HDMM: Deploying client and network-based Distributed Mobility Management

A hybrid approach

**Fabio Giust · Carlos J. Bernardos ·
Antonio de la Oliva**

Abstract Mobile operators are now facing the challenges posed by a huge data demand from users, mainly due to the introduction of modern portable devices and the success of mobile applications. Moreover, users are now capable to connect from different access networks and establish several active sessions simultaneously, while being mobile. This triggered the introduction of a new paradigm: the distributed mobility management (DMM) which aims at flattening the network and distributing the entities in charge of managing users' mobility.

In this article, we review existing DMM proposals and describe a hybrid solution which benefits from combining a network-based and a client-based approaches. We analyze the signaling cost and the handover latency of our proposal, comparing them with their centralized alternatives. We also include validation and performance results from experiments conducted with a Linux-based prototype, which show that achievable enhancements depend on the underlying network topology. We argue that the proposed hybrid DMM solution provides additional flexibility to the mobile network operators, which can decide when and how to combine these two approaches.

Keywords Distributed Mobility Management · IP mobility · PMIPv6 · wireless systems · address reachability · cellular architecture · handover mechanisms · experimental evaluation

Fabio Giust
Institute IMDEA Networks & University Carlos III of Madrid,
E-mail: fabio.giust@imdea.org

Carlos J. Bernardos · Antonio de la Oliva
University Carlos III of Madrid,
E-mail: {cjbc, aoliva}@it.uc3m.es

1 Introduction

Mobile connectivity is now far from being a luxury service. Users demand Internet access while on the move, and the volume of traffic generated by mobile subscribers has been exponentially increasing during the last few years. This has been motivated by the incredible success on the development and wider introduction in the market of smart-phones, tablets and netbooks, such as Android, iOS or Windows Phone 8 based terminals, which have changed not only the way users consume data services, but also the place where they do it from. Along with this, the number of available mobile applications has also exploded. Many of these applications benefit today from the use of Internet connectivity and cloud hosted functionality.

As a consequence of this paradigm shift, mobile network operators are witnessing how their networks need to cope with an increasing volume of data, saturating their access links, and triggering the need for additional access technologies to be made available to the users. As radio accesses with more capacity are deployed, and operators migrate their networks to full IP based architectures, such as the WiMAX[1] related standards or the 3GPP Evolved Packet System (EPS)[2], the load will spread between the different access networks. However, currently deployed network architectures assume that all traffic requires mobility support, which causes every packet to traverse the operator's core, leading to its congestion.

Because of the new requirements imposed by mobile users' traffic, operators with a large number of mobile subscribers are now looking for alternative mobility solutions that are more distributed in nature, allowing cheaper and more efficient network deployments capable of meeting their customers' requirements. In particular, there is an effort within the Internet Engineering Task Force (IETF), called *Distributed Mobility Management*[3] *(DMM)*, that is addressing exactly this particular problem. After defining the problem statement [12], the working group is currently analyzing the limitations of existing standardized mobility management protocols, identifying the gaps that need to be covered with new DMM protocols [41]. We summarize the main motivations of distributing the mobility management in Section 2, and we conduct a thorough review of the state of the art in Section 3.

In this article, we propose HDMM, a hybrid DMM solution composed of two independent pieces (Section 4): *i)* a client-based solution, which evolves the Mobile IPv6 architecture to tackle flat network deployments (Section 4.1); and, *ii)* a network-based approach, extending standard Proxy Mobile IPv6 to operate in a distributed way (Section 4.2). We argue that the combination of both approaches – which we describe in Section 4.3 – provides the operator with a very flexible and powerful framework, as the solution can be configured to adapt to different scenarios, taking into consideration not only net-

---

[1] http://www.wimaxforum.org/

[2] 3rd Generation Partnership Project, http://www.3gpp.org/

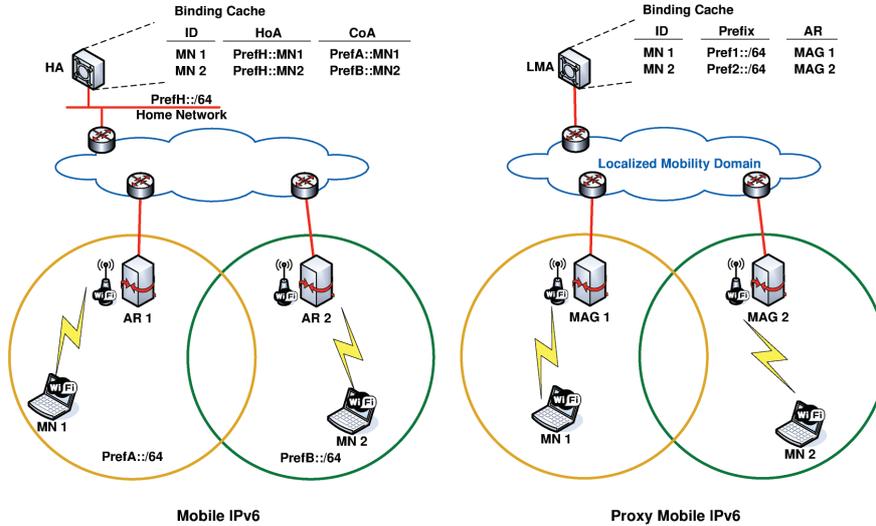[3] http://datatracker.ietf.org/wg/dmm/charter/

Fig. 1 Centralized IP mobility protocols operation.

work topology considerations (including administrative domain boundaries), but also traffic patterns, and terminal capabilities.

This article builds on top of some of our previous works [23–25], where we presented the first core ideas of the two independent DMM components (network and client based). Nevertheless, in this article we go some steps further, adding many refinements and extensions to the original designs, and more importantly, conducting an analytic performance evaluation and a practical validation, based on a Linux implementation. Last, but not least, we also propose how to combine the proposed approaches into a hybrid solution and discuss what the benefits and trade-offs of such a combination are.

The evaluation of HDMM is divided in two parts. We first present an analysis of the overhead, handover latency and end-to-end delay (Section 5), comparing each component of our hybrid DMM approach with Mobile IPv6 and Proxy Mobile IPv6. Then we report on the results obtained from an experimental evaluation using a Linux-based prototype (Section 6). To the best of our knowledge, this is the first working implementation of a DMM solution. Finally, we conclude this work in Section 7.

2 Background and motivation

Recent mobile architectures, such as the Evolved Packet System (EPS), are intended to be fully IP-based both for data and voice communications, triggering a real need for the optimization of IP protocols for mobile networks. In this scenario, IP mobility management plays a key-role in providing the *always-on* and ubiquitous service envisioned by future technologies.

Most of current mobility management solutions derive from Mobile IPv6 (MIPv6) [47], the first mobility protocol standardized by the IETF for IPv6. MIPv6 (see Fig. 1) enables global reachability and session continuity by introducing the home agent (HA), an entity located at the *home network* of the mobile node (MN) which anchors the permanent IP address used by the mobile node, called home address (HoA). The home agent is in charge of defending the HoA's reachability when the mobile node is not at home (i.e., where the HoA is not topologically valid), and redirecting received traffic to the node's current location. When away from its home network, the MN acquires a temporal IP address from the visited network – called care-of address (CoA) – and informs the home agent about its current location by sending a Binding Update (BU) message. An IP bi-directional tunnel between the mobile node and the home agent is then used to redirect traffic from and to the MN.

While MIPv6 requires the explicit participation of the mobile node in the signaling procedures (this is referred to as *client-based* mobility), there is also a family of protocols that provide mobility support without the active involvement of the mobile node[4] (the so-called *network-based* mobility). The effort led to the standardization of Proxy Mobile IPv6 (PMIPv6) [26], developed as an enhancement of MIPv6. In MIPv6, the home agent is replaced by the local mobility anchor (LMA), the network entity in charge of routing data packets in uplink and downlink containing the IPv6 prefixes assigned uniquely to MNs on a per user basis, the home network prefix (HNP), and also storing the MNs' mobility sessions information (see Fig. 1).

PMIPv6 evolved from MIPv6 by relocating relevant functionality for mobility management from the MN to a network node, called the mobile access gateway (MAG), which is the first IP hop and default gateway seen by the terminal. In PMIPv6 indeed, mobility is transparent for MNs: the network learns through standard terminal operation, such as router and neighbor discovery [45], about MN's movements and coordinates routing state information using Proxy Binding Update (PBU) and Proxy Binding Acknowledgment (PBA) messages. The former is sent by the mobile access gateways to the local mobility anchor to indicate the mobile node's location, and the latter is sent as a response to ensure that the procedure succeeded. The LMA stores a binding cache entry (BCE) containing the MN's identifier, its prefix and the serving MAG's address, called proxy care-of address (Proxy-CoA). Users' traffic is encapsulated between the LMA and the Proxy-CoAs. The set of deployed MAGs and the corresponding LMA forms the *localized mobility domain*, in which mobility is completely transparent to the IP stack of the mobile nodes.

Existing standardized IP mobility solutions come at the cost of handling operations at a central point – the mobility anchor – and burdening it with data forwarding and control mechanisms for a great amount of users. The use of a centralized IP mobility approach brings several limitations: *a)* sub-optimal routing, as traffic always traverses the central anchor, leading to paths that

---

[4] More precisely, we refer here to the active involvement of the IP stack of the mobile node in its mobility support.

are, in general, longer than the direct one between the mobile node and its communication peer; *b)* scalability problems, as existing mobile networks have to be dimensioned to support all the traffic traversing the central anchors, and the anchor itself has to be powerful enough, and; *c)* reliability, as the central entity is a potential single point of failure.

In order to address these limitations – which will soon start becoming an operational problem for large-scale mobile network operators – a new paradigm has gained momentum recently: the so-called Distributed Mobility Management [12,13]. DMM basically develops the concept of a flatter system, in which the mobility anchors are placed closer to the user, distributing the control and data infrastructures among the entities located at the edge of the access network [6]. In the next subsection, we provide an overview of existing DMM proposals.

3 Related work

A key distinguishing feature of a mobility protocol is the main entity in charge of performing the operations on the mobile side. This is the basis for the classical division in client and network-based solutions, which also holds for DMM. However, in DMM we can also categorize network-based solutions according to the level of distribution of the control plane [12, 55]:

- *Partially distributed solutions*, which are characterized by completely distributing the data path among several anchors deployed closer to the end user, but still keeping the control plane centralized.
- *Fully distributed solutions*, which completely distribute both the data and control planes (there is no centralized control entity).

In addition to classifying solutions as client or network-based, given the amount of different DMM solutions that can be found already today, we propose an additional categorization: *i)* clean-slate approaches, proposing novel network architectures, as opposed to the traditional evolutionary ones that usually do not tackle the root of the problems; *ii)* architecture-dependent solutions, such as the different efforts initiated in the 3GPP to offload and/or anchor some traffic flows closer to the user [59]; *iii)* peer-to-peer (P2P) approaches, distributing the mobility management functionality across a P2P network; and *iv)* solutions based on or extending existing IETF protocols [11].

3.1 Clean slate approaches

A quite representative *clean slate* DMM approach can be found in [44], where authors present a novel approach that breaks with current trends on mobility management. The solution proposes the use of routing updates between routers to manage the mobility of the nodes within the domain. It relies on Domain Name System (DNS) updates and lookups to detect the prefix assigned to the

node and Border Gateway Protocol (BGP) signaling to update the internal routing within the domain. Global roaming is also supported by issuing BGP route updates between several Autonomous Systems (ASs). Although the proposal has been discussed within the IETF, a deep performance analysis is still missing. Regarding our other classification criterion, this solution can be considered as client-based, as the mobile node has the responsibility to update its location in the DNS server. Note, however, that it is also partially network-based, as the routing is updated based on BGP signaling exchanged between the routers.

Dynamic Mobility Anchoring (DMA) [7] is a generic solution in which mobility management is offered on a per IP flow basis. Indeed, the design encompasses two roles for an access node, depending on the service offered to the data flows generated by an MN: first, the access node can behave as a visited access node (VAN) when the functionality provided to the MN includes only the provision of IP connectivity. Second, an access node can become an anchor access node (AAN) when it is in charge of anchoring MN's IP flows after it has moved to a different VAN. Packets arriving at the AAN are forwarded to the correct VAN by means of an IP tunnel. This tunnel is established without requiring any extra signaling with the access nodes. A VAN learns the corresponding AAN through packet inspection of uplink traffic. Similarly, an AAN learns the current VAN when receiving encapsulated traffic. In order to address the situation in which there is no uplink traffic, the mobile node is required to send uplink void packets to timely recover connectivity with an AAN. The side effect of this approach is the introduction of unnecessarily latencies at handover execution. This proposal is evaluated in [8] through simulations, but no validation via implementation is documented. This design is extended in [43] to support a prefix relocation mechanism, capable of relocating the prefixes used by the mobile node to prefixes allocated to the serving access router. This requires mobile node modifications to indicate to the network the best moment to perform the relocation.

