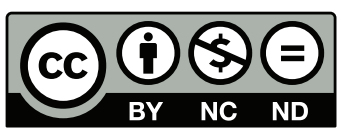
Introduction to IEEE 802.15.4 and IPv6 over 802.15.4 (6LowPAN)

Jürgen Schönwälder

JACOBS UNIVERSITY

AIMS 2009, Enschede, 2009-07-02



This tutorial was supported in part by the EC IST-EMANICS Network of Excellence (26854).

Outline of the Talk

Keep-Awake Questionaire

Question #1

What does “S” stand for in SNMP?

IEEE 802.15.4

IEEE 802.15.4

The IEEE standard 802.15.4 offers physical and media access control layers for low-cost, low-speed, low-power wireless personal area networks (WPANs)

Application Scenarios

- Home Networking
- Automotive Networks
- Industrial Networks
- Interactive Toys
- Remote Metering
- ...

IEEE 802.15.4 Standard Versions

802.15.4-2003

Original version using Direct Sequence Spread Spectrum (DSSS) with data transfer rates of 20 and 40 kbit/s

802.15.4-2006

Revised version using Direct Sequence Spread Spectrum (DSSS) with higher data rates and adding Parallel Sequence Spread Spectrum (PSSS)

802.15.4a-2007

Adding Direct Sequence Ultra-wideband (UWB) and Chirp Spread Spectrum (CSS) physical layers to the 2006 version of the standard (ranging support)

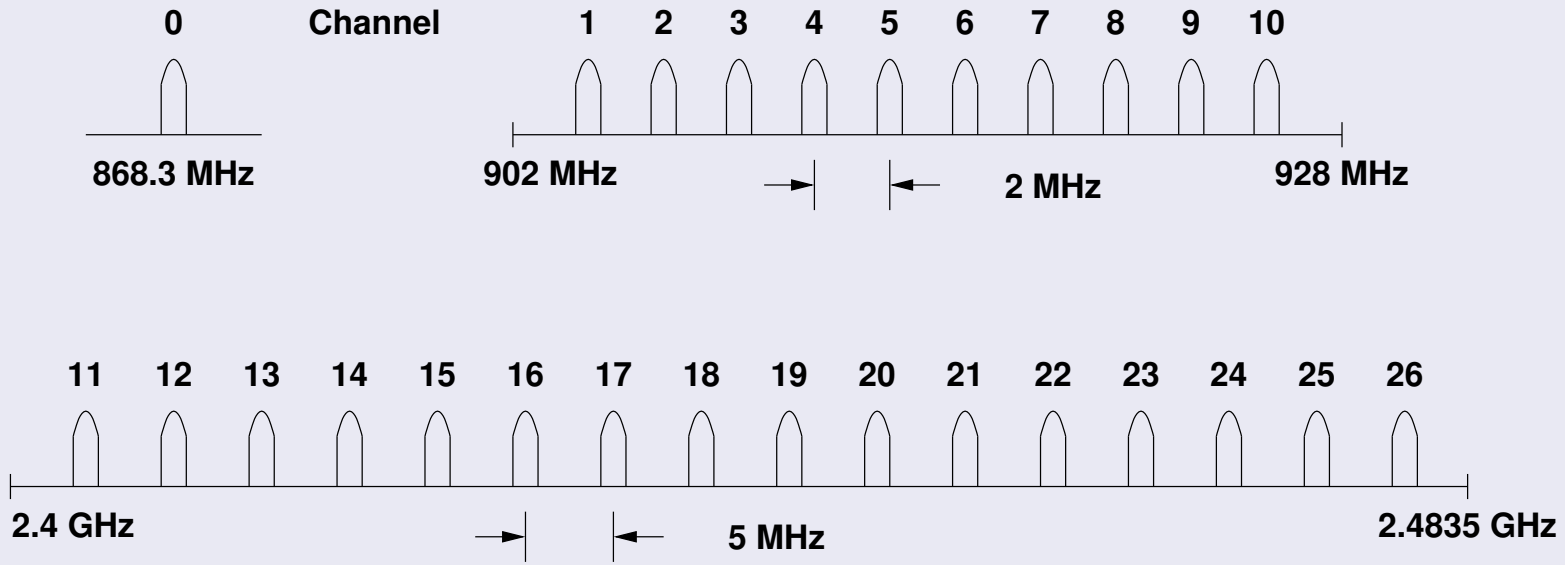
Keep-Awake Questionaire

Question #2

What is the difference between bit rate and baud rate?

Radio Characteristics (802.15.4-2003)

Frequencies and Data Rates



Frequency	Channels	Region	Data Rate	Baud Rate
868-868.6 MHz	0	Europe	20 kbit/s	20 kBaud
902-928 MHz	1-10	USA	40 kbit/s	40 kBaud
2400-2483.5 MHz	11-26	global	250 kbit/s	62.5 kBaud

IEEE 802.15.4 Device Classes

Full Function Device (FFD)

- Any topology
- PAN coordinator capable
- Talks to any other device
- Implements complete protocol set

Reduced Function Device (RFD)

- Reduced protocol set
- Very simple implementation
- Cannot become a PAN coordinator
- Limited to leafs in more complex topologies

IEEE 802.15.4 Definitions

Network Device

An RFD or FFD implementation containing an IEEE 802.15.4 medium access control and physical interface to the wireless medium.

