DMM H. Chan
Internet-Draft Huawei Technologies
Intended status: Informational J. Lee
Expires: September 24, 2015 Sangmyung University
S. Jeon
Instituto de Telecomunicacoes
March 23, 2015

Distributed Mobility Anchoring
draft-chan-dmm-distributed-mobility-anchoring-01

Abstract

This document defines the mobility management protocol solutions in the context of a distributed mobility management deployment. Such solutions consider the problem of assigning a mobility anchor and a gateway at the initiation of a session. In addition, the mid-session switching of the mobility anchor in a distributed mobility management environment is considered.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

A key requirement in distributed mobility management [RFC7333] is to enable traffic to avoid traversing single mobility anchor far from the optimal route. Recent developments in research and standardization with respect to future deployment models call for far more flexibility in network function operation and management. For example, the work on service function chaining at the IETF (SFC WG) has already identified a number of use cases for data centers. Although the work in SFC is not primarily concerned with mobile networks, the impact on IP-based mobile networks is not hard to see as by now most hosts connected to the Internet do so over a wireless medium. For instance, as a result of a dynamic re-organization of service chain a non-optimal route between mobile nodes may arise if one relies solely on centralized mobility management. This may also occur when the mobile node has moved such that both the mobile node and the correspondent node are far from the mobility anchor via which the traffic is routed.

Recall that distributed mobility management solutions do not make use of centrally deployed mobility anchor. As such, an application session SHOULD be able to have its traffic passing from one mobility anchor to another as the mobile node moves, or when changing operation and management (OAM) requirements call for mobility anchor switching, thus avoiding non-optimal routes. This draft proposes enhanced mobility anchoring.

2. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL","SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

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], the Proxy Mobile IPv6 specification [RFC5213], and the DMM current practices and gap analysis [RFC7429]. This includes terms such as mobile node (MN), correspondent node (CN), home agent (HA), home address (HoA), care-of-address (CoA), local mobility anchor (LMA), and mobile access gateway (MAG).

In addition, this document uses the following term:

Home network of an application session (or of an HoA): the network that has allocated the IP address (HoA) used for the session identifier by the application running in an MN. An MN may be running multiple application sessions, and each of these sessions can have a different home network.

Anchoring Function (AF): allocation to a mobile node of an IP address, i.e., Home Address (HoA), or prefix, i.e., Home Network Prefix (HNP) topologically anchored by the advertising node. That is, the anchor node is able to advertise a connected route into the routing infrastructure for the allocated IP prefixes. This is a basic function of a mobility anchor. With separation of control plane and data plane, this function may reside in a control plane anchor. Then the anchor function performs the IP prefix or address allocation and the route advertisement for an IP anchor in the data plane.

Session anchoring: A session or a flow is anchored to a node or nodes when the packets of the flow traverse at least one such nodes.

IP anchoring: An IP address or prefix is topologically anchored to a node by an anchor function. The IP packet will travel along a route which traverses that node. The packet will also traverse that node if the IP address does not change. Yet the IP address is changed at another node before it reaches that node, it will be redirected with the new IP address along a new route which may not traverse the original node.

Internetwork Location Management (LM) function: managing and keeping track of the internetwork location of an MN. The location information may be a binding of the IP advertised address/prefix, e.g., HoA or HNP, to the IP routing address of the MN or of a node that can forward packets destined to the MN. It is a control plane function.

In a client-server protocol model, location query and update messages may be exchanged between a Location Management client (LMc) and a Location Management server (LMs). With separation of control plane and data plane, this function may reside in a control plane anchor. It belongs to the session anchoring function.

Forwarding Management (FM) function: packet interception and forwarding to/from the IP address/prefix assigned 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.

This function belongs to session anchoring. With separation of control plane and data plane, FM may split into a FM part in the control plane (FM-CP) which may be a function in a control plane anchor or mobility controller and a FM part in the data plane (FM-DP) which may be the function of a data plane anchor.

Security Management (SM) function: The security management function controls security mechanisms/protocols providing access control, integrity, authentication, authorization, confidentiality, etc. for the control plane and data plane.