In [39], authors propose an architecture called Access Independent Mobile Service (AIMS) to improve scalability of the network management service. The proposal is a network-based mobility management protocol where the date plane and control plane are decoupled. Data plane nodes run mobility control functions that are in charge to establish the data paths to transport users' traffic, for instance creating IP in IP tunnels in case a handover takes place. This work can be counted in the partially distributed category, because the control plane functions rely on the Mobility Information Control Server (MICS), that acts as a central controller.

Other existing clean slate approaches leverage the concept of identifier/locator split to provide flatter architectures. In [33], the authors present a novel approach called HIMALIS (Heterogeneity Inclusion and Mobility Adaptation through Locator ID Separation) that advocates for mobility management built on top of the concept of locator and ID separation. End host traffic is routed through the optimal direct path by the swapping of the locators used in the communication, while the connection is not closed as the identifiers are

kept constant. The functionality provided by HIMALIS resembles classical approaches such as the Host Identity Protocol (HIP) [27] or SHIM6 [22], which are not just a proposal to enable mobility management, but rather a new network architecture. In the same way as the HIP/SHIM6 approaches, the main drawback of HIMALIS is on the difficulties to deploy it, given that the hosts' IP stack is considerably changed. A similar approach is followed in [58], where the Locator/Identifier split is obtained through the use of the Locator Identifier Separation Protocol (LISP) [20].

3.2 Architecture dependent solutions

Regarding the second category, *architecture dependent* solutions, it is worth mentioning the relevance of the work being performed in the 3GPP along the lines of flattening the network and distributing the anchors. The 3GPP is currently looking for solutions specifically tailored at reducing the volume of user data traffic traversing operators' core networks, by providing enhanced mechanisms for local breakout and offloading. There are several standardization efforts, such as Selected IP Traffic Offload (SIPTO) and Local IP Access (LIPA) [1], or its extension to provide improved mobility capabilities: LIPA Mobility and SIPTO at the local Network (LIMONET) [2].

Hahn *et al.* propose in [28] and [29] two complementary solutions for packet data network gateway (P-GW) relocation within the 3GPP Release 10 specification. The main idea proposed by both works is the definition of new mechanisms for application aware non-optimal path detection.

Additionally, the work in [5] explores the deployment of client and network based DMM solutions in the EPS architecture, providing a detailed description of the required operations and the re-use of the architectural elements and interfaces.

3.3 Peer-to-peer approaches

One of the key aspects of the DMM concept is the distribution of the mobility management functionality across multiple entities. *Peer-to-Peer* (P2P) paradigms naturally envisage the interaction of such entities.

In [19], the authors present m-Chord, a protocol used to distribute the home agent and foreign agent functionality of Mobile IPv4. Their performance analysis concludes that in some cases their solution performs even better than standard Mobile IP, although in the general case, there is a performance drawback from the use of the P2P technology.

Similar to the previous work, [57] presents a solution for mobility management that distributes the functionality of the home agent across multiple nodes through the use of a P2P approach. The protocol selected for the distribution of the information is Chord. In this solution, MNs and CNs are enabled with a MIPv6-capable module. During handover the MN sends BUs to all the

CNs to timely inform them about the new mobility parameters. The authors argue that one of the main drawbacks of using P2P overlays for mobility management is the lack of coherence between the overlay and the actual physical topology of the nodes. Hence they propose to extend the P2P protocol to consider physical information through a Markov decision process, optimizing the update and query performance.

In [21], a new mobility management protocol based on Distributed Hash Tables (DHT), called Distributed IP Mobility Approach (DIMA) is presented. The protocol is similar to Mobile IP but the home agent functionality is split and spread across different nodes that share a common binding distributed database. The data traffic towards the mobile node is intercepted by one of these nodes, which acts as home agent, anchoring the mobile node's home address. The distributed mobility is achieved by relocating the nodes acting as distributed home agents, closer to the mobile nodes. Differently from MIPv6, the MN does not take active part in handling location updates, as the set of home agents are in charge of transmitting the Binding Update and Acknowledgment signaling.

Finally, the work [56] also describes a DMM solution that leverages a DHT storing the MNs' ID/location pairs. Nevertheless this can be accounted as a client-based solution, because the entities located at the edge of the network are responsible to handle the MN's mobility context coordinated by the messages exchanged with the MN itself, which employs a dedicated hand-off module. The session continuity during handover is granted by the bi-casting mechanism. Authors claim that their DMM solution is less demanding than Fast Handover MIPv6 (FMIPv6) [35] in terms of signaling cost.

3.4 Extension of existing protocols

There are several benefits inherent to the *extension of already established protocols* to support DMM, such as an easier backwards compatibility.

DMM approaches focusing on Mobile IPv6 based solutions try to reduce the impact of the triangular routing on the overall performance. In [42], the ADA (Asymmetric Double Agents) extension to Mobile IP is presented to optimize handover latency and communication delays. These improvements come at the cost of introducing two new entities in the network, the local mobile proxy (LMP), that takes care of the functionality of the home agent in Mobile IP, but is located closer to the mobile node; and the correspondent mobile proxy (CMP), which is located near the correspondent node to provide an optimized route towards the LMP.

A different approach for reducing the HA-MN delay is taken in [52]. This work proposes a solution that enables the use of multiple home agents distributed through the Internet, interconnected by high speed links and communicated through anycast routing. Hence these nodes can be always placed near the mobile node, in this way reducing all the problems of centralized deployments.

Last, but not least, works based on Proxy Mobile IPv6 are mainly focused on providing route optimization mechanisms between mobile access gateways. In [10], authors perform an analysis of the different mobility functions provided by PMIPv6, to then propose a solution splitting these functions across several nodes in the network. Nevertheless, the proposed solution uses for the actual routing of the flows a centralized approach, not providing local breakout of the connections, hence no real distributed mobility is achieved.

In [18], PMIPv6 route optimization is proposed. In this solution, the MAGs serving the MN and CN leverage on the information stored at the LMA to establish a direct tunnel between them, so a better path can be used for the communication. This mechanism still makes use of a tunnel for the whole duration of the data session. The solution is only applicable to the case in which the CN is also attached to the same PMIPv6 domain than the mobile node.

Some of the previously highlighted drawbacks are partly mitigated by the solution proposed in [53], where a different Route Optimization technique for PMIPv6 is discussed. The proposed protocol either needs the CN to be connected to the PMIPv6 domain or to be able to interpret some modified PMIPv6 signaling messages.

The proposal described in [54] suggests to split the functionality of the localized mobility anchor (LMA) of PMIPv6 into two distinct nodes: a control plane LMA (CLMA) and a data plane LMA (DLMA). The former maintains the mobility sessions for the MNs, whereas the second is the anchor for the MNs' traffic. The CLMA also assigns the most suitable DLMA to the MNs. This proposal relieves the LMA's burden, but, in general, does not fit for flat architectures, as the DLMA/MAG hierarchy is preserved, along with the tunnels, which are established for the whole duration of a data session. The solution, however, envisions an operating mode by which, if the MN and CN are under the same CLMA's administration, route optimization can be set up between the corresponding MAGs.

Three mobility schemes are proposed in [32]: signal-driven PMIPv6, data-driven distributed PMIPv6 and signal-driven distributed PMIPv6 which explore partially and fully distributed solutions. The three mechanisms rely on control/data split (for the partially distributed solution) and multicast or peer-to-peer communication (for the fully distributed one) to route the data towards the mobile node through the optimal path.

In the article [9], the authors present an extension for Proxy Mobile IPv6 that enables the local mobility anchor to select an entity to handle a given mobile node's flow. The anchoring function will follow the mobile node as it roams across the mobility domain. The new entity in charge of performing route optimization between the MAGs is called intermediate anchor (IA). This entity is in charge of establishing tunnels with the old and the new MAGs, hence providing connectivity between them. The main problem of this solution is that it cannot provide the optimal path, but just an approximate one.

Finally, a modification of the DMA proposal [7] is proposed in [48] to take into account legacy PMIPv6. The modified DMA solution relies on mobility

capable access routers (called MARs) that exchange PBU and PBA messages to update the MN's location and IP addresses. MARs also interact with a central database to retrieve the mobility sessions and coordinate the routing state for the MNs. An analytic evaluation of such protocol is provided in [3].

Last, the following two articles envision a DMM-like scheme for the NEMO basic support protocol [16]. In [40], many distributed home agents (DHA) are deployed to facilitate a mobile router to establish an optimized path with the correspondent node. The coordination of the home agents is achieved through the home agents location registration agents (HALRA), which are responsible also for assigning an HA to the mobile router.

Conversely, the authors of [17] propose to use a PMIPv6-based DMM solution similar to [48] to provide mobility support to a network moving around the mobility domain, for instance for an automotive scenario.

To sum up this review of related DMM approaches, Table 1 presents the summary of the different solutions covered in this section, highlighting their main characteristics and classifying them following the proposed taxonomy.

4 HDMM: Hybrid DMM for future mobile network operators

In this section we describe our proposal, called HDMM: Hybrid Distributed Mobility Management for future mobile network operators. It has two main characteristics. On the one hand, it is based on combining a client and a network-based approaches, as we argue this provides operators with a great flexibility and freedom to deploy different configurations of the solution (i.e., different scenarios impose different requirements, which can be more easily met by complementary mobility approaches). Note that this is in line with current 3GPP architectures, in which both network and client-based centralized IP mobility approaches co-exist. On the other hand, our solution is based on extending/evolving current standardized solutions, namely Mobile IPv6 and Proxy Mobile IPv6, because we believe this represent the most feasible and cost-effective solution for both operators and vendors. This allows to build the DMM framework on top of existing product lines, network deployments and benefit from existing expertise in setting up and running standardized mobility protocols.

Network-based mobility approaches do not require any specific IP mobility support on the mobile node, which allows for an easier deployment in some situations. On the negative side, this kind of approach makes more challenging inter-technology mobility and inter-domain roaming, as some security associations have to be in place, and this is not always possible when crossing operator boundaries. HDMM extends Proxy Mobile IPv6 to operate in a distributed way, which can include control and data planes, or just data plane, as will be described later in this article.

Client-based mobility approaches do require specific IP mobility support on the mobile node, as well as potentially complex security configurations. However, if the support is available, and the mobile node can be properly

Table 1 Summary chart of main DMM proposed solutions

Solution	Client-based	Network-based	
		Partially	Fully
Clean slate approaches			
McCann [44]	BGP/IBGP/DNS based		
DMA-Bertin [7]			Automatic learning
AIMS [39]		Data and Control plane separation	
HIMALIS [33]	Loc./ID split		
Zhang [58]		LISP-based	
Architecture dependent solutions			
Hahn [28,29]			P-GW relocation in 3GPP EPC
Bernardos [5]	DSMIPv6-based for 3GPP EPS		GTP/PMIPv6-based for 3GPP EPS
P2P appraches			
m-Chord [19]			multiple HAs and FAs interact through Chord
Zhai [57]	MIPv6 and Chord based		
DIMA [21]			DHT updated with BU and BA messages
Yu [56]	Loc./ID pairs stored in DHT		
Extension of existing protocols			
Liu [42]	MIPv6 based		
Wakikawa [52]	MIPv6 based		
DMA-Chan [10]			PMIPv6 based
Ernst [18]		RO for PMIPv6	
Xue [53]		RO for PMIPv6	
D-PMIPv6 [54]		LMA split into CLMA and DLMA	
Jung [32]		PMIPv6 based	PMIPv6 based
Anchor PMIPv6 [9]		LMA for control plane IAs for data plane	
DMA-Seite [48]		PMIPv6 based	
Li [40]	Distributed HAs for NEMO		
Do [17]		PMIPv6 based for NEMO	

provisioned, this approach allows for more flexibility, as it is easier to perform mobility management when the mobile node plays an active role. Besides,

inter-domain mobility becomes easier, as there is no need for deploying security associations between network entities belonging to different operators, just between the mobile node and the home agent. In this case, HDMM extends Mobile IPv6 to support its distributed operation, as well as its combination with the network-based operation mode, for those cases in which this feature is required.