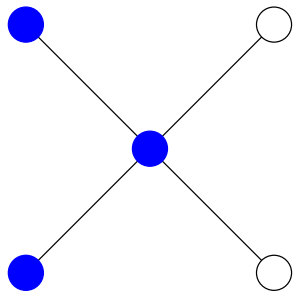
Coordinator

An FFD with network device functionality that provides coordination and other services to the network.

PAN Coordinator

A coordinator that is the principal controller of the PAN. A network has exactly one PAN coordinator.

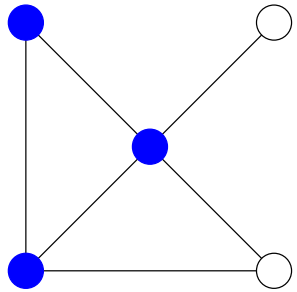
IEEE 802.15.4 Star Topology



Star Topology

- All nodes communicate via the central PAN coordinator
- Leafs may be any combination of FFD and RFD devices
- PAN coordinator is usually having a reliable power source

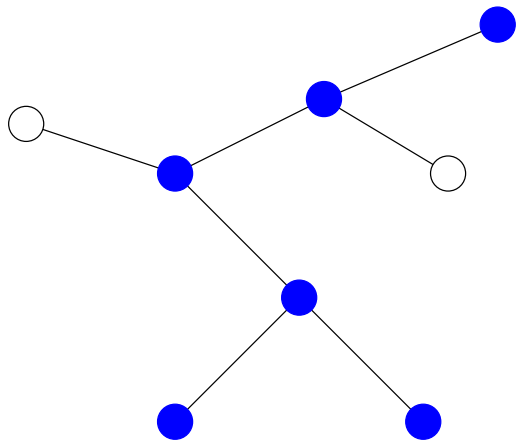
IEEE 802.15.4 Peer-to-Peer Topology



Peer-to-Peer Topology

- Nodes can communicate via the centeral PAN coordinator and via additional point-to-point links
- Extension of the pure star topology

IEEE 802.15.4 Cluster Tree Topology



Cluster Tree Topology

- Leafs connect to a network of coordinators (FFDs)
- One of the coordinators serves as the PAN coordinator
- Clustered star topologies are an important case (e.g., each hotel room forms a star in a HVAC system)

Keep-Awake Questionaire

Question #3

What is the size of a MAC address?

IEEE 802.15.4 Frame Formats

General Frame Format

octets: 2	1	0/2	0/2/8	0/2	0/2/8	variable	2
Frame control	Sequence number	Destination PAN identifier	Destination address	Source PAN identifier	Source address	Frame payload	Frame sequence check

bits: 0–2	3	4	5	6	7–9	10–11	12–13	14–15
Frame type	Security enabled	Frame pending	Ack. requested	Intra PAN	Reserved	Dst addr mode	Reserved	Src addr mode

- IEEE 64-bit extended addresses (globally unique)
- 16-bit “short” addresses (unique within a PAN)
- Optional 16-bit source / destination PAN identifiers
- max. frame size 127 octets; max. frame header 25 octets

IEEE 802.15.4 Frame Formats

Beacon Frames

- Broadcasted by the coordinator to organize the network

Command Frames

- Used for association, disassociation, data and beacon requests, conflict notification, ...

Data Frames

- Carrying user data — this is what we are interested in

Acknowledgement Frames

- Acknowledges successful data transmission (if requested)

Keep-Awake Questionaire

Question #4

Provide ~~two~~ three different expansions of the acronym MAC.

IEEE 802.15.4 Media Access Control

Carrier Sense Multiple Access / Collision Avoidance

Basic idea of the CSMA/CA algorithm:

- First wait until the channel is idle.
- Once the channel is free, start sending the data frame after some random backoff interval.
- Receiver acknowledges the correct reception of a data frame.
- If the sender does not receive an acknowledgement, retry the data transmission.

IEEE 802.15.4 Unslotted Mode

Node → PAN, Node → Node

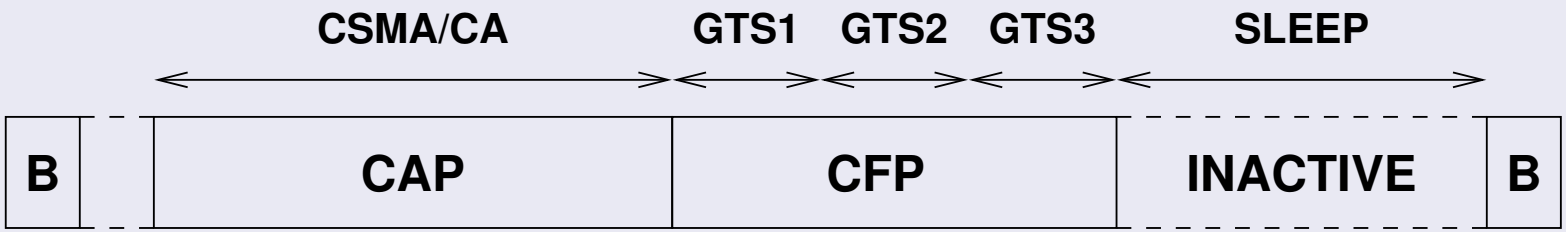
- The sender uses CSMA/CA and the receiver sends an ACK if requested by the sender.
- Receiver needs to listen continuously and can't sleep.

