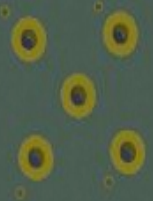


Multi-channel Wardriving Tools for IEEE 802.15.4 and Beyond

@tomx4096
@aurelsec

Plan:

Chapter I: IEEE 802.15.4: Brief Primer & History

Chapter II: Multi-channel, why, how and how not

Chapter III: Tomorrow’s Designs, Soon

Chapter I: IEEE 802.15.For Your Information

IEEE standard for PHY and MAC layers of **Short Range**, **Low Rate**, Wireless Networks

(<10meters, 250kbps)

Home and building automation, industrial control, Healthcare, smart meters IoT..

Chapter I: IEEE 802.15.For Your Information

IEEE standard for PHY and MAC layers of **Short Range**, **Low Rate**, Wireless Networks

(<10meters, 250kbps)

Home and building automation, industrial control, Healthcare, smart meters IoT..

Who uses this?

6LoWPAN

IPv6-based Low-power
Wireless Personal Area Networks

WirelessHART

ISA 100 WIRELESS

THREAD

ZigBee®

Home

Health

Energy

Telecom

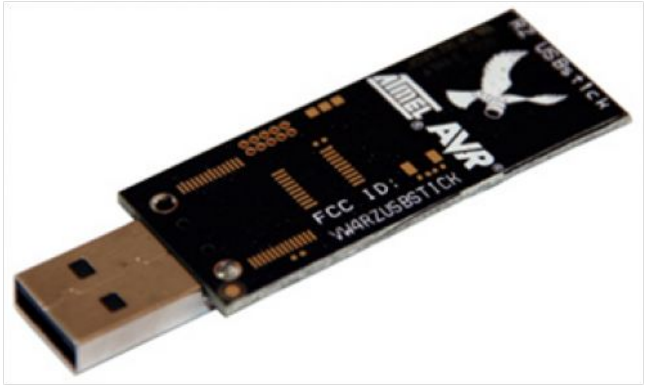
Retail

Building

Light

IEEE 802.15.4 In the News

Renaud Lifchitz "**ZigBee security review of a famous French set-top box**"



ZigBee RF4CE - Remote Controls

1 Force De-association
2 Sniff seed bytes
3 reconstruct key
…
Arbitrary Access to victim subscriber's LAN, phone line, voicemails, channel subscriptions!

IEEE 802.15.4 In the News

Renaud Lifchitz "**ZigBee security review of a famous French set-top box**"

Best practices for wireless security

Threats & countermeasures

Threats	Good countermeasures
Passive snooping	- Secure key exchange (ex.: Diffie-Hellman) - Encryption
Volontary or involuntary jamming	- Spread spectrum - Frequency/channel hopping
Usurpation (ex.: replay)	- Anti-replay mechanisms (cryptographic « nonce ») - Authentication using a challenge

P. 34 ZigBee security review of a famous French set-top box - Digital Security

Chapter I: IEEE 802.15.For Your Information

IEEE standard for PHY and MAC layers of **Short Range**, **Low Rate**, Wireless Networks

(<10meters, 250kbps)

Home and building automation, industrial control, Healthcare, smart meters IoT..

Why not 802.11?

Why not bluetooth?

IEEE 802.15.4 Features

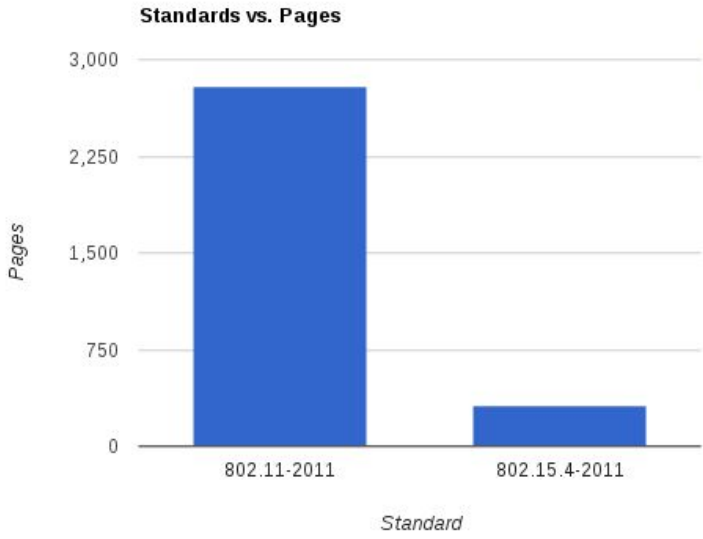
Simplicity <--> Good Economy ($, time and MWh)

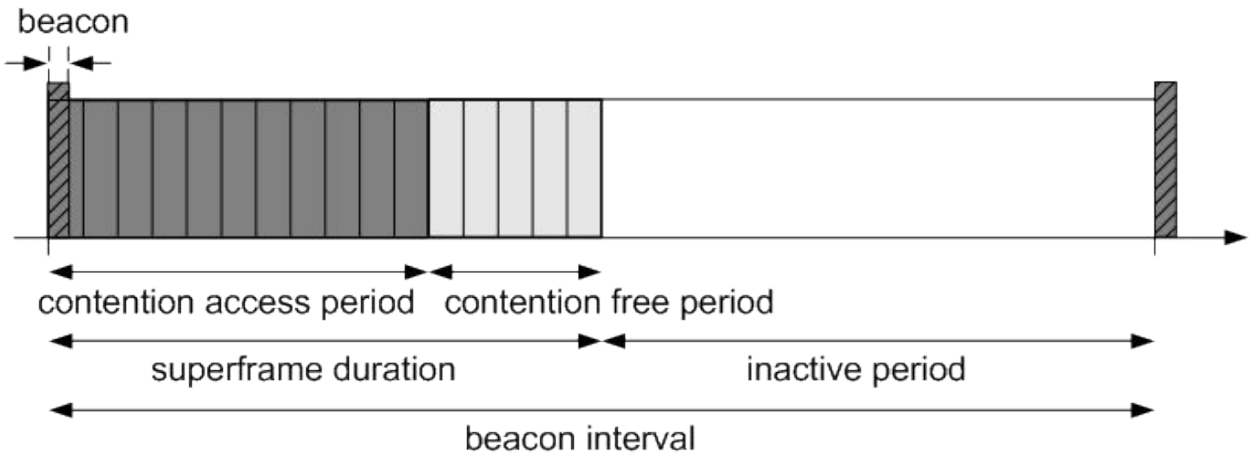
CSMA/CA

Guaranteed Time Slots

Contention Access/Contention Free periods

Security - Encryption, MACs





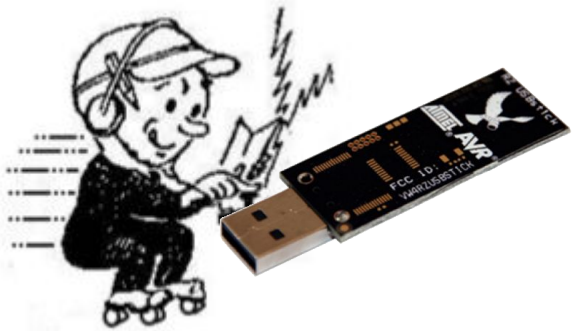
Chapter II: Multi-channel Motivation

~~1989 I want it all~~
~~1996 gotta catch ‘em all!~~
~~1998 don’t wanna miss a thing~~
2016 gotta catch ‘em all!

http://loops-of-fury.deviantart.com/art/Wall-of-Televisions-114119454

Multi-channel Motivation

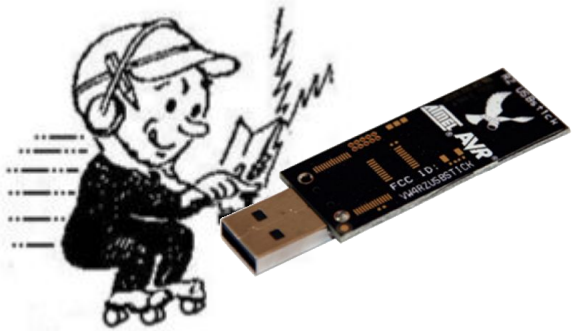
Typical Wardriving Scenario:



The wardriver's goal is to maximize the information collected from target networks in the course of moving through an unfamiliar environment

Multi-channel Motivation

Typical Wardriving Scenario:



KillerBee - passive and active scans

Maybe we'll get everything if we go slow enough..but we're busy and want to discover the most networks in the least amount of time

Multi-channel Motivation:

Low Rate wireless networks ->
quieter protocols, fewer messages

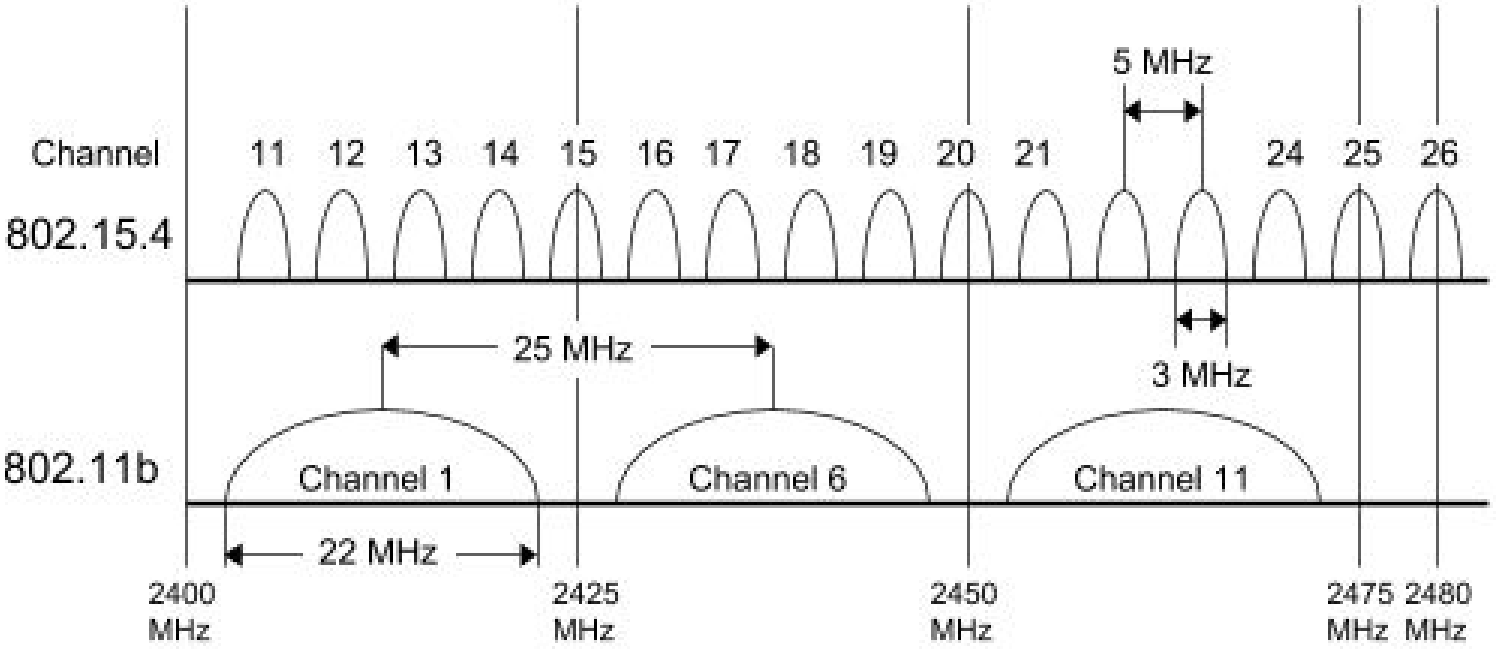
Mobility of wardrivers through **short range** ->
Time spent “in range” is reduced

Channel scanning ->
Is NOT the most effective use of this limited time

Channel hopping protocols ->
Make our precious time even less effective!

Every-channel sniffing improves our chance of stumbling upon new networks

Multi-channel Motivation



https://www.semanticscholar.org/paper/Improving-wireless-simulation-through-noise-Lee-Cerpa/0cd9928a64737e184b230c9121c3133910576831/figure/2

16 channels

80 MHz chunk of bandwidth

What can we do?

Build a cluster of receivers

Use an SDR or a cluster of SDRs

Build a new device

Multi-channel Tradition

Ban et al. (2007): Implementation of IEEE 802.15. 4 packet analyzer

L. Choong (2009): Multi-channel IEEE 802.15. 4 packet capture using software defined radio

Josh Wright. (2011): Killerbee: practical zigbee exploitation framework

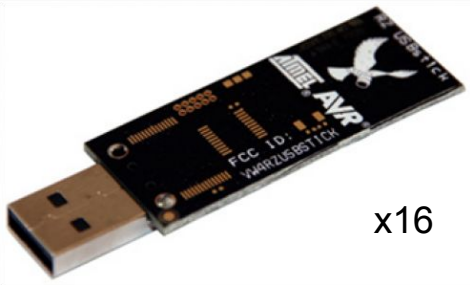
Speers et al. (2011): Api-do: Tools for Zig-Bee and 802.15. 4 Security Auditing

Goodspeed et al. (2012): Api-do: Tools for exploring the wireless attack surface in smart meters

Yoo et al. (2014): Multi-channel packet-analysis system based on IEEE 802.15. 4 packet-capturing modules

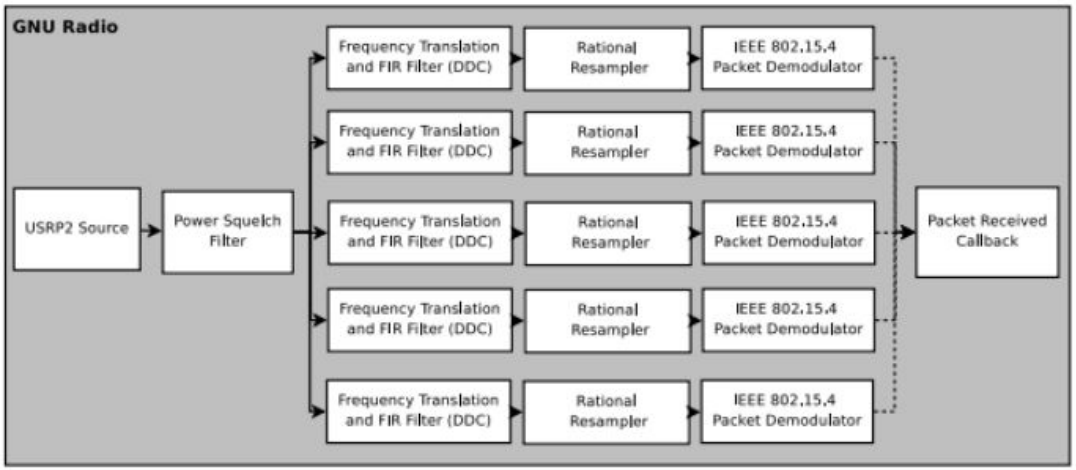
What can we do?

COTS Hardware Receiver arrays - use ZBOpenEar and a cluster of existing devices (RZUSBs or Api-Motes) for each channel



x16

Software Defined Radio - receive a chunk of bandwidth and carve out the different channels



Custom Hardware - specifically designed for multiple frequencies

Main board Radio board

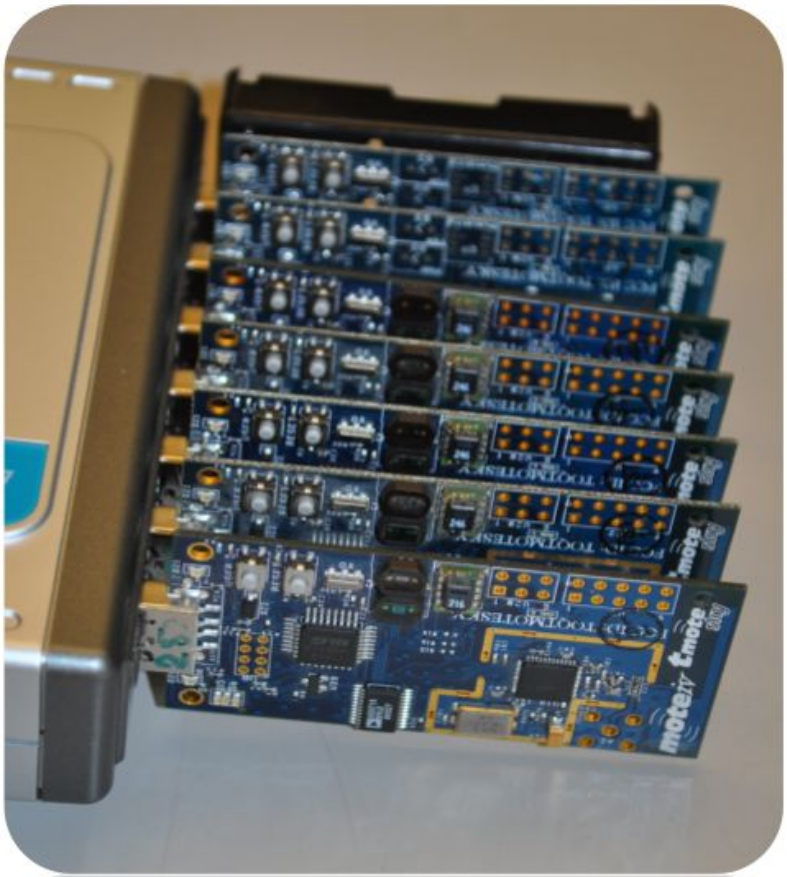
How about a hardware cluster?

