and, to a lesser extent, with the operational plane. It makes decisions about where traffic is sent. The control plane functions include system configuration, management, and exchange of routing table information. The *management plane (MP)* is the collection of functions responsible for monitoring, configuring, and maintaining one or more network devices or parts of network devices. The management plane is mostly related to the operational plane (it is related less to the forwarding plane). The *application plane* is the collection of applications and services that program network behaviour. The data plane (sometimes known as the user plane, forwarding plane, carrier plane or bearer plane) is the part of a network that carries user traffic. The data plane, the control plane and the management plane are the three basic components. The control plane and management plane serve the data plane, which bears the traffic that the network exists to carry.

DMM is distributed in the data plane, whereas the control plane may be either centralized or distributed. One of the key aspects of the Distributed Mobility Management (DMM) architecture is the separation of control plane (CP) and data plane (DP) functions of a network element. While data plane elements continue to reside on hardware, the control plane resides as a software element in the cloud. This is usually referred to as *CP-DP separation* and is the basis for the IETF's DMM architecture.

DMM can be mainly divided into two families of solutions:

I. Host-based DMM, and
II. Network-based DMM.

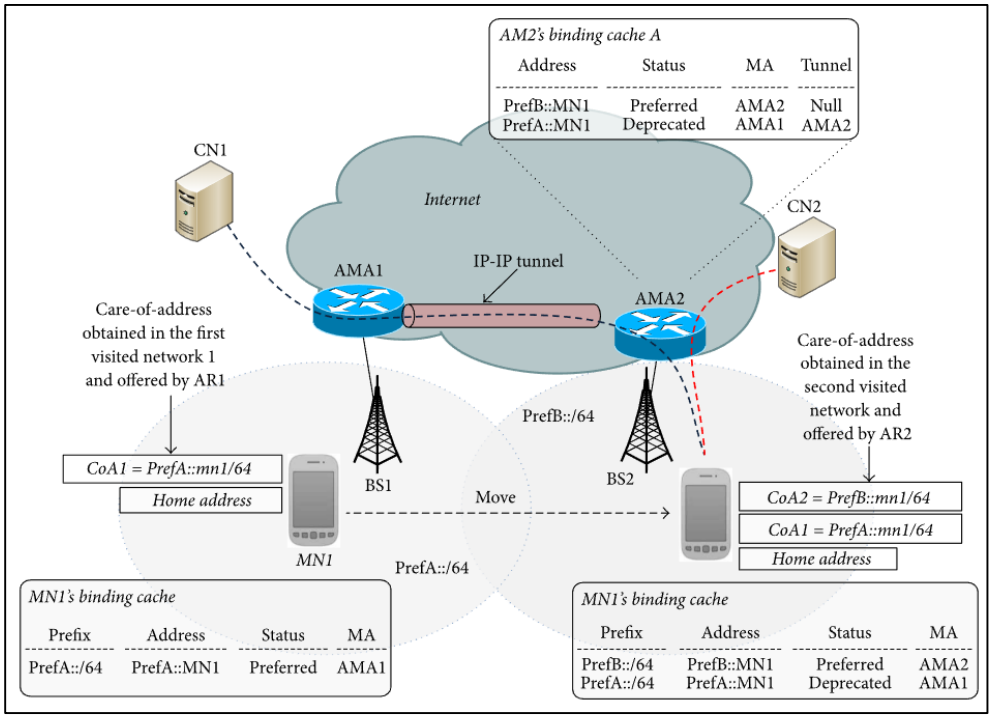


Fig.11. Host-based DMM Solution

CMM's HA is now the AMA (Access Mobility Anchor), which is a new mobility anchor defined for Host-Based DMM solution. The AMAs are distributed at the edge of the network level. The MN configures its address based on the provided network prefix from the AMA. When an MN moves to an adjacent network (served by another AMA), a new address is configured in the MN, while it keeps the previous address. As a result of the signalling between the serving AMA and the original AMA, a bidirectional tunnel is created between them. This solution creates multiple tunnels between AMAs and, in cases where a high mobility rate exists, the system performance might be critically compromised by the frequent registrations and maintenance of multiple tunnels.

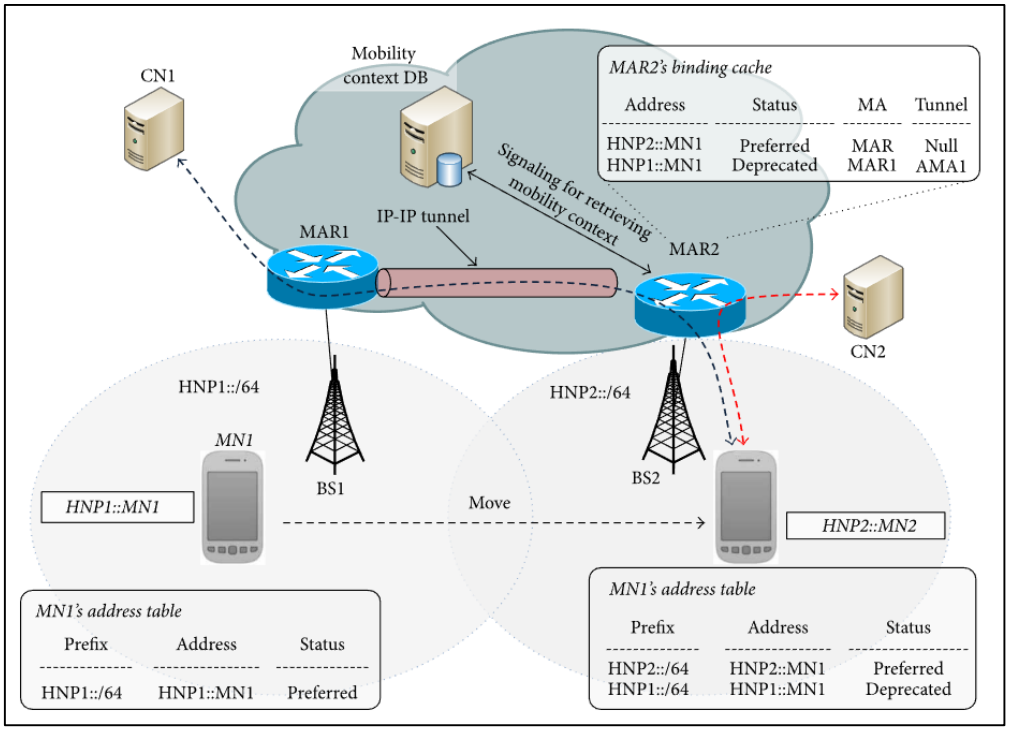


Fig.12. Network-based DMM Solution

The crucial mobility management functions of the already implemented CMM protocols are as follows:

- *Anchoring Function (AF)* means allocation of an IP address to the MN. It is a CP function.
- *Location Management (LM)* means keeping a tab on the current location of MN. It is a CP function. In a client-server model, location query and update messages are exchanged between Location Management client (LMc) and a Location Management server (LMs).
- *Forwarding Management (FM)* means actual sending of packets based on LM information. It may be split into FM-CP and FM-DP.

The mobility management functionalities are moved to the access routers level in order to anchor the traffic closer to the MN. Each AR is required to have both AF and LM functionalities, and is referred to as the mobility access router (MAR). A new session is anchored at the current MAR and initiated using the current IPv6 address. When a handover occurs before the end of the session, data is tunnelled between the current MAR and the anchoring MAR for this session. In order to achieve a network-based solution without the participation of the MN in the mobility signalling, the architecture is partially distributed and relies on a centralized database (Mobility Context DB). This DB stores ongoing sessions for the MNs. Thus, upon a handover, the new MAR retrieves the IP addresses of the anchoring MAR(s) for the MN's sessions from the database. Then, the new MAR proceeds to update the location by sending a PBU to each anchoring MAR.

These two families of solutions can again be divided into 4 different types of DMM solutions:

i. MIPv6-based DMM,
ii. PMIPv6-based DMM,
iii. Routing-based DMM, and
iv. SDN-based DMM.

3.2.1. MIPv6-based DMM (D-MIP)

MIPv6 is a *host-based* DMM solution. In MIPv6, HA is the AF. The LMs is at HA, and LMc is at MN. FM is distributed between the tunnel ends at HA and MN. The ways in which MIPv6 can be deployed in DMM environment is seen.

A nice approach is to distribute the anchors by having many HAs, and assigning the topologically closest anchor to each MN. MN is assigned to HA and uses a home address anchored by HA. This is done to communicate with the CN. Similarly, another MN is assigned to other HA. MN can use several anchors at the same time, each of them anchoring IP flows initiated at a different point of attachment. The goal is to avoid suboptimal routing. Here, route optimization (RO) support in MIPv6 can lead to a flatter network. This is because MIPv6 uses a bidirectional tunnel in which data traffic is always encapsulated between the MN and its HA before being directed to any other destination. This allows MN to update CNs about its current location and then there will be a direct path between MN and CN. But the RO mode has some drawbacks:

a. It is only supported in MIPv6, and requires signalling which leads to protocol overhead.
b. The signalling requires HA and thus HA can be still the single point of failure.
c. This mode needs the support of CN.

But still, this mode reduces traffic substantially.

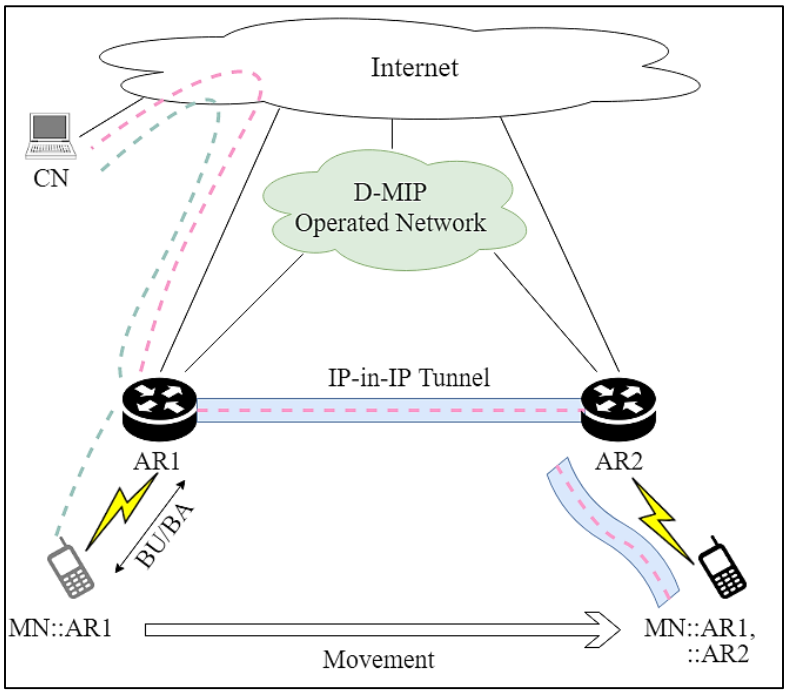


Fig.13. D-MIP Architecture

The basic concept is that a mobile node does not use a single IP address anchored at a central point. It configures and uses an additional IP address at each visited access network. MN uses the locally-anchored address to start new communications, but still maintains the reachability for those IP addresses that are still in use by active communications. This requires the mobile node to bind each of the active addresses with the locally-anchored address currently in use, which is actually playing the role of care-of address in these bindings. Session continuity is guaranteed by the use of bidirectional tunnels between the MN and each one of the home agents anchoring in-use addresses. MN1 initially attaches to the distributed anchor HA/AR1 and configures the IPv6 address HoA1 to communicate with a correspondent node CN1. If MN1 moves to HA/AR5, a new locally-anchored IPv6 address is configured (HoA2) and used for new communications (for example with CN2). The continuity of the session with CN1 is provided by a tunnel set-up between the mobile node and HA/AR1.

