2
IP Mobility Management

Nowadays, the mobile data services have become an essential part of many consumers' lives [1, 2]. So far, the users have been using their mobile devices (e.g., smartphones and tablets) not only for personal life (e.g., making voice/video calls, sending email, watching video/TV, playing online games, and so on) but also for work (general and job-specific work applications such as multimedia conferencing, and distance learning, etc.) on a regular basic [3, 4, 5]. As a result, the mobile data traffic has been almost doubled each year during the last few years [6]. This trend is expected to continue in the upcoming years, especially with the deployment of 4G networks. The widely usage of mobile data services has been driven by the variety of different reasons such as: the increasing number of mobile devices which become more and more powerful and intelligent, the enhancement of wireless access technology in terms of coverage, speed and quality, as well as the explosion of mobile applications [6]. The mobility of the devices puts a new requirement on the mobile operators to provide connectivity anywhere and at anytime. Moreover, providing consistent and seamless services is required for satisfying user's expectations and fulfilling even highly application requirements in terms of service disruption on the move [7].

In all-IP mobile networks, IP mobility is a crucial concept to meet the demand of ubiquitous Internet connectivity as well as new service requirements such as seamless handover across heterogeneous networks, consistent quality of experience and stringent delay constraints. IP mobility can be handled at different layers of protocol stack ranging from the link layer to the application layer [8, 9, 10]. The link layer mobility management protocols use the underlink information for mobility-related procedures when the MN roams among different physical points of attachment while keeping its layer 3 attachment (preservation of the IP address). The transport layer mobility management protocols [11, 12] provide an end-to-end mobility support without requiring to change the network layer infrastructure. Regarding the mobility protocols at the application layer, the most well-known protocol, Session Initiation Protocol (SIP) [13, 14], provides an end-to-end mobility management framework, which does not depend upon the network entities (e.g., HA) and can be deployed by any third-party application service providers. Due to the fact that most of the existing mobility management protocols are located at the network layer (since a network layer IP mobility is transparent to the upper layers as well as the applications [15, 10]), we focus on these protocols in our thesis.

Again, the mobility management protocols at the network layer can be classified according to different criteria such as the mobility range (micro- and macro-mobility) and the mobile host signaling (host- and network-based mobility) [8, 9, 16, 10]. Regarding the mobility range, the mobility management can be categorized into two types: the macro-mobility and the micro-mobility. The macro-mobility (global mobility or inter-domain mobility) refers to the mobility between different domains (with different architectures and access technologies) over a large area. MIPv6 and Host Identify Protocol (HIP) [17] fall in to

this category. On the other hand, the micro-mobility (or intra-domain mobility) is referred as a mobility between different cells/subnets inside a single administrative domain. Some examples of micro-mobility protocol are HMIPv6, FMIPv6, and PMIPv6. Considering the mobile host signaling, the host-based mobility protocols such as MIPv6 and Dual Stack Mobile IPv6 (DSMIPv6) [18], require the host to participate in mobility-related signaling process. On the contrary, in the network-based mobility, the network entities handle the mobility process on behalf of the host.
As stated above, the increasing penetration of the mobile devices, such as tablets and smart phones is generating a huge number of data traffic over the mobile networks. The mobile data traffic is expected to grow to 11.2 exabytes per month by 2017, a 13-fold increase over 2012 [1]. Despite the increasing volume of traffic, the mobile data revenue per user is falling fast. Thus, the mobile network is evolving towards the flat network architecture in order to be able to cope with the huge amount of traffic and reduce data transmission costs. Examples of this trend are traffic offloading (e.g., LIPA/SIPTO) and content delivery network (CDN) [19]. Considering the conventional IP mobility management (e.g., MIPv6, PMIPv6) which leverages on the centralized mobility management approach in a flat architecture, it raises several issues for the network operator like the inefficient use of network resources, poor performance, and scalability issues [20, 19, 21]. To overcome these problems, a novel concept, the so-called distributed (and dynamic) mobility management (DMM) has been introduced. A lot of research publications [22, 23, 24, 25, 26, 27] carried out the analysis on different DMM approaches and compared them with the conventional mobility managements in terms of signaling cost, packet delivery cost, handover delay, packet loss and end-to-end delay. The results from these analysis showed that DMM is a promising mobility management scheme.

In this section, we will briefly introduce a various IP mobility protocols ranging from the host-based to the network-based, from the centralized to the distributed approach. We focus on MIPv6 as a typical example of the macro-mobility and host-based mobility; and PMIPv6 as an example of the micro-mobility and network-based mobility. Finally, DMM will be presented, mainly focusing on the network-based approach.

2.1 Centralized Mobility Management

2.1.1 Mobile IPv6

Mobile IPv6 (MIPv6) [28] is the first mobility protocol standardized by the IETF for IPv6 networks. As a global mobility protocol, MIPv6 maintains the mobile node's reachability when it is away from home. It is done by introducing a central mobility, namely Home Agent (HA) located at the MN's home network, which is a topological anchor point of the permanent MN's IP address (Home Address or HoA). Using its home address, the MN can communicate regardless of its actual location in the Internet. When the MN is away from home, it may obtain a temporal IP address (namely care-of-address (CoA)) which can be used in the foreign network for routing purposes. This address identifies the current location of the MN. The MN then registers its current topological location (CoA) with its HA by means of Binding Update (BU)/Binding Acknowledgment (BA) messages. The HA keeps track of the MN's current location by maintaining a binding association between the MN's HoA and MN's CoA (namely Binding Cache Entry - BCE). A bi-directional tunnel is then established between the HA and the MN for redirecting packets from/to the current location of the MN. In more details, the HA, acting as a topological anchor point of HoA, intercepts the packets addressed to the MN and tunneled them to the MN's CoA.

On the other direction, the packets from MN are tunneled to the HA, before forwarding to the CN. However, a relevant drawback of MIPv6 is a triangular routing in which the packets have to pass through the HA, which is a typically longer route. To tackle this issue, the Router Optimization (RO) mode in which the MN communicates directly with the CN without passing through the HA is introduced. However, MIPv6 introduces several security vulnerabilities e.g., authentication and authorization of BUs during the RO process [29].
Additionally, MIPv6, as a global IP mobility solution, may cause a high handover latency (and packet loss) that could significantly affect the performance of the on-going sessions [30, 31]. The high signaling load is also required [30, 31]. Thus, it is not optimized to handle the micro-mobility management, where low-latency handover and low mobility-related signaling are essential. Various solutions have been proposed to improve the performance of MIPv6 such as Hierarchical Mobile IPv6 (HMIPv6) [32] and Fast Mobile IPv6 (FMIPv6) [33]. In HMIPv6, the Mobility Anchor Point (MAP) which is located at a local domain is introduced. Each MAP can be served as a local mobility anchor for a local domain. In this case, the mobile node sends BU messages to the local MAP rather than the HA when it moves inside a local domain. The MN sends BU message to the HA only when it moves between MAPs. As a result, the handover latency as well as signaling cost are reduced. On the other hand, FMIPv6 aims at reducing the handover latency and the number of lost packets. In this case, the handover is prepared in advance by using the lower-layer information, thus allowing the MN to configure a new CoA before it actually moves to the new subnet. As a result, the MN can use the CoA address immediately when it connects to the new subnet. The packets are also forwarded from the previous router to the new one, thus, reducing the number of lost packets.
As a host-based mobility protocol, in MIPv6, the MN needs to perform the mobility-related signaling by means of location update procedure. Consequently, the MIPv6 protocol stack is required at the MN. It is the major obstacle for the deployment of MIP in the reality. For this reason, the network-based localized mobility management (NetLMM[1]) is proposed to avoid the additional deployment in the MN so that the MN can be kept simple. Moreover, the complex security mechanism to authenticate the location update signaling can be avoided. In other words, the mobility can be transparently provided to all the legacy MNs.

