gr-ieee802-15-4:
A flexible IEEE 802.15.4 testbed for GNU Radio

Felix Wunsch, felix.wunsch@kit.edu

Communications Engineering Lab (CEL)
Prof. Dr.rer.nat. Friedrich K. Jondral

Outline

1. SDR and The Internet of Things
2. IEEE 802.15.4
3. gr-ieee802-15-4
4. Conclusion

SDR and The Internet of Things

- New possibilities arise through massive connectivity of sensors and devices
  - Applications in , e.g., transportation, building automation, environmental monitoring and healthcare
- In 2011, the German government launched a large research project called “Industry 4.0”
  - Buzzword: “Smart Factory”
  - Goals: Increased productivity, efficiency, and flexibility
- SDR allows rapid-prototyping and field tests of new protocols and algorithms
- Many popular industry standards are based on IEEE 802.15.4

IEEE 802.15.4

- The standard defines multiple PHY layers and a MAC layer
- Modes for different modulation schemes, frequency bands and data rates
- Most popular: OQPSK PHY in the 2.4 GHz ISM band (250 kb/s)
- Also discussed: CSS PHY

Modulation	Frequency band(s) [MHz]	PHY data rate(s) [kb/s]
OQPSK	779-787, 868-868.7, 902-928, 2400-2483.5	250, 25, 250, 250
BPSK	868-868.6, 902-928, 950-956	20, 40, 20
ASK	868-868.6, 902-928	250, 250
CSS	2400-2483.5	250 or 1000
UWB	240-750, 3244-4742, 5955-10234	110-27240
MPSK	779-787	250
GFSK	950-956	100

IEEE 802.15.4 - OQPSK PHY

- DSSS system with OQPSK-modulated chips
  - DSSS: Direct Sequence Spread Spectrum
  - OQPSK: Offset Quadrature Phase-Shift Keying
- Frame structure of the PPDU (PHY Protocol Data Unit):

<table>
<tr><td colspan="5">Bytes</td></tr>
<tr><td>4</td><td>1</td><td colspan="2">1</td><td>variable</td></tr>
<tr><td>Preamble</td><td>SFD</td><td>Frame length (7 bits)</td><td>Reserved (1 bit)</td><td>PSDU</td></tr>
<tr><td colspan="2">SHR</td><td colspan="2">PHR</td><td>PHY payload</td></tr>
</table>

- Modulator:

Binary Data From PPDU → Bit-to-symbol → Symbol-to-chip → OQPSK modulator → Modulated signal

PHR: PHY Header, SHR: Synchronization Header, SFD: Start-of-frame Delimiter, PSDU: PHY Service Data Unit

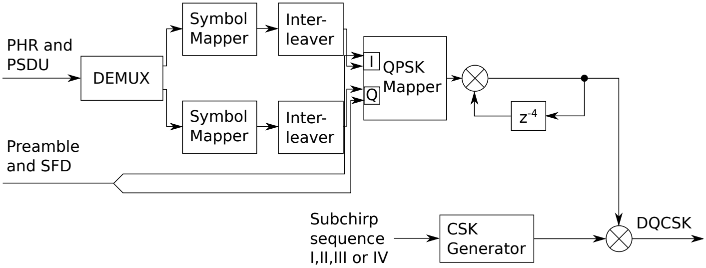
gr-ieee802-15-4 - A flexible IEEE 802.15.4 testbed for GNU Radio
Felix Wunsch, felix.wunsch@kit.edu
Communications Engineering Lab
Prof. Dr.rer.nat. Friedrich K. Jondral

IEEE 802.15.4 - CSS PHY (1)

- CSS: Chirp Spread Spectrum
- Part of the standard since 2007
- Wideband, high resilience against Doppler shifts
- Uses four (approximately) orthogonal sets of frequency ramps (chirps) for user separation
- Chirps are weighted with DQPSK symbols
  - DQPSK: Differential Quadrature Phase-Shift Keying
- Frame structure very similar to OQPSK PHY
- Two possible data rates: 1 Mb/s and 250 kb/s

