Internet of #allthethings

GNURadio for IEEE 802.15.4 Networking

FOSDEM'15

Christopher Friedt
Principle Embedded Firmware Engineer

chris@mmbnetworks.com
chrisfriedt@gmail.com

GNURadio
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

code available at http://github.com/cfriedt

Overview

Overview of IEEE 802.15.4
Some 802.15.4-Enabled Devices
Open-Source 802.15.4 Stack / HW?
Hardware Components
Software Components
Radio & Network Architecture
Observations / Discussion
Questions?
Citations

Simply Connected

Overview of IEEE 802.15.4
Some 802.15.4-Enabled Devices
Open-Source 802.15.4 Stack / HW?
Hardware Components
Software Components
Radio & Network Architecture
Observations / Discussion
Questions?
Citations

Overview of IEEE 802.15.4

- Standard for Physical Layer and Media Access Control Layer for several network protocols and application stacks
    - **ZigBee** - requires licensing / certification for commercial purposes
    - **6LowPan** - royalty free
    - **RIME** - used in the Contiki OS
- Low-Rate Wireless Personal Area Networks (LR-WPAN)
- Typically use in wireless sensor and control networks
    - Smart Switches, Door Locks, Thermostats, Blinds, Lighting, Fans
    - Appliances, Coffee Makers, Dishwashers, Laundry, Solar
    - Power Metering, Security Systems, Electric Vehicle Chargers, Light Rail
- Similar technologies: Z-Wave, Insteon - proprietary, not IEEE ratified

Simply Connected

Overview of IEEE 802.15.4: Spectrum

PHY (MHz)	Frequency band (MHz)	Spreading parameters		Data parameters		
		Chip rate (kchip/s)	Modulation	Bit rate (kb/s)	Symbol rate (ksymbol/s)	Symbols
780	779–787	1000	O-QPSK	250	62.5	16-ary orthogonal
780	779–787	1000	MPSK	250	62.5	16-ary orthogonal
868/915	868–868.6	300	BPSK	20	20	Binary
	902–928	600	BPSK	40	40	Binary
868/915 (optional)	868–868.6	400	ASK	250	12.5	20-bit PSSS
	902–928	1600	ASK	250	50	5-bit PSSS
868/915 (optional)	868–868.6	400	O-QPSK	100	25	16-ary orthogonal
	902–928	1000	O-QPSK	250	62.5	16-ary orthogonal
950	950–956	—	GFSK	100	100	Binary
950	950–956	300	BPSK	20	20	Binary
2450 DSSS	2400–2483.5	2000	O-QPSK	250	62.5	16-ary orthogonal

[1]

