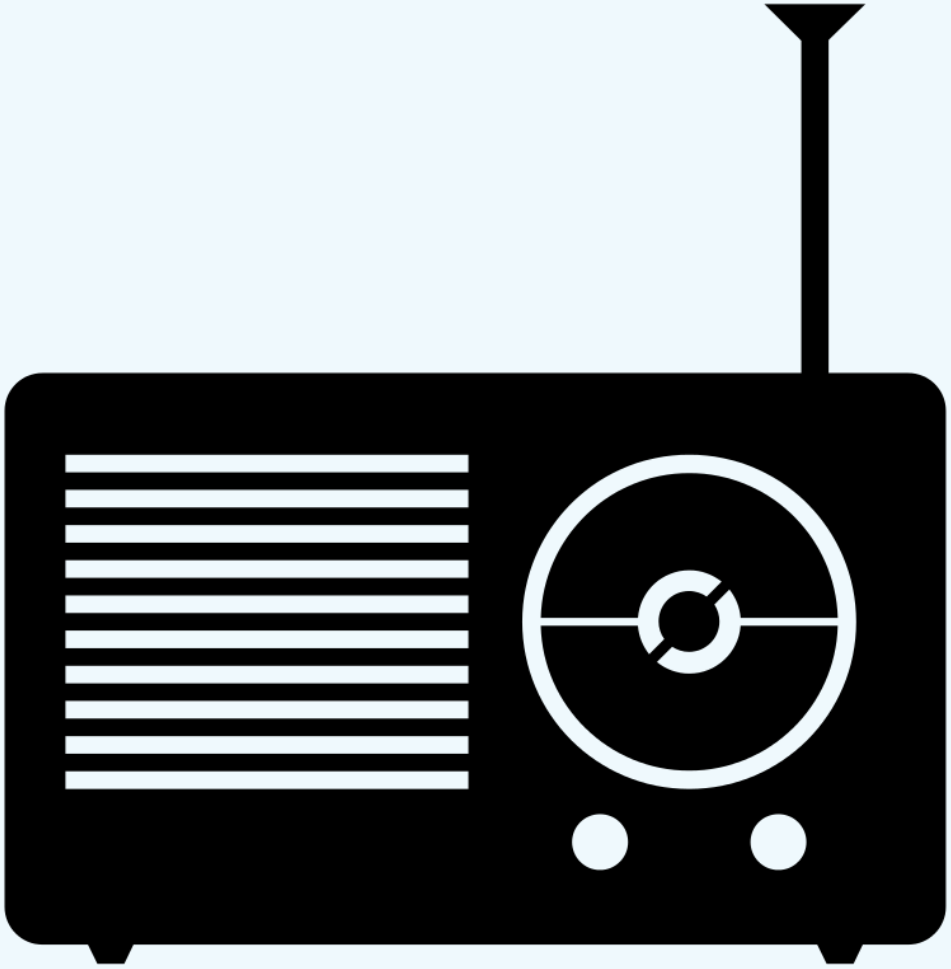
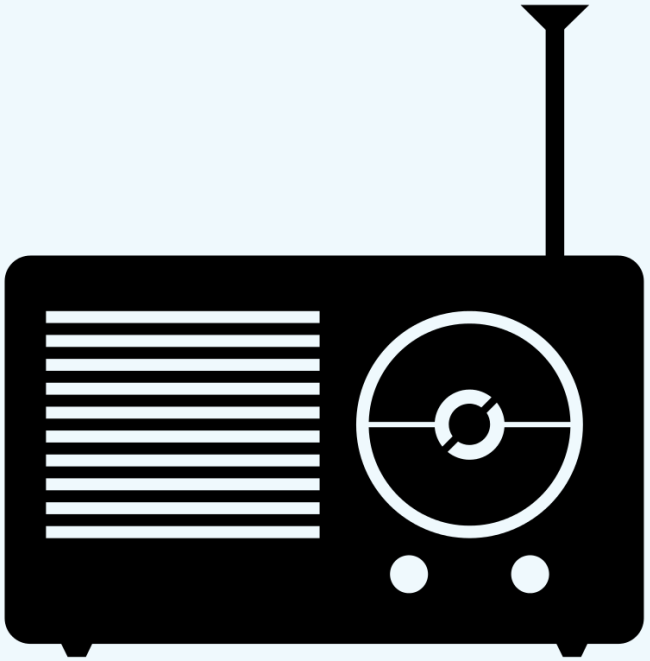
Hacking Wireless Networks of the Future: Security in Cognitive Radio Networks

