6lo
Internet-Draft
Updates: 6775 (if approved)
Intended status: Standards Track
Expires: November 25, 2017

B. Sarikaya
Huawei USA
P. Thubert
Cisco
M. Sethi
Ericsson

May 24, 2017

Address Protected Neighbor Discovery for Low-power and Lossy Networks
draft-ietf-6lo-ap-nd-02

Abstract

This document defines an extension to 6LoWPAN Neighbor Discovery, RFC 6775. Nodes supporting this extension compute a cryptographic Owner Unique Interface ID and associate it with one or more of their Registered Addresses. Once an address is registered with a Cryptographic ID, only the owner of that ID can modify the anchor state information of the Registered Address, and Source Address Validation can be enforced.

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 November 25, 2017.

Table of Contents

1. Introduction

Neighbor discovery for IPv6 [RFC4861] and stateless address autoconfiguration [RFC4862] and their extensions are collectively referred to as the IPv6 Neighbor Discovery Protocol (IPv6 NDP). In order to enable IPv6 NDP operations over a constrained low-power and lossy network (LLN), "Neighbor Discovery optimizations for 6LoWPAN networks" [RFC6775] (6LoWPAN ND), reduces the use of multicast in the original protocol and introduces a unicast host address registration technique. The registration mechanism leverages a new Address Registration Option (ARO) that is carried in the unicast Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages between the 6LoWPAN Node (6LN) and the 6LoWPAN Router (6LR), as well as the Duplicate Address Request (DAR) and Duplicate Address Confirmation (DAC) messages between the 6LR and the 6LoWPAN Border Router (6LBR), which is the central repository of all the registered addresses in its domain.

The registration mechanism in 6LoWPAN ND [RFC6775] was created for the original purpose of Duplicate Address Detection (DAD), whereby use of an address would be granted as long as the address is not already present in the subnet (first come first serve). In order to validate address ownership, the registration mechanism enables the 6LR and 6LBR to correlate further claims for a registered address from the device to which it is granted with a Owner Unique Interface IDentifier (OUID). With 6LoWPAN ND, the OUID is derived from the MAC address of the device (EUI-64), which can be spoofed. Therefore, any node connected to the subnet and aware of a registered-address-to-OUID mapping may effectively fake the OUID, steal the address and attract the traffic for that address towards a different Node. In order to allow a more secured registration mechanism, the "Update to 6LoWPAN ND" [I-D.ietf-6lo-rfc6775-update] opens the semantics of the ARO option and allows to transport alternate forms of OUIDs.

With this specification, a 6LN generates a cryptographic ID (Crypto-ID) and places it in the OUID field in the registration of one (or more) of its addresses with the 6LR(s) that it uses as default router(s). Proof of ownership of the cryptographic ID (Crypto-ID) is passed with the first registration to a given 6LR, and enforced at the 6LR, in a new Crypto-ID Parameters Option (CIPO). The 6LR validates ownership of the cryptographic ID upon the creation of a registration state, or a change in the anchor information, such as Link-Layer Address and associated Layer-2 cryptographic material.

The protected address registration protocol proposed in this document enables the enforcement of Source Address Validation (SAVI) [RFC7039], which ensures that only the correct owner uses a registered address in the source address field in IPv6 packets. With this specification, a 6LN that sources a packet has to use a 6LR to which the source address of the packet is registered to forward the packet. The 6LR maintains state information for the registered addressed along with the MAC address, and link-layer cryptographic key associated with that node. In SAVI-enforcement mode, the 6LR allows only packets from a connected Host if the connected Host owns the registration of the source address of the packet.

The 6lo adaptation layer framework ([RFC4944], [RFC6282]) expects that a device forms its IPv6 addresses based on Layer-2 address, so as to enable a better compression. This is incompatible with "Secure Neighbor Discovery (SEND)" [RFC3971] and "Cryptographically Generated Addresses (CGAs)" [RFC3972], which derive the Interface ID (IID) in the IPv6 addresses from cryptographic material. "Privacy Considerations for IPv6 Address Generation Mechanisms" [I-D.ietf-6man-ipv6-address-generation-privacy] places additional recommendations on the way addresses should be formed and renewed.

This specification allows a device to form and register addresses at will, without a constraint on the way the address is formed or the number of addresses that are registered in parallel. It enables to protect multiple addresses with a single cryptographic material and to send the proof only once to a given 6LR for multiple addresses and refresher registrations.