Note that even though HDMM comprises two solution components, each of them can be used independently. Before describing how each component works, we introduce below some common terminology that is used throughout the article:

- *Distributed Anchor Router (DAR)*. It corresponds to the first IP router (with mobility functionality) which a mobile node attaches to. Upon attachment, the distributed anchor router provides the mobile node with a topologically correct IPv6 address/prefix. In case the mobile node later moves to a different location, this DAR is in charge of ensuring the reachability of the previously delegated address/prefix. In this way, the DAR can be actually considered as a distributed version of the anchors defined by the classical centralized mobility protocols: the home agent and the local mobility anchor.
- *Serving DAR (S-DAR)*. This term is used to refer to the distributed anchor router where the mobile node is currently connected. Note that the mobile node may have visited different DARs before, and might still be using addresses configured from some of them. As described later, this entity can be considered as a modified version of the mobile access gateway (for the case of the network-based component of HDMM). In this article, we consider for simplicity, that a mobile node can only be attached to a single serving distributed anchor router at a time.
- *Previous DAR (P-DAR)*. This term denotes a distributed anchor router that has been previously visited by a mobile node and which is still anchoring an IP address used by one or more active IP flows of the mobile node. For a given mobile node, there might be multiple P-DARs active at a time.

4.1 Client-based HDMM

This section presents the client-based component of HDMM, which is basically a distributed version of Mobile IPv6. Following this idea, the functionality of the Mobile IPv6 centralized anchor – the home agent – is distributed and moved to the edge of the network, so an instance of it is deployed in each default gateway the mobile node may attach to, i.e. the distributed anchor router (DAR) introduced before. In the following we assume the presence of at least one DAR per access network. For some additional details on how the solution operates, the reader is referred to [24].
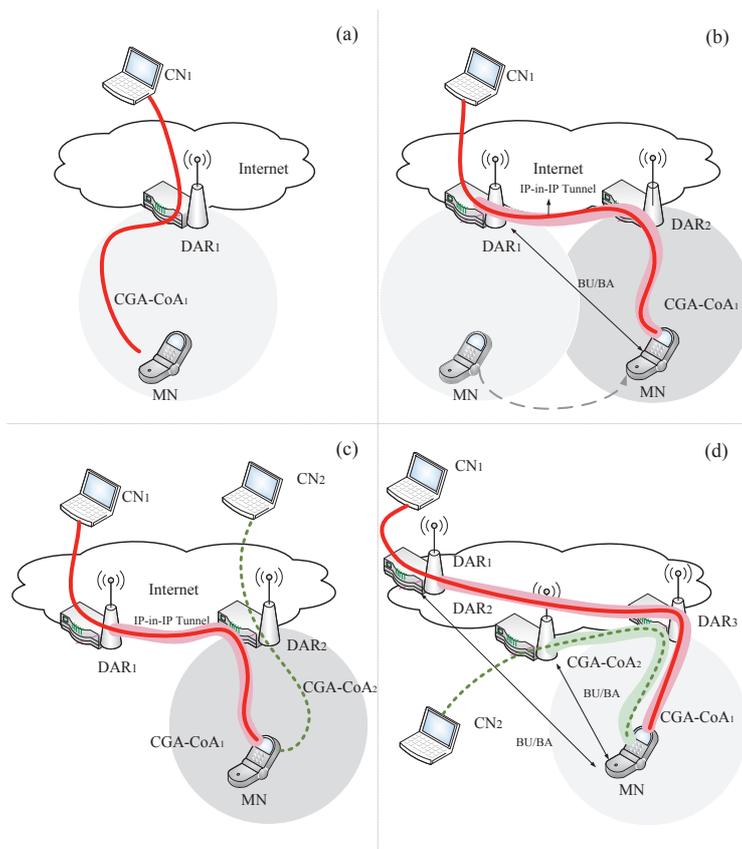
Fig. 2 HDMM client-based component operation.

4.1.1 Solution overview

On every attachment to a new access network served by a distributed anchor router, the MN configures an IPv6 address delegated and locally anchored by the S-DAR: this address can be seen as a home address for the home network managed by the S-DAR. If the mobile node previously visited other access networks in which there was a distributed anchor router deployed, and there are active flows using addresses delegated by some of them, the mobile node can maintain the reachability of these addresses. This is done by sending a regular Mobile IPv6 Binding Update message to each of the previous DARs anchoring an address used by an active flow (distributed anchor routers are effectively playing the role of home agents), using the address configured at the serving DAR as care-of address. A bi-directional tunnel is established between the mobile node and the anchoring P-DAR for each of the home addresses, which is then used to forward the respective data traffic. In this way, active connections

requiring mobility service are maintained, while new sessions can make use of the last configured IPv6 address (i.e., the one delegated by the S-DAR), hence using an IPv6 address that is topologically correct at the current mobile node's location. Compared with regular Mobile IPv6, client-based HDMM introduces the use of several (distributed) home agents, and the additional intelligence on the mobile node to be able to simultaneously manage several home addresses and tunnels, as well as to effectively select the best possible source address for new connections. Note that the operations performed by the mobile node are different from what is standardized in the IP flow mobility (IFOM) extensions, namely [50, 51], as in the DMM case multiple anchors are involved, while in the IFOM case only one anchor (the home agent) is involved, but the different sessions are delivered to the mobile node via multiple network accesses.

Although the operation of client-based HDMM and Mobile IPv6 are very similar, the distributed operation of HDMM might pose additional concerns in terms of security. Securing the communication between the mobile node and every P-DAR through IPsec [15], as done in traditional Mobile IPv6, would be challenging due to the large number of required security associations (note that every DAR may be playing the role of P-DAR). In order to overcome this problem and provide authentication between the distributed anchor routers and mobile nodes, we propose the use of cryptographically generated addresses (CGAs) [4], as introduced in [36]. CGAs are basically IPv6 addresses for which the interface identifier is generated by computing a cryptographic one-way hash function from a public key and the IPv6 prefix. The binding between the public key and the address can be verified by re-computing the hash function and comparing the result with the interface identifier. To authenticate a message, the packet is signed with the corresponding private key, hence the receiver is able to authenticate the message with the knowledge of the address and the public key. CGAs are a powerful mechanism allowing packet authentication without requiring any public-key infrastructure, and hence it is well-suited for this application.

We also suggest an lighter mechanism to authenticate signaling messages, based on the use of a Permanent Home Keygen Token (PHKT). This token is forwarded by a P-DAR to the mobile node in the Binding Acknowledgment message sent in reply to the first BU. For any subsequent movement requiring to maintain the reachability of an address for which the MN has already sent a BU, the following BU messages can be secured using the PHKT exchanged before, reducing the computational load at the receiving P-DAR.

Another security threat that is specific to HDMM is the possibility of performing a redirection attack, where a malicious node tries to use an incorrect care-of address in a Binding Update message. In order to provide a more robust solution, we propose a return routability (RR) procedure similar to the one defined for the Mobile IPv6 route optimization mechanism [47]. A return routability procedure is initiated after a handover, so instead of directly sending a BU message, the mobile node first sends a Care-of Test Init (CoTI) message to the respective P-DAR. This message is replied by the P-DAR with a Care-of Test (CoT) message containing a CoA Keygen Token. The mobile

node can now send a BU using both Home and CoA Keygen tokens to proof its reachability at both the HoA and the CoA. The message and the knowledge of both tokens is a proof that the mobile node is the legitimate node who has sent the Binding Update message and also is reachable at the CoA indicated. This last security improvement incurs in a performance penalty, namely an increase in the handover delay. The enhanced security approach requires four messages to be exchanged between the mobile node and the P-DAR, instead of the two messages of the original solution. In terms of handover delay, this increases the latency by a factor of two, as the new solution requires an amount of time equal to two MN-to-P-DAR round trip times (RTTs) to conclude, instead of just one. The performance of the solution is analyzed in more detail in Section (Section 5).

Fig. 2 shows an example of the operation of client-based HDMM: a mobile node first attaches to a distributed anchor router (DAR_1), configures a locally anchored IP address, starts a new session with CN_1 and then moves to DAR_2, where a new communication with a different CN (CN_2) is started, using the IP address locally anchored at the new DAR.

Note that the operation of HDMM is fully compatible with legacy centralized home agents, as it might be required for some traffic to traverse the mobile network operator's core (e.g., because of service agreements, location privacy or simply for sessions that are known in advance to be long-lived, so it is more efficient to anchor them centrally).

4.2 Network-based HDMM

This section summarizes the operation of the network-based component of HDMM, which is basically a distributed version of Proxy Mobile IPv6. Both the MAG and LMA functions are implemented by the distributed anchor router (DAR). For additional details, the reader is referred to [25].

The network-based HDMM component is characterized by the split between control and data planes. In the following sections we present two approaches for the control plane implementation: *i)* a partially distributed approach, which relies on a central entity to keep track of the movement of the users and the previously visited anchors; *ii)* a completely distributed version, in which the control plane does not use any central entity and signaling is exchanged between the involved anchors instead. Both approaches follow the same data forwarding scheme, which is illustrated next.

4.2.1 Data plane management

A serving DAR provides IP connectivity to the mobile node through a locally anchored IPv6 address. Packets using that address are forwarded by the S-DAR without encapsulation, as a plain IPv6 access router, both in downstream and upstream directions. If the mobile node moves, a new IPv6 address is obtained from the new S-DAR, which is (in general) preferred by the MN to

start new IP flows, so packets benefit from optimal routing. However, ongoing data sessions still need reachability of the old address. Hence a bi-directional tunnel is setup between the S-DAR and the previous DAR to not disrupt the communication. Borrowing PMIPv6's definition, the S-DAR behaves as a MAG, and the P-DAR as an LMA. The MN may have hence a number of flows directly routed by the S-DAR to and from the global Internet without encapsulation, and another set of streams anchored at the P-DAR. Depending on the previous MN's movement history and the active sessions, this situation might be replicated for multiple P-DARs.

At the control plane level, the key element to achieve this traffic configuration is to let the S-DAR interact with the P-DARs so that the correct routing state can be set up. This concept leads to the definition of a partially distributed scheme first.

4.2.2 Partially distributed approach

This solution leverages on a central entity to store the mobility sessions and maintaining the state about S-DAR and P-DARs for all the MNs in the domain. This entity is called central mobility database (CMD), and basically implements all the tasks related to keeping the Binding Cache up to date, as a regular PMIPv6 LMA does, updating its entries with the information received from the DARs. However, its operation differs from the one of a legacy LMA in that the CMD does not perform any data forwarding task, therefore users' data traffic does not traverse it.

Similar concepts can be found in the related work [17, 48]; a server acting as mobility/policy store is queried by the serving anchor, which interacts with the anchors indicated in the response to set up the proper routing configuration. A similar functionality can be found in our scheme, although with a key difference. In our proposal, the central server (the CMD) does not passively provide the response, but it rather takes an active role forwarding the messages to the MN's P-DAR(s), since it is the entity in possession of the whole picture in terms of involved P-DARs and prefixes allocated.

Initial registration: Upon mobile node's attachment to a DAR (see Fig. 3), say DAR_1, the MN's unique identifier in the domain (MN-ID) is retrieved, and an IPv6 global prefix belonging to the S-DAR's prefix pool is reserved for it ($Pref_1$). The pair MN-ID and the prefix are stored locally as part of a temporal binding cache entry (BCE) at the DAR. These parameters are conveyed to the CMD in a PBU message. Since the MN is attaching to the domain for the first time, the CMD has no previous entry for it. Hence a fresh BCE is created, containing as main fields the MN-ID, the MN's prefix and DAR_1's address (the proxy-CoA in the PMIPv6 terminology). The CMD then replies to DAR_1 with a Proxy Binding Acknowledgment (PBA) message, which is mainly a copy of the PBU message received before, meaning that the mobile node's registration is new and no additional information was available at the CMD. DAR_1 finalizes the registration for the temporal BCE previously
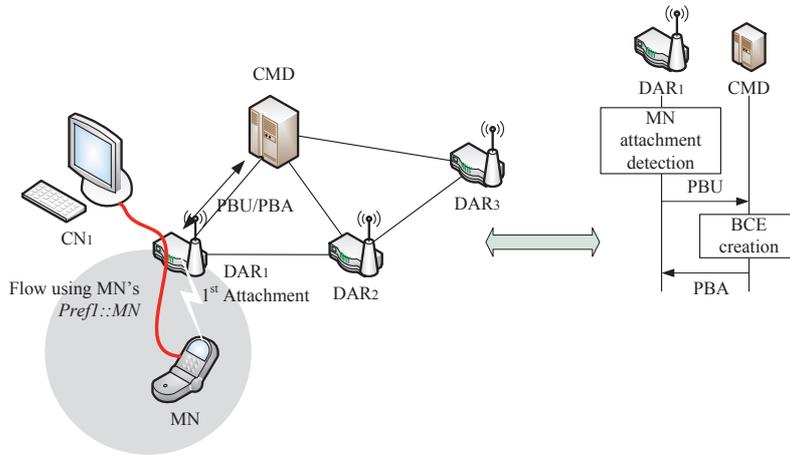
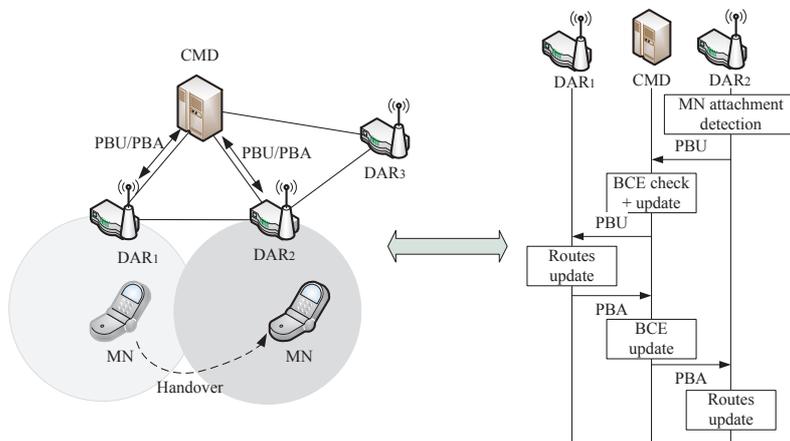**Fig. 3** Partially distributed network-based HDMM: initial registration.

