DMM WG
Internet-Draft
Intended status: Informational
Expires: June 22, 2013

JC. Zuniga
InterDigital
CJ. Bernardos
UC3M
T. Melia
Alcatel-Lucent
C. Perkins
Futurewei

December 19, 2012

Mobility Practices and DMM Gap Analysis
draft-zuniga-dmm-gap-analysis-03

Abstract

This document describes practices for the deployment of existing mobility protocols in a distributed mobility management (DMM) environment, and identifies the limitations in the current practices with respect to providing the expected DMM functionality.

The practices description and gap analysis are performed for IP-based mobility protocols, dividing them into three main families: IP client-based, IP network-based, and 3GPP mobility solutions.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

The Distributed Mobility Management (DMM) approach aims at setting up IP networks so that traffic is distributed in an optimal way and does not rely on centrally deployed anchors to manage IP mobility sessions.

A first step towards the definition of DMM solutions is the definition of the problem of distributed mobility management and the identification of the main requirements for a distributed mobility management solution [I-D.ietf-dmm-requirements].

We first analyze existing practices of deployment of IP mobility solutions from a DMM perspective [I-D.perkins-dmm-matrix], [I-D.patil-dmm-issues-and-approaches2dmm]. After that, a gap analysis is carried out, identifying what can be achieved with existing solutions and what is missing in order to meet the DMM requirements identified in [I-D.ietf-dmm-requirements].

2. Practices: deployment of existing solutions in a DMM fashion

This section documents practices for the deployment of existing mobility protocols in a distributed mobility management (DMM) fashion. The scope is limited to existing IPv6-based and 3GPP mobility protocols, such as Mobile IPv6 [RFC6275], NEMO Basic Support Protocol [RFC3963], Proxy Mobile IPv6 [RFC5213], 3GPP GPRS Tunnelling Protocol, and protocol extensions, such as Hierarchical Mobile IPv6 [RFC5380], Mobile IPv6 Fast Handovers [RFC5568], Localized Routing for Proxy Mobile IPv6 [RFC6705], or 3GPP Selective IP Traffic Offload (SIPTO), among others [RFC6301].

The section is divided in three parts: IP client-based mobility, IP network-based mobility and 3GPP mobility solutions.

2.1. Client-based IP mobility

Mobile IPv6 (MIPv6) [RFC6275] and its extension to support mobile networks, the NEMO Basic Support protocol (hereafter, simply NEMO) [RFC3963] are well-known client-based IP mobility protocols. They heavily rely on the function of the Home Agent (HA), a centralized anchor, to provide mobile nodes (hosts and routers) with mobility support. We next describe how Mobile IPv6/NEMO and several additional protocol extensions can be deployed to meet some of the DMM requirements [I-D.ietf-dmm-requirements].

2.1.1. Mobile IPv6 / NEMO

```
    <- INTERNET -> <- HOME NETWORK -> <---- ACCESS NETWORK ---->
       -------                          -------
       | CN1 |         -------          | AR1 |-(o) zzzz (o)
       -------         | HA1 |          -------           |
                       -------   (MN1 anchored at HA1) -------
                                        -------        | MN1 |
                                        | AR2 |-(o)    -------
                                        -------
                       -------
                       | HA2 |          -------
                       -------          | AR3 |-(o) zzzz (o)
                                        -------           |
       -------                   (MN2 anchored at HA2) -------
       | CN2 |                          -------        | MN2 |
       -------                          | AR4 |-(o)    -------
                                        -------

      CN1    CN2     HA1    HA2         AR1    MN1     AR3    MN2
       |      |       |      |           |      |       |      |
       |<------------>|<=================+=====>|       |      | BT mode
       |      |       |      |           |      |       |      |
       |      |<----------------------------------------+----->| RO mode
       |      |       |      |           |      |       |      |
```

Figure 1: Distributed operation of Mobile IPv6 (BT and RO) / NEMO

Due to the heavy dependence on the home agent role, the base Mobile IPv6 and NEMO protocols (i.e., without additional extensions) cannot be easily deployed in a distributed fashion. One approach to distribute the anchors can be to deploy several HAs (as shown in Figure 1), and assign to each MN the one closest to its topological location [RFC4640], [RFC5026], [RFC6611]. In the example shown in Figure 1, MN1 is assigned HA1 (and a home address anchored by HA1), while MN2 is assigned HA2. Note that current Mobile IPv6 / NEMO specifications do not allow the simultaneous use of multiple home agents by a single mobile node instance, and therefore the benefits of this deployment model shown here are limited (unless multiple MIPv6 MN instances are run in parallel, each of them associated to a different HA). For example, if MN1 moves and attaches to AR3, the path followed by data packets would be suboptimal, as they have to traverse HA1, which is no longer close to the topological attachment point of MN1.

2.1.2. Mobile IPv6 Route Optimization

One of the main goals of DMM is to avoid the suboptimal routing caused by centralized anchoring. By default, Mobile IPv6 and NEMO use the so-called Bidirectional Tunnel (BT) mode, in which data traffic is always encapsulated between the MN and its HA before being directed to any other destination. Mobile IPv6 also specifies the Route Optimization (RO) mode, which allows the MN to update its current location on the CNs, and then use the direct path between them. Using the example shown in Figure 1, MN1 is using BT mode with CN2 and MN2 is in RO mode with CN1. However, the RO mode has several drawbacks:

- The RO mode is only supported by Mobile IPv6. There is no route optimization support standardized for the NEMO protocol, although many different solutions have been proposed.

- The RO mode requires additional signaling, which adds some protocol overhead.

- The signaling required to enable RO involves the home agent, and it is repeated periodically because of security reasons [RFC4225]. This basically means that the HA remains as single point of failure, because the Mobile IPv6 RO mode does not mean HA-less operation.

- The RO mode requires additional support on the correspondent node (CN).

Notwithstanding these considerations, the RO mode does offer the possibility of substantially reducing traffic through the Home Agent, in cases when it can be supported on the relevant correspondent nodes.

