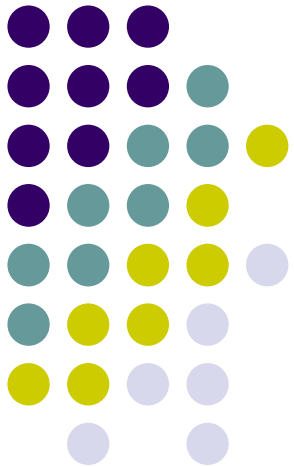
Lightweight and Secure Neighbor Discovery for Low-power and Lossy Networks

Behcet Sarikaya(sarikaya@ieee.org)
Frank Xia (xiayangsong@huawei.com)
IETF 90

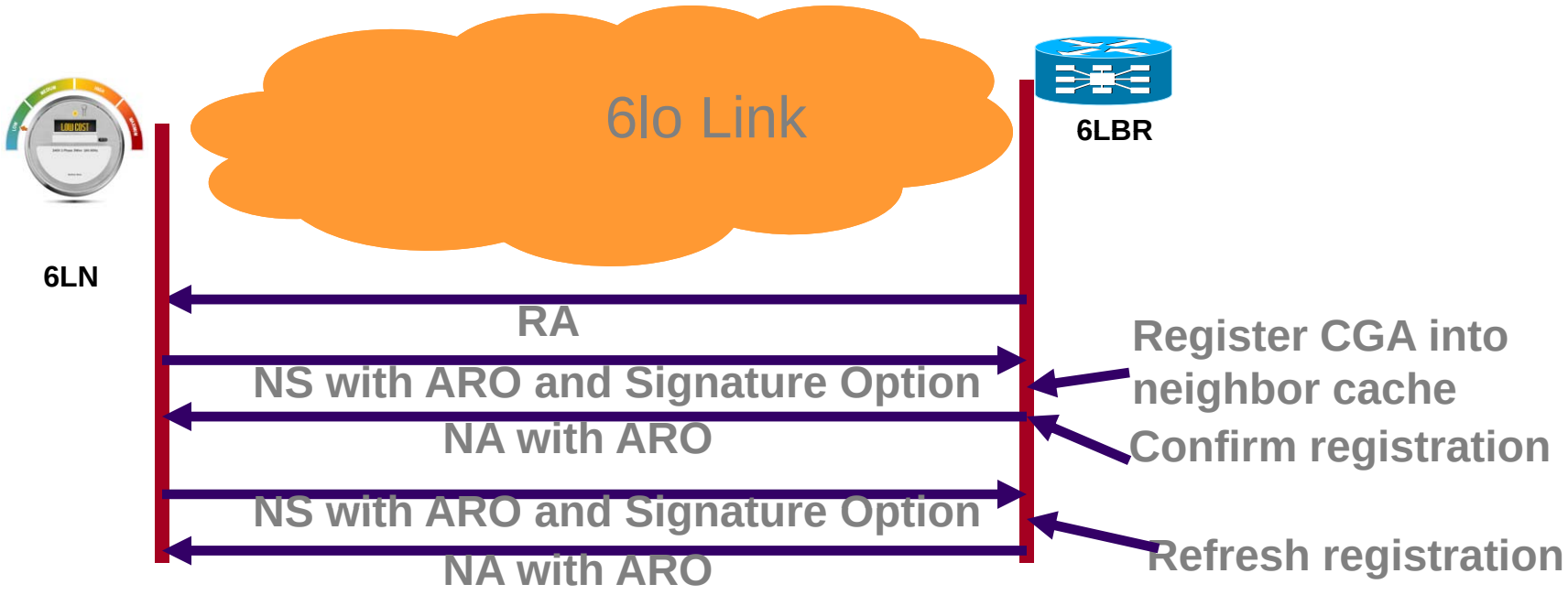


draft-sarikaya-6lo-cga-nd-00

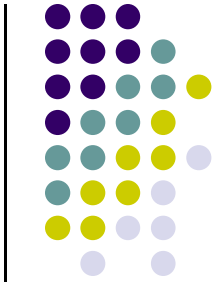
Lightweight Secure Neighbor Discovery for Low-power and Lossy Networks (LSEND) Motivation

- 6LoWPAN ND is not secure and subject to attacks, it needs to be secured
- Secure 6LoWPAN ND can not use SeND directly because SeND uses computationally heavy cryprographical algorithms, etc.
- Simple extension to SeND (RFC 3971 & 3972) is needed
  - Use Elliptic Curve Cryptography public keys
  - Use SHA-2
  - Use efficient design

LSEND Operation



Discussion



- Proposed on the list:
  - change SeND to use the Owner Interface Identifier (UII) for the CGA calculation as opposed to the source address.
  - Pros: UII is more stable and a device could register all its addresses with a single CGA-based UII / keypair
  - Note: UII is the target of NS
- Proposed on the list:
  - The signed material from the NS(ARO) must be passed as is into the DAR message (by 6LR in multihop deployments) so the 6LBR can (re)validate and store so as to make sure that the 6LR is not a fake
  - On exceptional loss, a 6LR that is missing the crypto information should be able to ask for it again
- What does WG think about these proposals?