2.1.2 Proxy Mobile IPv6

Unlike MIP6 and its host-based extensions in which the mobility functions need to be deployed at both network and terminal, a new approach, namely network-based localized mobility management (NetLMM), enables the mobility support without the MN's evolving in the signaling process. In this case, the mobility procedures are handled by the network entities. Proxy Mobile IPv6 (PMIPv6) [34], as an extension of MIPv6, was standardized by the IETF as a network-based mobility management protocol. PMIPv6 provides the mobility support within a localized area, namely a Localized Mobility Domain (LMD) or a PMIPv6 domain. While moving inside a LMD, the MN remains its IPv6 address. Thus, from IP layer point of view, the MN is unaware of mobility. This is achieved by introducing the network entity called the Mobile Access Gateway (MAG), which performs the mobility-related signaling on behalf of the MNs attached to its access links. In PMIPv6, the LMA, similar to HA in MIPv6, is responsible for maintaining the MN's reachability state and forwarding traffic from/to the current location of the MN. MN's traffic is always encapsulated and tunneled between the MN's LMA and the corresponding MAG. Each LMD consists of several LMAs and multiple MAGs, as illustrated in Fig. 2.1.

[1]NetLMM WG: http://datatracker.ietf.org/wg/netlmm/charter/

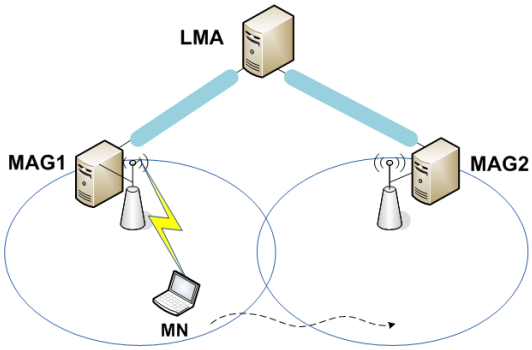


Figure 2.1 – The architecture of a PMIPv6 domain.

Compared to MIPv6, PMIPv6 brings some benefits such as: (i) avoiding the complexity of the protocol stack at the MN; (ii) supporting mobility without the MN's involvement; and (iii) reducing tunneling overhead (over the air) and decreasing handover latency [31].

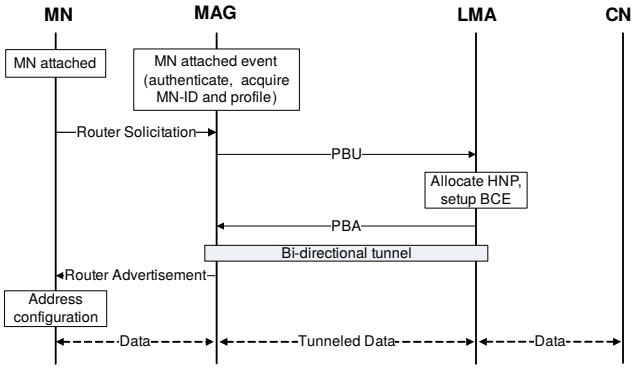


Figure 2.2 – Signaling when a mobile node attaches to the PMIPv6 domain.

The operation of PMIPv6 is briefly described as follows. Fig. 2.2 shows signaling for the MN's initial attachment to a PMIPv6 domain. When an MN enters a PMIPv6 domain (attaches to a MAG), upon the detection of a new MN, the MAG fetches the MN profile, for example from an Authentication, Authorization and Accounting (AAA) server, and verifies if the MN is authorized for the network-based mobility service. Upon a successful authorization, the MAG sends a Proxy Binding Update (PBU) message to LMA to register a new MN. After receiving the PBU message, the LMA allocates a Home Network Prefix (HNP) to the MN, creates a BCE for this MN (including the MN's identifier (MN-ID, for example using the Network Access Identifier (NAI) [35], or its Media Access Control (MAC) address), HNP and the MN's MAG address (Proxy Care-of-Address or Proxy-CoA)). The LMA then replies by a Proxy Binding Acknowledgment (PBA) message including the allocated HNP. The MAG, on receiving the PBA, sets up the forwarding policy for the MN. A bi-directional tunnel is then established between the MAG and the LMA for redirecting the traffic from/to the MN. It is noted that the PBU/PBA messages are based on BU/BA messages with some specific extensions, respectively [34]. The MAG then sends a Router Advertisement (RA) message including the allocated HNP to the MN. The MN, based on the HNP, configures its address and can use it to communicate with a corresponding node (CN).

When the MN performs a handover from the previous MAG (pMAG) to a new one (nMAG), the similar process as in the registration step will be executed to update the MN's current

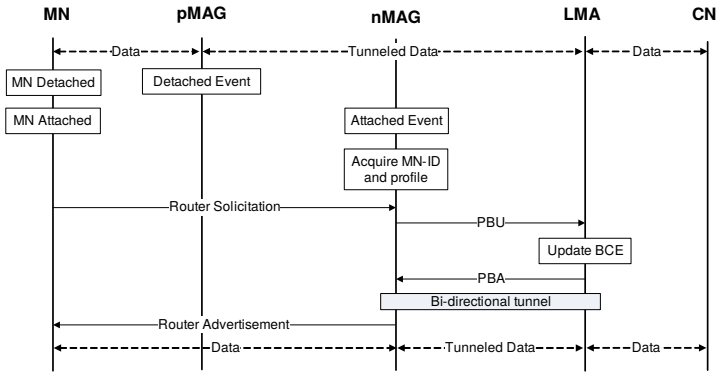


Figure 2.3 – Signaling when a mobile node performs a handover.

location at the LMA (see Fig. 2.3). In this case, the nMAG obtains the same HNP prefix for this MN and can emulate the MN's home network (through sending RA messages with the same HNP). As a result, the MN is not aware of the mobility and continues to use the same IP address as before. Moreover, the link shared with a given MN of all the MAGs in the domain should be configured with the same link local address to make sure that the MN does not detect link changes as well as avoid the potential address collision issue [34] during the handover process.