This function resides in all nodes such as control plane anchor, data plane anchor, and mobile node.

3. Anchor Initiation and Switching

When an IP prefix or address is topologically anchored to a node (data plane node), the anchor function will advertise connected route for it. Then an IP packet with this IP address as its destination address will be forwarded along a path that traverses through this IP anchoring node.

When a session or flow is anchored to a node (data plane node), the packets of the flow will traverse at least one such session anchoring node.

A session anchoring node may differ from an IP anchoring node for an IP address of the session.

3.1. IP anchoring in network of attachment

An IP prefix or address may be anchored to the access router to which the MN is attached.

For example, when an MN attaches to a network or moves to a new network, it is allocated an IP prefix from that network. It configures from this prefix an IP address which is typically a dynamic IP address. It then uses this IP address when it starts a new application session (an IP flow). Packets to the MN in this flow simply follows the forwarding table for as long as the MN stays in that network.

In this example, the flow may have terminated before the MN moves to a new network. Otherwise, the flow may close and then restart using a new IP address configured in the new network.

The security management function in the IP anchoring node at a new network must assign a valide IP prefix to a mobile node. In the example, the security management function in the node anchoring address IP2 assigns the valid IP prefix for the mobile node.

```
  Net1                                                     Net2
  +--------------+                                         +--------------+
  |node anchoring|                                         |node anchoring|
  | address IP1  |                                         | address IP2  |
  +--------------+                                         +--------------+
                                                           +--------------+
                                                           |MN(IP2)       |
                                                           |running       |
                                                           |session IP2   |
                                                           +--------------+
```

Figure 1. IP anchoring in network of attachment.

3.2. IP anchoring not in network of attachment

An IP prefix or address may be anchored to an access router in a different network to which the MN is attached. The anchor function is then in a network different from the network of attachment.

An example is in using a static IP address which does not belong to the network of attachment.

Another example when an MN moves to a new network is as follows. The MN has an ongoing session which was initialized in a prior network of attachment using an IP address belonging to the network where it was initialized as described in Section 3.1. When the session is unable to change its IP address it may continue to use its original IP address which is anchored not in the current network of attachment but in the network where the original IP address belongs. Mobility support is needed to enable the ongoing session to use this original IP address.

The security management function in the IP anchoring node at a new network must assign a valide IP prefix to a mobile node. The security management function must allow the mobile node to receive or send data packets with an IP address configured at a prior network of attachment of the mobile node.

```
  Net1                                                 Net2
  +--------------+                                     +--------------+
  |node anchoring|                                     |node anchoring|
  | address IP1  |                                     | address IP2  |
  +--------------+                                     +--------------+

                                                       +--------------+
                                                       |MN(IP2)       |
                                                       |running       |
                                                       |session IP1   |
                                                       +--------------+
```

Figure 2. IP anchoring not in network of attachment.

3.3. Keeping IP anchoring in mid-session

After the MN moves with an ongoing session to the new network (Net2), it obtains a new IP address or prefix from the new network (Net2). However, the ongoing session which was initialized in a prior network of attachment using an IP address belonging to the network where it was initialized as described in Section 3.1. IP mobility is needed to use the original IP address for the ongoing session continuity.

```
  Net1                                                 Net2
  +--------------+                                     +--------------+
  |node anchoring|                                     |node anchoring|
  | address IP1  |                                     | address IP2  |
  +--------------+                                     +--------------+

  +--------------+                                     +--------------+
  |MN(IP1) with  |                 move                |MN(IP1,IP2)   |
  |session over  |               =======>              |with session  |
  |IP1           |                                     |over IP1      |
  +--------------+                                     +--------------+
```

Figure 3. Keeping IP anchoring in mid-session.

3.4. Changing IP anchoring (with IP address change) in mid-session

With the MN in the example in Section 3.1 it may be desirable that the flow can change to the new IP address configured in the new network. The packets of this flow may then follow the forwarding table without requiring IP layer mobility support. Yet the flow may be using a higher layer mobility support which is not in the scope of this document to change the IP address of the flow.

