MEXT Working Group R. Kuntz
Internet-Draft Toyota ITC
Intended status: Informational D. Sudhakar
Expires: February 12, 2012 UCLA
R. Wakikawa
Toyota ITC
L. Zhang
UCLA
August 11, 2011

A Summary of Distributed Mobility Management
draft-kuntz-dmm-summary-01

Abstract

As stated in the MEXT charter, the working group will "work on operational considerations on setting up Mobile IPv6 networks so that traffic is distributed in an optimal way". This topic, referred to as Distributed Mobility Management (DMM), has motivated the submission of multiple problem statement and solution drafts. This document aims at summarizing the current status of the DMM effort, mainly focusing on Mobile IPv6-based solutions, in order to initiate more discussions within the working group.

Table of Contents

1. Introduction

In its charter, the MEXT working group mentions the need to work on "operational considerations on setting up Mobile IPv6 networks so that traffic is distributed in an optimal way". The expected deliverable is an Internet Draft on "Operational considerations for distributed use of Mobile IPv6" for publication as an informational document.

This topic of Distributed Mobility Management (DMM) has motivated the submission of multiple problem statement and solution drafts, that often share common concepts and ideas. This document first summarizes the motivation and problem statement documents submitted in the MEXT working group. Then, we expose an overview of four representative proposed approaches based on Mobile IPv6 (MIPv6). In the conclusion, we analyze the benefits and drawbacks of each approach. Three Proxy Mobile IPv6 (PMIPv6)-based solutions have also been considered and are summarized in the Appendix.

The goal of this document is to initiate discussion within the working group towards an agreement on the needed requirements and a unified DMM solution.

2. Summary of the Problem Statement

2.1. Issues of centralized mobility solutions

The following Internet Drafts have been considered in this section:

- [I-D.chan-distributed-mobility-ps],
- [I-D.liu-mext-distributed-mobile-ip] (that shares a vast portion of text with the previously mentioned draft),
- [I-D.patil-mext-dmm-approaches].

Centralized mobility solutions (i.e. which rely on the use of a single mobility anchor) suffer from the following drawbacks:

- Non-optimal routes, especially as Content Delivery Network (CDN) servers are being placed closer to the edge of the network. This results in long delays between mobile clients and content servers, as well as unecessary load in the core network.
- Low scalability that requires the deployment of several mobility anchors along with the increasing number of mobile nodes. Furthermore, more and more traffic is to be expected from and to these mobile devices, which could result in congestions at the mobility anchor.
- Mobility support is performed per node, and not per flow, which makes offloading (i.e. the possibility to bypass the mobility anchor) impossible for some of the traffic. We cannot expect route optimization capabilities to exists at every correspondent node. In such cases, all of the traffic from and towards a mobile node has to go through the centralized mobility anchor, which worsens the previously mentioned issues. This is especially true when Mobile Node communications are made in a fixed situation. In such case, mobility solutions systematically rely on the centralized mobility anchor whithout considering if the MN is really moving or not.
- The mobility anchor is a single point of failure: if a large number of mobile nodes share the same mobility anchor, they can all be affected by a single outage. In the specific case of Mobile IPv6, this issue is however supposed to be solved by the standardization of the Home Agent Reliability Protocol (HARP) [I-D.ietf-mip6-hareliability].
- Signaling messages of the mobility protocol, as well as reliability protocols such as HARP, can represent a significant

overhead, both for the MN and the mobility anchor. This is also true when considering route optimization modes that involves the MN, the mobility anchor and the CN.

2.2. Requirements of DMM

The following Internet Drafts have been considered in this section:

- [I-D.yokota-dmm-scenario],
- [I-D.liu-distributed-mobility],
- [I-D.liu-distributed-mobility-traffic-analysis].

DMM should be achieved by considering the following requirements:

- The distribution of the mobility anchors (e.g. the Home Agents) in order to achieve a more flat design. This would improve scalability and robustness of the mobility infrastructure.

- Placing the mobility management closer to the edge of the network (e.g. at the Access Router level) in order to attain routing optimality and lower delays. Beside, offloading near the edge of the network would become possible, to the benefit of the core network load.

- The dynamic use of mobility support by allowing the split of data flows along different paths that may travel through either the mobility anchor or non-anchor nodes, even though no specific route optimization support is available at the correspondent node. This would further improve the previously mentioned benefits.

- Separating control and data planes by splitting location and routing anchors. Keeping the control plane centralized while distributing the data plane, as previously suggested, could minimize the signaling overhead between the mobility anchors.

