Network Working Group   H. Chan (Ed.)
Internet-Draft   Huawei Technologies (more
Intended status: Informational   co-authors on P. 17)
Expires: November 9, 2013   D. Liu
                                                        China Mobile
                                                           P. Seite
                                              France Telecom - Orange
                                                          H. Yokota
                                                           KDDI Lab
                                                        J. Korhonen
                                             Nokia Siemens Networks
                                                        May 8, 2013

                Requirements for Distributed Mobility Management
                      draft-ietf-dmm-requirements-04

Abstract

   This document defines the requirements for Distributed Mobility
   Management (DMM) in IPv6 deployments. The hierarchical structure in
   traditional wireless networks has led to deployment models which are
   in practice centralized. Mobility management with logically
   centralized mobility anchoring in current mobile networks is prone to
   suboptimal routing and raises scalability issues. Such centralized
   functions can lead to single points of failure and inevitably
   introduce longer delays and higher signaling loads for network
   operations related to mobility management. The objective is to
   enhance mobility management in order to meet the primary goals in
   network evolution, i.e., improve scalability, avoid single points of
   failure, enable transparent mobility support to upper layers only
   when needed, and so on. Distributed mobility management must be
   secure and may co-exist with existing network deployments and end
   hosts.

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].

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 November 9, 2013.

Copyright Notice

Table of Contents

1. Introduction

   In the past decade a fair number of mobility protocols have been
   standardized [RFC6275] [RFC5944] [RFC5380] [RFC6301] [RFC5213].
   Although the protocols differ in terms of functions and associated
   message formats, we can identify a few key common features:

   o a centralized mobility anchor providing global reachability and an
      always-on experience to the user;

   o extensions to the base protocols to optimize handover performance
      while users roam across wireless cells; and

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

   The presence of the centralized mobility anchor allows a mobile node
   to remain reachable after it has moved to a different network. The
   anchor point, among other tasks, ensures connectivity by forwarding
   packets destined to, or sent from, the mobile node. In practice,
   most of the deployed architectures today have a small number of
   centralized anchors managing the traffic of millions of mobile nodes.
   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 have stringent requirements in terms
   of delay. Notions of localization and distribution of local agents
   have been introduced to reduce signaling overhead [Paper-
   Distributed.Centralized.Mobility]. Unfortunately, today we witness
   difficulties in getting such protocols deployed, resulting in sub-
   optimal choices for the network operators.

   Moreover, the availability of multiple-interface host and the
   possibility of using several network interfaces simultaneously have
   motivated the development of even more protocol extensions to add
   more capabilities to the mobility management protocol. In the end,
   deployment is further complicated with the multitude of extensions.

   As an effective transport method for multimedia data delivery, IP
   multicast support, including optimizations, have been introduced but
   by "patching-up" procedure after completing the design of reference
   mobility protocol, leading to network inefficiency and non-optimal
   routing.

Mobile users are, more than ever, consuming Internet content; such traffic imposes new requirements on mobile core networks for data traffic delivery. The presence of content providers closer to Internet Service Providers (ISP) network requires taking into account local Content Delivery Networks (CDNs) while providing mobility services. Moreover, 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 [TS.23.401]) through alternative access networks (e.g. WLAN) [Paper-Mobile.Data.Offloading]. A gateway selection mechanism also takes the user proximity into account within EPC [TS.29303]. These mechanisms were not pursued in the past owing to charging and billing reasons. Assigning a gateway anchor node from a visited network in roaming scenario has until recently been done and are limited to voice services only. Charging and billing require solutions beyond the mobility protocol.

Both traffic offloading and CDN mechanisms 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 towards so-called "flat networks" is reinforced by a shift in user traffic behavior. In particular, there are 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.

Today's mobile networks present service providers with new challenges. Mobility patterns indicate that mobile nodes remain attached to the same point of attachment for considerable periods of time [Paper-Locating.User]. Specific IP mobility management support is not required for applications that launch and complete their sessions while the mobile node is connected to the same point of attachment. However, currently, IP mobility support is designed for always-on operation, maintaining all parameters of the context for each mobile subscriber for as long as they are connected to the network. This can result in a waste of resources and unnecessary costs for the service provider. Infrequent node mobility coupled with application intelligence suggest that mobility support could be provided selectively, thus reducing the amount of context maintained in the network.