2.1.3. Hierarchical Mobile IPv6

```
     <- INTERNET -> <- HOME NETWORK -> <------- ACCESS NETWORK ------->
                                                    -----
                                                   /|AR1|-(o) zz (o)
                                         -------- / -----         |
                                         | MAP1 |<             -------
                                         -------- \ -----      | MN1 |
        -------                                    \|AR2|      -------
        | CN1 |                                     -----  HoA anchored
        -------                                     -----     at HA1
                        -------                    /|AR3|  RCoA anchored
                        | HA1 |          -------- / -----     at MAP1
                        -------          | MAP2 |<         LCoA anchored
                                         -------- \ -----     at AR1
                                                   \|AR4|
        -------                                     -----
        | CN2 |                                     -----
        -------                                    /|AR5|
                                         -------- / -----
                                         | MAP3 |<
                                         -------- \ -----
                                                   \|AR6|
                                                    -----

     CN1      CN2         HA1              MAP1      AR1         MN1
      |        |           |                | ________|__________ |
      |<------------------>|<==============>|<________+__________>| HoA
      |        |           |                |         |           |
      |        |<-------------------------->|<===================>| RCoA
      |        |           |                |         |           |
```

Figure 2: Hierarchical Mobile IPv6

Hierarchical Mobile IPv6 (HMIPv6) [RFC5380] allows reducing the amount of mobility signaling as well as improving the overall handover performance of Mobile IPv6 by introducing a new hierarchy level to handle local mobility. The Mobility Anchor Point (MAP) entity is introduced as a local mobility handling node deployed closer to the mobile node.

When HMIPv6 is used, the MN has two different temporal addresses: the Regional Care-of Address (RCoA) and the Local Care-of Address (LCoA). The RCoA is anchored at one MAP, that plays the role of local home agent, while the LCoA is anchored at the access router level. The mobile node uses the RCoA as the CoA signaled to its home agent. Therefore, while roaming within a local domain handled by the same MAP, the mobile node does not need to update its home agent (i.e., the mobile node does not change RCoA).

The use of HMIPv6 allows some route optimization, as a mobile node may decide to directly use the RCoA as source address for a communication with a given correspondent node, notably if the MN does not expect to move outside the local domain during the lifetime of the communication. This can be seen as a potential DMM mode of operation. In the example shown in Figure 2, MN1 is using its global HoA to communicate with CN1, while it is using its RCoA to communicate with CN2.

Additionally, a local domain might have several MAPs deployed, enabling hence different kind of HMIPv6 deployments (e.g., flat and distributed). The HMIPv6 specification supports a flexible selection of the MAP (e.g., based on the distance between the MN and the MAP, taking into consideration the expected mobility pattern of the MN, etc.).

2.1.4. Home Agent switch

The Home Agent switch specification [RFC5142] defines a new mobility header for signaling a mobile node that it should acquire a new home agent. Although the purposes of this specification do not include the case of changing the mobile node’s home address, as that might imply loss of connectivity for ongoing persistent connections, it could be used to force the change of home agent in those situations where there are no active persistent data sessions that cannot cope with a change of home address.

2.1.5. IP Flow Mobility

There are different specifications meant to support IP Flow Mobility (IFOM) with Mobile IPv6, namely the multiple care-of address registration [RFC5648], the flow bindings in Mobile IPv6 and NEMO [RFC6089] and the traffic selectors for flow bindings [RFC6088]. The use of these extensions allows a mobile node to associate different flows with different care-of addresses that the mobile owns at a given time. This could also be used, combined with the route optimization support, to improve the paths followed by data packets, avoiding the traversal of the core network for selected flows.

2.1.6. Source Address Selection

The IPv6 socket API for source address selection [RFC5014], [RFC6724] can be used by an application running on a mobile node to express its preference of using a home address or a care-of address in a given connection. This allows, for example, an application which can survive an IP address change to always prefer the use of a care-of address. Similarly, and as mentioned in [RFC6275], a mobile node can also prefer the use of a care-of address for sessions that are going to finish before the mobile node hands off to a different attachment point (e.g., short-lived connections like DNS dialogs). This could be based on user or operator policies, and it is typically performed by a connection manager (e.g., [I-D.seite-mif-cm]).

2.2. Network-based IP mobility

Proxy Mobile IPv6 (PMIPv6) [RFC5213] is the main network-based IP mobility protocol specified for IPv6. Architecturally, PMIPv6 is similar to MIPv6, as it relies on the function of the Local Mobility Anchor (LMA) to provide mobile nodes with mobility support, without requiring the involvement of the mobile nodes. The required functionality at the mobile node is provided in a proxy manner by the Mobile Access Gateway (MAG). We next describe how network-based mobility protocols and several additional extensions can be deployed to meet some of the DMM requirements [I-D.ietf-dmm-requirements].

2.2.1. Proxy Mobile IPv6

```
   <- INTERNET -><- HOME NET -><----------- ACCESS NETWORK ------------>
       -------
       | CN1 |                      --------      --------      --------
       -------      --------        | MAG1 |      | MAG2 |      | MAG3 |
                    | LMA1 |        ---+----      ---+----      ---+----
       -------      --------           |             |             |
       | CN2 |                        (o)           (o)           (o)
       -------      --------          x                           x
                    | LMA2 |         x                           x
       -------      --------       (o)                          (o)
       | CN3 |                      |                            |
       -------                   ---+---                      ---+---
                      Anchored   | MN1 |          Anchored    | MN2 |
                      at LMA1 -> -------          at LMA2 ->  -------

     CN1    CN2     LMA1   LMA2        MAG1   MN1     MAG3    MN2
      |      |       |      |           |      |       |       |
      |<------------>|<================>|<---->|       |       |
      |      |       |      |           |      |       |       |
      |      |<------------>|<========================>|<----->|
      |      |       |      |           |      |       |       |
```

Figure 3: Distributed operation of Proxy Mobile IPv6

As with Mobile IPv6, plain Proxy Mobile IPv6 operation cannot be easily decentralized, as in this case there also exists a single network anchor point. One simple but still suboptimal approach, would be to deploy several local mobility anchors and use a topological position-based assignment to attach mobile nodes (an example of this type of assignment is shown in Figure 3. This assignment can be static or dynamic (as described in Section 2.2.3). The main advantage of this simple approach is that the IP address anchor (i.e., the LMA) is placed close to the mobile node, and therefore resulting paths are close-to-optimal. On the other hand, as soon as the mobile node moves, the resulting path starts to deviate from the optimal one.

