

ace
Internet-Draft
Intended status: Standards Track
Expires: July 18, 2014

B. Sarikaya, Ed.
Huawei USA
F. Xia
Huawei Technologies Co., Ltd.
January 14, 2014

Lightweight Secure Neighbor Discovery for Low-power and Lossy Networks
draft-sarikaya-ace-cga-nd-00

Abstract

Modifications to 6lowpan Neighbor Discovery protocol are proposed in order to secure the neighbor discovery for low-power and lossy networks. This document defines lightweight and secure version of the neighbor discovery for low-power and lossy networks. The nodes generate a Cryptographically Generated Address, register the Cryptographically Generated Address with a default router and periodically refresh the registration. Cryptographically generated address and digital signatures are calculated using elliptic curve cryptography, so that the cryptographic operations are suitable for low power devices.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

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

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

This Internet-Draft will expire on July 18, 2014.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
2.	Terminology	3
3.	Problem Statement	3
4.	New Options	4
4.1.	CGA Parameters and Digital Signature Option	4
4.2.	Digital Signature Option	6
4.3.	Calculation of the Digital Signature and CGA Using ECC	7
5.	Protocol Interactions	8
5.1.	Packet Sizes	9
6.	Security Considerations	10
7.	IANA considerations	10
8.	Acknowledgements	10
9.	References	10
9.1.	Normative References	10
9.2.	Informative references	11
	Authors' Addresses	12

1. Introduction

Neighbor discovery for IPv6 [[RFC4861](#)] and stateless address autoconfiguration [[RFC4862](#)], together referred to as neighbor discovery protocols (NDP), are defined for regular hosts operating with wired/wireless links. These protocols are not suitable and require optimizations for resource constrained, low power hosts operating with lossy wireless links. Neighbor discovery optimizations for 6lowpan networks include simple optimizations such as a host address registration feature using the address registration option which is sent in unicast Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages [[RFC6775](#)].

Neighbor discovery protocols (NDP) are not secure especially when physical security on the link is not assured and vulnerable to attacks defined in [[RFC3756](#)]. Secure neighbor discovery protocol (SEND) is defined to secure NDP [[RFC3971](#)]. Cryptographically generated addresses (CGA) are used in SEND [[RFC3972](#)]. SEND mandates the use of the RSA signature algorithm which is computationally heavy and not suitable to use for low-power and resource constrained nodes. The use of an RSA public key and signature leads to long message sizes not suitable to use in low-bit rate, short range, asymmetric and non-transitive links such as IEEE 802.15.4.

In this document we extend the 6lowpan neighbor discovery protocol with cryptographically generated addresses. The nodes generate CGAs and register them with the default router. CGA generation is based on elliptic curve cryptography (ECC) and signature is calculated using elliptic curve digital signature algorithm (ECDSA) known to be lightweight, leading to much smaller packet sizes. The resulting protocol is called Lightweight Secure Neighbor Discovery Protocol (LSEND).

2. Terminology

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](#)].

The terminology in this document is based on the definitions in [[RFC3971](#)], [[RFC3972](#)] in addition to the ones specified in [[RFC6775](#)].

3. Problem Statement

In this section we state requirements of a secure neighbor discovery protocol for low-power and lossy networks.

The protocol MUST be based on the Neighbor Discovery Optimization for Low-power and Lossy Networks protocol defined in [[RFC6775](#)] due to the host-initiated interactions to allow for sleeping hosts, elimination of multicast-based address resolution for hosts, etc.

New options to be added to neighbor solicitation messages MUST lead to small packet sizes. Smaller packet sizes facilitate low-power transmission by resource constrained nodes on lossy links.

CGA generation, signature and key hash calculation MUST avoid the use of SHA-1 which is known to have security flaws. In this document, we use SHA-2 instead of SHA-1 and thus avoid SHA-1's flaws.

Public key and signature sizes MUST be minimized and signature calculation MUST be lightweight. In this document we adopt ECC and ECDSA with the P-256 curve in order to meet this requirement.

4. New Options

4.1. CGA Parameters and Digital Signature Option

This option contains both CGA parameters and the digital signature.

A summary of the CGA Parameters and Digital Signature Option format is shown below.