Fig. 4 Partially distributed network-based HDMM: CMD behaves as PBU/PBA relay.

created and unicasts a router advertisement (RA) to the mobile node, including the IPv6 prefix reserved before, that is used by the MN to configure an IPv6 address (e.g., with stateless auto-configuration). Since this address is locally anchored at the S-DAR, no encapsulation nor special handling is required to route packets of IP flows started there.

When a handover occurs, there are several possible signaling schema that can actually be used by the DARs to interact with the CMD and set up all the required state in the network. Each approach assigns a different role to the central mobility database, with different pros and cons associated, in terms of handover latency and signaling overhead:

– the CMD behaves as a PBU/PBA relay,

− the CMD behaves as a DAR locator,
− the CMD behaves as a PBU/PBA proxy.

The CMD behaves as a PBU/PBA relay: When the MN moves from its current access and attaches to another DAR (see Fig. 4), say DAR_2 (now the S-DAR), the L3 handover is handled in 4 phases:

1. DAR_2 reserves an IPv6 prefix ($Pref_2$) from its local pool, storing it in a temporal BCE, and sends a plain PBU to the CMD for registration (as the initial registration phase).
2. Upon PBU reception and binding cache lookup, the CMD retrieves an already existing BCE for the MN. The BCE indicates a DAR's address in the P-CoA field, so the CMD forwards the received PBU message to it (in our example DAR_1), appending to the message the S-DAR's global address (DAR_2). The P-CoA is changed indicating the new S-DAR's address.
3. Upon reception of the PBU from the CMD, DAR_1 sets up its end-point for the bi-directional tunnel towards DAR_2 and adds the required routing entries for $Pref_1$. DAR_1 informs the CMD that these steps have been successfully performed by sending a PBA message.
4. The CMD, after receiving the PBA, adds an item in the BCE called P-DARs list. An entry of the P-DARs list is composed by the pair P-DAR's address and the prefix it allocated to the MN (in our example DAR_1's address and $Pref_1$). Finally, the CMD sends a PBA to the current S-DAR, which includes the P-DAR's address and the associated anchored prefix. This message enables the S-DAR to finally establish the correct routing state, i.e., the bi-directional tunnel with the P-DAR (DAR_1) and the routing entries for $Pref_1$.
5. The S-DAR advertises the local anchored prefix to the MN, and sends an additional RA including the old prefix but indicating a non zero valid lifetime and a zero preferred lifetime. In this way the old address can be correctly used to terminate old data sessions, whilst it is deprecated for new ones, forcing the MN to pick the address advertised by the S-MAR.

Fig. 5 illustrates how old and new IP flows are routed in the domain. Any subsequent mobile node's handover follows the same procedure, involving all the P-DARs that are anchoring active flows incrementally. Indeed, when the CMD receives the first PBU message from the S-DAR, it forwards a copy of the message to the P-CoA and to all the P-DARs indicated in the P-DAR list. All these DARs reply back with a PBA message to the CMD, which then aggregates all the messages into a single PBA sent to the new S-DAR, hence the routing state has been re-configured in the whole domain.

The CMD behaves as DAR locator: This mobility update procedure follows the same steps defined before up to step 2, the moment when the P-DAR receives the PBU message from the CMD. At that point, the P-DAR is aware of the new mobile node's location (because the S-DAR address is contained in the PBU message). Therefore, the P-DAR signals with a PBA message directly
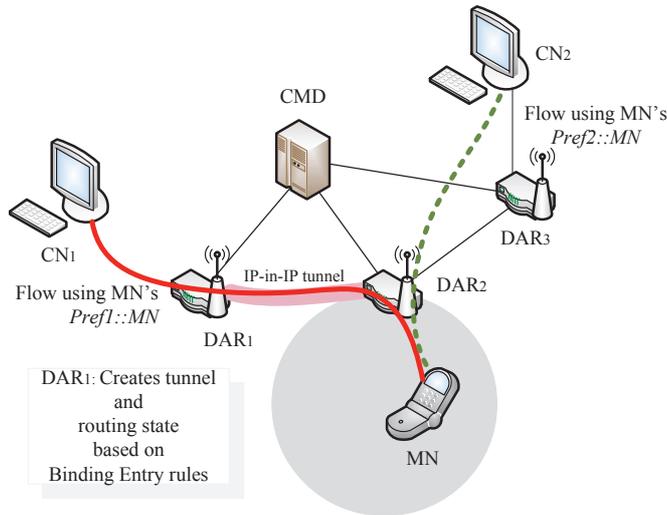
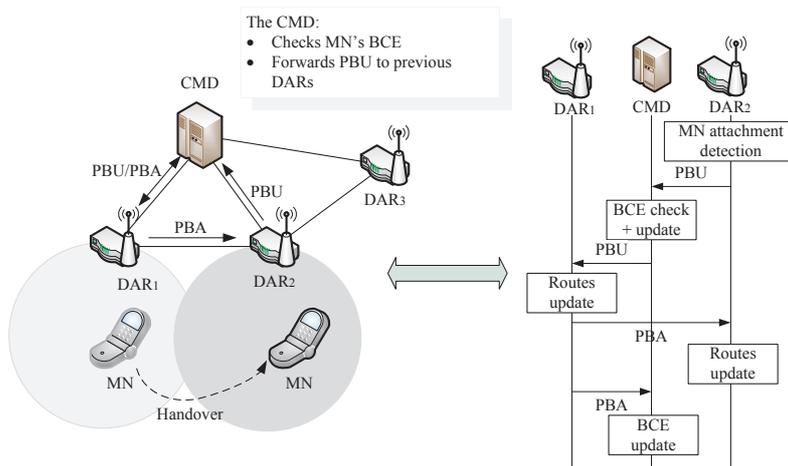**Fig. 5** Partially distributed network-based HDMM: data flow.

Fig. 6 Partially distributed network-based HDMM: CMD behaves as DAR locator.

to the S-DAR the prefix it is anchoring for the MN. A similar message is sent to the CMD too, to maintain the consistency in the database. The routing state can be recovered and the procedure is expected to terminate quicker than the previous scheme. Fig. 6 illustrates the new signaling sequence, while the data forwarding remains unaltered.

The CMD behaves as PBU/PBA proxy: Previous mechanism can be further sped up if the CMD simultaneously replies to the new S-DAR with a PBA message and notifies the P-DARs with a PBU. Indeed, the CMD possesses the
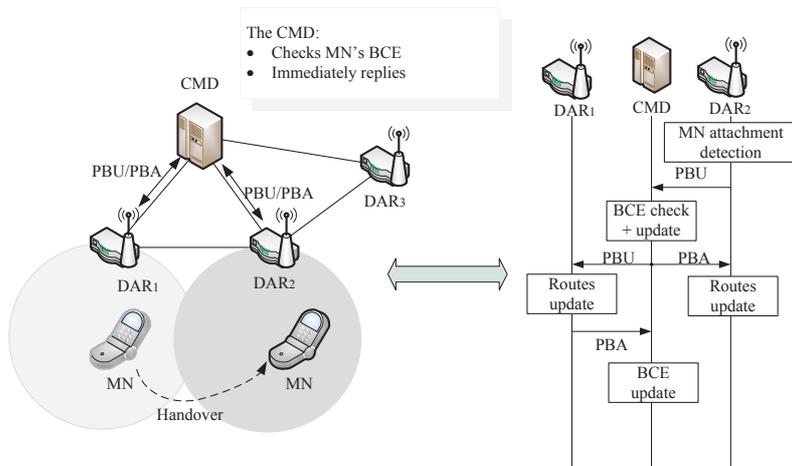
Fig. 7 Partially distributed network-based HDMM: CMD behaves as PBU/PBA proxy.

whole MN's picture, so the serving DAR is notified immediately with a PBA message, including the necessary parameters. In parallel, a PBU message is sent by the CMD to the P-DARs notifying them about the new mobile node's location, so they can establish the required tunnels and routing entries on their side. Every P-DAR, after completing the update, sends a PBA message to the central mobility database to indicate that the operation is concluded and the state has been updated. This scheme is depicted in Fig. 7, where, again, the data forwarding remains the same.

4.2.3 Fully distributed approach

With this approach, the prefix assignment and routing configuration concepts are identical to the schema previously presented, but with one key difference: the PBU/PBA handshake takes place between the new S-DAR and the P-DAR(s) without the involvement of other entities.

The illustrations in Fig. 8 show how an IP flow is handled when generated at the initial DAR (Fig. 8-(a)), how the flow is routed after a handover (Fig. 8-(b)) and how a second flow started at the new S-DAR is routed in the network as compared with previous flows (Fig. 8-(c)). Finally, Fig. 8-(d) exhibits the handover to a third (and in general, to all subsequent) DAR.

The key point is how the S-DAR finds out if the attached mobile node has any active flows anchored at previously visited P-DARs, and, if so, which these P-DARs are, and what IPv6 prefixes they are anchoring. We here propose the following alternative mechanisms:

– Multicasting the PBU sent by the S-DAR to the group formed by all the DARs of the domain. In case no answer (PBA) is received within a timeout interval, the S-DAR may assume this is the first time the MN is joining
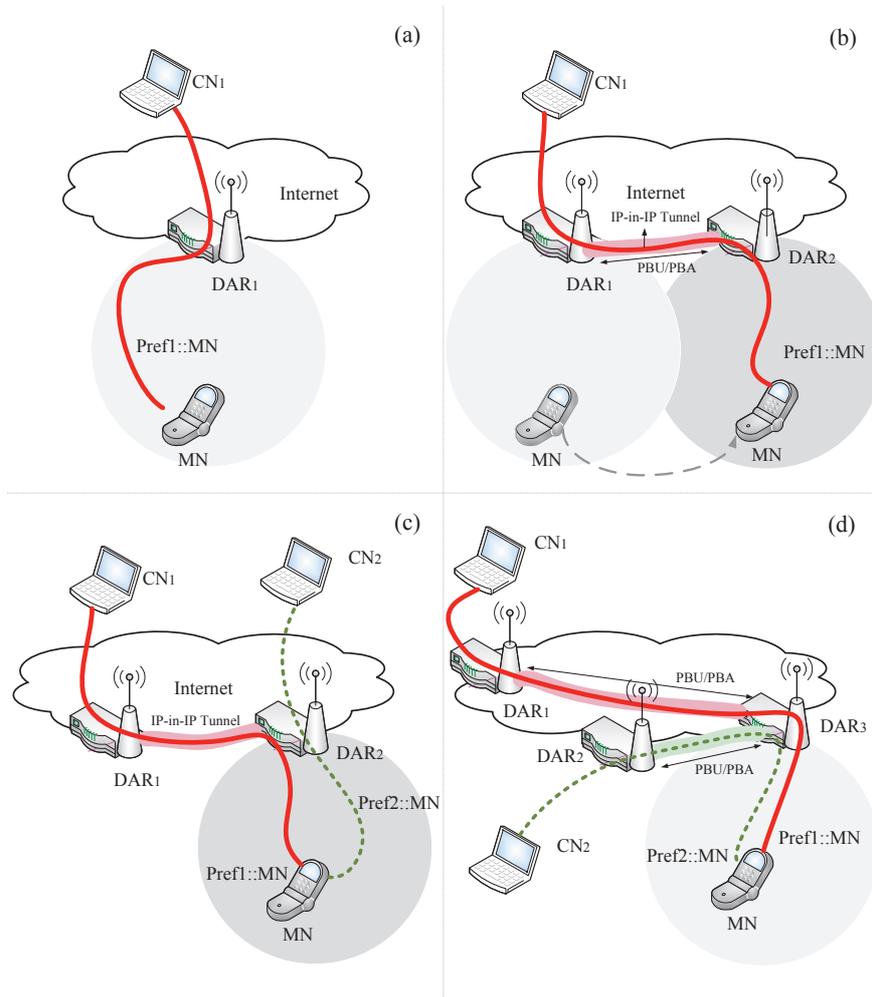
Fig. 8 Fully distributed network-based HDMM: protocol operation.

the network. Unfortunately this approach might not provide a good performance in terms of handover delay and adds unnecessary signaling in the network.