2.2.2. Local Routing

[RFC6705] enables optimal routing in Proxy Mobile IPv6 in three cases: i) when two communicating MNs are attached to the same MAG and LMA, ii) when two communicating MNs are attached to different MAGs but to the same LMA, and iii) when two communicating MNs are attached to the same MAG but have different LMAs. In these three cases, data traffic between the two mobile nodes does not traverse the LMA(s), thus providing some form of path optimization since the traffic is locally routed at the edge.

The main disadvantage of this approach is that it only tackles the MN-to-MN communication scenario, and only under certain circumstances.

In the context of 3GPP, the closest analogy is the use of the X2 interface between two eNBs to directly exchange data traffic during handover procedures. 3GPP does not foresee the use of local routing at any other point of the network given the structure of the EPS bearer model.

2.2.3. LMA runtime assignment

[RFC6463] specifies a runtime local mobility anchor assignment functionality and corresponding mobility options for Proxy Mobile IPv6. This runtime local mobility anchor assignment takes place during the Proxy Binding Update / Proxy Binding Acknowledgment message exchange between a mobile access gateway and a local mobility anchor. While this mechanism is mainly aimed for load-balancing purposes, it can also be used to select an optimal LMA from the routing point of view. A runtime LMA assignment can be used to change the assigned LMA of an MN, for example in case when the mobile node does not have any session active, or when running sessions can survive an IP address change.

2.2.4. Source Address Selection

Also in the context of network-based mobility, the use of a source address selection API can be considered as means to achieve better routing (by using different anchors). For instance, an MN connected to a PMIPv6 domain could attach two different wireless network interfaces to two different MAGs, hence configuring a different set of HNPs on both interfaces (potentially combining both IPv4 and IPv6). Based on application requirements or operator’s policies the connection manager logic could instruct the IP stack on the MN to route selected traffic on a specific wireless interface [I-D.seite-mif-cm]. It should be noted that source address selection mostly provides for better routing but not session continuity.

2.2.5. Multihoming in PMIPv6

PMIPv6 provides some multihoming support. RFC 5213 specifies that the LMA can maintain one mobility session per attached interface and that upon handover the full set of HNPs can be moved to another interface in case of inter-technology handover (MAGs providing different wireless access technology) or maintained on the same interface in case of intra-technology handover (MAGs providing the same wireless access technology). An MN can also attach two different interfaces to the same PMIPv6 domain (as described in Section 2.2.4), hence resulting in a multihomed device being able to send/receive traffic sequentially or simultaneously from both network interfaces. [I-D.ietf-netext-pmipv6-flowmob] extends the base RFC5213 capabilities so that a mobility session can be shared across two different access networks. It derives that a selected flow could be routed through different paths, hence achieving some sort of better routing. Yet all the traffic is anchored at centralized anchor points.

2.3. 3GPP mobility

Architecturally, the 3GPP Evolved Packet Core (EPC) network is also similar to PMIPv6 and MIPv6, as it relies on the Packet Data Gateway (PGW) anchoring services to provide mobile nodes with mobility support (see Figure 4). There are client-based and network-based mobility solutions in 3GPP, which for simplicity we will analyze together. We next describe how 3GPP mobility protocols and several additional completed or on-going extensions can be deployed to meet some of the DMM requirements. [I-D.ietf-dmm-requirements].

```
            +---------------------------------------------------------+
            |                           PCRF                          |
            +-----------+--------------------------+----------------+-+
                        |                          |                |
   +----+   +-----------+------------+    +--------+-----------+  +-+-+
   |    |   |          +-+           |    |  Core Network      |  |   |
   |    |   | +------+ |S|__         |    | +--------+  +---+  |  |   |
   |    |   | |GERAN/|_|G|  \        |    | |  HSS   |  |   |  |  |   |
   |    +-----+ UTRAN| |S|   \       |    | +---+----+  |   |  |  | E |
   |    |   | +------+ |N|  +-+-+    |    |     |       |   |  |  | x |
   |    |   |          +-+ /|MME|    |    | +---+----+  |   |  |  | t |
   |    |   | +---------+ / +---+    |    | |  3GPP  |  |   |  |  | e |
   |    +-----+ E-UTRAN |/           |    | |  AAA   |  |   |  |  | r |
   |    |   | +---------+\           |    | | SERVER |  |   |  |  | n |
   |    |   |             \ +---+    |    | +--------+  |   |  |  | a |
   |    |   |   3GPP AN    \|SGW+----- S5---------------+ P |  |  | l |
   |    |   |               +---+    |    |             | G |  |  |   |
   |    |   +------------------------+    |             | W |  |  | I |
   | UE |                                 |             |   |  |  | P |
   |    |   +------------------------+    |             |   +-----+   |
   |    |   |+-------------+ +------+|    |             |   |  |  | n |
   |    |   || Untrusted   +-+ ePDG +-S2b---------------+   |  |  | e |
   |    +---+| non-3GPP AN | +------+|    |             |   |  |  | t |
   |    |   |+-------------+         |    |             |   |  |  | w |
   |    |   +------------------------+    |             |   |  |  | o |
   |    |                                 |             |   |  |  | r |
   |    |   +------------------------+    |             |   |  |  | k |
   |    +---+  Trusted non-3GPP AN   +-S2a--------------+   |  |  | s |
   |    |   +------------------------+    |             |   |  |  |   |
   |    |                                 |             +-+-+  |  |   |
   |    +--------------------------S2c--------------------|    |  |   |
   |    |                                 |                    |  |   |
   +----+                                 +--------------------+  +---+
```

Figure 4: EPS (non-roaming) architecture overview

2.3.1. GPRS Tunnelling Protocol (GTP) and DSMIPv6

GPRS Tunnelling Protocol (GTP) [3GPP.29.060] is a network-based mobility protocol specified for 3GPP networks (S2a, S2b, S5 and S8 interfaces). Similar to PMIPv6, it can handle mobility without requiring the involvement of the mobile nodes. In this case, the mobile node functionality is provided in a proxy manner by the Serving Data Gateway (SGW), Evolved Packet Data Gateway (ePDG), or Trusted Wireless Access Gateway (TWAG).

