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

Jürgen Schönwälder

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

1. IEEE 802.15.4
   - Radio Characteristics
   - Topologies and Frame Formats
   - Media Access Control
   - Security

2. IPv6 over IEEE 802.15.4 (6LowPAN)
   - Motivation and Design Issues
   - Header Compression
   - Fragmentation and Reassembly
   - Interoperability Evaluation

3. Management of 6LowPAN Networks
   - SNMP and 6LowPANs
   - HTTP light over UDP

4. Summary
Question #1

What does “S” stand for in SNMP?
IEEE 802.15.4

1. IEEE 802.15.4
   - Radio Characteristics
   - Topologies and Frame Formats
   - Media Access Control
   - Security

2. IPv6 over IEEE 802.15.4 (6LowPAN)
   - Motivation and Design Issues
   - Header Compression
   - Fragmentation and Reassembly
   - Interoperability Evaluation

3. Management of 6LowPAN Networks
   - SNMP and 6LowPANs
   - HTTP light over UDP

4. Summary
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

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.15.4-2003</td>
<td>Original version using Direct Sequence Spread Spectrum (DSSS) with data transfer rates of 20 and 40 kbit/s</td>
</tr>
<tr>
<td>802.15.4-2006</td>
<td>Revised version using Direct Sequence Spread Spectrum (DSSS) with higher data rates and adding Parallel Sequence Spread Spectrum (PSSS)</td>
</tr>
<tr>
<td>802.15.4a-2007</td>
<td>Adding Direct Sequence Ultra-wideband (UWB) and Chirp Spread Spectrum (CSS) physical layers to the 2006 version of the standard (ranging support)</td>
</tr>
</tbody>
</table>
Question #2

What is the difference between bit rate and baud rate?
## Freqencies and Data Rates

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Channels</th>
<th>Region</th>
<th>Data Rate</th>
<th>Baud Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>868-868.6 MHz</td>
<td>0</td>
<td>Europe</td>
<td>20 kbit/s</td>
<td>20 kBaud</td>
</tr>
<tr>
<td>902-928 MHz</td>
<td>1-10</td>
<td>USA</td>
<td>40 kbit/s</td>
<td>40 kBaud</td>
</tr>
<tr>
<td>2400-2483.5 MHz</td>
<td>11-26</td>
<td>global</td>
<td>250 kbit/s</td>
<td>62.5 kBaud</td>
</tr>
</tbody>
</table>
## 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

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

- Nodes can communicate via the central PAN coordinator and via additional point-to-point links
- Extension of the pure star topology
IEEE 802.15.4 Cluster Tree Topology

- Leaf nodes 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).
Question #3

What is the size of a MAC address?
### IEEE 802.15.4 Frame Formats

#### General Frame Format

<table>
<thead>
<tr>
<th>octets: 2</th>
<th>1</th>
<th>0/2</th>
<th>0/2/8</th>
<th>0/2</th>
<th>0/2/8</th>
<th>variable</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame control</td>
<td>Sequence number</td>
<td>Destination PAN identifier</td>
<td>Destination address</td>
<td>Source PAN identifier</td>
<td>Source address</td>
<td>Frame payload</td>
<td>Frame sequence check</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>bits: 0–2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7–9</th>
<th>10–11</th>
<th>12–13</th>
<th>14–15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame type</td>
<td>Security enabled</td>
<td>Frame pending</td>
<td>Ack. requested</td>
<td>Intra PAN</td>
<td>Reserved</td>
<td>Dst addr mode</td>
<td>Reserved</td>
<td>Src addr mode</td>
</tr>
</tbody>
</table>

- 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

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Beacon Frames</strong></td>
<td>Broadcasted by the coordinator to organize the network</td>
</tr>
<tr>
<td><strong>Command Frames</strong></td>
<td>Used for association, disassociation, data and beacon requests, conflict notification, ...</td>
</tr>
<tr>
<td><strong>Data Frames</strong></td>
<td>Carrying user data — this is what we are interested in</td>
</tr>
<tr>
<td><strong>Acknowledgement Frames</strong></td>
<td>Acknowledges successful data transmission (if requested)</td>
</tr>
</tbody>
</table>
Question #4

Provide two three different expansions of the acronym MAC.
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

