Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 10, 2012

H. Chan (Ed.)
Huawei Technologies

June 8, 2012

Requirements of distributed mobility management
draft-chan-dmm-requirements-01

Abstract

The traditional hierarchical structure of cellular networks has led to deployment models which are heavily centralized. Mobility management with centralized mobility anchoring in existing hierarchical mobile networks is quite prone to suboptimal routing and issues related to scalability. Centralized functions present a single point of failure, and inevitably introduce longer delays and higher signaling loads for network operations related to mobility management. This document defines the requirements for distributed mobility management for IPv6 deployment. The objectives are to match the mobility deployment with the current trend in network evolution, to improve scalability, to avoid single point of failure, to enable transparency to upper layers only when needed, etc. The distributed mobility management also needs to be compatible with existing network deployments and end hosts, and be secured.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

In the past decade a fair number of mobility protocols have been standardized. Although the protocols differ in terms of functions and associated message format, we can identify a few key common features:

presence of a centralized mobility anchor providing global reachability and an always-on experience;

extensions to optimize handover performance while users roam across wireless cells;

extensions to enable the use of heterogeneous wireless interfaces for multi-mode terminals (e.g. cellular phones).

The presence of the centralized mobility anchor allows a mobile device to be reachable when it is not connected to its home domain. The anchor point, among other tasks, ensures reachability of forwarding of packets destined to or sent from the mobile device. Most of the deployed architectures today have a small number of centralized anchors managing the traffic of millions of mobile subscribers. Compared with a distributed approach, a centralized approach is likely to have several issues or limitations affecting performance and scalability, which require costly network dimensioning and engineering to resolve.

To optimize handovers from the perspective of mobile nodes, the base protocols have been extended to efficiently handle packet forwarding between the previous and new points of attachment. These extensions are necessary when applications impose stringent requirements in terms of delay. Notions of localization and distribution of local agents have been introduced to reduce signaling overhead. Unfortunately today we witness difficulties in getting such protocols deployed, often leading to sub-optimal choices.

Moreover, the availability of multi-mode devices and the possibility of using several network interfaces simultaneously have motivated the development of more new protocol extensions. Deployment is further complicated with so many extensions.

Mobile users are, more than ever, consuming Internet content; such traffic imposes new requirements on mobile core networks for data traffic delivery. When the traffic demand exceeds available capacity, service providers need to implement new strategies such as selective traffic offload (e.g. 3GPP work items LIPA/SIPTO) through alternative access networks (e.g. WLAN). Moreover, the localization of content providers closer to the Mobile/Fixed Internet Service

Providers network requires taking into account local Content Delivery Networks (CDNs) while providing mobility services.

When demand exceeds capacity, both offloading and CDN techniques could benefit from the development of mobile architectures with fewer levels of routing hierarchy introduced into the data path by the mobility management system. This trend in network flattening is reinforced by a shift in users traffic behavior, aimed at increasing direct communications among peers in the same geographical area. Distributed mobility management in a truly flat mobile architecture would anchor the traffic closer to the point of attachment of the user and overcome the suboptimal routing issues of a centralized mobility scheme.

While deploying [Paper-Locating.User] today’s mobile networks, service providers face new challenges. More often than not, mobile devices remain attached to the same point of attachment. Specific IP mobility management support is not required for applications that launch and complete while the mobile device is connected to the same point of attachment. However, the mobility support has been designed to be always on and to maintain the context for each mobile subscriber as long as they are connected to the network. This can result in a waste of resources and ever-increasing costs for the service provider. Infrequent mobility and intelligence of many applications suggest that mobility can be provided dynamically, thus simplifying the context maintained in the different nodes of the mobile network.