Hunter Scott / August 3, 2013



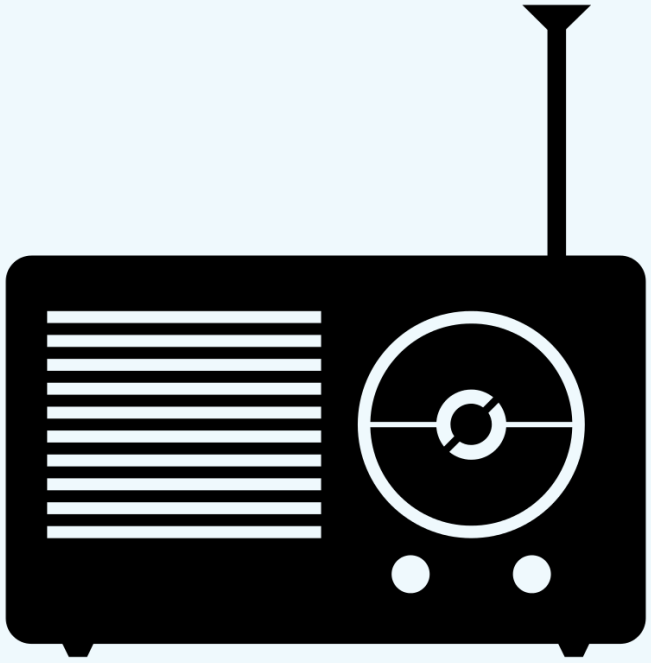
Radio



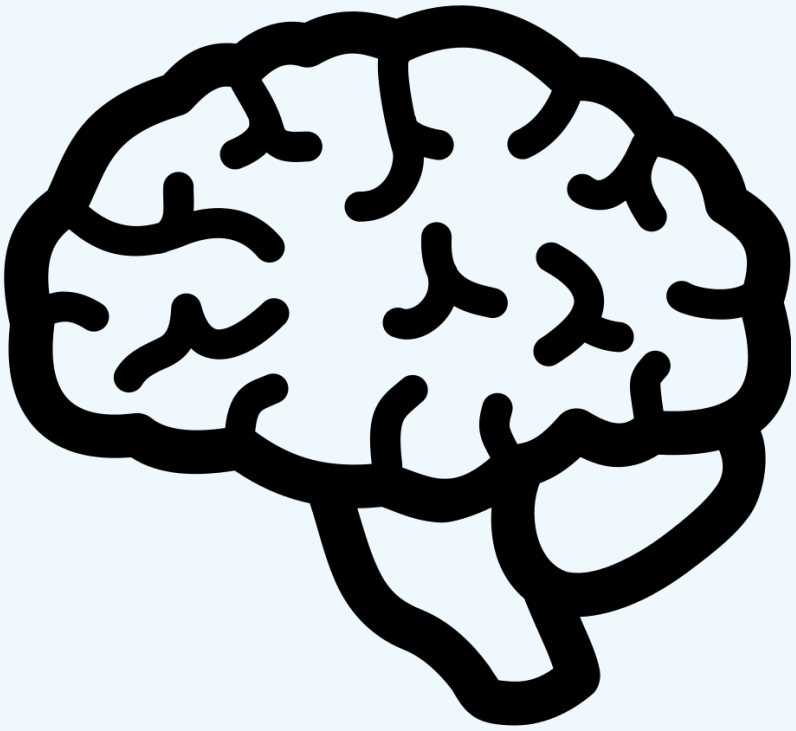
+

```
// 4 lines of ethernet hdr + 2 lines (word0 + timestamp)
// DSP Tx reads word0 (flags) + timestamp followed by samples

#define DSP_TX_FIRST_LINE         4
#define DSP_TX_SAMPLES_PER_FRAME    250 // not used except w/ debugging
#define DSP_TX_EXTRA_LINES        2 // reads word0 + timestamp

// Receive from ethernet
buf_cmd_args_t dsp_tx_recv_args = {
  PORT_ETH,
  0,
  BP_LAST_LINE
};

// send to DSP Tx
buf_cmd_args_t dsp_tx_send_args = {
  PORT_DSP,
  DSP_TX_FIRST_LINE,    // starts just past ethernet header
  0         // filled in from last_line register
};

dbsm_t dsp_tx_sm;   // the state machine

/*
 * send constant buffer to DSP TX
 */
static inline void
SEND_CONST_TO_DSP_TX(void)
{
  bp_send_from_buf(DSP_TX_BUF_0, PORT_DSP, 1,
           DSP_TX_FIRST_LINE,
           DSP_TX_FIRST_LINE + DSP_TX_EXTRA_LINES + DSP_TX_SAMPLES_PER_FRAME - 1);
}
```