IEEE 802.15.4 - CSS PHY (2)

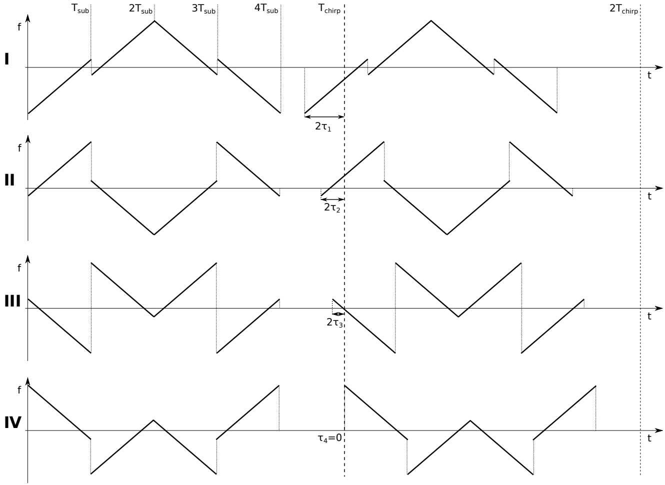
Modulator:



CSK: Chirp-Shift Keying, DQCSK: Differential Quadrature Chirp-Shift Keying

IEEE 802.15.4 - CSS PHY (3)

Time-frequency representation of the chirp sets:



gr-ieee802-15-4 - A flexible IEEE 802.15.4 testbed for GNU Radio
Felix Wunsch, felix.wunsch@kit.edu

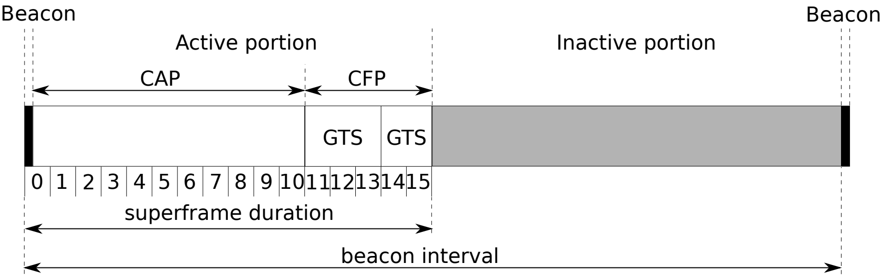
Communications Engineering Lab
Prof. Dr.rer.nat. Friedrich K. Jondral

IEEE 802.15.4 - MAC (1)

- Two modes: beacon-enabled (slotted) or nonbeacon-enabled (unslotted)
- Both modes use (variants of) CSMA-CA
  - CSMA-CA: Carrier Sense Multiple Access (Collision Avoidance)
- Nonbeacon-enabled:
  - Simplest mode
  - Devices are not synchronized
- Beacon-enabled:
  - All devices synchronize on super frames
  - Frame is divided into slots
  - Slots can be assigned exclusively to devices
    $\rightarrow$ Deterministic latency

IEEE 802.15.4 - MAC (2)

Structure of super frames in beacon-enabled mode:



CAP: Contention Access Period, CFP: Contention-free Period, GTS: Guaranteed Time Slot

gr-ieee802-15-4 (1)

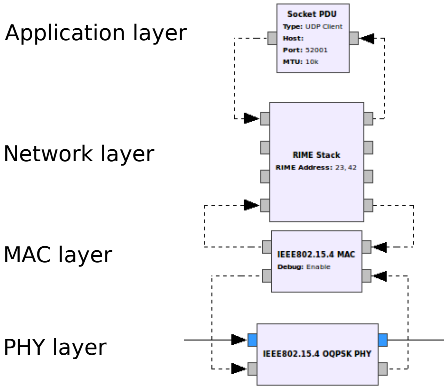
- Hosted on GitHub, maintained by Bastian Blössl
- Based on the OQPSK PHY implementation of Thomas Schmid at UCLA
- Components:
  - OQPSK and CSS PHY encapsulated in hierarchical blocks (interchangeable)
  - (Simplified) MAC block
  - Block that implements Rime, a lightweight communication stack for sensor networks (part of the Contiki OS)
- The modular design closely follows the OSI model
- Complete transceiver flowgraphs available
- Interoperable with TelosB sensor motes

