

An overview of internet engineering task force mobility management protocols: approaches and its challenges

Prabha Mahenthiran, Dinakaran Muruganadam

School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India

Article Info

Article history:

Received Oct 18, 2021

Revised Jul 23, 2022

Accepted Aug 18, 2022

Keywords:

Centralized mobility management

Distributed mobility management

Mobile IPv6

Proxy Mobile IPv6

ABSTRACT

In recent years, internet protocol mobility management has become one of the most popular research areas in networking. Mobility management protocols are in charge of preserving continuing communications as a user roam between different networks. All existing internet protocols (IP), like MIPv6, and PMIPv6, rely on a centralized mobility anchor to control mobile node traffic and signaling. The disadvantages of centralized mobility management (CMM) include ineffectiveness in handling massive volumes of traffic, poor scalability, wasteful use of network resources, and packet delay. When CMM is required to handle mobile media, which demands a huge amount of information and frequently needs quality of services (QoS) such as session continuance and reduced latency, these difficulties become apparent. It drives the need for distributed mobility management protocol (DMM) systems to manage the growing amount of mobile data, the overwhelming of this is video communication. DMM approaches could be regarded as an innovative and effective method to deal with mobility. An overview of the CMM protocol and its drawbacks are analyzed. This study examines the various DMM protocol techniques and their performance metrics are compared to highlight similarities and differences. The study reveals the network-based DMM protocol improves overall handoff time and packet loss.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Dinakaran Muruganadam

School of Information Technology and Engineering, Vellore Institute of Technology

Vellore, Tamil Nadu, India

Email: dinakaran.m@vit.ac.in

1. INTRODUCTION

According to Statista-2020 [1], Figure 1 shows 3.5 billion people own a smartphone around the world. This means that roughly 73% of them have a smartphone. This ratio is fast rising, as evidence suggests that there had been 1 billion users worldwide just 4 years ago, in 2016. It is estimated to be a tremendous growth of 3.8 billion by the year 2021. Customer expectations are evolving as digital information becomes more widely and freely accessible online. According to the most recent mobile statistics, 51 percent of individuals use their phones to make online purchases, and nearly two-thirds people (66%) use retail applications on their phones. Mobile web usage reports for 52.6 percent of all internet traffic. Mobile devices accounted for 31.16 percent of global online traffic at the start of 2015. This figure has risen to 52.6%. With the advent of 5G technology, which will deliver substantially better internet speeds and connectivity, we may anticipate a steady increase in mobile data usage. Different types of new wireless internet services are now being developed and are built on internet protocols (IP) technology [2]. On the IP, Physical & MAC layers, it is really important to provide an effective mobility protocol.

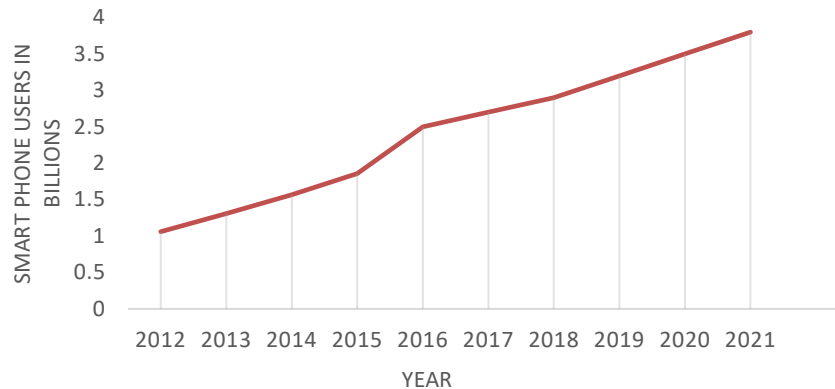


Figure 1. Smartphone users worldwide [1]

Mobility management protocols can be broadly classified into host-based and network-based mobility management protocols. Mobile IPv6 is a host-based mobility management protocol [3]–[6] suggested by the internet engineering task force (IETF) as the main protocol for mobility management. This protocol includes hierarchical mobile IPv6 (HMIPv6) [7], [8], fast handover protocol (FMIPv6) [9], [10], robust hierarchical mobile IPv6 (RH-MIPv6) [11], resource reservation pool [12] generally introduces a network cost in terms of handoff latency, packet drop and signal overhead when the mobile node moves frequently. A network-based protocol such as Proxy Mobile IPv6 [13]–[17] has been standardized by IETF. In the PMIPv6, the proxy mobile agent in the providing network handles mobility on account of the mobile nodes. Despite the introduction of various quick handover techniques, this protocol still struggles with handoff latency and loss rate during handover. MIPv6 protocol and PMIPv6 protocol are based on the centralized mobility management (CMM) approach. MIPv6's home agent (HA) and PMIPv6's local mobility anchor (LMA) serve as a centralized mobile anchor, processing all control and data packets. This centralized device makes a mobile node available when it is not at home, and it is also in charge of routing datagrams to and from the mobile node.

The CMM model is prone to many issues. It also causes a decrease in overall network quality and raises networking costs. IETF standardized distributed mobility management (DMM) [18], [19] concept to overcome the limitations of CMM and developed DMM methods based on existing protocols like MIPv6 and PMIPv6. DMM is generally encouraging the mobility management approach. The main idea behind the DMM is, that it brings the mobility anchor closer to the mobile node. DMM enables the network to be configured so that mobile data traffic is distributed appropriately without relying on a centrally installed anchor. In terms of handoff latency, packet drop, signal cost, and network stress reduction, DMM outperform existing mobility management protocols such as MIPv6 and PMIPv6.

2. METHOD

2.1. Centralized mobility management protocol

Several IP mobility management protocols have been standardized to ensure that mobile consumers continue to receive service even if their network connection changes. The IETF developed centralized mobile support systems for all-IP networks, in which a centralized mobile anchor control mobile node traffic and signaling. The most common CMM protocols are MIPv6 and PMIPv6. PMIPv6 adds a LMA to the domain to keep mobility internal, whereas MIPv6 includes a HA. Both mobile signals and user information transfer are handled by this mobility anchor in CMM.

2.1.1. Mobile IPv6 protocol

The IETF has defined the MIPv6 protocol as host-based. Figure 2(a) shows a working operation of mobile IPv6 and Figure 2(b) shows MIPv6 with route optimization. While traveling over the internet topology, mobile IPv6 permits mobile devices to be reached and sustain continuing connections such as file transfer protocol and streaming. Mobile nodes are given an Internet address called home address (HoA) to maintain such a connection. This home address is a permanent IP address that serves two functions: one is to make the mobile node reachable, and the second is to keep the IP layer movement/mobility hidden from higher layers. A mobile node gets a new IP address called care-of-address (CoA) as it moves from one location to another. The CoA is formed based on a stateless or stateful mechanism. Every time a mobile node

moves, it informs its HA of its current location. Binding update (BU) refers to the link between HA and its CoA. This BU message will be stored in the HA's binding cache and used to confirm receipt of the BU as binding acknowledgement (BA). The packets intended for MN's home address will be redirected by HA and tunneled to its new CoA position. The HA is the tunnel's point of entry, and the mobile node's care-of address is the tunnel's departure point. The entry point of the tunnel is the home agent and the exit point is the mobile node's care-of address. The tunnel is two-way, which ensures that the services offered by the home agent are transparent.