Similar to FMIPv6, Fast Handovers for PMIPv6 (FPMIPv6) [36] provides a fast handover mechanism for PMIPv6 in order to minimize the handover latency and the packet loss. Again, a bi-directional tunnel is established between the previous MAG and the current one to forward the packets to/from the MN. Also, the MN should provide information about the target network to the pMAG through L2 signaling. However, it inherits potential risks of erroneous movement and out-of-order packets delivery problem from FMIPv6

Extensions to PMIPv6 Typically, the performance of a mobility management protocol is measured using such well-known metrics as signaling cost, handover latency, and packet loss. The signaling cost consists of the location update cost and the packet delivery cost. Handover latency is defined as the total time needed to complete the handover procedures. During this time, the MN cannot send or receive any packets. The handover latency typically consists of layer 2 handover duration and layer 3 one. The packet loss is the amount of lost packets originated from or sent to an MN during its handover.

Various papers have been proposed which aim at improving PMIPv6 in terms of handover latency and signaling cost. In [37, 38], the authors applied the paging technologies to PMIPv6 to reduce the location update signaling cost for the mobile host in the idle mode. In [39], the authors used the Neighbor Discovery (ND) message of IPv6 to reduce the handover latency and packet buffering at the MAG. In this case, the pMAG sent the MN's profile to the neighbor MAGs through ND message. Similarly, in [40], the pMAG sent the MN's HNP to the adjacent MAGs in advance in order to perform the address configuration quickly after MN's handover. In [41], the improvement on handover latency was achieved by using the IEEE 802.21 Media Independent Handover services.

Similar to in MIPv6, in [42, 43], different route optimization schemes for PMIPv6 were also considered. Thus, the traffic could be routed in a better route bypassing the LMA. Unlike MIPv6, one of the main drawbacks of PMIPv6 is that the inter-domain handover is not supported. Thus, inter-domain mobility support in PMIPv6 has been proposed in [44, 45, 46, 47].

2.1.3 Mobility Management in the Current Cellular Networks

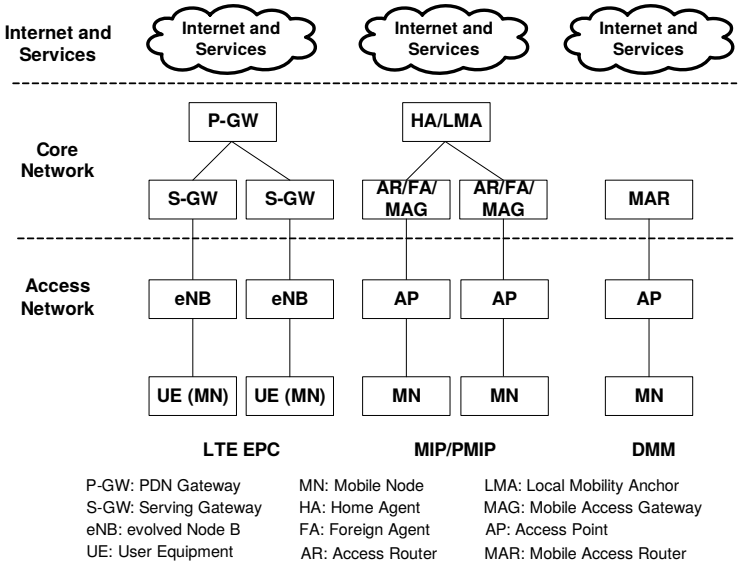


Figure 2.4 – Mobile network architecture.

The current mobile network architecture is highly centralized and hierarchical [22]. Following the hierarchical architecture, the network elements can be placed into three levels: Internet and services, core network, and access network. For example, the 3GPP cellular network consists of SGSN (Serving GPRS Support Node) and GGSN (Gateway GPRS Support Node). The evolved packet core (EPC) network [48] includes a packet data network gateway (P-GW), serving gateway (S-GW), and evolved Node B (eNB) as shown in the leftmost of Fig. 2.4. Thus IP mobility protocols, such as PMIPv6 and DSMIPv6, which have been adopted as IP mobility protocols for the 3GPP EPC architecture, are inline with the centralized and hierarchical of the network architecture.
Following the hierarchical architecture, the centralized mobility management protocols rely on the mobility anchor (HA in MIPv6 and LMA in PMIPv6) to enable the mobility support. Therefore, both the mobile context and traffic encapsulation need to be maintained at the mobility anchor. The number of mobile devices and their traffic demand increases exponentially make the centralized mobility management solutions encounter several problems and limitations as stated in [19, 21]. Among them, we just highlight the following issues:

- *Sub-optimal routing and end-to-end delay*: Since the data traffic always traverses the central mobility anchor, it often results in a longer route, especially when the CN and the MN are close to each other but far from the anchor. The same thing happens in case of Content Delivery Networks (CDN), in which the content providers place their data to the edge of the network. As a result, the end-to-end delay will be increased.

- *Scalability problem*: Maintaining MN's context and processing the packets from/to the MN usually require resources of the mobility anchor as well as the networks (require more bandwidth of the links close to the mobility anchor), thus reducing the scalability of the system.

- *Resource waste*: The mobility service is always provided even for the sessions that do not require the mobility management support e.g., the sessions which launch and

complete while the node is connected to the same layer 3 point of attachment, or the sessions which can handle mobility at the application layer e.g., SIP-based sessions. Thus, by providing mobility support for the MN/service when it is really needed, the network resource (e.g., reducing signaling load) can be saved.

- *Reliability*: The central mobility anchor in general poses a bottleneck and single point of failure.

2.2 Distributed Mobility Management

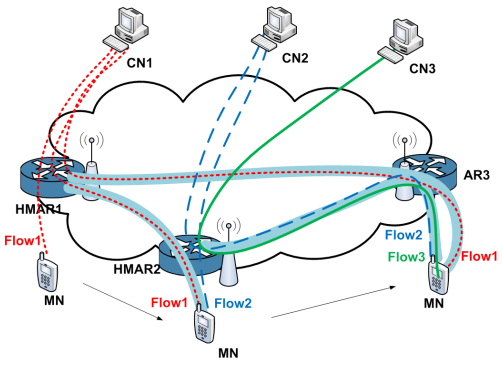
As stated in the previous section, the mobile network is currently evolving towards the flat architecture. To cope with this evolution, distributed mobility management (DMM) solutions have been proposed. DMM concept aims at addressing the limitations of the centralized mobility approach (e.g., bottleneck and single point of failure, etc.) raised when a large number of mobile devices and data traffic are considered in a flat architecture [19, 21]. DMM is currently a hot topic which gains much interest from both the academia and the industry. The IETF has recently chartered the Distributed Mobility Management (DMM) working group[2] which specifies the solutions allowing for setting up IP networks supporting a distributed anchoring model. The key concepts of DMM are: i) the mobility is distributed among network entities and placed as close as possible to the MN e.g., at the router edge of the access network; and ii) the mobility management is dynamically provided for the sessions that really require service continuity.
Following the DMM requirement (REQ4) in terms of reusing/extending the existing IETF IP mobility protocols (i.e., MIPv6 and PMIPv6, and so on), the existing proposals (e.g., [49, 50]) aim at making these solutions work in a distributed manner by deploying multiple mobility anchors (HA in MIPv6 and LMA in PMIPv6) at the edge of the access network, serving as the default gateway of the mobile node. From the IETF point of view, there are two main groups of solutions: the host-based and the network-based. The host-based approach provides a global (as well as a local) mobility support for the MNs while the network-based provides a local mobility support for the MNs moving in a single domain.

