Group Keying For TRILL

draft-eastlake-trill-group-keying

Donald E. Eastlake, III

Huawei Technologies

d3e3e3@gmail.com

Security

- TRILL standardizes communications protocols that sometimes need encryption and authentication services. Such services require that cryptographic keying material be distributed.
- Modern security standards impose a number of requirements on keying including a limited lifetime on keys.

Security

- Existing TRILL specified security is unicast:
  - Unicast security is pretty simple but you want session keys to exist only at the two end points.
  - TRILL uses existing point-to-point security and pairwise secret key negotiation:
    - RBridge Channel messages: [RFC7178] extended to add DTLS unicast security by [RFC7978].
    - TRILL over IP [draft-ietf-trill-over-ip] unicast IPsec security with IKEv2 key negotiation.

Multicast

- Where multicast / broadcast is supported, it can be inherently more efficient, decreasing link and source port utilization.
  - The RBridge Channel facility inherently supports multi-destination packets scoped by data label (VLAN or FGL).
  - Some IP networks/links support native IP multicast.

Multicast Security

- Possible Approaches
  1. You can just serially unicast to all the intended destinations but you lose the advantages of multicast and need to know who all destination are.
  2. You can distribute a shared secret key to all the group members. This is efficient but now any group member can forge packets as if they were from another group member

Multicast Security

- Approaches (continued)
  3. You can use public key cryptography with each packet. This supports good encryption and authentication but this is inefficient.
  4. You can perhaps do more exotic things.

TRILL Multicast Security

- The idea is for TRILL to initially support approach 2, a shared secret key.
- For networks where the diminished authentication of not protecting which group member originated a packet is a problem, they can always fall back to serial unicast.

Group Keying Protocol

- draft-eastlake-trill-group-keying specifies messages for a designated group member to distribute shared secret keying material to all other group members.
  - A companion draft will profile thisfor RBridge Channel messages and TRILL over IP.

Group Keying Protocol

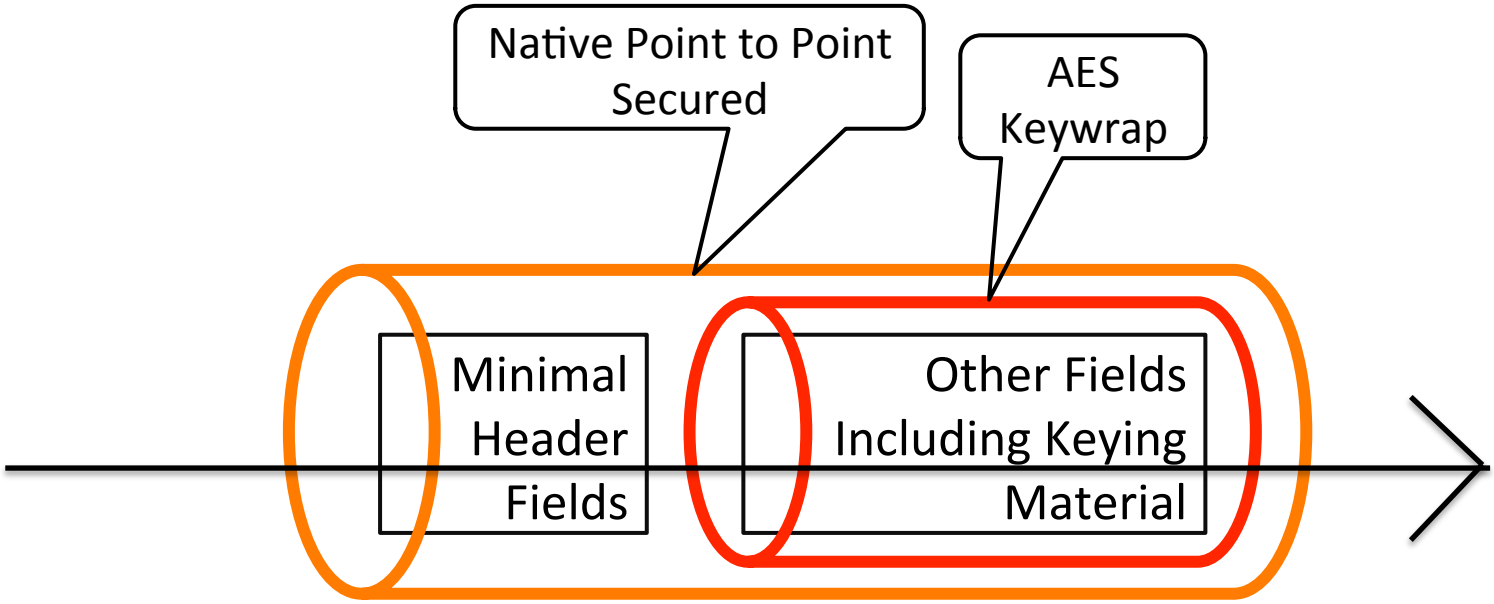
- draft-eastlake-trill-group-keying:
  - Leverages pairwise keying, which it assumes is already in place at least between the designated group member and all other group members.
  - Assumes group keying will be profiled for each application by specification of at least
    - the envelope around the group keying messages.
    - how the designated group member is determined