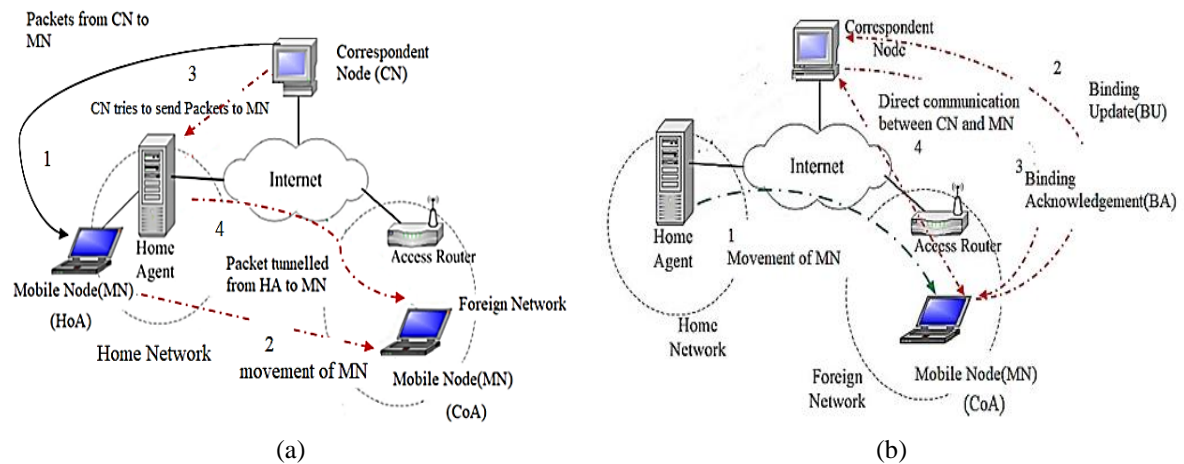


Figure 2. MIPv6 working operation in (a) normal communication and (b) route optimization

An operational overview of Mobile IPv6 is presented in RFC3775. A mobile node (MN) and a correspondent node (CN) can communicate in one of two ways. Datagrams to the correspondent node were transmitted from the MN to the HA, which subsequently redirected packets to the CN. The home network employs neighbor discovery to interrupt traffic in this phase. The delay introduced by routing packets from the home agent is significant. By forcing traffic via the home agent, the network gains a point of failure. Route optimization [20], [21] is the second way of communication. A mobile node must establish its present binding at the correspondent node for traffic from the CN to be routed directly to the mobile node. This mode of communication allows for the shortest communication path and also eliminates traffic at the home network. IPv6 also supports multiple home agents. In this situation, the mobile host uses dynamic home agent discovery mechanisms to automatically discover the IP addresses of home agents. The message flow of the MIPv6 diagram has been shown in Figure 3.

2.1.2. Drawback of MIPv6

The performance of the network gets degraded if the mobile node moves frequently in a local domain. In MIPv6, mobile devices are unable to retain their previous upper-layer connections, resulting in a scaling issue. This protocol faces a few problems to support loss-sensitive and real-time applications due to high signaling overhead and delay. At the time of registration, the mobile node may lose the connection with the correspondent node and it leads to packet loss. Mobile IP is not built to handle high-speed transmissions gracefully. Every handoff has a certain amount of latency, during which the mobile node is unable to receive messages. As a result, as the handoff rate rises, the rate of packet loss rises with it.

2.1.3. Proxy MIPv6 (PMIPv6) protocol

PMIPv6 is a network protocol. An IP mobility solution was implemented in a network. A mobile node is not engaged in the IP mobile solution, i.e., MN is not aware of what is going on inside. Then how can we achieve a network-based mobility management solution? The goal is to employ one of its network's components as a proxy. It may be an access router. The protocol is known as PMIPv6 since it extends the capability of MIPv6. The advantage of PMIPv6 is i) HA function and packets used in mobile signaling can be reused, ii) A common HA would act as a mobile agent for all kinds of IPv6 nodes, and iii) PMIPv6 allows less signaling compared to MIPv6 in each handoff because there is no duplicate address detection and return routability. The following entities are used in PMIPv6 and are shown in Figure 4.

- LMA: the mobile node's binding status is managed by LMA, which functions as its home agent.

- Mobile access gateway (MAG): a MN is attached to this gateway. This access router manages the mobility-related signaling for the MN. It also monitors the mobile node's movement to and from the accessibility connection, as well as signaling to LMA.
- MN: the router or an internet host whose movement is controlled by the network is referred to as MN.
- LMA address: the global IP defined at the LMA is referred to as the LMA address. Between LMA and MAG, a bidirectional path was built. MAG sends a proxy binding update (PBU) message to this address.
- Proxy care-of address (PCoA): his global address is established on the MAG's interface. This address is viewed by LMA as the mobile node's CoA, which registers in the MN's binding cache entry (BCE).
- PBU: MAG sent a request to LMA to establish a link between a mobile node's home network prefix (HNP) and its PCoA.
- Proxy binding acknowledgement (PBA): in reply to PBU, LMA sent a message to MAG.
- MN-HNP: it is a prefix for the connection between MAG and MN.
- MN home address (MN-HoA): this address is utilized as far as MN is connected to the access network.

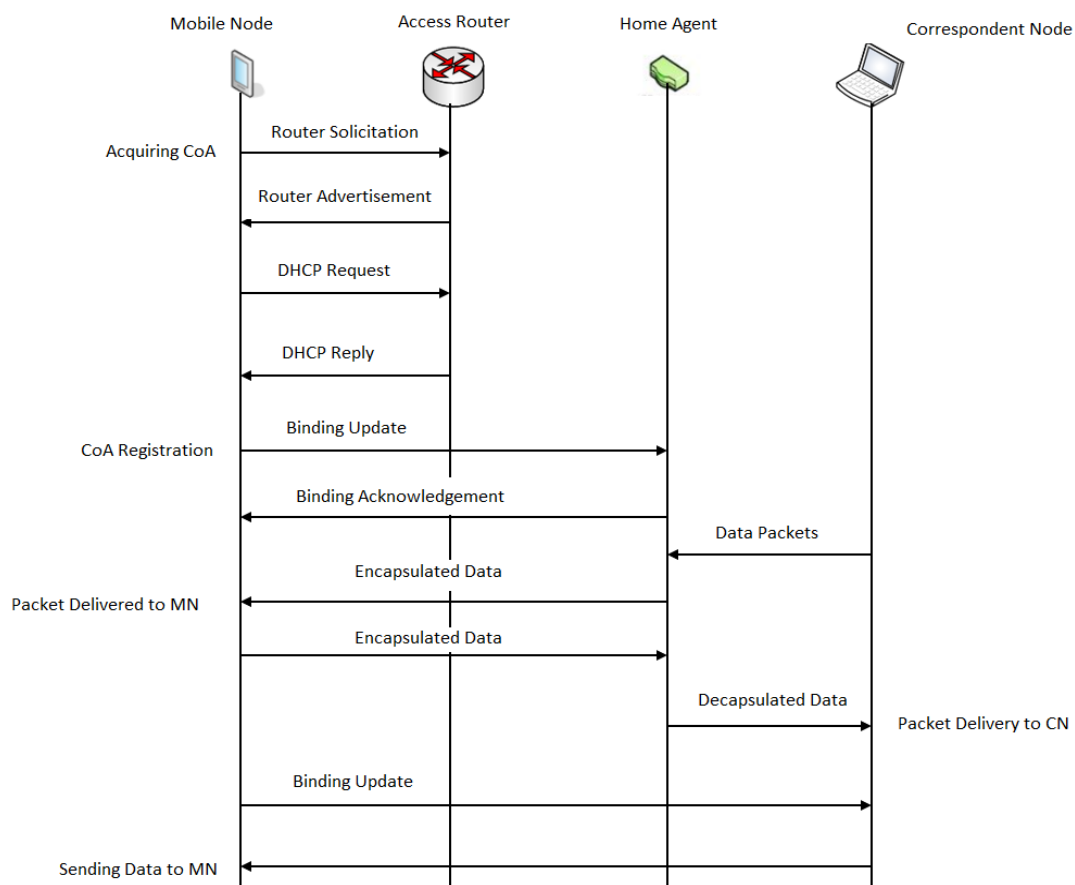


Figure 3. Signaling flow of MIPv6

The signaling flow of PMIPv6, as shown in Figure 5, is as follows: when a mobile node connects to MAG for the first time, it sends the router solicitation message to MAG [22]. The MAG sends a PBU message to LMA for updating. LMA sends a response as a PBA, which includes MN-HNP. The BCE is subsequently created, and a tunnel to MAG is established. In addition, MAG establishes a bidirectional tunnel with LMA. MAG now has all of the data for the mobile host. MAG sends router advertisements (RA) to gain access to the connection advertising the MN's HNP. MN has one or more legitimate addresses after a successive address configuration. The data transmitted to or from the MN is handled by LMA and MAG using the network prefix's address.

