6lowpan security considerations

Christian Schumacher
schumacher@danfoss.com

6lowpan WG
64th IETF
7th of November, 2005

Disposition

- 6lowpan problem areas and scope
- Current security considerations
- IEEE802.15.4 2003 specification
- Application scenario (6lowpan and the world)
- 6lowpan and key management
- Suggestions

6lowpan problem areas and scope

- **General problem areas identified:**
  - IP adaptation/Packet Formats and interoperability
  - Addressing schemes and address management
  - Network management
  - Routing in dynamically adaptive topologies
  - **Security, including set-up and maintenance**
  - Application programming interface
  - Discovery (of devices, of services, etc)
  - Implementation considerations

- **Security problem areas identified (http://6lowpan.tzi.org/SecurityObjectives)**
  - Authorization
    - Why devices are supposed to talk
  - Key management
    - Setting up network, Life-cycle issues

- **Current scope / charter**
  - Problem statement document (with security considerations)
  - Format of IPv6 packets document (with security considerations)

Current security considerations

- **Quotes from draft-6lowpan-problem-01**
  - “End-to-end security is needed.”
  - ”Bootstrapping of devices into a secure network…”
  - “6LoWPAN imposes unique set of challenges…”
  - “IEEE 802.15.4 provides AES link layer security…”

- **Quotes from draft-6lowpan-format-01**
  - “…security for such devices (RFDs) may rely quite strongly on the mechanisms defined at the link-layer by IEEE 802.15.4.”
  - ”…[IEEE802.15.4] does not, in particular, specify key management…”