A little idea can be given about HMIPv6 also. The LMs is at HA, and LMc is at MN. FM is distributed between the tunnel ends at HA and MAP, and between MN and MAP. It is an extension to provide less centralized mobility deployment. But it fails to provide session continuity if the MN moves outside the local domain. DMM can also use functions of FMIPv6 to improve handover performance.

3.2.2. PMIPv6-based DMM (D-PMIP)

PMIPv6 is a *network-based* DMM solution and *partially distributed*. In PMIPv6, LMA is the AF. The LMs is at LMA, and LMc is at MAG. FM is distributed between the tunnel ends at LMA and MAG. The ways in which PMIPv6 can be deployed in DMM environment is seen.
PMIPv6 protocol operation can be decentralized by deploying several LMAs, and then use of some selection procedure can be there to assign LMAs to MNs. Just like the host-based approach, MN can use several anchors at the same time, each of them anchoring IP flows initiated at a different point of attachment. This assignment can be static or dynamic. The main advantage here is that the LMA is closer to the MN. Thus, close to optimal routes can be provided. But if the MN moves, the path will deviate from remaining optimal. Here also, there are some functions to support the optimal routing paths, which is *Localized Routing (LR)*. LR enables optimal routing in PMIPv6 for three cases:

i. when two communicating MNs are attached to the same MAG and LMA,
ii. when two communicating MNs are attached to different MAGs but to the same LMA, and
iii. when two communicating MNs are attached to the same MAG but have different LMAs.

In all these three cases, traffic between two MNs does not traverse the LMAs. This provides some sort of optimization. But the drawback of this approach is that it only tackles the MN-to-MN communication scenario.

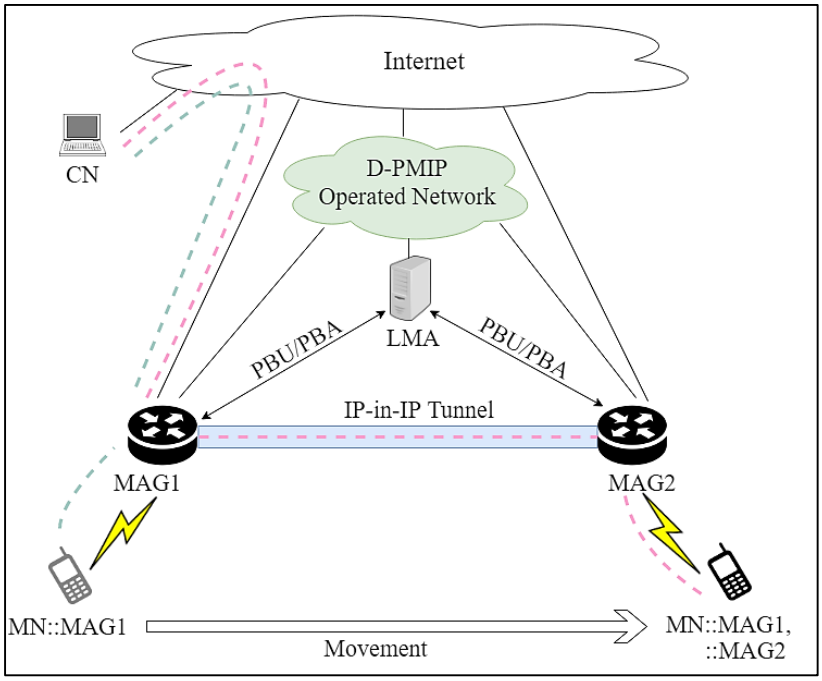


Fig.14. D-PMIP Architecture

D-PMIP is a protocol that is based on PMIPv6-based DMM. LMA is the control plane entity here, and stores all the prefixes of MN. Also, with the help of PBU/PBA signalling messages, the LMA helps in recovering ongoing IP flows after a handover. MN attaches to MAG1. MAG1 informs the LMA about the new attachment with PBU/PBA messages, which also contain the prefix that MAG1 is allocating to the MN. MAG1 then advertises the prefix to the MN. After handover, when LMA receives PBU/PBA messages from MAG2, the database entry for MN is again updated. This update information contains the MN's new location. Also, the LMA instructs the old and new MAGs to establish a tunnel between them. Here, the data plane is distributed among the MAGs, whereas the control plane is centralized to LMA.

PMIPv6 does not require participation of MN in signalling operations. The LMA and the MAG establish a tunnel for forwarding all traffic. In case both endpoints are located in the same PMIPv6 domain, it leads to suboptimal routes. To overcome the issues, LR is used to allow nodes attached to the same or different MAGs to directly exchange traffic by using localized forwarding or a direct tunnel between the MAGs. The initiation of LR is based on the following two criteria:

- MAG must initiate LR only when both the communicating MNs are attached to it and the MNs are anchored at different LMAs. The MAG must not initiate LR in any other case.
- LMA must initiate LR only when both the communicating MNs are anchored to it. The LMA must not initiate LR in any other case.

Network-based solution can be divided into two categories, *partially distributed model* and *fully distributed model*. It depends on whether the DP and CP are tightly coupled or not. In the fully distributed model, mobility anchors manage both DP and CP. In the partially distributed

model, DP and CP are separated and only DP is distributed. In the fully distributed model, both CP and DP are not bound to a central node; they are handled by routers in a distributed way. Network-based approaches pose more threats than host-based ones. This is because MN needs to handle different IP addresses for both the cases, and this is harder to achieve without the involvement of the host.

3.2.3. Routing-based DMM (D-Routing)

This is a *network-based* DMM solution and *fully distributed*. Routing-based solutions follow a totally different approach. In this case, when the mobile node attaches to an access router, it obtains an IP address that is then internally advertised within the domain using an intra-domain protocol (e.g., IBGP). When the node moves and attaches to a different access router, the access router finds out the address assigned to the mobile node during the authentication phase, and then proceeds to update its route via routing updates. In this way, the reachability of the node is ensured while moving within the domain. This approach has some limitations in terms of handover and scalability.

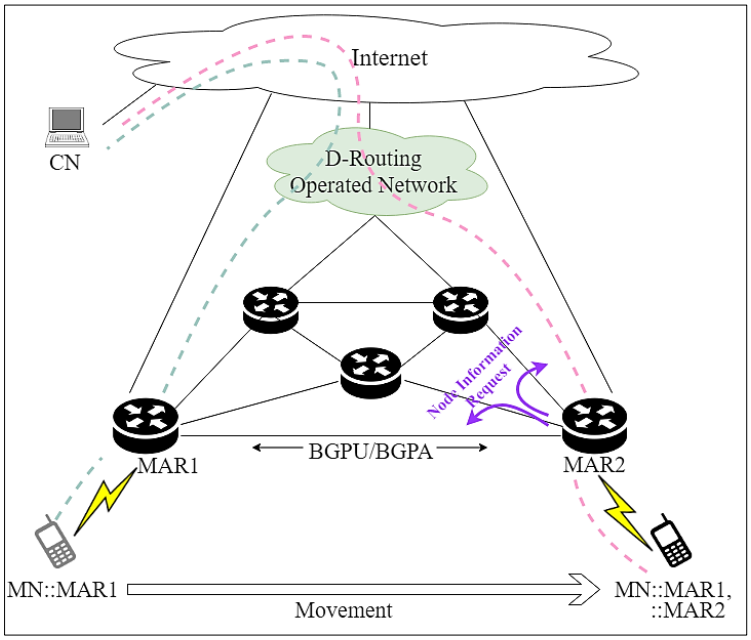


Fig.15. D-Routing Architecture

D-Routing is a protocol that is based on routing-based DMM. All the MARs in this protocol have both routing and managing functions since there is no central entity to support mobility here. The routers use various methods to exchange MN information among them, like broadcasting method or maintaining the last prefix. On MN attachment, the MAR1 learns about the MN through the DNS server. It retrieves the MN's IP address with the help of DNS, and declares itself as the next hop of MN. As soon as this happens, a routing update takes place in the network. This routing update is done with the help of routing protocols like BGP (Border Gateway Protocol). Thus the new location of MN is found out using the routing tables. The

data and control planes are not bound to a specific central entity, and are handled by the MARs in a distributed manner.

3.2.4. SDN-based DMM (D-SDN)

This is a *network-based* DMM solution and *partially distributed*. *Software-defined Networking (SDN)* is the ability of software programs to control network devices. A driving factor of SDN is DP-CP separation. CP is separated from the hardware and implemented as a software, and runs on a standard server in a centralized location. SDN has transformed the networks from a tightly coupled architecture to a distributed architecture. Thus lies its application in DMM. Location and handover management is done at the centralized SDN controller, while packet forwarding is fully distributed at access routers. In the control plane, a centralized controller maintains a global view on the network and computes the optimal path from CN to the new AR. The computed optimal path is established in the DP and the packets are routed to the new AR without any tunnelling overhead. Thus, SDN-based DMM can achieve path optimization and provide significant benefits in terms of network and traffic management.

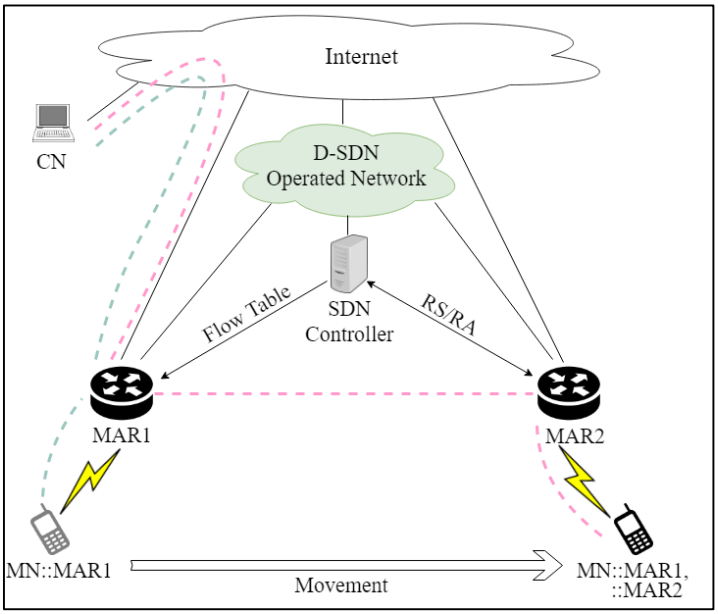


Fig.16. D-SDN Architecture

D-SDN is a protocol that is based on SDN-based DMM. SDN totally separates the control and data planes. Network devices can be programmed to control data traffic behaviour in a centralized way, without having to access them individually. Thus, the system can make the decision of where the traffic is sent (control plane), and what data to forward (data plane). The SDN-Controller configures all nodes in the network via a common API (like OpenFlow) [7]. It configures the forwarding rules on all MARs. On MN attachment, MAR1 informs the SDN-Controller, which assigns a prefix to MN. After attachment detection, the controller configures OpenFlow rules in each MAR visited by the MN. When the previous MAR receives the data

packet, it forwards the packet to the controller. The controller then sends the flow table to the previous MAR. Then the previous MAR easily forwards the data packets to the new MAR based on the flow table. Thus there is no need of tunnelling in this protocol. Since the data traffic does not pass through any central entity, the data plane is distributed; but the control plane is centralized at the SDN-Controller.