- Reusing existing protocols while minimizing changes, in order to allow faster adoption of the technology.

3. Solution Space

A number of solutions for distributing mobility management and flattening the centralized architecture have been proposed for Mobile IPv6 and Proxy Mobile IPv6. Some of these solutions attempt this distribution of mobility management by moving the mobility functionality closer to the edge of the network while others distribute the same functionality among several mobility agents near the core. In this section, we summarize four representative approaches based on Mobile IPv6 that all aim at achieving this purpose. Beside, three solutions based on PMIPv6 are overviewed in Appendix.

3.1. Hierarchical Mobile IPv6 (HMIPv6)

When talking about moving mobility functionality closer to the edge of the network, mention must be made of Hierarchical Mobile IPv6 (HMIPv6) [RFC5380]. HMIPv6 suggests the implementation of an additional mobility agent called the Mobility Anchor Point (MAP) in addition to or instead of the HA (in case of nomadic operations of the MN where a permanent HA is not required). The MAP can be implemented at different levels of the routing hierarchy, even in access routers where it can be most beneficial to the MN in reducing mobility handoff overhead. If the MN is mobile but its movements are very small, then there is a lot of overhead in binding its new location with the HA which could potentially be very far. In this scenario having a MAP closer to the edge of the network and thus closer to the MN can help reduce the time for signaling and handoff.

In HMIPv6, each MN is associated with 3 addresses: the HoA obtained from the HA, the Local Care of Address (LCoA) obtained on link and the Regional Care of Address (RCoA) obtained from stateless configuration using the prefix set advertised by the MAP. When the MN enters the MAP domain, it identifies the MAP it wants to use from router updates and configures its LCoA and RCoA. It then sends a local binding update (local BU) to the MAP to bind its LCoA with its RCoA. After the success of this local BU, the MN binds the RCoA with its HoA at the HA (and its CNs if the MN wants to perform route optimization) (Figure 1). Once this binding is in place, any movement of the MN within the domain of the MAP is hidden from the HA and the CNs as only the LCoA of the MN would change and the RCoA would remain the same. Thus only a local BU to the MAP with the new LCoA would be required and this is faster than sending a new binding update to the HA which could be much further away than the MAP.

```
   CN        HA      MAP      MN
    |        |        |        |
    |        |        |+------|  MN binds LCoA to RCoA at MAP
    |        |+--------------|  MN binds RCoA to HoA at HA
    |------>|======>|======>|  CN->MN without route optimization
    :        :        :        :
    |+----------------------|  MN binds RCoA to HoA at CN for RO
    |-------------->|======>|  CN->MN with route optimization
    |<--------------|<======|  MN->CN
```

Figure 1: Packet routing when MN is anchored at MAP and acquires LCoA on link and RCoA from MAP.

HMIPv6 allows the MN to bind with multiple MAPs simultaneously. This could allow the MN to use MAPs at different levels of the routing hierarchy. However, although HMIPv6 distributes mobility functionality amongst several MAPs, there still remains a centralized HA which is a single point of failure and failure of this HA could cause the location information of the MNs being serviced by the HA to be lost. The MAP also adds an additional layer of indirection to the architecture which may not always be desirable.

3.2. Flat Access and Mobility Architecture (FAMA)

In [I-D.bernardos-mext-dmm-cmip], a decentralized architecture called the Flat Access and Mobility Architecture (FAMA) is proposed. FAMA suggests moving the functionality of the Home Agent (HA) closer to the edge of the network and placing it in the default gateways that provide IP connectivity to the mobile nodes (MNs). Thus the first elements to provide access to the internet for these MNs also perform mobility management. These elements are called Distributed Access Routers (DARs) in FAMA.

When an MN attaches to a DAR, it gets a topologically correct IP address anchored at that DAR. The MN uses this IP address for all its flows while connected to the DAR. When the MN moves, it connects to a new DAR and gets an IP address anchored to the new DAR and uses this IP address for its connections. If, for some reason, the MN decides to retain use of and connectivity to its old IP address anchored with the old DAR, then the MN sends a binding update to the old DAR and the old DAR would then bind the old IP address with the new IP address of the MN (Figure 2). Thus, in MIPv6 terminology, the old DAR becomes the HA of the MN and the old IP address becomes the home address (HoA). Thus any DAR has the potential to act as HA if the MN decides to retain use of an IP address anchored at the DAR.

```
   CN2     CN1    H-DAR    DAR2    MN
    |       |       |       |       |
    |       |       |+--------------|  Binding Update to H-DAR
    |       |------>|==============>|  CN1->MN to HoA anchored at H-DAR
    |       |<------|<==============|  MN->CN1 from HoA anchored at
DAR1
    |       |       |       |       |
    |<----------------------|<------|  MN->CN2 from HoA anchored at
DAR2
    |---------------------->|------>|  CN2->MN to HoA anchored at DAR2
```

Figure 2: Packet routing when MN is anchored at DAR2 and uses the HoA anchored at DAR2 as well as an HoA anchored at some previously visited DAR1.