3GPP specifications also include client-based mobility support, based on adopting the use of Dual-Stack Mobile IPv6 (DSMIPv6) [RFC5555] for the S2c interface. In this case, the UE implements the mobile node functionality, while the home agent role is played by the PGW.

2.3.2. Local IP Access and Selected IP Traffic Offload (LIPA-SIPTO)

A Local IP Access (LIPA) and Selected IP Traffic Offload (SIPTO) enabled network [3GPP.23.829] allows offloading some IP services at the local access network, above the Radio Access Network (RAN) or at the macro, without the need to traverse back to the PGW.

Similarly to the runtime local mobility anchor assignment described in Section 2.2.3, considerations have been discussed in 3GPP with respect to SIPTO. SIPTO enables an operator to offload certain types of traffic at a network node close to the UE’s point of attachment to the access network, by selecting a set of GWs (SGW and PGW) that is geographically/topologically close to the UE’s point of attachment.

LIPA, on the other hand, enables an IP capable UE connected via a Home eNB (HeNB) to access other IP capable entities in the same residential/enterprise IP network without the user plane traversing the mobile operator’s network core. In order to achieve this, a Local GW (L-GW) collocated with the HeNB is used. LIPA is established by the UE requesting a new PDN connection to an access point name for which LIPA is permitted, and the network selecting the Local GW associated with the HeNB and enabling a direct user plane path between the Local GW and the HeNB.

2.3.3. LIPA Mobility and SIPTO at the Local Network (LIMONET)

Both SIPTO and LIPA have a very limited mobility support, specially in 3GPP specifications up to Rel-10. In Rel-11, there is currently a work item on LIPA Mobility and SIPTO at the Local Network (LIMONET) [3GPP.23.859] that is studying how to provide SIPTO and LIPA mechanisms with some additional, but still limited, mobility support. In a glimpse, LIPA mobility support is limited to handovers between HeNBs that are managed by the same L-GW (i.e., mobility within the local domain), while seamless SIPTO mobility is still limited to the case where the SGW/PGW is at or above Radio Access Network (RAN) level.

2.3.4. Data IDentification in ANDSF (DIDA) and Operator Policies for IP Interface Selection (OPIIS)

There are two ongoing work items in 3GPP that are currently addressing the issue of selecting a wireless interface or an IP address for a specific data application. The work item DIDA (Data IDentification in ANDSF) is addressing the need to map an application ID to a specific wireless interface, while the work item Operator

Policies for IP Interface Selection (OPIIS) is addressing the need of selecting the right APN for a given application.

Taking into account that there is a one to one link between APN and PDN connection (i.e., IP address) these work items clearly address from a 3GPP perspective the same problem space as [RFC6724], and the same considerations described in Section 2.2.4 apply here as well.

2.3.5. Multi-Access PDN Connectivity (MAPCON)

The Multi-Access PDN Connectivity (MAPCON) feature addresses the use of multiple PDN connections. Hence, this feature can make use of multiple wireless interfaces either sequentially or simultaneously.

3. Gap Analysis: limitations in current practices

This section identifies the limitations in the current practices (documented in Section 2) with respect to the requirements listed in [I-D.ietf-dmm-requirements].

The analysis is divided in three parts: IP client-based mobility, IP network-based mobility, and 3GPP mobility solutions. Each part analyzes how well the requirements listed in [I-D.ietf-dmm-requirements] are covered/met by the current practices, highlighting existing limitations and gaps.

3.1. Client-based IP mobility

3.1.1. REQ1: Distributed deployment

MIPv6 / NEMO A careful home agent deployment and policy configuration of the Mobile IPv6 / NEMO protocols can achieve some distribution. However, as soon as the mobile node moves and changes its initial attachment point, the anchors are no longer placed optimally, incurring in sub-optimal routes. This situation may be acceptable as long as the session is short-lived. If the mobile node is not expected to move within a limited area, this configuration might be considered sufficient. Otherwise, additional mechanisms to support dynamic anchoring would be needed. Note that a possible solution would be to run multiple instances of mobile IPv6 at the mobile node, each one managing a different HoA and bound to a different home agent. This would require, though, additional intelligence at the mobile node to be able to optimally select and manage source IP addresses for each session.

Mobile IPv6 RO The use of route optimization support enables a close-to anchor-less operation, which effectively can be considered as a fully distributed configuration. However, as explained before in this document, the home agent is still used for the signaling and therefore remains as a critical centralized component. Additionally, there is no standardized RO support for network mobility.

HMIPv6 The use of hierarchical mobile IPv6 can be seen as a step forward compared to a careful deployment of multiple home agents and its proper configuration, as it allows a mobile node to roam within a local domain, reducing the handover latency as well as the signaling overhead. If used together with mobile IPv6, traffic still has to traverse the centralized home agent, and therefore no distributed operation is achieved.

HA switch The home agent switch specification can be used to enable obtaining more benefits from a multiple-HA deployment, as the mobile node could be instructed to switch to a closer home agent. To avoid packet loss, this switch must be performed at periods of time in which the mobile node does not have any active connection running. Even if some packet loss were acceptable for active sessions, the change of home address would also require the mobile node to re-establish those sessions.

Flow mobility Considerations made for previous scenarios (e.g. for Route Optimization) could also apply here, extending those scenarios by the use of multiple attached interfaces.

SA selection API The use of proper source address selection decisions, enabled by smart connection managers [I-D.seite-mif-cm], or mobility aware applications using a selection API [RFC5014], [RFC6724], would allow the mobile node to realize substantial benefits from deployments providing multiple anchors.

3.1.2. REQ2: Transparency to Upper Layers when needed

MIPv6 / NEMO As a mobility protocol, the solution is transparent to the upper layers. However, as described before, this transparency comes with the cost of suboptimal routes if the MN moves away from its initial attachment point.

Mobile IPv6 RO The use of the route optimization support is transparent to the upper layers.