The MAG will notice the detachment of the mobile host from the connection if it alters its point of attachment. The MAG then instructs the LMA to delete the MN's binding status. LMA acknowledges the request and takes a certain amount of time for MAG to update the binding on the new link. If the LMA does

not receive an update within the time limit, it will erase MN's binding cache record. MAG will send a signal to the LMA to update the binding state when it detects MN's connection to its new access point. The MAG that is currently serving delivers a RA and MN-HNP, ensuring that the mobile host does not alter its layer 3 interface attachment.

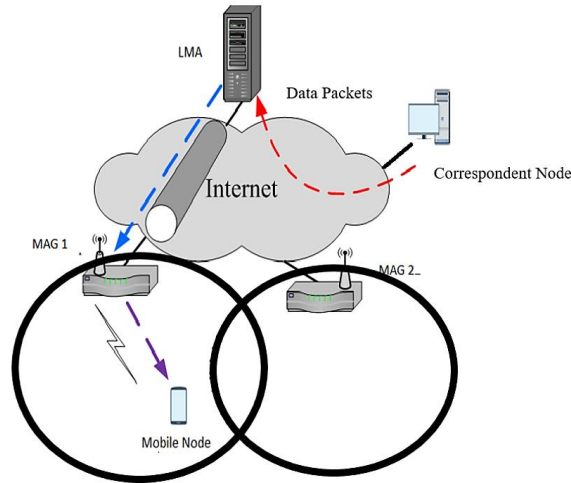


Figure 4. Proxy mobile IPv6

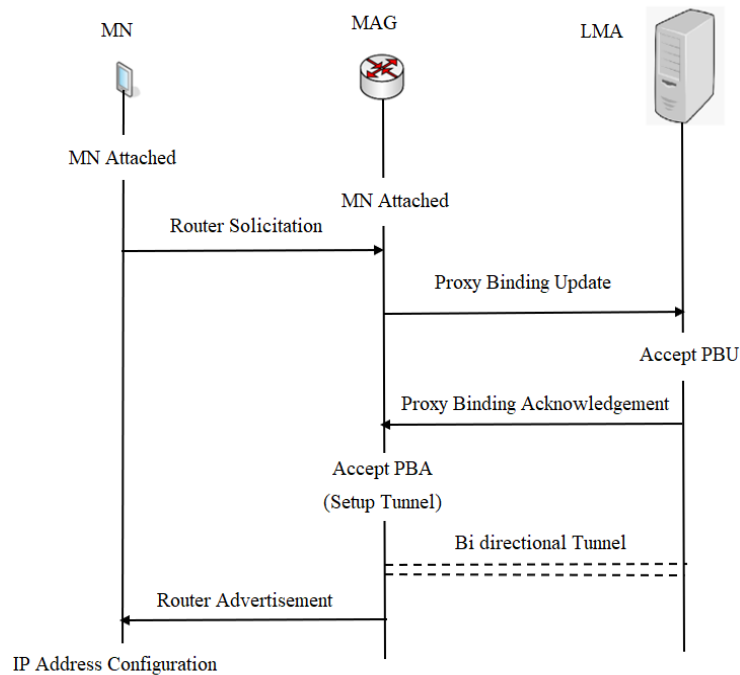


Figure 5. Signal flow of mobile node attachment in PMIPv6

2.1.4. ISSUES ENCOUNTERED IN PMIPv6

PMIPv6 mobility solutions that rely on networks will impose numerous constraints. They are:

- Handoff latency: in PMIPv6, the mobile node experienced a large handoff delay because the handoff signaling should go through LMA. Moreover, PMIPv6 does not have any buffering mechanism which leads to the loss of packets during handoff.
- Bottleneck problem: LMA is engaged in the transmission of both control and data packets. LMA must update the BCE as the mobile node traverses, producing congestion in the system.

- Route optimization: All incoming data must pass through the tunnel linking LMA and MAG, resulting in a non-optimal path.
- Network mobility: PMIPv6 is intended to support the mobility of a single MN. It does not encourage group movement.
- Load balancing: there is an absence of a load balancing mechanism. When the usage of mobile nodes grows, MAG may become overburdened. As a result, an effective load balancing technique must be proposed.

2.2. Need for DMM protocol

The limits of centralized systems are anticipated to be numerous [23], necessitating expensive network engineering and specifications. Routing through a central anchor that is not optimal often results in a lengthier path. The amount of data traffic is rapidly increasing. This would necessitate a significant upgrade to centralized architecture capabilities. In a centralized design with high growth in mobile nodes, maintaining the mobility context and setting up special routes for each mobile node is tough. The number of signaling messages grows, even more, when both endpoints are mobile. The system failure is more susceptible to the CMM protocol.

With these restrictions in mind, the IETF recently suggested the DMM paradigm, which can be regarded as an innovative and effective approach to mobile management. The primary idea behind DMM is that mobility anchors being dispersed throughout the system, topographically closer to users, that provides near-optimal route assistance and effective network resource use, allowing upcoming mobile networks to scale more easily. Accessibility to the top layer is only granted when it is required in DMM. Prefix provisioning, signal messages to upgrade the position, and address setting are all reduced to the absolute minimum. The following entities are used in DMM

- Mobile anchor access router (MAAR): it is the router, to which the node is attached. It performs the function of LMA and MAG. Also, act as a mobility manager.
- Central mobile database (CMD): the BCE for the mobile node is saved in CMD.
- Previous MAAR (PMAAR): MAAR that served the mobile node before moving to a foreign network, it is called PMAAR.
- Serving MAAR (SMAAR): it is the MAAR whereby the node is currently connected.
- Anchoring MAAR: an IPv6 address that the mobile node uses.
- Distributed logical interface (DLIF): DLIF is a logic interface at the IP layer of the MAAR.

2.2.1. Advantages of DMM protocol

The following advantages motivate the DMM solutions to handle mobile data traffic in an effective manner: i) by placing an internet service station nearer to the MN, mobility cost is decreased; ii) latency was reduced compared to the CMM protocol; iii) the data plane and control plane functions are divided; iv) DMM provides fast path updates during handover. DMM has an excellent handover performance compared to centralized mobility protocols; v) to improve packet delivery efficiency, DMM is beneficial. Out of sequence packet delivery can be avoided by using only one data forwarding per flow; vi) data are distributed among access nodes; thereby, scalability issues are avoided; vii) temporary tunnels are established between access nodes only when it is necessary; and viii) as a result of DMM's better traffic distribution among network entities, congestions and resource wastage can be avoided.

2.3. Approaches in distributed mobility management

According to the IP mobility support protocol, the DMM solution is based on mobility anchors and dynamic updating of the forwarding devices based on MN's location. Tunneling between the mobile host and the mobile anchor keeps its forwarding plane intact. Mobile traffic and movement control are also disseminated and dynamically engaged at the access network, as per MN. DMM can be approached in two ways. One of them aims at distributing host-based MIPv6 [24]–[26]. A Second approach aimed at making network-based PMIPv6 [27]–[31] in a scattered way. The following session elaborates host-based DMM and network-based DMM. In host-based DMM, the present location of MN, its IP sessions, and anchor positions are provided to the mobility system. In the event of network-based DMM, the DMM entity retrieves the same information without involving the node.

2.3.1. Host-based DMM protocol

DMM approach extends or reuses the existing MIPv6 protocols. In this method there is no single anchor but the anchors are distributed at several access router. The following elements are supported by the DMM method in a distributed way.

- Access mobility anchor (AMA): HA in MIPv6 is extended as AMA in the host-based DMM approach. The access router is usually where this AMA runs. AMA's features include allocating a network address to the mobile node and maintaining binding caches. Mobility signaling messages from the mobile node or its nearby AMA are used to update the binding cache. Serving AMA is the AMA where the mobile node is currently connected. Serving AMA configures the mobile node's IP address and initiates a message exchange with that IP address.
- Access binding update (ABU) and access binding acknowledgement (ABA): the mobile node and the serving AMA exchange BU and BA messages. In addition to this, signaling messages are also mentioned in DMM. Serving AMA sends ABU messages to originating AMA(s). A tunnel is established between both AMA's with the help of ABU messages. In response, an acknowledgement is sent.