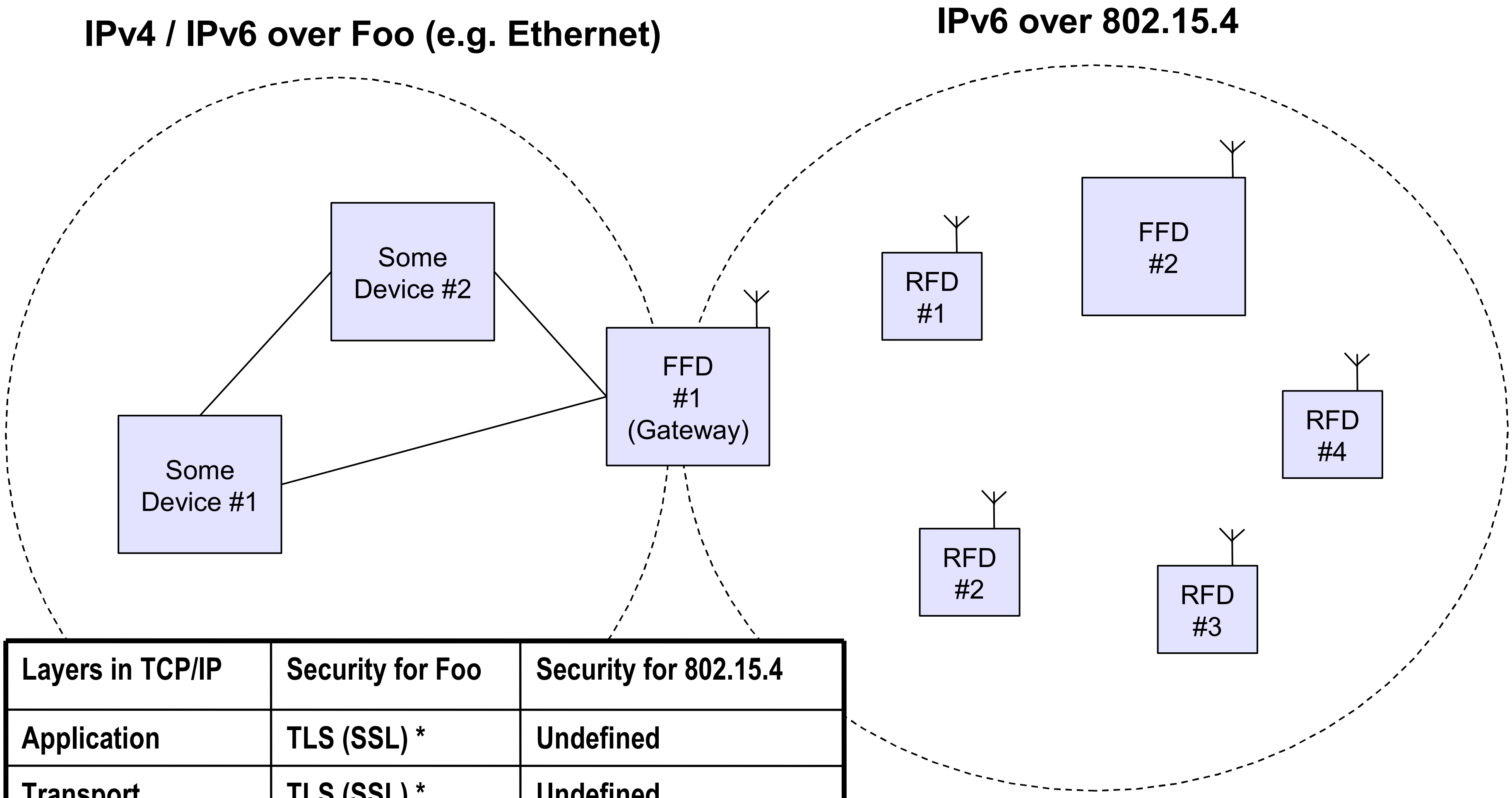
IEEE802.15.4 2003 specification

- **Security issues with IEEE802.15.4 2003 spec**
  - Paper by Naveen Sastry and David Wagner indicates that 2003 spec. has many pitfalls.
    - Download ”Security Considerations for IEEE 802.15.4 Networks” from http://www.cs.berkeley.edu/~daw/papers/

- **IEEE802.15.4b WG**
  - This WG aims to clarify ambiguities and pitfalls in original IEEE802.15.4 2003 spec.
  - WG is also specifying new PHY modes, which may make 802.15.4b more attractive.
  - WG is resolving security pitfalls identified by the before mentioned paper.
  - Specification should be available for download July 2006

- **Main differences between 802.15.4b security and legacy 802.15.4-2003 security (input from Rene Struik, security expert from Certicom)**
  - Protection of broadcast and multicast frames possible
  - Easier setup of protection parameters possible
  - Possibility to vary protection per frame, using a single key
  - Consideration of system lifecycle issues
  - Optimization of storage for keying material

