Address Protected Neighbor Discovery for Low-power and Lossy Networks

draft-sarikaya-6lo-ap-nd-01

Behcet Sarikaya, Pascal Thubert
IETF 94

Yokohama, October 2015
Address Spoofing

Need for defense against spoofing like classical ND?
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
Draft operation

Crypto ID passed in ARO, DAR, DAC

Q: Should we hide it in EUI-64?

Public key & “CGA parms” passed on demand to the 6LR for verification

Never needed if no movement

Movement can be indicated by 6LBR in DAC
Ask 6lo to decide if

Real problem?
Valid approach?