<table>
<thead>
<tr>
<th>Node → PAN, Node → Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>- The sender uses CSMA/CA and the receiver sends an ACK if requested by the sender.</td>
</tr>
<tr>
<td>- Receiver needs to listen continuously and can’t sleep.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PAN → Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>- The receiver polls the PAN whether data is available.</td>
</tr>
<tr>
<td>- The PAN sends an ACK followed by a data frame.</td>
</tr>
<tr>
<td>- Receiving node sends an ACK if requested by the sender.</td>
</tr>
<tr>
<td>- Coordinator needs to listen continuously and can’t sleep.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Security Suite</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>No security (default)</td>
</tr>
<tr>
<td>AES-CTR</td>
<td>Encryption only, CTR Mode</td>
</tr>
<tr>
<td>AES-CBC-MAC-128</td>
<td>128 bit MAC</td>
</tr>
<tr>
<td>AES-CBC-MAC-64</td>
<td>64 bit MAC</td>
</tr>
<tr>
<td>AES-CBC-MAC-32</td>
<td>32 bit MAC</td>
</tr>
<tr>
<td>AES-CCM-128</td>
<td>Encryption and 128 bit MAC</td>
</tr>
<tr>
<td>AES-CCM-64</td>
<td>Encryption and 64 bit MAC</td>
</tr>
<tr>
<td>AES-CCM-32</td>
<td>Encryption and 32 bit MAC</td>
</tr>
</tbody>
</table>

- Key management must be provided by higher layers
- Implementations must support AES-CCM-64 and Null
IPv6 over IEEE 802.15.4 (6LowPAN)

1. IEEE 802.15.4
   - Radio Characteristics
   - Topologies and Frame Formats
   - Media Access Control
   - Security

2. IPv6 over IEEE 802.15.4 (6LowPAN)
   - Motivation and Design Issues
   - Header Compression
   - Fragmentation and Reassembly
   - Interoperability Evaluation

3. Management of 6LowPAN Networks
   - SNMP and 6LowPANs
   - HTTP light over UDP

4. Summary
Question #5

What is the size of an IPv6 header?
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.
5. IP-based devices can be connected readily to other IP-based networks, without the need for intermediate entities like translation gateways or proxies.
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 requires that links support an MTU of 1280 octets

Link-layer fragmentation / reassembly is needed
The 6LowPAN protocol is an adaptation layer allowing to transport IPv6 packets over 802.15.4 links. It 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, it supports fragmentation/reassembly of IPv6 packets, compression of IPv6 and UDP/ICMP headers, mesh routing support (mesh under), and low processing/storage costs.
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.

<table>
<thead>
<tr>
<th>Bit Pattern</th>
<th>Short Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 xxxxx</td>
<td>NALP</td>
<td>Not A LoWPAN Packet</td>
</tr>
<tr>
<td>01 000001</td>
<td>IPv6</td>
<td>uncompressed IPv6 addresses</td>
</tr>
<tr>
<td>01 00010</td>
<td>LOWPAN_HC1</td>
<td>HC1 Compressed IPv6 header</td>
</tr>
<tr>
<td>01 010000</td>
<td>LOWPAN_BC0</td>
<td>BC0 Broadcast header</td>
</tr>
<tr>
<td>01 111111</td>
<td>ESC</td>
<td>Additional Dispatch octet follows</td>
</tr>
<tr>
<td>10 xxxxx</td>
<td>MESH</td>
<td>Mesh routing header</td>
</tr>
<tr>
<td>11 000xxx</td>
<td>FRAG1</td>
<td>Fragmentation header (first)</td>
</tr>
<tr>
<td>11 100xxx</td>
<td>FRAGN</td>
<td>Fragmentation header (subsequent)</td>
</tr>
</tbody>
</table>
### Uncompressed IPv6/UDP (worst case scenario)

- Dispatch code (01000001) 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

![Uncompressed IPv6/UDP Format](image-url)
### Compressed Link-local IPv6/UDP (best case scenario)

<table>
<thead>
<tr>
<th>Preamble</th>
<th>802.15.4 MAC header</th>
<th>DSP</th>
<th>HC1</th>
<th>IPv6</th>
<th>UDP</th>
<th>Payload</th>
<th>FCS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>max. 23 / 44</td>
<td>1 1 1 3 8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>max. 23 / 44</td>
<td>1 1 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Dispatch code (01000010₂) 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-compressible 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 too 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)

<table>
<thead>
<tr>
<th>preamble</th>
<th>802.15.4 MAC header</th>
<th>FRAG1</th>
<th>DSP</th>
<th>HC1</th>
<th>HC2</th>
<th>IPv6 UDP</th>
<th>payload</th>
<th>FCS</th>
</tr>
</thead>
</table>

| max. 23 / 44 | 4 | 1 | 1 | 1 | 1 | 3 |

<table>
<thead>
<tr>
<th>preamble</th>
<th>802.15.4 MAC header</th>
<th>FRAGN</th>
<th>payload</th>
<th>FCS</th>
</tr>
</thead>
</table>

| max. 23 / 44 | 5 |

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?
### 6LowPAN Implementations