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].

Readers are expected to be familiar with all the terms and concepts that are discussed in [RFC3971], [RFC3972], [RFC4861], [RFC4919], [RFC6775], and [I-D.ietf-6lo-backbone-router] which proposes an evolution of [RFC6775] for wider applicability.

This document defines Crypto-ID as an identifier of variable size which in most cases is 64 bits long. It is generated using cryptographic means explained later in this document.

The document also conforms to the terms and models described in [RFC5889] and uses the vocabulary and the concepts defined in [RFC4291] for the IPv6 Architecture.

This document uses [RFC7102] for Terminology in Low power And Lossy Networks.

3. Updating RFC 6775

With this specification, a node SHOULD use a cryptographic identifier (Crypto-ID) as OUID in its registration; the Crypto-ID is calculated as described in Section 4.1. The fact that a OUID is a Crypto-ID is indicated in a new 'C' flag in the NS(ARO) message.

This specification also introduces a new option, the CIPO, that is used to prove ownership of the Crypto-ID. A node that registers for the first time to a 6LR SHOULD place a CIPO option to its registration but is not expected to place the option in the next periodic refresher registrations for that address, or for the registration of other addresses with the same OUID. When a 6LR receives a NS(ARO) registration with a new Crypto-ID as a OUID, then it SHOULD challenge by responding with a NA(ARO) with a status of "Proof requested". This whole process MAY be skipped in networks where there is no or ultra low expectations of mobility.

The challenge will also be triggered in the case of a registration for which the Source Link-Layer Address is not consistent with a state that already exists either at the 6LR or the 6LBR. In the latter case, the 6LBR returns a status of "Proof requested" in the DAR/DAC exchange, which is echoed by the 6LR in the NA (ARO) back to the registering node. This flow should not alter a preexisting state in the 6LR or the 6LBR.

Upon a NA(ARO) with a status of "Proof requested", the registering node SHOULD retry its registration with a CIPO option that proves its ownership of the Crypto-ID.

If the 6LR cannot validate the proof, it responds with a status of "Incorrect Proof". Upon a NA(ARO) with a status of "Incorrect Proof", the registering node SHOULD NOT use this Crypto-ID for registering with that 6LR anymore.

4. New Fields and Options

4.1. New Crypto-ID

Elliptic Curve Cryptography (ECC) is used in the calculation of the Crypto-ID. The digital signature is constructed by using the 6LN's private key over its EUI-64 (MAC) address. The signature value is computed using the ECDSA signature algorithm and the hash function used is SHA-256 [RFC6234]. Public Key is the most important parameter in CGA Parameters (sent by 6LN in an NS message). 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 can further reduce the key size by about 32 octets.

First, the modifier is set to a random or pseudo-random 128-bit value. Next, concatenate from left to right the modifier, 9 zero octets and the ECC public key. SHA-256 algorithm is applied on the concatenation. The 112 leftmost bits of the hash value is taken. Concatenate from left to right the modifier value, the subnet prefix and the encoded public key. NIST P-256 is executed on the concatenation. The leftmost bits of the result is used as the Crypto-ID. With this specification, the last 64 bits are retained, but it could be expanded to more bits in the future by increasing the size of the OUID field.

In respecting the cryptographic algorithm agility [RFC7696], Curve 25519 [RFC7748] can also be used instead of NIST P-256. This is indicated by 6LN by setting the Crypto Type field in the CIPO option to a value of 1. If 6LBR does not support Curve 25519, it will set

Crypto Type field to zero. This means that the default algorithm (NIST P-256) will be used.

