

Mobility Optimizations: MIPSHOP WG
Internet-Draft
Expires: January 9, 2008

W. Haddad
S. Krishnan
Ericsson Research
F. Dupont
CELAR
July 8, 2007

Mobility Signaling Delegation
draft-haddad-mipshop-mobisig-del-03

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on January 9, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Internet-Draft

Mobility Signaling Delegation

July 2007

Abstract

This memo describes a mechanism which delegates the exchange of mobility signaling messages between the mobile and correspondent nodes to the network infrastructure. Goals outlining the proposed delegation are to further reduce the IP handoff latency and to relieve the mobile node from exchanging a considerable amount of signaling messages with correspondent nodes while retaining full control on the critical ones.

Table of Contents

1.	Introduction	3
2.	Conventions used in this document	4
3.	Motivation	5
4.	Suggested Solution	7
5.	New Options and Messages	9
6.	Security Considerations	10
7.	References	11
7.1.	Normative References	11
7.2.	Informative References	11
	Authors' Addresses	12
	Intellectual Property and Copyright Statements	13

1. Introduction

Optimized Mobile IPv6 (OMIPv6) protocol (described in [\[OMIPv6\]](#)) provides a mechanism, which allows significant reduction in the amount of signaling messages generated by the Mobile IPv6 protocol ([\[MIPv6\]](#)), a shorter handoff latency and a better overall security. However, a care-of address (CoA) test exchange between the mobile node (MN) and each correspondent node (CN) remains a compulsory step prior to exchanging critical mobility signaling messages between them, namely binding updates (BU) and acknowledgments (BA) messages. The CoA reachability test involves two mobility signaling messages (CoTI/CoT) and is unaffected by the optimization introduced by OMIPv6 protocol.

This memo describes a mechanism which delegates the exchange of mobility signaling messages between the MN and CN(s) to the network infrastructure, as part of the ongoing work on designing an optimization to the IPv6 secure neighbor discovery (described in [\[SeND\]](#)) protocol. Goals outlining the proposed delegation are to further reduce the IP handoff latency and to relieve the MN from exchanging a considerable amount of signaling messages with each CN while retaining full control on the BU/BA messages.

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 [[TERM](#)].

[3.](#) Motivation

OMIPv6 protocol achieves three different goals: it alleviates the mobility signaling messages load, improves the overall security and reduces the IP handoff latency.

The latency reduction caused by OMIPv6 is mainly due to eliminating the MN's home address reachability test, which requires a signaling message exchange through the MN's Home Agent (HA). Another set of factors (excluding the link layer), e.g., network detection, network prefix discovery and IP address configuration are still among the main contributors to the handoff latency. These factors remain totally unaffected by using OMIPv6.

In addition, OMIPv6 still require a CoA reachability test with each CN, prior to updating them with its new CoA (nCoA), i.e., exchanging BU/BA messages. Consequently, such exchange guarantees a residual latency and additional mobility signaling messages.

Furthermore, it is important to mention that a fast growing class of mobile devices tend to have very limited battery power. Thus, the available energy must be meticulously controlled and consumed, i.e.,

not to be wasted on exchanging non-critical signaling messages. Such requirement becomes more challenging when the MN is talking to different CNs at the same time (which may probably be a very common case) while moving fast.

In fact, it has been shown that the wireless transmission of one bit can require over 1000 times more energy than a single 32-bit computation [[EALDC](#)]. Consequently, a fast moving MN communicating with multiple CNs will have to dedicate a significant amount of its available energy to exchange only mobility signaling messages with the CNs.

OMIPv6 provides a credit-based Authorization (CBA) mechanism, which aims to reduce further the latency caused by the care-of address test exchange. However, such mechanism has two drawbacks: the CN may not provide this feature, in which case the latency problem remains unsolved, and it consumes battery power in both scenarios due to exchanging signaling messages (i.e., as they get only delayed). Note that the suggested protocol does not prevent both endpoints from using the CBA mechanism on top of the suggested protocol.

On the other side, the Optimized Secure Neighbor Discovery protocol (described in [[OptiSeND](#)]) is an ongoing work, which aims to better adapt the requirements for securing the IPv6 neighbor discovery to low computation and battery power devices (e.g., mobile devices and sensors). OptiSeND enables fixed/mobile nodes to avoid using

expensive RSA signatures to secure neighbor discovery messages exchange by providing a mechanism to quickly share a long lifetime symmetric key with the AR(s). On the infrastructure side, OptiSeND enables ARs to use one-way hash chains to authenticate the Router Advertisement (RtAdv) messages sent to the fixed/mobile node(s) attached to the same link.

[4.](#) Suggested Solution

Our proposal delegates the task of performing CoA reachability test(s) to the network infrastructure, which in turn enables eliminating the residual latency due to the CoA reachability test, ensures that the messages exchanged are authenticated and optimizes the battery power consumption by relieving the MN from performing CoA reachability tests. In fact, our protocol adopts another approach to

perform reachability tests, which consists on testing the reachability of the new MN's 64-bit subnet prefix only instead of testing the reachability of the whole nCoA, and thus relies on two new messages to perform such test.

For these purposes, the MN must securely send to the access network infrastructure necessary information (called mobility package) to enable performing the CoA reachability test(s) on its behalf and to forward the mobility package to potential new ARs (nARs). To achieve this goal, a new message called "Router Mobility Solicitation" (RtMoSol) is used by the MN to send its mobility package to its current AR(s). The RtMoSol message MUST carry all CNs'IPv6 addresses and the MN's IPv6 home address(es) (HoAs) and MUST be authenticated with the shared key obtained from OptiSeND.