Simply Connected

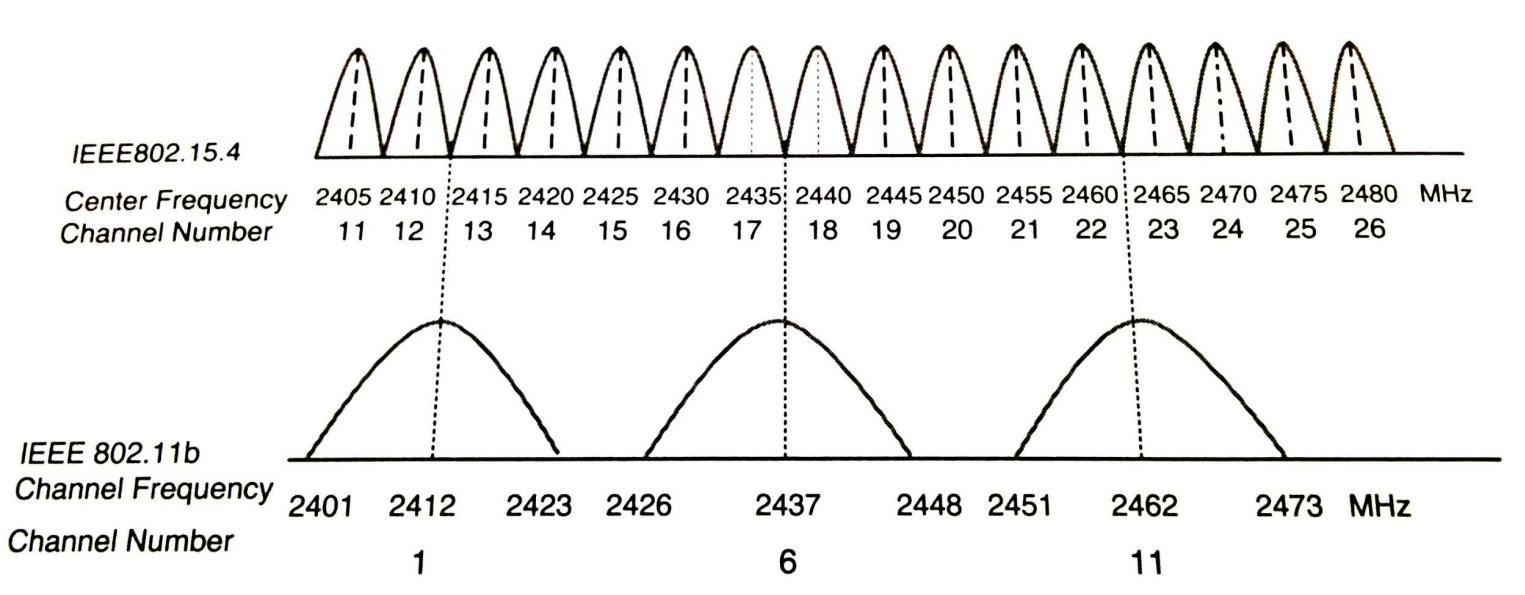
Overview of IEEE 802.15.4: Spectrum

UWB sub-gigahertz (optional)	250–750	As defined in 14.4.1				
2450 CSS (optional)	2400–2483.5	As defined in 13.2		250	167 (as defined in 13.4.2)	
		As defined in 13.2		1000	167 (as defined in 13.4.2)	
UWB low band (optional)	3244–4742	As defined in 14.4.1				
UWB high band (optional)	5944–10 234	As defined in 14.4.1				

[1]

Simply Connected

Overview of IEEE 802.15.4: ISM Channels



[2]

Simply Connected

Overview of IEEE 802.15.4: O-QPSK PHY

The PHY Protocol Data UNIT (**PPDU**)

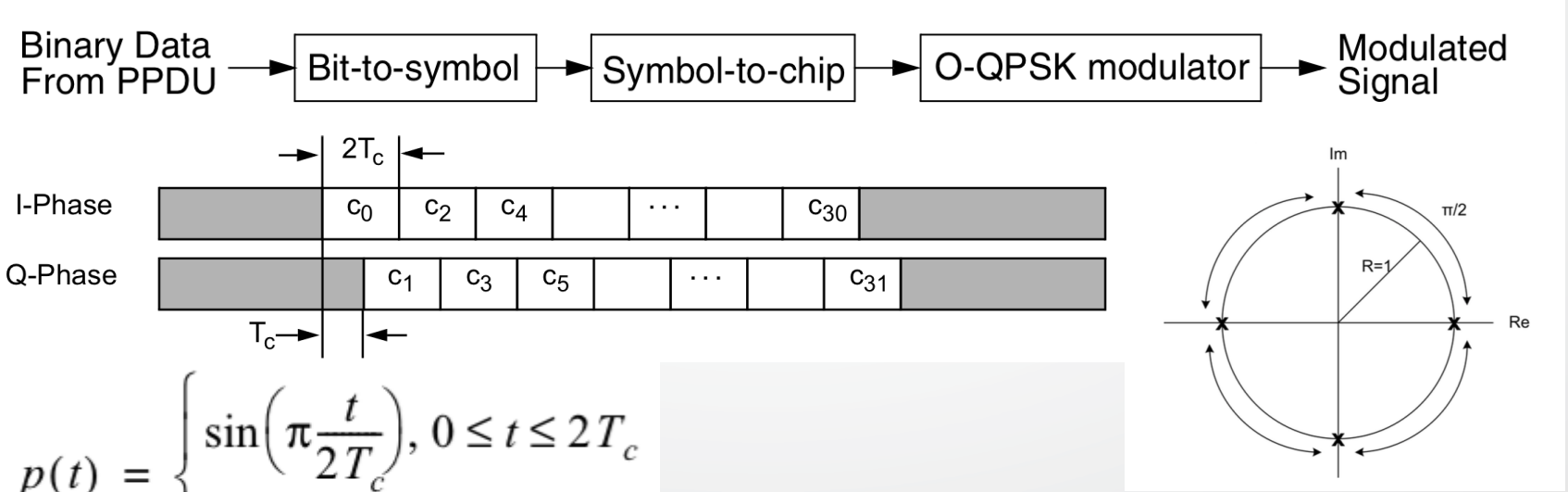
- Synchronization Header (**SHR**), Physical Header (**PHR**)
- PHY Service Data Unit (**PSDU**) - from MAC layer
- Preamble is 4 octets - all zero
- Start of Frame Delimiter (**SFD**) - 1 octet 0xA7
- Maximum frame length of 127 octets
- transmitted ***LITTLE ENDIAN, least significant octet first*** !!