4.2. Updated EARO

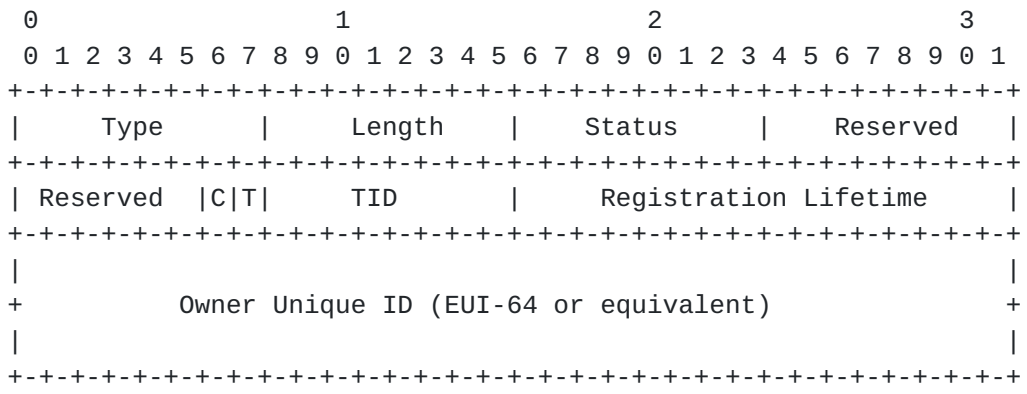

Figure 1: Enhanced Address Registration Option

Type:

33

Length:

8-bit unsigned integer. The length of the option (including the type and length fields) in units of 8 bytes.

Status:

8-bit unsigned integer. Indicates the status of a registration in the NA response. MUST be set to 0 in NS messages. This specification leverages values introduced in the Update to 6LoWPAN ND [I-D.ietf-6lo-rfc6775-update], such as 5: Proof Requested, and does not require additional values to be defined.

Reserved:

This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

C:

This specification introduces a C bit, which is set to indicate that the Owner Unique ID field contains a Crypto-ID.

T and TID:

Defined in [I-D.ietf-6lo-rfc6775-update].

Owner Unique ID:

When using this specification, this field contains a Crypto-ID.

4.3. New Crypto-ID Parameters Option

This specification introduces a new option, the Crypto-ID Parameters Option (CIPO), that carries the proof of ownership of a crypto-ID.