FAMA allows an MN to simultaneously use several IP addresses anchored at different DARs. However, FAMA does not specify when and under what conditions an MN would want to retain use of its old IP address. FAMA also does not specify whether the MN is associated with a permanent address that can be used to reach it by default. The use of multiple anchored address mandates a mechanism (such as DNS) on the correspondent node side to retrieve a proper and valid destination address for the MN. Care should also be taken to avoid routing loops between DARs and routing dead ends whenever the MN mutually binds a new and old address to two different DARs. This issue is however not peculiar to FAMA. [I-D.ng-intarea-tunnel-loop] discusses this issue and exposes solutions.

3.3. Dynamic Mobile IP (DMI)

Dynamic Mobile IP (DMI) proposed in [I-D.kassi-mobileip-dmi] suggests a use case for establishing when an MN would want to retain use of its old IP address. It proposes that an MN only requires use of an old IP address when there is an ongoing connection/session that has been established using that IP address. Thus, Mobile IP functionality to retain IP address obtained from an old subnet after moving to a new subnet is put to use only when there is ongoing communication while the MN is in motion between subnets. At all other times, regular IP networking using topologically correct IP addresses is used. Thus DMI suggests a different mode for mobility usage in IP networks. This helps reduce the signaling overhead and the number of binding cache entries that have to be maintained by Correspondent Node (CN) in regular MIPv6.

Each MN is associated with a permanent home subnet having a permanent HA which gives the MN a permanent HoA. As long as the MN is

anchored
to the permanent home subnet, usual IP communication takes place without any need for Mobile IP. When the MN moves from the home subnet and anchors itself to a new subnet (referred to as the

temporary home subnet), it identifies the mobility agent in that subnet (referred to as the temporary HA) and obtains a temporary HoA from it. The MN sends a binding update to the permanent HA to register its current location (Figure 3). The MN then proceeds to use its temporary HoA and regular IP connections for all flows initiated after the move has taken place. Mobility routing functions would only be required when there exist flows that have been initiated in the permanent home subnet using the permanent HoA. In this case, triangular routing would have to be performed, in order to maintain location transparency for the CN which sees only the permanent HoA.

```
   CN1    P-HA   T-HA1   MN    T-HA2  CN2
    |      |      |      |      |      |
    |      |+------------|      |      | Binding update to P-HA
    |      |      |+-----|      |      | Binding update to previous T-
HA
    |------------>|=====>|      |      | CN1->MN to old temporary HoA
    |<------------|<=====|      |      | MN->CN1 from old temporary HoA
    |      |      |      |------------>| MN->CN2 from new temporary HoA
    |      |      |      |<------------| CN2->MN to new temporary HoA
    |      |      |      |      |      |
```

Figure 3: Packet routing when MN is associated and registered with permanent HA (P-HA) and has moved from temporary HA1 (T-HA1) to T-HA2. MN uses the HoA acquired form T-HA1 for ongoing flows with CN1 and the HoA acquired from T-HA2 for new flows with CN2.

Every time the MN moves from one subnet to another, the MN sends a binding update to the permanent HA and then continues to use regular IP connections using the new temporary HoA obtained at the new subnet for all flows initiated after the move. If there are any ongoing flows using an old IP address (from an old temporary or permanent subnet), the MN has to additionally perform a binding update with the home agent that provided the IP address with which the flow had been initiated. Thus any temporary HA might have to perform binding updates and mobility routing if an MN initiates a flow using an IP address obtained from that temporary home agent and moves to a different subnet. By ensuring that mobile IP is used only when strictly required, DMI reduces the number of control messages required in MIPv6.