Upon receiving a valid RtMoSol message, the selected AR SHOULD reply with an authenticated unicast "Router Mobility Acknowledgment" (RtMAck) message. The RtMoSol message content SHOULD be forwarded to neighboring ARs and should be stored together with data obtained from running OptiSeND protocol.

The RtMoSol message is also used by the MN to add or delete entries from a mobility package stored in the AR cache memory. For example, when the MN establishes a session with a new CN, it SHOULD send a RtMoSol message to its current AR and SHOULD set a new bit (called Add "A" bit) to request the AR to forward the new CN's IPv6 address to potential new AR(s). Similarly, the MN MAY also set another bit (called Suppress "S" bit) to request the AR(s) to remove an existing CN's IPv6 address from its list.

In order to eliminate the residual latency due to performing the CoA reachability test, the nAR SHOULD perform the test immediately after receiving a first hint (e.g., on layer 2) indicating an attachment of the MN (e.g., when using [FRD](#)) and SHOULD forward the message(s) sent by the CN(s) to the MN after it attaches to the nAR. For this purpose, the nAR SHOULD use its source address, which includes the prefix advertised on the link and MUST authenticate the message with a mobility signaling key (Kms). We call such message "Prefix Test Init" (PreTI). In addition, the PreTI message MUST carry the MN's HoA to allow the CN to fetch/generate the Kms associated with the corresponding Binding Cache Entry (BCE) in order to validate the

Upon receiving a valid PreTI message, the CN computes a prefix keygen (prekey) token from the prefix used in the IPv6 source address and the long lifetime shared secret (i.e., kbmperm) generated from using OMIPv6 protocol. After computing the token, the CN SHOULD send back an acknowledgment message called "Prefix Test" (PreT), which carries the prekey token to the same IPv6 source address carried in the PreTI message. The PreT message MUST also carry the MN's HoA and MUST be authenticated with Kms.

The Prekey token MUST be computed by the CN in the following way:

Prekey Token = First [64, SHA1 (SA_Prefix | nonce | SHA1 (Kbmperm))]

Where SA_Prefix is the 64-bit prefix included in the IPv6 source address sent in the PreTI message and Kbmperm is the long lifetime shared secret generated by the CN when running OMIPv6 protocol.

As mentioned above, the prefix reachability test SHOULD be authenticated with Kms. In order to do so, Kms SHOULD be computed from using the symmetric key generated from running OptiSeND protocol and the MN's HoA, and MUST be send encrypted to each CN. One way to achieve a confidential transmission of Kms is to send it encrypted in the first BU message sent by the MN. In such scenario, the MN will use its Kbm (computed from running the return routability procedure) to encrypt Kms. Finally, Kms will be carried in a new option called signaling delegation (SID).

Upon receiving a BU message carrying a SID option, the CN decrypts Kms and stores it in the MN's corresponding BCE. All subsequent reachability test messages SHOULD be sent by the MN's current AR on behalf of the MN and SHOULD be authenticated with Kms.

[5.](#) New Options and Messages

TBD

[6.](#) Security Considerations

This draft proposes a scheme to delegate mobility signaling from the mobile node to the network infrastructure. Since the network infrastructure nodes are well known and trustworthy, it makes firewalling easier at the administrative boundaries. Also, since the network infrastructure nodes are likely to have more resources than mobile nodes, this scheme will allow us to use higher strength crypto to protect the signaling. This draft does not introduce any new security holes into existing route optimization solutions.

[7.](#) References

[7.1.](#) Normative References

- [MIPv6] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", [RFC 3775](#), June 2004.
- [OMIPv6] Vogt, C., Arkko, J., and W. Haddad, "Enhanced Route Optimization for Mobile IPv6", [RFC 4866](#), June 2006.
- [SeND] Arkko, J., Kempf, J., Sommerfield, B., Zill, B., and P. Nikander, "Secure Neighbor Discovery (SeND)", [RFC 3971](#), March 2005.
- [TERM] Bradner, S., "Key Words for Use in RFCs to Indicate Requirement Levels", [RFC 2119](#), BCP , March 1997.

[7.2.](#) Informative References

- [EALDC] Barr, K. and K. Asanovic, "Energy Aware Lossless Data Compression", ACM Proceedings of MobiSys, May 2003.
- [FRD] Choi, J., Shin, D., and W. Haddad, "Fast Router Discovery with L2 Support", Internet Draft, [draft-ietf-dna-frd-01.txt](#), June 2006.
- [OptiSeND] Haddad, W., Krishnan, S., and J. Choi, "Secure Neighbor Discovery (SeND) Optimization: The OptiSeND Protocol", Internet Draft, [draft-haddad-mipshop-optisend-03.txt](#), July 2007.

Authors' Addresses

Wassim Haddad
Ericsson Research
Torshamnsgatan 23
SE-164 80 Stockholm
Sweden

Phone: +46 8 4044079
Email: Wassim.Haddad@ericsson.com

Suresh Krishnan
Ericsson Research
8400 Decarie Blvd.
Town of Mount Royal, QC
Canada

Phone: +1 514 345 7900
Email: Suresk.Krishnan@ericsson.com

Francis Dupont
CELAR

Email: Francis.Dupont@fdupont.fr

Haddad, et al.

Expires January 9, 2008

[Page 12]

Internet-Draft

Mobility Signaling Delegation

July 2007

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).