Group Keying Protocol

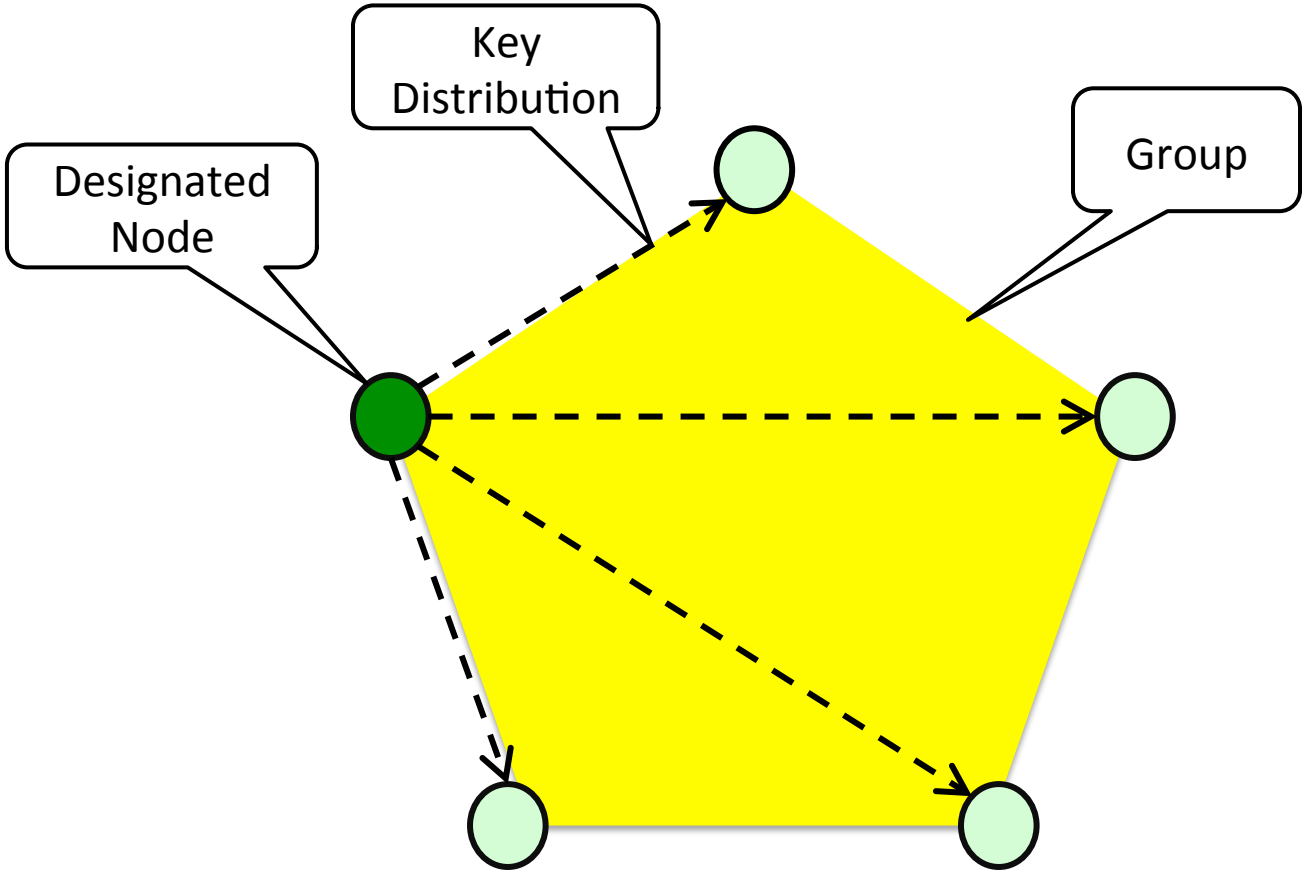
- draft-eastlake-trill-group-keying (cont):
  - Provides for key identifiers so you can pre-position the next key before switching to it and deprecating the current key. This avoid a dropout when doing a key rollover.
- Note: All this just relates to keying. The actual secured packet formats and cryto algroithms for encryption and authentication are unchanged.

Group Keying Protocol

Group Keying
Message Structure



Group Keying Protocol



END

Donald E. Eastlake, III
Huawei Technologies
d3e3e3@gmail.com