The proposed charter will address two complementary aspects of mobility management procedures: the distribution of mobility anchors to achieve a more flat design and the dynamic activation/deactivation of mobility protocol support as an enabler to distributed mobility management. The former has the goal of positioning mobility anchors (HA, LMA) closer to the user; ideally, these mobility agents could be collocated with the first hop router. The latter, facilitated by the distribution of mobility anchors, aims at identifying when mobility must be activated and identifying sessions that do not impose mobility management -- thus reducing the amount of state information to be maintained in the various mobility agents of the mobile network. The key idea is that dynamic mobility management relaxes some constraints while also repositioning mobility anchors; it avoids the establishment of non optimal tunnels between two topologically distant anchors.

Considering the above, the distributed mobility management working group is chartered with the following tasks:

Define the problem statement of distributed mobility management and identity the requirements for a distributed mobility management solution.

Document practices for the deployment of existing mobility protocols in a distributed mobility management environment.

Identify the limitations in the current practices with respect to providing the expected functionality.

If limitations are identified as part of the above deliverable, specify extensions to existing protocols that removes these limitations within a distributed mobility management environment.

This document describes the motivations of distributed mobility management and the proposed work in Section 1.1. Section 1.2 summarizes the problems with centralized IP mobility management compared with distributed and dynamic mobility management, which is elaborated in Section 4. The requirements to address these problems are given in Section 5. A companion document [I-D.yokota-dmm-scenario] discusses the use case scenarios.

Much of the problems explained in this document together with the contents in [I-D.yokota-dmm-scenario] have been merged and elaborated into the following review paper: [Paper-Distributed.Mobility.Review].

2. Conventions used in this document

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].

3. Centralized versus distributed mobility management

Mobility management functions may be implemented at different layers of the network protocol stack. At the IP (network) layer, they may reside in the network or in the mobile node. In particular, a network-based solution resides in the network only. It therefore enables mobility for existing hosts and network applications which are already in deployment but lack mobility support.

At the IP layer, a mobility management protocol to achieve session continuity is typically based on the principle of distinguishing between identifier and routing address and maintaining a mapping between them. With Mobile IP, the home address serves as an identifier of the device whereas the care-of-address takes the role of routing address, and the binding between them is maintained at the mobility anchor, i.e., the home agent. If packets can be continuously delivered to a mobile device at its home address, then all sessions using that home address can be preserved even though the routing or care-of address changes.

The next two subsections explain centralized and distributed mobility management functions in the network.

3.1. Centralized mobility management

With centralized mobility management, the mapping information between the stable node identifier and the changing IP address of a mobile node (MN) is kept at a centralized mobility anchor. Packets destined to an MN are routed via this anchor. In other words, such mobility management systems are centralized in both the control plane and the data plane.

Many existing mobility management deployments make use of centralized mobility anchoring in a hierarchical network architecture, as shown in Figure 1. Examples of such centralized mobility anchors are the home agent (HA) and local mobility anchor (LMA) in Mobile IPv6 [RFC6275] and Proxy Mobile IPv6 [RFC5213], respectively. Current mobile networks such as the Third Generation Partnership Project (3GPP) UMTS networks, CDMA networks, and 3GPP Evolved Packet System (EPS) networks also employ centralized mobility management, with Gateway GPRS Support Node (GGSN) and Serving GPRS Support Node (SGSN) in the 3GPP UMTS hierarchical network and with Packet data network Gateway (P-GW) and Serving Gateway (S-GW) in the 3GPP EPS network.

```
       UMTS                3GPP SAE              MIP/PMIP
     +------+              +------+              +------+
     | GGSN |              | P-GW |              |HA/LMA|
     +------+              +------+              +------+
        /\                    /\                    /\
       /  \                  /  \                  /  \
      /    \                /    \                /    \
     /      \              /      \              /      \
    /        \            /        \            /        \
+------+  +------+    +------+  +------+    +------+  +------+
| SGSN |  | SGSN |    | S-GW |  | S-GW |    |FA/MAG|  |FA/MAG|
+------+  +------+    +------+  +------+    +------+  +------+
```

Figure 1. Centralized mobility management.

