DMM
Internet-Draft
Intended status: Informational
Expires: December 19, 2013

D. Liu, Ed.
China Mobile
JC. Zuniga, Ed.
InterDigital
P. Seite
Orange
H. Chan
Huawei Technologies
CJ. Bernardos
UC3M

June 17, 2013

Distributed Mobility Management: Current practices and gap analysis
draft-ietf-dmm-best-practices-gap-analysis-01

Abstract

The present document analyses deplyment practices of existing mobility protocols in a distributed mobility management environment. It also identifies some limitations compared to the expected functionality of a fully distributed mobility management system. The comparison is made taking into account the identified DMM requirements.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

The distributed mobility management (DMM) WG has studied the problems of centralized deployment of mobility management protocols and the related requirements [I-D.ietf-dmm-requirements]. In order to guide the deployment and before defining any new DMM protocol, the DMM WG is chartered to investigate first whether it is feasible to deploy current IP mobility protocols in a DMM scenario in a way that can fullfil the requirements of DMM. This document discusses current deployment practices of existing mobility protocols in a distributed mobility management environment and identifies the limitations in these practices with respect to the expected functionality.

The rest of this document is organized as follows. Section 3 analyzes existing IP mobility protocols by examining their functions and how these functions can be reconfigured to work in a DMM environment. Section 4 presents the current practices of IP flat wireless networks and 3GPP architectures. Both network- and host-based mobility protocols are considered. Section 5 presents the gap analysis with respect to the current practices.

2. Terminology

All general mobility-related terms and their acronyms used in this document are to be interpreted as defined in the Mobile IPv6 base specification [RFC6275] and in the Proxy mobile IPv6 specification [RFC5213]. These terms include mobile node (MN), correspondent node (CN), home agent (HA), local mobility anchor (LMA), and mobile access gateway (MAG).

In addition, this document uses the following terms:

Mobility routing (MR) is the logical function that intercepts packets to/from the IP address/prefix delegated to the mobile node and forwards them, based on internetwork location information, either directly towards their destination or to some other network element that knows how to forward the packets to their ultimate destination.

Home address allocation is the logical function that allocates the IP address/prefix (e.g., home address or home network prefix) to a mobile node.

Location management (LM) is the logical function that manages and keeps track of the internetwork location information of a mobile node, which includes the mapping of the IP address/prefix delegated to the MN to the MN routing address or another network element that knows where to forward packets destined for the MN.

Home network of an application session (or an HoA IP address) is the network that has allocated the IP address used as the session identifier (home address) by the application being run in an MN. The MN may be attached to more than one home networks.

In the document, several references to a distributed mobility management environment are made. By this term, we refer to an scenario in which the IP mobility, access network and routing solutions allow for 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.

3. Functions of existing mobility protocols

The host-based Mobile IPv6 [RFC6275] and its network-based extension, PMIPv6 [RFC5213], are both logically centralized mobility management approaches addressing primarily hierarchical mobile networks. Although they are centralized approaches, they have important mobility management functions resulting from years of extensive work to develop and to extend these functions. It is therefore fruitful to take these existing functions and examine them in a DMM scenario in order to understand how to deploy the existing mobility protocols in a distributed mobility management environment.

The existing mobility management functions of MIPv6, PMIPv6, and HMIPv6 are the following:

1. Anchoring function (AF): allocation to a mobile node of an IP addres/prefix (e.g., a HoA or HNP) topologically anchored by the delegating node (i.e., the anchor node is able to advertise a connected route into the routing infrastructure for the delegated IP prefixes).

2. Mobility Routing (MR) function: packets interception and forwarding to/from the IP address/prefix delegated to the MN, based on the internetwork location information, either to the destination or to some other network element that knows how to forward the packets to their destination;

3. Internetwork Location Management (LM) function: managing and keeping track of the internetwork location of an MN, which includes a mapping of the IP delegated address/prefix (e.g., HoA or HNP) to the mobility anchoring point where the MN is anchored to;

4. Location Update (LU): provisioning of MN location information to the LM function;

In Mobile IPv6 [RFC6275], the home agent typically provides the anchoring function (AF), Mobility Routing (MR), and Internetwork Location Management (LM) functions, while the mobile node provides the Location Update (LU) function. Proxy Mobile IPv6 [RFC5213] 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). With network-based IP mobility protocols, the local mobility anchor typically provides the anchoring function (AF), Mobility Routing (MR), and Internetwork Location Management (LM) functions, while the mobile access gateway provides the Location Update (LU) function.