The distributed mobility managemetn (DMM) charter addresses two complementary aspects of mobility management procedures: the distribution of mobility anchors towards a more flat network and the dynamic activation/deactivation of mobility protocol support as an enabler to distributed mobility management. The former aims at positioning mobility anchors (e.g., HA, LMA) closer to the user;

ideally, mobility agents could be collocated with the first-hop
router. The latter, facilitated by the distribution of mobility
anchors, aims at identifying when mobility support must be activated
and identifying sessions that do not require mobility management
support -- thus reducing the amount of state information that must be
maintained in various mobility agents of the mobile network. The key
idea is that dynamic mobility management relaxes some of the
constraints of previously-standardized mobility management solutions
and, by doing so, it can avoid the unnecessary establishment of
mechanisms to forward traffic from an old to a new mobility anchor.

This document compares distributed mobility management with
centralized mobility management in Section 3. The problems that can
be addressed with DMM are summarized in Section 4. The requirements
to address various problems are given in Section 5. Finally,
security considerations are discussed in Section 6.

The problem statement and the use cases [I-D.yokota-dmm-scenario] can
be found in [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].

2.1. Terminology

All the general mobility-related terms and their acronyms used in
this document are to be interpreted as defined in the Mobile IPv6
base specification [RFC6275], in the Proxy mobile IPv6 specification
[RFC5213], and in Mobility Related Terminology [RFC3753]. These
terms include the following: mobile node (MN), correspondent node
(CN), and home agent (HA) as per [RFC6275]; local mobility anchor
(LMA) and mobile access gateway (MAG) as per [RFC5213], and context
as per [RFC3753].

In addition, this draft introduces the following term.

Mobility context

   is the collection of information required to provide mobility
   management support for a given mobile node.

3. Centralized versus distributed mobility management

   Mobility management functions may be implemented at different layers
   of the 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 supporting session
   continuity is typically based on the principle of distinguishing
   between identifier and routing address and maintaining a mapping
   between the two. In Mobile IP, the home address serves as an
   identifier of the device whereas the care-of-address (CoA) takes the
   role of the routing address. The binding between these two is
   maintained at the home agent (mobility anchor). If packets can be
   continuously delivered to a mobile node at its home address, then all
   sessions using that home address are unaffected even though the
   routing address (CoA) changes.