3.2. Distributed mobility management

Mobility management functions may also be distributed to multiple locations in different networks as shown in Figure 2, so that a mobile node in any of these networks may be served by a closeby mobility function (MF).

```
+-------+  +-------+  +-------+  +-------+
|  MF   |  |  MF   |  |  MF   |  |  MF   |
+-------+  +-------+  +-------+  +-------+
                          |
                         ----
                        | MN |
                         ----
```

Figure 2. Distributed mobility management.

Mobility management may be partially distributed, i.e., only the data plane is distributed, or fully distributed where both the data plane and control plane are distributed. These different approaches are described in detail in [I-D.yokota-dmm-scenario].

[Paper-New.Perspective] discusses some initial steps towards a clear definition of what mobility management may be, to assist in better developing distributed architecture. [Paper-Characterization.Mobility.Management] analyses current mobility solutions and proposes an initial decoupling of mobility management into well-defined functional blocks, identifying their interactions, as well as a potential grouping, which later can assist in deriving more flexible mobility management architectures. According to the split functional blocks, this paper proposes three ways into which mobility management functional blocks can be groups, as an initial way to consider a better distribution: location and handover management, control and data plane, user and access perspective.

A distributed mobility management scheme is proposed in [Paper-Distributed.Dynamic.Mobility] for future flat IP architecture consisting of access nodes. The benefits of this design over centralized mobility management are also verified through simulations in [Paper-Distributed.Centralized.Mobility].

Before designing new mobility management protocols for a future flat IP architecture, one should first ask whether the existing mobility management protocols that have already been deployed for the hierarchical mobile networks can be extended to serve the flat IP architecture. MIPv4 has already been deployed in 3GPP2 networks, and PMIPv6 has already been adopted in WiMAX Forum and in 3GPP standards.

Using MIP or PMIP for both centralized and distributed architectures would ease the migration of the current mobile networks towards a flat architecture. It has therefore been proposed to adapt MIP or PMIPv6 to achieve distributed mobility management by using a distributed mobility anchor architecture.

In [Paper-Migrating.Home.Agents], the HA functionality is copied to many locations. The HoA of all MNs are anycast addresses, so that a packet destined to the HoA from any corresponding node (CN) from any network can be routed via the nearest copy of the HA. In addition, distributing the function of HA using a distributed hash table structure is proposed in [Paper-Distributed.Mobility.SAE]. A lookup query to the hash table will retrieve the location information of an MN is stored.

In [Paper-Distributed.Mobility.PMIP], only the mobility routing (MR) function is duplicated and distributed in many locations. The location information for any MN that has moved to a visited network is still centralized and kept at a location management (LM) function in the home network of the MN. The LM function at different networks constitutes a distributed database system of all the MNs that belong to any of these networks and have moved to a visited network. The location information is maintained in the form of a hierarchy: the LM at the home network, the CoA of the MR of the visited network, and then the CoA to reach the MN in the visited network. The LM in the home network keeps a binding of the HoA of the MN to the CoA of the MR of the visited network. The MR keeps the binding of the HoA of the MN to the CoA of the MN in the case of MIP, or the proxy-CoA of the Mobile Access Gateway (MAG) serving the MN in the case of PMIP.

[I-D.jikim-dmm-pmip] discusses two distributed mobility control schemes using the PMIP protocol: Signal-driven PMIP (S-PMIP) and Signal-driven Distributed PMIP (SD-PMIP). S-PMIP is a partially distributed scheme, in which the control plane (using a Proxy Binding Query to get the Proxy-CoA of the MN) is separate from the data plane, and the optimized data path is directly between the CN and the MN. SD-PMIP is a fully distributed scheme, in which the Proxy Binding Update is not performed, and instead each MAG will multicast a Proxy Binding Query message to all of the MAGs in its local PMIP domain to retrieve the Proxy-CoA of the MN.

4. Problem statement

This section identifies problems and limitations of centralized mobility approaches, and compares against possible distributed approaches. A few other related problems that may not be specific to the centralized approach are also described.

4.1. Non-optimal routes

PS1: Routing via a centralized anchor often results in a longer route, and the problem is especially manifested when accessing a local or cache server of a Content Delivery Network (CDN).