Padding

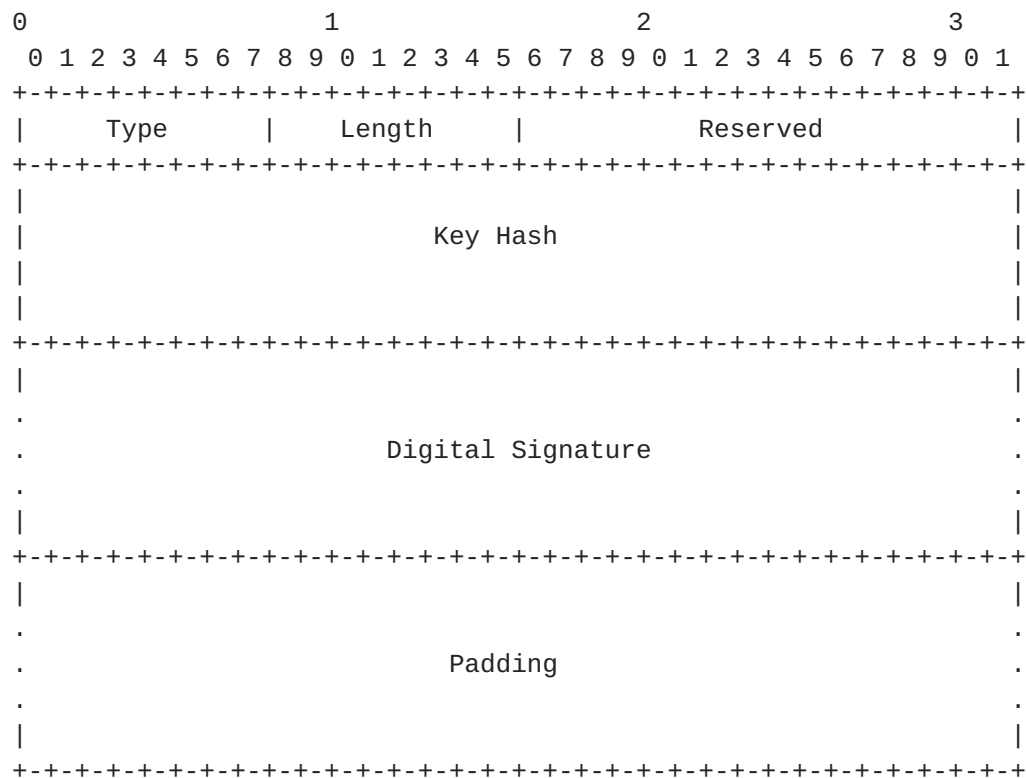
The Padding field contains a variable-length field making the CGA Parameters and Digital Signature Option length a multiple of 8.

4.2. Digital Signature Option

This option contains the digital signature.

A summary of the Digital Signature Option format is shown below. Note that this option has the same format as RSA Signature Option defined in [RFC3971]. The differences are that Digital Signature field carries an ECDSA signature not an RSA signature, and in calculating Key Hash field SHA-2 is used instead of SHA-1.

In the sequence of octets to be signed using the sender's private key includes 128-bit CGA Message Type tag. In LSEND, CGA Message Type tag of 0xE8C47FB7FD2BB885DAB2D31A0F2808B4 MUST be used.



Type

TBA2 for Digital Signature

Length

The length of the option (including the Type, Length, Reserved, Key Hash, Digital Signature and Padding fields) in units of 8 octets.

Key Hash

The Key Hash field is a 128-bit field containing the most significant (leftmost) 128 bits of a SHA-2 hash of the public key used for constructing the signature. This is the same as in [\[RFC3971\]](#) except for SHA-1 which has been replaced by SHA-2.

Digital Signature

Same as in [Section 4.1](#).

Padding

The Padding field contains a variable-length field containing as many bytes long as remain after the end of the signature.

[4.3](#). Calculation of the Digital Signature and CGA Using ECC

Due to the use of Elliptic Curve Cryptography, the following modifications are needed to [\[RFC3971\]](#) and [\[RFC3972\]](#).

The digital signature is constructed by using the sender's private key over the same sequence of octets specified in [Section 5.2 of \[RFC3971\]](#) up to all neighbor discovery protocol options preceding the Digital Signature option containing the ECC-based signature. The signature value is computed using the ECDSA signature algorithm as defined in [\[SEC1\]](#) and hash function SHA-256.

