An Extension to Mesh Link Establishment (MLE) for Host Identity Protocol Diet Exchange (HIP DEX)

draft-ohba-mle-hip-dex-00

Yoshihiro Ohba

Background

- HIP DEX (Host Identity Protocol Diet EXchange) [I-D.moskowitz-hip-dex] is a light-weight key exchange protocol designed for constrained devices
  - 4-way handshake for authenticated static ECDH to establish session key materials
- MLE (Mesh Link Establishment) [I-D.kelsey-intarea-mesh-link-establishment] is defined for establishing and configuring secure links in IEEE 802.15.4 mesh networks
  - 3-way handshake for exchanging PSK-based authenticated link-layer parameters such as a frame counter
- Integration of HIP DEX and MLE can make
  - MLE support keying with public-key based mutual authentication
  - total handshake of HIP DEX and MLE 5-way (or 2.5 roundtrips), instead of 7-way (or 3.5 roundtrips)

Example Use Case: ZigBee NAN (Neighborhood Area Network)

- ZigBee NAN: a 6LoWPAN-basd mesh network stack (up to Network Layer) intended for AMI (Advanced Metering Infrastructure)
  - IEEE 802.15.4g PHY and IEEE 802.15.4e MAC
  - RPL for routing (RFC 6550)
  - MPL for multicast (I-D.ietf-roll-trickle-mcast)

Proposal: HIP DEX over MLE

- A HIP DEX message is encapsulated in an MLE message as a HIP TLV
- Two phases:
  - Key Establishment Phase: to establish a HIP DEX SA
  - Key Update Phase: to update the HIP DEX SA
- Optional feature to distribute X.509 CRL (Certificate Revocation List)

Key Establishment Phase

MLE messages marked * are protected by MLE itself

```
(EI)   (ER)
   -->     Advertisement [HIP{DEX-I1}, Link Quality]

   <--     Advertisement [HIP{DEX-R1}, Link Quality]

   -->     Link Request  [HIP{DEX-I2}, Source Address, Mode,
                          Timeout, Challenge]*

   <--     Link Accept and Request
                         [HIP{DEX-R2}, LLFC, MLFC, Source Address, Mode,
                          Timeout, Response, Challenge]*

   -->     Link Accept   [LLFC, MLFC, Response]*
```

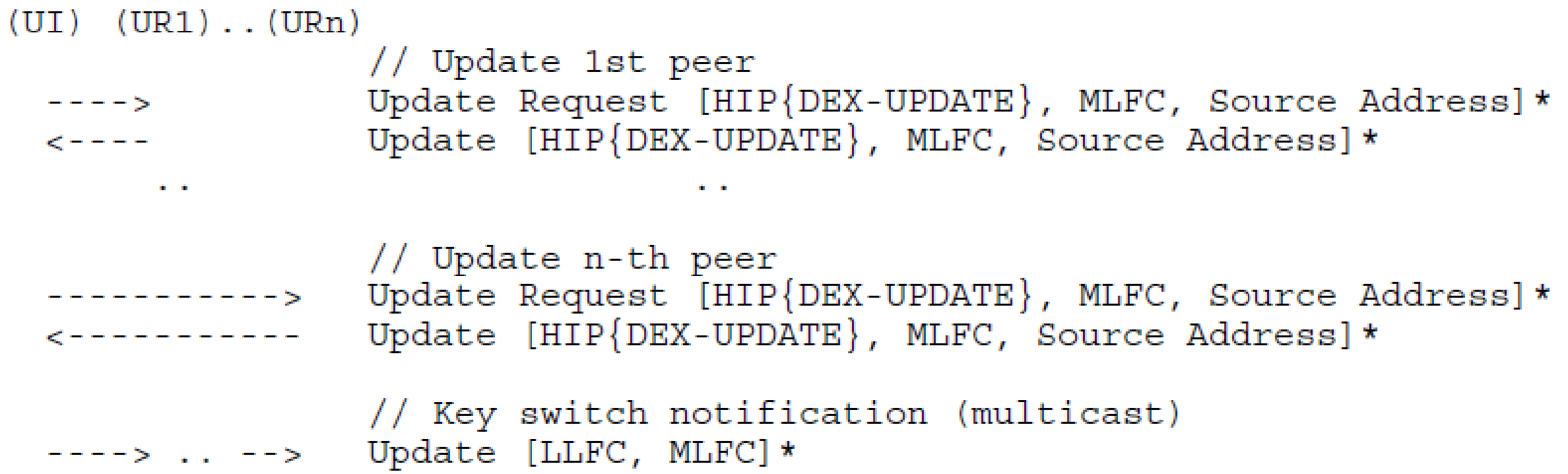
Keys established (besides DH shared secret):

- Group keys: GroupL2Key, GroupMLEKey
- Pairwise keys: L2 unicast key

EI: HIP DEX Key Establishment Initiator
ER: HIP DEX Key Establishment Responder
DEX-I1, DEX-R1, DEX-I2, DEX-R2: HIP DEX I1, R1, I2, R2 messages
LLFC: Link-Layer Frame Counter
MLFC: MLE Frame Counter

Key Update Phase

MLE messages marked * are protected by MLE itself



UI: HIP DEX Key Update Initiator
UR: HIP DEX Key Update Responder
DEX-I1, DEX-R1, DEX-I2, DEX-R2: HIP DEX I1, R1, I2, R2 messages
LLFC: Link-Layer Frame Counter
MLFC: MLE Frame Counter

MLE Security

- Reuses IEEE 802.15.4 security based on AES-CCM*

- Parameters
  - Key: GroupMLEKey
  - Key Identifier Mode: 0x03
  - 5-octet Frame Counter
  - Default security level: MIC-64

- Several considerations due to optimized messaging, including recommended use of OOB mechanism for certificate update

Next Step

- ZigBee NAN WG uses this draft in their profile specification
- This draft has dependency on MLE [I-D.kelsey-intarea-mesh-link-establishment], which is currently in dead state
  - A requirement on reviving MLE draft is coming from ZigBee NAN WG
- Intended status: Experimental RFC
  - Feedback from 6lo WG is appreciated