Simple, gets the job done

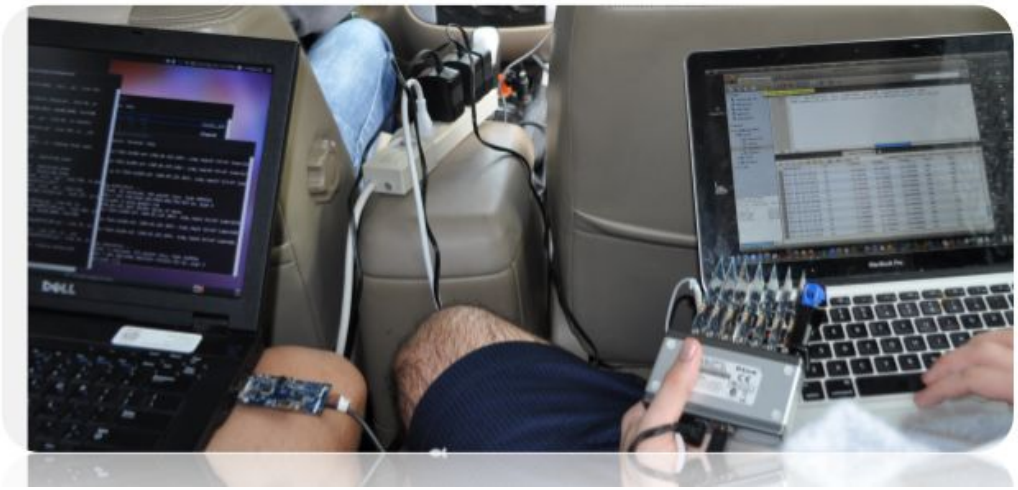
….for a price.. ($40 * 16 + USB Hub ~ $700 USD)

ZBOpenEar, KillerBee tools

Conspicuous, rigid hardware setup



802.15.4 find, fix finish: Ryan Speers and Ricky Melgares
ToorCon Seattle



How about SDR?

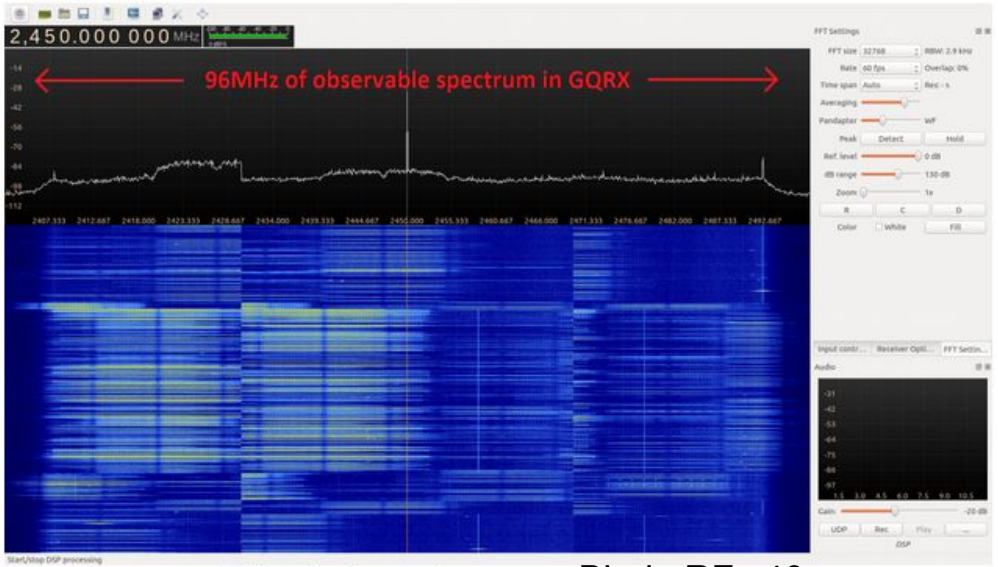
Hopefully, one day..

Analog-Digital Conversion is the weak link- dynamic range limits performance of the receiver

Sampling ~80 MHz of bandwidth well enough to decode packets?

Large computational effort to demod packets

Cost, learning curve, power...

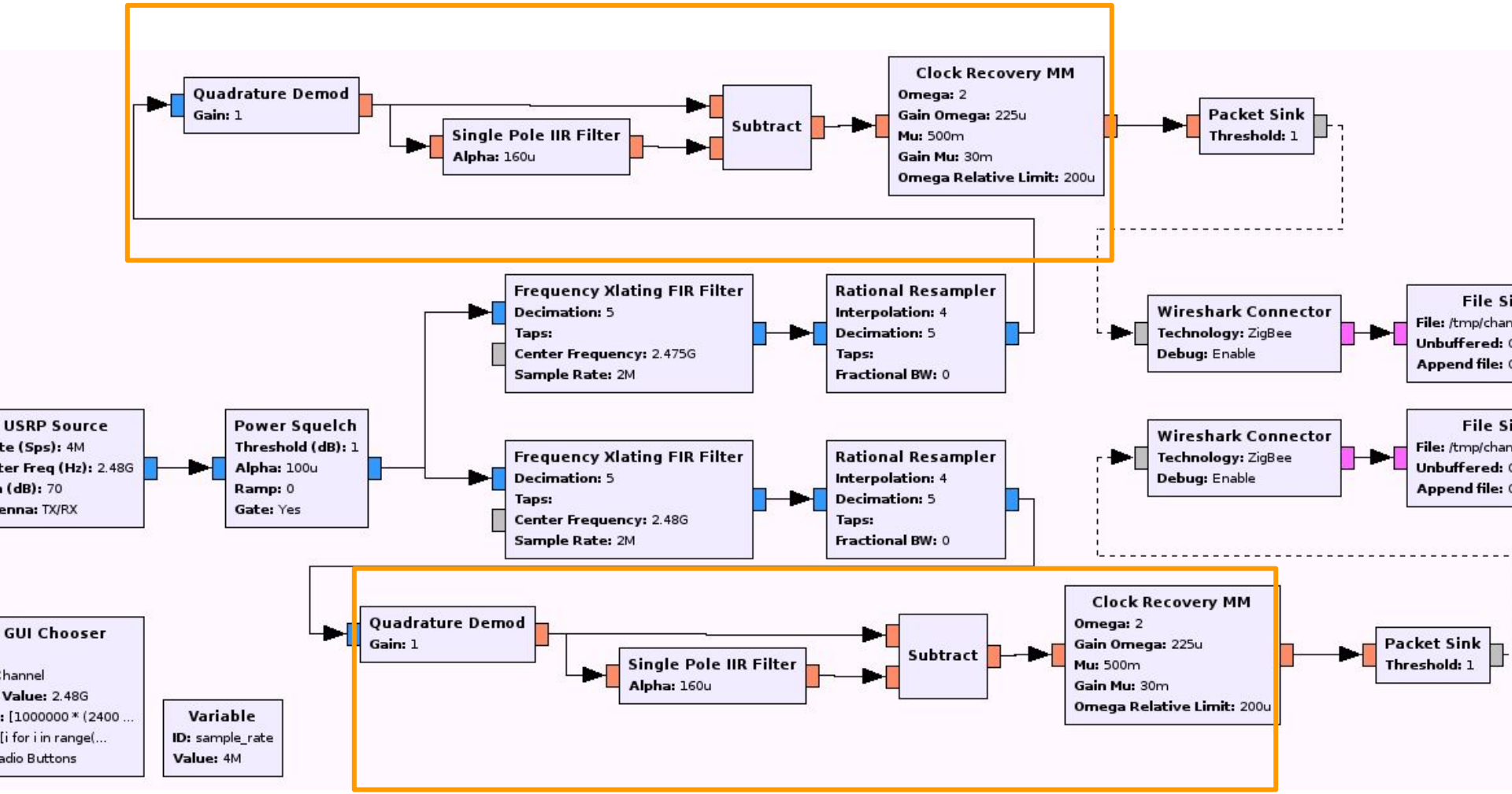


Monitor the entire 2.4GHz band with one radio.