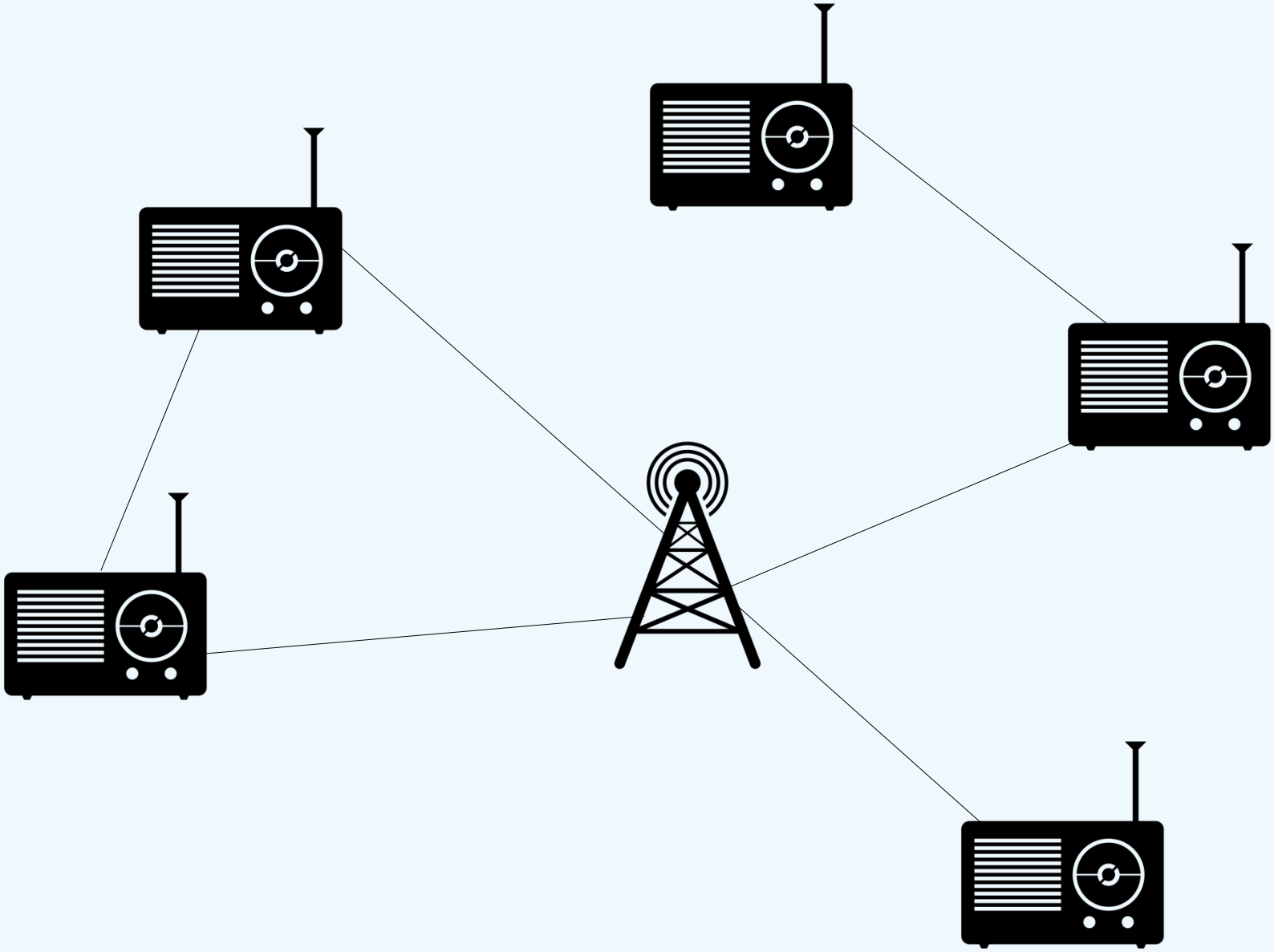
Software Defined Radio



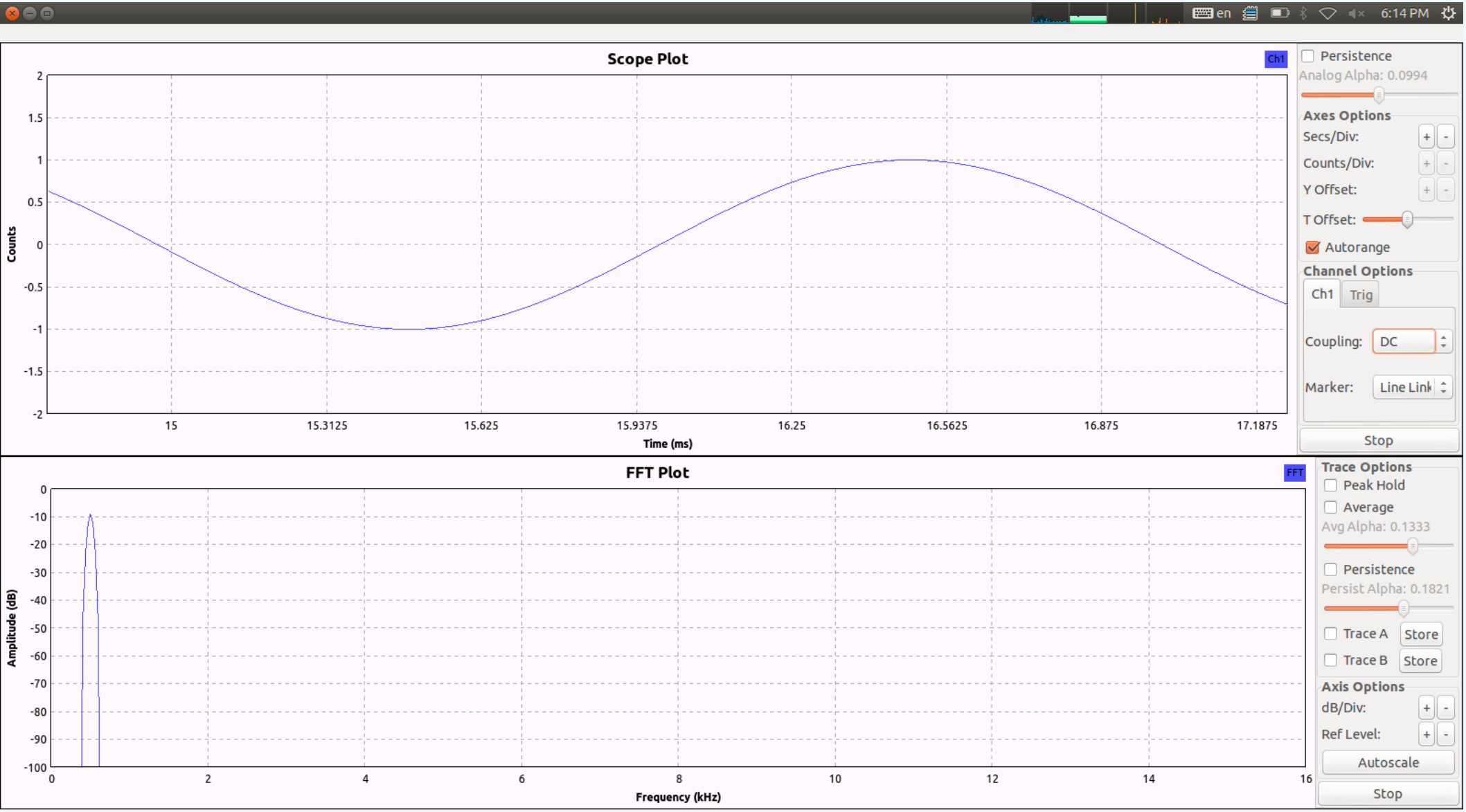
+

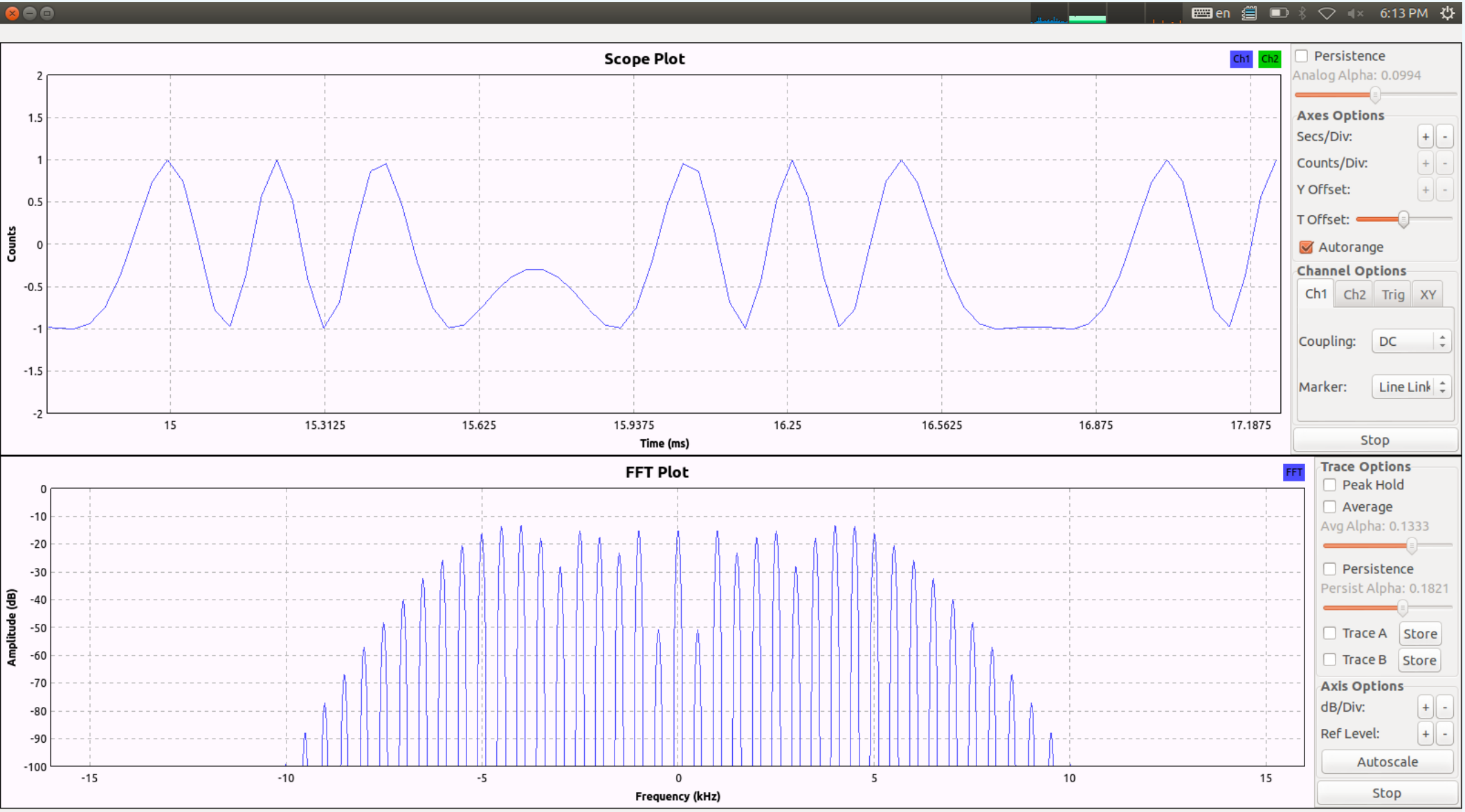


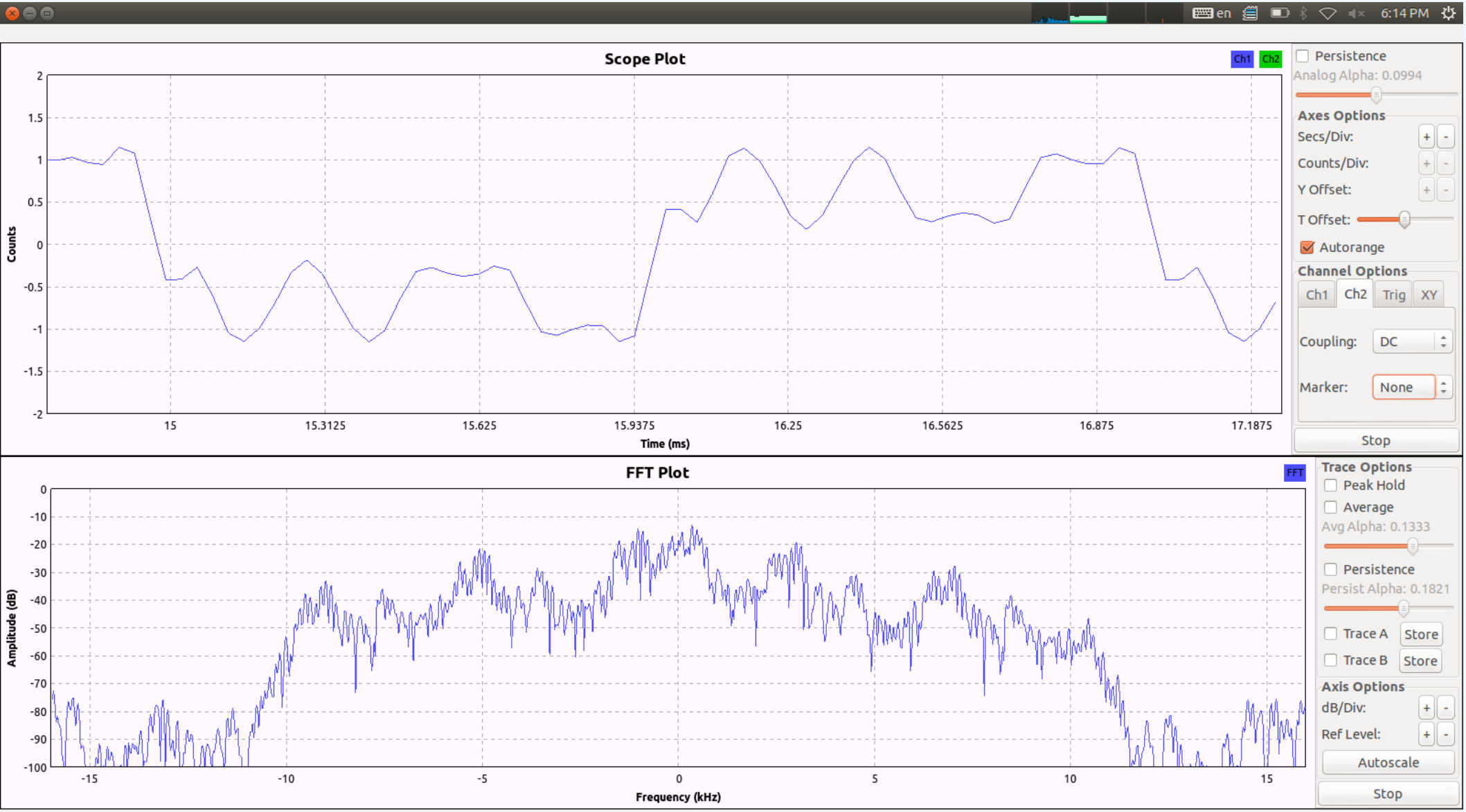
Cognitive Radio

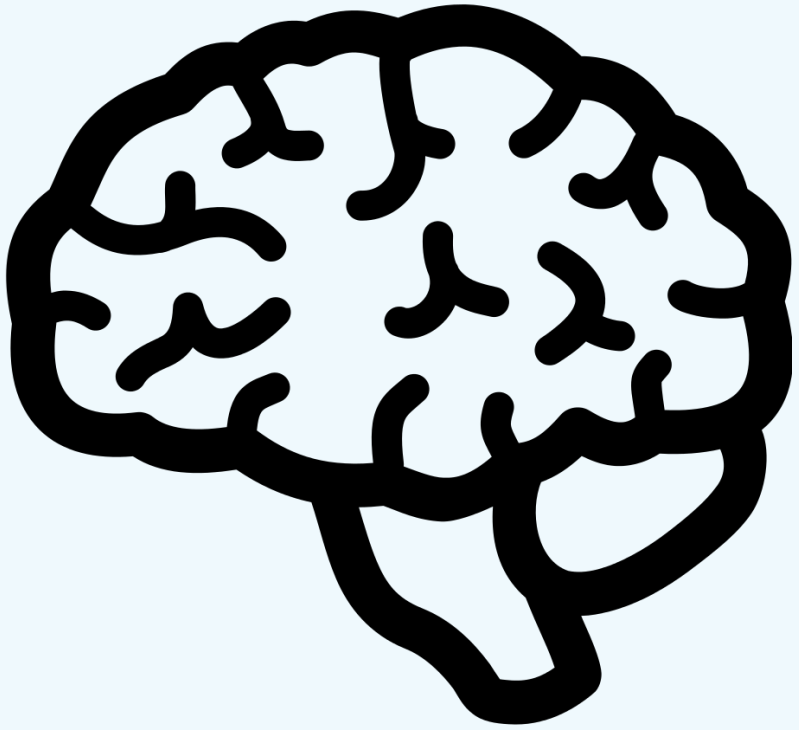


Cognitive Radio Network


Scope Plot
Ch1
Counts
Time (ms)
2
1.5
1
0.5
0
-0.5
-1
-1.5
-2
15
15.3125
15.625
15.9375
16.25
16.5625
16.875
17.1875
Persistence
Analog Alpha: 0.0994
Axes Options
Secs/Div:
Counts/Div:
Y Offset:
T Offset:
Autorange
Channel Options
Ch1
Trig
Coupling:
DC
Marker:
Line Link
Stop
FFT Plot
FFT
Amplitude (dB)
Frequency (kHz)
0
-10
-20
-30
-40
-50
-60
-70
-80
-90
-100
0
2
4
6
8
10
12
14
16
Trace Options
Peak Hold
Average
Avg Alpha: 0.1333
Persistence
Persist Alpha: 0.1821
Trace A
Store
Trace B
Store
Axis Options
dB/Div:
Ref Level:
Autoscale
Stop


Scope Plot
Ch1
Ch2
Counts
Time (ms)
2
1.5
1
0.5
0
-0.5
-1
-1.5
-2
15
15.3125
15.625
15.9375
16.25
16.5625
16.875
17.1875
Persistence
Analog Alpha: 0.0994
Axes Options
Secs/Div:
Counts/Div:
Y Offset:
T Offset:
Autorange
Channel Options
Ch1
Ch2
Trig
XY
Coupling:
DC
Marker:
Line Link
Stop
FFT Plot
FFT
Amplitude (dB)
Frequency (kHz)
0
-10
-20
-30
-40
-50
-60
-70
-80
-90
-100
-15
-10
-5
0
5
10
15
Trace Options
Peak Hold
Average
Avg Alpha: 0.1333
Persistence
Persist Alpha: 0.1821
Trace A
Store
Trace B
Store
Axis Options
dB/Div:
Ref Level:
Autoscale
Stop


Scope Plot
Ch1
Ch2
Counts
Time (ms)
2
1.5
1
0.5
0
-0.5
-1
-1.5
-2
15
15.3125
15.625
15.9375
16.25
16.5625
16.875
17.1875
Persistence
Analog Alpha: 0.0994
Axes Options
Secs/Div:
Counts/Div:
Y Offset:
T Offset:
Autorange
Channel Options
Ch1
Ch2
Trig
XY
Coupling:
DC
Marker:
None
Stop
FFT Plot
FFT
Amplitude (dB)
Frequency (kHz)
0
-10
-20
-30
-40
-50
-60
-70
-80
-90
-100
-15
-10
-5
0
5
10
15
Trace Options
Peak Hold
Average
Avg Alpha: 0.1333
Persistence
Persist Alpha: 0.1821
Trace A
Store
Trace B
Store
Axis Options
dB/Div:
Ref Level:
Autoscale
Stop