In principles, DMI and FAMA are very similar. FAMA explicitly places the mobility anchor at the access router. DMI better defines when the MN retains use of its old IP addresses. Since the MN is always associated with a permanent HoA, it can always be reached by a CN that does not know the MN's current location. Failure of the permanent HA does not cause the MN to lose connectivity to the network. It can still continue flows that have been initiated using the temporary HoAs.

3.4. Global HA to HA (GHAHA)

Global HA to HA (GHAHA) [I-D.wakikawa-mext-global-haha-spec] builds on the Home Agent Reliability Protocol (HARP) proposed in [I-D.ietf-mip6-hareliability]. HARP provides reliability and availability of HAs by having several redundant HAs form a group. One HA from the group becomes the active HA and receives binding requests and updates from the MNs. The other HAs in the group are standby HAs and are state-synchronized with the active HA. When the active HA fails, one of the HAs in the group takes over as active HA and sends a switch message to all the MNs which will cause them to bind with the new HA. The aliveness of the HAs is determined through periodic HA-Hello messages exchanged among the HAs in the group. The HAs in the group may be either on the same link or on different links (to provide geographic redundancy). The HA switch may also occur when the active HA wants to go offline for maintenance operations.

GHAHA uses the redundant HA architecture suggested by HARP to provide distributed mobility management. A number of geographically distributed HAs form a global HA set and the HAs in the global set form HA links among themselves. All of them advertise the same HA subnet prefix to leverage anycast routing. The MN discovers the topologically closest HA using dynamic home agent address discovery protocol or DNS and binds to it. This HA becomes the primary HA for that MN. When the binding registration with the primary HA is complete, the primary HA sends a state synchronization message to all other HAs in the global set which then create a routing entry for the MN with the primary HA as the next hop.

When a CN anywhere in the internet tries to send a packet to the MN, the packet is routed to the HA in the global set that is nearest to the CN via anycast routing (Figure 4). This HA then looks up its global binding entries and tunnels the packet to the primary HA of the MN. The primary HA then tunnels the packet to the MN. When an MN tries to send a packet to a CN, the packet is tunneled to the primary HA which then routes it to the CN.

```
   MN        HA1       HA2       CN
    |         |         |         |
    |-----+(Primary)    |         |   Binding Registration
    |         |--------+|         |   State Synchronization
    |<========|<========|<--------|   Data from CN to MN
    |========>|------------------>|   Data from MN to CN
    |         |         |         |
```

Figure 4: Packet routing when the MN is anchored to HA1 which is now the primary HA for the MN. HA1 and HA2 have HA links established. HA2 is the closest HA to CN.

The HAs in a global set periodically transmit HA-Hello messages that can be used for checking the aliveness of the HAs. When a HA fails, the nearest HA takes over as the new primary HA for the MNs anchored to the failed HA.

When the MN moves and reattaches to a different subnet, it sends a binding update to its last known primary HA. This binding update gets routed to the currently closest HA via anycast routing. This HA would then forward the binding update to the intended HA. The intended HA would recognize that the packet has been forwarded by a different HA and thus informs the MN that it must now switch to the topologically closest HA. The MN sends a binding request to the new primary HA. All the other HAs modify their global binding when the binding registration and synchronization process is complete.

GHAHA eliminates the problem of single point of failure. Failure of the primary HA does not cause the MN to lose connectivity. The synchronization between all the HAs in the global set ensure that the MN's flows are not disrupted as another HA takes over as the primary HA for the client. Since the HAs are globally distributed, the overhead due to triangular routing is also minimized. GHAHA's major disadvantage is the signaling overhead due to the need to synchronize the state all the HAs. This overhead grows linearly with the number of HAs in the system. The use of anycast routing has also raised concerns on security, as IPsec cannot be applied to communications which endpoints are anycast addresses, and on its impact on the BGP routing system scalability.

It is worth noting that the Scalable Approach for Wide-Area IP Mobility [SAIL] proposes an approach to reduce the signaling overhead by distributing the binding management with one-hop DHT. Through a performance evaluation, it has proven being prone to failure as well as reducing GHAHA's overhead while achieving equal or even better end-to-end delay in most cases.

4. Conclusion

A summary of each approach is presented in Table 1. The base protocol on which the solution relies is stated in the "Reuse protocol" column. "(P)MIPv6" means that the scheme can apply to both MIPv6 and PMIPv6.

Scheme name	Base protocol	Distributed mobility anchors	Dynamic mobility support	Splitting location & routing	Number of HoAs per MN	Required changes
HMIPv6	MIPv6	Yes	No	No	Single one	MN/HA
FAMA	MIPv6	Yes	Partial	No	1 per net	MN
DMI	MIPv6	Yes	Partial	No	1 per net	MN
GHAHA	MIPv6	Yes	No	No	Single one	HA

Table 1: Summary of the solution space.