3.2.5. Comparison Chart

Solutions / Issues	MIPV6-BASED DMM	PMIPV6-BASED DMM	ROUTING-BASED DMM	SDN-BASED DMM
Distributed Deployment	Present with drawbacks	Present (partial distribution)	Present (full distribution)	Present (partial distribution)
Signalling Cost	Reduces to an extent with lesser mobility	Reduces drastically with lesser mobility	High	Highest
Single Point of Failure	Largely Present	Almost non-existent	Not Present	Almost non-existent
Packet Delivery Cost	Highest	Moderate	Moderate	Lowest
Tunnelling Overhead	Highest	Lowest	Null (no tunnelling)	Null (no tunnelling)
Handover Latency	Moderate	Low	Highest	Lowest

Table.1. Comparison Chart

3.3. DMM for future 5G networks

Before moving on to 5G, a list of wireless telephone technology generations needs to be defined, and their evolution. Since 1G was introduced in the early 1980s, a new wireless mobile technology has been released roughly every ten years. All of them refer to the technology used by the mobile carrier and device itself and they have different speeds and features that improve on the generation prior to it.

- **1G: Only Voice**

1G is an analog technology and its maximum speed is 2.4 Kbps.

- **2G: SMS & MMS, Slow Data**

2G replaced 1G by 1991 and it took cell phones from analog to digital. The 2G telephone technology introduced call and text encryption, data services like SMS, picture messages, and MMS. The max speed of 2G with General Packet Radio Service (GPRS) is 50 Kbps or 1 Mbps with Enhanced Data Rates for GSM Evolution (EDGE).

- **3G: Finally Good Speed Data**

3G allows mobile phones to access the internet – from surfing web pages to making video calls and downloading music. It revolutionized data usage in 1998. The max speed of 3G is estimated to be around 2 Mbps for non-moving devices and 384 Kbps in moving vehicles. The theoretical max speed for HSPA+ is 21.6 Mbps.

- **4G: The Current Standard**

4G released in 2008 and it supports mobile web access like 3G along with gaming services, HD mobile TV, video conferencing, 3D TV and other things that demand higher speeds. The max speed of a 4G network when the device is moving is 100 Mbps or 1 Gbps.

- **5G: Coming Soon**

5G is an upcoming technology and is also referred to as beyond 2020 mobile communications technologies. It tends to improve on the current 4G standards. 5^{th} generation technology is designed to provide incredible and remarkable data capabilities, unhindered call volumes, and immeasurable data broadcast within the latest mobile operating system. Hence, it is more intelligent technology, which will interconnect the entire world without limits. Likewise, our world would have universal and uninterrupted access to information, communication, and entertainment that will open a new dimension to our lives and will change our lifestyle meaningfully.

With increasing demand for mobile traffic, operators need to increase bandwidth per user but also decrease network load in a cost effective way, keeping in mind their future 5G deployments. In 5G networks, there will be disparate types of services with varied connectivity requirements. They are expected to be more flexible, relaxing the constraint of binding user traffic to a central core entity, and allowing internet services to be located closer to the users. Thus, DMM is emerging as a valid framework with a flatter architecture for future 5G deployments. The DMM solution space for 5G networks has three main families: i) PMIPv6-based, ii) SDN-based, and iii) routing-based. These three has already been discussed before. The first two solutions are partially distributed, whereas the last one is fully distributed.

3.4. Applications of DMM along with 5G

USE CASE	APPLICATIONS
▪ Exchanging huge data among millions of devices in Internet-of-Things (IoT) ▪ Autonomous driving ▪ Autonomous cooking	Reduction of human involvement
Downloading of videos	High-speed video streaming
Sitting in a moving car	Interactive gaming
▪ Sitting in a flying aeroplane ▪ Participating in distributed classroom conferencing ▪ Connecting with doctors anytime anywhere	Video conferencing

Table.2. Application Chart

Chapter 4

PERFORMANCE ANALYSIS

An analytical model has been created to calculate the total cost and handover latency of the four DMM protocols: MIPv6-based DMM, PMIPv6-based DMM, SDN-based DMM, and Routing-based DMM. These protocols have been abbreviated for the analysis as D-MIP, D-PMIP, D-SDN, and D-Routing. Signalling cost and data cost have been calculated to give way to the total cost. Handover latency and packet loss have also been calculated. The results have been shown with the help of line graphs.

4.1. Preliminaries

4.1.1. Performance Metrics

1) *Signalling Cost:* It consists of two parts: the initial connection establishment cost and the binding update cost.
2) *Data Delivery Cost:* It represents the cost of delivering data packets to a mobile node per unit time.
3) *Total Cost:* It is the summation of the signalling cost and the data delivery cost.
4) *Handover Latency:* It is the time interval during which a mobile node cannot send or receive any packets, while it performs its handover operations between different access networks.
5) *Packet Loss:* It is the sum of all lost packets destined for a mobile node during its handover process.

4.1.2. Network Model

The figure shown below is the considered network model. It is a generic network topology wherein all communication entities are shown. The notations used are described below:

- Signalling Cost (SC): It is the product of signalling message size and the hop distance.
- Data Delivery Cost (DC): It is the product of data packet size and hop distance.
- Total Cost (TC): It is the summation of SC and DC.
- Packet Tunnelling Cost (PTC): It is the product of size of IPv6 tunnelling and the hop distance.
- Direct Packet Cost (DPC): It is the sole cost of data packets, excluding any other parameters.
- Mobility Binding Time ($T_{Binding}^{(.)}$): It is the elapsed time of mobility binding phase. This is necessary to update MN location and recover ongoing IP flows. (.) represents each protocol.
- Handover latency ($T_{HOL}^{(.)}$): It is the difference between the time when MN currently sends/receives data and the time when MN last sent/received data. (.) represents each protocol.
- Packet Loss ($PL^{(.)}$): It is the summation of data traffic lost during handover. (.) represents each protocol.

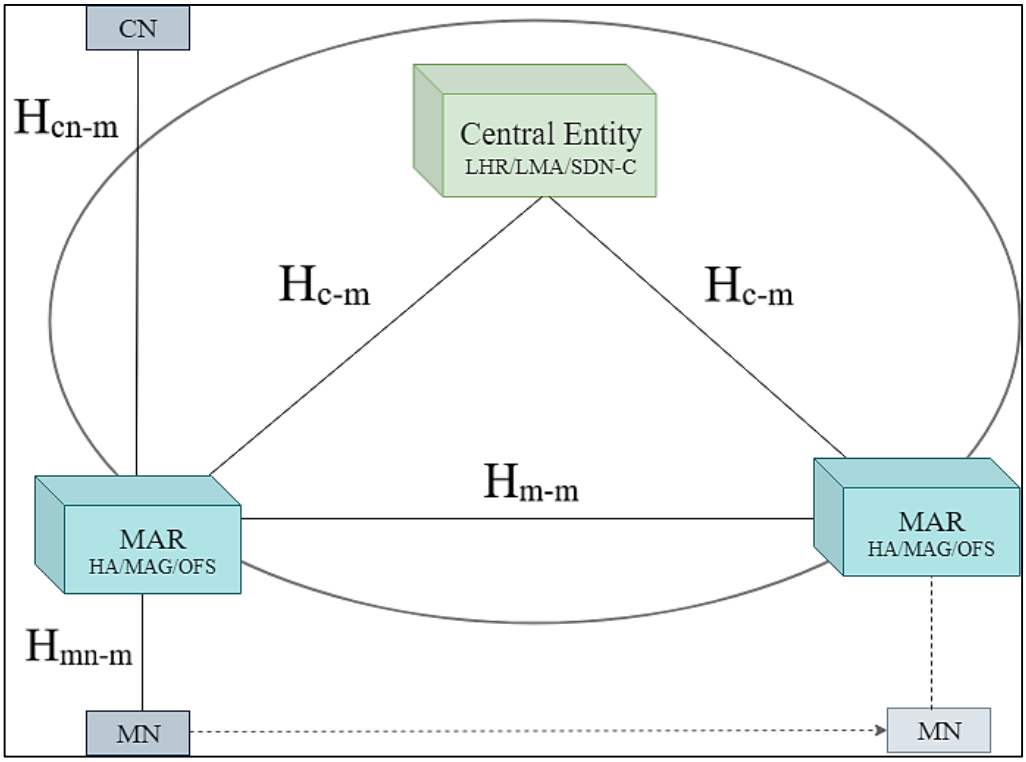


Fig.17. Network Model for Performance Analysis

Central Entity (CE) works as the local head router (LHR) in D-MIP (just like MAP in HMIPv6), LMA for D-PMIP, and SDN-controller (SDN-C) for D-SDN. There is no CE in D-Routing. Mobile Access Router (MAR) represents HA in D-MIP, MAG in D-PMIP, and OpenFlow switch (OFS) in D-SDN. The movement of MN is restricted in the domain where CE acts as an edge router connected to the Internet. The communication paths are defined as follows:

- $H_{c\text{-}m}$: It is the average number of hops between CE and MAR.
- $H_{m\text{-}m}$: It is the average number of hops between MAR and MAR.
- $H_{cn\text{-}m}$: It is the average number of hops between CN and MAR.
- $H_{mn\text{-}m}$: It is the average number of hops between MN and MAR.
- $H_{s\text{-}s}$: It is the average number of hops between SDN-controller and MN as controller.

4.1.3. Mobility Support Messages

The table below shows all the values that have been used in this analysis. It consists of messages used in DMM and OpenFlow. OpenFlow protocol uses TCP protocol, and thus uses TCP header size and acknowledgement.