		Octets		
		1		variable
Preamble	SFD	Frame length (7 bits)	Reserved (1 bit)	PSDU
SHR		PHR		PHY payload

[1]

Overview of IEEE 802.15.4: O-QPSK PHY

The PHY transmitter maps 4-information bits to for chips



$$p(t) = \begin{cases} \sin\left(\pi \frac{t}{2T_c}\right), & 0 \le t \le 2T_c \\ 0, & \text{otherwise} \end{cases}$$

[1], [4]

Simply Connected

Overview of IEEE 802.15.4: O-QPSK PHY

Symbol-to-Chip Mapping

- Block code characterized as $(n,k,d)_q \Leftrightarrow (4,32,12)_2$
- Recall from Channel Coding 101
  - d : minimum Hamming distance between dissimilar chips
  - n: data symbol size
  - k: channel symbol size
  - q: alphabet cardinality
- More about that later

Data symbol	Chip values (c_0 c_1 … c_{30} c_{31})
0	11011001111000011010100100010111 0
1	11101101100111000011010100100010
2	00101111011011001111000011010100 10
3	00100010111011011001111000011010 1
4	01010010001011101101100111000011
5	00110101001000101110110110011100
6	11000011010100100010111011011001
7	10011100001101010010001011101101
8	10001100100101100000011101111011
9	10111000110010010110000001110111
10	01111011100011001001011000000111
11	01110111101110001100100101100000
12	00000111011110111000110010010110
13	01100000011101111011100011001001
14	10010110000001110111101110001100
15	11001001011000000111011110111000

[1]

Simply Connected

Overview of IEEE 802.15.4: O-QPSK PHY

The PHY is additionally responsible for providing

- Link Quality Indicator (**LQI**)
  - measure of *data integrity*
  - propagated up to the Application Support Sublayer (**APS**)
- Receiver Energy Detection (**ED**)
  - often called Received Signal Strength Indicator (**RSSI**)
  - measure of in-channel power
  - propagated up to APS

[1]

Overview of IEEE 802.15.4: MAC

The MAC Frame Format and Frame Control Field

- MAC Header (MHR), MAC Footer (MFR)
- Frame Checksum (FCS) - CRC16
- Acknowledgement Request (AR)

Octets: 2	1	0/2	0/2/8	0/2	0/2/8	0/5/6/10/14	variable	2
Frame Control	Sequence Number	Destination PAN Identifier	Destination Address	Source PAN Identifier	Source Address	Auxiliary Security Header	Frame Payload	FCS
		Addressing fields						
MHR							MAC Payload	MFR

[1]

Bits: 0–2	3	4	5	6	7–9	10–11	12–13	14–15
Frame Type	Security Enabled	Frame Pending	AR	PAN ID Compression	Reserved	Dest. Addressing Mode	Frame Version	Source Addressing Mode

Overview of IEEE 802.15.4: MAC

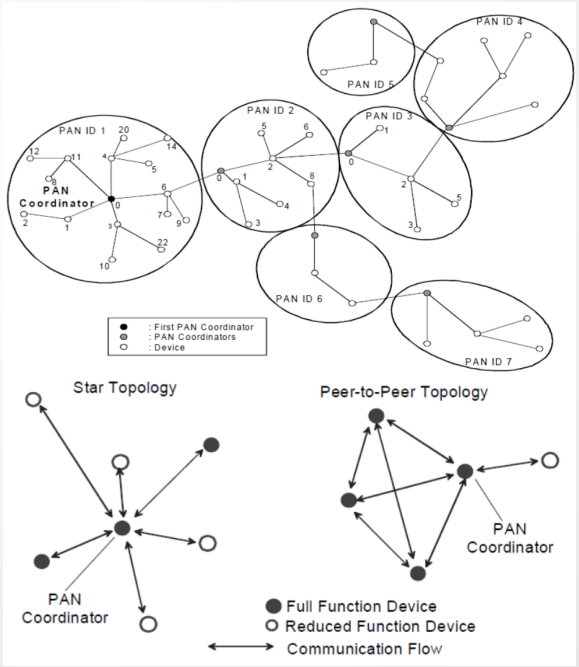
The MAC is additionally responsible for providing