– Layer-2 handover support through Media Independent Handover Services specification (IEEE 802.21) [37]. The latest revisions of the most used wireless technologies such as IEEE 802.11 or IEEE 802.16, already provide support to the so-called *Link Layer Events*. Through these mechanisms, a network interface is able to indicate changes in e.g., point of attachment or re-connection. Therefore, a handover is handled by a dedicated control plane infrastructure by which the movement is prepared, executed and
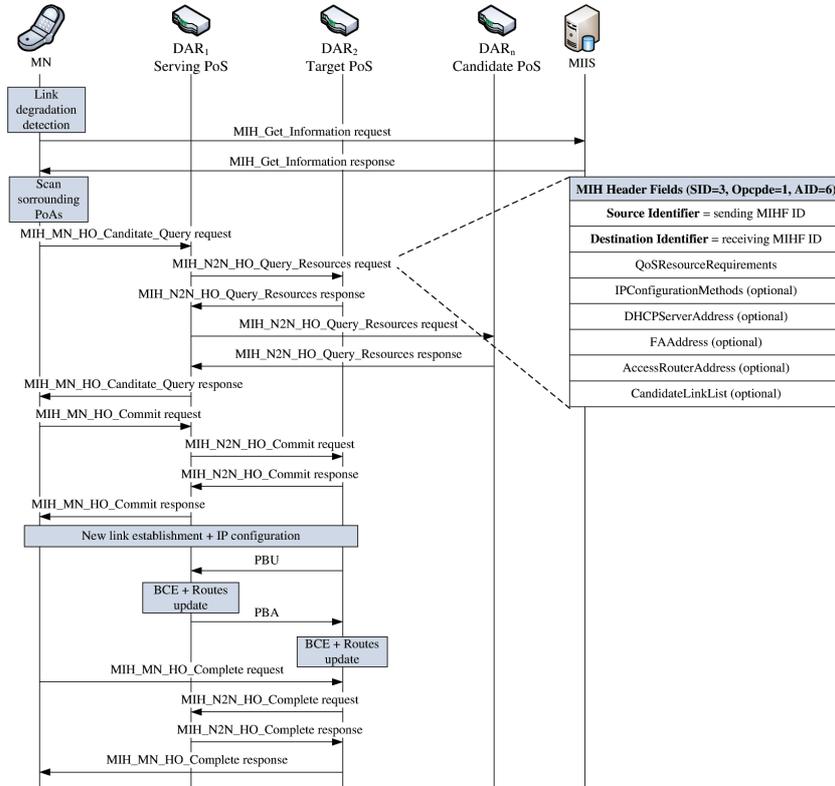
Fig. 9 Fully distributed network-based HDMM: IEEE 802.21-aided message exchange sequence during handover.

completed in a controlled and assisted way, according to the *make-before-break* philosophy. Additionally, the IEEE 802.21 suite is intended to allow inter-technology handovers, providing support to mobile nodes roaming within a heterogeneous environment. Fig. 9 presents the detailed procedure including the IEEE 802.21 signaling required to perform a fully distributed network-based handover. In the figure, DARs and Points of Service (PoS) are co-located, whilst Points of Attachment (PoA) are omitted to keep the chart simple. Indeed, the diagram highlights the message exchanges between the MN and the S-DAR, and also among DARs.

A fully distributed approach, although perfectly feasible, requires in all cases some support from the mobile nodes, and even the deployment of a whole control infrastructure (as in the case of IEEE 802.21). This might be not desirable, but the deployment of such an architecture would yield to a more scalable and bottleneck-free operator infrastructure, where no single point of failure could bring the network down.
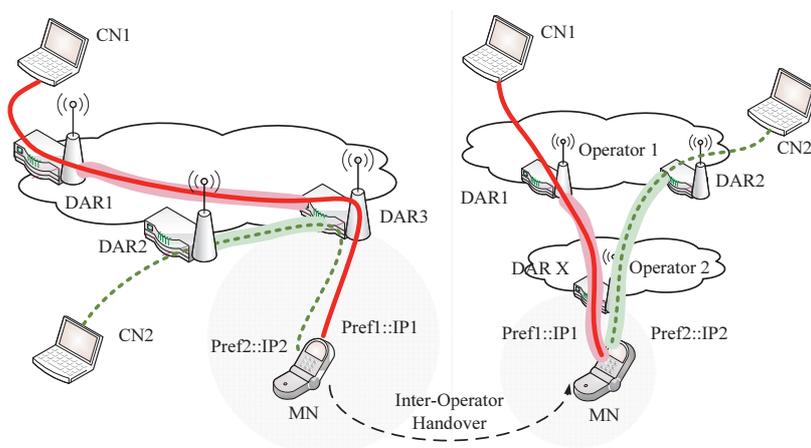
Fig. 10 An example use-case of HDMM: inter-operator mobility.

4.3 Hybrid DMM: combining network and client-based mobility

The network and client-based components of HDMM can be used as standalone solutions. However, we argue that future mobile network operators can benefit from a framework allowing a seamless integration of both solutions (some example scenarios were mentioned in Section 1). Actually, current mobile operator architectures, such as the 3GPP one, support both network and client-based *centralized* mobility solutions, offering in this way more flexibility to the operator. Therefore, HDMM basically takes this situation one step further, by also proposing a framework that includes network and client-based *distributed* mobility approaches.

We take inter-domain mobility as one representative scenario of combined HDMM deployment and use it in this section to explain how our proposed hybrid scheme works and the advantages it brings to mobile operators.

Fig. 10 shows an example of hybrid DMM operation. A mobile node first attaches to a mobile operator and benefits from network-based distributed mobility management (by using either the partially or the fully distributed variant described in Section 4.2).

While roaming within the same operator network, the security associations required among the involved distributed anchor routers can be easily set up (on demand or can be already pre-configured). If the mobile node moves to an access network managed by a different operator, the new operator might not even support DMM (i.e., there are no distributed anchor routers deployed) or, if DMM is supported, setting up security associations that cross operator boundaries might not be possible. In both cases, using a client-based DMM approach appears as the best possible solution to provide those sessions anchored at the previous domain with session continuity. HDMM supports this by activating the client-based component of the solution, and using the IP

address configured on the new domain as care-of address where active sessions anchored elsewhere can be redirected. This operation can be executed exploiting enhanced features of the terminal's connection manager.

The connection manager is a software construct widely available in most of today's portable devices. In the last years, and due to the availability of different networks where the mobile nodes can connect to, this piece of software has gained quite a lot of relevance. The connection manager, upon detection that the target point of attachment does not belong to the home operator or it does not support DMM, can activate the mobility client at the mobile node.

Let's consider the example shown in Fig. 10. A mobile node has been moving within its DMM-enabled home domain. In this example, we consider that the DMM solution used is network-based, as this represents the most complex situation, as we explain next. In this case, there are two possible solutions when the mobile node performs an inter-operator hand-off: *i)* the connection manager of the mobile node has tracked all the active P-DARs (i.e., all the DARs visited by the MN in the home dome domain anchoring an IP address used by an active session), or *ii)* the connection manager is only aware of the last S-DAR it was attached to before roaming to a new domain. In the former case, which requires a bit more of intelligence in the connection manager, the mobile node can just follow the client-based approach and update each of the P-DARs with its current location by sending a BU message. Note that this results in optimizing the path followed by data traffic between each of the P-DARs and the current location of the mobile node[5]. In the later case, the mobile node just updates its location on the last visited S-DAR (and sets up a tunnel), which then takes care of forwarding all the traffic received from the active P-DARs to the MN, using the tunnel established with the MN. This requires less complexity on the connection manager, but does not fully optimize the data path between the active P-DARs and the current location of the mobile node (i.e., packets have to traverse to chained tunnels: one from the MN to the last visited S-DAR, and one from this S-DAR to the corresponding P-DAR). Fig. 10 illustrates the case *i)*.

Note that if the new domain also supports HDMM, then subsequent handovers within that domain could be transparently managed by the network-based mobility solution in place, without requiring any action on the client-mobility stack running on the mobile node[6].

The previous example clearly shows how each distributed anchor router can be simultaneously playing – on a prefix basis – the roles of plain IPv6 access router (for prefixes locally anchored used by attached mobile nodes), as local mobility anchor (for prefixes locally anchored that are in use by mobile nodes

---

[5] This does not optimize the overall route between the mobile node and the peers it is communicating with. This fully optimized route can be achieved if the communication peer supports the correspondent node Mobile IPv6 route optimization (RO) functionality.

[6] In this case, the mobile node could actually decide if it prefers to update the care-of address used in the bi-directional tunnels established with P-DARs located at the other domain, or just let the network-based distributed mobility support deployed in the new domain provide address continuity to the care-of address used to set-up the tunnels.

which are no longer directly attached), as mobile access gateway (to enable address continuity for prefixes anchored at a different DAR) and as home agent (for locally anchored prefixes used by mobile nodes which are no longer directly attached and that are using the client-based HDMM component).

5 Analytic evaluation

This section provides the analytic evaluation of HDMM. The analysis is conducted considering the following three key performance metrics of an IP mobility protocol: *i)* packet and signaling overhead, *ii)* handover latency, and *iii)* end-to-end delay. Similar to the works [30] and [38], where different mobility protocols are compared, in the next paragraphs we carry out our analysis with respect to Mobile IPv6 and Proxy Mobile IPv6.

5.1 Overhead analysis

Both client and network-based HDMM enable the use of a locally locally anchored address provided by the serving DAR for new MN's communications, thus benefiting from no additional encapsulation. This is a clear performance advantage compared to centralized schema, where tunnel ling is always used (unless the mobile node is at home, and only for the case of Mobile IPv6).

Nowadays, users enjoy from a very large catalog of mobile applications. Some of them do not require IP address continuity, meaning that the applications themselves can cope with an IP address change (e.g., progressive HTTP download). This opens the door for not providing IP mobility support by default to every address/service (which is the current practice), but just to those that really require it, helping in this way to reduce the overall load in the network's core. This feature is known as *dynamic* mobility management, which is inherently supported by our HDMM approach.

In terms of packet overhead, the use of IPv6-in-IPv6 tunneling adds 40 extra bytes to every packet, and it also requires additional processing resources for the encapsulation/de-encapsulation operations and for the tunnel management itself. A difference between network and client-based solutions is that the extra tunnel overhead is not present in the last hop (which is wireless) for the case of the network-based solutions, and that the tunnel operations are performed by (usually powerful) network nodes, without the mobile node being involved. This is important from the point of view of energy and processing power efficiency, as the mobile node is usually more limited.

We next describe our analysis of the signaling overhead. A general expression of the average signaling cost for a mobility scheme is given by [49]:

$$C_{SIGNAL} = \frac{1}{SMR \cdot \sqrt{M}} \left[(\sqrt{M} - 1)C_{INTRA} + C_{INTER} \right], \qquad (1)$$

where SMR is the *session-to-mobility ratio*, M is the number of subnets for a single domain, C_{INTRA} and C_{INTER} are the binding update signaling

costs for the intra and inter-domain handover respectively. These costs are proportional to $d(X, Y)$, distance in number of hops from a node X to a node Y[7], multiplied by the link factors τ and ω, for a wired and a wireless link respectively. Therefore, the cost for transferring a packet from the MN to the S-DAR is $C_{MN,S\text{-}DAR} = \omega\, d(MN, S\text{-}DAR) = \omega$, whereas from a S-DAR to a P-DAR it is $C_{S\text{-}DAR,P\text{-}DAR} = \tau\, d(S\text{-}DAR, P\text{-}DAR)$. Note, that this last value depends on the size and configuration of the network.

The signaling cost of intra and inter-domain handovers, C_{INTRA} and C_{INTER} respectively, depends on the mobility solution that is used. The following cases are possible:

- INTRA domain handover. Both network and client-based solutions can be used to enable intra-domain mobility. Since we are also considering the centralized schema, we have:

$$C_{INTRA} = C_{PMIPv6} \mid C_{MIPv6} \mid C_{HDMM\text{-}net} \mid C_{HDMM\text{-}client}. \qquad (2)$$

- INTER domain handover. In this case, and for the reasons presented earlier in this article, we argue that client-based mobility is more appropriate. Therefore, we have:

$$C_{INTER} = C_{MIPv6} \mid C_{HDMM\text{-}client}. \qquad (3)$$

We next analyze each of these cost components, for both HDMM and the classic IP centralized mobility approaches.