NOTATION	MEANING	VALUES
α	weighing factor for wired link	1
β	weighing factor for wireless link	1.5
γ	weighing factor for tunnelling link	40
R	radius	200 m
v	average velocity of MN	0-100 m/s
L_{PBU}	PBU message	84 B
L_{PBA}	PBA message	84 B
L_{RS}	RS message	52 B
L_{RA}	RA message	52 B
L_{BGPU}	BGP update message	84 B
L_{BGPA}	BGP acknowledgement message	84 B
λ_s	average session arrival rate at MN	[0-1]
E(S)	average session length in packets	10
L_p	data packet length	64 B
$L_{PacketIn}$	PacketIn message in OpenFlow	92 B
L_{FMod}	flow modification	116 B
L_{TCPack}	TCP acknowledgement message	60 B
$L_{PacketOut}$	PacketOut message in OpenFlow	103 B
BW_{wl}	bandwidth of wireless link	10 Mbps
BW_{wd}	bandwidth of wired link	100 Mbps
D_{wl}	latency of wireless link	[10, 40] ms
D_{wd}	latency of wired link	0.5 ms
P_f	probability that the wireless link fails / frame error rate	0.5
$\mathbf{T_{PC}^{MAR}}$	processing time of MAR	10 ms
$\mathbf{T_{PC}^{CE}}$	processing time of CE	20 ms
T_{L2}	elapsed time for Layer 2 link establishment	45.35 ms
T_{Auth}	elapsed time for MN authorization	13.25 ms
T_{DAD}	DAD latency	1000 ms
$\mathbf{T_{PC}^{BGP}}$	processing time of BGP update	2500 ms
N	no. of cells of each router	40

Table.3. Values for Protocol Messages

It is assumed that each router contains N number of cells and its radius is R. Coverage of each router is S [8] [9].

$$S = \sqrt{\pi * R^2} \tag{1}$$

μ_s is cell crossing rate of MN.

$$\mu_s = \frac{2\,v}{\pi\,S} * \frac{\sqrt{N-1}}{\sqrt{N}} \tag{2}$$

$E(N_s)$ is the average number of movements in the same domain. It is calculated as follows:

$$E(N_s) = \frac{\mu_s}{\lambda_s} \quad (3)$$

The default value for λ_s is taken as 0.5 for numerical analysis in the graphs [10].

4.1.4. One-Way Packet Transportation Delay over Wireless Link

The delay of sending a packet p between MN and MAR or CN and MAR is calculated as follows [11]:

$$d_{MN,CN-MAR} = \left(\frac{L_p}{BW_{wl}} + D_{wl}\right)\left(\frac{1}{1-P_f}\right)H_{mn,cn-m} \quad (4)$$

4.1.5. One-Way Packet Transportation Delay over Wired Link

The delay of sending a packet p between CE and MAR or MAR and MAR is calculated as follows:

$$d_{CE,MAR-MAR} = \left(\frac{L_p}{BW_{wd}} + D_{wd}\right)H_{c,m-m} \quad (5)$$

4.2. Cost Analysis of DMM Protocols

4.2.1. D-MIP

According to the model, data and control packets that are being exchanged between MN and CN must be routed through CE. The MN moves to a new router and configures its IP address. Then tunnel is set up between the new and the previous router with the help of MN. Thus, the signalling cost can be expressed as follows [12]:

$$SC = [\beta(L_{RS} + L_{RA})H_{mn-m} + \alpha(L_{PBU} + L_{PBA})H_{c-m}]E(N_s) \quad (6)$$

The MN is required to create a tunnel for data delivery. Thus, the data delivery cost can be expressed as follows:

$$DC = \lambda_s\, E(S)\, DPC \quad (7)$$

$$DPC = \alpha L_p H_{cn-m} + PTC + \beta L_p H_{mn-m} \quad (8)$$

$$PTC = 2[\alpha(\gamma + L_p)H_{m-m}] \quad (9)$$

The total cost, using (6) and (7) is:

$$TC = SC + DC \quad (10)$$

4.2.2. D-PMIP

In a partially distributed environment, the new router sends PBU to CE when MN moves to a new router. CE creates the tunnel to receive data from the previous router. Thus, the signalling cost can be expressed as follows:

$$SC = [\beta(L_{RS} + L_{RA})H_{mn-m} + 2\alpha(L_{PBU} + L_{PBA})H_{c-m}]E(N_s) \quad (11)$$

Tunnelling is necessary to receive data. Thus, the data delivery cost can be expressed as follows:

$$DC = \lambda_s \, E(S) \, DPC \quad (12)$$

$$DPC = \alpha L_p H_{cn-m} + PTC + \beta L_p H_{mn-m} \quad (13)$$

$$PTC = \alpha(\gamma + L_p)H_{m-m} \quad (14)$$

The total cost, using (11) and (12) is:

$$TC = SC + DC \quad (15)$$

4.2.3. D-SDN

MN updates about its current whereabouts to the DMM service because in return MN wants mobility support. Thus, the signalling cost can be expressed as follows:

$$SC = [\alpha L_{PacketIn} H_{s-s} + 2\alpha L_{FMod} H_{s-s} + \alpha L_{PacketOut} H_{s-s} + 5L_{TCPack}]E(N_s) \quad (16)$$

Tunnelling is not necessary to receive data because data path is set up by a flow table made by the CE (SDN-controller). Thus, the data delivery cost can be expressed as follows:

$$DC = \lambda_s \, E(S) \, DPC \quad (17)$$

$$DPC = \alpha L_p H_{cn-m} + PTC + \beta L_p H_{mn-m} \quad (18)$$

$$PTC = 0 \quad (19)$$

The total cost, using (16) and (17) is:

$$TC = SC + DC \quad (20)$$

4.2.4. D-Routing

In fully distributed environments, distribution is done for both CP and DP. Therefore, node information should be received from the other routers. To exchange node information among routers, a broadcasting method is used by DMM. Thus, the signalling cost can be expressed as follows:

$$SC = [\beta(L_{RS} + L_{RA})H_{mn-m} + \alpha(L_{BGPU} + L_{BGPA})H_{m-m} + \alpha(L_{RS} + L_{RA})H_{m-m}]E(Ns) \quad (21)$$

Tunnelling must be used to get the data flow from the previous router. Thus, the data delivery cost can be expressed as follows:

$$DC = \lambda_s \, E(S) \, DPC \tag{22}$$

$$DPC = \alpha L_p H_{cn-m} + PTC + \beta L_p H_{mn-m} \tag{23}$$

$$PTC = \alpha(\gamma + L_p) H_{m-m} \tag{24}$$

The total cost, using (21) and (22) is:

$$TC = SC + DC \tag{25}$$

4.3. Handover Latency Analysis of DMM Protocols

4.3.1. D-MIP

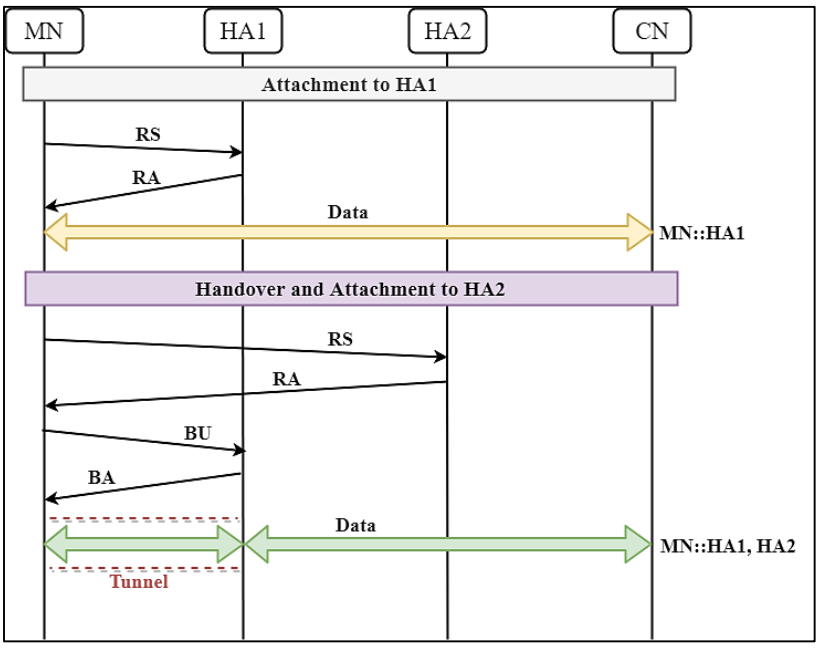


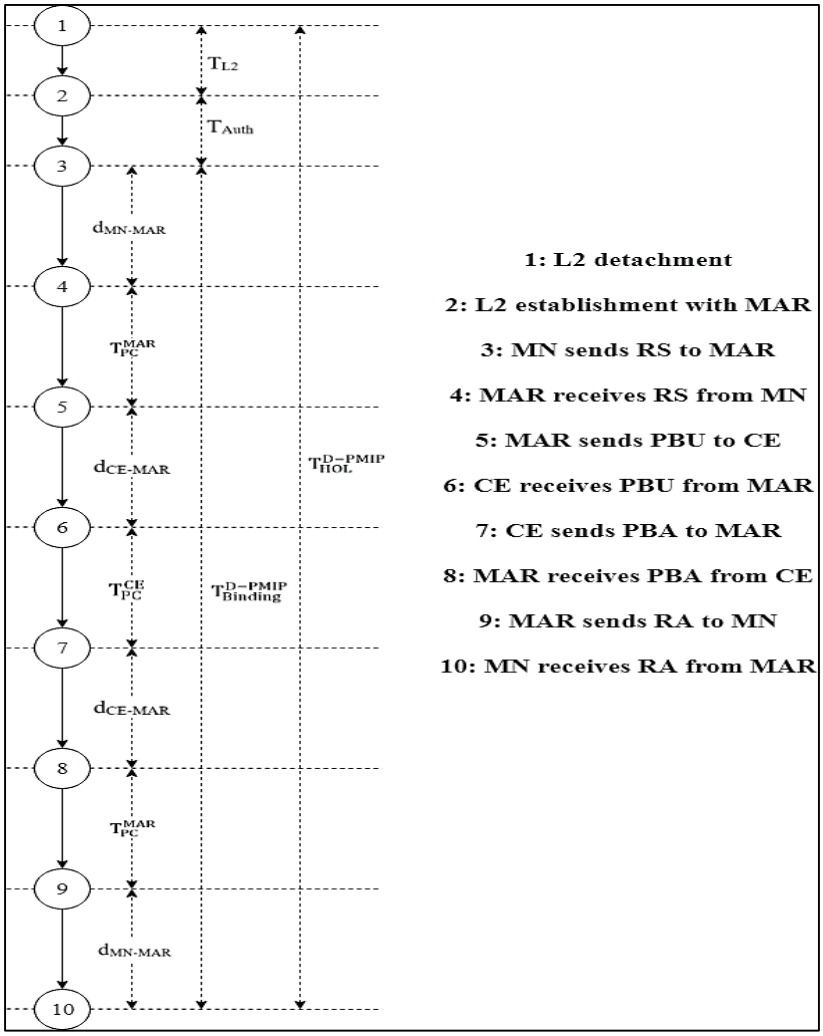
Fig.18. Timing Diagram for D-MIP Handover

The handover latency is calculated as follows:

$$T_{HOL}^{D-MIP} = T_{L2} + T_{Auth} + T_{Binding}^{D-MIP} \tag{26}$$

$$T_{Binding}^{D-MIP} = 2d_{MN-MAR} + T_{PC}^{CE} + 2T_{PC}^{MAR} + \quad T_{DAD} + 2(d_{MN-MAR} + d_{CE-MAR}) \tag{27}$$