Figure 6 illustrates the architecture of the host-based DMM protocol which supports the mobile node's handover in a distributed manner. While the mobile node stays at AMA1 it acquires IP Address as Pref A::MN1 and the status is preferred. When it moves to AMA2, MN acquires a new IP address as Pref B::MN1. The mobile node registers this information to AMA2 by sending the binding update message. AMA2 forwards this information to AMA1. AMA1 accepts AMA2's request and responds with an acknowledgment (ABA) message. As a result, a bidirectional channel connecting AMA1 and AMA2 is established. MN packets for Pref A::MN1 are sent through a bidirectional channel linked to the AMA1. Due to the deprecation of Pref A::MN1, AMA2 does not use this IP address for communication with new CNs. The new IP address, PreB::MN1, is used for new communication sessions with CN2 that do not require tunneling in the example above.

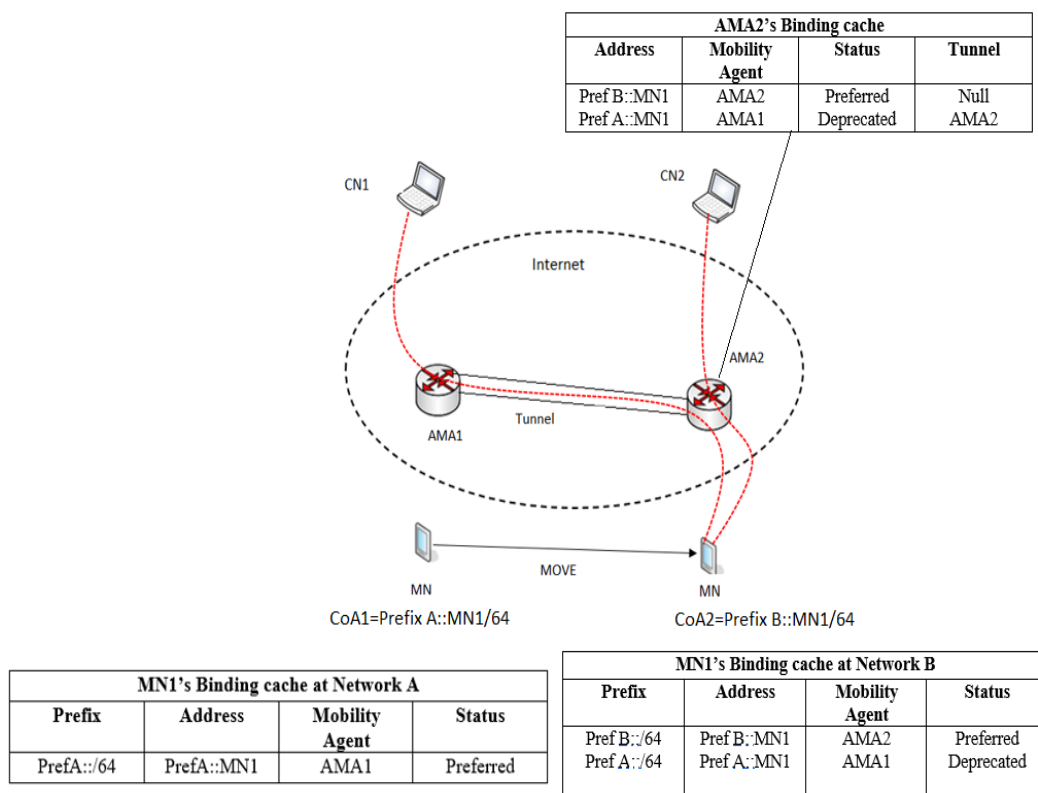


Figure 6. The structure of host-based DMM protocol

The host-based DMM removes a single mobile anchor i.e., the home agent in MIPv6. In DMM AMA's are distributed at the access level. It eliminates the problem of system failure Mobile nodes are involved in signaling because it is a host-based technique. To continue the mobility session of the mobile node, tunnels are formed between AMA's. So, tunneling overhead issues are reduced compared to MIPv6. The creation of such multiple bi-directional tunnels produces a higher mobility rate and the system performance requires frequent registration and management of several tunnels.

2.3.2. Network-based DMM protocol

The mobile node does not send or receive mobility signals. Mobility anchors were distributed and performed signaling in favor of mobile nodes, similar to PMIPv6. In NB-DMM, the functional elements are:

- Mobility access router (MAR): similar to MAG in PMIPv6. It detects the attachment of the node and provides HNP to the attached node. MAR maintains a binding cache to store the mobile node’s mobile context dB for obtaining the information of the mobile node. The MAR where the mobile node is currently connected is called serving MAR. The source MAR is the anchor point of HNP. The network packets are sent through a bilateral tunnel formed between the origin MAR and the serving MAR.
- Mobility contextual database (MCDB): it is a repository that keeps track of the HNP's origin MAR. It gives the Serving MAR mobility information of the mobile node.
- MAR binding update (MBU) and MAR binding acknowledgement (MBA): this signaling message is exchanged between the MAR's. For tunnel establishment, Serving MAR sends MAR binding update messages to the origin MAR. Origin MAR will send the response as the MAR binding acknowledgement to SMAR.
- Mobile contextual request (MCReq) and response (MCRes): between the database and the serving MAR, this message is used. Request is transmitted by SMAR to upgrade or receive the information about the mobile node in the database. MCDB will send the response message to the serving MAR.

The architecture of the network-based DMM protocol is depicted in Figure 7. In this architecture, MN moves from the MAR1 access network to MAR2. While MN resides at MAR1 it uses an IP address as HNP A::MN1. The mobile node then connects to the MAR2 access network. When MAR2 discovers the MN connection it initially sends and receives the MCReq message & MCRep message to update & recover mobile context information from DB. MAR2 obtain the previous MN prefix as HNPA::/64 and its relevant information. MAR2 then sends the Router Advertisement message containing HNPA::/64, “Deprecated” choices & allocates the latest home network prefix as HNP B::MN1. The mobile node retains the former IP Address and allocates a current address. This new address is used for new correspondence and the former address is solely for ongoing correspondence. The ongoing communication to HNPA::MN1 is anchored to MAR1 and then it is tunneled from MAR1 to MAR2. The new correspondence session is routed without tunneling.