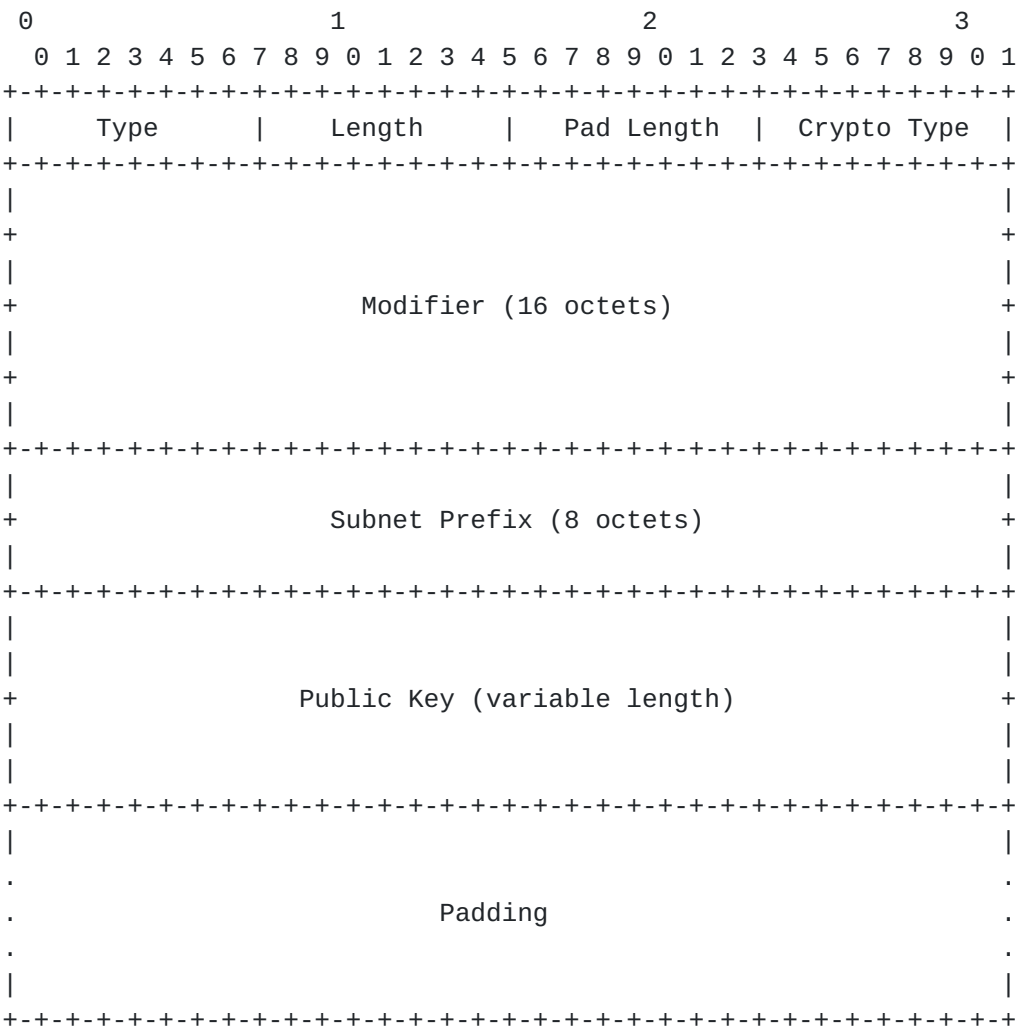

Figure 2: Crypto-ID Parameters Option

Type:

CIPO, to be assigned by IANA.

Length:

The length of the option in units of 8 octets.

Pad Length:

The length of the Padding field.

Crypto Type:

The type of cryptographic algorithm used in calculation Crypto-ID. Default value of all zeros indicate NIST P-256. A value of 1 is assigned for Curve 25519. New values may be defined later.

Modifier:

128 bit random value.

Subnet Prefix:

64 bit subnet prefix.

Public Key:

ECC public key of 6LN.

Padding:

A variable-length field making the option length a multiple of 8, containing as many octets as specified in the Pad Length field.

5. Protocol Overview

5.1. Protocol Scope

The scope of the present work is a 6LoWPAN Low Power Lossy Network (LLN), typically a stub network connected to a larger IP network via a Border Router called a 6LBR per [RFC6775].

The 6LBR maintains a registration state for all devices in the attached LLN, and, in conjunction with the first-hop router (the 6LR), is in a position to validate uniqueness and grant ownership of an IPv6 address before it can be used in the LLN. This is a fundamental difference with a classical network that relies on IPv6 address auto-configuration [RFC4862], where there is no guarantee of

ownership from the network, and any IPv6 Neighbor Discovery packet must be individually secured [RFC3971].

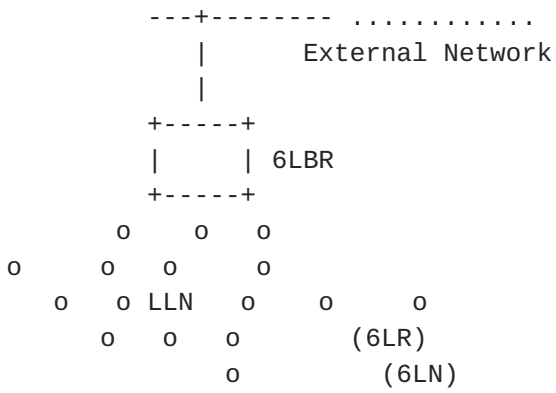

Figure 3: Basic Configuration

In a mesh network, the 6LR is directly connected to the host device. This specification expects that the peer-wise layer-2 security is deployed so that all the packets from a particular host are securely identifiable by the 6LR. The 6LR may be multiple hops away from the 6LBR. Packets are routed between the 6LR and the 6LBR via other 6LRs. This specification expects that a chain of trust is established so that a packet that was validated by the first 6LR can be safely routed by the next 6LRs to the 6LBR.

5.2. Protocol Flows

The 6TiSCH Architecture [I-D.ietf-6tisch-architecture] suggests to use of RPL [RFC6550] as the routing protocol between the 6LRs and the 6LBR. In that model, a registration flow happens as shown in Figure 4.