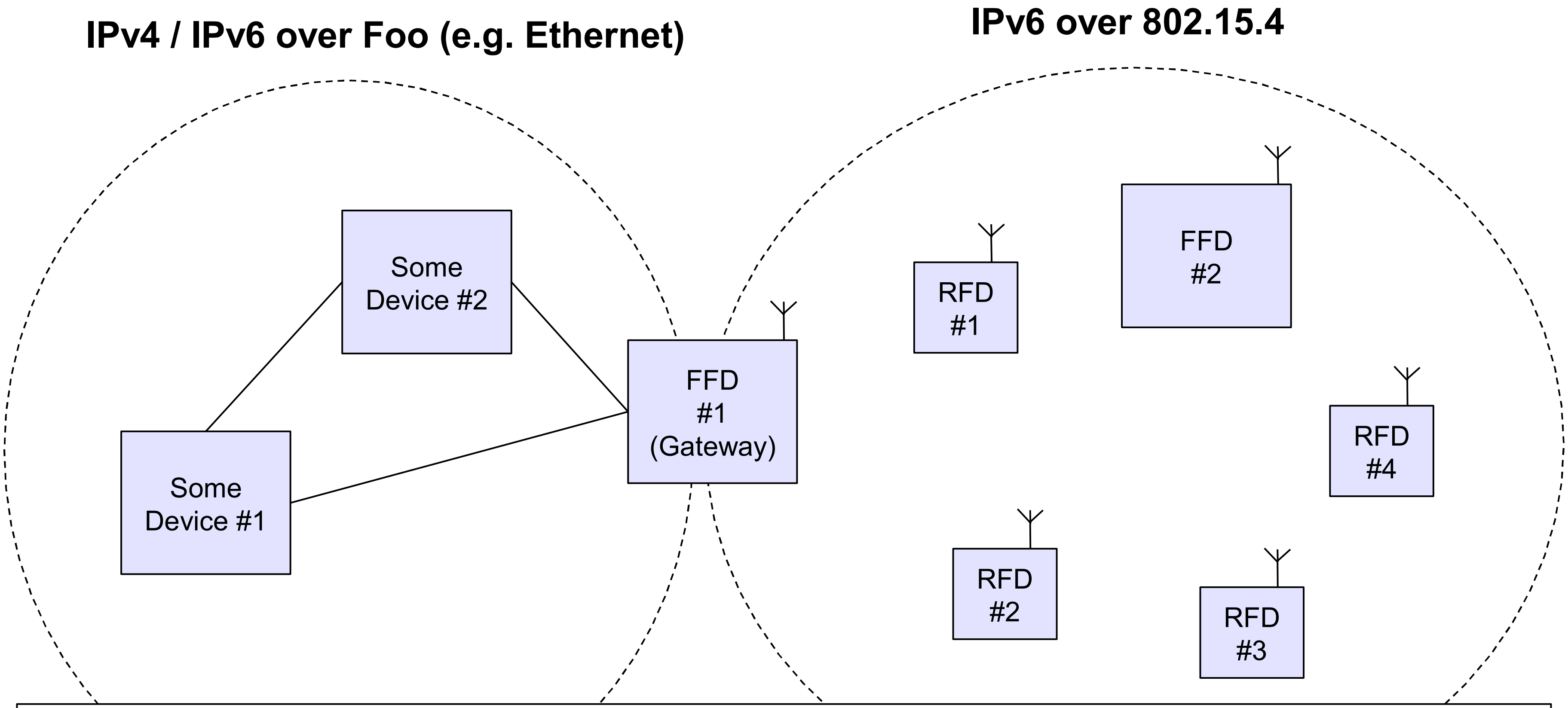
Application scenario (6lowpan and the world)



Layers in TCP/IP	Security for Foo	Security for 802.15.4
Application	TLS (SSL) *	Undefined
Transport	TLS (SSL) *	Undefined
Network	IPSec / Foo	(802.15.4)
Link	Foo	802.15.4

* Operates between Application and Transport layer

Application scenario (6lowpan and the world)



- Secure communications between ”Some Device on Foo” and a ”Device on IEEE802.15.4” is most likely to happen thru a gateway.
- This gateway will handle TLS / IPSec on the Foo network and a utilize a To-Be-Defined security protocol on the 802.15.4 network.
- With TLS / IPSec there are protocols for negotiating keys (key-management) on the fly.
- With 802.15.4 security these protocols are missing.
- Ad-hoc wireless networks require secure communications on-the-fly!

6lowpan and key management

- **First of all: We need input from security experts!**

- **What methods could be used for exchanging keys?**
  - Bootstrapping keys
    - Logistical nightmare (trust your manufacturer for book-keeping of keys)
    - Maintenance issues (how to renew keys?)
    - Resellability
  - Unencrypted key exchange, accept moment of vulnerability
    - Will work, but no guarantee of security
    - Careless implementation could lead to easy access to keys
  - Public-key based methods
    - What technology to use (RSA, ECC)

Suggestions

- **Advocate IEEE802.15.4b**
  and amend current security considerations to reflect this decision.

- **Recharter to work on document(s) which focus on key-management**
  - Where to get inspiration?
    - SNMP v3 security models (RFC 3411, RFC 3418)
    - SSL on 8-bit processors (http://www.embedded.com/showArticle.jhtml?articleID=45400043)
    - IETF security WGs
    - Security experts input
      (e.g. papers on sensor networks by David Wagner, http://www.cs.berkeley.edu/~daw/papers/)