5.1.1 PMIPv6

The hand-off signaling consists of a PBU/PBA handshake between the new MAG and the LMA, so the cost is given by:

$$C_{PMIPv6} = 2\,\tau\, d(LMA, MAG). \qquad (4)$$

5.1.2 MIPv6

In plain Mobile IPv6 there is a single BU/BA exchange per handover (we just assume no route optimization support is used for simplicity), so the signaling cost is given by:

$$C_{MIPv6} = 2\,[\omega + \tau\, d(AR, HA)]. \qquad (5)$$

---

[7] We assume that the links are symmetric, $d(X, Y) = d(Y, X)$.

5.1.3 HDMM network-based component

Partially distributed approach: Depending on the actual procedure used to update the central mobility database, the total signaling load varies:

- CMD behaves as PBU/PBA relay. Besides the handshake between the CMD and the S-DAR, there is an additional PBU/PBA exchange with n active P-DARs. This accounts for a total number of $2n + 2$ messages:

$$C_{HDMM\text{-}net}^{partially-relay} = 2\,\tau\,d(CMD, S\text{-}DAR) + 2n\,\tau d(CMD, P\text{-}DAR)$$
$$= (2n + 2)\,\tau\,d(CMD, DAR), \tag{6}$$

  where $d(CMD, DAR)$ is the average distance between the CMD and the DARs in the domain.
- CMD behaves as DAR locator. In this case, the amount of PBU and PBA messages is $3n + 1$: a first PBU message sent by the new S-DAR, plus n copies sent by the CMD to the active P-DARs, and $2n$ PBA messages sent back by the P-DARs to the CMD and the S-DAR:

$$C_{HDMM\text{-}net}^{partially-locator} = \tau\,d(CMD, S\text{-}DAR) + 2n\,\tau\,d(CMD, P\text{-}DAR) + $$
$$+ n\,\tau\,d(S\text{-}DAR, P\text{-}DAR). \tag{7}$$

- CMD behaves as a PBU/PBA proxy. Apart from the re-ordering, the number of messages sent is identical to the *relay* case, $2n + 2$, thus Eq. (6) holds in this case as well:

$$C_{HDMM\text{-}net}^{partially-proxy} = C_{INTRA}^{partially-relay}. \tag{8}$$

Fully distributed approach: Regardless the method adopted to learn that a handover occurred, the S-DAR has to perform a PBU/PBA handshake with n active P-DARs. Being n the number of IPv6 addresses that need to be kept reachable and $d_{S-DAR,P-DAR}$ the average number of hops, the result is a total of $2n$ control messages:

$$C_{HDMM\text{-}net}^{fully} = 2n\,\tau\,d(S\text{-}DAR, P\text{-}DAR). \tag{9}$$

5.1.4 HDMM client-based component

The client-based component of HDMM involves n BU/BA exchanges (plus the CoTI/CoT ones in case of additional security), where n is the number of IPv6 addresses that need to be kept reachable. This accounts for a total of $2n$ ($+2n$ in case of additional security) control messages. MIPv6 messages traverse a wireless link from the MN to S-DAR, and the wired path from the S-DAR to the home agent. In client HDMM, after the wireless segment, message packets are delivered by the S-DAR to the P-DAR(s). In total we have:

$$C_{HDMM\text{-}client} = 2n\left[\omega + \tau\, d(S\text{-}DAR, P\text{-}DAR)\right] \quad \text{w/o add. security,} \quad (10)$$
$$C_{HDMM\text{-}client} = 4n\left[\omega + \tau\, d(S\text{-}DAR, P\text{-}DAR)\right] \quad \text{w/ add. security.}$$

Note that this analysis assumes the solution variant in which the connection manager of the mobile node is capable of keeping track of every active P-DAR, so it can update all of them. With the other variant, in which only the previous S-DAR is updated, the cost is reduced.

5.1.5 Comparison

From the previous analysis, we can observe that the HDMM solutions are more costly in terms of signaling, as they introduce more messages than the centralized solutions because there are more anchors to update. However, if we focus on the network-based solutions, the cost of a fully distributed scheme may be close to the PMIPv6 one, for scenarios in which there are very few active P-DARs and they are much closer to the S-DAR than the LMA to the MAG.

If we focus on the client-based solutions. HDMM introduces more traffic at the control plane level, but it allows using optimal or close to optimal routes for data traffic. On the other hand, MIPv6 requires less signaling but all the user's data need to traverse the home agent. The route optimization procedure enables the MN to use an optimal path with the CNs, but all the CNs need to be notified with some signaling, leading to an equal or larger number of control messages than client HDMM.

5.2 Handover latency

We define the handover latency as the time during which a node does not have IP connectivity as a result of a change of point of attachment. During this time, the IPv6 address that was being used by the mobile node is not usable. Multiple operations are performed during this process, such as layer-2 attachment, movement detection, address configuration and duplicate address detection, and the mobility signaling. We next briefly summarize the different components of the handover delay:

- Layer-2 handover time (T_{L2}^{ho}). This is defined as the time required by the layer-2 technology to perform a handover (i.e., disconnecting from its current point of attachment and connecting to a new one).
- Movement detection time (T_{MD}). This delay corresponds to the time required by the terminal to detect that it has moved to a different layer-3 point of attachment. In IPv6 this can be done in different ways. The most simple (and the most widely supported) consists in the appropriate use of the router advertisement (RA) messages. An access router periodically

multicasts unsolicited RA messages. Movement detection can also be assisted by the use of layer-2 triggers, such the ones implemented by IEEE 802.21. In this case, the movement detection delay can be extremely low.

– IP address configuration and duplicate address detection (T_{DAD}). This time corresponds to the configuration of the IP address based on the prefix received in the RA (i.e., the MN uses stateless auto-configuration) and the address uniqueness test in the network. Note that DAD is only used for new prefixes in the network-based approach, since old prefixes are maintained from previous allocations and do not require of new DAD processes.

– Network authentication delay (T_{auth}). The handover delay also depends on the particular authentication method used in the network being accessed by the user terminal.

– Mobility signaling delay ($T_{binding}$). This is the time required to update the mobility anchor (i.e., the home agent, the localized mobility anchor or the distributed anchor router) with the new location of the mobile node (denoted by its care-of address or the associated proxy care-of address). It is highly dependent on the distance between the entities participating in the user mobility management. For client-based approaches this is the distance between the mobile node and the home agent/distributed anchor router, while for network-based approaches, this is the distance between the mobile access gateway and the local mobility anchor, or the distance between the serving DAR and the previous DAR, or the the distance between the central mobility database and the involved DARs, depending on the solution flavor.

The handover latency can be then expressed as follows:

$$T_{handover} = T_{L2}^{ho} + T_{MD} + T_{DAD} + T_{auth} + T_{binding}, \tag{11}$$

in which the most relevant component for the comparison of different solutions is $T_{binding}$. The other delay components can be considered common to any of the analyzed mobility solutions[8]. The term $T_{binding}$ can be expressed, for each of the different scenarios, as follows:

– Mobile IPv6:
$$T_{binding}^{MIPv6} = RTT_{MN \leftrightarrow HA}. \tag{12}$$

– Client-based HDMM:
$$T_{binding}^{HDMM-client} = RTT_{MN \leftrightarrow P\text{-}DAR}. \tag{13}$$

– Proxy Mobile IPv6:
$$T_{binding}^{PMIPv6} = RTT_{MAG \leftrightarrow LMA}. \tag{14}$$

---

[8] Actually T_{auth} has a different form in the client DMM solution when the additional security procedure is in place. We omit this procedure in the analysis.

– Partially distributed network-based HDMM, CMD behaves as PBU/PBA relay:

$$T_{binding}^{HDMM-net-part-relay} = RTT_{S\text{-}DAR \leftrightarrow CMD} + RTT_{P\text{-}DAR \leftrightarrow CMD}$$
$$\approx 2 \cdot RTT_{DAR \leftrightarrow CMD}. \tag{15}$$

– Partially distributed network-based HDMM, CMD behaves as DAR locator:

$$T_{binding}^{HDMM-net-part-locator} = \frac{RTT_{S\text{-}DAR \leftrightarrow CMD} + RTT_{P\text{-}DAR \leftrightarrow CMD} + RTT_{S\text{-}DAR \leftrightarrow P\text{-}DAR}}{2}$$
$$\approx RTT_{DAR \leftrightarrow CMD} + \frac{RTT_{S\text{-}DAR \leftrightarrow P\text{-}DAR}}{2}. \tag{16}$$

– Partially distributed network-based HDMM, CMD behaves as PBU/PBA proxy:

$$T_{binding}^{HDMM-net-part-proxy} = \max(RTT_{S\text{-}DAR \leftrightarrow CMD}; \frac{RTT_{S\text{-}DAR \leftrightarrow CMD} + RTT_{P\text{-}DAR \leftrightarrow CMD}}{2})$$
$$\approx RTT_{DAR \leftrightarrow CMD}. \tag{17}$$

– Fully distributed network-based HDMM:

$$T_{binding}^{HDMM-net-fully} = RTT_{S\text{-}DAR \leftrightarrow P\text{-}DAR}. \tag{18}$$

For the cases of partially distributed network-based HDMM, we assume that the distance between the central mobility database and all the distributed anchor routers is approximately the same ($RTT_{DAR \leftrightarrow CMD}$).

Comparing Eqs. (12) and (13), it is clear that the main difference between client-based HDMM and Mobile IPv6 in terms of handover delay corresponds to the distance between the mobile node and the home agent/distributed anchor router. This is the main advantage of a distributed mobility management approach as compared with classical centralized mobility solutions, because the delay between the mobile node and its anchor is likely lower in the distributed approach (as the anchor in this case resides at the edge of the network, instead of at the core of the operator). It is also worth noting how as the mobile node gets farther away from an active previous DAR, the handover delay increases, thus HDMM is better suited for flows with short duration or mobile nodes with low mobility. This characteristic is explored in more detail in the next section.

Similarly, from Eqs. (14) and (18), we can see that network-based HDMM produces a shorter latency as long as the distance between the serving and previous DARs is shorter than the one between the MAG and LMA for the case of Proxy Mobile IPv6. This parameter strictly depends on the size of the operator's network, but, we can safely assume that an LMA would always be always farther than active previous DARs for the case of short communications with users of limited mobility.

Moreover, it can be noted by inspecting Eqs. (15)-(17) that the network-based HDMM solution with the CMD behaving as message proxy outperforms

all the others partially distributed proposals. For all partially distributed solutions, the handover delay approximates to the one of Proxy Mobile IPv6: $RTT_{LMA\leftrightarrow MAG}$. This is so because as the central mobility database is pushed into the core of the operator, the distance from the CMD to all DARs is similar.

5.3 End-to-end delay

We next analyze the delay experienced by packets exchanged between the mobile node and its communication peer (i.e., a correspondent node).

In Mobile IPv6, user data traffic always traverses the home agent, although this path may not be the shortest one between the mobile node and the correspondent node. This operation mode is called Bidirectional Tunneling (BT) and the resulting way of forwarding packets is known as angular routing. In this case, the end-to-end delays might be large, since the packets must go through the MN's home network, which can be located at a long distance from the mobile node. Due to the large delays introduced by the angular routing, Mobile IPv6 [47] already includes a procedure called route optimization (RO) that basically builds a secure direct path between the mobile node and the correspondent node. Thanks to the use of route optimization, packets exchanged between the mobile and the correspondent node can flow directly through the shortest path between the two nodes, without passing through the home agent. This mechanism needs additional support from the correspondent node, required to enable the optimization of the path. In the case of our HDMM approach, packets flow between the mobile node and the correspondent node traversing the serving DAR as in the case of Mobile IPv6 in BT mode. The difference between both approaches is that in our case, DARs are expected to be located near the mobile node, hence the effect of angular routing is highly minimized, obtaining delays of the order of RO-enabled Mobile IPv6. As mentioned earlier in the paper, the use of DMM is better suited for flows with short duration or low mobility MNs. The reason for this is the fact that as the mobile node moves away from the serving DAR handling a flow, the inefficiency introduced by the angular routing increases.

In order to assess how far and how fast a mobile node can move, we performed the following analysis. Lets suppose a VoIP communication between two peers, being one of them a mobile node making using of one of the HDMM schema. Considering the maximum mouth-to-ear delay as specified in [31] of 150 ms, we can assume that Eq. (19) holds:

$$T_{CN\rightarrow HOME-AR} + T_{HOME-AR\rightarrow MN} \leq 150ms, \qquad (19)$$

in which $HOME-AR$ stands for the serving DAR or HA/LMA according to the solution in place.