4. DMM practices

This section documents deployment practices of existing mobility protocols in a distributed mobility management environment. This description is divided into two main families of network architectures: i) IP flat wireless networks (e.g., evolved WiFi hotspots) and, ii) 3GPP network flattening approaches.

While describing the current DMM practices, references to the generic mobility management functions described in Section 3 will be provided, as well as some initial hints on the identified gaps with respect to the DMM requirement documented in [I-D.ietf-dmm-requirements].

4.1. Assumptions

There are many different approaches that can be considered to implement and deploy a distributed anchoring and mobility solution. Since this document cannot be too exhaustive, the focus is on current mobile network architectures and standardized IP mobility solutions. In order to limit the scope of our analysis of current DMM practices, we consider the following list of technical assumptions:

1. Both host- and network-based solutions should be covered.

2. Solution should allow selecting and using the most appropriate IP anchor among a set of distributed ones.

3. Mobility management should be realized by the preservation of the IP address across the different points of attachment during the mobility (i.e., provision of IP address continuity). IP flows of applications which do not need a constant IP address should not be handled by DMM. It is typically the role of a connection manager to distinguish application capabilities and trigger the mobility support accordingly. Further considerations on application management are out of the scope of this document.

4. Mobility management and traffic redirection should only be triggered due to IP mobility reasons, that is when the MN moves from the point of attachment where the IP flow was originally initiated.

4.2. IP flat wireless network

This section focuses on common IP wireless network architectures and how they can be flattened from an IP mobility and anchoring point of view using common and standardized protocols. Since WiFi is the most widely deployed wireless access technology nowadays, we take it as example in the following. Some representative examples of WiFi deployed architectures are depicted on Figure 1.

```
                    +-------------+          _----_
    +---+           |   Access    |        _(      )_
    |AAA|. . . . . .| Aggregation |----------( Internet )
    +---+           |   Gateway   |        (_      _)
                    +-------------+          '----'
                       |  |   |
                       |  |   +-------------+
                       |  |                 |
                       |  |              +-----+
        +----------------+  |              | AR  |
        |                 |              +--+--+
     +-----+           +-----+         *----+----*
     | RG  |           | WLC |        (    LAN    )
     +-----+           +-----+         *---------*
        .              /    \             /    \
       / \         +----+  +----+     +----+  +----+
      MN MN        |WiFi|  |WiFi|     |WiFi|  |WiFi|
                   | AP |  | AP |     | AP |  | AP |
                   +----+  +----+     +----+  +----+
                     .                  .
                    / \                / \
                   MN MN              MN MN
```

Figure 1: IP WiFi network architectures

In the figure, three typical deployment options are shown [I-D.gundavelli-v6ops-community-wifi-svcs]. On the left hand side of the figure, mobile nodes directly connect to a Residential Gateway (RG) which is a network device that is located in the customer premises and provides both wireless layer-2 access connectivity (i.e., it hosts the 802.11 Access Point function) with layer-3 routing functions. In the middle, mobile nodes connect to WiFi Access Points (APs) that are managed by a WLAN Controller (WLC), which performs radio resource management on the APs, system-wide mobility policy enforcement and centralized forwarding function for the user traffic. The WLC could also implement layer-3 routing functions, or attach to an access router (AR). Last, on the right-hand side of the figure, access points are directly connected to an access router, which can also be used a generic connectivity model.

In some network architectures, such as the evolved Wi-Fi hotspot, operators might make use of IP mobility protocols to provide mobility support to users, for example to allow connecting the IP WiFi network to a mobile operator core and support roaming between WLAN and 3GPP accesses. Two main protocols can be used: Proxy Mobile IPv6 [RFC5213] or Mobile IPv6 [RFC6275], [RFC5555], with the anchor role (e.g., local mobility anchor or home agent) typically being played by the Access Aggregation Gateway or even by an entity placed on the

mobile operator's core network.

Existing IP mobility protocols can also be deployed in a "flatter" way, so the anchoring and access aggregation functions are distributed. We next describe several practices for the deployment of existing mobility protocols in a distributed mobility management environment. We limit our analysis in this section to protocol solutions based on existing IP mobility protocols, either host- or network-based, such as Mobile IPv6 [RFC6275], [RFC5555], Proxy Mobile IPv6 [RFC5213], [RFC5844] and NEMO [RFC3963]. Extensions to these base protocol solutions are also considered. We pay special attention to the management of the use of care-of-addresses versus home addresses in an efficient manner for different types of communications. Finally, and in order to simplify the analysis, we divide it into two parts: host- and network-based practices.