Blade RF x40

Spot the SDRs

The GNURadio approach



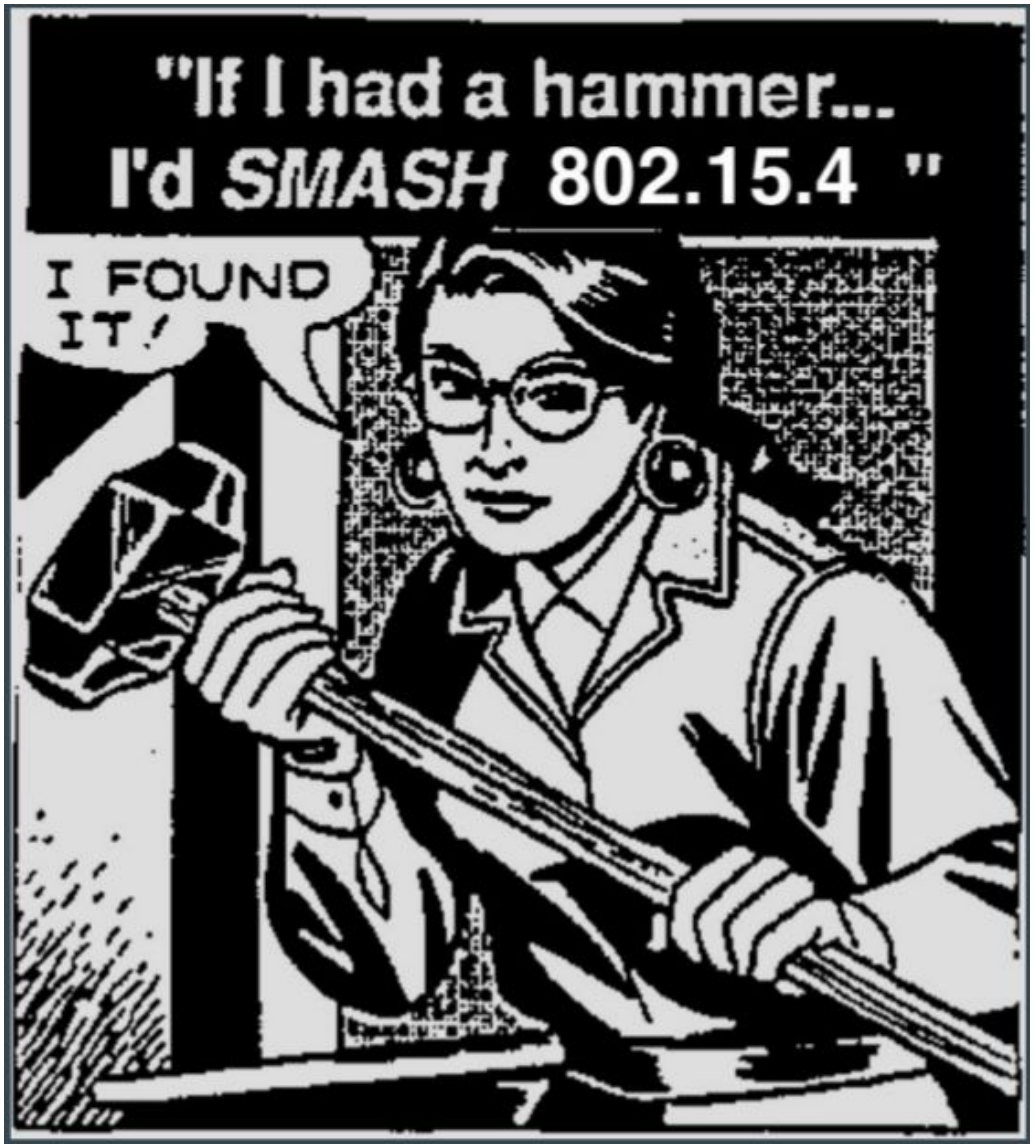
Leslie Choong's multi-channel approach + Bastian Bloessel's IEEE 802.15.4 demodulation

How about a new device?

Solutions in academic literature are often not portable/ hackable/open source (exception: Api-Mote)

Hardware clusters are **big**, **expensive**, **power hungry**

SDRs are **big**, **clunky**, **expensive**, **power hungry**, have a **steep learning curve,** and **limited performance** in some cases



Chapter III: Goals for a new design:

DG1. Complete simultaneous coverage

Parallel reception of all 16 channels of the 2.4 GHz 802.15.4 band

DG2. Easy to use

No learning curve beyond "Plug it in and run KillerBee tools"

DG3. Relatively cheap

The price to beat is 16 RZUSBs + USB hubs

DG4. Portable and discreet

One piece, one antenna, fits in a shoe box, will not capture the wrong attention

DG5. Extensible

Accommodates peripherals like GPS, WiFi, SD card, etc.

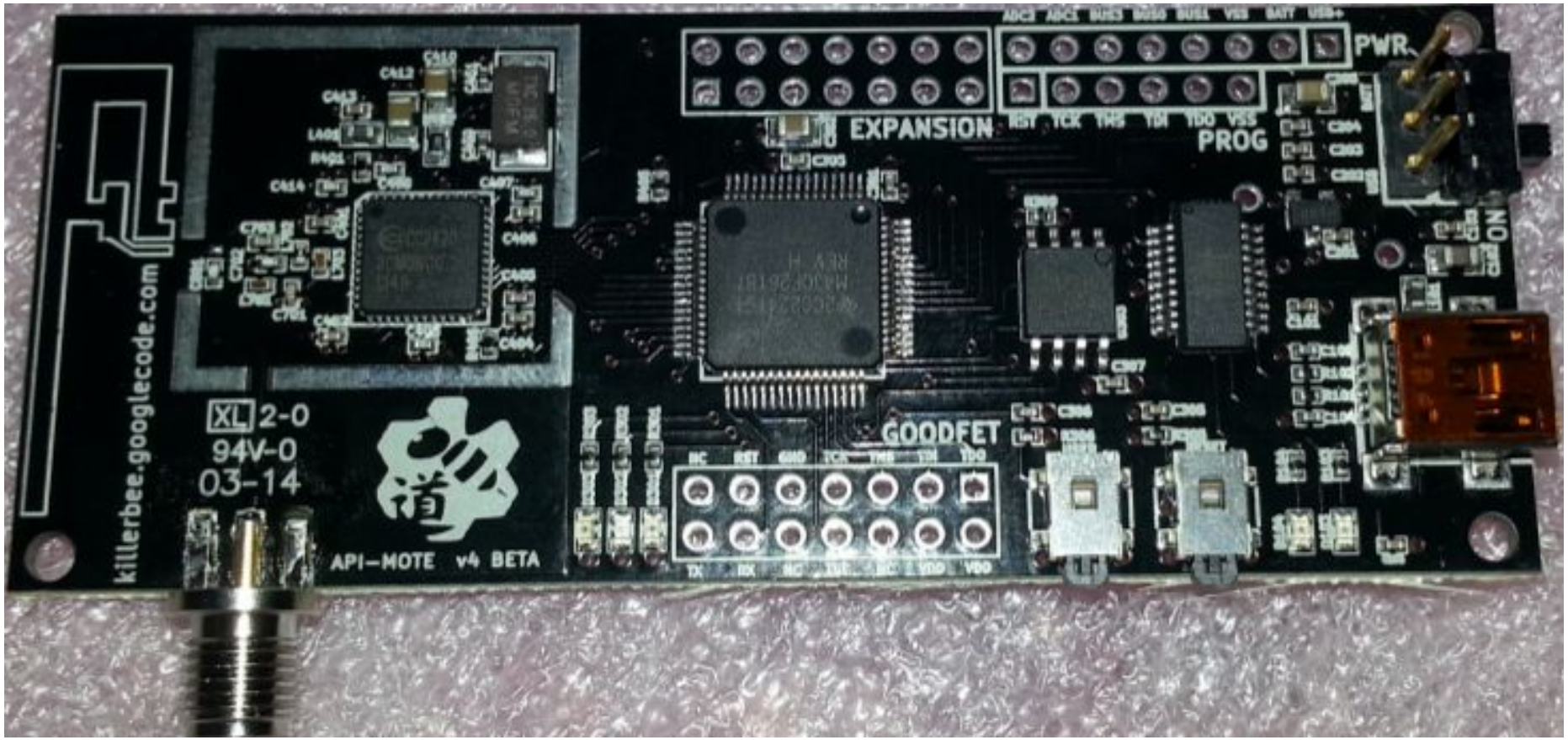
DG6. Robust performance

Good reception indoors, outdoors, with Wifi/Bluetooth interference

Properties of 802.15.4 multi-channel sniffers

	Full Coverage	Easy	Cheap	Discreet	Extensible	Performant
COTS RX array	✓					
SDR						
Custom Hardware		✓	✓	✓		

