

Mobility Optimizations
Internet-Draft
Expires: January 10, 2008

W. Haddad
S. Krishnan
Ericsson Research
J. Choi
Samsung AIT
J. Laganier
Docomo Euro-Labs
July 9, 2007

Secure Neighbor Discovery (SeND) Optimizations: The OptiSeND Protocol
draft-haddad-mipshop-optisend-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/1id-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 10, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Internet-Draft

OptiSeND

July 2007

Abstract

This memo describes a new set of mechanisms, which aim to increase the Secure Neighbor Discovery protocol usability, provide additional deployment incentives and a better adaptation to mobile environment.

Table of Contents

1.	Introduction	3
2.	Conventions used in this document	4
3.	Glossary	5
4.	Motivation and Goal	6
5.	Overview of OptiSeND	7
6.	New Options and Messages Formats	10
7.	Security Considerations	11
8.	Acknowledgments	12
9.	References	13
9.1.	Normative References	13
9.2.	Informative Reference	13
	Authors' Addresses	14
	Intellectual Property and Copyright Statements	15

1. Introduction

Securing Neighbor Discovery Protocol [[SeND](#)] has been designed to mitigate potential threats against IPv6 Neighbor Discovery Protocol [[NDP](#)]. SeND protocol is based uniquely on the Cryptographically Generated Address [[CGA](#)] technology.

The reliance on RSA signature may severely hamper SeND protocol usability and deployment in the wireless world. This is mainly due to the fact that the vast majority of mobile devices share a severe limitation in terms of processing power (and battery consumption).

This memo describes a new protocol called OptiSeND, which aims to increase SeND protocol usability, provide additional deployment incentives and a better adaptation to mobile environment.

We achieve our goals by reducing the reliance on RSA signature to validate the flow of periodic multicast router advertisement (RtAdv), authenticating the NDP messages and removing the latency caused by running the duplicate address detection (DAD) procedure. Other features may also be provided.

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.](#) Glossary

Access Router (AR)

The Access Router is the mobile node's default router.

Attached Node (AN)

An attached node (AN) is a node, which is already attached to the infrastructure via one or many Access Router(s). An AN is able to validate a multicast RtAdv message(s) without checking its signature. An AN can be static or mobile.

Soliciting Node (SN)

A soliciting node is a node, which has started the procedure to attach itself to the infrastructure by sending a router solicitation (RtSol) message signed with CGA technology to a selected AR. After exchanging the first RtSol/RtAdv messages, the SN is supposed to become an AN.

One-Way Chain

A one-way chain ($V_0 \dots V_n$) is a collection of values such that each value V_i (except the last value V_n) is a one-way function of the next value V_{i+1} . In particular, we have $V_i = H(V_{i+1})$, for i belonging to $[0, n[$. For clarity purpose and to avoid confusion, we'll use in the rest of this document the notation $V[i]$ instead of V_i , which means $V[i+1]$ points to $V_{i+1} \dots$

Neighbors

Nodes attached to the same link.

For more details about the one-way chain, please refer to [\[OWHC\]](#).

[4.](#) Motivation and Goal

IPv6 NDP has been designed to enable nodes on the same link to discover each other's presence and link-layer addresses, to find routers, and to maintain reachability information about the paths to active neighbors. NDP is used by both hosts and routers. Its functions include Neighbor Discovery, Router Discovery, Address Autoconfiguration and Resolution, Neighbor Unreachability Detection, Duplicate Address Detection (DAD), and Redirection.

[NDT] describes different threats, which may appear when NDP is applied without any protection (e.g., public WLAN network). These threats can materialize on a particular link in a severe disruption of information exchange, e.g., due to launching DoS attacks against one or many nodes. SeND protocol has been designed to counter

threats described in the NDT. For this purpose, SeND relies solely on CGA technology to provide IPv6 address proof of ownership, sign NDP messages and consequently, build a form of trust relationship between different nodes. SeND protocol is highly recommended when attached nodes (ANs) are using NDP to communicate with the infrastructure and/or between themselves as neighbors.