4.2.1. Host-based IP DMM practices

Mobile IPv6 (MIPv6) [RFC6275] and its extension to support mobile networks, the NEMO Basic Support protocol (hereafter, simply NEMO) [RFC3963] are well-known host-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. In these approaches, the home agent typically provides the anchoring function (AF), Mobility Routing (MR), and Internetwork Location Management (LM) functions, while the mobile node provides the Location Update (LU) function. We next describe some practices on how Mobile IPv6/NEMO and several additional protocol extensions can be deployed in a distributed mobility management environment.

One approach to distribute the anchors can be to deploy several HAs (as shown in Figure 2), and assign to each MN the one closest to its topological location [RFC4640], [RFC5026], [RFC6611]. In the example shown in Figure 2, MN1 is assigned HA1 (and a home address anchored by HA1), while MN2 is assigned HA2. Note that Mobile IPv6 / NEMO specifications do not prevent the simultaneous use of multiple home agents by a single mobile node. This deployment model could be exploited by a mobile node to meet assumption #4 and use several anchors at the same time, each of them anchoring IP flows initiated at different point of attachment. However there is no mechanism specified to enable an efficient dynamic discovery of available anchors and the selection of the most suitable one.

```
    <- 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 2: Distributed operation of Mobile IPv6 (BT and RO) / NEMO

Since one of the goals of the deployment of mobility protocols in a distributed mobility management environment is to avoid the suboptimal routing caused by centralized anchoring, the Route Optimization (RO) support provided by Mobile IPv6 can also be used to achieve a flatter IP data forwarding. 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. The Route Optimization (RO) mode 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 2, 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.

o 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.

```
     <- 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 3: Hierarchical Mobile IPv6

Hierarchical Mobile IPv6 (HMIPv6) [RFC5380] is another host-based IP mobility extension that can be considered as a complement to provide a less centralized mobility deployment. It 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 3, 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.).

An additional extension that can be used to help deploying a mobility protocol in a distributed mobility management environment is the the Home Agent switch specification [RFC5142], which defines a new mobility header for signaling a mobile node that it should acquire a new home agent. Even though 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.

4.2.2. Network-based IP DMM practices

Proxy Mobile IPv6 (PMIPv6) [RFC5213] is the main network-based IP mobility protocol specified for IPv6 ([RFC5844] defines some IPv4 extensions). 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). With network-based IP mobility protocols, the local mobility anchor typically provides the anchoring function (AF), Mobility Routing (MR), and Internetwork Location Management (LM) functions, while the mobile access gateway provides the Location Update (LU) function. We next describe some practices on how network-based mobility protocols and several additional protocol extensions can be deployed in a distributed mobility management environment.

```
<- 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 4: 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, can be to deploy several local mobility anchors and use some selection criteria to assign LMAs to attaching mobile nodes (an example of this type of assignment is shown in Figure 4). As per the client based approach, a mobile node may use several anchors at the same time, each of them anchoring IP flows initiated at different point of attachment. This assignment can be static or dynamic (as described later in this document). The main advantage of this simple approach is that the IP address anchor (i.e., the LMA) could be placed closer 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 would start to deviate from the optimal one.

As for host-based IP mobility, there are some extensions defined to mitigate the sub-optimal routing issues that might arise due to the use of a centralized anchor. The Local Routing extensions [RFC6705] enable 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.

An interesting extension that can also be used to facilitate the deployment of network-based mobility protocols in a distributes mobility management environment is the LMA runtime assignment [RFC6463]. This extension 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.

4.3. 3GPP network flattening approaches

The 3rd Generation Partnership Project (3GPP) is the standard development organization that specifies the 3rd generation mobile network and LTE (Long Term Evolution).

Architecturally, the 3GPP Evolved Packet Core (EPC) network is similar to an IP wireless network running PMIPv6 or MIPv6, as it relies on the Packet Data Gateway (PGW) anchoring services to provide mobile nodes with mobility support (see Figure 5). 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 5: EPS (non-roaming) architecture overview

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.

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 (see Figure 6.

```
  +---------+ IP traffic to mobile operator's CN
  |  User   |....................................(Operator's CN)
  | Equipm. |..................
  +---------+                 . Local IP traffic
                              .
                        +-----------+
                        |Residential|
                        |enterprise |
                        |IP network |
                        +-----------+
```

Figure 6: LIPA scenario

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.