Api-mote v4 Design



v4 Design

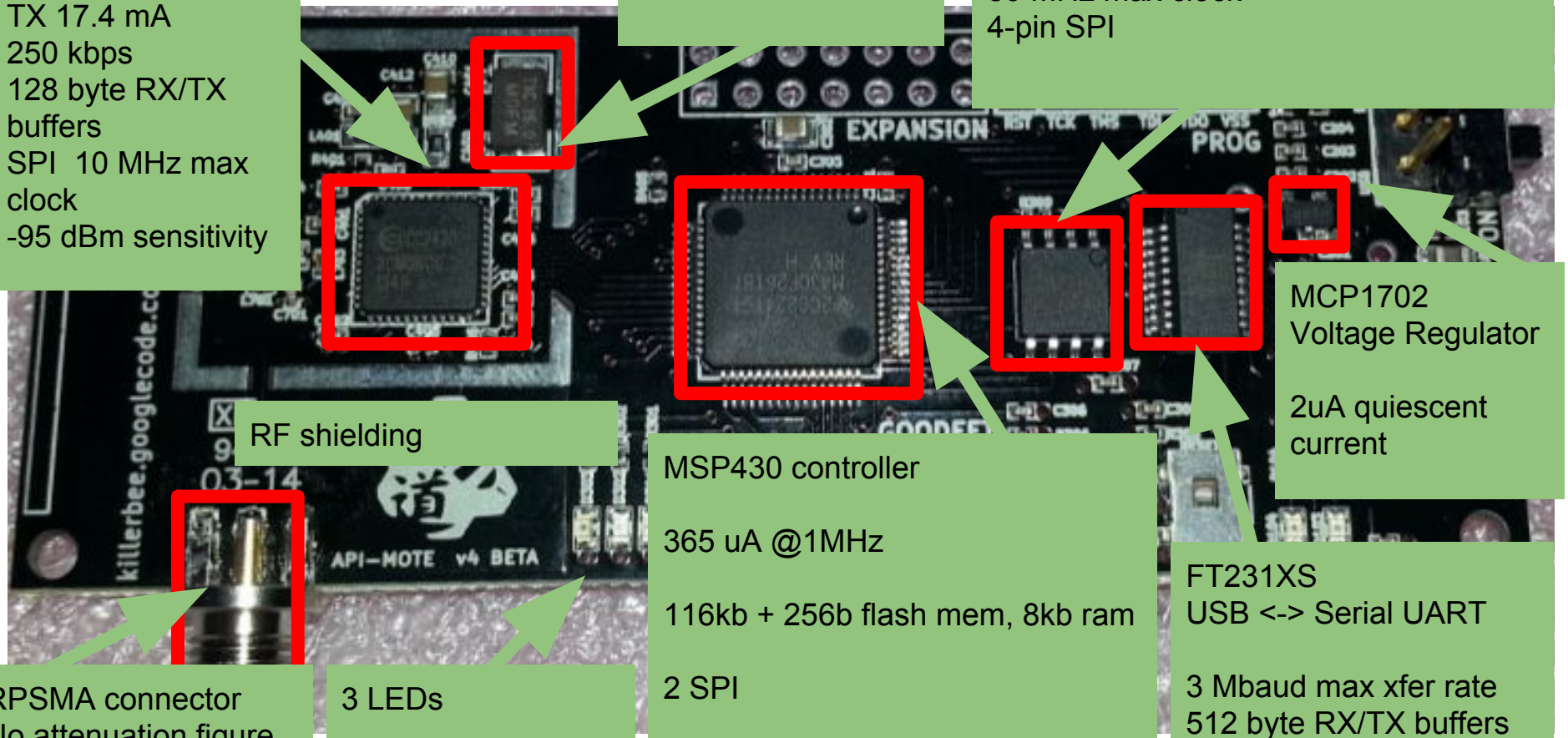
CC2420 radio
OBSOLETED

RX 18.8 mA
TX 17.4 mA
250 kbps
128 byte RX/TX buffers
SPI 10 MHz max clock
-95 dBm sensitivity

16 MHz Oscillator

SST25 flash memory OBSOLETED
On the board but not used by firmware!

10mA active, 5 uA standby
80 MHz max clock
4-pin SPI



RF shielding

MSP430 controller

365 uA @1MHz

116kb + 256b flash mem, 8kb ram

2 SPI

MCP1702
Voltage Regulator

2uA quiescent current

FT231XS
USB <-> Serial UART

3 Mbaud max xfer rate
512 byte RX/TX buffers
8.4 mA active
USB or self powered

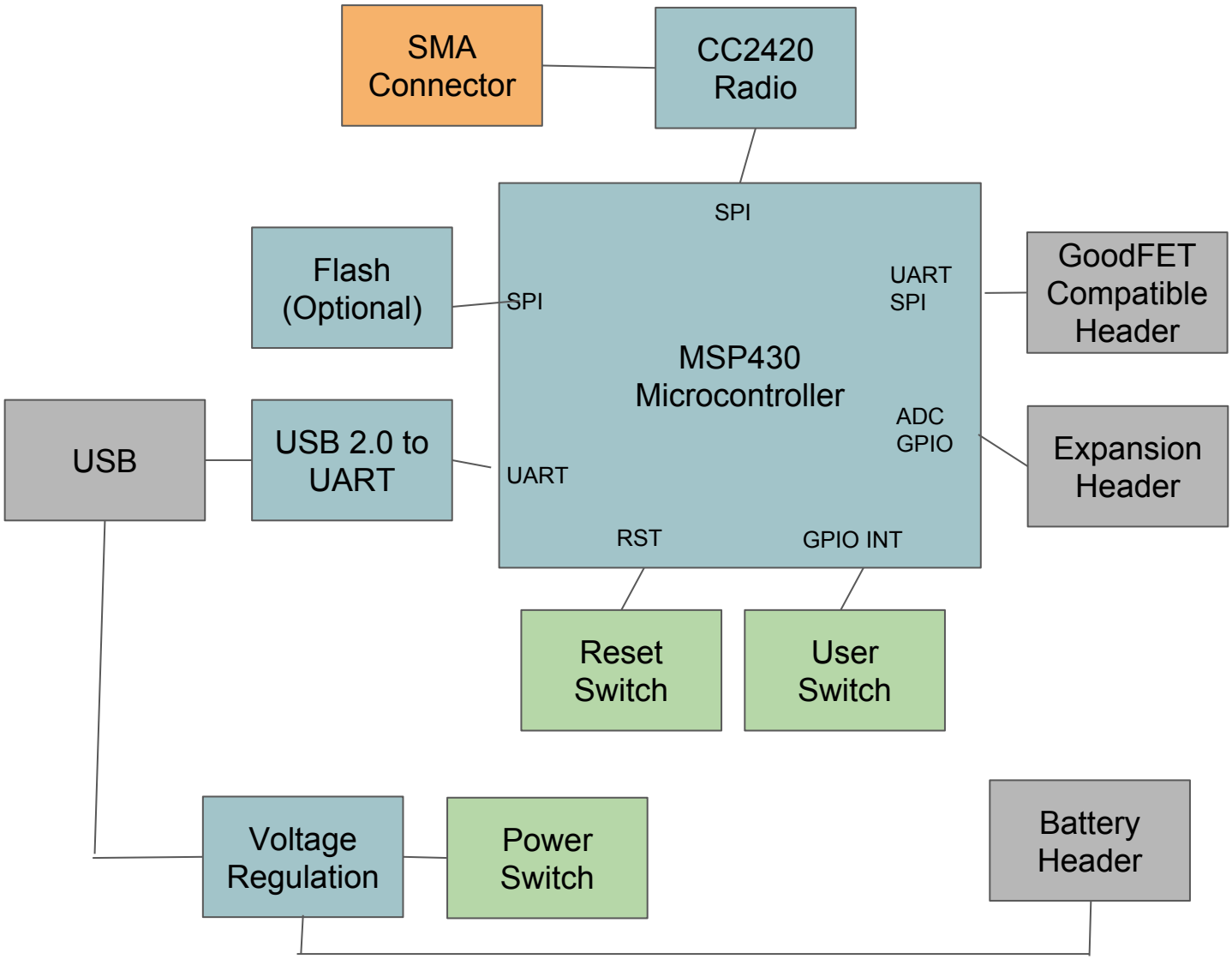
RPSMA connector
No attenuation figure on datasheet,
0.3 db loss expected