Cognitive Engine

Center Frequency

Bandwidth

Transmit power

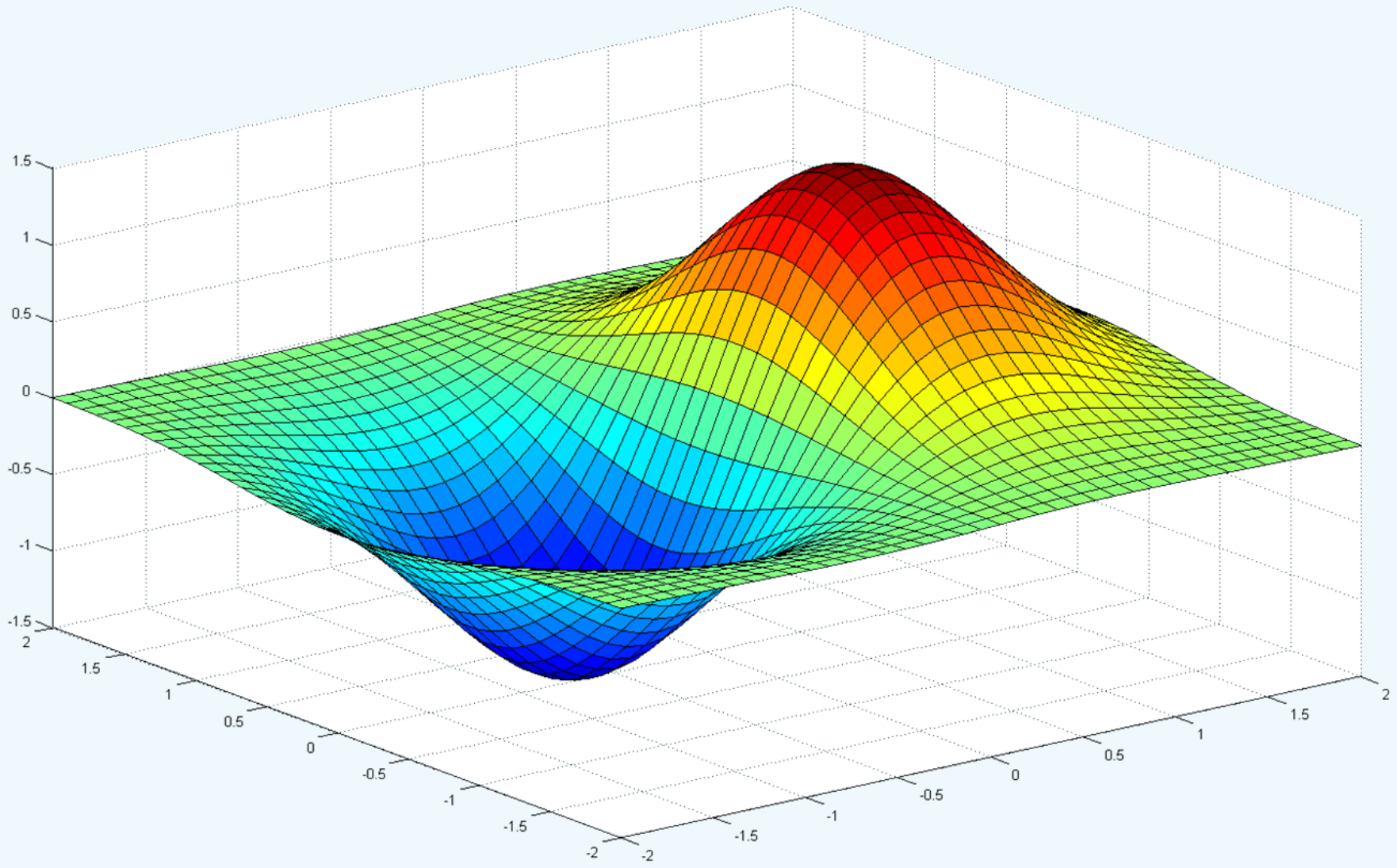
Type of modulation