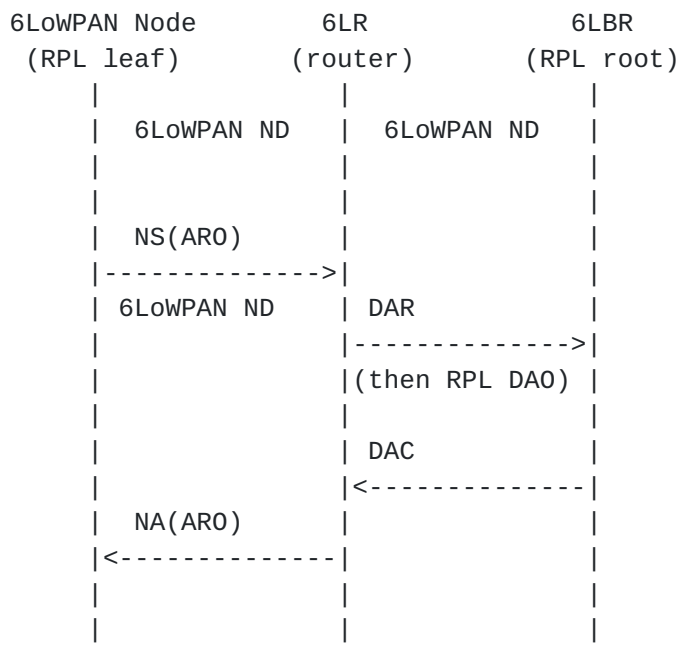

Figure 4: (Re-)Registration Flow

A new device that joins the network auto-configures an address and performs an initial registration to an on-link 6LR with an NS message that carries an Address Registration Option (ARO) [RFC6775]. The 6LR validates the address with the central 6LBR using a DAR/DAC exchange, and the 6LR confirms (or denies) the address ownership with an NA message that also carries an Address Registration Option.

In a multihop 6LoWPAN, the registration with Crypto-ID is propagated to 6LBR as described in Section 5.3. If a chain of trust is present between the 6LR and the 6LBR, then there is no need to propagate the proof of ownership to the 6LBR. All the 6LBR needs to know is that this particular OUID is randomly generated, so as to enforce that any update via a different 6LR is also random.

Local or on-link protocol interactions are shown in Figure 5. Crypto-ID and ARO are passed to and stored by the 6LR/6LBR on the first NS and not sent again in the next NS. The operation starts with 6LR sending a Router Advertisement (RA) message to 6LN.

The 6LR/6LBR ensures first-come/first-serve by storing the ARO and the Crypto-ID correlated to the node being registered. The node is free to claim any address it likes as long as it is the first to make such a claim. After a successful registration, the node becomes the owner of the registered address and the address is bound to the Crypto-ID in the 6LR/6LBR registry. This binding can be verified later, which prevents other nodes from stealing the address and

trying to attract traffic for that address or use it as their source address.

A node may uses multiple IPv6 addresses at any time. This condition may happen for privacy reasons [I-D.ietf-6man-ipv6-address-generation-privacy], or when the node moves at a different place and auto-configures an new address from a different prefix. In those situations, the node may use the same Crypto-ID to protect multiple IPv6 addresses. The separation of the address and the Crypto-ID avoids the constrained device to compute multiple keys for multiple addresses. The registration process allows the node to tie all of its addresses to the same Crypto-ID and have the 6LR/6LBR enforce first-come first-serve after that.