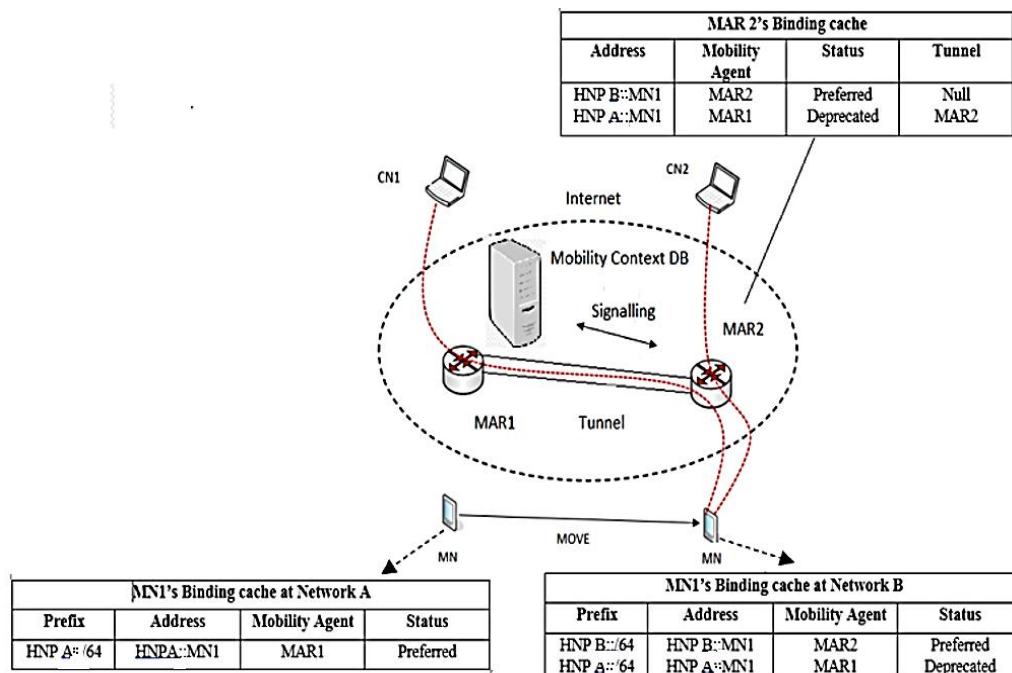


Figure 7. The architecture of the network-based DMM protocol

Network-based DMM is categorized into 1, Partially DMM 2, Fully DMM, and Partially DMM comprises MAAR and CMD [32], [33]. Mobile node's mobility information is managed by CMD in the control plane. In the data plane, MAAR is an important component of PMIPv6's LMA and MAG. There is no CMD in fully distributed mobility management. MAAR, which is positioned at the network's edge, handles both the planes.

a. Partial network-based DMM protocol

The functions of the information plane and controlling plane are separated. MAAR distributes and manages its data plane. The central mobility database is used by the control layer. LMA is replaced as CMD and able to send PBU and PBA messages. MAG is renamed MAAR. It maintains BCE for a mobile node. This cache stores the PMAAR's information. Each MAAR allocates global Prefixes to its mobile node. The same Prefix cannot be allocated by some other MAAR. To retrieve the past data of the mobile node, MAAR needs to contact the CMD.

The communication flow for the initial setup of the mobile host has been depicted in Figure 8. When a mobile node is attached to MAAR1 for the first time, it assigns an IPv6 prefix to MN and stores this prefix in BCE. MAAR1 sends PBU along with the mobile node prefix and its ID to CMD. CMD stores a BCE since it is the first registration. Then CMD sends a proxy binding acknowledgment to MAAR1. MAAR1 stores it in BCE and unicast a routing advertisement message.

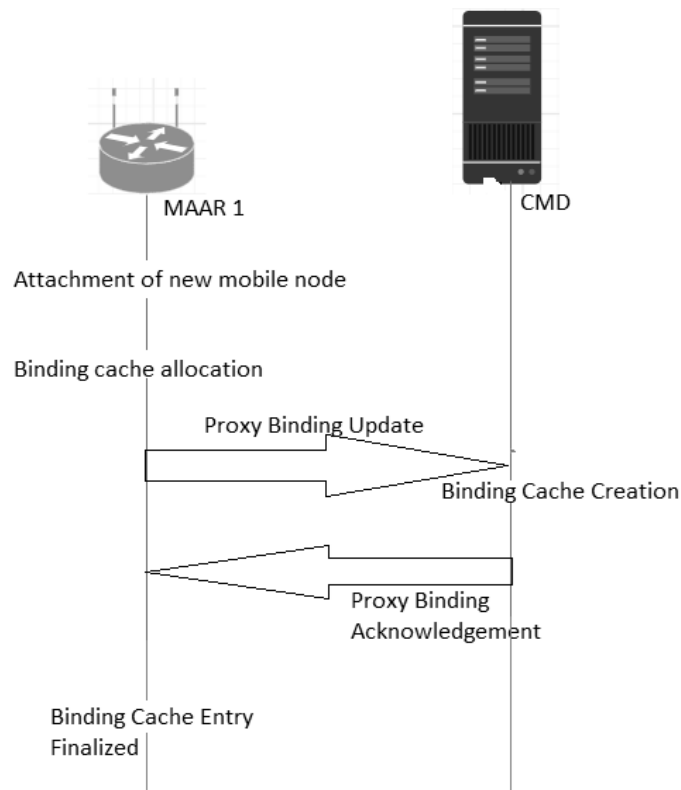


Figure 8. Communication flow for the initial setup of MN

A scenario after handover has been shown in Figure 9. When a mobile node moves to a new MAAR2, CMD behaves in the following steps. The new MAAR2 assigns Prefix2 to the mobile node and stores this information in BCE and sends PBU to CMD. CMD retrieves the existing data of the mobile node and forwards this PBU to PMAAR1. After receiving a PBU, MAAR1 installs a passage towards MAAR2, then sends PBA to CMD. CMD updates this information in BCE and sends PBA to SMAAR2 containing previous Proxy CoA and its prefix. Now the bidirectional tunnel is established between PMAAR1 and SMAAR2. MAAR1 now receives packets addressed to prefix1 and forwards them to MAAR2. Packet flow after handover is shown in Figure 10.

The scenario after handover where CMD act as a proxy is shown in Figure 11. PBU sent by the PMAAR, requires a longer time to hit the CMD. SMAAR receives multiple PBA's from the CMD in response to PBU. Retransmission needs to be taken place by the CMD. It leads to a burst in the packet. To avoid this burst paging mechanism must be introduced.

- DE-Registration: only serving MAAR is allowed to deregister the whole mobile node session.
- RE-Transmission: to configures the retransmission INITIAL BINDACK-TIMEOUT should be used.

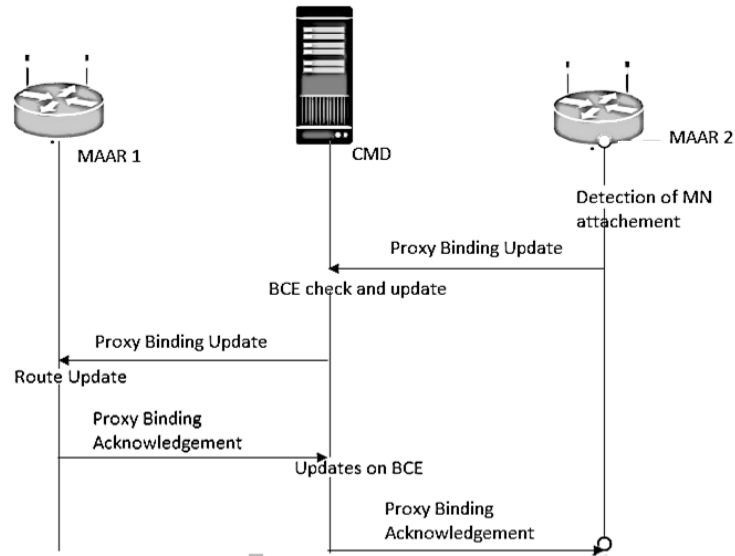


Figure 9. Signaling flow after handover

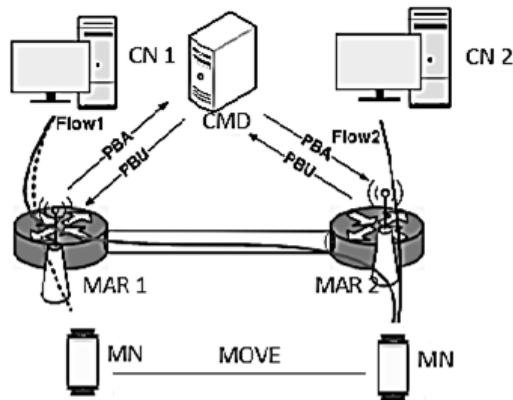


Figure 10. Packet flow after handover

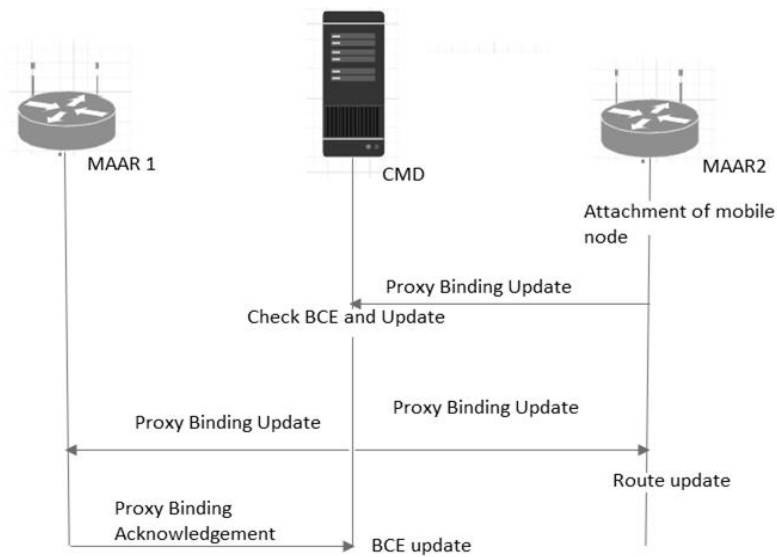


Figure 11. Handover where CMD acts as a proxy

b. Fully network-based DMM

On the access link, every MAARS does have a collection of IPv6 prefixes that can be given to MN. Fully proxy based DMM architecture does not have any central control entity [34]–[36]. Each MAAR has its cache for the mobile node. The MAARs are now in charge of both planes. Packet flow after the handover in fully Proxy based DMM is shown in Figure 12.

