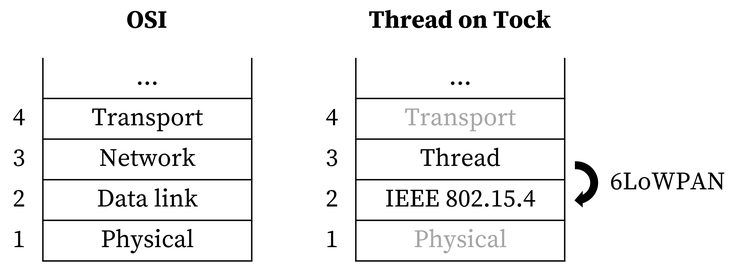
Bringing IP Networking to the Internet of Things

Mateo Garcia, Hubert Teo, Paul Crews
CURIS 2017

Motivation

The goal of our CURIS project this summer was to add low-power wireless networking support to the Tock operating system. Tock is a secure embedded OS designed for the future of the Internet of Things (IoT), when embedded devices will run multiple concurrent, mutually distrustful applications on a single embedded device.

We were tasked with enabling IPv6 packet transmission over a low-rate (and hence, low-power) wireless personal area network (WPAN), the type of network (Layer 3) used to connect IoT devices. The most widely adopted standard in the IoT space is IEEE 802.15.4, which specifies the physical (Layer 1) and data link (Layer 2) layers that support a WPAN. A number of network (Layer 3) protocols have been defined on top of IEEE 802.15.4, but because the IoT is still young, a de facto L3 standard has not yet been set. So far, only one such network protocol has been defined with IPv6 in mind: Thread, created by Nest Labs. The Thread protocol makes use of 6LoWPAN, a compression scheme defined by the IETF that allows IPv6 packets to be fragmented and sent over an IEEE 802.15.4 based network.



Related Work

- IEEE 802.15.4 standard
- 6LoWPAN standard (IETF in RFC 4944)
- OpenThread
- Rust, a systems programming language that lends itself to security with semantics like type and memory safety enforced at compile time

Background on Mesh Link Establishment (MLE)

- Mesh Link Establishment (MLE) is the process by which a Thread device joins a Thread mesh network.
- MLE for network attaching comprises a four-step handshake that works as follows:
    1. A child device multicasts a Parent Request MLE command.
    2. Each potential parent device on the network unicasts a Parent Response MLE command.
    3. The child device selects a parent based on a hierarchy of connectivity metrics and unicasts a Child ID Request MLE command.
    4. The selected parent unicasts a Child ID Response MLE command.
- MLE messages consist of a command type and a series of Type-Length-Value (TLV) parameters. TLVs are used to serialize information exchanged during mesh link establishment

Findings on MLE Using Type-Length-Value (TLV) Structures

- It’s possible to construct a packet that’s too long using TLVs
- ‘Hole’ in the specification
- Jonathan Hui @ Nest, “Let's say the limit is 10 TLVs”