HMIPv6 The use of HMIPv6 is transparent to the upper layers.

HA switch The use of the home agent switch functionality is not transparent to the upper layers, as a change of home agent normally implies a change of home address. Therefore, the home agent can only be switched when there is no active session running on the mobile node. Since IP address continuity cannot be achieved at the relocated home agents, one gap that would need to be filled is the ability for the mobile node to convey HoA context from the previous home agent.

Flow mobility The use of flow mobility mechanisms is transparent to the upper layers.

SA selection API The use of an intelligent source address mechanisms is transparent to the upper layers if performed by the connection manager. However if the selection is performed by the applications themselves, via the use of the API, then applications have to be mobility-aware.

3.1.3. REQ3: IPv6 deployment

MIPv6 / NEMO Mobile IPv6 / NEMO protocols primarily support IPv6, although there are some extensions defined to also offer some IPv4 support [RFC5555].

Mobile IPv6 RO Route optimization only supports IPv6.

HMIPv6 HMIPv6 is only defined for IPv6.

HA switch The home agent switch specification supports only IPv6, although the use of the defined mechanisms to support dual stack IPv4/IPv6 mobile nodes would also enable some IPv4 support.

Flow mobility Flow mobility is only defined for IPv6.

SA selection API The use of source address selection mechanisms supports both IPv6 and IPv4.

3.1.4. REQ4: Existing mobility protocols

MIPv6 / NEMO These approaches are ones of the base IETF-standardized mobility protocols: [RFC6275] and [RFC3963].

Mobile IPv6 RO This approach is based on an existing protocol [RFC6275].

HMIPv6 This approach is based on an existing protocol [RFC5380].

HA switch This approach is based on an existing protocol [RFC5142].

Flow mobility This approach is based on existing protocols [RFC5648], [RFC6089] and [RFC6088].

SA selection API This approach is based on existing protocols [RFC6724] and [RFC5014].

3.1.5. REQ5: Compatibility

MIPv6 / NEMO This approach would be compatible with other protocols and work between trusted administrative domains, although as described before its operation would not provide the benefits of a fully distributed mechanism. The combination of different IP mobility protocols might have a performance/complexity cost associated, as described in [A. de la Oliva, et al.].

Mobile IPv6 RO This approach would be compatible with other protocols and work between trusted administrative domains, as long as mobile IPv6 is allowed. However, as highlighted before, mobile IPv6 route optimization requires specific support at the correspondent nodes.

HMIPv6 HMIPv6 is compatible with other protocols.

HA switch This approach would be compatible with other protocols and work between trusted administrative domains.

Flow mobility This approach would be compatible with other protocols and work between trusted administrative domains.

SA selection API This approach has no impact in terms of compatibility or use between trusted administrative domains.

3.1.6. REQ6: Security considerations

MIPv6 / NEMO This approach includes security considerations.

Mobile IPv6 RO This approach includes security considerations.

HMIPv6 This approach includes security considerations.

HA switch This approach includes security considerations.

Flow mobility This approach includes security considerations.

SA selection API This approach does not have security issues.

3.2. Network-based IP mobility

3.2.1. REQ1: Distributed deployment

PMIPv6 As for the case of MIPv6, a careful deployment of the local mobility anchors and policy configuration of the Proxy Mobile IPv6 protocol can achieve some distribution. However, as soon as the mobile node moves and changes its initial attachment point, the anchor is no longer placed optimally, incurring in sub-optimal routes, which might be quite noticeable in case of medium to large PMIPv6 domains. If the mobile node movement is restricted to a well known limited area and/or the PMIPv6 domain is not large, this configuration might be considered sufficient. Otherwise, additional mechanisms to support dynamic anchoring would be needed.

Local Routing As mentioned before, it enables optimal routing in three cases: the LMA manages the traffic of two mobile nodes connected to the same MAG, the LMA manages the traffic of two mobile nodes connected to different MAGs, the MAG manages the traffic of two mobile nodes connected to different LMAs. LR does not consider the case where the traffic should be optimized considering different MAGs and different LMAs. Inter LMA communication is not in scope. LR only enables better routing and does not consider the distribution of mobility anchors as such.

LMA Runtime Assignment The LMA runtime assignment is used to allocate an optimal LMA mostly for load balancing purposes, for instance in scenarios where LMAs run in a datacenter-like infrastructure. It can be used to allocate a different LMA based on other policies such as routing, although it is not clear how the technology can be used to achieve distributed mobility management, especially considering scalability issues. There are different gaps that would prevent using this mechanism as a way to meet all the DMM requirements: i) LMA runtime assignment can only performed at the MN’s attachment, so it would need to be extended to allow LMA re-location at any time; ii) LMA runtime assignment can only be initiated by current LMA; iii) it is not in the scope of the specification how the context is transferred between the involved LMAs.

Source Address Selection It can help in selecting a given IP source address although the current specifications have many limitations (for instance prefer IPv6 over IPv4, prefer HoA instead of CoA) and the socket extensions [RFC5014] require changes in the node. This solution alone is not sufficient to achieve anchors distribution in case of session continuity requirements, as some control logic (e.g., from a connection manager [I-D.seite-mif-cm]) is needed to intelligently perform source address selection.

Multihoming in PMIPv6 As summarized in the previous section a single mobility session belongs to a single LMA (at the most the same mobility session is shared across two access networks). As of today there is no possibility to distribute anchors and to move the session between different LMAs.

3.2.2. REQ2: Transparency to Upper Layers when needed

PMIPv6 As a mobility protocol, the solution provides transparent mobility support for a mobile node while roaming within the PMIPv6 domain (e.g., if a mobile node moves outside the domain, established sessions cannot be maintained, unless the MN implements Mobile IPv6). However, as for the MIPv6 case, this transparent mobility support comes with the cost of suboptimal routes if the MN moves away from its initial attachment point, especially in large PMIPv6 domains.

Local Routing During HO the standard mechanisms are used. In this sense if there is a MAG change while LR is enabled signaling is exchanged to inform the target MAG that upon handover LR should be re-established. The inter LMA case is not supported. For this solution the mobility context is always up, all the traffic receive seamless service.