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

3.1. Centralized mobility management

   In centralized mobility management, the mapping information between
   the persistent node identifier and the locator IP address of a mobile
   node (MN) is kept at a single mobility anchor. At the same time,
   packets destined to the 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
   cellular networks such as the Third Generation Partnership Project
   (3GPP) GPRS networks, CDMA networks, and 3GPP Evolved Packet System
   (EPS) networks employ centralized mobility management too. In
   particular, the Gateway GPRS Support Node (GGSN), Serving GPRS
   Support Node (SGSN) and Radio Network Controller (RNC) in the 3GPP
   GPRS hierarchical network, and the Packet Data Network Gateway (P-GW)
   and Serving Gateway (S-GW) in the 3GPP EPS network, respectively, act
   as anchors in a hierarchy.

```
        3G GPRS                    3GPP EPS                   MIP/PMIP
        +------+                   +------+                   +------+
        | GGSN |                   | P-GW |                   |HA/LMA|
        +------+                   +------+                   +------+
          /\                         /\                         /\
         /  \                       /  \                       /  \
        /    \                     /    \                     /    \
       /      \                   /      \                   /      \
      /        \                 /        \                 /        \
     /          \               /          \               /          \
   +------+    +------+    +------+    +------+   +------+        +------+
   | SGSN |    | SGSN |    | S-GW |    | S-GW |   |MN/MAG|        |MN/MAG|
   +------+    +------+    +------+    +------+   +------+        +------+
     /\           /\
    /  \         /  \
   /    \       /    \
  +---+ +---+ +---+ +---+
  |RNC| |RNC| |RNC| |RNC|
  +---+ +---+ +---+ +---+
```
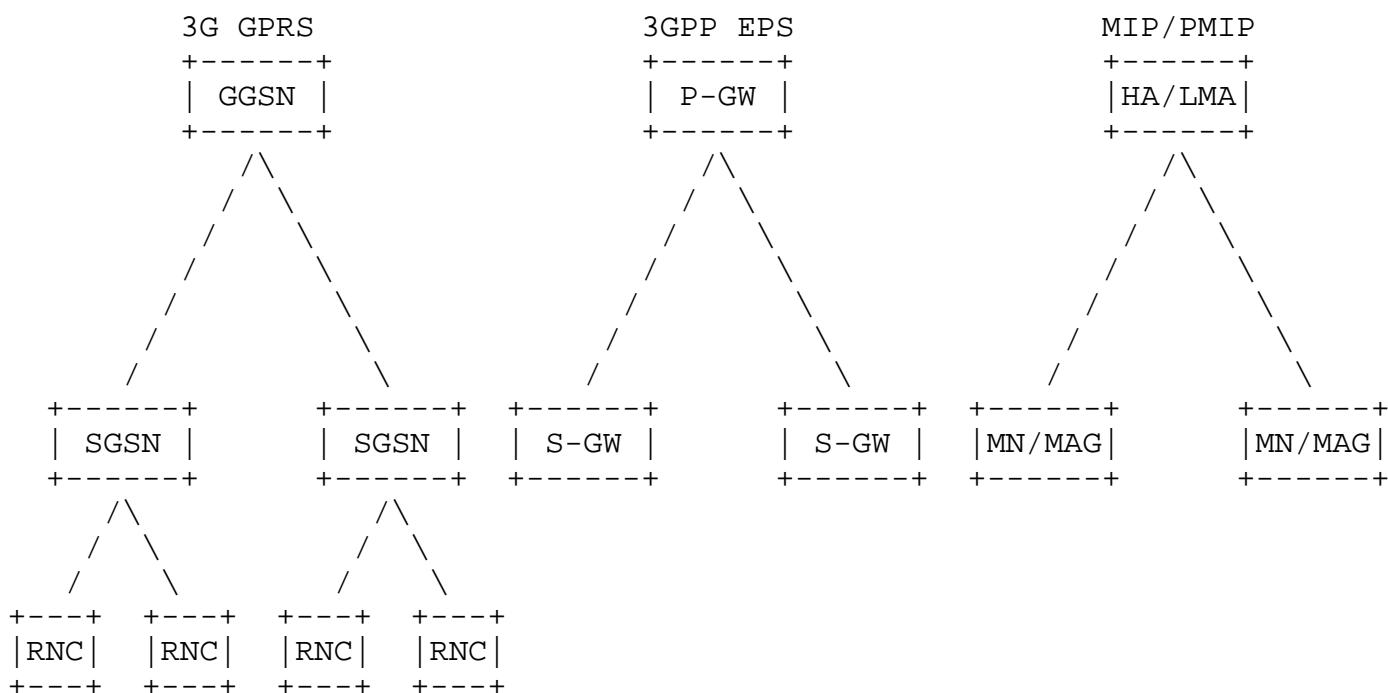
       Figure 1. Centralized mobility management.

3.2. Distributed mobility management

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

```
           +------+  +------+  +------+  +------+
           |  MF  |  |  MF  |  |  MF  |  |  MF  |
           +------+  +------+  +------+  +------+
                                  |
                               +----+
                               | MN |
                               +----+
```
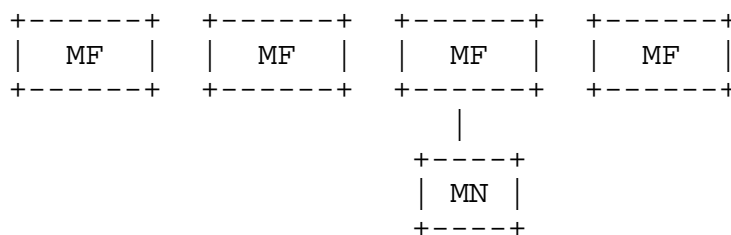
   Figure 2. Distributed mobility management.

