6lo B. Sarikaya, Ed.
Internet-Draft Huawei USA
Intended status: Standards Track F. Xia
Expires: April 13, 2015 Huawei Technologies Co., Ltd.
October 10, 2014

Lightweight and Secure Neighbor Discovery for Low-power and Lossy Networks
draft-sarikaya-6lo-cga-nd-01

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

Copyright Notice

Table of Contents

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

6LowPAN neighbor discovery protocol [RFC6775] needs to be extended to make it secure and also for being more efficient as well as other use cases. Requirements on such enhancements are stated in [I-D.thubert-6lo-rfc6775-update-reqs].

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.

```
    0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     Type      |    Length     |   Pad  Length |  Sig. Length  |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    .                                                               .
    .                        CGA Parameters                         .
    .                                                               .
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    .                                                               .
    .                       Digital Signature                       .
    .                                                               .
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    .                                                               .
    .                           Padding                             .
    .                                                               .
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type

TBA1 for CGA Parameters and Digital Signature

Length

The length of the option (including the Type, Length, Pad Length, Signature Length, CGA Parameters, Digital Signature and Padding fields) in units of 8 octets.

Pad Length

The length of the Padding field.

Sig Length

The length of the Digital Signature field.

CGA Parameters

The CGA Parameters field is variable-length containing the CGA Parameters data structure described in Section 4 of [RFC3972].

Digital Signature

The Digital Signature field is a variable length field containing a Elliptic Curve Digital Signature Algorithm (ECDSA) signature (with SHA-256 and P-256 curve of [FIPS-186-3]). Digital signature is constructed as explained in Section 4.3.

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.

```
       0                   1                   2                   3
        0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |     Type      |    Length     |           Reserved            |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                                                               |
       |                          Key Hash                             |
       |                                                               |
       |                                                               |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                                                               |
       .                                                               .
       .                       Digital Signature                       .
       .                                                               .
       |                                                               |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                                                               |
       .                                                               .
       .                           Padding                             .
       .                                                               .
       |                                                               |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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 ECParameters 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 crypotographically generated address. An LSEND for LLN node MUST set the Extended Unique Identifier (EUI-64) field [Guide] in ARO to the rightmost 64 bits of its crypotographically generated address. The Subnet Prefix field of CGA Parameters MUST be set to the leftmost 64 bits of its crypotographically 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 successfuly 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.

```
     6LN                                                        6LBR
      |                                                          |
      |<-----------------------RA-------------------------------|
      |                                                          |
      |---------------NS with ARO and CGA Option--------------->|
      |                                                          |
      |<-----------------------NA with ARO----------------------|
      |                                                          |
      |---------------NS with ARO and Digital Signature Option->|
      |                                                          |
      |<-----------------------NA with ARO----------------------|
      |                                                          |
      |---------------NS with ARO and Digital Signature Option->|
      |                                                          |
      |<-----------------------NA with ARO----------------------|
```

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.

The overhead of LSEND is valid initially and in base LSEND, possibly after bootstrapping at the address registration neighbor solicitation message. It disappears after that as we explain below in Section 6 in case optimal LSEND is used.

6. Optimizations

In this section we present optimizations to the base LSEND defined above. We use EUI-64 identifier instead of source address in CGA calculations. We also extend LSEND operation to 6LoWPAN multihop network.

Digital signature and CGA are calculated over EUI-64 or interface id of the node. It is only done initially at once not repeated with every message the node sends. The calculation does not change even if the node has a new address since EUI-64 does not change. This means that this CGA can be used to claim multiple targets. The calculation is ECC based as described in Section 4.3.

Protocol interactions are as defined in Section 5. The address registration NS message contains CGA Parameters and Digital Signature Option defined in Section 4.1. The node MUST set the Extended Unique Identifier (EUI-64) field [Guide] in ARO to the crypotographically generated address. The Subnet Prefix field of CGA Parameters MUST be set to the 64-bit prefix in the RA message received from 6LBR. Source address MUST be set to the prefix concatenated with the node's crypotographically generated address. The Public Key field of CGA Parameters MUST be set to the node's ECC Public Key.