LMA Runtime Assignment Seamless support is provided as per RFC 5213. Since the LMA cannot be changed at runtime, the solution provides transparency to the upper layers. However, if the solution were extended to allow dynamic LMA re-location, some extensions would be needed to provide IP address continuity.

Source Address Selection No seamless support is currently provided, since it requires solutions such as IP flow mobility for PMIPv6 [I-D.ietf-netext-pmipv6-flowmob].

Multihoming in PMIPv6 Seamless support falls back to standard PMIPv6 operations extended for IP flow mobility support. For this solution the mobility context is always up, all the traffic receive seamless service.

3.2.3. REQ3: IPv6 deployment

PMIPv6 Although Proxy Mobile IPv6 primarily support IPv6, there are also extensions defined to also offer some limited IPv4 support [RFC5844].

Local Routing It supports both IPv4 (limited to the support provided by [RFC5844]) and IPv6.

LMA Runtime Assignment It supports both IPv4 (limited to the support provided by [RFC5844]) and IPv6.

Source Address Selection It supports both IPv4 and IPv6.

Multihoming in PMIPv6 It supports both IPv4 (limited to the support provided by [RFC5844]) and IPv6.

3.2.4. REQ4: Existing mobility protocols

PMIPv6 This approach is one of the base IETF-standardized mobility protocols: [RFC5213].

Local Routing It reuses [RFC5213].

LMA Runtime Assignment It reuses [RFC5213].

Source Address Selection This approach is based on local support on the terminal only.

Multihoming in PMIPv6 It reuses [RFC5213].

3.2.5. REQ5: Compatibility

PMIPv6 This protocol is compatible with other protocols and can operate between trusted administrative domains, although there may be an associated penalty in terms of performance and/or complexity [A. de la Oliva, et al.].

Local Routing Since it extends [RFC5213], compatibility with existing network deployments and end hosts is provided.

LMA Runtime Assignment Since it extends [RFC5213], compatibility with existing network deployments and end hosts is provided.

Source Address Selection To enable the full set of use cases mentioned above extensions are required thus impacting the landscape of mobile devices. The extensions should not impact the network.

Multihoming in PMIPv6 Since it extends [RFC5213], compatibility is provided.

3.2.6. REQ6: Security considerations

PMIPv6 This approach includes security considerations.

Local Routing It reuses [RFC5213]. As such, the same security considerations apply.

LMA Runtime Assignment It reuses [RFC5213]. As such, the same security considerations apply.

Source Address Selection There is not signaling involved to perform this action.

Multihoming in PMIPv6 It reuses [RFC5213]. As such, the same security considerations apply.

3.3. 3GPP mobility

3.3.1. REQ1: Distributed deployment

SIPTO enables a certain degree of distribution, as SGW/PGW can be selected to be the closest geographically to the UE. This, together with the use of OPIIS (and MAPCON for the case the UE is using multiple interfaces), could be used to allow the use of different anchors as the UE moves. However, as described below, there is no support for dynamically changing the anchor while providing IP address continuity, which might be OK for short-lived sessions.

3.3.2. REQ2: Transparency to Upper Layers when needed

Seamless mobility at the local network is still not considered in SIPTO. Therefore, although SIPTO and LIPA allow offloading traffic from the network core similarly to the DMM approaches, even with LIMONET they just provide localized mobility support, requiring packet data network connections to be deactivated and re-activated when the UE is not moving locally.

3.3.3. REQ3: IPv6 deployment

3GPP specs support IPv6 as described in [RFC6459].

3.3.4. REQ4: Existing mobility protocols

Current 3GPP specifications make use of both IETF standardized mechanisms (e.g., PMIPv6, DSMIPv6), and custom made mechanisms, such as GTP.

3.3.5. REQ5: Compatibility

All the 3GPP extensions listed in this document are compatible with 3GPP networks, at least for the same release these extensions are introduced or newer ones.

3.3.6. REQ6: Security considerations

3GPP extensions are assumed to be secure. TBD: refine (possibly extending) this section.

4. Conclusions

In this section we identify the gaps between existing mobility solutions and the DMM requirements and expected functionalities. We first summarize the identified IP-mobility protocols and provide a mapping (e.g., YES, NO, LIMITED) to the different DMM requirements listed in [I-D.ietf-dmm-requirements]. Following the independent analysis, a comparison between the solutions and the main DMM functionalities is provided. Finally, the possibility of using multiple solutions is addressed by combining different solutions according to the results found in the independent and functional analysis.

4.1. Independent solution analysis

	REQ1	REQ2	REQ3	REQ4	REQ5	REQ6
MIPv6/NEMO	NO	LIM	v6/v4	YES	LIM	YES
MIPv6 RO	NO	YES	v6	YES	LIM	YES
HMIPv6	NO	YES	v6	YES	LIM	YES
HA switch	NO	NO	v6	YES	YES	YES
FlowMob	NO	YES	v6/LIM v4	YES	YES	YES
SAS w/ CB	NO	YES	v6/v4	YES	YES	YES
PMIPv6	NO	LIM	v6/LIM v4	YES	LIM	YES
LR	NO	LIM	v6/LIM v4	YES	YES	YES
LMA RA	LIM	LIM	v6/LIM v4	YES	YES	YES
SAS w/ NB	NO	NO	v6/v4	YES	YES	YES
MuHo PMIPv6	NO	LIM	v6/LIM v4	YES	YES	YES

4.2. Functional analysis

The goal of this section is to identify and analyze the main functions that a DMM solution should provide in order to meet the DMM requirements [I-D.ietf-dmm-requirements]. This analysis is on purpose kept at high level, and will be used in the following section as main guideline for the final assessment of the gaps that cannot be covered with existing specified and deployed solutions (even if combined).

4.2.1. Multiple anchoring

Multiple (distributed) anchoring refers to the ability to anchor different sessions of a single mobile node at different anchors. In order to make this feature "DMM-friendly", some anchors should be placed closer to the mobile node. This implies the ability to deploy routers and assign locally anchored IP addresses at the edge of the network. This feature also requires potentially assigning multiple IP addresses to a single mobile node for its simultaneous use.