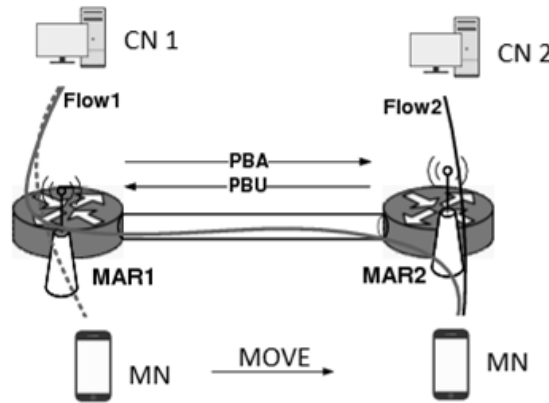


Figure 12. Packet flow after the handover in full proxy-based DMM

In fully DMM, a lack of awareness about other MAARs and their advertising prefixes becomes a significant bottleneck. When a mobile node attaches, this MAAR has to know two things to effectively ensure its mobility and the continuity of its data flow: i) whether the node contains any P-MAAR and ii) if it does, which prefixes were broadcast by which MAAR. Various approaches can be used to accomplish this: i) make a prior approach that employs layer 2 or layer 3 techniques. Because the present MAAR knows the target MAAR before handoff, the mobility information can be communicated; ii) schemes for MAAR identity: they can use a peer-to-peer method or a unicast/multicast/ broadcast query technique; iii) the MN's explicit confirmation; and iv) additional MN-MAAR connection protocols.

3. RESULTS AND DISCUSSION

3.1. Performance analysis of CMM and DMM protocols

The introduced DMM protocols have the same properties as their corresponding CMM protocols. In comparison to earlier CMM protocols, Table 1 shows the features of DMM methods. Both CMM and DMM protocol is described in [3]–[18]. The comparison reveals the DMM protocol outperforms the existing CMM protocols.

Table 1. Comparison between CMM and DMM protocol

PARAMETER	MIPv6	PMIPv6	MIPv6- DMM	PMIPv6 -DMM
Type of motility management	Host protocol	Network protocol	Host protocol	Network protocol
Mobile node address	HoA, CoA	HoA	IP addresses configured at the access network	IP addresses configured at the access network
Number of mobile node addresses associated	Two	One	N	N
Signaling message	BU/Back between MN and HA	PBU/Proxy binding between MAG and LMA	BU/BA between serving AMA and MN, Anchor BU/Anchor BA.	MBU/MBA and MCREQUEST/MCRESPONSE
Tunneling	HA-MN tunnel	LMA-MAG tunnel	Origin AMA(s)- current AMA tunnel	Origin MAR(s)- serving MAR tunnel
Tunneling per MN	1	1	n-1(shared with another mobile Node)	n-1(shared with another mobile Node)

Mobility has an impact on both the control plane and the data plane in communication in general. When a mobile node enters a new position, signaling is introduced, so it is necessary to alter the route to deliver all packets. To provide seamless mobility to the user, the mobility management protocol introduces

tunneling as an implicit mechanism. The following are the performance metrics used to measure the efficiency of the protocol.

- a. Signaling cost: as mentioned earlier, the fundamental process of IP is to ensure the mobility event of a node is up-to-date when it hops between subnets. This task necessitates the transmission of control packets across motility agents. When a mobile node moves, it must send a notification to its mobility anchor. The location registration is needed even if the mobile node does not communicate with others. The cost of signaling for location updates will become more critical as the number of MNs grows. Host-based DMM has lower expenses compared to CMM [37], [38]. Network-based DMM has the highest signaling burden because it has additional signaling involvement.
- b. Cost of data packet delivery: the quantity of incoming packets and the number of hops influences the cost of delivery of data packet [39], [40]. It rises in a straight manner with the speed of transmission. DMM performs well compared to CMM since it avoids long routes and forwards traffic in an optimized way. All messages in CMM are sent through a central entity resulting in a longer path.
- c. Tunneling cost: for data packet transmission, all the mobility management protocol uses the tunnel. This metric is represented by adding the tunneling burden cost to the message distribution cost. The tunnel expense of DMM [41], [42] is lower compared to the CMM protocol.
- d. Processing cost: processing cost is nothing but the number of signaling messages sent by a mobile node per unit time to a network entity [43]. In specific, count the average number of proxy binding updates transmitted for each time unit to the local mobile anchor and the average number of proxy binding updates transmitted to the MAR as in the case of the distributed mobility management protocol. Higher values of this metric would reflect the possibility of encountering scalability problems.
- e. Packet loss and handover latency during a session: the number of packets lost during a session is another relevant measure [44]. This metric is based on handover latency [45], [46] and is determined as the total number of packets lost per mobile node throughout handover operations. A mobile node cannot accept packets until the handover process is completed. Handover latency is the time difference between transmission and reception of an IP packet. This handover delay is affected by the following parameters:
 - Layer 2 handover time: the time required by link layer (L2) to perform handover
 - Movement detection time: it is the time required by the device to detect that it has moved to Layer 3.
 - IP configuration and duplicate address detection: the time required to verify the uniqueness of an IPv6 address.
- f. Handover failure probability: if the mobile node leaves the subnetwork or cell residence before completing the necessary signaling messages, handover gets fails. As a result, the handover probability of failure is based on the possibility that the residence time of a subnetwork or cell is much less than handoff latency (HL). The minimizing of probabilities [47] is critical for mobile management methods since HFP is deemed to be more important.
- g. Security authentication delay: the handoff period is also dependent upon that network's specific authentication technique [48] that the user terminal acquires.
- h. Registration delay: it is defined as the number of hops between the MN and the HA. As the hop count increases, registration delay increases for all protocols except host-based DMM [49]. There may be a significant registration problem related to the participation of the mobile context database & mobile anchor.
- i. Mobility anchor load: the proportion of a mobile node's total amount of ongoing sessions to the number of mobility anchors is known as mobility anchor load [50], [51]. In comparison to the DMM protocol, a mobility anchor load of said CMM protocol increases

4. CHALLENGES IN THE DEVELOPMENT OF DISTRIBUTED MOBILITY MANAGEMENT PROTOCOL

Distributed mobility management protocol has several challenges and some of the circumstances are summarized below.

- a. Complex address and tunnel management: as a mobile node may obtain a current address while retaining its prior addresses, the n volume of addresses, as well as the n-1 volume of tunnels linked with the MN rises. Therefore, it is essential to design efficient tunneling and address management scheme.
- b. Delay for registration and high signal cost: signaling messages to manage bidirectional tunnel from serving mobile anchor and origin mobile anchor are necessary when the number of tunnels connected with the mobile node grows. Even when the mobile anchor tries to handle the signal message, it increases the registration latency and signals overhead.
- c. High handover latency: DMM incurs high latency as the mobile nodes move rapidly. For instance, smartphone consumers in fast-moving vehicles with long-term sessions.