Let's assume the correspondent node and the mobile node are in the same geographical region or even city. In order to model this delay, we took average values from the PingER project[9], between several client-server pairs located

---

[9] Ping end-to-end reporting: `http://www-iepm.slac.stanford.edu/pinger/`

in the same regional area. The average delay obtained corresponds to roughly 20 ms, so Eq. (19) indicates the delay between the HOME-AR and the MN is upper bounded by 130ms. If we consider the network-based HDMM solution, we can assume that the DMM domain has a good internal connectivity. In this way, we can also assume that the delay between two distributed anchor routers is similar to a local delay between two servers located in the same organization (from the PingER project this delay is on average equal to 5 ms). To simplify, we suppose that the access network is deployed in such a way that going farther away from the first DAR visited by the mobile node increases the delay in a linear way (note that this is a worst case scenario). The maximum number of hops allowed for the VoIP communication can then be derived from Eq. (19), resulting in a maximum distance of 26 hops. This number represents a limit on the diameter of the DMM domain, which depends on the access technology used.

In the case of client-based HDMM, we could follow a similar analysis but considering that the distance between the distributed anchor routers is longer than in the network-based case. If we assume a inter-DAR delay of roughly 10ms (intermediate value between a regional and local delay), our solution allows approximately 10-13 hops before degrading the VoIP call.

The same delay assumptions hold for the centralized approaches, but we have to also consider the the angular routing intrinsic to Mobile IPv6 and Proxy Mobile IPv6. For instance, we can assume that the distance between a mobile node and a correspondent node is twice the client-server distance mentioned before: one to get to the HA/LMA, and another to reach the recipient (we can safely assume that the anchor is equidistant from the communication endpoints, as they are all located in the same region). With these assumptions, after 4/5 hops HDMM performance degrades to be the same of a centralized scheme. However, the advantage of HDMM is that when the delay becomes not tolerable, the application might be restarted, or the communication refreshed, so that the most suitable IP address can be picked, thus leading to traverse a shorter (direct) path with better delay.

In order to evaluate the advantages and disadvantages of DMM, it would be desirable to understand what are the constraints in terms of mobility due to the number of hops previously calculated. In the case of a WAN technology such as WiMAX or 3G, one access router can serve a cell of few Km of radius, while in the case of a LAN technology such as IEEE 802.11, the cell radius is reduced to less than 100m. Now let's look at a typical use case, where a user starts a VoIP conversation and walks across a DMM domain using IEEE 802.11. The typical speed for pedestrians is 4-5 Km/h [34] and the average call duration is roughly 3 minutes [46]. This means that during the call, the user will walk around 250m, hence performing two handovers and adding a delay of roughly 10ms more than the direct path between the CN and MN. This simple example shows two of the benefits of DMM: simplicity and low added end-to-end communications delay.

6 Experimental evaluation

This section provides an experimental evaluation based on real tests conducted with an HDMM prototype. The goal is two-fold: on the one hand, to show that the designed solution is feasible in a real testbed; and, on the other hand, to assess some performance metrics.

Client-based HDMM is conceptually similar to Mobile IPv6, being the main difference the fact that the mobile node is able to simultaneously operate with multiple home addresses anchored at different home agents. Therefore, and from the point of view of performance evaluation, there is little value in developing a prototype of the client-based HDMM component, as the results would not differ from those already available for Mobile IPv6 (of course, using the same mobile node - anchor delay). Because of this, we prefer to focus or implementation and evaluation efforts on the network-based component of HDMM, which does present significant differences as compared to legacy Proxy Mobile IPv6. One of the main contributions of this study is to compare the partially and fully distributed approaches when delivering real traffic.

The prototype of network-based HDMM is written in C and runs in Linux-operated machines. It is based on the OAI PMIPv6 implementation[10], extended with the new characteristics explained in Section 4.2. The testbed is composed of five Linux Ubuntu 10.04 boxes (running a Linux-2.6.32 kernel): four desktop PCs playing the role of three DARs and one CMD, plus one laptop playing the role of mobile node. In terms of connectivity between the different entities, both the central mobility database and the distributed anchor routers are connected to the same Ethernet switch, while the mobile nodes obtains connectivity using IEEE 802.11g as wireless technology.

The partially distributed approach is implemented following the *CMD as Proxy* variant because it provides the quickest reaction to the handover event in terms of routing state re-configuration. Also, it yields to the least number of signaling messages exchanged.

Regarding the fully distributed approach, the complete IEEE 802.21 signaling is not implemented, as the messaged are exchanged before the actual Layer-2 handover, and therefore, they do not impact the performance metrics collected here. Based on that, we have only implemented a custom Layer-2 attachment and detachment detection mechanism. Nevertheless, it is worth highlighting that we are currently working together with the authors of [14] to integrate an open source IEEE 802.21 implementation (called ODTONE[11]) with our HDMM prototype within the framework of the MEDIEVAL[12] European project. Since the IEEE 802.21 framework is not yet fully integrated into our prototype, we statically configured the nodes with the P-DARs' addresses to be used for the signaling during the tests. Note that none of these

---

[10] OpenAir Interface PMIPv6: `http://www.openairinterface.org/components/page1103.en.htm`

[11] `http://helios.av.it.pt/projects/odtone`

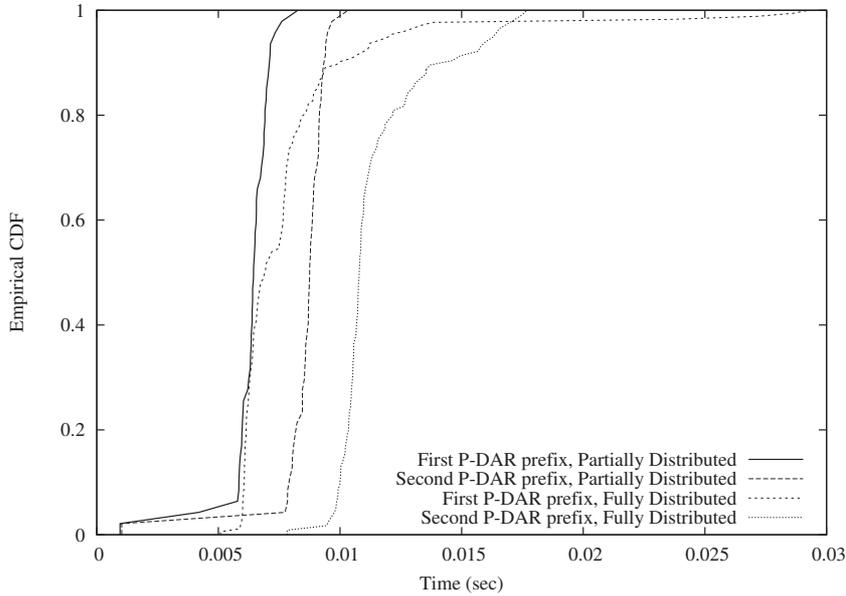[12] `http://www.ict-medieval.eu`

Fig. 11 Comparison of the CDF of the handover latency with different number of active prefixes.

implementation simplifications have an impact on the obtained performance results.

In order to compare and understand the performance of the partially and the fully distributed solutions, we measured the handover latency for both approaches (with one and two active prefixes). Fig. 11 shows the empirical cumulative distribution function (eCDF) of measured results. Each of the experiments consists in the MN connecting to DAR_1, next moving to DAR_2 and DAR_3, and finally disconnecting. By doing this, after the first handover, only one prefix (the one anchored at DAR_1) is updated, whereas after the second movement, two prefixes are updated (the ones anchored at DAR_1 and DAR_2). To better understand the contribution of the IP mobility operations to the overall handover latency, we added timers in the code to extract the timestamps when the PBU, PBA, RS and RA messages are sent and received. With this information we can derive $T_{binding}$ as characterized in Section 5.2. Note that not analyzing $T_{L2}{}^{ho}$, T_{auth}, T_{DAD} and T_{MD} in our experiments does not impact the comparison of the partially and fully distributed approaches, as all those values are identical in the analyzed situations.

A first observation that is worth analyzing from the obtained results is the difference in the delay incurred to maintain the first prefix (observed during both handovers) and the second one (observed in the last handover only). The reason is inherent to how the implementation handles multiple prefix updates, because each prefix is handled sequentially within a single execution

thread, rather than simultaneously with parallel threads. Therefore, the handover latency of a prefix increases with each additional active prefix, as shown in Fig. 11.

We can also observe that the handover latency is shorter for the case of the partially distributed approach than for the fully distributed one. The reason for this can be found by analyzing the number of messages used to convey the required information. For the partially distributed case, the CMD provides to the serving DAR the list of P-DARs' addresses and associated anchored prefixes in one single packet, while for the fully distributed case, the serving DAR obtains the information about each prefix through a different message. This results in a difference in the processing time required for both operations.

The results for the fully distributed approach also show a slightly higher dispersion. This is because there are more machines and more links involved in this case compared to the partially distributed one, which adds random variation effects. These facts lead to a more evident heterogeneity in the measurements observed for the fully distributed scheme. Note that in the partially distributed case, the main time consuming operations take place at the CMD.

We can safely conclude from Fig. 11, that in a real-life deployment there would not be significant differences in terms of handover delay between the partially and fully distributed solutions, as in this scenario the most relevant contribution to the overall latency would be due to the the distance between the involved network entities. Note that in our in-lab experiments, this distance is almost negligible, as involved machines are attached to the same network segment.

The network distance between the different involved entities is a critical factor, as mentioned above and highlighted in the analysis performed in Section 5. We next report on the experiments conducted in order to assess the impact of the delay between the serving and the previous DARs for the fully distributed solution, and the impact of the delay between the CMD and the DARs for the partially distributed one.

Using different delays between the relevant network entities, several handoff iterations were conducted, measuring the total handover latency for both the partially and the fully distributed approaches. The ratio of these two measured latencies versus the S-DAR to P-DAR delay is plot in Fig. 12, for different DAR-to-CMD delays (a line for the ratio equal to one is also plotted, for an easier performance comparison). Obtained results show that both approaches behave as expected: for S-DAR-to-P-DAR delays smaller than S-DAR-to-CMD ones, the handover of the fully distributed approach is faster than the one of the partially distributed. For the case of comparable delays between the involved network entities, obtained results show that both approaches offer a similar handover performance, as was also shown by the previous experiment. Hence, we argue that the decision on the solution approach (partially versus fully distributed) should be performed taking into consideration the network infrastructure characteristics where the solution is going to be deployed. As an example, if the architecture of the operator is already distributed in nature and the IEEE 802.21 framework is available, then the fully distributed
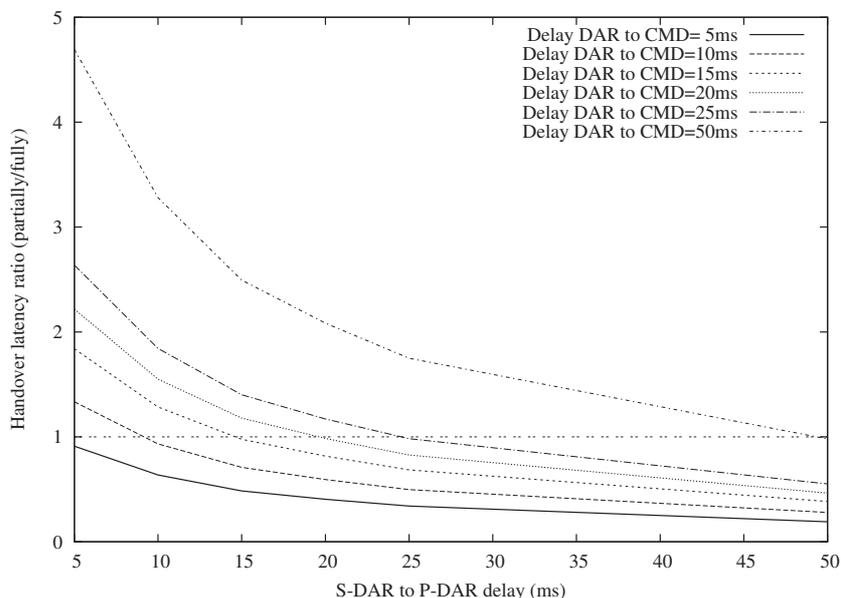
Fig. 12 Comparison of the handover latency ratio between the partially and fully distributed solutions versus the DAR-DAR and DAR-CMD delays.

approach seems the most appropriate solution. In contrast, if the operator is evolving a mature network, where the underlying network was dimensioned for use with a centralized solution, then the partially distributed solution is better suited.