- Transmission of data
- Purge data (opt)
- Reception of data
- Beacon management
- Transmit beacons (opt)
- Receive beacons
- Channel access mechanism
- Frame validation
- ACK delivery
- Security
- Unsecured mode
- ED
- Passive scanning
- Orphan scanning
- Store one transaction

[1]

Overview of IEEE 802.15.4: Network

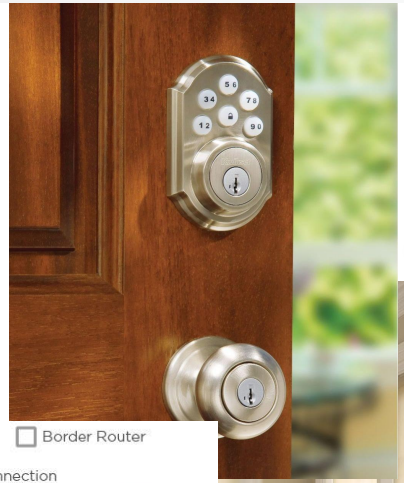
- Mesh networking topologies
  - star - devices connect to a single coordinator
  - tree - devices connect to a router, routers connect to coordinator
  - mesh - devices communicate with multiple routers and 1 coord.
- Nodes are either
  - coordinators (1 per net, powered, often acts as gateway or bridge)
  - routers (powered)
  - end-devices (do not forward packets, often battery powered)

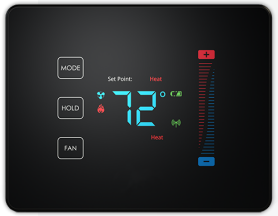


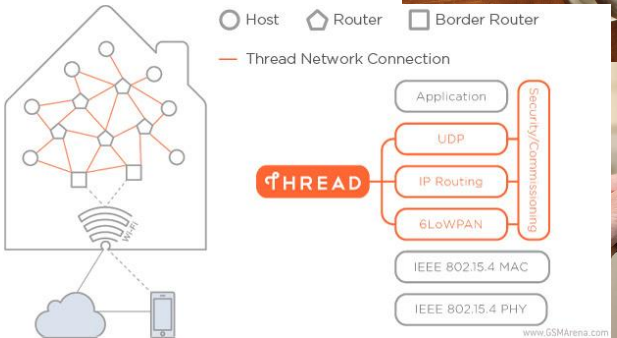
[1]

Overview of IEEE 802.15.4
Some 802.15.4-Enabled Devices
Open-Source 802.15.4 Stack / HW?
Hardware Components
Software Components
Radio & Network Architecture
Observations / Discussion
Questions?
Citations

Some 802.15.4-Enabled Devices: Consumer







Simply Connected

Simply Connected

Open-Source IEEE 802.15.4 Stack / HW?

Why?

- Quickly develop application logic in a native application
- Design & extensively test new products before costly certification
- Develop IEEE 802.15.4 compatible networking stack
- Security research

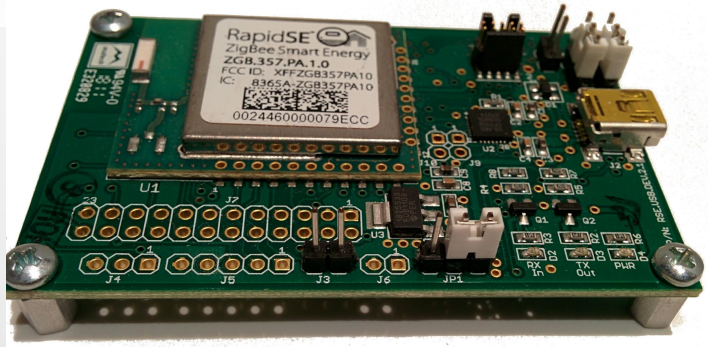
Overview of IEEE 802.15.4
Some 802.15.4-Enabled Devices
Open-Source 802.15.4 Stack?
Hardware Components
Software Components
Radio & Network Architecture
Observations / Discussion
Questions?
Citations