All of the previously mentioned solutions propose a distributed approach for mobility management, by locating multiple mobility anchors closer to the edge of the network. FAMA locate them at the access router, i.e. at the first element to provide access to the internet to the MNs. DMI requires that a mobility anchor is located in the same IP network than the MN (not necessarily co-located with the access router). HMIPv6 and GHAHA are more flexible as mobility anchors do not need to be located in every IP network where the MN will travel. However, having more mobility anchors improves performance and reliability in case of a failure and decreases latency. HMIPv6 still relies on a centralized HA, which makes it prone to failure and triangular routing.

The use of multiple mobility anchors raise the question of how the IPsec Security Associations (SA) would be deployed and enforced on all of them. This is a matter of concern especially for securing the signaling messages. For that purpose, FAMA proposes to use Cryptographically Generated Addresses, as introduced in [I-D.laganier-mext-cga]. GHAHA relies on HARP to perform such IPsec SA synchronization. The other solutions do not mention how this could be achieved.

The approaches that grant the MN the capability to register to multiple mobility anchors at the same time (HMIPv6, FAMA, DMI) should also implement a mechanism to avoid routing loops between them (e.g.when the MN mutually binds a new and old address to two different mobility anchors). For example, [I-D.ng-intarea-tunnel-loop] discusses this issue and proposes solutions.

Dynamic mobility (i.e. the ability for flows to travel through either the mobility anchor or non-anchor nodes, even though no specific route optimization support is available at the correspondent node), is only partially supported in FAMA, and DMI. These protocols indeed reduce triangular routing by assigning topologically valid IP addresses to the MN every time it moves in a new network. However, it is still unclear how applications could select the desired source address for their sessions. In the case of FAMA, the IPv6 address states could be used to make such decision: when in the "Active/Preferred state", the address could be used for any new flow/transport connection. When in the "Active/Deprecated" state, the address would only be used to maintain existing communication sessions. Addresses allocated in a previous DAR would be kept as "Active/Deprecated" in order to avoid their use for new communications/flows. However, in the case of DMI, one could be interested in using the permanent address anchored at the permanent HA, or the newly assigned address in the network where the MN resides. In other words, how could one bind a specific address to a specific socket? A mobility-aware API, as described by Section 6 of [I-D.patil-mext-dmm-approaches], could help making such decisions. In addition, more work may be needed to better define use-cases for dynamic mobility. For example, the benefits offered depend on how frequently the MN changes its anchor point, how long the sessions last, and also where the correspondent nodes are located.

By design, FAMA and DMI relies on the use of multiple anchored addresses. With DMI, the MN is always associated with a permanent HoA, and thus can always be reached by a CN that does not know the MN's current location. However, FAMA fails to specify whether the MN will be associated with a permanent address. In the absence of such, reachability of the MN from the CN is not guaranteed, so mechanisms should be specified for the CN to chose a valid destination address. The dynamic DNS update as specified by [RFC5026] cannot be used in this case. Beside, how HoAs would be assigned is not clearly defined by these solutions. Especially, how does it affect the HoA bootstrapping mechanism defined by [RFC5026]? Last but not least, how would the HoAs be recycled? They need to be released at some point and put back by the mobility anchor into the pool of available HoAs. As HMIPv6 and GHAHA always rely on a single permanent

address,
these solutions are not affected by these issues.

The idea of splitting location and routing management as exposed by DLMA or SAIL could improve GHAHA scalability by reducing the signaling overhead caused by the HA's synchronization. However, in the case of DMLA, care should be taken to avoid that the location anchor becomes a single point of failure.

In terms of required changes to the base Mobile IPv6 specifications and standardized extensions, all of the overviewed solutions mandate modifications on either the HA (GHAHA), or the MN (FAMA, DMI) or both (HMIPv6). In any case it is preferable to limit the changes to the minimum, especially on the mobile client side, as it is generally easier for a mobility operator to modify and maintain its infrastructure rather than the mobile nodes owned by its clients.

It is clear that there are several issues that must be kept in mind and tradeoffs that have to be made while designing an effective DMM solution. Some (not all) of them are:

(1) Ensuring reachability of the MN by the CN,

(2) Signaling overhead and binding latency,

(3) More vs less mobility agents,

(4) Distribution of mobility functions among these mobility agents,

(5) Assigning and recycling addresses to MNs,

(6) Required changes on the the current Mobile IPv6 specifications.