PAN → Node

- The receiver polls the PAN whether data is available.
- The PAN sends an ACK followed by a data frame.
- Receiving node sends an ACK if requested by the sender.
- Coordinator needs to listen continuously and can't sleep.

IEEE 802.15.4 Slotted Mode

Superframes



- A superframe consists of three periods:
  1. During the Contention-Access-Period (CAP), the channel can be accessed using normal CSMA/CA.
  2. The Contention-Free-Period (CFP) has Guaranteed Time Slots (GTS) assigned by the PAN to each node.
  3. During the Inactive-Period (IP), the channel is not used and all nodes including the coordinator can sleep.
- The PAN delimits superframes using beacons.

IEEE 802.15.4 Security

Security Services

Security Suite	Description
Null	No security (default)
AES-CTR	Encryption only, CTR Mode
AES-CBC-MAC-128	128 bit MAC
AES-CBC-MAC-64	64 bit MAC
AES-CBC-MAC-32	32 bit MAC
AES-CCM-128	Encryption and 128 bit MAC
AES-CCM-64	Encryption and 64 bit MAC
AES-CCM-32	Encryption and 32 bit MAC

- Key management must be provided by higher layers
- Implementations must support AES-CCM-64 and Null

IPv6 over IEEE 802.15.4 (6LowPAN)

Keep-Awake Questionaire

Question #5

What is the size of an IPv6 header?

6LowPAN Motivation

Benefits of IP over 802.15.4 (RFC 4919)

1. The pervasive nature of IP networks allows use of existing infrastructure.
2. IP-based technologies already exist, are well-known, and proven to be working.
3. Open and freely available specifications vs. closed proprietary solutions.
4. Tools for diagnostics, management, and commissioning of IP networks already exist.
5. IP-based devices can be connected readily to other IP-based networks, without the need for intermediate entities like translation gateways or proxies.

6LowPAN Challenge

Header Size Calculation...

- IPv6 header is 40 octets, UDP header is 8 octets
- 802.15.4 MAC header can be up to 25 octets (null security) or 25+21=46 octets (AES-CCM-128)
- With the 802.15.4 frame size of 127 octets, we have
  - 127-25-40-8 = 54 octets (null security)
  - 127-46-40-8 = 33 octets (AES-CCM-128)

  of space left for application data!

IPv6 MTU Requirements

- IPv6 requires that links support an MTU of 1280 octets
- Link-layer fragmentation / reassembly is needed

6LowPAN Overview (RFC 4944)

Overview

- The 6LowPAN protocol is an adaptation layer allowing to transport IPv6 packets over 802.15.4 links
- Uses 802.15.4 in unslotted CSMA/CA mode (strongly suggests beacons for link-layer device discovery)
- Based on IEEE standard 802.15.4-2003
- Fragmentation / reassembly of IPv6 packets
- Compression of IPv6 and UDP/ICMP headers
- Mesh routing support (mesh under)
- Low processing / storage costs

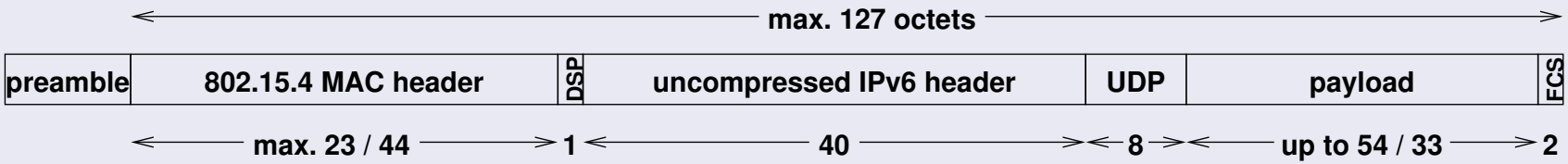
6LowPAN Dispatch Codes

- All LoWPAN encapsulated datagrams are prefixed by an encapsulation header stack.
- Each header in the stack starts with a header type field followed by zero or more header fields.

Bit Pattern	Short Code	Description
00 xxxxxx	NALP	Not A LoWPAN Packet
01 000001	IPv6	uncompressed IPv6 addresses
01 000010	LOWPAN_HC1	HC1 Compressed IPv6 header
01 010000	LOWPAN_BC0	BC0 Broadcast header
01 111111	ESC	Additional Dispatch octet follows
10 xxxxxx	MESH	Mesh routing header
11 000xxx	FRAG1	Fragmentation header (first)
11 100xxx	FRAGN	Fragmentation header (subsequent)