2.2.1 DMM from IETF Point of View

Host-based DMM Approach The terminology used by this subsection names an access router that provides the host-based DMM mobility support is a Host-based Mobile Access Router (HMAR). The HMAR, similar to HA, is a mobility anchor which allocates a network prefix to the MN and maintains the binding cache for its registered MNs. The current HMAR (cHMAR) is the one to which the MN is currently attached, while the anchor HMAR (aHMAR) of an address/session is the one where the prefix in use is allocated (and the session is initiated using this address as the source address).
In the host-based approach, the MN is required to participate to the signaling process. There are two main schemes for the host-based approach. In the first scheme, the tunneling for the handover session is established between the anchor HMAR and the MN as similar to the MIPv6 protocol. In the second scheme, the tunnel is established between the current HMAR and the anchor one.
Regarding the first host-based DMM scheme as proposed in [51, 26], whenever an MN attaches to a HMAR it gets an IPv6 address. The cHMAR plays the role of HA for the address allocated at its network. While attaching to the cHMAR, the MN can start

[2]IETF DMM WG: https://ietf.org/wg/dmm/charter/

new communications (flows) with the CNs using the current address as the source address of the flows. These new flows are then routed in a standard way without the tunneling mechanism. When the MN performs a handover, if these ongoing flows are still alive, these flows are routed via the routers where the flows were originally initiated (aHMAR) using the tunneling mechanism. Thus, the MN needs to register its current topological location to each aHMAR (corresponding to each active HoA in use) by means of BU/BA messages. In this case, the current HoA actually plays the role of CoA. A bi-directional tunnel is then established between each aHMAR and the MN. Thus, the traffic passes through the mobility anchor via the bi-directional tunnel. Fig. 2.5 and Fig. 2.6 represent an example scenario of host-based DMM support.
It is noted that the MN should perform a location update process for each active IP address. As a result, it requires the MN to manage the list of active HoAs and the associated aHMARs, as well as the list of active sessions using the corresponding HoA. Moreover, the MN needs an additional mechanism which allows to select the right IP address to use for each session. The binding cache of the HMARs and the list of active sessions of the MN are illustrated in Fig.2.5b.



(a)

HMAR1's Binding Cache

HoA	CoA
Pref1::MN	Pref3::MN

HMAR2's Binding Cache

HoA	CoA
Pref2::MN	Pref3::MN

MN's Binding List

HoA	Anchor	Flow
Pref2::MN	HMAR2	Flow3
Pref2::MN	HMAR2	Flow2
Pref1::MN	HMAR1	Flow1

(b)

Figure 2.5 – Mobility management in the host-based approach (scheme 1): (a) Operation description. (b) Binding cache.

Additionally, as a global mobility, another scenario should be taken into account in which the MN moves to a typical access router's area (without supporting the host-based DMM) as discussed in [27, 25]. In this circumstance, the MN should select one among the active IP addresses to be served as the source address, and the associated aHMAR as the HA. The MN then performs the normal MIPv6 operation. For example, as shown in Fig.2.5, the MN attaches to a typical access router (AR3). After getting a prefix (Prefix3::/64), the MN configures its IP address (Pref3::MN/64). When the MN starts a new session (Flow3), it selects HoA2 and HMAR2 as the source address and the corresponding HA, respectively. As a result, the Flow3 is routed via the tunnel HMAR2-MN. Regarding the ongoing flows, the Flow1 and Flow2 are then routed via HMAR1 and HMAR2 using the tunnel HMAR1-MN and HMAR2-MN, respectively.
As stated earlier, the MN needs to inform all active aHMARs about its current location by means of BU/BA messages. Thus, the mobility signaling cost (over the air) is relatively high. As a result, the second host-based DMM scheme is proposed in order to reduce the mobility signaling cost of the MN (see Fig.2.7). In this case, the MN only needs to exchange the

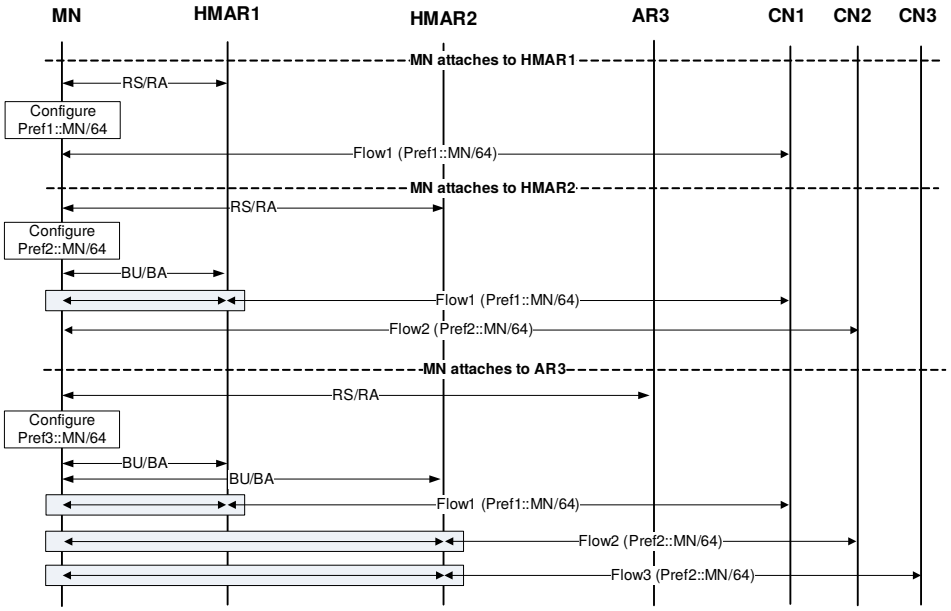
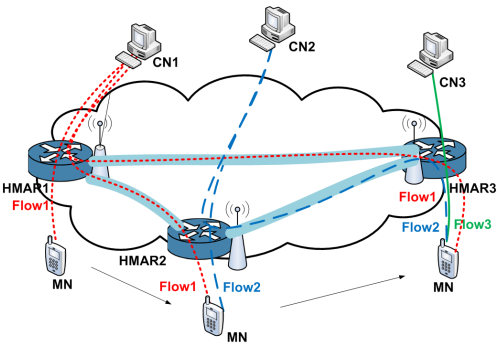


Figure 2.6 – Signaling for the mobility management in the host-based approach (scheme 1).