3 LEDs

3*20mA = 60mA

60mA +365 uA + 8.4 mA +2uA + 10mA + 18.8mA = 97.56mA current

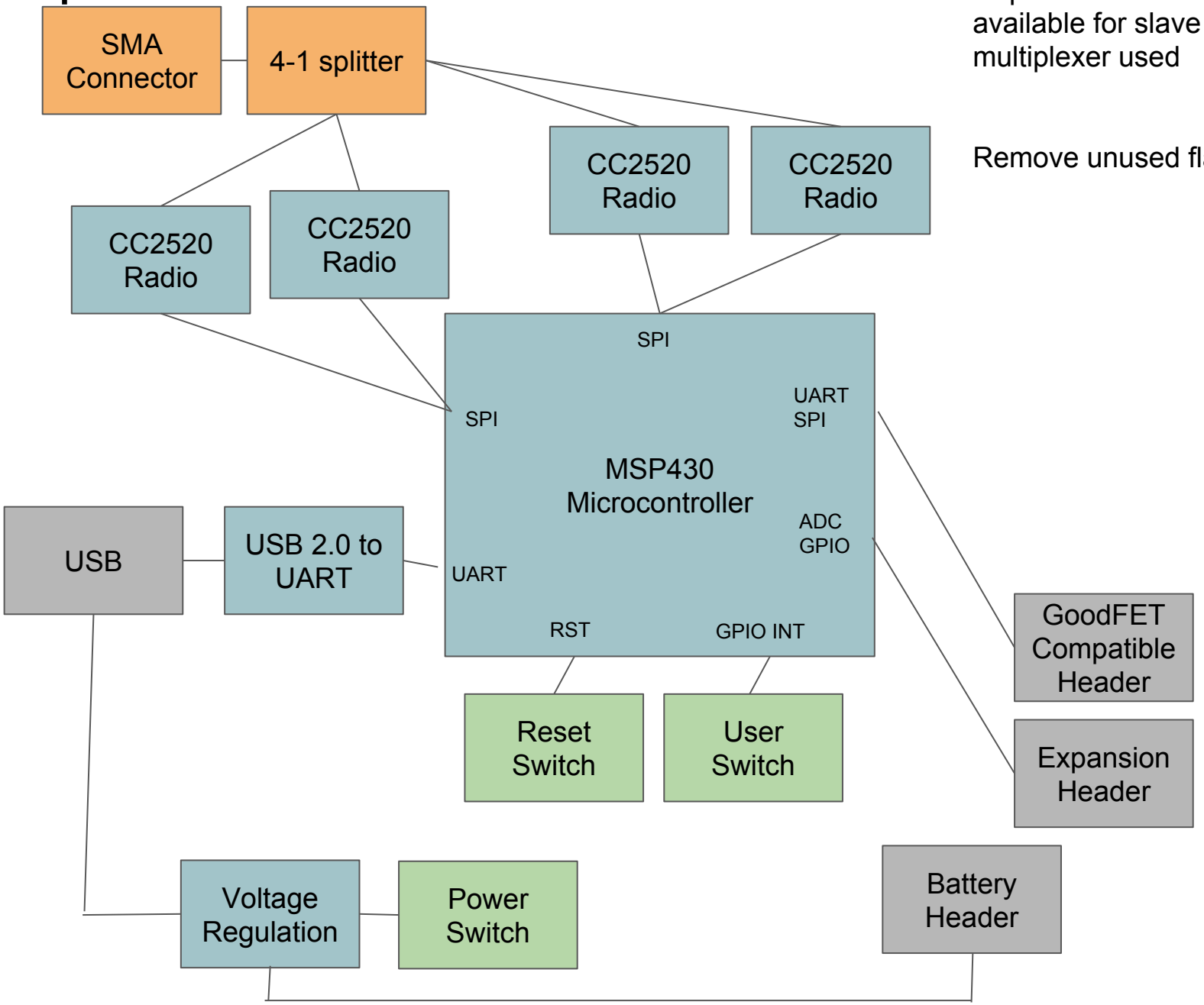
Api-Mote v4 design



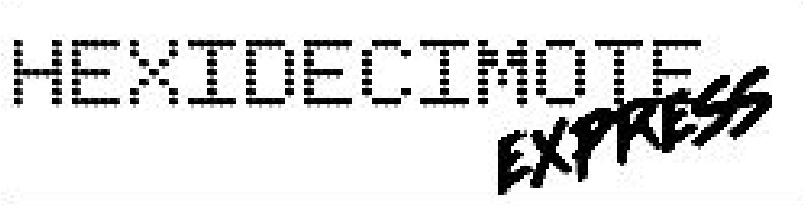
Proposed modification

Number of SPI slaves
Depends on GPIO pins
available for slave select, unless
multiplexer used

Remove unused flash chip



Express Design



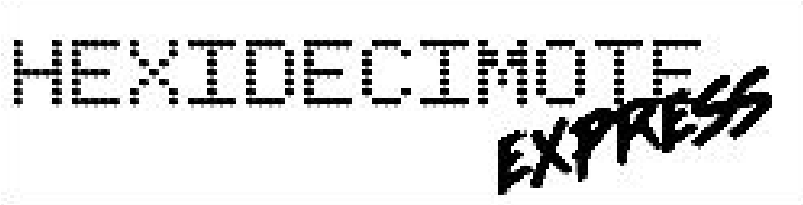
How can this be simplified?

Delegate non-radio functionality to devices off of the board and provide an interface to the radios alone

Remove microprocessor, USB, JTAG connector, and amplifier. This is the user's responsibility now!

More extensible/modular
Cheaper to produce
Simpler, mitigates risk of catastrophic design mistakes

Express Design



How can this be simplified?

Delegate non-radio functionality to devices off of the board and provide an interface to the radios alone

Remo
ampli

Michael Ossmann: Simple RF Circuit Design

https://www.youtube.com/watch?v=TnRn3Kn_aXg

More extensible/modular
Cheaper to produce
Simpler, mitigates risk of catastrophic design mistakes

RF View:

Surface Mount

Power Splitter/Combiner

4 Way-0° 50Ω 2100 to 2500 MHz

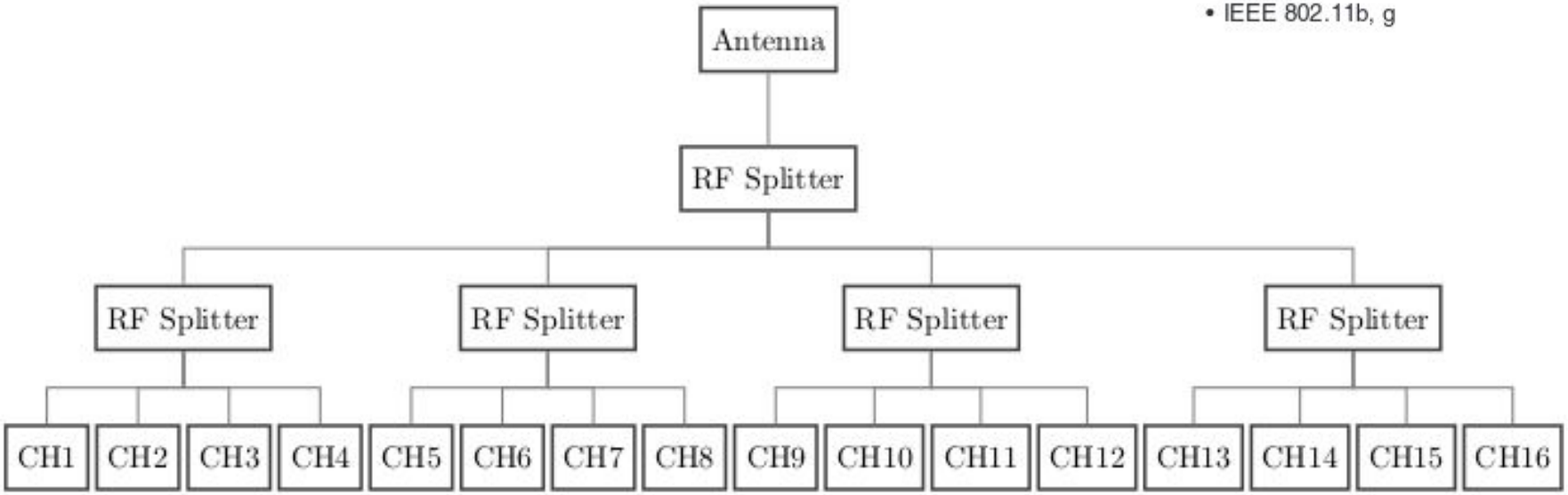
BP4U+

Features

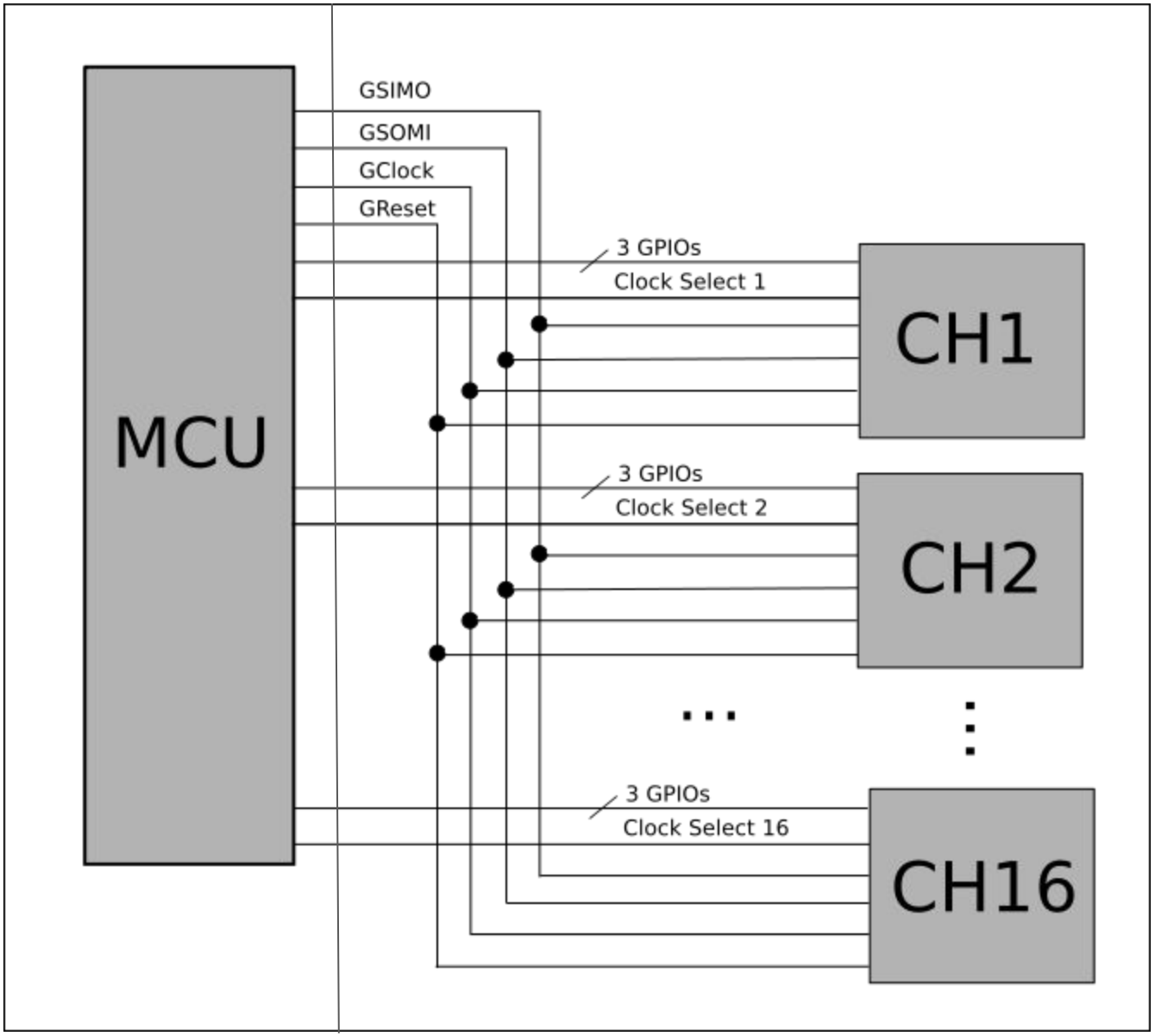
- low insertion loss, 0.7 dB typ
- excellent isolation, 23 dB typ.
- excellent VSWR, 1.15:1 typ.
- umplitude unbalance, 0.6 dB typ.
- aqueous washable
- excellent power handling, 1.5W