Public Key is the most important parameter in CGA Parameters defined in [Section 4.1](#). Public Key MUST be DER-encoded ASN.1 structure of the type SubjectPublicKeyInfo formatted as ECC Public Key. The AlgorithmIdentifier, contained in ASN.1 structure of type SubjectPublicKeyInfo, MUST be the (unrestricted) id- ecPublicKey algorithm identifier, which is OID 1.2.840.10045.2.1, and the subjectPublicKey MUST be formatted as an ECC Public Key, specified in [Section 2.2 of \[RFC5480\]](#).

Note that the ECC key lengths are determined by the namedCurves parameter stored in ECPParameters field of the AlgorithmIdentifier. The named curve to use is secp256r1 corresponding to P-256 which is OID 1.2.840.10045.3.1.7 [\[SEC2\]](#).

ECC Public Key could be in uncompressed form or in compressed form where the first octet of the OCTET STRING is 0x04 and 0x02 or 0x03, respectively. Point compression using secp256r1 reduces the key size

by 32 octets. In LSEND, point compression MUST be supported.

5. Protocol Interactions

Lightweight Secure Neighbor Discovery for Low-power and Lossy Networks (LSEND for LLN) modifies Neighbor Discovery Optimization for Low-power and Lossy Networks [[RFC6775](#)] as explained in this section. Protocol interactions are shown in Figure 1.

6LoWPAN Border Routers (6LBR) send router advertisements (RA). 6LoWPAN Nodes (6LN, or simply "nodes") receive these RAs and generate their own cryptographically generated addresses using elliptic curve cryptography as explained in [Section 4.3](#). The node sends a neighbor solicitation (NS) message with the address registration option (ARO) to 6LBR. Such a NS is called an address registration NS.

An LSEND for LLN node MUST send an address registration NS message after adding CGA Parameters and Digital Signature Option defined in [Section 4.1](#). Source address MUST be set to its cryptographically generated address. An LSEND for LLN node MUST set the Owner Interface Identifier field (EUI-64) in ARO to the rightmost 64 bits of its cryptographically generated address. The Subnet Prefix field of CGA Parameters MUST be set to the leftmost 64 bits of its cryptographically generated address. The Public Key field of CGA Parameters MUST be set to the node's ECC Public Key.

6LBR receives the address registration NS. 6LBR then verifies the source address as described in [Section 5.1.2. of \[RFC3971\]](#) using the claimed source address and CGA Parameters field in the message. After successfully verifying the address 6LBR next does a cryptographic check of the signature included in the Digital Signature field in the message. If all checks succeed then 6LBR performs a duplicate address detection procedure on the address. If that also succeeds 6LBR registers the CGA in the neighbor cache. 6LBR also caches the node's public key.

6LBR sends an address registration neighbor advertisement (NA) as a reply to confirm the node's registration. Status is set to 0 to indicate success. This completes initial address registration. The address registration needs to be refreshed after the neighbor cache entry times out.

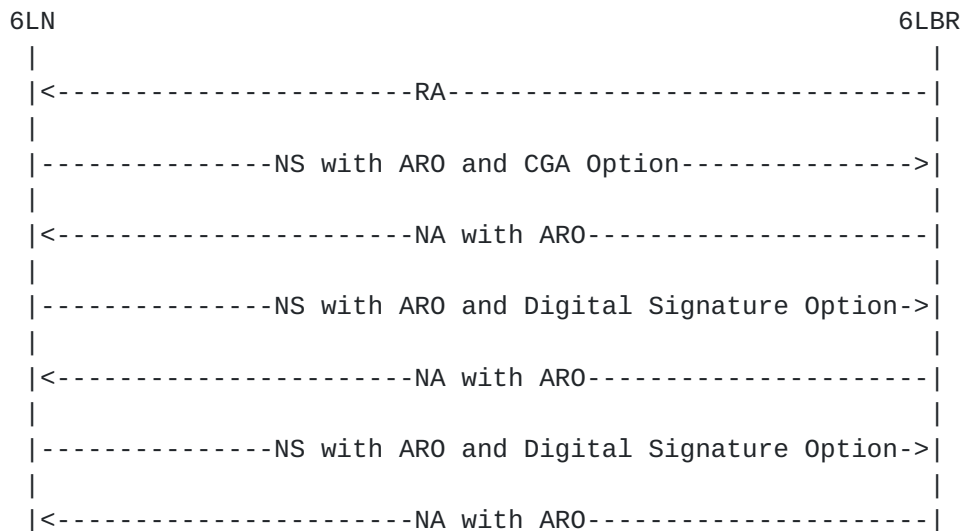


Figure 1: Lightweight SEND for LLN Protocol

In order to refresh the neighbor cache entry, an LSEND for LLN node MUST send an address registration NS message after adding the Digital Signature Option defined in [Section 4.2](#). The Key Hash field is a hash of the node's public key and MUST be set as described in [Section 4.2](#). The Digital Signature field MUST be set as described in [Section 4.2](#).