BU/BA messages with the current mobility anchor [24]. The BU includes the MN's prefixes in use and the corresponding aHMAR. Based on this information, the BU/BA messages are exchanged between the cHMAR and each aHMAR which allows establishing the tunnel between them. The active sessions are then routed via the corresponding aHMAR utilizing the tunneling mechanism. Again, if the MN moves to a typical AR's area, the tunnel is established between the MN and the aHMAR as similar to the previous host-based scheme.



(a)

HMAR1's Binding Cache

HoA	Tunnel
Pref1::MN	HMAR3

HMAR2's Binding Cache

HoA	Tunnel
Pref2::MN	HMAR3

HMAR3's Binding Cache

HoA	Tunnel
Pref1::MN	HMAR1
Pref2::MN	HMAR2
Pref3::MN	Null

MN's Binding List

HoA	Anchor	Flow
Pref3::MN	HMAR3	Flow3
Pref2::MN	HMAR2	Flow2
Pref1::MN	HMAR1	Flow1

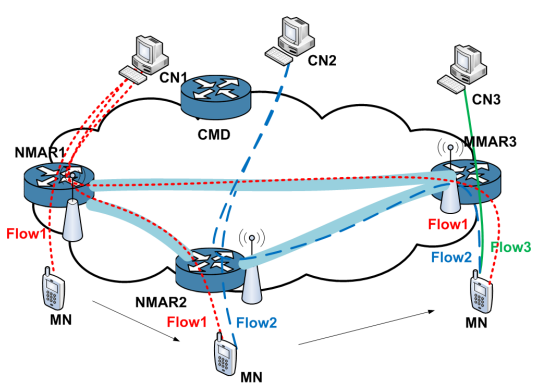
(b)

Figure 2.7 – Mobility management in the host-based approach (scheme 2): (a) Operation description. (b) Binding cache.

It is important to note that the MN keeps the information of the active HoAs and their associated aHMAR when having at least one active session using this HoA. Otherwise, the information will be deleted. Thus, in this thesis, we suggest that at least one HoA should be considered as a global address and should be kept throughout its lifetime e.g., an address allocated at the MN's typical location.

Network-based DMM approach Unlike the host-based DMM, the network-based approach does not require the MN to participate in the mobility signaling process. To do so, a new network entity, namely Network-based DMM Access Router (NMAR) is introduced. The NMAR is an access router supporting the network-based DMM mobility. The NMAR thus performs both LMA's and MAG's functionality. Acting as a MAG, the NMAR detects the attachment of the MN, while as an LMA it allocates a HNP to the MN. Again, we introduce two logical NMARs: i) a current NMAR (cNMAR) is the NMAR to which the MN is currently attached; and ii) an anchor NMAR (aNMAR) is the NMAR to which the MN's HNP is allocated (the session is initiated).

Similar to the host-based DMM, when an MN attaches to a NMAR, it obtains an IPv6 address. Typically, it uses the current IP address to start new sessions. The data traffic is routed using the normal IP routing without any tunneling mechanism. If the MN performs a handover and some sessions are still alive (namely handover sessions), the mobility management procedure is activated as follows. The cNMAR, acting as the MAG, exchanges PBU/PBA messages with the aNMAR which acts as the LMA of the flows initiated at the aNMAR. Once the PBU/PBA signaling is completed, a tunnel is established between the cNMAR and the aNMAR for the sessions initiated at the aNMAR. However, an important question raised is that how the nNMAR learn about the addresses of the aNMARs.



(a)

NMAR1's Binding Cache

HoA	P-CoA
Pref1::MN	NMAR3

MN's Binding List

HoA	Anchor	Flow
Pref3::MN	NMAR3	Flow3
Pref2::MN	NMAR2	Flow2
Pref1::MN	NMAR1	Flow1

CMD's Binding Cache

MN_ID	(Prefix, Anchor)	Current
MN_ID	(Pref3::, NMAR3), (Pref2::, NMAR2), (Pref1::, NMAR1)	NMAR3

(b)

Figure 2.8 – Mobility management in the PMIP-based approach: (a) Operation description. (b) Binding cache.

There is several mechanisms allowing the nNMAR to know the address of the aNMARs. The first method [49] relies on a centralized database (namely centralized mobility database, or CMD) which stores the mobility-related information of each MN in the domain such as the list of MN's HoAs, the associated aNMARs' address as similar to in [52]. Although it ensures that the mobility process is totally transparent to the MN, this mechanism introduces again a centralized anchor, however, for control plane only. The data plane is still fully distributed among the network entities. That is the reason why this scheme is considered as a partially distributed scheme. The second method relies on the information provided by the MN as specified in [23]. In other words, the NMAR retrieves the address of the anchor NMARs from the MN. As a result, the MN is no longer transparent to the mobility process. Therefore, in some papers [27, 24] this method is considered as a host-based scheme as stated above.

The diagram in Fig. 2.9 depicts the operations of the partially distributed DMM. When an MN attaches to the network-based DMM domain (for example at NMAR1), after detecting

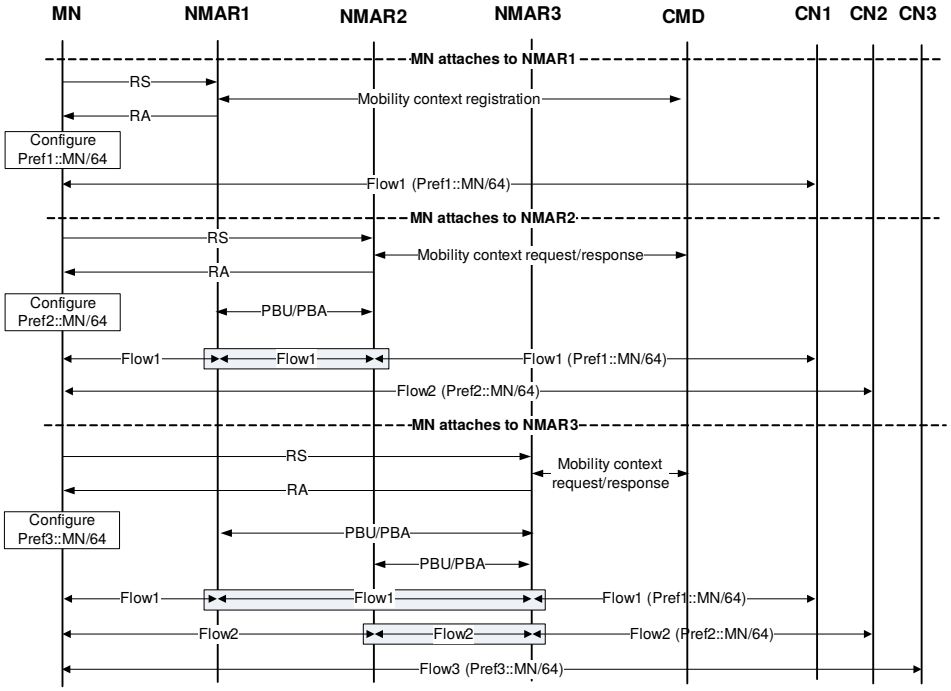


Figure 2.9 – Signaling for the mobility management in the network-based approach.