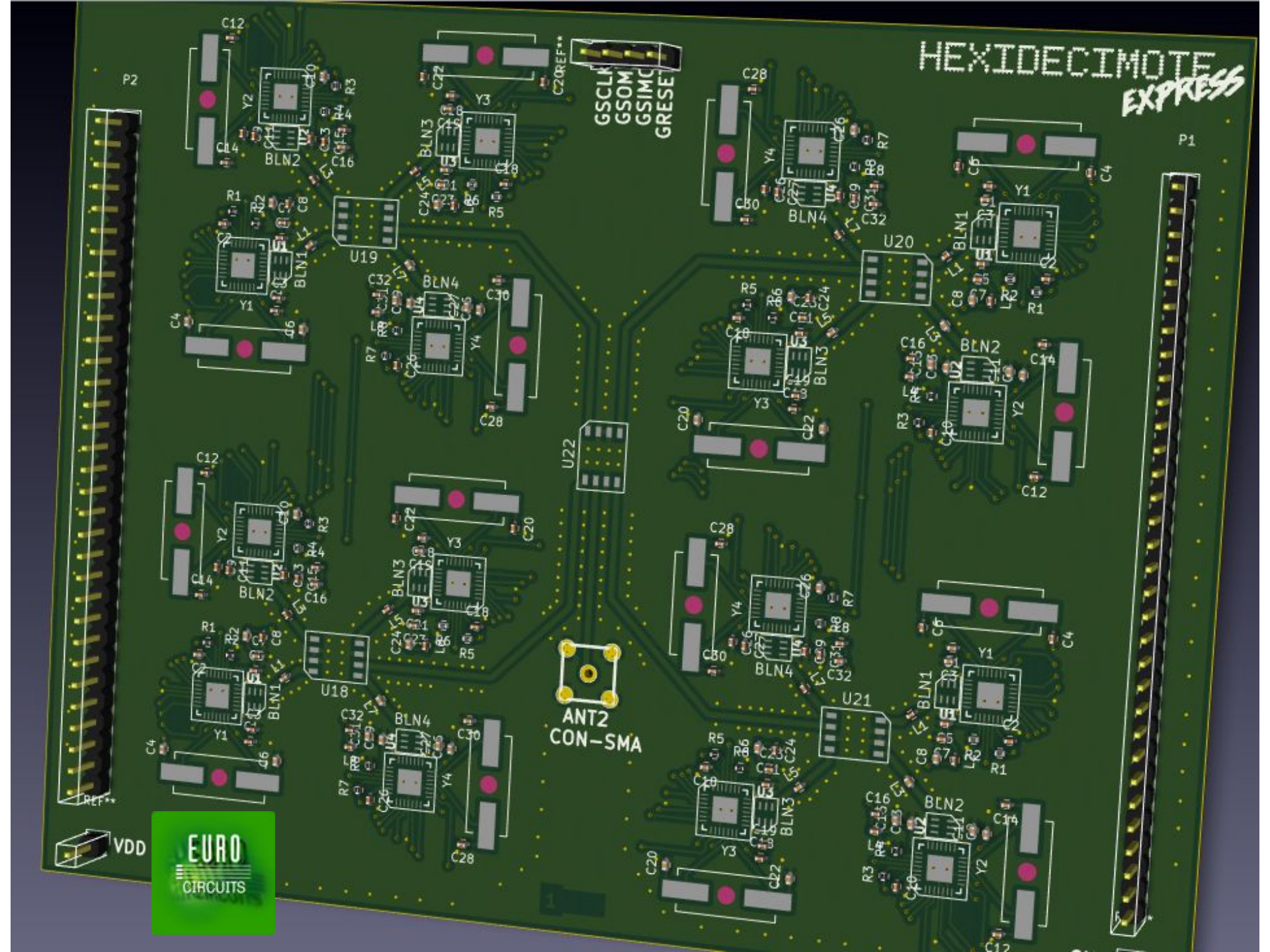
Applications

- bluetooth
- IEEE 802.11b, g

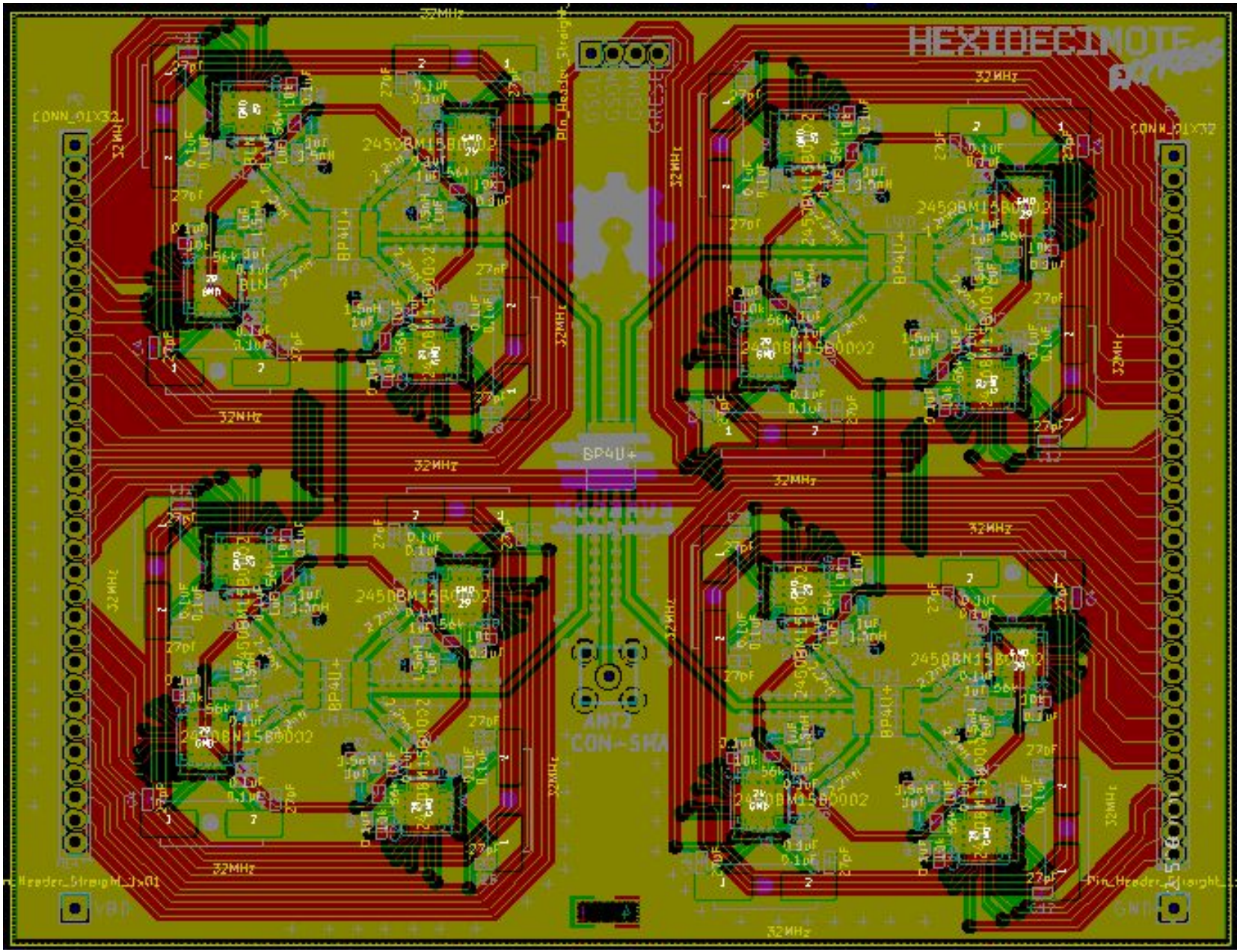


Digital View:

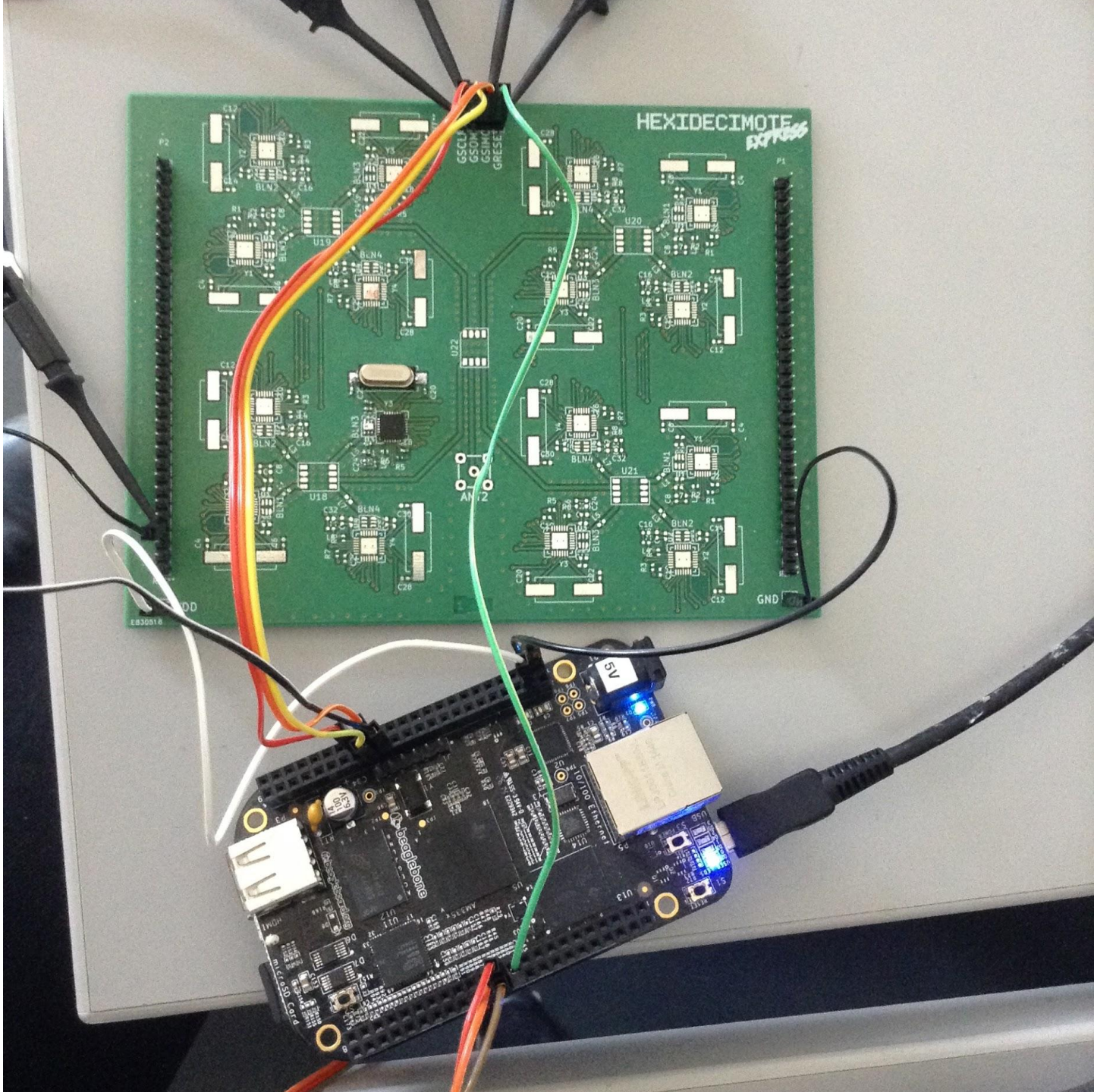



HEXIDECIMOTE
EXPRESS
P1
P2
U19
U20
U21
U22
U18
ANT2
CON-SMA
BLN1
BLN2
BLN3
BLN4
VDD
EURO
CIRCUITS

Device Design R3



HDME +
BBB



Only 6.25% completion

1/16 radios soldered ✓

SPI (CC2520 driver in linux kernel) ✓

wpan-tools compatibility ✓

Packet reception **X**

Multi-radio driver **X**

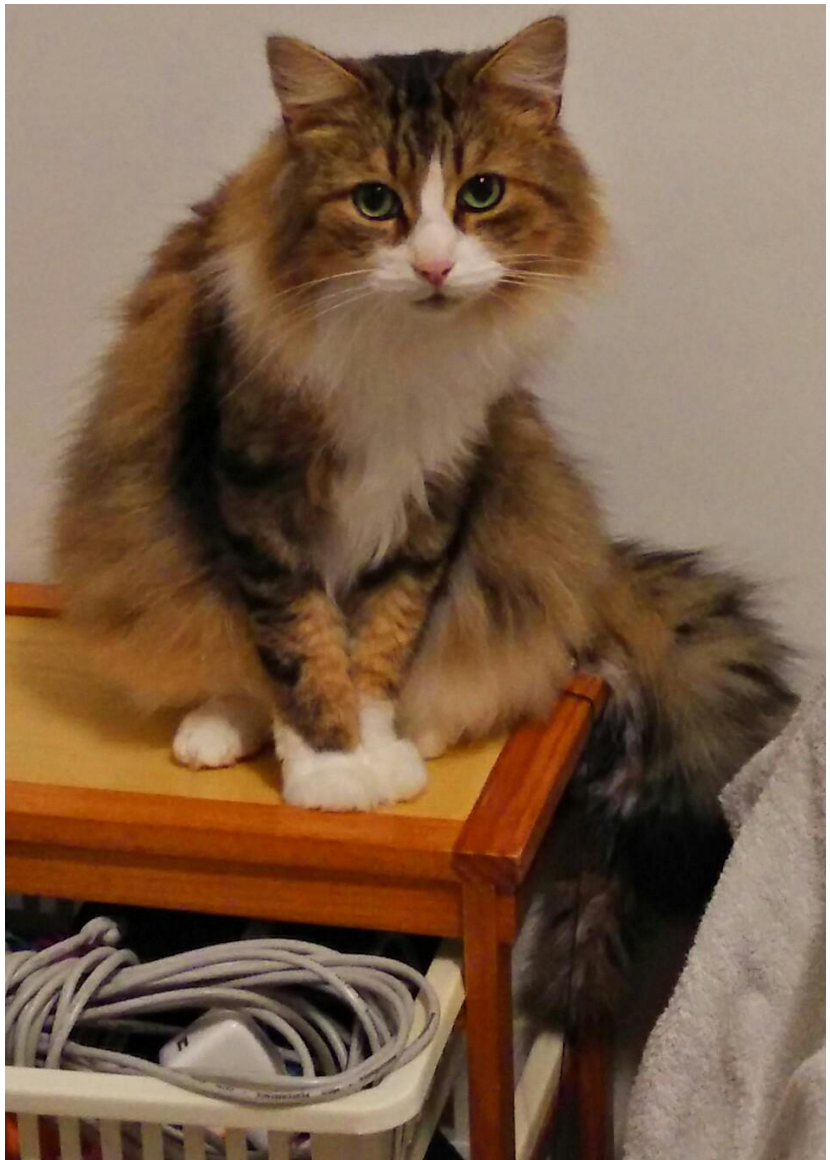
Performance testing **X**

BBB “cape” form factor **X**

….please contribute!

github.com/tomx4096

Thank you, village people



IEEE 802.15.4 PHY Layers in IEEE 802.15.4-2011 and current amendments			
Standard	PHY (Modulation)	Frequency Band (MHz)	Vendor
802.15.4-2011	O-QPSK (DSSS) BPSK (DSSS) ASK (PSSS) CSS (DQPSK) UWB (BPM/BPSK) MPSK GFSK	780, 868, 915, 2450 868, 915, 950 868, 915 2450 <1000, 3000-10000 780 950	TI/Atmel . . Nanotron Decawave . .
802.15.4f-2012 Active RFID	MSK (CPFSK) LRP UWB (OOK/PPM)	433, 2450 69000	Zebra Dart Tag [1]
802.15.4g-2012 Smart Meter Utility Networks (SUNs)	MR-FSK MR-OFDM MR-O-QPSK (DSSS/MDSSS)	169, 460 ... 470-2450 470	Atmel [2] / Semtech/[3] Silabs [4]
802.15.4j-2013 Medical Body Area Networks (MBANs)	O-QPSK (DSSS)	2380	[5]
802.15.4k-2013 Low Energy Critical Infrastructure Monitoring (LECIM)	LECIM DSSS LECIM FSK	470-2450 169-928	OnRamp Wireless/ Ingenu [6]
802.15.4m-2014 TV White Space PHYs	TVWS-FSK TVWS-OFDM TVWS-NB-OFDM	54-862 54-862 54-862	[7] [8]
802.15.4p-2014 Rail Communication and Control (RCC)	RCC LMR (GMSK, C4FM, QPSK,DQPSK,DPSK) RCC DSSS BPSK	160-960 902-5850	LiLee Systems [9] [10]