6LowPAN Frame Formats

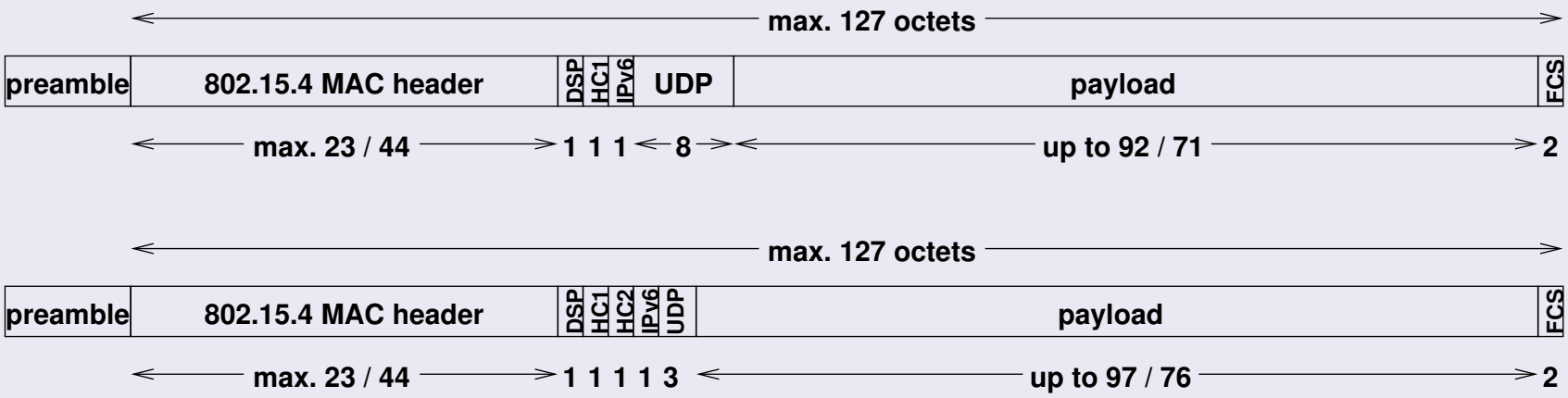
Uncompressed IPv6/UDP (worst case scenario)



- Dispatch code (01000001_2) indicates no compression
- Up to 54 / 33 octets left for payload with a max. size MAC header with null / AES-CCM-128 security
- The relationship of header information to application payload is obviously really bad

6LowPAN Frame Formats

Compressed Link-local IPv6/UDP (best case scenario)



- Dispatch code (01000010_2) indicates HC1 compression
- HC1 compression may indicate HC2 compression follows
- This shows the maximum compression achievable for link-local addresses (does not work for global addresses)
- Any non-compressable header fields are carried after the HC1 or HC1/HC2 tags (partial compression)

Header Compression

Compression Principles (RFC 4944)

- Omit any header fields that can be calculated from the context, send the remaining fields unmodified
- Nodes do not have to maintain compression state (stateless compression)
- Support (almost) arbitrary combinations of compressed / uncompressed header fields

Ongoing Work

- Compression for globally routable addresses (HC1G)
- Stateful compression (IPHC, NHC)

Fragmentation and Reassembly

Fragmentation Principles (RFC 4944)

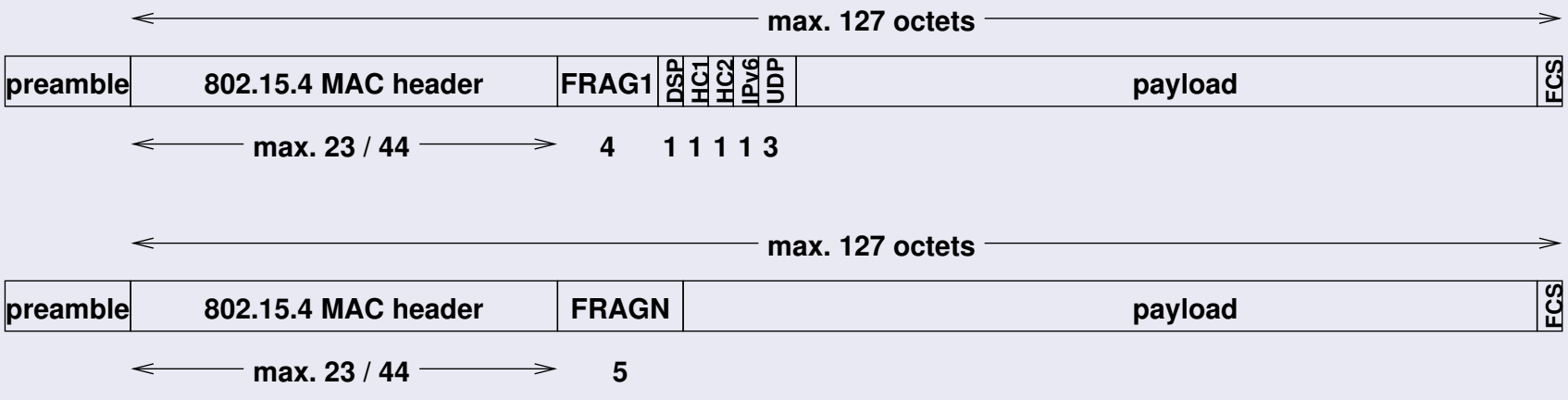
- IPv6 packets to large to fit into a single 802.15.4 frame are fragmented.
- A first fragment carries a header that includes the datagram size (11 bits) and a datagram tag (16 bits).
- Subsequent fragments carry a header that includes the datagram size, the datagram tag, and the offset (8 bits).
- Time limit for reassembly is 60 seconds.