We have presented, what we hope would be the first steps to reinitiating discussion within the MEXT WG on DMM which in turn would lead to a robust and efficient DMM solution.

5. Acknowledgments

The authors would like to thank Philippe Bertin and Pierrick Seite for their comments.

6. Changes

Changes since version 00:

- o Moved the PMIP-based solutions to an appendix. This draft now focuses mainly on Mobile IPv6 based solutions,
- o Added the "Required changes" criterion in the conclusion table,
- o Considered 1 more solution in Appendix: [I-D.sjkoh-mext-pmip-dmc],
- o Various text updates to address comments from the ML.

7. Informative References

[I-D.bernardos-mext-dmm-cmip]
Bernardos, C. and F. Giust, "A IPv6 Distributed Client Mobility Management approach using existing mechanisms", draft-bernardos-mext-dmm-cmip-00 (work in progress), March 2011.

[I-D.chan-distributed-mobility-ps]
Chan, A., "Problem statement for distributed and dynamic mobility management", draft-chan-distributed-mobility-ps-03 (work in progress), July 2011.

[I-D.chan-netext-distributed-lma]
Chan, H., Xia, F., Xiang, J., and H. Ahmed, "Distributed Local Mobility Anchors", draft-chan-netext-distributed-lma-03 (work in progress), March 2010.

[I-D.ietf-mip6-hareliability]
Wakikawa, R., "Home Agent Reliability Protocol (HARP)", draft-ietf-mip6-hareliability-09 (work in progress), May 2011.

[I-D.kassi-mobileip-dmi]
Kassi-Lahlou, M., "Dynamic Mobile IP (DMI)", draft-kassi-mobileip-dmi-01 (work in progress), January 2003.

[I-D.laganier-mext-cga]
Laganier, J., "Authorizing Mobile IPv6 Binding Update
with
Cryptographically Generated Addresses", draft-laganier-mext-cga-01 (work in progress), October 2010.

[I-D.liu-distributed-mobility]
Liu, D., Cao, Z., Seite, P., and H. Chan, "Distributed mobility management", draft-liu-distributed-mobility-02 (work in progress), July 2010.

[I-D.liu-distributed-mobility-traffic-analysis]
Liu, D., Song, J., and W. Luo, "Distributed Mobility Management Traffic analysis", draft-liu-distributed-mobility-traffic-analysis-00 (work in progress), March 2011.

[I-D.liu-mext-distributed-mobile-ip]

Liu, D., "Distributed Deployment of Mobile IPv6", draft-liu-mext-distributed-mobile-ip-00 (work in progress), March 2011.

[I-D.ng-intarea-tunnel-loop]
Ng, C., Lim, B., and M. Jeyatharan, "Tunnel Loops and its Detection", draft-ng-intarea-tunnel-loop-00 (work in progress), October 2008.

[I-D.patil-mext-dmm-approaches]
Patil, B., Williams, C., and J. Korhonen, "Approaches to Distributed mobility management using Mobile IPv6 and its extensions", draft-patil-mext-dmm-approaches-01 (work in progress), July 2011.

[I-D.seite-netext-dma]
Seite, P. and P. Bertin, "Dynamic Mobility Anchoring", draft-seite-netext-dma-00 (work in progress), May 2010.

[I-D.sjkoh-mext-pmip-dmc]
Koh, S., Kim, J., Jung, H., and Y. Han, "Use of Proxy Mobile IPv6 for Distributed Mobility Control", draft-sjkoh-mext-pmip-dmc-03 (work in progress), June 2011.

[I-D.wakikawa-mext-global-haha-spec]
Wakikawa, R., Zhu, Z., and L. Zhang, "Global HA to HA Protocol Specification", draft-wakikawa-mext-global-haha-spec-01 (work in progress), July 2009.

[I-D.yokota-dmm-scenario]
Yokota, H., Seite, P., Demaria, E., and Z. Cao, "Use case scenarios for Distributed Mobility Management", draft-yokota-dmm-scenario-00 (work in progress), October 2010.

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

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

[SAIL] Zhu, Z., Wakikawa, R., and L. Zhang, "SAIL: A Scalable Approach for Wide-Area IP Mobility", INFOCOM 2011 MobiWorld Workshop, April 2011.