- d. Network setup and resource organization: in a distributed environment, resource managerial functions like self-optimization, QoS provision and network configuration are required.
- e. Security consideration: End-to-End security and access network control are essential to secure DMM.

5. CONCLUSION




This article focuses on the detailed study of centralized mobility management protocol, its limitation, and distributed mobility management protocol with the primary objective of providing flexibility and scalability for the next-generation mobile networks. The study result shows that the DMM protocol offers more benefits than the CMM protocol. In addition to this study, we discussed a few challenges that should be focused on while designing the distributed mobility management protocol. Even though the DMM protocol helps to save network resources, there are numerous circumstances in which the protocol results in a decrease in network quality. The future work includes i) the simulation analysis of the network-based DMM protocol to improve the network performance and ii) to focus on DMM handover issues for the multiple MN and reducing the packet loss.

REFERENCES




- [1] J. Clement, "Global mobile data traffic from 2017 to 2022," *statista.com*, 2017. <https://www.statista.com/statistics/271405/global-mobile-data-traffic-forecast/>. Accessed: Feb. 28, 2020.
- [2] A. B. Abdulkarem and L. Audah, "Design and development of handover simulator model in 5G cellular network," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 4, pp. 3310–3318, Aug. 2021, doi: 10.11591/ijece.v11i4.pp3310-3318.
- [3] D. Johnson, C. Perkins, and J. Arkko, "Mobility support in IPv6," RFC 3775, 2004.
- [4] J.-H. Lee, J.-M. Bonnin, I. You, and Ta.-M. Chung, "Comparative handover performance analysis of IPv6 mobility management protocols," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 3, pp. 1077–1088, Mar. 2013, doi: 10.1109/TIE.2012.2198035.
- [5] X. Pérez-Costa, M. Torrent-Moreno, and H. Hartenstein, "A performance comparison of Mobile IPv6, Hierarchical Mobile IPv6, fast handovers for Mobile IPv6 and their combination," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 7, no. 4, pp. 5–19, Oct. 2003, doi: 10.1145/965732.965736.
- [6] C. Makaya and S. Pierre, "An analytical framework for performance evaluation of IPv6-based mobility management protocols," *IEEE Transactions on Wireless Communications*, vol. 7, no. 3, pp. 972–983, Mar. 2008, doi: 10.1109/TWC.2008.060725.
- [7] H. Soliman, C. Castelluccia, K. El Malki, and L. Bellier, "A hierarchical mobile IPv6 proposal," HMIPv6, 2005.
- [8] J.-H. Lee, Y.-H. Han, S. Gundavelli, and T.-M. Chung, "A comparative performance analysis on Hierarchical Mobile IPv6 and Proxy Mobile IPv6," *Telecommunication Systems*, vol. 41, no. 4, pp. 279–292, Aug. 2009, doi: 10.1007/s11235-009-9163-z.
- [9] C. Perkins, G. Dommety, K. El-Malki, G. Tsirtsis, and A. Yegin, "Fast Handovers for Mobile Ipv6," RFC 4068, 2000.
- [10] M. M. Sajjad, D. Jayalath, and C. J. Bernardos, "A comprehensive review of enhancements and prospects of fast handovers for mobile IPv6 protocol," *IEEE Access*, vol. 7, pp. 4948–4978, 2019, doi: 10.1109/ACCESS.2018.2887146.
- [11] S. Pack, T. You, and Y. Choi, "Performance analysis of robust hierarchical mobile IPv6 for fault tolerant mobile services," *IEICE Transactions on Communications*, vol. E87-B, no. 5, pp. 1158–1165, 2004.
- [12] M. Li, X. She, L. Chen, and H. Otsuka, "A novel resource reservation scheme for fast and successful handover," in *2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, Sep. 2009, pp. 556–560, doi: 10.1109/PIMRC.2009.5450358.
- [13] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy mobile IPv6," *IETF RFC 5213*, 2008.
- [14] H.-Y. Choi, S.-G. Min, Y.-H. Han, J. Park, and H. Kim, "Implementation and evaluation of proxy mobile IPv6 in NS-3 network simulator," in *2010 Proceedings of the 5th International Conference on Ubiquitous Information Technologies and Applications*, Dec. 2010, pp. 1–6, doi: 10.1109/ICUT.2010.5677817.
- [15] A. J. Jabir, S. Shamala, Z. Zuriati, and N. Hamid, "A comprehensive survey of the current trends and extensions for the proxy mobile IPv6 protocol," *IEEE Systems Journal*, vol. 12, no. 1, pp. 1065–1081, Mar. 2018, doi: 10.1109/JSYST.2015.2497146.
- [16] I. Soto, C. J. Bernardos, M. Calderón, and T. Melia, "PMIPv6: A network-based localized mobility management solution," *The Internet Protocol Journal*, vol. 13, no. 3, pp. 2–15, 2010.
- [17] W. Siang Hoh, B.-L. Ong, S.-K. Yoon, and R. B. Ahmad, "A comprehensive performance evaluation of MIPv6 and PMIPv6 mobility management protocols in wireless mesh network," *International journal of electrical and computer engineering systems*, vol. 12, pp. 1–8, Nov. 2021, doi: 10.32985/ijeces.12.si.1.
- [18] A. Chan, D. Liu, P. Seite, H. Yokota, and J. Korhonen, "Requirements for distributed mobility management," RFC 7333, 2014.
- [19] S. Jeon, S. Figueiredo, R. L. Aguiar, and H. Choo, "Distributed mobility management for the Future mobile networks: A comprehensive analysis of Key design options," *IEEE Access*, vol. 5, pp. 11423–11436, 2017, doi: 10.1109/ACCESS.2017.2713240.
- [20] O. D. Adeniji and A. Osofisan, "Route optimization in MIPv6 experimental test bed for network mobility: Tradeoff analysis and evaluation," *International Journal of Computer Science and Information Security*, vol. 18, no. 5, pp. 19–28, 2020.
- [21] A. K. Barbudhe, V. K. Barbudhe, and C. Dhawale, "Comparison of mechanisms for reducing handover latency and packet loss problems of route optimization in MIPv6," in *2015 IEEE International Conference on Computational Intelligence & Communication Technology*, Feb. 2015, pp. 323–329, doi: 10.1109/CICT.2015.119.
- [22] K. Vasu, S. Mahapatra, and C. S. Kumar, "Block prefix mechanism for flow mobility in PMIPv6 based networks," *arXiv preprint arXiv:1907.05102*, Jul. 2019.
- [23] F. Giust, C. J. Bernardos, S. Figueiredo, P. Neves, and T. Melia, "A hybrid MIPv6 and PMIPv6 distributed mobility management: The MEDIEVAL approach," in *2011 IEEE Symposium on Computers and Communications (ISCC)*, Jun. 2011, pp. 25–30, doi: 10.1109/ISCC.2011.5984020.
- [24] J.-H. Lee, J.-M. Bonnin, and X. Lagrange, "Host-based distributed mobility management support protocol for IPv6 mobile networks," in *2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications*