   Mobility management may be partially or fully distributed. In the
   former case only the data plane is distributed. Fully distributed
   mobility management implies that both the data plane and the control
   plane are distributed. Such concepts of data and control plane
   separation are not yet described in the IETF developed mobility
   protocols so far but are described in detail in [I-D.yokota-dmm-
   scenario]. While mobility management can be distributed, it is not
   necessary for other functions such as subscription management,

subscription database, and network access authentication to be similarly distributed.

A distributed mobility management scheme for flat IP-based mobile network architecture consisting of access nodes is proposed in [Paper-Distributed.Dynamic.Mobility]. Its benefits over centralized mobility management are shown through simulations in [Paper-Distributed.Centralized.Mobility]. Moreover, the (re)use and extension of existing protocols in the design of both fully distributed mobility management [Paper-Migrating.Home.Agents] [Paper-Distributed.Mobility.SAE] and partially distributed mobility management [Paper-Distributed.Mobility.PMIP] [Paper-Distributed.Mobility.MIP] have been reported in the literature. Therefore, before designing new mobility management protocols for a future flat IP architecture, it is recommended to first consider whether existing mobility management protocols can be extended to serve a flat IP architecture.

4. Problem Statement

The problems that can be addressed with DMM are summarized in the following:

PS1: Non-optimal routes

      Routing via a centralized anchor often results in a longer route. The problem is manifested, for example, when accessing a local server or servers of a Content Delivery Network (CDN), or when receiving locally available IP multicast or sending IP multicast packets.

PS2: Divergence from other evolutionary trends in network architectures such as distribution of content delivery.

      Centralized mobility management can become non-optimal with a flat network architecture.

PS3: Low scalability of centralized tunnel management and mobility context maintenance

      Setting up tunnels through a central anchor and maintaining mobility context for each MN requires more resources in a centralized design, thus reducing scalability. Distributing the tunnel maintenance function and the mobility context maintenance function among different network entities with proper signaling protocol design can increase scalability.

PS4:   Single point of failure and attack

       Centralized anchoring designs may be more vulnerable to single
       points of failures and attacks than a distributed system. The
       impact of a successful attack on a system with centralized
       mobility management can be far greater as well.

PS5:   Unnecessarily reserving resources to provide mobility support
       to nodes that do not need such support

       IP mobility support is not always required, and not every
       parameter of mobility context is always used. For example,
       some applications do not need a stable IP address during a
       handover to maintain session continuity. Sometimes, the entire
       application session runs while the terminal does not change the
       point of attachment. Besides, some sessions, e.g. SIP-based
       sessions, can handle mobility at the application layer and
       hence do not need IP mobility support; it is then more
       efficient to deactivate IP mobility support for such sessions."

PS6:   (Related problem) Mobility signaling overhead with peer-to-peer
       communication

       Wasting resources when mobility signaling (e.g., maintenance of
       the tunnel, keep alive signaling, etc.) is not turned off for
       peer-to-peer communication. Peer-to-peer communications have
       particular traffic patterns that often do not benefit from
       mobility support from the network. Thus, the associated
       mobility support signaling (e.g., maintenance of the tunnel,
       keep alive signaling, etc.) wastes network resources for no
       application gain. In such a case, it is better to enable
       mobility support selectively.

PS7:   (Related problem) Complicated deployment with many MIP variants
       and extensions

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

PS8:   Duplicate multicast traffic

       IP multicast distribution over architectures using IP mobility
       solutions (e.g. RFC6224) may lead to convergence of duplicated
       multicast subscriptions towards the downstream tunnel entity
       (e.g. MAG in PMIPv6). Concretely, when multicast subscription
       for individual mobile nodes is coupled with mobility tunnels
       (e.g. PMIPv6 tunnel), duplicate multicast subscription(s) is

prone to be received through different upstream paths. This
problem may also exist or be more severe in a distributed
mobility environment.

