Minimal security framework for 6TiSCH

draft-vucinic-6tisch-minimal-security-00

October 28th, 2016

Mališa Vučinić, Inria
Jonathan Simon, Linear Technology
Kris Pister, UC Berkeley
Context

• Terminology
  • **JN**: Joining Node
  • **JCE**: Join coordinating entity
  • **JA**: Join assistant - radio neighbor of JN
  • JN provisioned with a “join” credential
    • Pre-Shared Key (PSK)
    • raw public key (RPK)
    • Locally-valid certificate and a trust anchor
  • Expects to be configured with
    • K2 from [ietf-6tisch-minimal]
    • short 802.15.4 address
Goals

• Minimize number of exchanges -> single round trip with PSKs

• Minimize join-specific code -> reuse of existing protocols

• Security -> end-to-end AES-CCM
Join protocol

optional with PSKs

uses EDHOC [draft-selander-ace-cose-ecdhe-03]

Figure 1: Message sequence for join protocol.
Protocol Specification

- Implemented with CoAP
  - JN is a CoAP client, JCE a server
- JA is a CoAP proxy
  - Stateless using app-level info
- E2E encryption *through JA* using OSCOAP + COSE
- Actual “traffic keys” and nonces are derived from PSK
Example (PSK)

- Link local commun.
- Global commun. using pre-existing routes

[] - authenticated
{}

Encodes to 15 bytes

Encodes to 26 bytes