Ongoing Work

- Recovery protocol for lost fragments (RFC 4944 requires to resend the whole set of fragments)

Fragmentation and Reassembly

Fragmentation Example (compressed link-local IPv6/UDP)



Homework Question (consult RFC 4944 first)

- How many fragments are created for an 1280 octet IPv6 packet with no / maximum compression and none / AES-CCM-128 link-layer security?
- How many fragmented datagrams can be in transit concurrently for a 802.14.5 source / destination pair?

Interoperability Evaluation

6LowPAN Implementations

Name	OS / License	Hardware	Maintained
Jacobs	TinyOS / 3BSD	Telos B, ...	no
Berkley IP	TinyOS / 3BSD	Telos B, ...	active
Arch Rock	TinyOS / EULA	Raven, ...	active
SICSlowpan	Contiki / 3BSD	Raven, ...	active
Sensinode	Own / EULA	Sensinode	active
Hitachi	Own / EULA	Renesas	unknown

Unfortunately...

- The Jacobs implementation uses the TinyOS Active Message framing format and thus does not interoperate

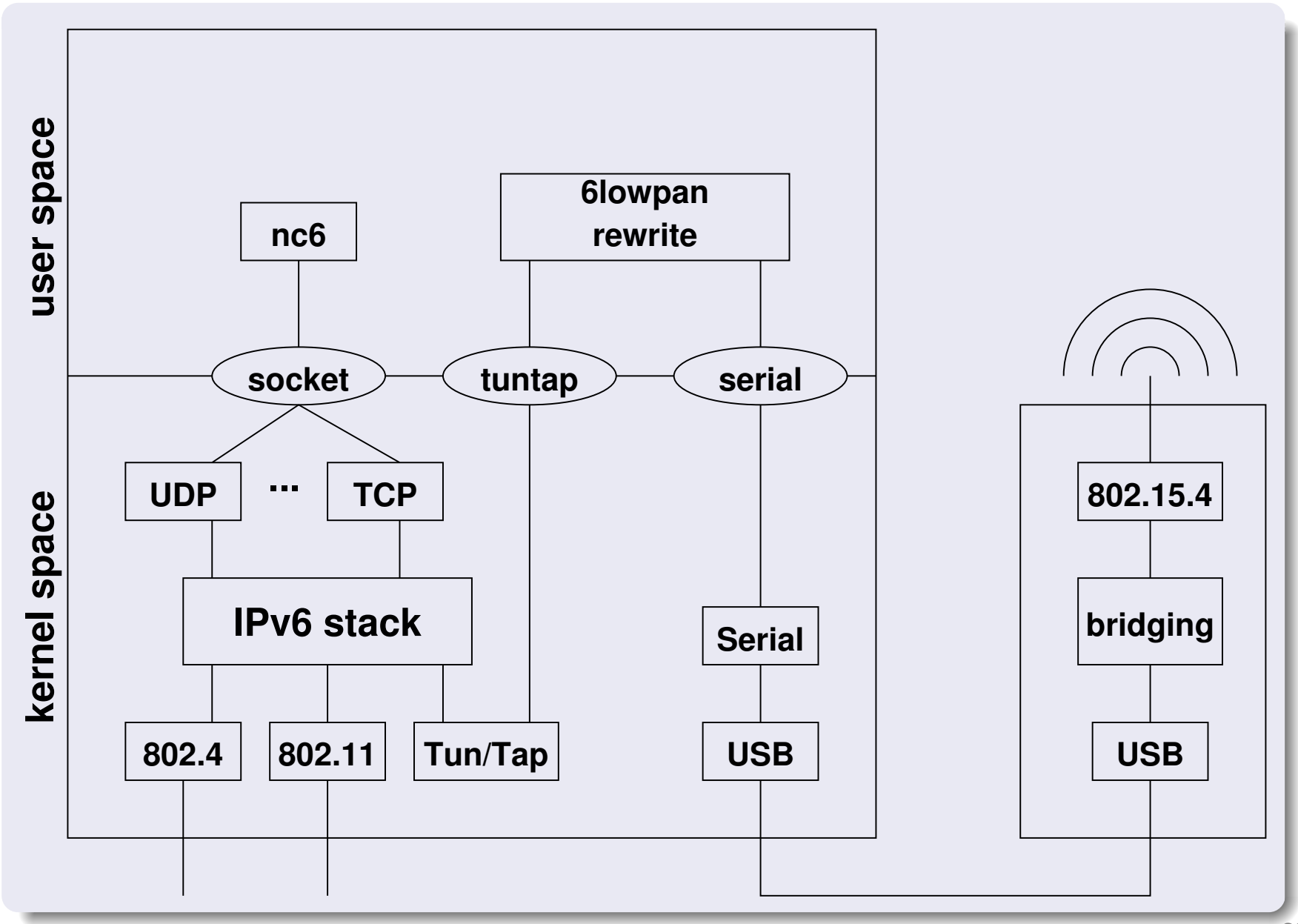
Interoperability Evaluation

Feature Comparison

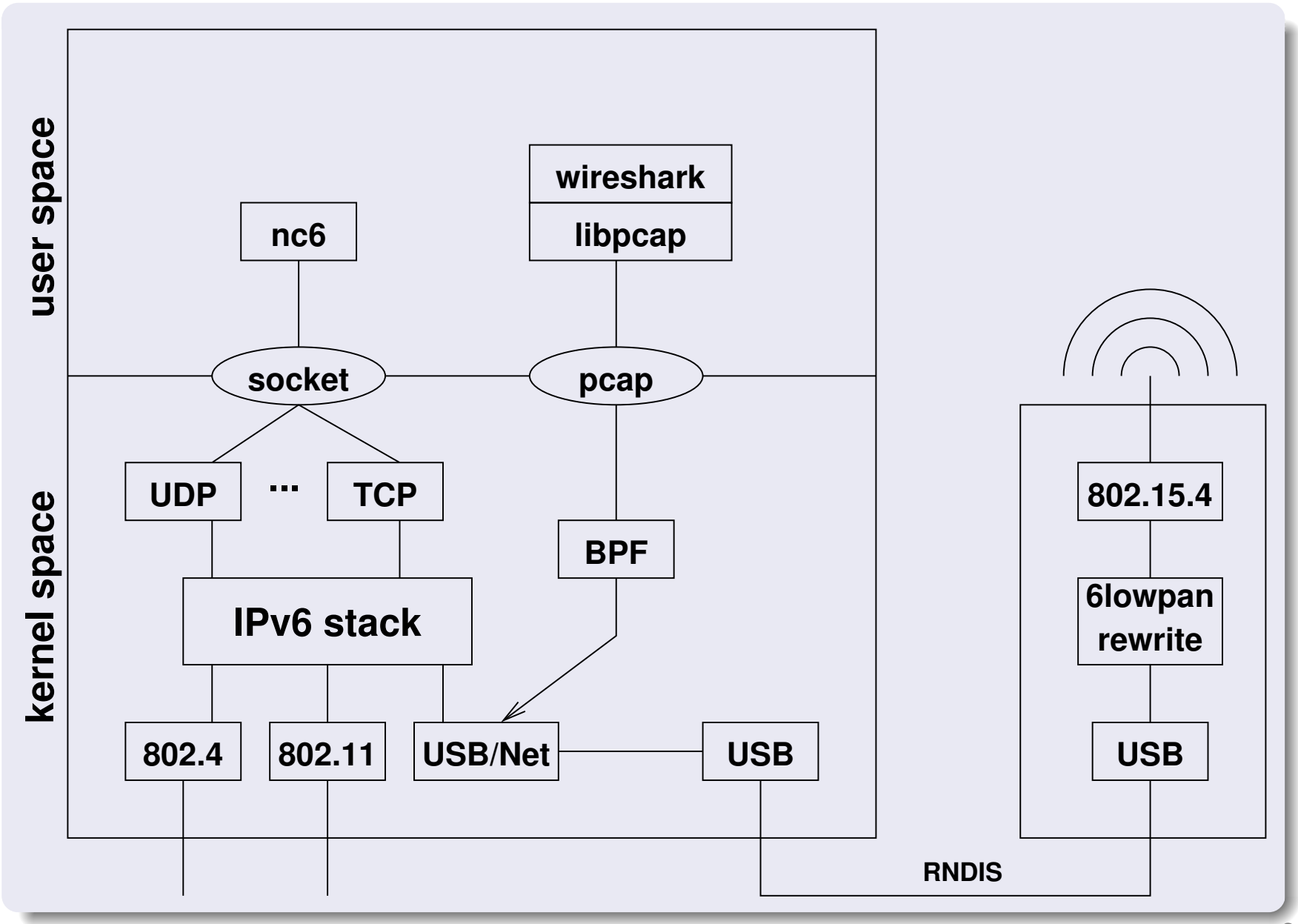
Feature	Jacobs	Berkley	Contiki	Arch Rock
Dispatch Header	+	+	+	+
Dispatch Type	+	+	+	+
Mesh Header	-	+	+	+
Mesh Routing	-	*	*	+
Multicasting Header	-	+	+	+
Multicasting	+	+	+	+
Fragmentation	*	*	*	*
HC1	+	+	+	+
HC2 for UDP	-	-	-	+
HC1g	-	-	o	o
ICMPv6 Echo	+	+	+	+

+ = supported and tested, o = supported but not tested,
- = not supported, * = see [12] for details

Implementation via USB Serial Interfaces



Implementation via USB Network Interfaces



Management of 6LowPAN Networks

Keep-Awake Questionaire

Question #6

What is the difference between SNMP proxies and SNMP master/subagents?

Management of 6LowPANs

Why 6LowPAN Management?