- (*WiMob*), Oct. 2012, pp. 61–68, doi: 10.1109/WiMOB.2012.6379140.
- [25] T.-T. Nguyen and C. Bonnet, “A hybrid centralized-distributed mobility management for supporting highly mobile users,” in *2015 IEEE International Conference on Communications (ICC)*, Jun. 2015, pp. 3945–3951, doi: 10.1109/ICC.2015.7248940.
- [26] M. Balfaqih, Z. Balfaqih, V. Shepelev, S. A. Alharbi, and W. A. Jabbar, “An analytical framework for distributed and centralized mobility management protocols,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 7, pp. 3393–3405, Jul. 2022, doi: 10.1007/s12652-020-01749-x.
- [27] C. J. Bernardos, A. de la Oliva, A. F. Giust, J. C. Zuniga, and A. Mourad, “Proxy mobile IPv6 extensions for distributed mobility management,” *DMM Working Group*, 2020.
- [28] M. Balfaqih, M. Ismail, R. Nordin, A. A. Rahem, and Z. Balfaqih, “Fast handover solution for network-based distributed mobility management in intelligent transportation systems,” *Telecommunication Systems*, vol. 64, no. 2, pp. 325–346, Feb. 2017, doi: 10.1007/s11235-016-0178-y.
- [29] F. Giust, L. Cominardi, and C. Bernardos, “Distributed mobility management for future 5G networks: overview and analysis of existing approaches,” *IEEE Communications Magazine*, vol. 53, no. 1, pp. 142–149, Jan. 2015, doi: 10.1109/MCOM.2015.7010527.
- [30] F. Giust, C. J. Bernardos, and A. de la Oliva, “Analytic evaluation and experimental validation of a network-based IPv6 distributed mobility management solution,” *IEEE Transactions on Mobile Computing*, vol. 13, no. 11, pp. 2484–2497, Nov. 2014, doi: 10.1109/TMC.2014.2307304.
- [31] H. Ali-Ahmad, M. Ouzif, P. Bertin, and X. Lagrange, “Performance analysis on network-based distributed mobility management,” *Wireless Personal Communications*, vol. 74, no. 4, pp. 1245–1263, 2014.
- [32] Y. Wang, X. Li, and W. Zhang, “A comparative study on PMIPv6 and partially DMM network architecture,” *International Journal of Multimedia and Ubiquitous Engineering*, vol. 11, no. 8, pp. 203–212, 2016.
- [33] M. K. Murtadha, N. K. Noordin, B. M. Ali, and F. Hashim, “Design and evaluation of distributed and dynamic mobility management approach based on PMIPv6 and MIH protocols,” *Wireless Networks*, vol. 21, no. 8, pp. 2747–2763, Nov. 2015, doi: 10.1007/s11276-015-0950-z.
- [34] F. Giust, C. J. Bernardos, and A. de la Oliva, “HDMM: deploying client and network-based distributed mobility management,” *Telecommunication Systems*, vol. 59, no. 2, pp. 247–270, Jun. 2015, doi: 10.1007/s11235-014-9959-3.
- [35] M. K. Murtadha, N. K. Noordin, B. M. Ali, and F. Hashim, “Design and simulation analysis of network-based fully distributed mobility management in flattened network architecture,” *Telecommunication Systems*, vol. 65, no. 2, pp. 253–267, Jun. 2017, doi: 10.1007/s11235-016-0226-7.
- [36] M. K. Murtadha, N. K. Noordin, B. M. Ali, and F. Hashim, “Fully distributed mobility management scheme for future heterogeneous wireless networks,” in *2015 IEEE 12th Malaysia International Conference on Communications (MICC)*, Nov. 2015, pp. 270–275, doi: 10.1109/MICC.2015.7725446.
- [37] J. Lee, J. Bonnin, P. Seite, and H. Chan, “Distributed IP mobility management from the perspective of the IETF: motivations, requirements, approaches, comparison, and challenges,” *IEEE Wireless Communications*, vol. 20, no. 5, pp. 159–168, Oct. 2013, doi: 10.1109/MWC.2013.6664487.
- [38] S. Figueiredo, S. Jeon, D. Gomes, and R. L. Aguiar, “D3M: Multicast listener mobility support mechanisms over distributed mobility anchoring architectures,” *Journal of Network and Computer Applications*, vol. 53, pp. 24–38, Jul. 2015, doi: 10.1016/j.jnca.2015.02.006.
- [39] J. Carmona-Murillo, V. Friderikos, and J. L. González-Sánchez, “A hybrid DMM solution and trade-off analysis for future wireless networks,” *Computer Networks*, vol. 133, pp. 17–32, Mar. 2018, doi: 10.1016/j.comnet.2018.01.030.
- [40] L. T. Jung and A. Ali Wagan, “Distributed network mobility management scheme for network mobility,” in *2018 4th International Conference on Computer and Information Sciences (ICCOINS)*, Aug. 2018, pp. 1–6, doi: 10.1109/ICCOINS.2018.8510603.
- [41] M. Balfaqih, M. Ismail, R. Nordin, and Z. Balfaqih, “Handover performance evaluation of centralized and distributed network-based mobility management in vehicular urban environment,” in *2017 9th IEEE-GCC Conference and Exhibition (GCCCE)*, May 2017, pp. 1–5, doi: 10.1109/IEEGCC.2017.8447938.
- [42] P. P. Ernest, H. A. Chan, O. E. Falowo, and L. A. Magagula, “Distributed mobility management with distributed routing management at access routers for network-based mobility support,” *Wireless Personal Communications*, vol. 84, no. 1, pp. 181–205, Sep. 2015, doi: 10.1007/s11277-015-2602-0.
- [43] S. Pack and Y. Choi, “Performance analysis of hierarchical mobile IPv6 in IP-based cellular networks,” in *14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003.*, pp. 2818–2822, doi: 10.1109/PIMRC.2003.1259259.
- [44] M. Balfaqih, M. Ismail, R. Nordin, and Z. Balfaqih, “Handover performance analysis of distributed mobility management in vehicular networks,” in *2015 IEEE 12th Malaysia International Conference on Communications (MICC)*, Nov. 2015, pp. 145–150, doi: 10.1109/MICC.2015.7725424.
- [45] J. Wozniak, “Mobility management solutions for current IP and future networks,” *Telecommunication Systems*, vol. 61, no. 2, pp. 257–275, Feb. 2016, doi: 10.1007/s11235-015-9999-3.
- [46] Z. Balfaqih, “Design and development of network simulator module for distributed mobility management protocol,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 7, pp. 3407–3421, Jul. 2022, doi: 10.1007/s12652-020-01764-y.
- [47] S. Alam, S. Sulisty, I. W. Mustika, and R. Adrian, “Handover decision for V2V communication in VANET based on moving average slope of RSS,” *Journal of Communications*, vol. 16, no. 7, pp. 284–293, 2021, doi: 10.12720/jcm.16.7.284-293.
- [48] L. Zhang, M. Ma, and Y. Qiu, “An enhanced handover authentication solution for 6LoWPAN networks,” *Computers & Security*, vol. 109, Oct. 2021, doi: 10.1016/j.cose.2021.102373.
- [49] M. Aman, S. Mahfooz, M. Zubair, N. Mukhtar, K. Imran, and S. Khusro, “Tunnel-free distributed mobility management (DMM) support protocol for future mobile networks,” *Electronics*, vol. 8, no. 12, Dec. 2019, doi: 10.3390/electronics8121519.
- [50] 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,” *Mobile Information Systems*, vol. 2017, pp. 1–15, 2017, doi: 10.1155/2017/2568983.
- [51] T.-T. Nguyen and C. Bonnet, “On the efficiency of dynamic multicast mobility anchor selection in DMM: Use cases and analysis,” in *2014 IEEE International Conference on Communications (ICC)*, Jun. 2014, pp. 2828–2834, doi: 10.1109/ICC.2014.6883753.

BIOGRAPHIES OF AUTHORS

Prabha Mahenthiran    received the B.Tech. and MTech degrees in Computer Science Engineering from SASTRA University, Thanjavur, India, in 2010 and 2012, respectively. She is pursuing a Ph.D. degree in the School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, Tamil Nādu-India. Her research interests include computer networks, mobile computing, image processing, real-time systems, and database management systems. She can be contacted at email: prabhamani_88@yahoo.co.in, prabha.m2019@vitstudent.ac.in.



Dinakaran Muruganadam    has completed his B.Tech. (IT), M.Tech (IT-Networking) in Vellore Institute of Technology and Ph.D in Anna University, Chennai, Tamil Nadu and India. He worked in TATA Consultancy Services as Assistant System Engineer from September 2006 to July 2009. Currently he is working as Associate Professor and Head-Department of IT, School of Information Technology and Engineering, VIT University, Vellore. He has published around 50+ articles in various International Conferences and Journals. His research interests are mobile networks and software engineering. He can be contacted at email: dinakaran.m@vit.ac.in, dinakaran.bpm@gmail.com.