The security management function in the IP anchoring node at a new network must assign a valide IP prefix to a mobile node.

```
  Net1                                                    Net2
  +--------------+                                      +--------------+
  |node anchoring|                                      |node anchoring|
  | address IP1  |                                      | address IP2  |
  +--------------+                                      +--------------+

  +--------------+                                      +--------------+
  |MN(IP1) with  |                 move                 |MN(IP2) with  |
  |session over  |               =======>               |session IP1   |
  |IP1           |                                      |changed to IP2|
  +--------------+                                      +--------------+
```

Figure 4. Changing IP anchoring.

3.5. Moving IP anchoring (without IP address change in mid-session

The IP anchoring may move without changing the IP address of the flow.

```
  Net1                                                    Net2
  +--------------+                                      +--------------+
  |node anchoring|                 move                 |node anchoring|
  | address IP1  |               =======>               | address IP1  |
  +--------------+                                      +--------------+

  +--------------+                                      +--------------+
  |MN(IP1)       |                 move                 |MN(IP2)       |
  |running       |               =======>               |running       |
  |session IP1   |                                      |session IP1   |
  +--------------+                                      +--------------+
```

Figure 5. Moving IP anchoring.

As an MN with an ongoing session moves to a new network, the session may preserve session continuity by moving the IP anchoring of its original IP address to the new network. Then the IP anchoring which was advertising the prefix in the original network will need to move to the new network. As the IP anchoring in the new network advertises the prefix of the session in the new network, the forwarding tables will be updated so that packets of the ongoing session will follow the updated forwarding tables.

3.6. Anchoring a session

As an MN with an ongoing session moves to a new network, the session may use the original IP address for session continuity by anchoring the session to some nodes (data plane nodes) and redirecting the packets of this session to traverse through these session anchoring nodes.

```
                             Net3
                             +--------------+
  Net1                       |node anchoring|           Net2
  +--------------+          /|address of CN |           +--------------+
  |     anchoring|         / +--------------+           |     anchoring|
  |   session    |        /                             |   session    |
  |  identified  |       /   +--------------+           |  identified  |
  |   with IP1   |      /    |      CN      |           |   with IP1   |
  |              |     /     +--------------+           |              |
  |session IP1   |    /                                 |session IP1   |
  |--> addr AR2  |   /                                  |--> MN        |
  |--------------|  /                                   |--------------|
  |node anchoring|<-                                    |AR2  anchoring|
  | address IP1  | ------------------------------------>| address IP2  |
  +--------------+                                      +--------------+

  +--------------+                                      +--------------+
  |MN(IP1)       |                 move                 |MN(IP2)       |
  |running       |               =======>               |running       |
  |session IP1   |                                      |session IP1   |
  +--------------+                                      +--------------+
```

Figure 6. Session anchoring.

For example, a first node to anchor the session may be at the IP anchoring of the original IP address in the original network. A second node to anchor the session may be in the new network. Then packets of this session traverse the session anchoring in both the original network and the new network. Forwarding management function at these nodes may be used to direct the flow to traverse them.

The session’s packets from the CN to the MN will then first be forwarded to the IP anchoring node in the original network where it is intercepted by the first session anchoring node. The session anchoring node may possess forwarding management function to forward the packets to the second session anchoring node in the new network.

In host-based mobility management, the session may be anchored in the new network to the MN itself.

In network-based mobility management, the session may be anchored to an access router to which the MN is attached in the new network. The access router may then forward the packet to the MN at L2.

The security management function in the IP anchoring node must ensure that the forwarding management function establishes a secure session anchoring with a relevant node. The security management function in the end communication nodes (i.e., mobile node and correspondent node) may be used to ensure a secure data plane between them.

3.7. Changing session anchoring in mid-session

The route of the packets of an ongoing session traversing the original network and the MN’s new network of attachment is not necessarily optimal. It can be unnecessarily long especially when the session anchoring nodes are far from each other even when the MN and CN are close to each other. A shorter route results when the session is anchored in both the CN’s network and the MN’s network. An example to achieve this is to move the session anchoring from the original network to the CN’s network.