Figure 3 shows two cases of non-optimized routes.

```
         MIP/PMIP
         +------+
         |HA/LMA|
         +------+
           /\ \  \                   +---+
          /  \   \    \              |CDN|
         /    \     \      \         +---+
        /      \       \        \      |
       /        \         \          \ |
   +------+  +------+  +------+   +------+
   |FA/MAG|  |FA/MAG|  |FA/MAG|   |FA/MAG|
   +------+  +------+  +------+   +------+
                          |          |
                        ----       ----
                       | CN |     | MN |
                        ----       ----
```

Figure 3. Non-optimized route when communicating with a CN and when accessing a local or cache server of a CDN.

In the first case, the mobile node and the correspondent node are close to each other but are both far from the mobility anchor. Packets destined to the mobile node need to be routed via the mobility anchor, which is not on the shortest path. The second case involves a content delivery network (CDN). A user may obtain content from a server, such as when watching a video. As such usage becomes more popular, resulting in an increase in the core network traffic, service providers may relieve the core network traffic by placing these contents closer to the users in the access network in the form of cache or local CDN servers. Yet as the MN is getting content from a local or cache server of a CDN, even though the server is close to the MN, packets still need to go through the core network to route via the mobility anchor in the home network of the MN, if the MN uses the HoA as its identifier.

In a distributed mobility management design, one possibility is to have mobility anchors distributed in different access networks so that packets may be routed via a nearby mobility anchor function, as shown in Figure 4.

```
                                        +---+
                                        |CDN|
                                        +---+
                                          |
                                          |
   +------+  +------+  +------+   +------+
   |  MF  |  |  MF  |  |  MF  |   |  MF  |
   +------+  +------+  +------+   +------+
                           |          |
                         ----       ----
                        | CN |     | MN |
                         ----       ----
```

Figure 4. Mobile node in any network is served by a close by mobility function.

Due to the above limitation, with the centralized mobility anchor design, route optimization extensions to mobility protocols are therefore needed. Whereas the location privacy of each MN may be compromised when the CoA of an MN is given to the CN, those mobility protocol deployments that lack such optimization extensions will encounter non-optimal routes, which affect the performance.

In contrast, route optimization may be naturally an integral part of a distributed mobility management design. With the help of such intrinsic route optimization, the data transmission delay will be reduced, by which the data transmission throughputs can be enhanced. Furthermore, the data traffic overhead at the mobility agents such as the HA and the LMA in the core network can be alleviated significantly.

4.2. Non-optimality in Evolved Network Architecture

PS2: The centralized mobility management can become non-optimal as a network architecture evolves and becomes more flattened.

Centralized mobility management is currently deployed to support the existing hierarchical mobile data networks. It leverages on the hierarchical architecture. However, the volume of wireless data traffic continues to increase exponentially. The data traffic increase would require costly capacity upgrade of centralized architectures. It is thus predictable that the data traffic increase will soon overload the centralized data anchor point, e.g., the P-GW in 3GPP EPS. In order to address this issue, a trend in the evolution of mobile networks is to distribute network functions close to access networks. These network functions can be the content servers in a CDN, and also the data anchor point.

Mobile networks have been evolving from a hierarchical architecture to a more flattened architecture. In the 3GPP standards, the GPRS network has the hierarchy GGSN "C SGSN "C RNC "C NB (Node B). In 3GPP EPS networks, the hierarchy is reduced to P-GW "C S-GW "C eNB (Evolved NB). In some deployments, the P-GW and the S-GW are collocated to further reduce the hierarchy. Reducing the hierarchy this way reduces the number of different physical network elements in the network, contributing to easier system maintenance and lower cost. As mobile networks become more flattened, the centralized mobility management can become non-optimal. Mobility management deployment with distributed architecture is then needed to support the more flattened network and the CDN networks.

4.3. Low scalability of centralized route and mobility context maintenance

PS3: Setting up such special routes and maintaining the mobility context for each MN is more difficult to scale in a centralized design with a large number of MNs. Distributing the route maintenance function and the mobility context maintenance function among different networks can be more scalable.