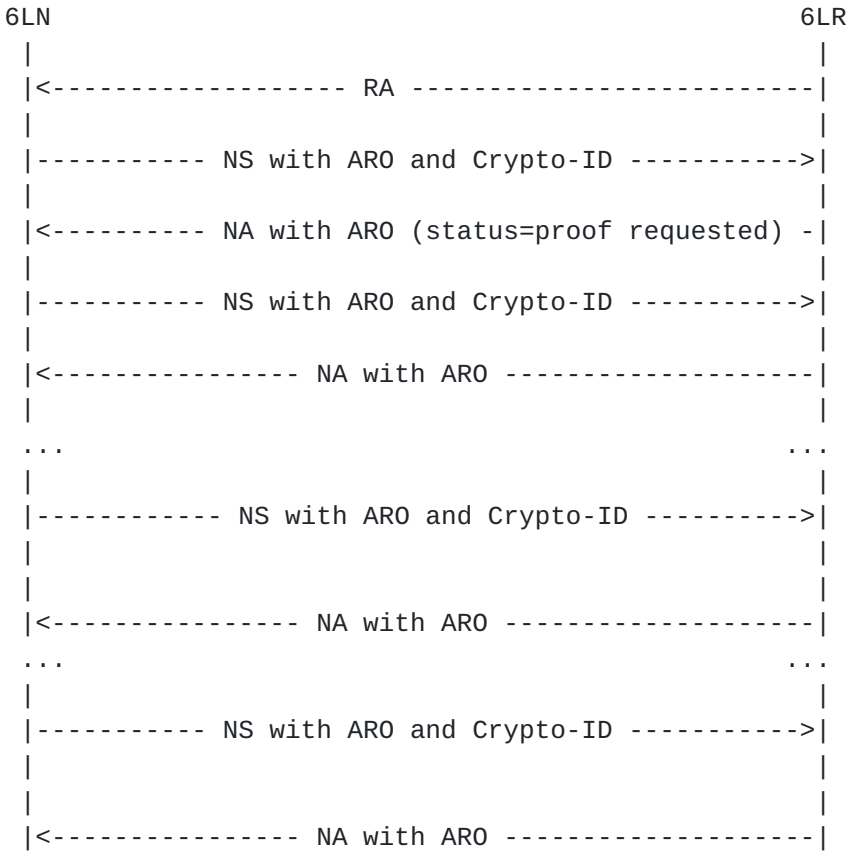

Figure 5: On-link Protocol Operation

5.3. 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 ND-PAR we extend DAR/DAC messages to carry cryptographically generated OUID. In a multihop 6LoWPAN, the node exchanges the messages shown in Figure 4. The 6LBR must be aware of who owns an address (EUI-64) to defend the first node 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 the DAR message sent by 6LR to 6LBR MUST contain the CIPO option. DAR message also contains ARO.

It is possible that occasionally, a 6LR may miss the node's OUID (that it received in ARO). 6LR should be able to ask for it again. This is done by restarting the exchanges shown in Figure 5. The result enables 6LR to refresh the information that was lost. 6LR MUST send DAR message with 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 information to make sure that the 6LR is not a fake.

In some cases 6LBR may use DAC message to signal to 6LR that it expects Crypto-ID from 6LR also asks 6LR to verify the EUI-64 6LR received from 6LN. This may happen when a 6LN node is compromised and a fake node is sending the Crypto-ID as if it is the node's EUI-64. Note that the detection in this case can only be done by 6LBR not by 6LR.

6. Security Considerations

The observations regarding the threats to the Local Link Network in [RFC3971] also apply to this specification.

This document inherits threats discussed in 6LoWPAN ND [RFC6775] and its update [I-D.ietf-6lo-rfc6775-update] and addresses the potential attacks related to address stealing and spoofing within a LLN. Compared with SeND, this specification saves about 1Kbyte in every NS/NA message. Also, this specification separates the cryptographic identifier from the registered IPv6 address so that a node can have more than one IPv6 address protected by the same cryptographic identifier. SeND forces the IPv6 address to be cryptographic since it integrates the CGA as the IID in the IPv6 address. This specification frees the device to form its addresses in any fashion, so as to enable the classical 6LoWPAN compression which derives IPv6 addresses from Layer-2 addresses, as well as privacy addresses.

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

Collisions of Crypto-ID is a possibility that needs to be considered. The formula for calculating probability of a collision is 1 - e^{-k^2/(2n)}. If the Crypto-ID is 64-bit long, then the chance of finding a collision is 0.01% when the network contains 66 million nodes. It is important to note that the collision is only relevant when this happens within one stub network (6LBR). A collision of ID in ND-PAR is a rare event. However, when such a collision does happen, the protocol operation is not affected, although it opens a window for a node to hijack an address from another. The link-layer security ensures that the nodes would normally not be aware of a collision on the subnet. If a malicious node is able to gain knowledge of a collision through other means, the only thing that it could do is to steal addresses from the other honest node. This would be no different from what is already possible in a 6lo network today.

7. IANA considerations

IANA is requested to assign two new option type values for the CIPO under the subregistry "IPv6 Neighbor Discovery Option Formats".

8. Acknowledgements

We are grateful to Rene Struik and Robert Moskowitz for their comments that lead to many improvements to this document.

9. Change Log

- submitted version -00 as a working group draft after adoption, and corrected the order of authors
- submitted version -01 with no changes
- submitted version -02 with these changes: Moved Requirements to Appendix A, Section 4.2 moved to Section 3, New section 4 on New Fields and Options, Section 4 changed to Protocol Overview as Section 5 with Protocol Scope and Flows subsections.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <http://www.rfc-editor.org/info/rfc4291>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <http://www.rfc-editor.org/info/rfc4861>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <http://www.rfc-editor.org/info/rfc4862>.

[RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012, <http://www.rfc-editor.org/info/rfc6775>.