For anchor switching of a session in mid-session, the relevant context with regard to MN should be delivered to CN’s anchor from the AR in Net 1, while the anchor switching should be notified to AR1 to receive packets directly forwarded by CN’s anchor. Existing IP mobility signaling messages such as Proxy Binding Update (PBU) and Proxy Binding Acknowledgment (PBA) can be used for the both communications with smaller option extensions as possible. When CN’s anchor receives packets from the CN, it encapsulates the packet with a tunnel header specified with IP address of CN’s anchor for outer source IP and AR2’s IP address for outer destination IP. For the transparent packet delivery operation in AR2 perspective, CN’s anchor needs to forward packets encapsulated with a tunnel header specified with AR1’s IP address for outer source IP and AR2’s IP address for outer destination IP.

The security management function in the IP anchoring node must ensure that the forwarding management function re-establishes a secure session anchoring with a relevant node during mid-session. The security management function in the end communication nodes may be used to ensure a secure data plane between them during mid-session.

```
                             Net3
                             +--------------+
                             |     anchoring|
                             |   session    |
                             |  identified  |
                             |   with IP1   |
                             |              |
                          ..>|session IP1   |
                         .   |--> addr AR2  |
                        .    |--------------|
  Net1                 .     |node anchoring|           Net2
  +--------------+    .      |address of CN |\          +--------------+
  |     anchoring|   .       +--------------+ \         |     anchoring|
  |   session    |  .                          \        |   session    |
  |  identified  | .         +--------------+   \       |  identified  |
  |   with IP1   |.          |      CN      |    \      |   with IP1   |
  |              |           +--------------+     \     |              |
  |session IP1   |                                 \    |session IP1   |
  |--> addr AR2  |                                  \   |--> MN L2 addr|
  |--------------|                                   \  |--------------|
  |node anchoring|                                    ->|AR2  anchoring|
  | address IP1  |                                      | address IP2  |
  +--------------+                                      +--------------+

  +--------------+                                      +--------------+
  |MN(IP1)       |                 move                 |MN(IP2)       |
  |running       |               =======>               |running       |
  |session IP1   |                                      |session IP1   |
  +--------------+                                      +--------------+
```

Figure 7. Changing session anchoring in mid-session.

4. Security Considerations

TBD

5. IANA Considerations

This document presents no IANA considerations.

6. References

6.1. Normative References

[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-17 (work in progress), June 2014.

[I-D.seite-dmm-dma]
Seite, P., Bertin, P., and J. Lee, "Distributed Mobility Anchoring", draft-seite-dmm-dma-07 (work in progress), February 2014.

[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.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

[RFC6241] Enns, R., Bjorklund, M., Schoenwaelder, J., and A. Bierman, "Network Configuration Protocol (NETCONF)", RFC 6241, June 2011.

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

[RFC7333] Chan, H., Liu, D., Seite, P., Yokota, H., and J. Korhonen, "Requirements for Distributed Mobility Management", RFC 7333, August 2014.

[RFC7429] Liu, D., Zuniga, JC., Seite, P., Chan, H., and CJ. Bernardos, "Distributed Mobility Management: Current Practices and Gap Analysis", RFC 7429, January 2015.

6.2. Informative References

[Paper-Distributed.Mobility.PMIP]
Chan, H., "Proxy Mobile IP with Distributed Mobility Anchors", Proceedings of GlobeCom Workshop on Seamless Wireless Mobility, December 2010.

[Paper-Distributed.Mobility.Review]

Chan, H., Yokota, H., Xie, J., Seite, P., and D. Liu, "Distributed and Dynamic Mobility Management in Mobile Internet: Current Approaches and Issues", February 2011.

Authors' Addresses

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

Email: h.a.chan@ieee.org

Jong-Hyouk Lee
Sangmyung University
708 Hannuri Building
Cheonan 330-720
Korea

Email: jonghyouk@smu.ac.kr

Seil Jeon
Instituto de Telecomunicacoes
Campus Universitario de Santiago
Aveiro 3810-193
Portugal

Email: seiljeon@av.it.pt