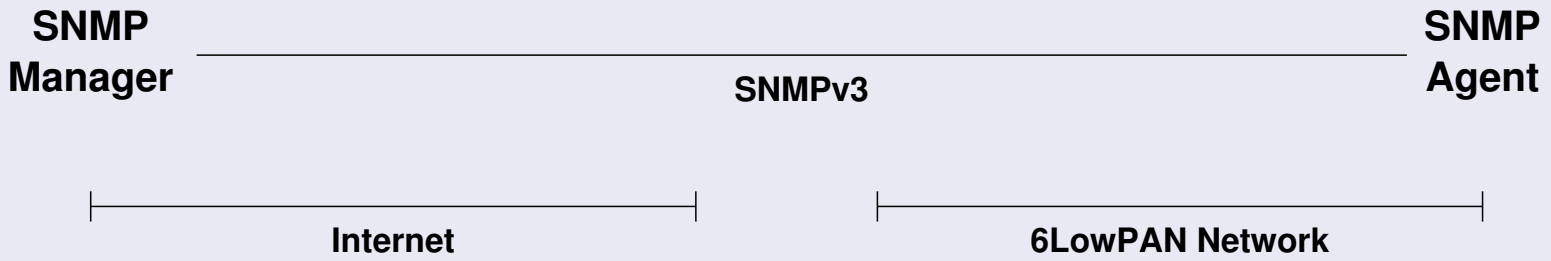
- "Autonomic devices won't need management — so don't waste your time on the wrong problem..."
- Well, no, for the foreseeable future, you will end up managing the autonomic system (one more control loop)
- Key management is for example a largely unsolved problem (but specialized keying protocols might help)

Example Management Questions:

- How much energy is left in my nodes/network?
- How many nodes disappeared during the last night/day?
- What is the temperature, pressure, (add your favorite sensor here) distribution within the network?

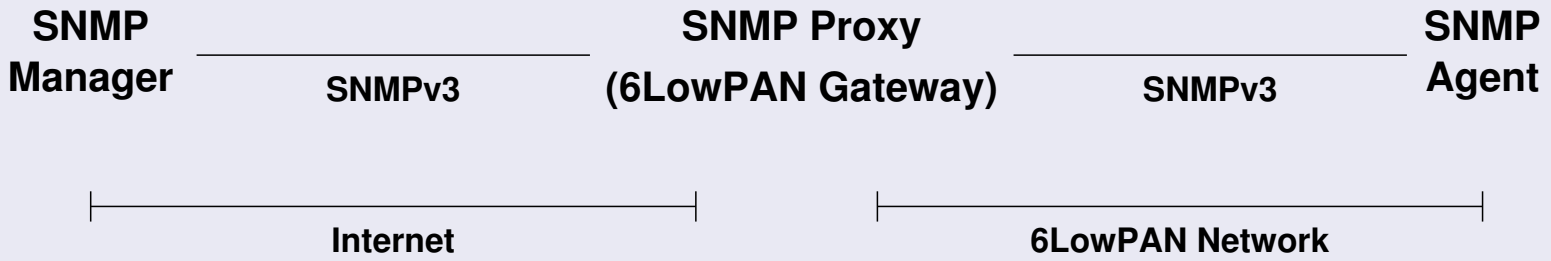
SNMP and 6LowPAN

Using SNMPv3 End-to-End



+ Straight forward access to individual 6LowPAN nodes
+ Reuse of existing deployed SNMP-based tools
o End-to-end security, end-to-end key management
- Message size and potential fragmentation issues
- 6LowPAN nodes must run an SNMP engine
- Polling nature of SNMP has high energy costs

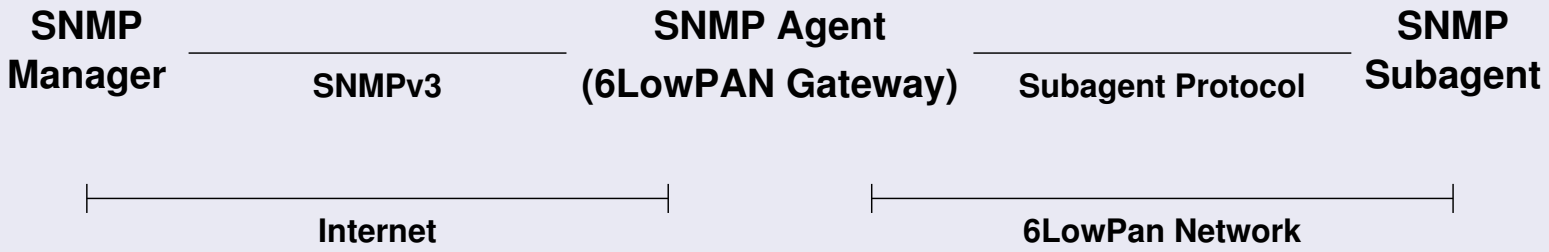
Using SNMPv3 Proxies



+ Indirect access to individual 6LowPAN nodes
+ Alternate transport encoding can reduce message sizes
o Reuse of existing SNMP-based tools supporting proxies
o Two security domains, different key management schemes
- 6LowPAN nodes must run an SNMP engine
- Polling nature of SNMP has high energy costs