Special routes are set up to enable session continuity when a handover occurs. Packets sent from the CN need to be tunneled between the HA and FA in MIP and between the LMA and MAG in PMIP. However, these network elements at the ends of the tunnel are also routers performing the regular routing tasks for ordinary packets not involving a mobile node. These ordinary packets need to be directly routed according to the routing table in the routers without tunneling. Therefore, the network must be able to distinguish those packets requiring tunneling from the regular packets. For each packet that requires tunneling owing to mobility, the network will encapsulate it with a proper outer IP header with the proper source and destination IP addresses. The network therefore needs to maintain and manage the mobility context of each MN, which is the relevant information needed to characterize the mobility situation of that MN to allow the network to distinguish their packets from other packets and to perform the required tunneling.

Setting up such special routes and maintaining the mobility context for each MN is more difficult to scale in a centralized design with a large number of MNs. Distributing the route maintenance function and the mobility context maintenance function among different networks can be more scalable.

4.4. Single point of failure and attack

PS4: Centralized anchoring may be more vulnerable to single point of failure and attack than a distributed system.

A centralized anchoring architecture is generally more vulnerable to a single point of failure or attack, requiring duplication and backups of the support functions.

On the other hand, a distributed mobility management architecture has intrinsically mitigated the problem to a local network which is then of a smaller scope. In addition, the availability of such functions in neighboring networks has already provided the needed architecture to support protection.

4.5. Wasting resources to support mobile nodes not needing mobility support

PS5: IP mobility support is not always required. For example, some applications do not need a stable IP address during handover, i.e., IP session continuity. Sometimes, the entire application session runs while the terminal does not change the point of attachment. In these situations that do not require IP mobility support, network resources are wasted when mobility context is set up.

The problem of centralized route and mobility context maintenance is aggravated when the via routes are set up for many more MNs that are not requiring IP mobility support. On the one hand, the network needs to provide mobility support for the increasing number of mobile devices because the existing mobility management has been designed to always provide such support as long as a mobile device is attached to the network. On the other hand, many nomadic users are connected to a network in an office or meeting room. Such users will not move for the entire network session. It has been measured that over two-thirds of a user mobility is local [Paper-Locating.User]. In addition, it is possible to have the intelligence for applications to manage mobility without needing help from the network. Network resources are therefore wasted to provide mobility support for the devices that do not really need it at the moment.

It is necessary to dynamically set up the via routes only for MNs that actually undergo handovers and lack higher-layer mobility support. With distributed mobility anchors, such dynamic mobility management mechanism may then also be distributed. Therefore, dynamic mobility and distributed mobility may complement each other and may be integrated.

4.6. Other related problems

Other related problems that may not be specifically owing to a centralized architecture but are desirable to solve are described in this subsection.

4.6.1. Mobility signaling overhead with peer-to-peer communication

O-PS1: Wasting resources when mobility signaling (e.g., maintenance of the tunnel, keep alive, etc.) is not turned off for peer-to-peer communication.

In peer-to-peer communications, end users communicate by sending packets directly addressed to each other’s IP address. However, they need to find each other’s IP address first through signaling in the network. While different schemes for this purpose may be used, MIP already has a mechanism to locate an MN and may be used in this way. In particular, MIPv6 Route Optimization (RO) mode enables a more efficient data packets exchange than the bidirectional tunneling (BT) mode, as shown in Figure 5.

```
      MIP/PMIP
      +------+
      |HA/LMA|
      +------+
        /\ \  \
       /  \   \    \
      /    \     \      \
     /      \       \        \
    /        \         \          \
+------+  +------+  +------+   +------+
|FA/MAG|  |FA/MAG|  |FA/MAG|   |FA/MAG|
+------+  +------+  +------+   +------+
                       |          |
                     ----       ----
                    | MN |<--->| CN |
                     ----       ----
```

Figure 5. Non-optimized route when communicating with CN and when accessing local content.