Simply Connected

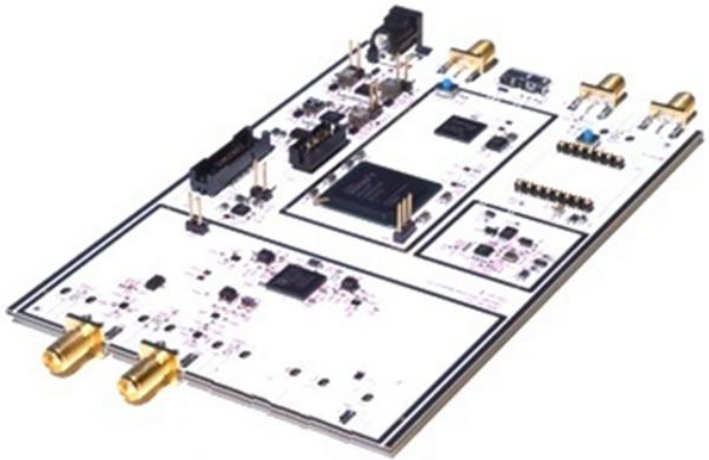
Hardware Components

USB Module from RapidConnect Kit*

Dev Board from RapidConnect Kit*



USRP B200 from Ettus Research



* products of MMB Networks

Overview of IEEE 802.15.4
Some 802.15.4-Enabled Devices
Open-Source 802.15.4 Stack?
Hardware Components
Software Components
Radio & Network Architecture
Observations / Discussion
Questions?
Citations

Software Components

FreakZ Zigbee* Stack

- BSD (+ ZigBee Clause) License
- i.e. you must be part of the ZigBee Alliance to use ZigBee spec for commercial purposes
- Portable code - I added autotools support
- added native shared library (libfreakz)
- modified test_sim => test_udp
- no requirement for Contiki runtime
- discussion...

gr-ieee802154

- Code originally came from UCLA (Shmid)
- Seemingly lost for some time when CGRAN was down
- Updated to use Protocol Data Unit (PDU) (Bloessl et al), on GitHub. RIME support added
- removed RIME block from demo
- discussion...

* MMB Networks does not endorse the FreakZ stack as being ZigBee certified.

Overview of IEEE 802.15.4
Some 802.15.4-Enabled Devices
Open-Source 802.15.4 Stack?
Hardware Components
Software Components
Radio & Network Architecture (See Demo)
Observations / Discussion
Questions?
Citations