SNMP and 6LowPAN

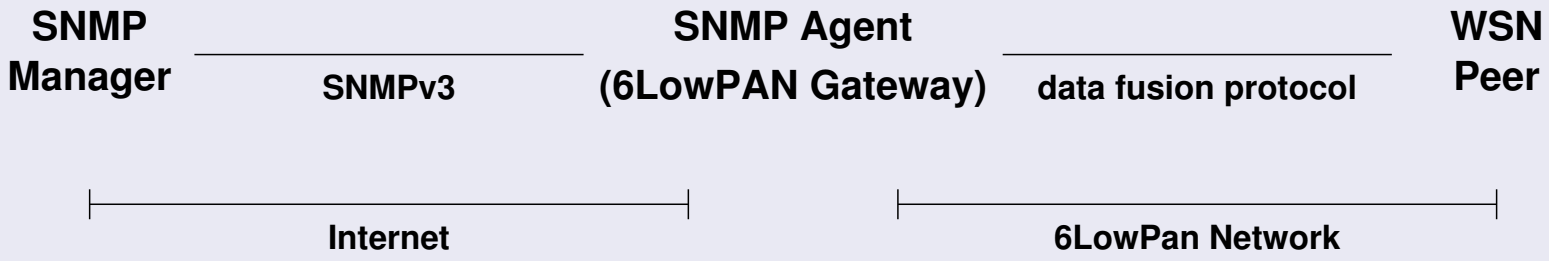
Using SNMPv3 Subagents



+ Indirect access to individual 6LowPAN nodes
+ Alternate transport encoding can reduce message sizes
o Reuse of existing SNMP-based tools supporting contexts
o Two security domains, different key management schemes
o 6LowPAN nodes must run an SNMP subagent
- Polling nature of SNMP has high energy costs

SNMP and 6LowPAN

Using SNMPv3 with Data Fusion Protocols



+ Indirect access to individual 6LowPAN nodes
+ Leveraging data fusion protocols
+ SNMP agent acting as a cache, no expensive polling
o Reuse of existing SNMP-based tools supporting contexts
o Two security domains, different key management schemes
? No real advantage of 6LowPAN technology — oops

HTTP light over UDP

HTTP light over UDP

- Most people prefer HTTP-like protocols over SNMP
- HTTP has elaborate caching support, which allows RFD nodes to be offline while the cache serves requests
- Since UDP is the preferred 6LowPAN transport, several adaptations are needed, similar to some SIP optimizations
- Ideas currently being drafted in the 6LowPAN working group of the IETF (see mailing list)
- Ideally, this develops into a generic 6LowPAN application protocol substrate (and might take years to complete)

Summary

Keep-Awake Questionaire

Question #7

What is the difference between slotted and unslotted mode of IEEE 802.15.4-2003?

Summary

Main Points to Remember

- IEEE 802.15.4 is a relatively recent standard for low-cost, low-speed, low power wireless networks.
- The MAC layer supports slotted and unslotted modes and different network topologies
- The 6LowPAN standard makes IEEE 802.15.4 enabled devices directly Internet accessible via IPv6
- Main 6LowPAN functions are fragmentation/reassembly and header compression
- Ongoing IETF work dealing with routing, neighbour discovery, and stateful compression schemes
- Management of 6LowPAN networks is yet to be defined

Reading Material I

IEEE.

IEEE Std 802.15.4-2003.
Technical Report 802.15.4-2003, IEEE, October 2003.

IEEE.

IEEE Std 802.15.4-2006.
Technical Report 802.15.4-2006, IEEE, September 2006.

IEEE.

IEEE Std 802.15.4a-2007.
Technical Report 802.15.4a-2007, IEEE, August 2007.

N. Kushalnagar, G. Montenegro, and C. Schumacher.

IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals.
RFC 4919, Intel Corp, Microsoft Corporation, Danfoss A/S, August 2007.

G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler.

Transmission of IPv6 Packets over IEEE 802.15.4 Networks.
RFC 4944, Microsoft Corporation, Intel Corp, Arch Rock Corp, September 2007.

Y. Xiao, H.-H. Chen, B. Sun, R. Wang, and S. Sethi.

MAC Security and Security Overhead Analysis in the IEEE 802.15.4 Wireless Sensor Networks.
Journal on Wireless Communications and Networking, 2006:1–12, 2006.

E. Callaway, P. Gorday, L. Hester, J. A. Gutierrez, M. Naeve, B. Heile, and V. Bahl.

Home Networking with IEEE 802.15.4: A Developing Standard for Low-Rate Wireless Personal Area Networks.
IEEE Communications Magazine, 40(8):70–77, August 2002.

Reading Material II

L. D. Nardis and M.-G. Di Benedetto.

Overview of the IEEE 802.15.4/4a standards for low data rate Wireless Personal Data Networks.
In Proc. of the 4th IEEE Workshop on Positioning, Navigation and Communication 2007 (WPNC'07), Hannover, March 2007. IEEE.

S. Labella M. Petrova, J. Riihijarvi, P. Mahonen.

Performance Study of IEEE 802.15.4 Using Measurements and Simulations.
In Proc. IEEE Wireless Communications and Networking Conference (WCNC 2006), pages 487–492, 2006.

Z. Sahinoglu and S. Gezici.

Ranging in the IEEE 802.15.4a Standard.
In Proc. IEEE Wireless and Microwave Technology Conference (WAMICON 2006), December 2006.

M. Harvan and J. Schönwälder.

TinyOS Motes on the Internet: IPv6 over 802.15.4 (6lowpan).
Praxis der Informationsverarbeitung und Kommunikation, 31(4):244–251, December 2008.

K. D. Korten, I. Tumar, and J. Schönwälder.

Evaluation of IPv6 over Low-Power Wireless Personal Area Networks Implementations.
In (under review), 2009.