Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 6, 2012

D. Liu
H. Deng
China Mobile
W. Luo
ZTE

March 5, 2012

# DMM Dynamic Anchor Discussion
# draft-liu-dmm-dynamic-anchor-discussion-00

Abstract

Distributed mobility management aims to distribute the mobility anchor to the access network level to avoid the centralized mobility anchor problem. By distributing the mobility anchor, the traffic can be distributed in an optimal way. There are many different proposals for DMM solution, one of those types of solution is called "dynamic anchor". This document analyses the limitations of current dynamic anchor solution and discusses the possible solution to overcome those limitations.

## Requirements Language

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 RFC 2119 [RFC2119].

## Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 6, 2012.

## Copyright Notice

Table of Contents

## 1. Problem of dynamic anchor and potential solution

As draft [I-D.draft-seite-dmm-dma-00] introduced, the main idea of dynamic anchor is distributing the mobility anchor function in the access router (MAR). The newly initiated session is routed through the current MAR, only the original sessions that established before handover will be maintained at the previous anchor. As the following figure shows, flow1 is anchored to MAR1, flow2 is anchored to MAR2. Two different prefixes are assigned to the MN.

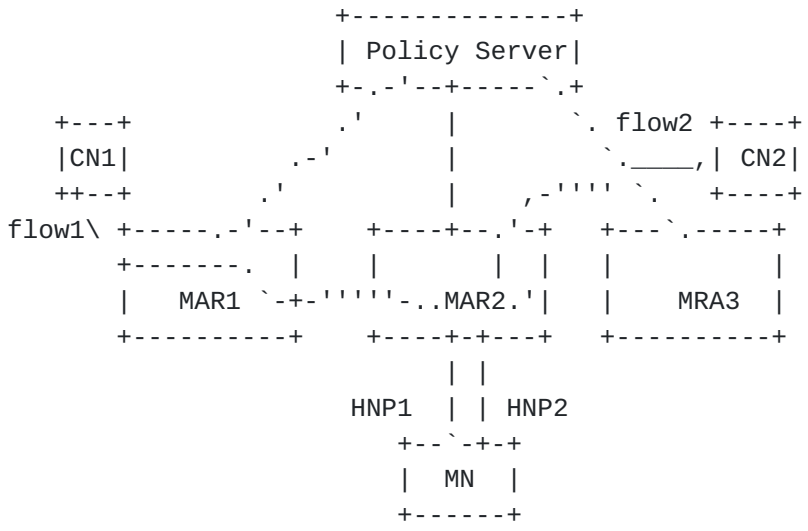


Figure 1 There are several potential problems for this solution

### 1.1. Active session managment

In this dynamic anchor solution, the MAR needs to know whether a prefix is active, if not, the MAR need to release the mobility binding. For instance, when the MN attach to MAR1, MAR1 detects the attachment of MN and allocate HNP1 to the MN. When the MN moves to MAR2, MAR2 needs to know that there is one on-going session in the MN and needs to trigger mobility binding update to MAR1 to update the binding.

The question is how MAR2 know that there is an active session for HNP1 in MN? The first approach is to use policy server to store the MN-ID and corresponding home network prefix that allocate to the MN. When MN moves to MAR2, as mentioned in [I-D.draft-seite-dmm-dma-00], MAR2 first check the policy server and find that MN is anchored to MAR1, then it can send binding update message to MAR1. But only that is not enough. MAR2/MAR1 has to have some mechanism to trigger the release HNP1, otherwise the MAR1 will always be occupied by the MN as one of its anchor point. This will lead system capacity waste. For example, after the on-going session is terminated, the MAR2 need to release the HNP1.

The question is that the policy server does not know when to release HNP1. One of possible solution is that MAR2 can inspect the traffic that has the source address prefix equals to HNP1. When MAR2 finds that there is no traffic sourced from HNP1 for a certain time, it can send deregistration binding update to MAR1 and release the binding state for HNP1. It seems that MAR2 needs a certain kind of timer to support the inspection for each sessions. If in this way, system capacity consumed by those timers can not be ignored since the traffic from hundreds of mobile nodes which are in a same MAR may have many thousands of sessions.