This RO mode is expected to be used whenever possible unless the MN is not interested in disclosing its topological location, i.e., the CoA, to the CN (e.g., for privacy reasons) or some other network constraints are put in place. However, MIPv6 RO mode requires exchanging a significant amount of signaling messages in order to establish and periodically refresh a bidirectional security association (BSA) between an MN and its CN. While the mobility signaling exchange impacts the overall handover latency, the BSA is needed to authenticate the binding update and acknowledgment messages (note that the latter is not mandatory). In addition, the amount of mobility signaling messages increases further when both endpoints are mobile.

A dynamic mobility management capability that turns off these signaling when they are not needed will enable the RO mode between two mobile endpoints at minimum or no cost. It will also reduce the handover latency owing to the removal of the extra signaling. These benefits for peer-to-peer communications will encourage the adoption and large-scale deployment of dynamic mobility management.

4.6.2. Complicated deployment with too many variants and extensions of MIP

O-PS2: Deployment is complicated with many variants and extensions of MIP. When introducing new functions which may add to the complicity, existing solutions are more vulnerable to break.

Mobile IP, which has primarily been deployed in a centralized manner for the hierarchical mobile networks, already has numerous variants and extensions including PMIP, Fast MIP (FMIP) [RFC4068] [RFC4988] , Proxy-based FMIP (PFMIP) [RFC5949] , hierarchical MIP (HMIP) [RFC5380] , Dual-Stack Mobile IP (DSMIP) [RFC5454] [RFC5555] and there may be more to come. These different modifications or extensions of MIP have been developed over the years owing to the different needs that are found afterwards. Deployment can then become complicated, especially when interoperability with different deployments is an issue.

A desirable feature of mobility management is to be able to work with network architectures of both hierarchical networks and flattened networks, so that the mobility management protocol possesses enough flexibility to support different networks. In addition, one goal of dynamic mobility management is the capability to selectively turn on and off mobility support and certain mobility signaling. Such flexibility in the design is compatible with the goal to integrate different mobility variants as options. Some additional extensions to the base protocols may then be needed to improve the integration while avoiding existing functions to break.

5. Requirements

After reviewing the problems and limitations of centralized deployment in Section 4, this section states the requirements as follows:

5.1. Distributed deployment

REQ1: Distributed deployment

IP mobility, network access and routing solutions provided by DMM SHALL enable a distributed deployment of mobility management of IP sessions so that the traffic can be routed in an optimal manner without traversing centrally deployed mobility anchors.

Motivation: The motivations of this requirement are to match mobility deployment with current trend in network evolution: more cost and resource effective to cache and distribute contents when combining distributed anchors with caching systems (e.g., CDN); improve scalability; avoid single point of failure; mitigate threats being focused on a centrally deployed anchor, e.g., home agent and local mobility anchor.

This requirement addresses the problems PS1, PS2, PS3, and PS4 explained in Section 4 above.

5.2. Transparency to Upper Layers when needed

REQ2: Transparency to Upper Layers when needed

The DMM solutions SHALL provide transparency above the IP layer when needed. Such transparency is needed, when the mobile hosts or entire mobile networks change their point of attachment to the Internet, for the application flows that cannot cope with a change of IP address. Otherwise the support to maintain a stable home IP address or prefix during handover may be declined.

Motivation: The motivation of this requirement is to enable more efficient use of network resources and more efficient routing by not maintaining a stable IP home IP address when there is no such need.

This requirement addresses the problems PS5 as well as the other related problem O-PS1 which are explained in Section 4 above.

5.3. IPv6 deployment

REQ3: IPv6 deployment

The DMM solutions SHOULD target IPv6 as primary deployment and SHOULD NOT be tailored specifically to support IPv4, in particular in situations where private IPv4 addresses and/or NATs are used.

Motivation: The motivation for this requirement is to be inline with the general orientation of IETF. Moreover, DMM deployment is foreseen in mid-term/long-term, hopefully in an IPv6 world. It is also unnecessarily complex to solve this problem for IPv4, as we will not be able to use some of the IPv6-specific features/tools.