the presence of a new MN by means of receiving a RS message (including the MN's ID), the NMAR1 allocates a HNP (Pref1::/64) for the MN. It then sends a mobility context request (MC-Req) message including the MN_ID and the Pref1::/64 to the CMD to register the new prefix and retrieve the existing mobility context of the MN (if exist). The CMD then checks its mobility database for this MN. Since it is the first time the MN is attached to this domain, there is no entry for it. Therefore, the CMD creates an entry (for the MN) including the MN_ID, Pref1::/64 and the associated NMAR (NMAR1). The CMD sends a mobility context response (MC-Res) message indicating that the information of the MN is successfully registered. Afterwards, the NMAR1 sends a RA including the allocated prefix (Pref1::/64) to the MN. Based on this information, the MN configures its IPv6 address (Pref1::MN/64) and starts a new communication with the CN1 (Flow1), following the normal way. As the MN moves to the access network of NMAR2, the NMAR2 allocates a new HNP (let say Pref2::/64) for the MN. It then sends a MC-Req message to the CMD for the new prefix registration and for retrieving the existing mobility context of the MN. Upon receiving the MC-Req message and searching its mobility context table, the CMD updates the MN's mobility entry corresponding to the new prefix (as in Fig. 2.8). The CMD then replies by a MC-Res message including the MN_ID and the list of its active prefixes, and the associated NMARs (in this case is Pref1::/64 and NMAR1). Upon the reception of the MC-Res message, the NMAR2 updates its BCE and routing for Pref2 and sends a RA to the MN which includes the Pref2::/64. The PBU/PBA messages are then exchanged between the NMAR2 and the NMAR1 to sets up the bi-directional tunnel between them for the Flow1. Regarding the MN, after receiving a RA, it configures its IP address (Pref2::MN) and uses it to start a new communication with the CN2 (Flow2) in a normal way. The similar thing happens when the MN moves to NMAR3. In this case, the Flow1 and Flow2 are routed through the NMAR1 and NMAR2, respectively. In the mean time, the Flow3 which is initiated when the MN attaches to NMAR3, is routed in a normal way without

the tunneling mechanism.

Besides, there are proposals which apply the DMM concepts into the PMIPv6 domain. For example, in [53], the locally assigned prefixes mechanism within a PMIPv6 domain is proposed. In this case, the MAG can attribute its own prefix (the so-called local prefix) to the MN which can be used for the communication by passing the LMA when the MN is currently attached to the MAG. The MN can still use the IP address allocated by the LMA in a typical PMIPv6 way.

2.2.2 DMM Consideration in 3GPP

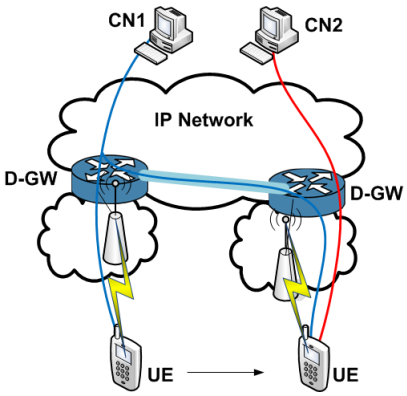


Figure 2.10 – Mobility management for 3GPP

In order to deal with a huge number of traffic demands as well as the revenue per data decreasing phenomenon, 3GPP proposes such traffic offload mechanisms as SIPTO, LIPA and IP Flow Mobility (IFOM). The main idea is that the user data can be routed bypassing the core network based on certain conditions. In more details, SIPTO supports offload of certain types of traffic directly to the Internet and away from the mobile core network. It is done by selecting a set of S-GWs and P-GWs that are geographically/topologically close to the User Equipment's point of attachment (UE is an MN following the 3GPP terminology). However, the offloaded traffic cannot access the operator services. On the other hand, LIPA enables a UE connected via a Home eNB (HeNB) to access the IP capable entities in the same residential/enterprise IP network without the data traversing the mobile operator's core. Although, SIPTO/LIPA is similar to DMM in terms of traffic offloading (mitigating the traffic aggregation at the core network), there is a limited mobility support. For example, LIPA supports only the mobility between HeNBs managed by the same Local-GW (L-GW) while SIPTO enables mobility support for the case S-GW/P-GW is at/above Radio Access Network (RAN). In other words, 3GPP has not yet considered the mobility of UE, which may result in service disruption when a UE is on the move. In fact, SIPTO/LIPA can be considered as a step towards DMM from conventional centralized/hierarchical approaches. It comes from the fact that based on SIPTO/LIPA the functionality of P-GW is distributed by deploying multiple L-GWs. In the next step, by re-using the existing S5 interface (PMIPv6 tunneling), the mobility between the L-GWs can be enabled. From that point, it is feasible to support DMM in LTE/SAE by simply installing the DMM functionality at the distributed L-GWs (called Distributed Gateway or D-GW) as illustrated in Fig. 2.10.

2.3 Other Considerations

2.3.1 Mobility across Heterogeneous Networks

With the evolution of mobile communication systems (wireless technology and network architecture), heterogeneous networks provide the possibility to greatly increasing capacity at a low cost. In this context, the seamless mobility across different types of wireless access technology e.g., WLAN, WiMAX and LTE needs to be taken into account. Regarding the network infrastructure, IEEE 802.21 Media Independent Handover (MIH) services allow optimizing the handovers between heterogeneous IEEE 802 and cellular networks. The handover performance can be enhanced using the layer-2 information available from IEEE 802.21 services. From the mobile node point of view, to maintain the session continuity, additional techniques (as specified in [54]) should be considered which allow the MN to obtain the same IPv6 address after handover across different access technologies. Among them, the logical interface technique [55] can help to hide the different access technologies, thus, the changing of interface is transparent to the IP stack. Moreover, the interfaces of the MN can be active at the same time, which helps reducing the handover latency.

2.3.2 Network Mobility

Network Mobility (NEMO)[3] refers to the mobility of an entire network which changes its point of attachment to the Internet. Thus, the main purpose of NEMO support is that it allows every node in the mobile network to be reachable while moving around. Moreover, the mobility should be transparent to the nodes insides the mobile network. The basic network mobility support is based on MIPv6 to enable the network mobility in an IPv6 network.
In order to provide the mobility support for a Mobile Network, a specific gateway called Mobile Router (MOR) is introduced. The MOR will be connected to the fixed infrastructure and provides connectivity to the nodes inside the Mobile Network. Like the mobility support of a mobile node (host-based approach), the NEMO basic support (as specified in [56]) is also based on the bi-directional tunnel between the MOR and its HA to enable mobility support when the MOR is away from home. Thus, as a topological anchor point of MOR's address, the data packets addressed to the mobile network are delivered to the HA, which then tunnel them towards the MOR. The MOR, after removing the tunnel headers, forwards the data packets to the destination inside the mobile network. Note that similar to normal MIPv6 operation where the binding association between the HoA and the CoA is maintained in the Binding Cache, in NEMO, the HA might also keep the Mobile Network Prefixes (MNP) in the corresponding BCE. As a result, in a large-scale development, the MNP allocation should be considered as in [57].