5. Requirements

   After comparing distributed mobility management against centralized
   deployment in Section 3, this section identifies the following
   requirements:

5.1. Distributed deployment

   REQ1:   Distributed deployment

           IP mobility, network access and routing solutions provided by
           DMM MUST enable distributed deployment for mobility management
           of some flows so that traffic does not need to traverse
           centrally deployed mobility anchors and thus can be routed in
           an optimal manner.

           Motivation: This requirement is motivated by current trends in
           network evolution: (a) it is cost- and resource-effective to
           cache and distribute content by combining distributed mobility
           anchors with caching systems (e.g., CDN); (b) the
           significantly larger number of mobile nodes and flows call for
           improved scalability; (c) single points of failure are avoided
           in a distributed system; (d) threats against centrally
           deployed anchors, e.g., home agent and local mobility anchor,
           are mitigated in a distributed system.

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

5.2. Transparency to Upper Layers when needed

   REQ2:   Transparency to Upper Layers when needed

           DMM solutions MUST provide transparent mobility support above
           the IP layer when needed. Such transparency is needed, for
           example, when, upon change of point of attachment to the
           network, an application flow cannot cope with a change in the
           IP address. However, it is not always necessary to maintain a
           stable home IP address or prefix for every application or at
           all times for a mobile node.

           Motivation: The motivation of this requirement is to enable
           more efficient use of network resources and more efficient

routing by not maintaining context at the mobility anchor when
there is no such need.

This requirement addresses the problem PS5 as well as the related
problem PS6 in Section 4.

5.3. IPv6 deployment

REQ3: IPv6 deployment

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

Motivation: This requirement conforms to the general
orientation of IETF work. DMM deployment is foreseen in mid-
to long-term horizon, when IPv6 is expected to be far more
common than today. 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. Existing mobility protocols

REQ4: Existing mobility protocols

A DMM solution SHOULD first consider reusing and extending
IETF-standardized protocols before specifying new protocols.

5.5. Co-existence

REQ5: Co-existence with deployed networks and hosts

The DMM solution MUST be able to co-exist with existing
network deployments and end hosts. For example, depending on
the environment in which DMM is deployed, DMM solutions may
need to be compatible with other deployed mobility protocols
or may need to co-exist with a network or mobile hosts/routers
that do not support DMM protocols. The mobile node may also
move between different access networks, where some of them may
neither support DMM nor another mobility protocol.
Furthermore, a DMM solution SHOULD work across different
networks, possibly operated as separate administrative
domains, when allowed by the trust relationship between them.

Motivation: (a) to preserve backwards compatibility so that
existing networks and hosts are not affected and continue to
function as usual, and (b) enable inter-domain operation if

         desired.

    This requirement addresses the following related problem PS7 in
    Section 4.

5.6. Security considerations

   REQ6:   Security considerations

           DMM protocol solutions MUST consider security risks introduced
           by DMM into the network. Examples of such risks to be
           considered are authentication and authorization mechanisms
           that allow a legitimate mobile host/router to use the mobility
           support provided by the DMM solution; redirecting traffic to
           the wrong host when providing DMM support; signaling message
           protection in terms of authentication, encryption, data
           integrity and confidentiality.

           Motivation: Various attacks such as impersonation, denial of
           service, man-in-the-middle attacks, and so on, can be mounted
           against a DMM network and need to be protected against. Proof
           of possession of past and new IP addresses may be needed.

           Signaling messages can be subject to various attacks since
           they carry critical context information about a mobile node/
           router. For instance, a malicious node can forge a number of
           signaling messages thus redirecting traffic from its
           legitimate path. Consequently, the specific node is under a
           denial of service attack, whereas other nodes do not receive
           their traffic. As signaling messages may travel over the
           Internet, end-to-end security between communicating hosts must
           be required.