5.4. Compatibility

REQ4: Compatibility

The DMM solution SHOULD be able to work between trusted administrative domains when allowed by the security measures deployed between these domains. Furthermore, the DMM solution SHOULD preserve backwards compatibility with existing network deployment and end hosts. For example, depending on the environment in which dmm is deployed, the dmm solutions may need to be compatible with other existing mobility protocols that are deployed in that environment or may need to be interoperable with the network or the mobile hosts/routers that do not support the dmm enabling protocol.

Motivation: The motivation of this requirement is to allow inter-domain operation if desired and to preserve backwards compatibility so that the existing networks and hosts are not affected and do not break.

5.5. Existing mobility protocols

REQ5: Existing mobility protocols

A DMM solution SHOULD first consider reusing and extending the existing mobility protocols before specifying new protocols.

Motivation: The purpose is to reuse the existing protocols first before considering new protocols.

5.6. Security considerations

REQ6: Security considerations

The protocol solutions for DMM SHALL consider security, for example authentication and authorization mechanisms that allow a legitimate mobile host/router to access to the DMM service, protection of signaling messages of the protocol solutions in terms of authentication, data integrity, and data confidentiality, opti-in or opt-out data confidentiality to signaling messages depending on network environments or user requirements.

Motivation and problem statement: Mutual authentication and authorization between a mobile host/router and an access router providing the DMM service to the mobile host/router are required to prevent potential attacks in the access network of the DMM service. Otherwise, various attacks such as impersonation, denial of service, man-in-the-middle attacks, etc. are present to obtain illegitimate access or to collapse the DMM service.

Signaling messages are subject to various attacks since these messages carry context of a mobile host/router. For instance, a malicious node can forge and send a number of signaling messages to redirect traffic to a specific node. Consequently, the specific node is under a denial of service attack, whereas other nodes are not receiving their traffic. As signaling messages travel over the Internet, the end-to-end security is required.

6. Security Considerations

Distributed mobility management (DMM) requires two kinds of security considerations: 1) access network security that only allows a legitimate mobile host/router to access the DMM service; 2) end-to-end security that protects signaling messages for the DMM service. Access network security is required between the mobile host/router and the access network providing the DMM service. End-to-end security is required between nodes that participate in the DMM protocol.

It is necessary to provide sufficient defense against possible security attacks, or to adopt existing security mechanisms and protocols to provide sufficient security protections. For instance, EAP based authentication can be used for access network security, while IPsec can be used for end-to-end security.

7. IANA Considerations

None

8. Co-authors and Contributors

This problem statement document is a joint effort among the following participants. Each individual has made significant contributions to this work.

Dapeng Liu: liudapeng@chinamobile.com

Pierrick Seite: pierrick.seite@orange-ftgroup.com

Hidetoshi Yokota: yokota@kddilabs.jp

Charles E. Perkins: charliep@computer.org

Melia Telemaco: telemaco.melia@alcatel-lucent.com

Elena Demaria: elena.demaria@telecomitalia.it

Peter McCann: Peter.McCann@huawei.com

Wassim Michel Haddad: Wassam.Haddad@ericsson.com

Hui Deng: denghui@chinamobile.com

Tricci So: tso@zteusa.com

Jong-Hyouk Lee: jh.lee@telecom-bretagne.eu

Seok Joo Koh: sjkoh@knu.ac.kr

9. References

9.1. Normative References

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

9.2. Informative References

[I-D.ietf-netext-pd-pmip]
Zhou, X., Korhonen, J., Williams, C., Gundavelli, S., and C. Bernardos, "Prefix Delegation for Proxy Mobile IPv6",

draft-ietf-netext-pd-pmip-02 (work in progress), March 2012.

[I-D.jikim-dmm-pmip]
Kim, J., Koh, S., Jung, H., and Y. Han, "Use of Proxy Mobile IPv6 for Distributed Mobility Control", draft-jikim-dmm-pmip-00 (work in progress), March 2012.