CGA calculated may need to be modified before it is used as EUI-64. The b2 bit or U/L or "u" bit MUST be set to zero for globally unique and b1 bit or I/G or "g" bit MUST be set to zero for unicast before using it in IPv6 address as the interface identifier. In LSEND, senders and receivers ignore any differences in the three leftmost bits and in bits 6 and 7 (i.e., the "u" and "g" bits) in the interface identifiers [RFC3972].

The Target Address field in NS message is set to the prefix concatenated with the node's crypotographically generated address. This address does not need duplicate address detection as EUI-64 is globally unique. So a host cannot steal an address that is already registered unless it has the key for the EUI-64. The same EUI-64 can thus be used to protect multiple addresses e.g. when the node receives a different prefix. The node adds CGA Parameters (including Public Key) and Digital Signature Option defined in Section 4.1 into NS message. The node sends the address registration option (ARO) which is set to the CGA calculated.

Protocol interactions given in xref target="Dynamic-fig"/> are modified a bit in that Digital Signature option with the public key and ARO are passed to and stored by the 6LR/6LBR on the first NS and not sent again the in the next NS.

The 6LR/6LBR ensures first-come/first-serve by storing the ARO and the cryptographical material correlated to the target being registered. Then, if the node is the first to claim any address it likes, then it becomes owner of that address and the address is bound to the CGA in the 6LR/6LBR registry. This procedure avoids the constrained device to compute multiple keys for multiple addresses. The registration process allows the node to tie all the addresses to

the same EUI-64 and have the 6LR/6LBR enforce first come first serve after that.

6.1. Multihop Operation

In multihop 6LoWPAN, 6LBR sends RAs with prefixes downstream and it is the 6LR that receives and relays them to the nodes. 6LR and 6LBR communicate with the ICMPv6 Duplicate Address Request (DAR) and the Duplicate Address Confirmation (DAC) messages. The DAR and DAC use the same message format as NS and NA with different ICMPv6 type values.

In LSEND we extend DAR/DAC messages to carry CGA Parameters and Digital Signature Option defined in Section 4.1.

In a multihop 6LoWPAN, the node exchanges the messages shown in Figure 1 with 6LR not with 6LBR. 6LBR must be aware of who owns an address (EUI-64) to defend the first user if there is an attacker on another 6LR. Because of this the content that the source signs and the signature needs to be propagated to the 6LBR in DAR message. For this purpose we need the DAR message sent by 6LR to 6LBR MUST contain CGA Parameters and Digital Signature Option carrying the CGA that the node calculates and its public key. DAR message also contains ARO.

It is possible that occasionally, 6LR may miss the node's CGA (that it received in ARO) or the crypto information (that it received in CGA Parameters and Digital Signature Option). 6LR should be able to ask for it again. This is done by restarting the exchanges shown in Figure 1. The result enables 6LR to refresh CGA and public key information that was lost. 6LR MUST send DAR message with CGA Parameters and Digital Signature Option and ARO to 6LBR. 6LBR as a reply forms a DAC message with the information copied from the DAR and the Status field is set to zero. With this exchange, the 6LBR can (re)validate and store the CGA and crypto information to make sure that the 6LR is not a fake.

7. 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.

8. 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.

9. Acknowledgements

Greg Zaverucha from RIM made contributions to this document. Comments from Pascal Thubert are appreciated.

10. References

10.1. 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 Crtptography Group. SEC 1: Elliptic Curve Cryptography Version 2.0", May 2009.

[Guide] "Guidelines for 64-bit global Identifier (EUI-64TM)", November 2012, <http://standards.ieee.org/develop/regauth/tut/eui64.pdf>.

[ANSIX9.62] "American National Standards Institute (ANSI), ANS X9.62-2005: The Elliptic Curve Digital Signature Algorithm (ECDSA)", November 2005.

10.2. Informative references

[SEC2] "Standards for Efficient Crtptography 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>.

[I-D.rafiee-6man-ssas] Rafiee, H. and C. Meinel, "A Simple Secure Addressing Scheme for IPv6 AutoConfiguration (SSAS)", draft-rafiee-6man-ssas-11 (work in progress), September 2014.

[I-D.thubert-6lo-rfc6775-update-reqs] Thubert, P., "Requirements for an update to 6LoWPAN ND", draft-thubert-6lo-rfc6775-update-reqs-04 (work in progress), August 2014.

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