5.7. Multicast considerations

   REQ7:   DMM should enable multicast solutions in flexible distribution
           scenario. This flexibility pertains to the preservation of IP
           multicast nature from the perspective of a mobility entiry and
           transmission of mulitcast packets to/from varius multicast-
           enabled entities. Therefore, this flexibility enables
           different IP multicast flows with respect to a mobile host to
           be managed (e.g., subscribed, received and/or transmitted)
           using multiple multicast-enabled endpoints.

           Motivation: The motivation of this requirement is to consider
           multicast early so that solutions can be developed to avoid
           network inefficiency issues in multicast traffic delivery.
           The multicast solution should therefore avoid restricting the

        managment of all IP multicast traffic relative to a host
        through a dedicated interface on multicast-capable access
        routers.

   This requirement addresses the problems PS1 and PS8 in Section 4.

6. Security Considerations

   Distributed mobility management (DMM) requires two kinds of security
   considerations: First, access network security that only allows a
   legitimate mobile host/router to use DMM; Second, end-to-end security
   between the end hosts, which protects signaling messages for DMM.
   Access network security is required between the mobile host/router
   and the access network deploying DMM. 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 numerous
   participants. Each individual has made significant contributions to
   this work and have been listed as co-authors.

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.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.MIP]
              Chan, H., "Distributed Mobility Management with Mobile
              IP", Proceedings of IEEE International Communication
              Conference (ICC) Workshop on Telecommunications: from
              Research to Standards, June 2012.

   [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.

   [Paper-Mobile.Data.Offloading]
                    Lee, K., Lee, J., Yi, Y., Rhee, I., and S. Chong, "Mobile
                    Data Offloading: How Much Can WiFi Deliver?", SIGCOMM
                    2010, 2010.

   [RFC3753]   Manner, J. and M. Kojo, "Mobility Related Terminology",
                    RFC 3753, June 2004.

   [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.

   [RFC5944]   Perkins, C., "IP Mobility Support for IPv4, Revised",
                    RFC 5944, November 2010.

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

   [RFC6301]   Zhu, Z., Wakikawa, R., and L. Zhang, "A Survey of Mobility
                    Support in the Internet", RFC 6301, July 2011.

   [TS.23.401]
                    3GPP, "General Packet Radio Service (GPRS) enhancements
                    for Evolved Universal Terrestrial Radio Access Network
                    (E-UTRAN) access", 3GPP TR 23.401 10.10.0, March 2013.

   [TS.29303]
                    3GPP, "Domain Name System Procedures; Stage 3", 3GPP
                    TR 23.303 11.2.0, September 2012.

Authors' Addresses

   H Anthony Chan (editor)
   Huawei Technologies (more co-authors on P. 17)
   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

Jouni Korhonen
Nokia Siemens Networks
Email: jouni.korhonen@nsn.com
-
Charles E. Perkins
Huawei Technologies
Email: charliep@computer.org
-
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
-
Kostas Pentikousis
Huawei Technologies
Carnotstr. 4 10587 Berlin, Germany
Email: k.pentikousis@huawei.com
-
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
        -
    Sri Gundavelli
    sgundave@cisco.com
        -
    Marco Liebsch
    NEC Laboratories Europe
    Email: liebsch@neclab.eu
        -
    Carl Williams
    MCSR Labs
    Email: carlw@mcsr-labs.org
        -
    Seil Jeon
    Email: seiljeon@av.it.pt
        -
    Sergio Figueiredo
    Email: sfigueiredo@av.it.pt
        -
    Stig Venaas
    Email: stig@venaas.com
        -
    Luis Miguel Contreras Murillo
    Email: lmcm@tid.es
        -
    Juan Carlos Zuniga
    Email: JuanCarlos.Zuniga@InterDigital.com
        -
    Alexandru Petrescu
    Email: alexandru.petrescu@gmail.com
        -

Georgios Karagiannis
Email: g.karagiannis@utwente.nl
-
Julien Laganier
jlaganier@juniper.net
-
Wassim Michel Haddad
Wassam.Haddad@ericsson.com
-
Dirk von Hugo
Dirk.von-Hugo@telekom.de
-
Ahmad Muhanna
amuhanna@awardsolutions.com
-