Radio & Network Architecture

FreakZ Zigbee* Stack

- NWK Layers & Above
- Simply connected to GRC via UDP socket

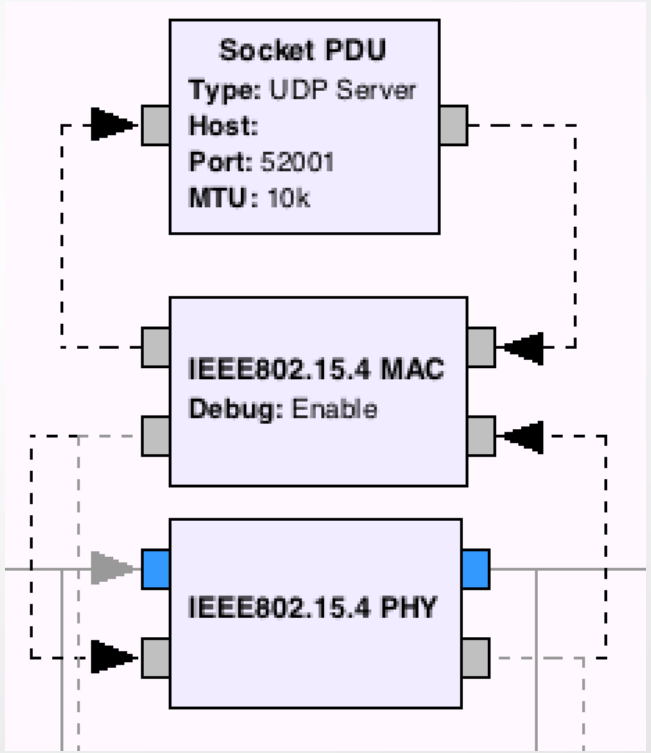
gr-ieee802154

- PHY implemented as hierarchical block

Radio & Network Architecture

FreakZ Zigbee Stack

- NWK Layers & Above
- Simply connected to GRC via UDP socket

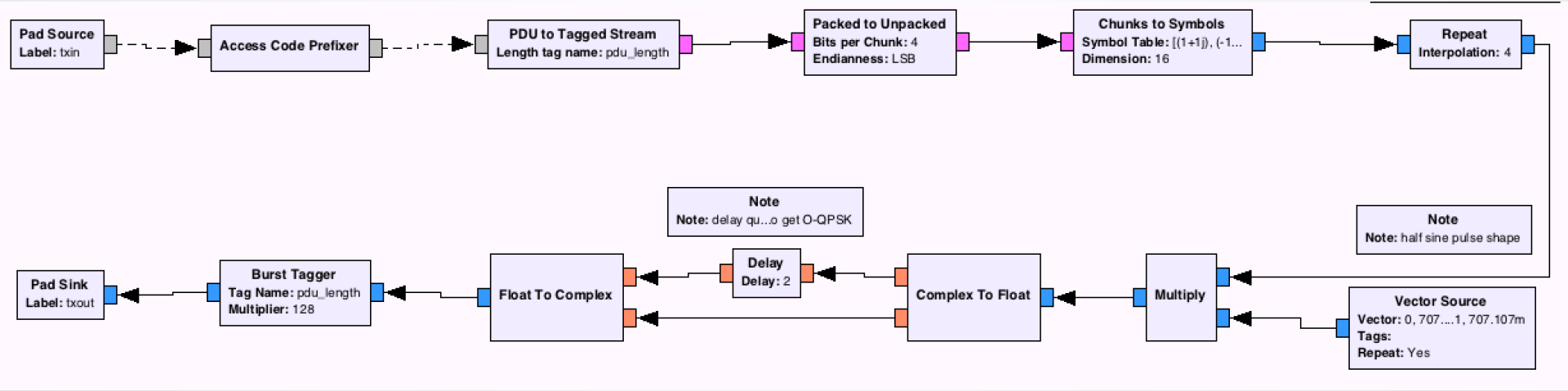


based on [5]

