KMP for IEEE 802.15

Adding Key Management for the IEEE 802.15 MAC Security

Robert Moskowitz
rgm@labs.htt-consult.com
Verizon

Problem

- IEEE 802.15.4 DOES provide for single hop datagram security
  - But designates Key Management of 'out of scope'
  - Has NO 'hook' for a general solution
    - Each Higher Layer 15.4 application MUST solve this
    - History of 802.15 to 'keep the MAC simple'
- IEEE 802.15.4e opens the door to new functionality
  - Multipurpose Frame
  - Information Element

The Challenge

- 802.15.4 PSDU currently limited to 127 octets
  - SUN devices (802.15.4g) support 2047 octets
- MOST deployments of 802.15.4 are not beacon-enabled PANs
  - No Association phase
- Need to support Security PIB (ie data elements)
  - We THINK this is complete enough
- Not dictate a specific Key Management Protocol
  - As much as I would like to!

Approach

- IEEE 802.15.4 Recommended Practice
  - PAR targeted for November!
- Create KMP shim
  - A specific Information Element carried in the Multipurpose Frame
    - Or Associate Frame in BEACON PAN
  - Provide KMP payload fragmentation
    - Chaining using 802.15.4 forced ACK
  - KMPs supported listed
    - HIP, IKEv2, 802.1X, SAE, PSK, ...
    - With implementation considerations

Work

- Public documents
  - Old documents at
    - https://mentor.ieee.org/802.15/documents?is_group=0hip
  - New documents at
    - https://mentor.ieee.org/802.15/documents?is_group=0kmp
- Mailing list at
  - http://grouper.ieee.org/groups/802/15/pub/Subscribe.html#802.15.hip
    - Lose archive if changed to KMPIG
    - Probably not open to non-IEEE members, sorry
    - But email me if interested