Appendix A. Other DMM solutions

A.1. Dynamic Local Mobility Anchors (DLMA)

The Dynamic Local Mobility Anchors (DLMA) scheme suggested in [I-D.chan-netext-distributed-lma] builds on the distributed architecture proposed by GHAHA while offsetting some of the disadvantages of GHAHA in requiring complete synchronization of all the HAs in a global set and the large amount of signaling traffic required for this complete synchronization. DLMA decouples the logical functionalities of a mobility anchor into:

(1) Allocation of HoA or HNPs to MNs,

(2) Location management which includes managing IP addresses and locations of MNs,

(3) Mobility routing which includes intercepting and forwarding packets.

DLMA then centralizes functionalities (1) and (2) in a Home Location Mobility Anchor (H-LMA) while distributing functionality (3) across several Visited Location Mobility Anchors (V-LMAs). The term Visited LMA here is used loosely, regardless of whether the MN has visited the subnet or not. All the LMAs advertise the same prefix using anycast routing. However it is required that the HoA or HNP assigned to an MN is unique to an H-LMA, i.e. it is possible to uniquely identify the H-LMA of an MN from its HoA.

An MN acquires a HoA (or HNP) from its H-LMA. When it moves out of the home subnet and anchors itself to a V-LMA, the V-LMA informs the H-LMA of the MN that it is the current anchoring point of the MN. The H-LMA then maintains this location information for the MN. When a CN anywhere in the Internet tries to send a packet to the MN, the packet is intercepted by the V-LMA closest to the CN via anycast routing. This V-LMA, called the O-LMA, tunnels the packet to the H-LMA of the MN which then tunnels the packet to the V-LMA where the MN is currently anchored. This V-LMA is called the D-LMA which then delivers the packet to the MN (Figure 5). Thus O-LMA and D-LMA for a flow are the V-LMAs that are closest to the CN and MN of that flow respectively. This is the route taken by a packet from the CN to the MN when there is no route optimization. When there is route optimization, the O-LMA caches location information about the MN from its H-LMA and thereafter directly tunnels the packet to its D-LMA. When an MN moves from D-LMA to another, an update must be sent to the previous D-LMA in addition to the H-LMA if route optimization is used, in case some O-LMA has cached information about the old D-LMA of the MN. The old D-LMA could then tunnel packets to the new D-LMA of the MN and also inform the O-LMA to update the location information in its cache. In the reverse direction, a packet sent by the MN is captured by its D-LMA and routed to the CN directly.

```
MN      D-LMA   H-LMA   O-LMA   CN
 |        |       |       |      |
 |        |       |       |      |
 |=======>|--------------------->| MN->CN
 |<=======|<======|<======|<-----| CN->MN without route optimization
 :        :       :       :      :
 |<=======|<==============|<-----| CN->MN with route optimization
 |        |       |       |      |
```

Figure 5: Packet routing to and from the MN. The LMA closest to the MN becomes the D-LMA and the LMA closest to the communication CN becomes the O-LMA. The H-LMA is the LMA that handles location information for the MN.

Every LMA acts as a H-LMA for a subset of MNs for which it assigns HoAs or HNPs and maintains location information. It also performs mobility routing for MNs not in this subset (i.e.) acts as a V-LMA for these MNs. The DLMA scheme works for both Mobile IPv6 and Proxy Mobile IPv6. The mobility functionalities can also be moved to the edge of the routers and packets may be tunneled directly to and from the mobile access gateways (MAGs) bypassing the V-LMAs.

A.2. Signal-driven and Signal-driven Distributed PMIP (S-PMIP/SD-PMIP)

The signal-driven PMIP (S-PMIP) and signal-driven distributed PMIP (SD-PMIP) [I-D.sjkoh-mext-pmip-dmc] are two distributed mobility control schemes based on the PMIP protocol.

S-PMIP (Figure 6) is a partially distributed scheme. The control plane is centralized at the LMA. Using Proxy Binding Query (PBQ) and Proxy Query Ack (PQA), a MAG can retrieve the Proxy-CoA of the MN at the LMA. Data from a CN can then be sent directly from MAG to MAG, bypassing the LMA.

```
   CN     MAG2    LMA    MAG1    MN
    |      |       |       |      |
    |      |       |+------|      | Binding registration with LMA
    |----->|       |       |      | CN sends data to MN via MAG2
    |      |------>|       |      | MAG2 sends PBQ to LMA
    |      |<------|       |      | LMA replies with PQA
    |------|==============>|----->| Data sent directly from MAG2 to
MAG1
    |      |       |       |      |
```

Figure 6: S-MIPv6 centralizes the control plane and distributes the data plane. Data from CN can bypass the LMA once the MAG that hosts the MN has been looked-up using PBQ/PQA messages.