<table>
<thead>
<tr>
<th>Name</th>
<th>OS / License</th>
<th>Hardware</th>
<th>Maintained</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jacobs</td>
<td>TinyOS / 3BSD</td>
<td>Telos B, ...</td>
<td>no</td>
</tr>
<tr>
<td>Berkley IP</td>
<td>TinyOS / 3BSD</td>
<td>Telos B, ...</td>
<td>active</td>
</tr>
<tr>
<td>Arch Rock</td>
<td>TinyOS / EULA</td>
<td>Raven, ...</td>
<td>active</td>
</tr>
<tr>
<td>SICSslowpan</td>
<td>Contiki / 3BSD</td>
<td>Raven, ...</td>
<td>active</td>
</tr>
<tr>
<td>Sensinode</td>
<td>Own / EULA</td>
<td>Sensinode</td>
<td>active</td>
</tr>
<tr>
<td>Hitachi</td>
<td>Own / EULA</td>
<td>Renesas</td>
<td>unknown</td>
</tr>
</tbody>
</table>

Unfortunately... The Jacobs implementation uses the TinyOS Active Message framing format and thus does not interoperate.
## Feature Comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>Jacobs</th>
<th>Berkley</th>
<th>Contiki</th>
<th>Arch Rock</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dispatch Header</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Dispatch Type</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Mesh Header</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Mesh Routing</td>
<td>-</td>
<td>*</td>
<td>*</td>
<td>+</td>
</tr>
<tr>
<td>Multicasting Header</td>
<td>-</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Multicasting</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Fragmentation</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>HC1</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>HC2 for UDP</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
</tr>
<tr>
<td>HC1g</td>
<td>-</td>
<td>-</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>ICMPv6 Echo</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>

+ = supported and tested, o = supported but not tested, - = not supported, * = see [12] for details
Implementation via USB Serial Interfaces

- IPv6 stack
- Tun/Tap
- 802.11
- 802.4
- USB

User space:
- nc6
- 6lowpan rewrite

Kernel space:
- socket
- tuntap
- serial
- UDP
- TCP
- IPv6 stack
- 802.15.4
- bridging

Serial:
- USB
- 802.11
- Tun/Tap
- 802.4
- rewrite
Implementation via USB Network Interfaces

socket

nc6

libpcap

wireshark

pcap

udp tcp

kernel space

user space

IPv6 stack

802.4 802.11 USB/Net USB

BPF

6lowpan rewrite

802.15.4

USB

RNDIS
Management of 6LowPAN Networks

1. IEEE 802.15.4
   - Radio Characteristics
   - Topologies and Frame Formats
   - Media Access Control
   - Security

2. IPv6 over IEEE 802.15.4 (6LowPAN)
   - Motivation and Design Issues
   - Header Compression
   - Fragmentation and Reassembly
   - Interoperability Evaluation

3. Management of 6LowPAN Networks
   - SNMP and 6LowPANs
   - HTTP light over UDP

4. Summary
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?
Using SNMPv3 End-to-End

- Straight forward access to individual 6LowPAN nodes
- Reuse of existing deployed SNMP-based tools
  - 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
  - Reuse of existing SNMP-based tools supporting proxies
  - Two security domains, different key management schemes
    - 6LowPAN nodes must run an SNMP engine
    - Polling nature of SNMP has high energy costs
Using SNMPv3 Subagents

- Indirect access to individual 6LowPAN nodes
- Alternate transport encoding can reduce message sizes
  - Reuse of existing SNMP-based tools supporting contexts
  - Two security domains, different key management schemes
  - 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
  - Reuse of existing SNMP-based tools supporting contexts
  - Two security domains, different key management schemes
- No real advantage of 6LowPAN technology — oops
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

1. IEEE 802.15.4
   - Radio Characteristics
   - Topologies and Frame Formats
   - Media Access Control
   - Security

2. IPv6 over IEEE 802.15.4 (6LowPAN)
   - Motivation and Design Issues
   - Header Compression
   - Fragmentation and Reassembly
   - Interoperability Evaluation

3. Management of 6LowPAN Networks
   - SNMP and 6LowPANs
   - HTTP light over UDP

4. Summary
Question #7

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

IEEE.
IEEE Std 802.15.4-2006.

IEEE.
IEEE Std 802.15.4a-2007.

IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals.

G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler.
Transmission of IPv6 Packets over IEEE 802.15.4 Networks.

MAC Security and Security Overhead Analysis in the IEEE 802.15.4 Wireless Sensor Networks.

Home Networking with IEEE 802.15.4: A Developing Standard for Low-Rate Wireless Personal Area Networks.
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.

S. Labella M. Petrova, J. Riihijarvi, P. Mahonen.
Performance Study of IEEE 802.15.4 Using Measurements and Simulations.

Z. Sahinoglu and S. Gezici.
Ranging in the IEEE 802.15.4a Standard.

M. Harvan and J. Schönwälder.
TinyOS Motes on the Internet: IPv6 over 802.15.4 (6lowpan).

K. D. Korten, I. Tumar, and J. Schönwälder.
Evaluation of IPv6 over Low-Power Wireless Personal Area Networks Implementations.
In (under review), 2009.