4.3.2. D-PMIP



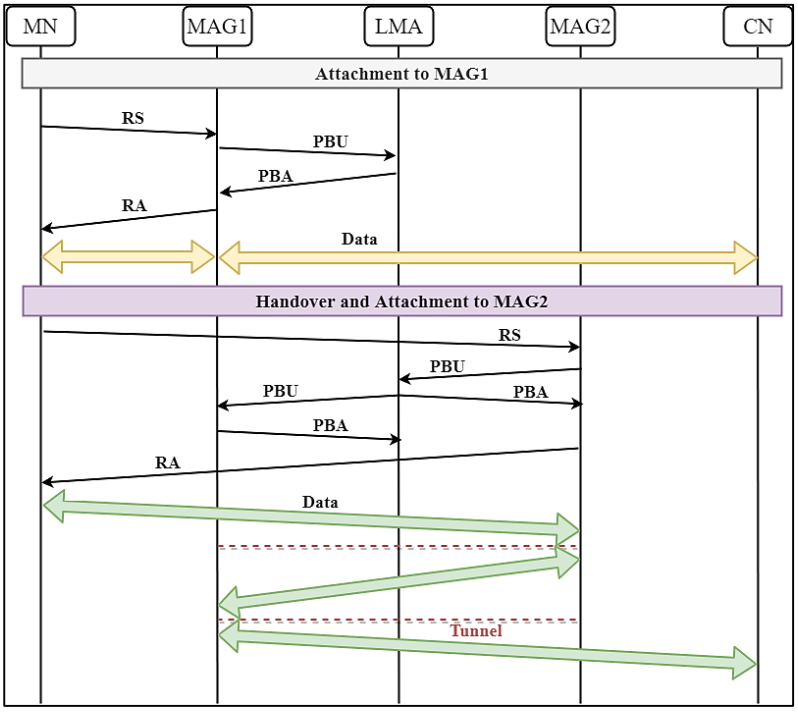


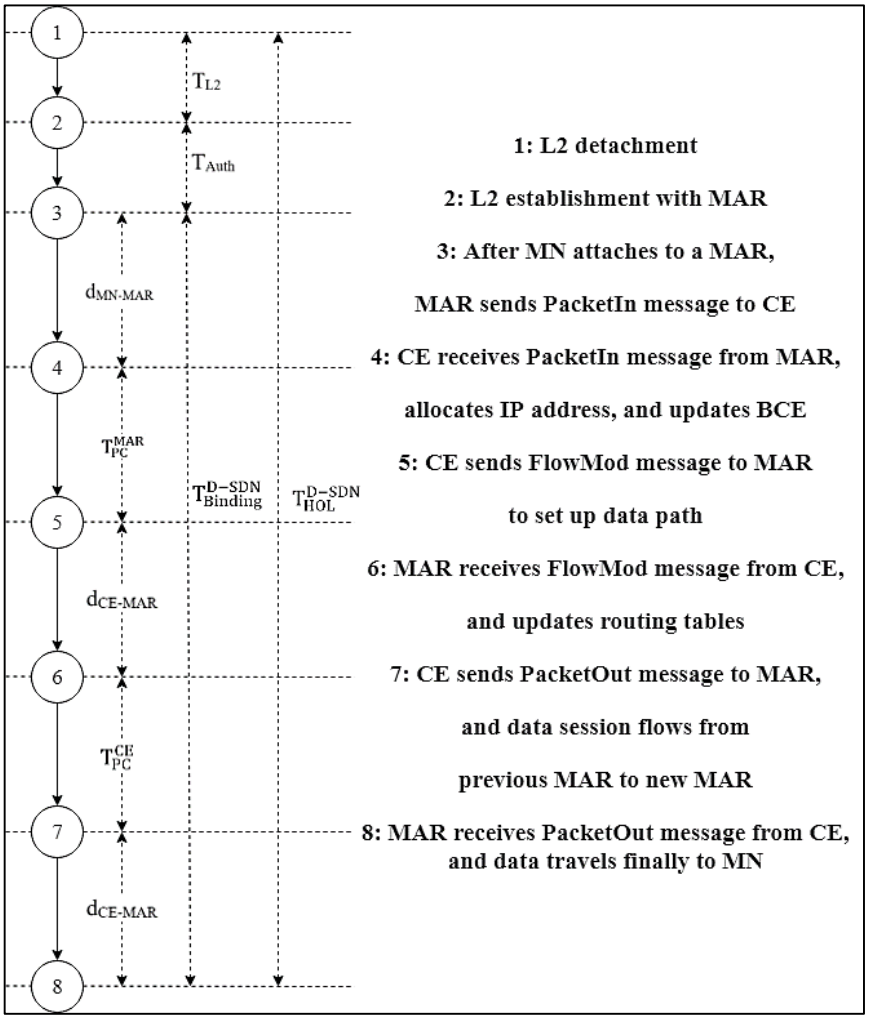
Fig.19. Timing Diagram for D-PMIP Handover

The handover latency is calculated as follows:

$$T_{HOL}^{D-PMIP} = T_{L2} + T_{Auth} + T_{Binding}^{D-PMIP} \quad (28)$$

$$T_{Binding}^{D-PMIP} = 2d_{MN-MAR} + 2d_{CE-MAR} + T_{PC}^{CE} + 2T_{PC}^{MAR} \quad (29)$$

4.3.3. D-SDN



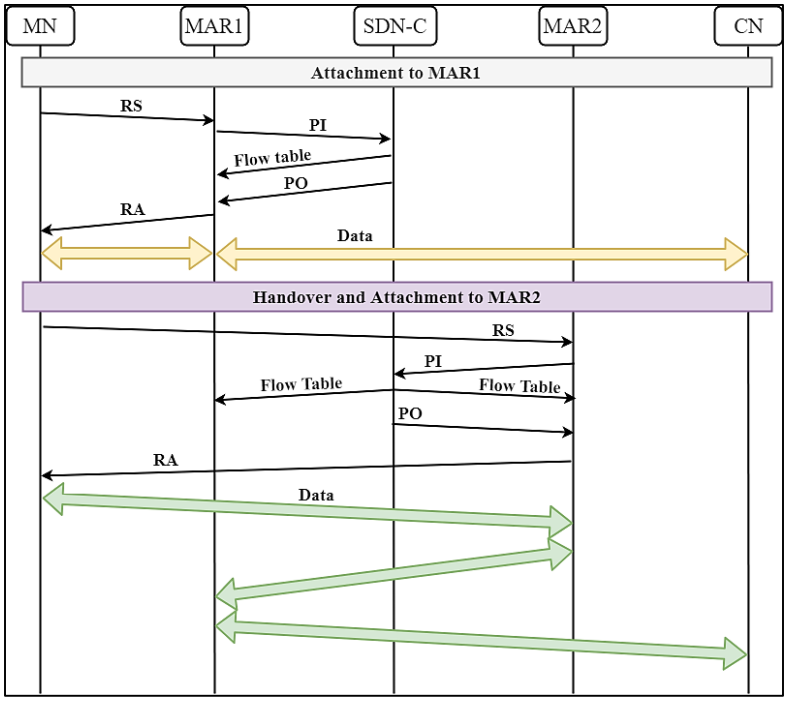


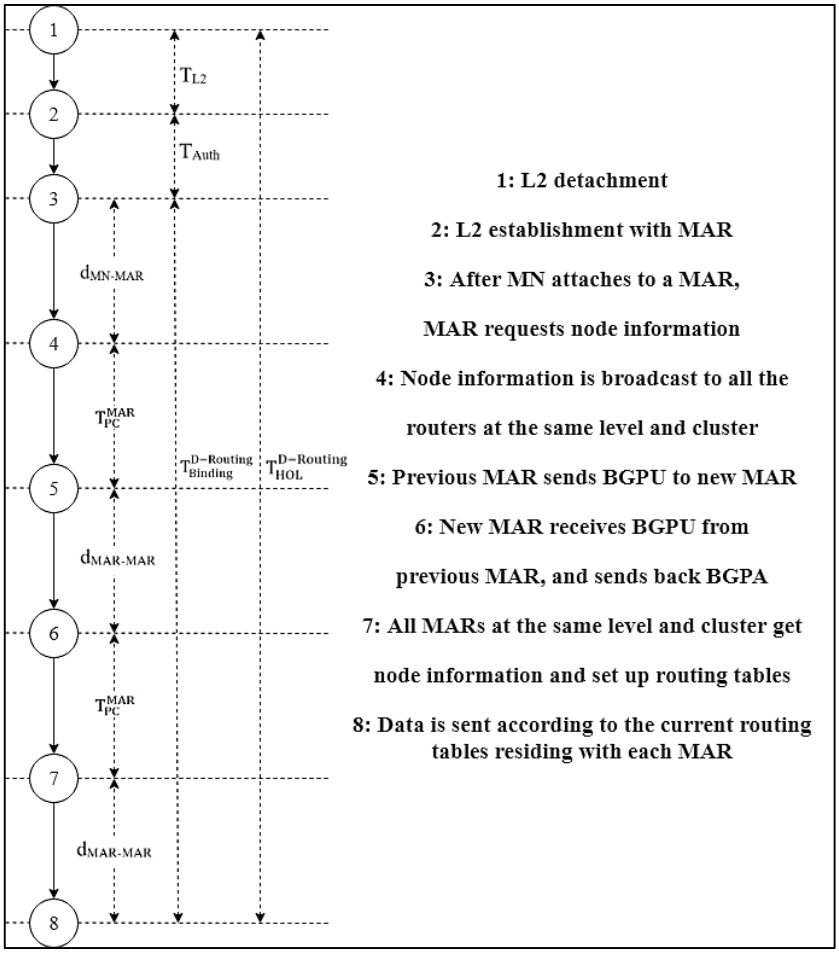
Fig.20. Timing Diagram for D-SDN Handover

The handover latency is calculated as follows:

$$T_{HOL}^{D-SDN} = T_{L2} + T_{Auth} + T_{Binding}^{D-SDN} \quad (30)$$

$$T_{Binding}^{D-SDN} = d_{MN-MAR} + 2d_{CE-MAR} + T_{PC}^{CE} + T_{PC}^{MAR} \quad (31)$$

4.3.4. D-Routing



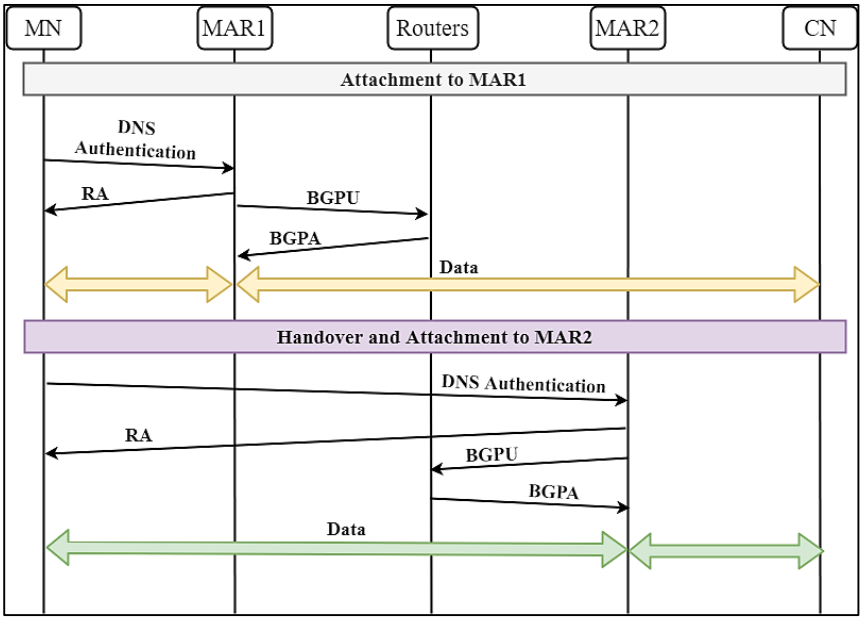


Fig.21. Timing Diagram for D-Routing Handover

The handover latency is calculated as follows:

$$T_{HOL}^{D-Routing} = T_{L2} + T_{Auth} + T_{Binding}^{D-Routing} \quad (32)$$

$$T_{Binding}^{D-Routing} = 2d_{MN-MAR} + 10d_{MAR-MAR} + T_{PC}^{BGP} + 10T_{PC}^{MAR} \quad (33)$$

4.4. Packet Loss Analysis of DMM Protocols

Packet loss is directly proportional to session arrival rate and handover. (.) denotes each protocol.

$$PL(.) = \lambda_s E(S)\, T_{HOL}^{(.)} \quad (34)$$

4.5. Graphical Analysis

Using the above equations and calculations, performance analysis and evaluation of the considered four protocols have been done with the help of the following graphs.