2.3.3 Comparison between the Mobility Management Approaches

As stated earlier, the performance of a mobility management protocol is typically measured using such metrics as signaling cost, handover latency, and packet loss. Based on these metrics, various papers have been presented to evaluate the performance of the mobility management protocols.
Comparative performance analysis for the host-based mobility management protocols e.g., MIPv6, FMIPv6, HMIPv6 and F-HMIPv6 in terms of signaling cost, handover latency, and packet loss has been carried out in [58, 30, 59]. In [31, 60, 61], the authors also took into

[3]NEMO IETF WG: http://datatracker.ietf.org/wg/nemo/

account the network-based mobility management protocols e.g., PMIPv6 and FPMIPv6 in the comparative performance analysis. From these analysis, some conclusions are: i) Using layer 2 information generally helps to reduce the handover latency and packet loss at a cost of signaling overhead. However, it depends on each link-layer technology; ii) The network-based mobility management protocols reduce the signaling overhead over the air of the MN compared to the host-based mobility protocols; and iii) Typically, the handover latency and the signaling cost depend on the network topology in use. In other words, the hop distance between the network entities is an important factor influencing the performance of these protocols.

Regarding DMM, a lot of research publications [22, 23, 24, 25, 26, 27] have carried out the analysis on different DMM approaches, compared them with the conventional mobility managements in terms of signaling cost, packet delivery cost, handover delay, packet loss and end-to-end delay. The results from these analysis showed that DMM is a promising mobility management scheme. In details, in [22] the authors conducted a simulation to compare DMM and MIPv6 (with handover optimizations). The simulation results showed that DMM outperforms MIPv6 in terms of handover delay and TCP delay. In [24], both qualitative and quantitative comparison for centralized mobility management protocols and DMM protocols are provided. Also, the comparison in terms of handover latency, signaling cost and data delivery cost has been conducted in [25].

Bibliography

[1] "Cisco visual networking index: Global mobile data traffic forecast update, 2012-2017," White Paper, Cisco Inc., Feb. 2013.

[2] S. Kurnia, H. Lee, and S. Yang, "Understanding consumers' expectations of mobile data services in australia," in *Management of Mobile Business (ICMB)*, July 2007.

[3] "Cisco vni service adoption forecast, 2012–2017'," White Paper, Cisco Inc., 2013.

[4] "Tablet demand and disruption: Mobile users come of age'," Blue Paper, Morgan Stanley, Feb. 2011.

[5] A. Smith, "Mobile access 2010," Pew Research Center, Tech. Rep., Jul. 2010.

[6] "Ericsson mobility report: On the pulse of the networked society," Ericsson, Tech. Rep., Jun. 2013.

[7] C. Makaya and P. Samuel, "An architecture for seamless mobility support in ip-based next-generation wireless networks," *Vehicular Technology, IEEE Transactions on*, vol. 57, no. 2, pp. 1209–1225, 2008.

[8] Z. Zhu, R. Wakikawa, and L. Zhang, "A survey of mobility support in the internet," RFC 6301, Jul. 2011.

[9] I. Akyildiz, J. Xie, and S. Mohanty, "A survey of mobility management in next-generation all-ip-based wireless systems," *Wireless Communications, IEEE*, vol. 11, no. 4, pp. 16–28, 2004.

[10] K. Zhu, D. Niyato, P. Wang, E. Hossain, and D. In Kim, "Mobility and handoff management in vehicular networks: A survey," *Wirel. Commun. Mob. Comput.*, vol. 11, no. 4, pp. 459–476, Apr. 2011.

[11] A. C. Snoeren and H. Balakrishnan, "An end-to-end approach to host mobility," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '00, 2000.

[12] M. Atiquzzaman and A. Reaz, "Survey and classification of transport layer mobility management schemes," in *Personal, Indoor and Mobile Radio Communications (PIMRC)*, Sep. 2005.

[13] E. Wedlund and H. Schulzrinne, "Mobility support using sip," in *ACM International Workshop on Wireless Mobile Multimedia (WOWMOM)*, 1999.

[14] H. Schulzrinne and E. Wedlund, "Application-layer mobility using sip," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 4, no. 3, pp. 47–57, Jul. 2000.

[15] D. Damic, *Introducing L3 network-based mobility management for mobility-unaware IP hosts.* Springer Netherlands, 2007, pp. 195–205.

[16] D. Saha, A. Mukherjee, I. Misra, and M. Chakraborty, "Mobility support in ip: A survey of related protocols," *IEEE Network*, vol. 18, pp. 34 – 40, 2004.

[17] R. Moskowitz and P. Nikander, "Host Identity Protocol (HIP) Architecture," RFC 4423, May 2006.

[18] H. Soliman, "Mobile ipv6 support for dual stack hosts and routers," RFC 5555, Jun. 2009.

[19] H. A. Chan, H. Yokota, J. Xie, P. Seite, and D. Liu, "Distributed and dynamic mobility management in mobile internet: Current approaches and issues," *Journal of Communications*, vol. 6, no. 1, 2011.

[20] H. Chan, D. Liu, P. Seite, H. Yokota, and J. Korhonen. (2013, Dec.) Requirements for distributed mobility management. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-ietf-dmm-requirements-12

[21] H. Chan. (2011, Oct.) Problem statement for distributed and dynamic mobility management. Internet draft. [Online]. Available: http://tools.ietf.org/search/draft-chan-distributed-mobility-ps-05

[22] P. Bertin, S. Bonjour, and J.-M. Bonnin, "Distributed or centralized mobility?" in *Proceedings of the 28th IEEE Conference on Global Telecommunications, GLOBECOM*, 2009.

[23] F. Giust, A. De La Oliva, C. J. Bernardos, and R. Da Costa, "A network-based localized mobility solution for distributed mobility management," in *Wireless Personal Multimedia Communications (WPMC)*, 2011, pp. 1–5.

[24] J.-H. Lee, J.-M. Bonnin, P. Seite, and H. Chan, "Distributed ip mobility management from the perspective of the ietf: motivations, requirements, approaches, comparison, and challenges," *Wireless Communications, IEEE*, vol. 20, no. 5, pp. 159–168, 2013.

[25] T. Condeixa and S. Sargento, "Dynamic mobile ip anchoring," in *Communications (ICC), 2013 IEEE International Conference on*, 2013, pp. 3607–3612.