Figure 5 shows an example of the multiple anchoring function, in which a mobile network operator (MNO) has deployed multiple anchors, placed closer to or at the access network level. These (distributed) anchors provide attaching terminals with IP addresses that are locally anchored, allowing MNs’ traffic (Internet and operator services) to be locally offloaded (i.e., not traversing the MNO’s core).

```
                       +-----+          +-----+
                       | CN1 |          | CN2 |
                       +-----+          +-----+
                          |                |
                        +--------------------+
                       (                      )
                      (        Internet        )
                       (                      )
                        +--------------------+
                                  ||
         +------------------------------------------------+
        (                                                  )
       (      --------------------                          )
      (       |   centralized    |      Mobile Network       )
     (        |   anchor (e.g.,  |        Operator’s          )
      (       | LMA/HA/PGW/GGSN) |          core             )
       (      --------------------                          )
        (                                                  )
         +------------------------------------------------+
              /                  |                  \
             /    * Internet     |      x Internet   \       + Internet
            /    * / access      |     x / access     \     + / access
           /    * /              |    x /              \   + /
        --+------+-----      ----+-----+----      ------+---+----
        | distributed | * * *| distributed |      | distributed |
        |   anchor 1  |      |   anchor i  |      |   anchor n  |
        ---+-----------      ---+-----------      ---+-----------
           |                    |                    |
          (o)                  (o)                  (o)
                   session    * x  session          +  session
                   anchored  * x   anchored        +   anchored
                     at 1   * x      at i         +      at n
                           (o)                  (o)
                            |                    |
                         +--+--+              +--+--+
                         | MN1 |              | MN2 |
                         +-----+              +-----+
```

Figure 5: Multiple anchoring

4.2.2. Dynamic anchor assignment

Dynamic anchor re-location is the ability to i) optimally assign initial anchor, and ii) change the initially assigned anchor and/or assign a new one. This can be achieved either by changing anchor for all ongoing sessions (which might only be achievable with routing-based solutions), or by assigning new anchors for new sessions.

Figure 6 shows an example of what the dynamic anchor assignment function provides. A mobile node MN1, initially attached to the distributed anchor 1, establishes a session X (anchored at 1, i.e., optimal initial anchor assignment), which finishes before MN1 moves to the distributed anchor i. While connected to the distributed anchor i, a new session Y is established, which is anchored at i (i.e. assignment of a new anchor). Then MN1 moves and attaches to the distributed anchor n, while having session Y active, where MN1 is assigned n as its anchor for new sessions and (optionally) existing sessions are moved (i.e., change of assigned anchor).

```
        (                                                  )
         +------------------------------------------------+
              /                  |                  \
             /    * Internet     |     x Internet    \       x Internet
            /    * / access      |    x / access      \     x / access
           /    * /              |   x /               \   x /
        --+------+-----      ----+----+-----      ------+---+----
        | distributed |      | distributed |      | distributed |
        |   anchor 1  |      |   anchor i  |      |   anchor n  |
        ---+-----------      ---+-----------      ---+-----------
           |                    |                    |
          (o)                  (o)                  (o)
               *               x  session Y         x  session Y
      session X    *          x   anchored         x   anchored
      anchored          *    x      at i          x     (moved)
        at 1               (o)                  (o)      at n
                            |                    |
                         +--+--+          \   +--+--+
                         | MN1 |  =========)  | MN1 |
                         +-----+          /   +-----+
```

Figure 6: Dynamic anchor assignment

4.2.3. Multiple address management

Multiple IP address management refers to the ability of the mobile node to simultaneously use multiple IP addresses and select the best one (from an anchoring point of view) to use on a per-session/application/service basis. Depending on the mobile node support, this functionality might require more or less support from the network side.

Figure 7 shows an example of multiple address management, in which MN1 initially obtained an IP address (IP a) when connected to the distributed anchor 1, which is then used for a session which remains active after MN1 moves and attaches to the distributed anchor i. MN1 also obtains a new IP address (IP b) to be used for sessions initiated while attached to i. MN1 therefore needs to simultaneously manage and use multiple IP addresses, selecting the best one for each session. This selection might be performed by the mobile node solely or might be aided/performed with network support.

```
        (                                                  )
         +------------------------------------------------+
              /                  |                  \
             /    * Internet     |      x Internet   \         Internet
            /    * / access      |     x / access     \       / access
           /    * / (IP a)       |    x / (IP b)       \     /
        --+------+-----      ----+-----+----      ------+---+----
        | distributed | * * *| distributed |      | distributed |
        |   anchor 1  |      |   anchor i  |      |   anchor n  |
        ---+-----------      ---+-----------      ---+-----------
           |                    |                    |
          (o)                  (o)                  (o)
                  session X   * x  session Y
                   anchored  * x   anchored
                     at 1   * x      at i
                    (IP a) (o)      (IP b)
                            |
                         +--+--+
                         | MN1 |
                         +-----+
```

Figure 7: Multiple address management

4.3. Combined solutions analysis

The goal of this section is to evaluate how a solution based on combining the different standardized IP mobility solutions could meet the DMM requirements, making reference to the high-level functions identified above.

Both the main client- and network-based IP mobility protocols, namely (DS)MIPv6 and PMIPv6 allows to deploy multiple anchors (i.e., home agents and localized mobility anchors), therefore providing the functionality of multiple anchoring. However, existing solutions does only provide an optimal initial anchor assignment, a gap being the lack of dynamic anchor change/new anchor assignment. Neither the HA switch nor the LMA runtime assignment allow changing the anchor during an ongoing session.

Even if dynamic anchor change and new anchor assignment were supported, default address selection mechanisms would need to be improved, as mobile nodes would likely be assigned multiple IP addresses, anchored at different places. Therefore, smart address selection, trying to always use the shortest path, would be required.

5. IANA Considerations

No IANA considerations.

6. Security Considerations

This is an informational document that analyzes practices for the deployment of existing mobility protocols in a distributed mobility management environment, and identifies the limitations in the current practices. One of the requirements that these practices has to meet is to take into account security aspects, including confidentiality and integrity. This is briefly analyzed for each of the considered practices, and will be extended in future versions of this document.