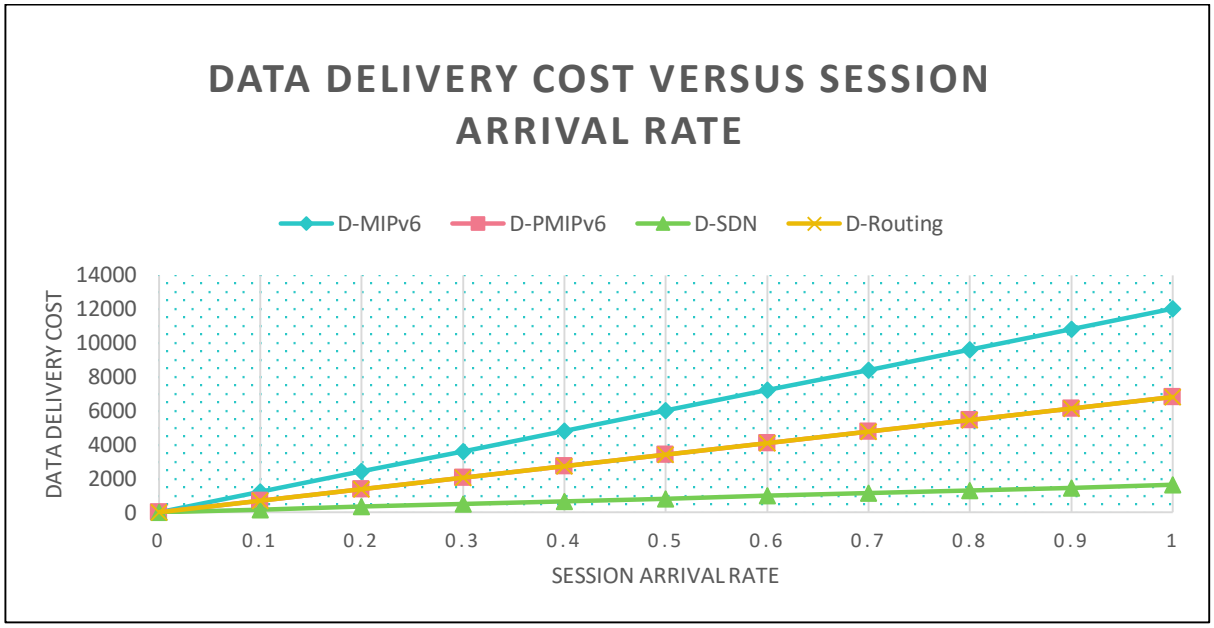


Fig.22. DC versus λ_s

Fig. 22 shows that D-MIP has the highest packet delivery cost because it uses a bi-directional tunnel to forward data, wherein MN itself is involved. D-SDN has the lowest cost because it can forward data without tunnelling. The other two network-based protocols does not involve MN during handover process, and thus have more or less same data delivery cost.

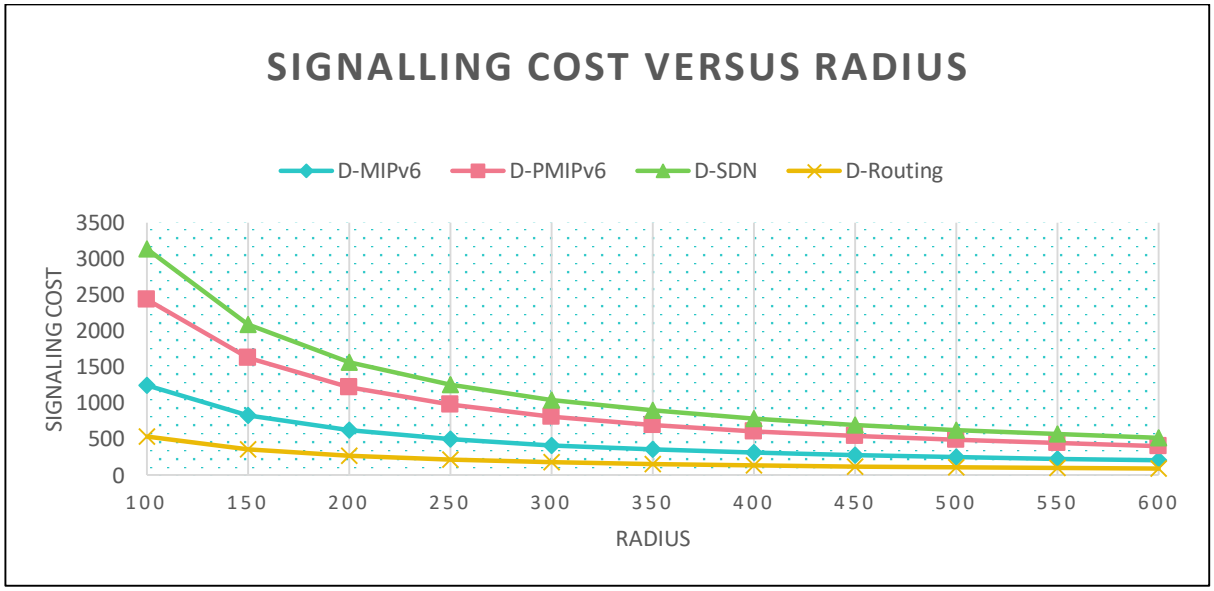


Fig.23. SC versus R

v is kept constant as 50 m/s in Fig. 23. As R increases, SC decreases. This is because SC decreases with reduced number of movements. D-SDN ranks the highest because it requires signalling messages that use a TCP connection. TCP is needed for flow setup and MN attachment.

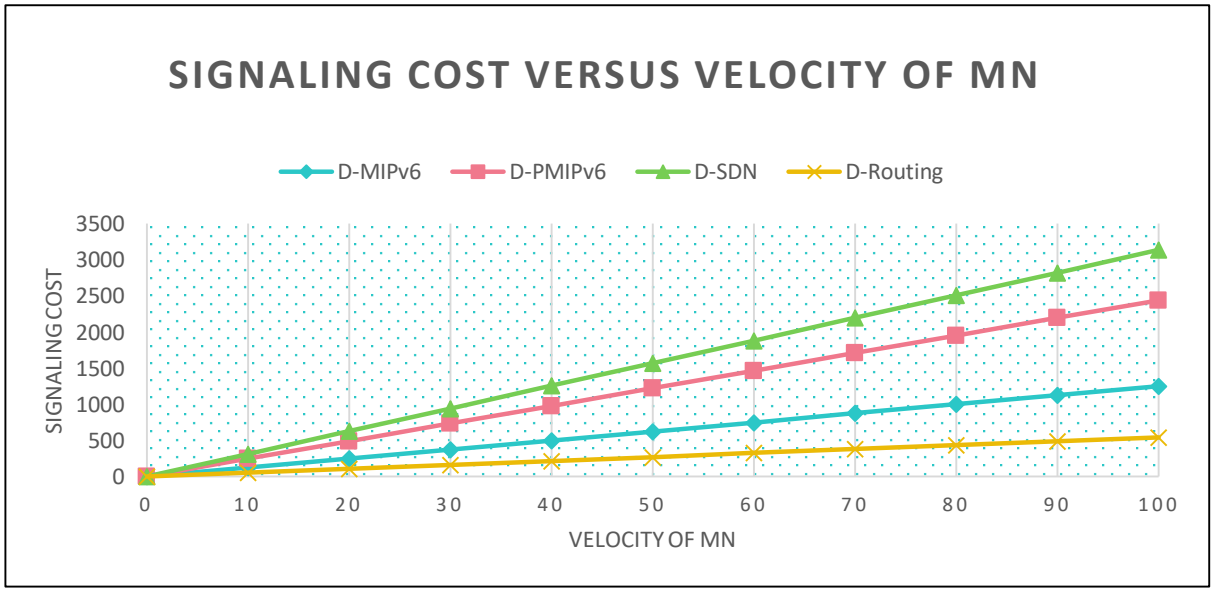


Fig.24. SC versus v

R is kept constant as 200 m in Fig. 24. SC increases with v. Again, D-SDN ranks the highest because it requires signalling messages that use a TCP connection. TCP is needed for flow setup and MN attachment.

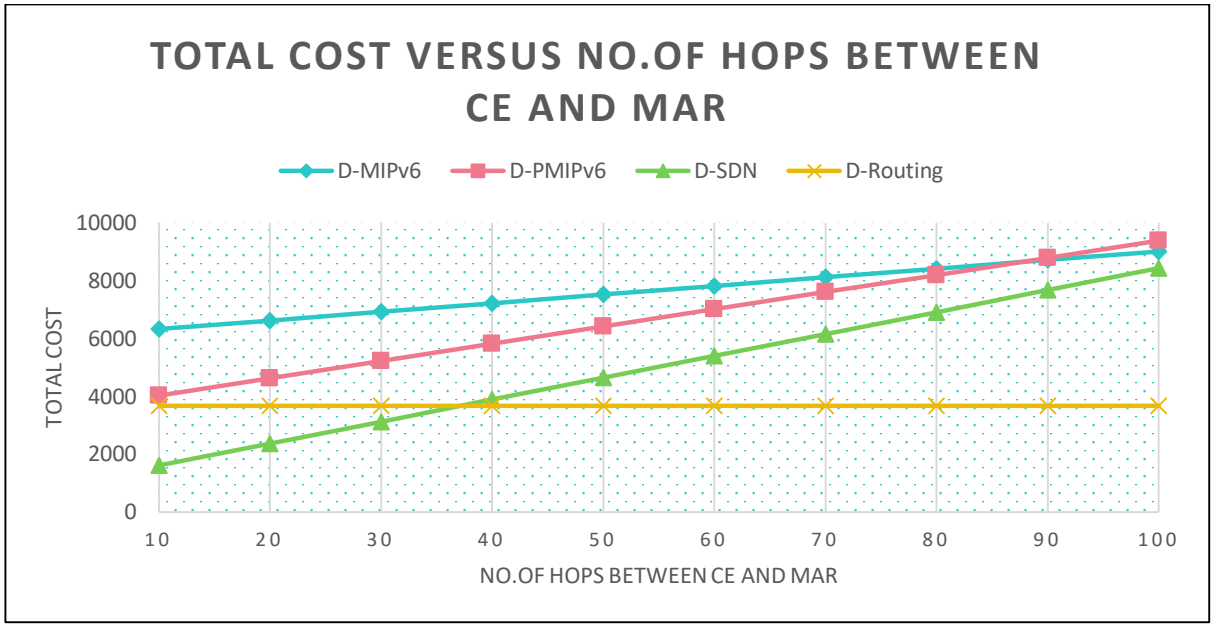


Fig.25. TC versus $H_{c\text{-}m}$

Fig. 25 shows that D-Routing is not affected by the change in number of hops between CE and MAR because it is a fully distributed protocol. So, there is no concept of CE in D-Routing. D-MIP uses this path between CE and MAR the most and that is why it has the highest total cost. D-SDN has the lowest total cost due to the fact that it has zero tunnelling cost. D-PMIP accounts for the middle ground because it uses a fair amount of tunnelling.