Radio & Network Architecture

gr-ieee802154

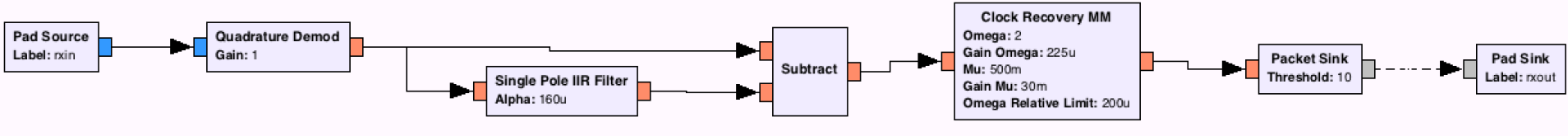
- PHY implemented as hierarchical block



Radio & Network Architecture

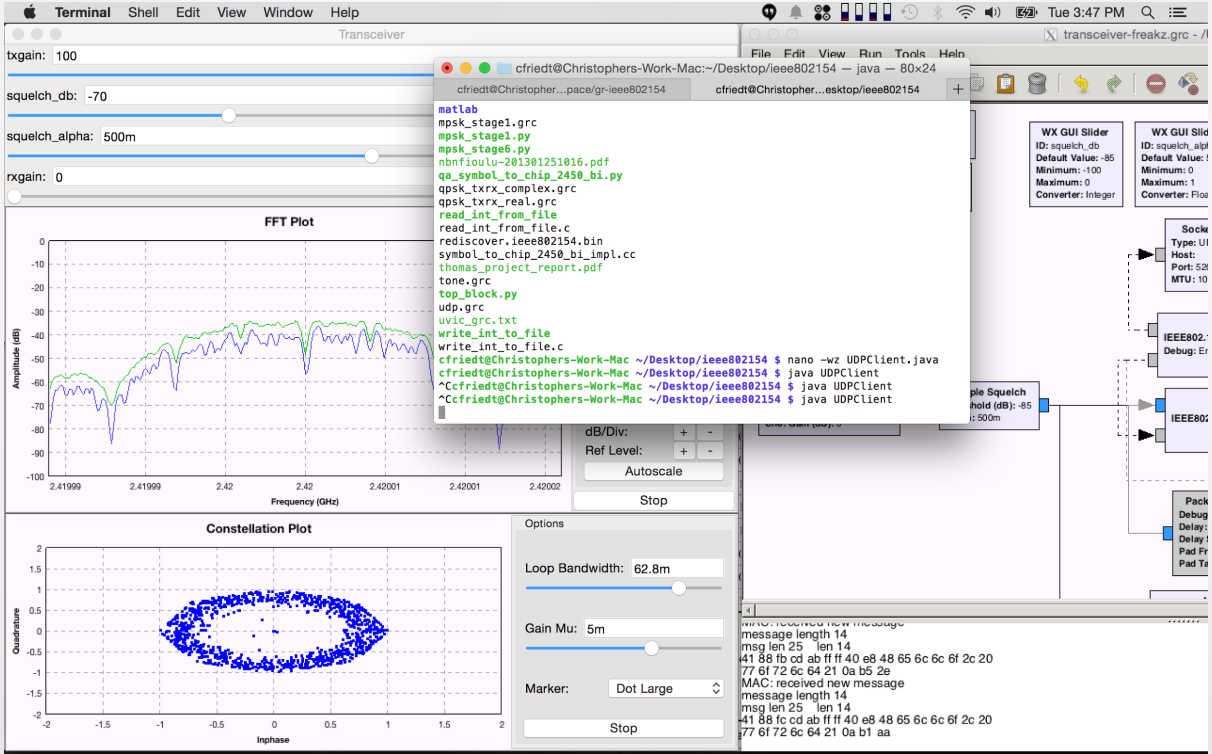
gr-ieee802154

- PHY implemented as hierarchical block



- Overview of IEEE 802.15.4
- Some 802.15.4-Enabled Devices
- Open-Source 802.15.4 Stack?
- Hardware Components
- Software Components
- Radio & Network Architecture
- Observations / Discussion
- Questions?
- Citations

Observations / Discussion



Simply Connected

Observations / Discussion

gr-ieee802154

- shift register was encoded incorrectly upstream
- chip 0 eventually shifted into MSB rather than LSB
- FEC: block code $(n,k,d)_q$ $(4,32,12)_2$ code can theoretically only detect d-1 = 11 errors, and can correct up to floor((d-1)/2) = 5 errors.
- packet_sink.threshold = 10. Best effort -> CRC16? Needs additional check < 5 => MMSE gives correct result.
- Still requires improved CR & freq / phase compensation

GNURadio

- might have found a bug in block execution (max_noutput_items)
- for that purpose, PDU's / messages / tagged stream worked much better
- PDU's / message passing still a bit unclear for (at least 1) beginner

gr_modtool

- surprisingly easy to get started with

Overview of IEEE 802.15.4
Some 802.15.4-Enabled Devices
Open-Source 802.15.4 Stack?
Hardware Components
Software Components
Radio & Network Architecture
Observations / Discussion
Questions?
Thanks
Citations

Thanks!

- the various people on **#gnuradio** on FreeNode
- **Philip Ballister**, **Matt Ettus** for answering some USRP questions
- **Marcus Müller** and others on the gnuradio-discuss mailing list
- **Thomas Schmid**, **Bastian Bloessl** for initial work on **gr-ieee802_15_4**
- **Hongbo Zhong** for the BSD+ZigBee licenced **FreakZ** stack
- **GNURadio** authors and contributors

Citations

[1] IEEE Std 802.15.4-2011
[2] Elahi, A., Gschwender, A. “ZigBee Wireless Sensor and Control Network”, 2009.
[3] Schmid, T. “GNU Radio 802.15.4 En- and Decoding”, 2006.
[4] Koteng, R.M. “Evaluation of SDR-implementation of IEEE 802.15.4 Physical Layer”, 2006.
[5] Bloessl, B. et al, “A GNU Radio-based IEEE 802.15.4 Testbed”, 2013.