When SeND protocol is used between nodes and the infrastructure, an AR is expected to use CGA technology in all messages sent to any AN. As previously mentioned, CGA technology allows the AR to provide a proof of ownership of its claimed IP address(es) and enables the receiving node(s) to validate information carried in these messages. Note that the SN may or may not be SeND enabled and thus may not be able to secure the RtSol message sent to the AR(s). Similarly, applying SeND protocol to secure NDP exchange enables each node to provide a proof of ownership of its newly configured IP address(es), thus eliminating certain malicious behavior, e.g., when checking its uniqueness via the DAD procedure.

The main goal of this document is to provide an alternative solution to the RSA signature, which on one side, encourages all nodes to use SeND and increases the deployment scale, but on the other side, eliminates the reliance on CGA technology whenever possible. Our current design is limited to the exchange of NDP messages between AN and the infrastructure and slightly cover the ND messages exchange between neighbors. This part is left for future work.

[5.](#) Overview of OptiSeND

The first goal behind designing OptiSeND protocol is to eliminate the need for ANs to validate RSA signatures whenever possible. We achieve our goal by exploiting the fact that the content of the router advertisement message itself does not get modified frequently. It follows that prefixes advertised on one particular link together with their associated parameters are likely to appear unmodified in

each subsequent RA message. However, there are cases where prefixes do change when renumbering is needed. Such scenario is also supported in our approach.

In the following, we refer to such message (i.e., plain message) by RA message and we use the RtAdv notation to refer to an RA message with SeND protection, i.e., carrying RSA signature and associated parameters.

Another goal is to enable each SN to share a secret with its AR when exchanging the first pair of RtSol/RtAdv messages. The shared secret is then used to authenticate all NDP messages as they get exchanged via the AR instead of doing it on the link. The NDP messages re-routing is needed in order to avoid sharing secrets between each and every neighbor. In addition, ANs should skip the DAD procedure by delegating such task to the AR whenever possible, in order to reduce the handoff latency in a mobile environment.

OptiSeND protocol removes the need to verify RSA signatures in an entire set of RtAdv messages carrying an identical multicast RA message, except for the first one, which MUST be sent to the SN in unicast mode. Note that in our context, "identical" refers to prefixes and associated parameters. We achieve this goal in two steps. The first one consists on using a particular OWHC value as a "hook" to enable the SN to quickly validate the sequence of subsequent RtAdv messages. Such requirement imposes on the AR to send to the SN the last disclosed value, i.e., to be used as the hook, of its OWHC. For this purpose, the OWHC value is carried by the unicast (and first) RtAdv message. The second step is achieved by inserting in the same (first) unicast RtAdv message sent to the SN the hash value, i.e., called "Z", of the next RtAdv message concatenated with the next, i.e., yet undisclosed, OWHC value and the next timestamp value. This means that if OWHC[i] is the last disclosed OWHC value sent to the SN, then "Z" is computed in the following way:

$$Z = \text{First} [64, \text{Hash} [\text{RA}[i+1] \mid \text{OWHC}[i+1] \mid \text{Timestamp}[i+1]]]$$

Where:

message.

- First (size, input) indicates truncation of "input" data so that only the first "size" bits remain to be used.
- RA[i+1] is the next multicast router advertisement sent after sending the unicast RtAdv to the SN.
- OWHC[i+1] is the new and undisclosed value of the OWHC.
- Timestamp[i+1] is the timestamp value which is sent in the next RtAdv message, i.e., RtAdv[i+1].

It follows that the content of the unicast RtAdv message sent to the SN is as it follows:

$$\text{RtAdv}[i] = \{ \text{RA}[i] \mid Z \mid \text{OWHC}[i] \mid \text{Timestamp}[i] \mid \text{SIG}(\text{Kp}, \text{RtAdv}[i]) \}$$

Where SIG(K, M) is the signature computed over the entire message M with key K.

Such procedure is then repeated in each subsequent multicast RtAdv messages sent on the link. Doing so, enables ANs to easily validate all subsequent multicast RtAdv messages by checking first if the disclosed OWHC value carried in the newly received message is valid and then use it to compute "Z" and compare it to the one sent in the previous RtAdv message. Note that the timestamp used in the RtAdv message will also be used to keep AN(s) synchronized to the OWHC. In case, an AN misses one multicast RtAdv message, it should solicit a re-synchronization by sending an authenticated RtSol message. In this case, the AR SHOULD send back an authenticated unicast RtAdv message similar to the first one sent to any SN in unicast mode. The AR MAY also sign the unicast RtAdv message but the signature validation is not needed.