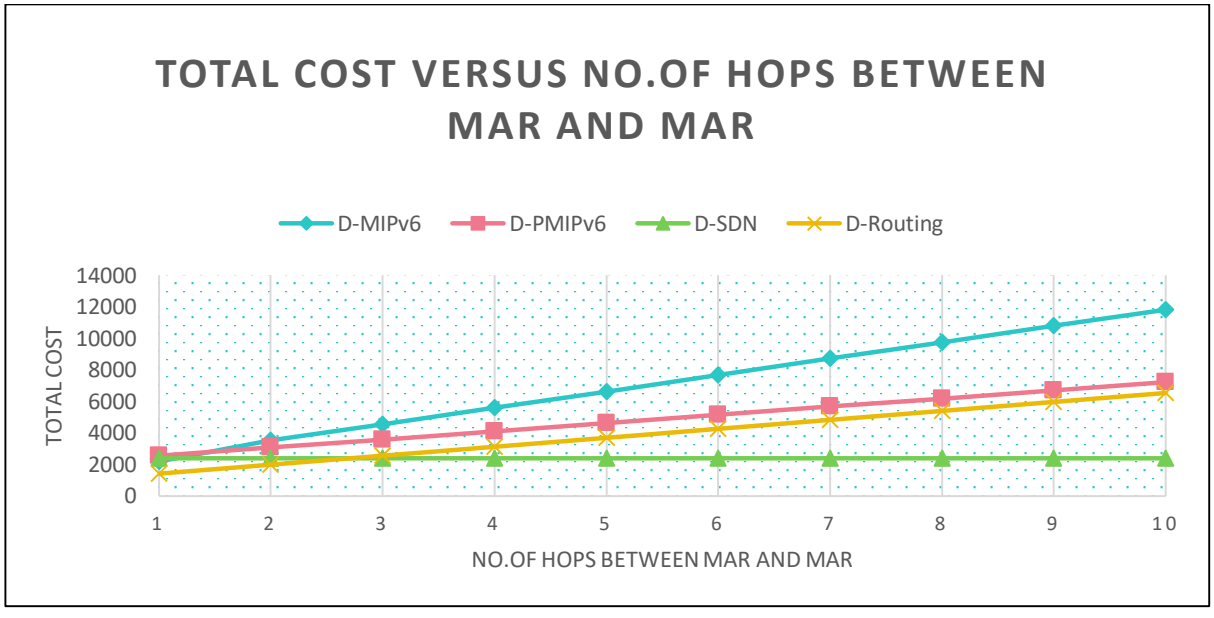


Fig.26. TC versus $H_{m\text{-}m}$

Fig. 26 shows that D-SDN is not affected by the change in number of hops between MAR and MAR. This is because D-SDN does not involve any tunnelling. D-Routing comes in the next

best place since it is a fully distributed protocol, and uses this path in CP and DP lesser than the partially distributed ones. Since the MN itself is involved in the total process in D-MIP, it generates the highest cost.

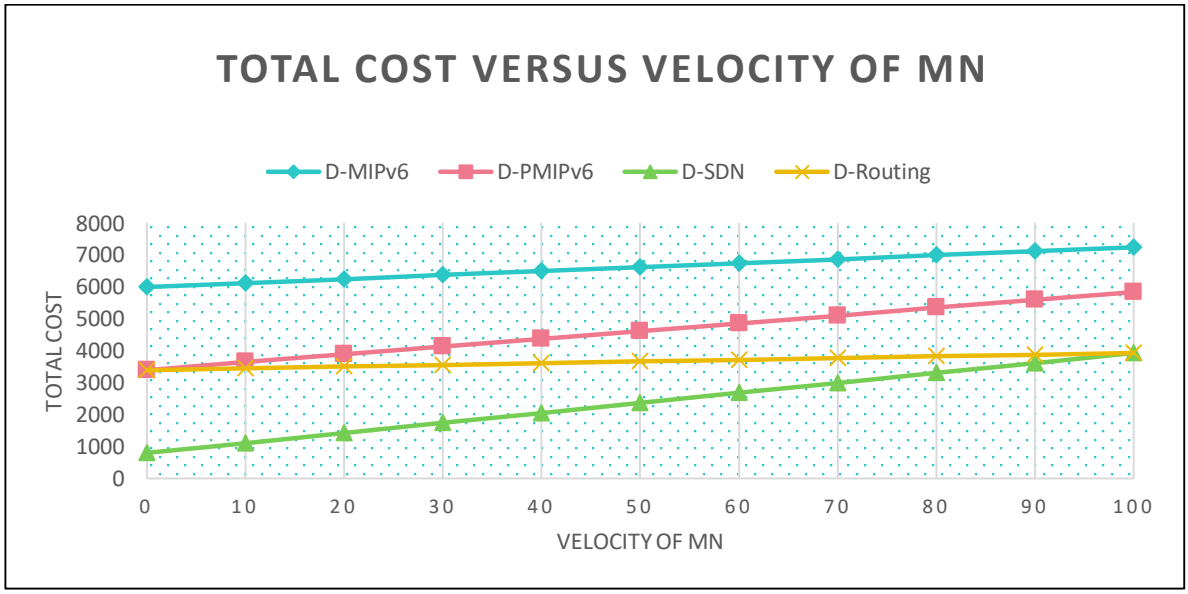


Fig.27. TC versus v

Fig. 27 shows that total cost increases linearly with changing velocity of MN. D-MIP has highest DC and so it takes the highest place. D-PMIP and D-Routing has same DC but D-PMIP has higher SC than the latter. So, TC is higher in D-PMIP. D-SDN has highest SC but lowest DC, and since tunnelling cost is zero, total cost decreases drastically compared to the other protocols.

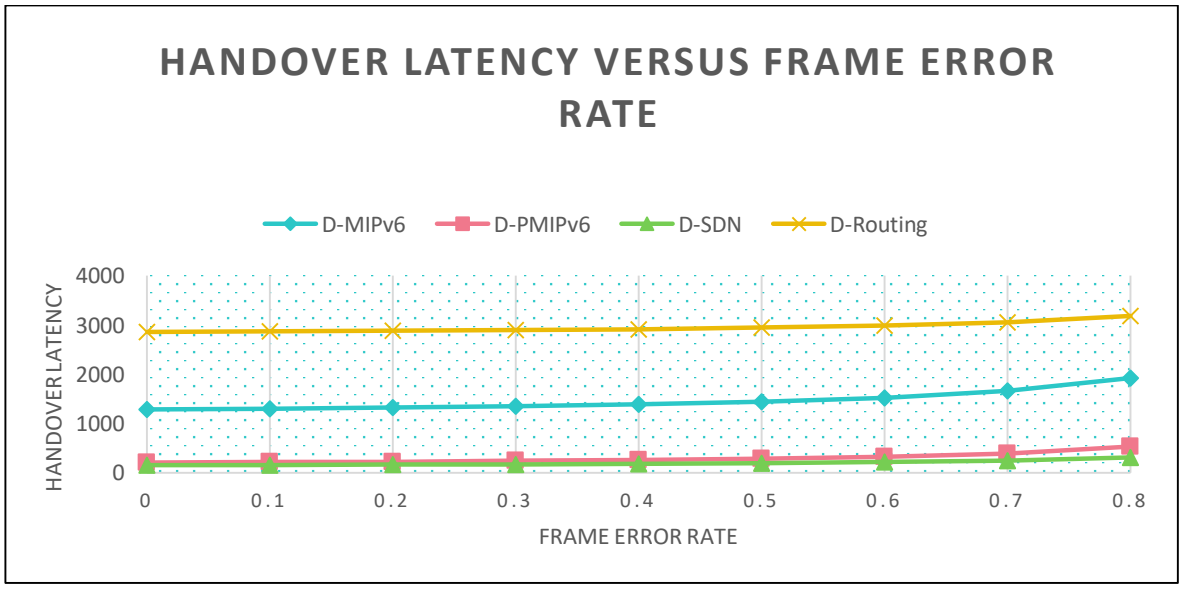


Fig.28. Handover Latency versus P_f

Fig. 28 shows that a higher value of P_f increases the probability of erroneous packet transmission over wireless link. Accordingly, signalling increases as retransmissions increase. This leads to increase in handover latency. Layer 2 switch is the latency for MN to change from one MAR to another. Layer 3 handover is the time spent since the MN de-associates from the old MAR, to the time when it gets RA, meaning that MN's IP has been already configured. Now, in case of D-MIP, we have to consider the time taken by DAD that is performed after an IP has been configured. Finally, after the handover, MN is ready to send/receive packets. On MN attachment detection, a MAR queries a database in order to get the details of the connecting MN. This database can be a local head router, LMA, SDN-controller, or the DNS server, respectively for D-MIP, D-PMIP, D-SDN, and D-Routing. Thus, layer 2 switch and layer 3 handover time differences are almost negligible for all the protocols. The main difference lies in the time taken to recover ongoing data flows. D-PMIP and D-SDN operate in a conceptually similar way and thus have very close results. They have the lowest increase in handover latency because both recover the ongoing data flow pretty quickly. D-PMIP uses a tunnel and D-SDN installs new switching rules in old and new MARs. D-Routing does not have CE, that is, no central entity controls its data path. When the new MAR receives the IP address of the connecting MN from the DNS server, the new MAR installs a route for the MN, and sends the other routers a BGP update notifying itself as the next-hop for the MN. Thus, to recover the data flow, all the routers in the data path must be updated, leading to a huge difference in handover latency time. Moreover, this problem increases with larger domains in D-Routing. D-MIP lies somewhere in the middle because it is host-based and thus is greater than the network-based protocols but lesser than routing-based.