[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.

[Paper-Distributed.Centralized.Mobility]
Bertin, P., Bonjour, S., and J-M. Bonnin, "A Distributed or Centralized Mobility", Proceedings of Global Communications Conference (GlobeCom), December 2009.

[Paper-Distributed.Dynamic.Mobility]
Bertin, P., Bonjour, S., and J-M. Bonnin, "A Distributed Dynamic Mobility Management Scheme Designed for Flat IP Architectures", Proceedings of 3rd International Conference on New Technologies, Mobility and Security (NTMS), 2008.

[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, Journal of Communications, vol. 6, no. 1, pp. 4-15, Feb 2011.", Proceedings of GlobeCom Workshop on Seamless Wireless Mobility, February 2011.

[Paper-Distributed.Mobility.SAE]
Fisher, M., Anderson, F., Kopsel, A., Schafer, G., and M. Schlager, "A Distributed IP Mobility Approach for 3G SAE", Proceedings of the 19th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2008.

[Paper-Locating.User]
Kirby, G., "Locating the User", Communication

International, 1995.

[Paper-Migrating.Home.Agents]
Wakikawa, R., Valadon, G., and J. Murai, "Migrating Home Agents Towards Internet-scale Mobility Deployments", Proceedings of the ACM 2nd CoNEXT Conference on Future Networking Technologies, December 2006.

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

[RFC4068] Koodli, R., "Fast Handovers for Mobile IPv6", RFC 4068, July 2005.

[RFC4988] Koodli, R. and C. Perkins, "Mobile IPv4 Fast Handovers", RFC 4988, October 2007.

[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.

[RFC5454] Tsirtsis, G., Park, V., and H. Soliman, "Dual-Stack Mobile IPv4", RFC 5454, March 2009.

[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.

[RFC5949] Yokota, H., Chowdhury, K., Koodli, R., Patil, B., and F. Xia, "Fast Handovers for Proxy Mobile IPv6", RFC 5949, September 2010.

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

Author’s Address

H Anthony Chan (editor)
Huawei Technologies
5340 Legacy Dr. Building 3, Plano, TX 75024, USA
Email: h.a.chan@ieee.org

-
Dapeng Liu
China Mobile
Unit2, 28 Xuanwumenxi Ave, Xuanwu District, Beijing 100053, China
Email: liudapeng@chinamobile.com
-
Pierrick Seite
France Telecom - Orange
4, rue du Clos Courtel, BP 91226, Cesson-Sevigne 35512, France
Email: pierrick.seite@orange-ftgroup.com
-
Hidetoshi Yokota
KDDI Lab
2-1-15 Ohara, Fujimino, Saitama, 356-8502 Japan
Email: yokota@kddilabs.jp
-
Charles E. Perkins
Huawei Technologies
Email: charliep@computer.org
-
Jouni Korhonen
Nokia Siemens Networks
Email: jouni.korhonen@nsn.com
-
Melia Telemaco
Alcatel-Lucent Bell Labs
Email: telemaco.melia@alcatel-lucent.com
-
Elena Demaria
Telecom Italia
via G. Reiss Romoli, 274, TORINO, 10148, Italy
Email: elena.demaria@telecomitalia.it
-
Jong-Hyouk Lee
RSM Department, Telecom Bretagne
Cesson-Sevigne, 35512, France
Email: jh.lee@telecom-bretagne.eu
-
Tricci So
ZTE
Email: tso@zteusa.com
-
Carlos J. Bernardos
Universidad Carlos III de Madrid
Av. Universidad, 30, Leganes, Madrid 28911, Spain
Email: cjbc@it.uc3m.es
-
Peter McCann

Huawei Technologies
Email: PeterMcCann@huawei.com
-
Seok Joo Koh
Kyungpook National University, Korea
Email: sjkoh@knu.ac.kr
-
Wen Luo
ZTE
No.68, Zijinhua RD,Yuhuatai District, Nanjing, Jiangsu 210012, China
Email: luo.wen@zte.com.cn
-