7 Conclusions

The unexpected success of smart-phones, tablets and netbooks has fostered a very important increase of the mobile data traffic. Large-scale mobile operators are very much concerned about how their networks are going to tackle the exponentially growing users' traffic demand in the near future. Current mobility architectures are heavily centralized, making the network dimensioning extremely challenging, as the core has to be able to cope with all this traffic load. This has triggered a special interest on a new mobility paradigm, the so-called Distributed Mobility Management (DMM), where the network architecture is flattened and the mobility task is no longer performed by a centralized entity.

This article discusses a novel solution that proposes the combined deployment of a network-based DMM approach with a client-based one. The resulting Hybrid DMM (HDMM) solution aims at providing mobile network operators with a powerful, yet flexible, framework that could lead them towards effectively flattening their networks and distributing the mobility management.

HDMM is composed of two main components: a distributed version of Proxy Mobile IPv6, and a distributed version of Mobile IPv6. For the former case, different signaling schemes are proposed and analyzed. An analytic and experimental evaluation has been conducted, showing that HDMM solutions are comparable in terms of overhead and handover delay to existing centralized approaches (Mobile IPv6 or Proxy Mobile IPv6), while the use of HDMM solutions would heavily alleviate the mobile operator's core.

References

1. 3GPP: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access. TS 23.401, 3rd Generation Partnership Project (3GPP) (2011)
2. 3GPP: LIPA Mobility and SIPTO at the Local Network. TR 23.859, 3rd Generation Partnership Project (3GPP) (2011)
3. Ali-Ahmad, H., Ouzzif, M., Bertin, P., Lagrange, X.: Comparative performance analysis on dynamic mobility anchoring and proxy mobile IPv6. In: Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on, pp. 653 –657 (2012)
4. Aura, T.: Cryptographically Generated Addresses (CGA). RFC 3972 (2005)
5. Bernardos, C., Zuniga, J., Reznik, A.: Towards Flat and Distributed Mobility Management: a 3GPP Evolved Network Design. In: Communications (ICC), 2012 IEEE International Conference on, pp. 6855 –6861 (2012). DOI 10.1109/ICC.2012.6364784
6. Bertin, P., Bonjour, S., Bonnin, J.: Distributed or centralized mobility? In: Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE, pp. 1–6. IEEE (2009)
7. Bertin, P., Bonjour, S., Bonnin, J.M.: A Distributed Dynamic Mobility Management Scheme Designed for Flat IP Architectures. In: New Technologies, Mobility and Security, 2008. NTMS '08., pp. 1–5 (2008)
8. Bertin, P., Bonjour, S., Bonnin, J.M.: An Evaluation of Dynamic Mobility Anchoring. In: Vehicular Technology Conference Fall (VTC 2009-Fall), 2009 IEEE 70th, pp. 1–5 (2009)
9. Boc, M., Petrescu, A., Janneteau, C.: Anchor-based routing optimization extension for Proxy Mobile IPv6 in flat architectures. In: Wireless Personal Multimedia Communications (WPMC), 2011 14th International Symposium on, pp. 1 –5 (2011)
10. Chan, H.: Proxy Mobile IP with distributed mobility anchors. In: GLOBECOM Workshops (GC Wkshps), 2010 IEEE, pp. 16 –20 (2010). DOI 10.1109/GLOCOMW.2010.5700231
11. Chan, H.: Distributed Mobility Management with Mobile IP. In: Communications (ICC), 2012 IEEE International Conference on, pp. 6850 –6854 (2012). DOI 10.1109/ICC.2012.6364868
12. Chan, H.: Requirements for Distributed Mobility Management. Internet-Draft (work in progress), draft-ietf-dmm-requirements-03.txt (2012)
13. Chan, H.A., Yokota, H., Xie, J., Seite, P., Liu, D.: Distributed and Dynamic Mobility Management in Mobile Internet: Current Approaches and Issues. Journal of Communications **6**(1), 4–15 (2011)
14. Corujo, D., Guimaraes, C., Santos, B., Aguiar, R.: Using an open-source IEEE 802.21 implementation for network-based localized mobility management. Communications Magazine, IEEE **49**(9), 114 –123 (2011)
15. Devarapalli, V., Dupont, F.: Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture. RFC 4877 (2007)
16. Devarapalli, V., Wakikawa, R., Petrescu, A., Thubert, P.: Network Mobility (NEMO) Basic Support Protocol. RFC 3963 (2005)
17. Do, T.X., Kim, Y.: Distributed network mobility management. In: Advanced Technologies for Communications (ATC), 2012 International Conference on, pp. 319 –322 (2012). DOI 10.1109/ATC.2012.6404284

18. Ernest, P., Chan, H.: Enhanced handover support and routing path optimization with distributed mobility management in flattened wireless networks. In: Wireless Personal Multimedia Communications (WPMC), 2011 14th International Symposium on, pp. 1 –5 (2011)
19. Farha, R., Khavari, K., Abji, N., Leon-Garcia, A.: Peer-to-Peer mobility management for all-IP networks. In: Communications, 2006. ICC'06. IEEE International Conference on, vol. 5, pp. 1946–1952. IEEE (2006)
20. Farinacci, D., Fuller, V., Meyer, D., Lewis, D.: The Locator/ID Separation Protocol (LISP). RFC 6830 (2013)
21. Fischer, M., Andersen, F.U., Kopsel, A., Schafer, G., Schlager, M.: A Distributed IP Mobility Approach for 3G SAE. In: Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on, pp. 1 –6 (2008). DOI 10.1109/PIMRC.2008.4699735
22. García-Martínez, A., Bagnulo, M., Van Beijnum, I.: The Shim6 architecture for IPv6 multihoming. Communications Magazine, IEEE **48**(9), 152–157 (2010)
23. Giust, F., Bernardos, C., Figueiredo, S., Neves, P., Melia, T.: A hybrid MIPv6 and PMIPv6 distributed mobility management: The MEDIEVAL approach. In: Computers and Communications (ISCC), 2011 IEEE Symposium on, pp. 25–30 (2011)
24. Giust, F., de la Oliva, A., Bernardos, C.J.: Flat Access and Mobility Architecture: an IPv6 Distributed Client Mobility Management solution. In: 2011 IEEE INFOCOM MobiWorld Workshop, pp. 361–366 (2011)
25. Giust, F., de la Oliva, A., Bernardos, C., Da Costa, R.: A network-based localized mobility solution for Distributed Mobility Management. In: Wireless Personal Multimedia Communications (WPMC), 2011 14th International Symposium on, pp. 1 –5 (2011)
26. Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., Patil, B.: Proxy Mobile IPv6. RFC 5213 (2008)
27. Gurtov, A., Komu, M., Moskowitz, R.: Host identity protocol: identifier/locator split for host mobility and multihoming. Internet Protocol J **12**(1), 27–32 (2009)
28. Hahn, W.: 3GPP Evolved Packet Core support for distributed mobility anchors: Control enhancements for GW relocation. In: ITS Telecommunications (ITST), 2011 11th International Conference on, pp. 264–267. IEEE (2011)
29. Hahn, W.: Flat 3GPP Evolved Packet Core. In: Wireless Personal Multimedia Communications (WPMC), 2011 14th International Symposium on, pp. 1–5 (2011)
30. Hossain, M., Atiquzzaman, M.: Cost analysis of mobility protocols. Telecommunication Systems pp. 1–15 (2011)
31. ITU-T, R., Recommend, I.: G. 114. One-way transmission time **18** (2000)
32. Jung, H., Gohar, M., Kim, J., Koh, S.: Distributed mobility control in Proxy Mobile IPv6 networks. IEICE Transactions on Communications **94**(8), 2216 (2011)
33. Kafle, V., Kobari, Y., Inoue, M.: A Distributed Mobility Management scheme for future networks. In: Kaleidoscope 2011: The Fully Networked Human? - Innovations for Future Networks and Services (K-2011), Proceedings of ITU, pp. 1 –7 (2011)
34. Knoblauch, R., Pietrucha, M., Nitzburg, M.: Field studies of pedestrian walking speed and start-up time. Transportation Research Record: Journal of the Transportation Research Board **1538**, 27–38 (1996)
35. Koodli, R.: Mobile IPv6 Fast Handovers. RFC 5268 (2008)
36. Laganier, J.: Authorizing Mobile IPv6 Binding Update with Cryptographically Generated Addresses. Internet-Draft (work in progress), draft-laganier-mext-cga-01.txt (2010)
37. LAN/MAN Committee of the IEEE Computer Society: IEEE Std 802.21-2008, Standards for Local and Metropolitan Area - Part 21: Media Independent Handover Services (2008)
38. Lee, J.H., Han, Y.H., Gundavelli, S., Chung, T.M.: A comparative performance analysis on Hierarchical Mobile IPv6 and Proxy Mobile IPv6. Telecommunication Systems **41**(4), 279–292 (2009)
39. Lee, K.H., Lee, H.W., Ryu, W., Han, Y.H.: A scalable network-based mobility management framework in heterogeneous ip-based networks. Telecommunication Systems pp. 1–14 (2011)
40. Li, C.S., Lin, F., Chao, H.C.: Routing optimization over network mobility with distributed home agents as the cross layer consideration. Telecommunication Systems **42**(1-2), 63–76 (2009)

41. Liu, D., an P. Seite, J.C.Z., Chan, H., Bernardos, C.J.: Distributed Mobility Management: Current practices and gap analysis. Internet-Draft (work in progress), draft-ietf-dmm-best-practices-gap-analysis-00.txt (2013)
42. Liu, M., Guo, X., Zhou, A., Wang, S., Li, Z., Dutkiewicz, E.: Low latency IP mobility management: protocol and analysis. EURASIP Journal on Wireless Communications and Networking **2011**(1), 1–16 (2011)
43. Louin, P., Bertin, P.: Network and host based distributed mobility. In: Wireless Personal Multimedia Communications (WPMC), 2011 14th International Symposium on, pp. 1 –5 (2011)
44. McCann, P.: Design of a flat wireless Internet Service Provider network. In: Wireless Personal Multimedia Communications (WPMC), 2011 14th International Symposium on, pp. 1 –5 (2011)
45. Narten, T., Nordmark, E., Simpson, W., Soliman, H.: Neighbor Discovery for IP version 6 (IPv6). RFC 4861 (2007)
46. Noll, A.: Cybernetwork technology: Issues and uncertainties. Communications of the ACM **39**(12), 27–31 (1996)
47. Perkins, C., Johnson, D., Arkko, J.: Mobility Support in IPv6. RFC 6275 (2011)
48. Seite, P., Bertin, P.: Distributed Mobility Anchoring. Internet-Draft (work in progress), draft-seite-dmm-dma-06.txt (2013)
49. Skorepa, M., Klugl, R.: Enhanced analytical method for IP mobility handover schemes cost evaluation. Telecommunication Systems pp. 1–10 (2011)
50. Tsirtsis, G., Soliman, H., Montavont, N., Giaretta, G., Kuladinithi, K.: Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support. RFC 6089 (2011)
51. Wakikawa, R., Devarapalli, V., Tsirtsis, G., Ernst, T., ami, K.N.: Multiple Care-of Addresses Registration. RFC 5648 (Proposed Standard) (2009)
52. Wakikawa, R., Valadon, G., Murai, J.: Migrating home agents towards internet-scale mobility deployments. In: Proceedings of the 2006 ACM CoNEXT conference
53. Xue, K., Li, L., Hong, P., McCann, P.: Routing optimization in DMM. Internet-Draft (work in progress), draft-xue-dmm-routing-optimization-01.txt (2012)
54. Yi, L., Zhou, H., Huang, D., Zhang, H.: D-PMIPv6: A distributed mobility management scheme supported by data and control plane separation. Mathematical and Computer Modelling (0), – (2012)
55. Yokota, H., Seite, P., Demaria, E., Cao, Z.: Use case scenarios for Distributed Mobility Management. Internet-Draft (work in progress), draft-yokota-dmm-scenario-00.txt (2010)
56. Yu, L., Zhijun, Z., Tao, L., Hui, T.: Distributed Mobility Management Based on Flat Network Architecture. In: Wireless Internet Conference (WICON), 2010 The 5th Annual ICST, pp. 1–6 (2010)
57. Zhai, Y., Wang, Y., You, I., Yuan, J., Ren, Y., Shan, X.: A DHT and MDP-based Mobility Management Scheme for Large-Scale Mobile Internet. In: 2011 IEEE INFOCOM MobiWorld Workshop, pp. 379–384 (2011)
58. Zhang, H., Qiu, F., Zhou, H., Li, X., Song, F.: A Distributed Mobility Management Solution in LISP networks. Internet-Draft (work in progress), draft-zhang-dmm-lisp-00.txt (2012)
59. Zuniga, J., Bernardos, C., de la Oliva, A., Costa, R., Reznik, A.: Distributed Mobility Management: A Standards Landscape. Communications Magazine **51** (2013)