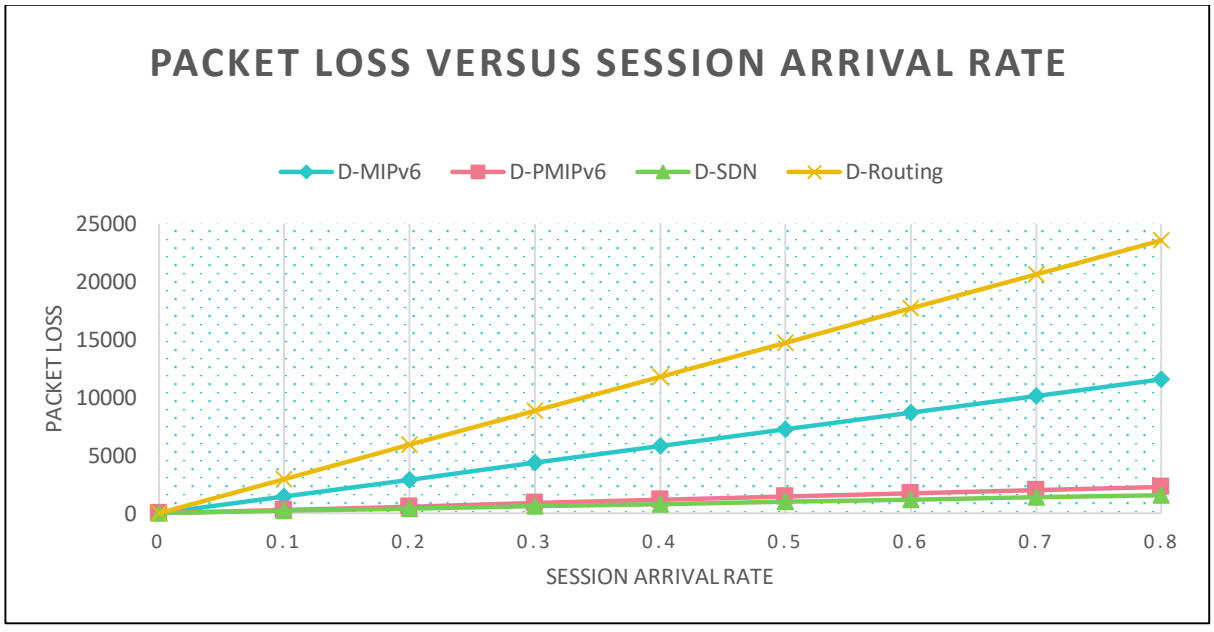


Fig.29. PL versus λ_s

Fig. 29 shows that PL is directly affected by λ_s. Buffering mechanisms can be used as a solution for packet loss in DMM protocols. This is because each MAR is responsible for a group of

MNs rather than all of them. But the buffer size may increase with centralized databases (that is, partially distributed protocols). Both the partially distributed protocols thus show similar results. Even though we can use buffer in D-Routing, its size is terribly increased due to the fact that all the routing tables need to be updated.

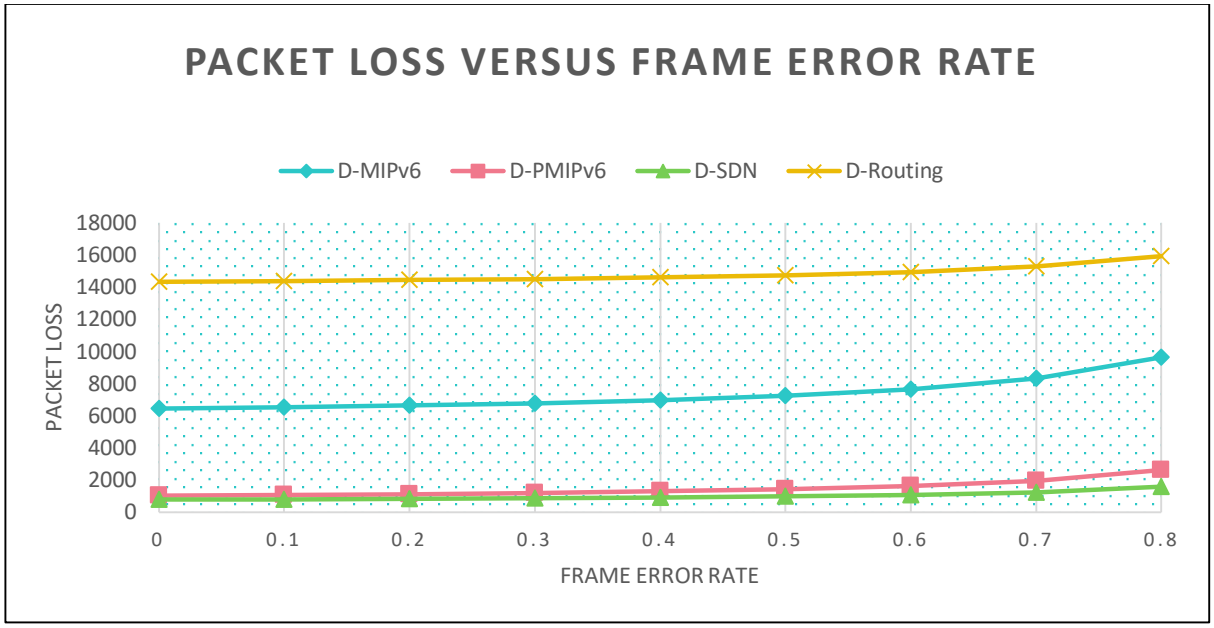


Fig.30. PL versus P_f

Fig. 30 shows that PL is directly proportional to handover latency. In D-PMIP, the number of active prefixes increases with increase in MN's mobility. Thus, signalling cost is increased. But even if the MN has large number of active prefixes, handover latency is affected only by the distance of the furthest MAR. The same thing goes for D-SDN. Thus, they have similar results. The number of messages sent in D-Routing totally depends on the network size (BGP update needs to be sent to all routers). Since handover latency is affected by the network size, D-Routing fares worst in packet loss when the network size is large. And, in reality, we do need large domains.

CONCLUSION

The trend of mobile IP in networking infrastructure has been discussed in this report. The impact of growing use of mobile devices is evident by the fact that more and more users are connecting to the internet on a daily basis. Also, users are bombarding operators with more data traffic request. This leads to delay in data packet transmission, and due to this, many other problems follow its tail. CMM does its job quite nicely but it is not able to handle the immense pressure on the whole network, and this leads to handover latency. This has led to the invention of DMM, and it is a great hope for future mobile networks.

D-MIP is a host-based protocol which induces a lot of overhead on the MN. It is certainly not a scheme that we want in the future. Because it is essential for MN to perform independently of the handover operations that take place at the access router levels. D-PMIP and D-SDN are network-based protocols and relieves the MN of any handover duty. They are more efficient than D-MIP. D-PMIP has evolved from the original PMIPv6 protocol that used to be centralized. D-SDN uses a software defined approach. D-Routing employs the BGP routing protocol to perform mobility functions. D-PMIP and D-SDN react faster to any changes in the network, but they are partially distributed and require special central entities on their behalf to perform mobility functions. D-Routing is fully distributed but inherits the problems related to higher handover latency and signalling overhead. In terms of cost, both D-SDN and D-Routing are on an equal stand. This is a great opportunity for application of fully distributed protocols in the future, where we are striving for a fully distributed environment. D-SDN, though it is partially distributed has its own advantages. But when we consider handover latency, D-Routing comes in the worst position. This makes D-SDN a probable candidate for future mobile networks.

REFERENCES

[1] J. Carmona-Murillo, I. Soto, F. J. Rodríguez-Pérez, D. Cortés-Polo, and J. L. González-Sánchez, "Performance Evaluation of Distributed Mobility Management Protocols: Limitations and Solutions for Future Mobile Networks", Hindawi, Mobile Information Systems, Volume 2017.

[2] Hassan Ali-Ahmad, Meryem Ouzzif, Philippe Bertin, and Xavier Lagrange, "Distributed Dynamic Mobile IPv6: Design and Evaluation", IEEE Wireless Communications and Networking Conference (WCNC): NETWORKS, 2013.

[3] Fabio Giust, Luca Cominardi, Carlos J. Bernardos, "Distributed Mobility Management for future 5G networks: overview and analysis of existing approaches", project iJOIN, 2013.

[4] Hyunsik Yang, Younghan Kim, "SDN-based Distributed Mobility Management", IEEE ICOIN 2016.

[5] Hassan Ali-Ahmad, Meryem Ouzzif, Philippe Bertin, and Xavier Lagrange, "Distributed Mobility Management: Approaches and Analysis", IEEE ICC'13.

[6] Jong-Hyouk Lee, Jean-Marie Bonnin, Pierrick Seite, H Anthony Chan, "Distributed IP mobility management from the perspective of the IETF: Motivations, requirements, approaches, comparison, and challenges", IEEE 2013.

[7] Tien-Thinh Nguyen, Christian Bonnet, Jerome Harri, "SDN-Based Distributed Mobility Management for 5G Networks", IEEE Wireless Communications and Networking Conference 2016.

[8] Mohammed Balfaqih, Mahamod Ismail, Rosdiadee Nordin, Zain Balfaqih, "Handover Performance Analysis of Distributed Mobility Management in Vehicular Networks", IEEE 12th Malaysia International Conference on Communications (MICC), 2015.

[9] Li Yi, Huachun Zhou, Fei Ren, Hongke Zhang, "Analysis of Route Optimization Mechanism for Distributed Mobility Management", JOURNAL OF NETWORKS, VOL. 7, NO. 10, OCTOBER 2012.

[10] Ji In Kim, Seok Joo Koh, "Distributed Mobility Management in Proxy Mobile IPv6 using Hash Function", IEEE ICOIN 2013.

[11] Jong-Hyouk Lee, Jean-Marie Bonnin, Ilsun You, Tai-Myoung Chung, "Comparative Handover Performance Analysis of IPv6 Mobility Management Protocols", IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013.

[12] Fabio Giust, Carlos J. Bernardos, Antonio de la Oliva, "Analytic Evaluation and Experimental Validation of a Network-based IPv6 Distributed Mobility Management Solution", JOURNAL OF LATEX CLASS FILES, VOL. 6, NO. 1, JANUARY 2007.

[13] Petro P. Ernest, Olabisi E. Falowo, H. Anthony Chan, "Network-based Distributed Mobility Management: Design and Analysis", IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2013.

[14] Kuljaree Tantayakul, Riadh Dhaou, Beatrice Paillassa, "Impact of SDN on Mobility Management", 2017.

[15] C. Perkins, Ed., RFC 5944, "IP Mobility Support for IPv4, Revised", November 2010.

[16] C. Perkins, Ed., D. Johnson, J. Arkko, RFC 6275, "Mobility Support in IPv6", July 2011.

[17] S. Gundavelli, Ed., K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, RFC 5213, "Proxy Mobile IPv6", August 2008.

[18] Mobile Communications by Jochen Schiller.

[19] H. Soliman, C. Castelluccia, K. ElMalki, L. Bellier, RFC 5380, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", October 2008.

[20] R. Koodli, Ed., RFC 5568, "Mobile IPv6 Fast Handovers", July 2009.

[21] Jun Lei, Xiaoming Fu, "Evaluating the Benefits of Introducing PMIPv6 for Localized Mobility Management".

[22] Charles E. Perkins, "Mobile IP".

[23] H. Chan, Ed., D. Liu, P. Seite, H. Yokota, J. Korhonen, RFC 7333, "Requirements for Distributed Mobility Management", August 2014.

[24] S. Gundavelli, S. Jeon, Internet-Draft, "DMM Deployment Models and Architectural Considerations draft-ietf-dmm-deployment-models-02.txt", August 29, 2017.

[25] Shi Yan, Cheng Jiayin, Chen Shanzhi, "A Mobile IPv6 based Distributed Mobility Management Mechanism of Mobile Internet".

[26] E. Haleplidis, Ed., K. Pentikousis, Ed., S. Denazis, J. Hadi Salim, D. Meyer, O. Koufopavlou, RFC 7426, "Software-Defined Networking (SDN): Layers and Architecture Terminology", January 2015.