GNURadio
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

&

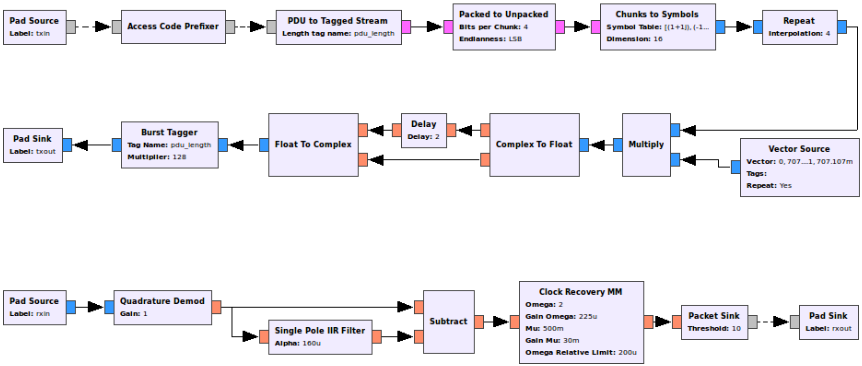
gr-ieee802-15-4 (2)

GRC flowgraph following the OSI model:



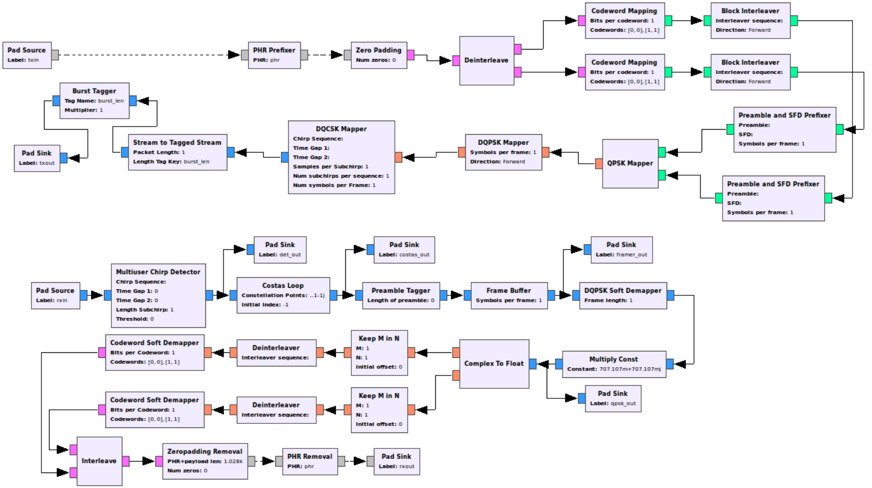
gr-ieee802-15-4 (3)

OQPSK PHY hier block:



gr-ieee802-15-4 (4)

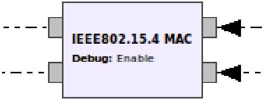
CSS PHY hier block:



gr-ieee802-15-4 (5)

MAC block:

- Only a simplified version implemented:
  - Adds the MAC header for a data frame
  - Calculates and adds a 16 bit CRC word
  - No medium access algorithm
- Non-deterministic latencies are too large
- Example: The maximum wait time for an ACK frame is less than a millisecond



Conclusion

- Implements two IEEE 802.15.4 PHY layers, a simplified MAC and a network layer protocol
- Full GRC integration with a design following the OSI model
- Interoperable with commercially available sensor devices
- Fully customizable
- Easily extendable (even with `gr_modtool`):
  - Additional PHY layers
  - Medium access algorithms
  - ... and more!

Thank you for your attention! Questions?