In a mobile environment, the mobile node (MN) may miss the RtAdv message due to switching between ARs. In this particular case, the new AR (nAR) and the MN should share a new secret to authenticate subsequent NDP messages. It follows that the MN should send a new RtSol message signed with CGA in order to get an encrypted copy of the shared secret from the nAR. An optimization to the handoff procedure would consist on enabling a closer collaboration between ARs, in order to avoid sharing a new secret each time the MN switches to a new AR. Such optimization requires secure links and trust between ARs.

As mentioned earlier, the proposed solution removes the need to verify the RSA signature in each RtAdv message. This also means that the AR will always sign each RtAdv message sent in unicast or multicast mode. However, the AN will first rely on the OWHC technique to validate its content. In case, crucial data have been

modified in the latest multicast RtAdv message, then the signature MUST be checked. Otherwise, the AN can skip such procedure and store the carried hash value (Z) whose components will be disclosed in the next RtAdv. Finally, the AN SHOULD discard any multicast RtAdv message, which carries a non-valid timestamp unless it has been received after a layer 2 handoff.

An AR should store in its cache the AN's CGA public key, its MAC address, the CGA-based interface identifier(s) (IID(s)) and the corresponding shared secret (called Ks). Storing the IID(s) can also be used to remove the need for running DAD procedures, and additional IID(s) MAY be generated from combining Ks with additional parameters. Note that an AR can store the AN's corresponding parameters for a limited amount of time after which, it should check again its presence on the link. Ks is computed by the AR and MUST be sent encrypted to SN. For this purpose, the AR MUST use SN's CGA public key sent in the (first) RtSol message to encrypt Ks. The shared secret should be refreshed when its lifetime expires.

When a NDP messages exchange is needed between two neighboring ANs, NDP messages MUST be exchanged via the AR in order to avoid using CGA signature in each message while protecting their integrity. For this purpose, and in order to avoid inflating each NDP message with an additional IPv6 header, a new option is defined to indicate to the AR the destination address to be queried. If the received message is valid, the AR sends the NDP message to the destination and authenticates the message with the corresponding shared secret. After receiving a valid response from the destination, the AR sends back an authenticated ND message to the sender, which carries the response provided by the destination.

Internet-Draft

OptiSeND

July 2007

[6.](#) New Options and Messages Formats

TBD

[7.](#) Security Considerations

This memo introduces a new mechanism which is built on top of SeND protocol. The main goal behind OptiSeND design is to improve the usability, make a strong(er) case for potential deployment and widen its scope to include new features. We believe that this goal can be achieved without introducing new threats nor amplifying existing ones.

However, expanding OptiSeND protocol in order to enable additional features, e.g., fast mobility, signaling delegation, etc, requires secure links and trust between ARs and possibly between ARs and the access points.

[8.](#) Acknowledgments

Authors would like to thank Pekka Nikander for his valuable input at the early stage of this work.

[9.](#) References

[9.1.](#) Normative References

- [CGA] Aura, T., "Cryptographically Generated Addresses (CGA)", [RFC 3792](#), March 2005.
- [NDP] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP Version 6 (IPv6)", Internet Draft, [draft-ietf-ipv6-2461bis-11.txt](#), March 2007.
- [NDT] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Model and Threats", [RFC 3756](#), May 2004.
- [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.

[9.2.](#) Informative Reference

[OWHC] Hu, Y., Jakobsson, M., and A. Perrig, "Efficient Constructions for One-Way Hash Chains", ACNS Conference, June 2005.

Haddad, et al. Expires January 10, 2008 [Page 13]

Internet-Draft OptiSeND 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: Suresh.Krishnan@ericsson.com

JinHyeock Choi
Samsung AIT
Communication & N/W Lab
Suwon 440-600
P.O. Box 111
KOREA

Phone: +82 31 280 9233
Email: jinchoe@samsung.com

Julien Laganier
Docomo Communications Laboratories Europe GmbH
Landsberger Strasse 312
Munich 80687
Germany

Phone: +49 89 56824 231
Email: Julien.ietf@laposte.net
URI: <http://www.docomolab-euro.com>

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).