## 1.2. Soure address selection

MN may be configured with multiple addresses. For example, MN can have HNP1 and HNP2 at the same time. In this case, the MN's application need to select the correct source address. For example, there maybe a VoIP session running using HNP1 when MN attaches to MAR1. When MN moves to MAR2 , the VoIP session need to continue. When the user start a web browser, MAR2 will allocate a new perfix: HNP2. The VoIP software need to select HNP1 as the source address and the web browser need to select HNP2 as source address. RFC3484 specifies the source address selection rules for IPv6 but RFC3484 is not enough to cope with this situation since RFC3284 does not specify how to select source address for a particular application.

To solve this problem, the host may use the following rules for source address selection:

a. For any on-going session, keep to use the original address even there is a newly address been configured for the same interface.

b. For any new session, always choose to use the newly allocated address. The new MAR need to advertise the newly allocated prefix as the highest priority.

## 1.3. CN address selection

From the CN's perspective, the MN has multiple addresses, the CN needs to know which one it should use when it wants to initiate a session to MN.

## 1.4. IPv4 support

It will worse the IPv4 address depletion problem if use the dynamic anchor solution for IPv4 since each MN will need multiple IP addresses in that case.

### 1.5. Resource consumption consideration

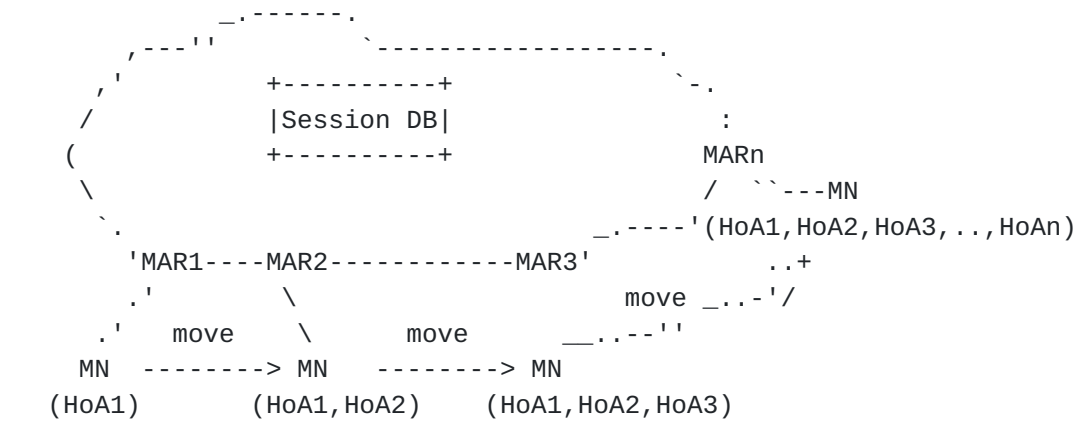


Figure2. Resource consumption

As illustrated in figure2, during the movement, mobile node gets more and more HoAs and more and more MARs will be occupied by this mobile node as its anchor points. The mobile node could maintain its HoAs by keep on sending packets at very low data rate for each sessions. In this way, capacity of the network will be consumed, e.g. many tunnels should be maintained among those MARs, many mobility contexts for this mobile node should be maintained among those MARs, and the operator will gain almost nothing from this mobile node. Additionally, the scenario described above provides a possibility for attackers to consume network resource maliciously.

## 2. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

## 3. Security Considerations

TBD

## 4. Acknowledgements

TBD

## 5. References

### 5.1. Normative References

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

### 5.2. Informative References

[I-D.draft-seite-dmm-dma-00] Seite , P. and P. Bertin, "Distributed Mobility Anchoring, draft-seite-dmm-dma-00", February 2012.

## Authors' Addresses

Dapeng Liu
China Mobile
32 Xuanwumen West Street
Beijng, Xicheng District, 100053
China

Phone: +86-13911788933
Email: liudapeng@chinamobile.com

Hui Deng
China Mobile
32 Xuanwumen West Street
Beijng, Xicheng District, 100053
China

Phone: +86-13911788933
Email: denghui@chinamobile.com

Wen Luo
ZTE
No.68, Zijinhua RD,Yuhuatai District
Nanjing, Jiangsu 210012
China

Email: luo.wen@zte.com.cn