SD-PMIP (Figure 7) is a fully distributed scheme. Proxy Binding Update is not performed by the MAG that hosts the MN. Instead, when a MAG has to forward data to a MN, it can get the Proxy-CoA of the MN by sending a PBQ using multicast to all of the MAG in the local domain. The MAG that acts on behalf of the MN replies with a PQA using unicast. Data from a CN can then be sent directly from MAG to MAG, bypassing the LMA.

```
   CN     MAG2    MAG3    MAG1    MN
    |      |       |       |      |
    |----->|       |       |      | CN sends data to MN via MAG2
    |      |-------+------+|      | MAG2 sends multicast PBQ to all
MAGs
    |      |<--------------|      | MAG1 replies with PQA
    |------|==============>|----->| Data sent directly from MAG2 to
MAG1
    |      |       |       |      |
```

Figure 7: SD-MIPv6 distributes both the control and data planes. Multicast PBQ are used to query all of the MAGs in the domain. Only the MAG that hosts the MN replies with a PQA.

A.3. Dynamic Mobility Anchoring (DMA)

Dynamic Mobility Anchoring (DMA) proposed in [I-D.seite-netext-dma] has similar approaches than FAMA and DMI but builds on Proxy Mobile IP (PMIP) in a flattened architecture where mobility functions are distributed among access routers. The access routers are mobility-enabled and provide traffic anchoring and location management functionalities to the MNs. These mobility-enabled access routers (MARs) allocate Home Network Prefixes (HNP) for MNs. When an MN is anchored at a MAR, it uses the HNP provided by that MAR and regular IPv6 routing applies for flows initiated at the MAR. When an MN moves to another MAR, it acquires a HNP from the new MAR and uses

this HNP for new flows. A routing tunnel must now be set up between the old MAR and new MAR if there are any ongoing flows during the IP handover.

The new MAR thus acts as a Home MAR (H-MAR) for flows using HNP allocated by itself and as a Visited MAR (V-MAR) for flows using HNP allocated by a previously visited MAR (Figure 8). As a result, any MAR can act as both an H-MAR and a V-MAR for flows belonging to the same MN. Even if the MN is moving across several MARs, the tunnel endpoints are always on the initial H-MAR (whose HNP is being used) and the current V-MAR.

```
   CN2    CN1    MAR1    MAR2    MN
    |      |       |       |      |
    |      |       |+------|      |  Binding registration with H-MAR
    |      |------>|======>|----->|  MAR1 acts as H-MAR and MAR2 acts
as
    |      |<------|<======|<-----|    V-MAR for flow between MN and
CN1
    |<---------------------|<-----|  MAR2 acts as H-MAR for flow
between
    |--------------------->|----->|   MN and CN2
    |      |       |       |      |
```

Figure 8: Packet routing when MN moves from MAR1 to MAR2 but has an ongoing flow with CN1 during the movement. After the movement MN initiates flow with CN2.

DMA's dynamic provision of flow based traffic indirection can also be applied to multiple interfaces and IP flow mobility. However, DMA suffers from some of the same issues as FAMA. It fails to specify whether the MN will be associated with a permanent address it can be reached with and in the absence of such, how a CN will lookup MN's address to initiate communication. DMA would need to specify how to maintain one address (or prefix) in a given MAR dedicated to anchor incoming communications, like it would be done in a centralized HA maintaining global Home Addresses. In addition, DMA also requires that each MAR advertises different per-MN prefixes set.

Authors' Addresses

Romain Kuntz
Toyota InfoTechnology Center USA, Inc.
465 Bernardo Ave
Mountain View, California 94045
USA

Phone: +1-650-694-4152
Fax: +1-650-694-4901
Email: rkuntz@us.toyota-itc.com

Divya Sudhakar
UCLA

Phone: +1-408-896-7526
Email: divyasudhakar@ucla.edu

Ryuji Wakikawa
Toyota InfoTechnology Center USA, Inc.
465 Bernardo Ave
Mountain View, California 94045
USA

Email: ryuji@us.toyota-itc.com

Lixia Zhang
UCLA
3713 Boelter Hall
Los Angeles, California 90095-1596
USA

Email: lixia@cs.ucla.edu