Address Protected Neighbor Discovery for Low-power and Lossy Networks

draft-sarikaya-6lo-ap-nd-02

Behcet Sarikaya, Pascal Thubert
IETF 95

Buenos Aires
SeND for 6LoWPAN?

Address Spoofing

Need for defense against spoofing like classical ND? IEEE appears to think so (Dorothy’s presentation Sunday)
Attack is not on NS lookup since we use not onlink model
Spoofing happens at registration time
From devices with a join key (misplaced trust, compromised)
Thus the need to ensure first come first serve registration
Proposal

Cryptographic token proving identity

Used as a replacement for the MAC address in ARO
State in 6LR/6LBR associates first come with token
Could be a RSA public key but that’s at least 384 bits
That’s potentially a lot of state at the 6LR
CGA has IPR

Suggestion: use private key on MAC address (SLLAO) and ECC
What changed since 01

• Added <Updates: 6775 (if approved)>
• New/updated section 4.2. Updating RFC 6775
• Added comparison with SeND
  => this specification saves ~1Kbytes in every NS/NA
• Added crypto ID computation and a bit in the ARO indicating crypto ID
Questions

Do people see that address spoofing may occur in IOT?

Is this a valid approach?

Where do we go from here?
FIRST REGISTRATION
LP Node → 6LR → 6LBR → 6BBR

Radio 1 Hop

NS (ARO)
SRC = LPN_II *
DST = 6LR
TGT = LPN **
TLLA = LPN
TID included
UID = cryptoUID

* link local addr based on EUI-64 or registered address if legacy 6LR
** registered address, same cryptoUID for all

DAR (ARO)
SRC = 6LR *
DST = 6LBR
REG = LPN
TID included
UID = cryptoUID

* Global / ULA

Create binding state

NS (ARO)
SRC = 6LBR
DST = 6BBR *
TGT = LPN
TLLA = L6BR
TID included
UID = cryptoUID

* Can be Anycast

Create proxy state

NS DAD (ARO)
SRC = UNSPEC
DST = SNMA
TGT = LPN
TID included
UID = cryptoUID

* Can be Anycast

Registered address, same cryptoUID for all
**Network Design**

- **LP Node**
  - Radio 1 Hop

- **6LR**
  - RPL

- **6LBR**
  - Ethernet

- **6BBR**
  - Ethernet

- **DAD time out**
  - NA (O) *

**Routing Path**

- **SRC = 6LR**
  - **DST = 6LBR**
  - **REG = LPN**
  - TID included
  - **UID = cryptoUID**

- **SRC = 6LR_ll**
  - **DST = LPN_ll**
  - **TGT = LPN**
  - TID included
  - **UID = cryptoUID**

- **SRC = 6BBR**
  - **DST = 6LBR**
  - **TGT = LPN**
  - **TLLA = L6BR**
  - TID included
  - **UID = cryptoUID**

- **SRC = 6BBR_ll** **
  - **DST = NS SRC**
  - **TLLA = L6BR**
  - **TGT = LPN**
  - **UID = cryptoUID**

* Omitted in general
** link local
If trust between 6LR and 6LBR no Need to carry proof All the way

If Policy to check cryptoUID on first use

Check Crypto proof

DAR (ARO, proven bit)

DAC (ARO)

Status= 0 (OK)

Proof ~1Kb

Status= 5 (validate)

NA (ARO)

NS (ARO)

Status= 0 (OK)

NA (ARO)

NS (ARO)
Collision of binding state
Same UID for addr. LPN
Either original or this registration indicates UID is a cryptoID
No state change at this time

Status= 5 (validate)

Check Crypto proof valid
Proof ~1Kb

Status= 0 (OK)

DAR(ARO, proven bit)

Status= 0 (OK)

Collision of binding state
Same UID for addr. LPN
Proven bit set
State updated as if it is a movement
Collision of binding state
Same UID for addr. LPN
Either original or this registration indicates UID is a cryptoID
No state change at this time

Collision of binding state
Same UID for addr. LPN
Proven bit set
State updated as if it is a movement
Collision of binding state
Same UID for addr. LPN
Either original or this registration indicates UID is a cryptoID
No state change at this time

Unlikely to occur