6LBR receives the address registration refresh NS. 6LBR uses the key hash field in Digital Signature Option to find the node's public key from the neighbor cache. 6LBR verifies the digital signature in the NS. In case of successful verification, 6LBR sends back an address registration neighbor advertisement (NA) to the node and sets the status to 0 indicating successful refreshment of the CGA of the node. Similar refresh NS and NA exchanges happen afterwards as shown in Figure 1.

5.1. Packet Sizes

An original address registration NS message that contains a 40 byte header and ARO is 16 octets. DER-encoded ECC Public Key for P-256 curve is 88 octets long uncompressed and $88-32=56$ octets with point compression. Digital Signature field when using ECDSA for P-256 curve is 72 octets long without padding bytes for a DER encoding of the ASN.1 type "ECDSA-sig-value" [[ANSIX9.62](#)].

CGA Parameters and Digital Signature Option's CGA Parameters include 16 octet modifier, 8 octet prefix obtained from the router advertisement message sent from 6LBR, 1 octet collision count and 56 octet Public Key. Digital Signature is 72 octets. The option is 160

octets with Padding of 7 octets. The total message size of an original LSEND address registration NS message is 216 octets and such a message can be encapsulated into three 802.15.4 frames.

An address registration refresh NS message contains an ARO which is 16 octets and the digital signature option containing 16 octet key hash and 71 octet signature and 5 octet Padding. The message is 152 octets long with the header. Such a message could be encapsulated in two 802.15.4 frames.

6. Security Considerations

The same considerations regarding the threats to the Local Link Not Covered (as in [[RFC3971](#)]) apply.

The threats discussed in [Section 9.2 of \[RFC3971\]](#) are countered by the protocol described in this document as well.

As to the attacks to the protocol itself, denial of service attacks that involve producing a very high number of packets are deemed unlikely because of the assumptions on the node capabilities in low-power and lossy networks.

7. IANA considerations

This document defines two new options to be used in neighbor discovery protocol messages and new type values for CGA Parameters and Digital Signature Option (TBA1) and Digital Signature Option (TBA2) need to be assigned by IANA.

This document defines 0xE8C47FB7FD2BB885DAB2D31A0F2808B4 for LSEND CGA Message Type Tag.

8. Acknowledgements

Greg Zaverucha from RIM made contributions to this document.

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.

- [RFC3756] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", [RFC 3756](#), May 2004.
- [RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", [RFC 3971](#), March 2005.
- [RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", [RFC 3972](#), March 2005.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#), September 2007.
- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", [RFC 4862](#), September 2007.
- [RFC5480] Turner, S., Brown, D., Yiu, K., Housley, R., and T. Polk, "Elliptic Curve Cryptography Subject Public Key Information", [RFC 5480](#), March 2009.
- [RFC6775] Shelby, Z., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", [RFC 6775](#), November 2012.
- [SEC1] "Standards for Efficient Crptography Group. SEC 1: Elliptic Curve Cryptography Version 2.0", May 2009.
- [ANSIX9.62] "American National Standards Institute (ANSI), ANS X9.62-2005: The Elliptic Curve Digital Signature Algorithm (ECDSA)", November 2005.

9.2. Informative references

- [SEC2] "Standards for Efficient Crptography Group. SEC 2: Recommended Elliptic Curve Domain Parameters Version 2.0", January 2010.
- [FIPS-186-3] "National Institute of Standards and Technology, "Digital Signature Standard"", June 2009.
- [NIST-ST] "National Institute of Standards and Technology, "NIST Comments on Cryptanalytic Attackts on SHA-1"", January 2009,
<<http://csrc.nist.gov/groups/ST/hash/statement.html>>.

Authors' Addresses

Behcet Sarikaya (editor)
Huawei USA
5340 Legacy Dr. Building 3
Plano, TX 75024

Email: sarikaya@ieee.org

Frank Xia
Huawei Technologies Co., Ltd.
101 Software Avenue, Yuhua District
Nanjing, Jiangsu 210012, China

Phone: ++86-25-56625443
Email: xiayangsong@huawei.com