7. References

7.1. Normative References

[RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.

[RFC5026] Giaretta, G., Kempf, J., and V. Devarapalli, "Mobile IPv6 Bootstrapping in Split Scenario", RFC 5026, October 2007.

[RFC5142] Haley, B., Devarapalli, V., Deng, H., and J. Kempf, "Mobility Header Home Agent Switch Message", RFC 5142, January 2008.

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC5380] Soliman, H., Castelluccia, C., ElMalki, K., and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", RFC 5380, October 2008.

[RFC5555] Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, June 2009.

[RFC5568] Koodli, R., "Mobile IPv6 Fast Handovers", RFC 5568, July 2009.

[RFC5648] Wakikawa, R., Devarapalli, V., Tsirtsis, G., Ernst, T., and K. Nagami, "Multiple Care-of Addresses Registration", RFC 5648, October 2009.

[RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.

[RFC6088] Tsirtsis, G., Giarreta, G., Soliman, H., and N. Montavont, "Traffic Selectors for Flow Bindings", RFC 6088, January 2011.

[RFC6089] Tsirtsis, G., Soliman, H., Montavont, N., Giaretta, G., and K. Kuladinithi, "Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support", RFC 6089, January 2011.

[RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

[RFC6463] Korhonen, J., Gundavelli, S., Yokota, H., and X. Cui, "Runtime Local Mobility Anchor (LMA) Assignment Support for Proxy Mobile IPv6", RFC 6463, February 2012.

[RFC6611] Chowdhury, K. and A. Yegin, "Mobile IPv6 (MIPv6) Bootstrapping for the Integrated Scenario", RFC 6611, May 2012.

[RFC6705] Krishnan, S., Koodli, R., Loureiro, P., Wu, Q., and A. Dutta, "Localized Routing for Proxy Mobile IPv6", RFC 6705, September 2012.

[RFC6724] Thaler, D., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, September 2012.

7.2. Informative References

[3GPP.23.829] 3GPP, "Local IP Access and Selected IP Traffic Offload (LIPA-SIPTO)", 3GPP TR 23.829 10.0.1, October 2011.

[3GPP.23.859] 3GPP, "LIPA Mobility and SIPTO at the Local Network", 3GPP TR 23.859 0.5.0, June 2012.

[3GPP.29.060] 3GPP, "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface", 3GPP TS 29.060 3.19.0, March 2004.

[A. de la Oliva, et al.]
de la Oliva, A., Soto, I., Calderon, M., Bernardos, C., and M. Sanchez, "The costs and benefits of combining different IP mobility standards", Computer Standards & Interfaces, accepted for publication, doi:10.1016/j.csi.2012.08.003 , 2012.

[I-D.ietf-dmm-requirements]
Chan, A., "Requirements for Distributed Mobility Management", draft-ietf-dmm-requirements-02 (work in progress), September 2012.

[I-D.ietf-netext-pmipv6-flowmob]
Bernardos, C., "Proxy Mobile IPv6 Extensions to Support Flow Mobility", draft-ietf-netext-pmipv6-flowmob-05 (work in progress), October 2012.

[I-D.patil-dmm-issues-and-approaches2dmm]
Patil, B., Williams, C., and J. Korhonen, "Approaches to Distributed mobility management using Mobile IPv6 and its extensions", draft-patil-dmm-issues-and-approaches2dmm-00 (work in progress), March 2012.

[I-D.perkins-dmm-matrix]
Perkins, C., Liu, D., and W. Luo, "DMM Comparison Matrix", draft-perkins-dmm-matrix-04 (work in progress), July 2012.

[I-D.seite-mif-cm]
Seite, P. and J. Zuniga, "MIF API Conn Mngr Considerations", draft-seite-mif-cm-00 (work in progress), September 2012.

[RFC4225] Nikander, P., Arkko, J., Aura, T., Montenegro, G., and E. Nordmark, "Mobile IP Version 6 Route Optimization Security Design Background", RFC 4225, December 2005.

[RFC4640] Patel, A. and G. Giaretta, "Problem Statement for bootstrapping Mobile IPv6 (MIPv6)", RFC 4640, September 2006.

[RFC5014] Nordmark, E., Chakrabarti, S., and J. Laganier, "IPv6 Socket API for Source Address Selection", RFC 5014, September 2007.

[RFC6301] Zhu, Z., Wakikawa, R., and L. Zhang, "A Survey of Mobility Support in the Internet", RFC 6301, July 2011.

[RFC6459] Korhonen, J., Soininen, J., Patil, B., Savolainen, T., Bajko, G., and K. Iisakkila, "IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS)", RFC 6459, January 2012.

Appendix A. Acknowledgments

The work of Carlos J. Bernardos and Telemaco Melia has been partially supported by the European Community's Seventh Framework Programme (FP7-ICT-2009-5) under grant agreement n. 258053 (MEDIEVAL project). The work of Carlos J. Bernardos has also been partially supported by the Ministry of Science and Innovation of Spain under the QUARTET project (TIN2009-13992-C02-01). The authors would like to thank Konstantinos Pentikousis, Georgios Karagiannis, Jouni Korhonen, Jong-Hyouk Lee, Marco Liebsch, Elena Demaria, Peter McCann, Luo Wen and Julien Laganier for their valuable comments.

Authors' Addresses

Juan Carlos Zuniga
InterDigital Communications, LLC
1000 Sherbrooke Street West, 10th floor
Montreal, Quebec H3A 3G4
Canada

Email: JuanCarlos.Zuniga@InterDigital.com
URI: http://www.InterDigital.com/

Carlos J. Bernardos
Universidad Carlos III de Madrid
Av. Universidad, 30
Leganes, Madrid 28911
Spain

Phone: +34 91624 6236
Email: cjbc@it.uc3m.es
URI: http://www.it.uc3m.es/cjbc/

Telemaco Melia
Alcatel-Lucent Bell Labs
Route de Villejust
Nozay, Ile de France 91620
France

Email: telemaco.melia@alcatel-lucent.com

Charles E. Perkins
Futurewei
USA

Email: charliep@computer.org