```
                           SIPTO Traffic
                               |
                               .
                               .
                           +------+        +------+
                           |L-PGW |   ---- | MME  |
                           +------+  /     +------+
                               |    /
+--------+     +------+    +------+/       +------+
|  UE    |.....|eNB   |....| S-GW |........| P-GW |...> CN Traffic
+--------+     +------+    +------+        +------+
```

Figure 7: SIPTO architecture

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.

```
   +---------------+-------+  +----------+  +-------------+    =====
   |Residential |  |H(e)NB |  | Backhaul |  |Mobile       |   ( IP  )
   |Enterprise  |..|-------|..|          |..|Operator     |..(Network)
   |Network     |  |L-GW   |  |          |  |Core network |   =======
   +---------------+-------+  +----------+  +-------------+
                       /
                       |
                       /
                    +------+
                    | UE  |
                    +------+
```

Figure 8: LIPA architecture

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.

5. Gap analysis

The goal of this section is to identify the limitations in the current practices with respect to providing the expected DMM functionality.

From the analysis performed in Section 4, we can first identify a basic set of functions that a DMM solution needs to provide:

o Multiple (distributed) anchoring: ability to anchor different sessions of a single mobile node at different anchors. In order to make this feature "DMM-friendly", some anchors might need to be placed closer to the mobile node.

o Dynamic anchor assignment/re-location: ability to i) optimally assign initial anchor, and ii) dynamically change the initially assigned anchor and/or assign a new one (this may also require to transfer mobility context between anchors). This can be achieved either by changing anchor for all ongoing sessions, or by assigning new anchors just for new sessions.

o Multiple IP address management: 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. This is typically the role of a connection manager.

In order to summarize the previously listed functions, Figure 9 shows an example of a conceptual DMM solution deployment.

```
        (                                                  )
         +-------------------------------------------------+
              /                  |                  \
             /    * 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 9: DMM functions

Based on the analysis performed in Section 4, the following list of gaps can be identified:

o 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 multiple anchoring function. However, existing solutions do 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. This actually comprises several gaps: ability to perform anchor assignment at any time (not only at the initial MN's attachment), ability of the current anchor to initiate/trigger the relocation, and ability of transferring registration context between anchors.

- The dynamic anchor relocation needs to ensure that IP address continuity is guaranteed for sessions that need it at the relocated anchor. This for example implies having the knowledge of which sessions are active at the mobile node, which is something typically known only by the MN (namely, by its connection manager). Therefore, (part of) this knowledge might need to be transferred to/shared with the network.

- Dynamic discovery and selection of anchors. There might be more than one available anchor for a mobile node to use. Currently, there is no efficient mechanism that allows to dynamically discover the presence of nodes that can play the role of anchor, discover their capabilities and allow the selection of the most suitable one.

- NOTE: This section is in progress. More gaps are still to be identified and more text added to these bullets (perhaps even assigning one subsection to each one). More discussion/feedback from the group is still needed.

6. Security Considerations

TBD.

7. IANA Considerations

None.

8. 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, "Local IP access (LIPA) mobility and Selected IP Traffic Offload (SIPTO) at the local network", 3GPP TR 23.859 12.0.1, April 2013.

[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.

[I-D.gundavelli-v6ops-community-wifi-svcs]

Gundavelli, S., Grayson, M., Seite, P., and Y. Lee, "Service Provider Wi-Fi Services Over Residential Architectures", draft-gundavelli-v6ops-community-wifi-svcs-06 (work in progress), April 2013.

[I-D.ietf-dmm-requirements]
Chan, A., Liu, D., Seite, P., Yokota, H., and J. Korhonen, "Requirements for Distributed Mobility Management", draft-ietf-dmm-requirements-05 (work in progress), June 2013.

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

[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.

[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.

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

[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.

Authors' Addresses

Dapeng Liu (editor)
China Mobile
Unit2, 28 Xuanwumenxi Ave, Xuanwu District
Beijing 100053
China

Email: liudapeng@chinamobile.com

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

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

Pierrick Seite
Orange
4, rue du Clos Courtel, BP 91226
Cesson-Sevigne 35512
France

Email: pierrick.seite@orange.com

H Anthony Chan
Huawei Technologies
5340 Legacy Dr. Building 3
Plano, TX 75024
USA

Email: h.a.chan@ieee.org

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/