[I-D.ietf-6lo-rfc6775-update] Thubert, P., Nordmark, E., and S. Chakrabarti, "An Update to 6LoWPAN ND", draft-ietf-6lo-rfc6775-update-05 (work in progress), May 2017.

10.2. Informative references

[RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <http://www.rfc-editor.org/info/rfc3971>.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, DOI 10.17487/RFC3972, March 2005, <http://www.rfc-editor.org/info/rfc3972>.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007, <http://www.rfc-editor.org/info/rfc4944>.

[RFC6282] Hui, J., Ed. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, DOI 10.17487/RFC6282, September 2011, <http://www.rfc-editor.org/info/rfc6282>.

[RFC4919] Kushalnagar, N., Montenegro, G., and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", RFC 4919, DOI 10.17487/RFC4919, August 2007, <http://www.rfc-editor.org/info/rfc4919>.

[RFC5889] Baccelli, E., Ed. and M. Townsley, Ed., "IP Addressing Model in Ad Hoc Networks", RFC 5889, DOI 10.17487/RFC5889, September 2010, <http://www.rfc-editor.org/info/rfc5889>.

[RFC6234] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, DOI 10.17487/RFC6234, May 2011, <http://www.rfc-editor.org/info/rfc6234>.

[RFC6550] Winter, T., Ed., Thubert, P., Ed., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, DOI 10.17487/RFC6550, March 2012, <http://www.rfc-editor.org/info/rfc6550>.

[RFC7102] Vasseur, JP., "Terms Used in Routing for Low-Power and Lossy Networks", RFC 7102, DOI 10.17487/RFC7102, January 2014, <http://www.rfc-editor.org/info/rfc7102>.

[RFC7039] Wu, J., Bi, J., Bagnulo, M., Baker, F., and C. Vogt, Ed., "Source Address Validation Improvement (SAVI) Framework", RFC 7039, DOI 10.17487/RFC7039, October 2013, <http://www.rfc-editor.org/info/rfc7039>.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <http://www.rfc-editor.org/info/rfc7217>.

[RFC7696] Housley, R., "Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms", BCP 201, RFC 7696, DOI 10.17487/RFC7696, November 2015, <http://www.rfc-editor.org/info/rfc7696>.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <http://www.rfc-editor.org/info/rfc7748>.

[I-D.ietf-6lo-backbone-router]
Thubert, P., "IPv6 Backbone Router", draft-ietf-6lo-backbone-router-03 (work in progress), January 2017.

[I-D.ietf-6tisch-architecture]
Thubert, P., "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4", draft-ietf-6tisch-architecture-11 (work in progress), January 2017.

[I-D.ietf-6man-ipv6-address-generation-privacy]
Cooper, A., Gont, F., and D. Thaler, "Privacy Considerations for IPv6 Address Generation Mechanisms", draft-ietf-6man-ipv6-address-generation-privacy-08 (work in progress), September 2015.

Appendix A. Requirements Addressed in this Document

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]. RFC6775 utilizes optimizations such as host-initiated interactions for sleeping resource-constrained hosts and elimination of multicast address resolution.

- New options to be added to Neighbor Solicitation messages MUST lead to small packet sizes, especially compared with existing protocols such as SEcure Neighbor Discovery (SEND). Smaller packet sizes facilitate low-power transmission by resource-constrained nodes on lossy links.

- The support for this registration mechanism SHOULD be extensible to more LLN links than IEEE 802.15.4 only. Support for at least the LLN links for which a 6lo "IPv6 over foo" specification exists, as well as Low-Power Wi-Fi SHOULD be possible.

- As part of this extension, a mechanism to compute a unique Identifier should be provided with the capability to form a Link Local Address that SHOULD be unique at least within the LLN connected to a 6LBR.

- The Address Registration Option used in the ND registration SHOULD be extended to carry the relevant forms of Unique Interface IDentifier.

- The Neighbour Discovery should specify the formation of a site-local address that follows the security recommendations from [RFC7217].

Authors' Addresses

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

Email: sarikaya@ieee.org

Pascal Thubert
Cisco Systems, Inc
Building D
45 Allee des Ormes - BP1200
MOUGINS - Sophia Antipolis 06254
FRANCE

Phone: +33 497 23 26 34
Email: pthubert@cisco.com

Mohit Sethi
Ericsson
Hirsalantie
Jorvas 02420

Email: mohit@piuha.net