[26] H. Ali-Ahmad, M. Ouzzif, P. Bertin, and X. Lagrange, "Distributed dynamic mobile ipv6: Design and evaluation," in *Wireless Communications and Networking Conference (WCNC)*, 2013.

[27] ——, "Distributed mobility management: Approaches and analysis," in *Communications Workshops (ICC), 2013 IEEE International Conference on*, 2013.

[28] D. Johnson, C. Perkins, and J. Arkko, "Mobility support in ipv6," RFC 3775, Jun. 2004.

[29] K. Ren, W. Lou, K. Zeng, F. Bao, J. Zhou, and R. H. Deng, "Routing optimization security in mobile ipv6," *Computer Networks*, vol. 50, no. 13, pp. 2401 – 2419, 2006.

[30] C. Makaya and P. Samuel, "An analytical framework for performance evaluation of ipv6-based mobility management protocols," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 3, pp. 972–983, 2008.

[31] J.-H. Lee, J.-M. Bonnin, I. You, and T.-M. Chung, "Comparative handover performance analysis of ipv6 mobility management protocols," *Industrial Electronics, IEEE Transactions on*, vol. 60, no. 3, pp. 1077–1088, 2013.

[32] H. Soliman, C. Castelluccia, K. E. Malki, and L. Bellier, "Hierarchical mobile ipv6 mobility management (hmipv6)," RFC 5380, Oct. 2008.

[33] R. Koodli, "Mobile ipv6 fast handovers," RFC 5568, Jul. 2009.

[34] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy mobile ipv6," RFC 5213, Aug. 2008.

[35] B. Aboba, M. Beadles, J. Arkko, and P. Eronen, "The network access identifier," RFC 4282, Dec. 2005.

[36] H. Yokota, K. Chowdhury, R. Koodli, B. Patil, and F. Xia, "Fast handovers for proxy mobile ipv6," RFC 5949, Sep. 2010.

[37] K. Hong and S. Lee, "Dynamic multi-step paging scheme in pmipv6-based wireless networks," *Wireless Networks*, vol. 18, no. 1, pp. 33–44, Jan. 2012.

[38] J.-H. Lee, T.-M. Chung, S. Pack, and S. Gundavelli, "Shall we apply paging technologies to proxy mobile ipv6?" in *Proceedings of the 3rd International Workshop on Mobility in the Evolving Internet Architecture*, ser. MobiArch '08, 2008, pp. 37–42.

[39] J.-E. Kang, D.-W. Kum, Y. Li, and Y.-Z. Cho, "Seamless handover scheme for proxy mobile ipv6," in *Wireless and Mobile Computing, Networking and Communications (WIMOB)*, Oct 2008.

[40] G. Kim, "Low latency cross layer handover scheme in proxy mobile ipv6 domain," in *Next Generation Teletraffic and Wired/Wireless Advanced Networking*, ser. Lecture Notes in Computer Science, vol. 5174, 2008.

[41] L. Magagula and H. Chan, "Ieee802.21 optimized handover delay for proxy mobile ipv6," in *Military Communications Conference (MILCOM)*, Nov 2008.

[42] S. Krishnan, R. Koodli, P. Loureiro, Q. Wu, and A. Dutta, "Localized routing for proxy mobile ipv6," RFC 6705, Sep. 2012.

[43] A. Rasem, C. Makaya, and M. St-Hilaire, "O-pmipv6: Efficient handover with route optimization in proxy mobile ipv6 domain," in *Wireless and Mobile Computing, Networking and Communications (WiMob)*, Oct 2012.

[44] G. Giaratta, "Interactions between pmipv6 and mipv6: Scenarios and related issues," RFC 6612, May 2012.

[45] N. Neumann, J. Lei, X. Fu, and G. Zhang, "I-pmip: An inter-domain mobility extension for proxy-mobile ip," in *IWCMC*, Jun. 2009.

[46] Z. Ma, K. Wang, and F. Zhang. (2012, Jan.) Network-based inter-domain handover support for pmipv6'. Internet draft. [Online]. Available: https://tools.ietf.org/html/draft-ma-netext-pmip-handover-02

[47] T.-T. Nguyen and C. Bonnet, "Dmm-based inter-domain mobility support for proxy mobile ipv6," in *Wireless Communications and Networking Conference (WCNC)*, April 2013.

[48] "3rd generation partnership project (3gpp); technical specification group services and system aspects; network architecture (release 12)," TS, 3GPP TS 23.002, Dec. 2012.

[49] J. L. P. Seite, P. Bertin. (2013, Feb.) Distributed mobility anchoring. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-seite-dmm-dma-07

[50] F. G. CJ. Bernardos, A. de la Oliva. (2013, Jul.) A pmipv6-based solution for distributed mobility management. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-bernardos-dmm-pmip-02

[51] ——. (2013, Jul.) An ipv6 distributed client mobility management approach using existing mechanisms. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-bernardos-dmm-cmip-00

[52] T. Nguyen and C. Bonnet, "Dmm-based inter-domain mobility support for proxy mobile ipv6," in *Wireless Communications and Networking Conference (WCNC)*, 2013.

[53] J. Korhonen, T. Savolainen, and S. Gundavelli. (2013, Jul.) Local prefix lifetime management for proxy mobile ipv6. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-korhonen-dmm-local-prefix-01

[54] T.-T. Nguyen, C. Bonnet, and J. Harri, "Proxy mobile ipv6 for electric vehicle charging service: Use cases and analysis," in *Personal Indoor and Mobile Radio Communications (PIMRC)*, 2013.

[55] T. Melia and S. Gundavelli. (2013, Oct.) Logical interface support for multi-mode ip hosts. Internet draft. [Online]. Available: http://tools.ietf.org/html/draft-ietf-netext-logical-interface-support-08

[56] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network mobility (nemo) basic support protocol," RFC 3963, Jan. 2005.

[57] R. Droms, P. Thubert, F. Dupont, W. Haddad, and C. Bernardos, "Dhcpv6 prefix delegation for network mobility (nemo)," RFC 6276, Jul. 2011.

[58] N. Montavont and T. Noel, "Handover management for mobile nodes in ipv6 networks," *Communications Magazine, IEEE*, vol. 40, no. 8, pp. 38–43, Aug 2002.

[59] 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," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 7, no. 4, pp. 5–19, Oct. 2003.

[60] J.-H. Lee, T.-M. Chung, and S. Gundavelli, "A comparative signaling cost analysis of hierarchical mobile ipv6 and proxy mobile ipv6," in *Personal, Indoor and Mobile Radio Communications (PIMRC)*, Sep 2008.

[61] J.-H. Lee, T. Ernst, and T.-M. Chung, "Cost analysis of ip mobility management protocols for consumer mobile devices," *Consumer Electronics, IEEE Transactions on*, vol. 56, no. 2, pp. 1010–1017, May 2010.