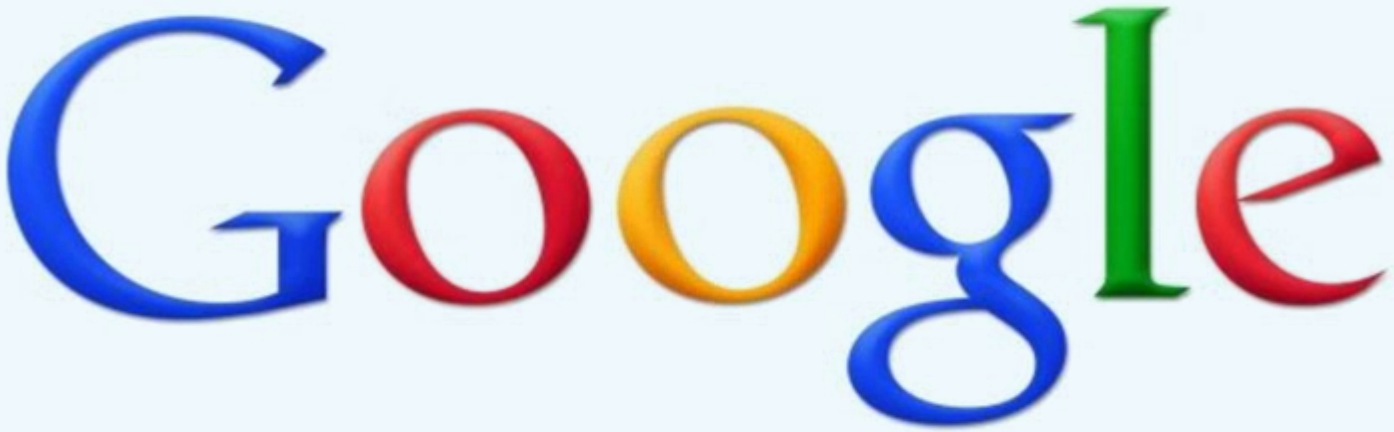
Coding rate

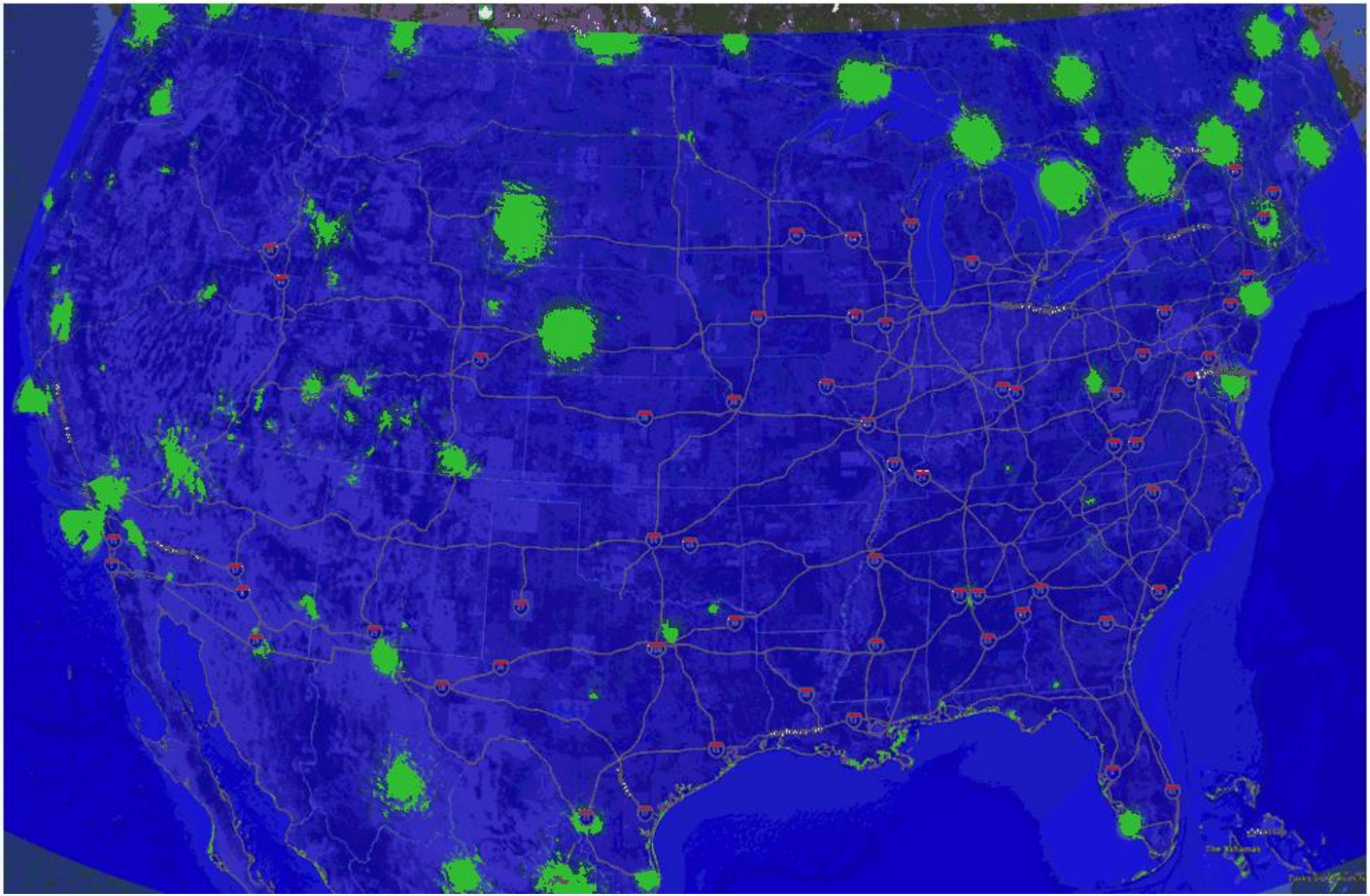
Channel access protocol

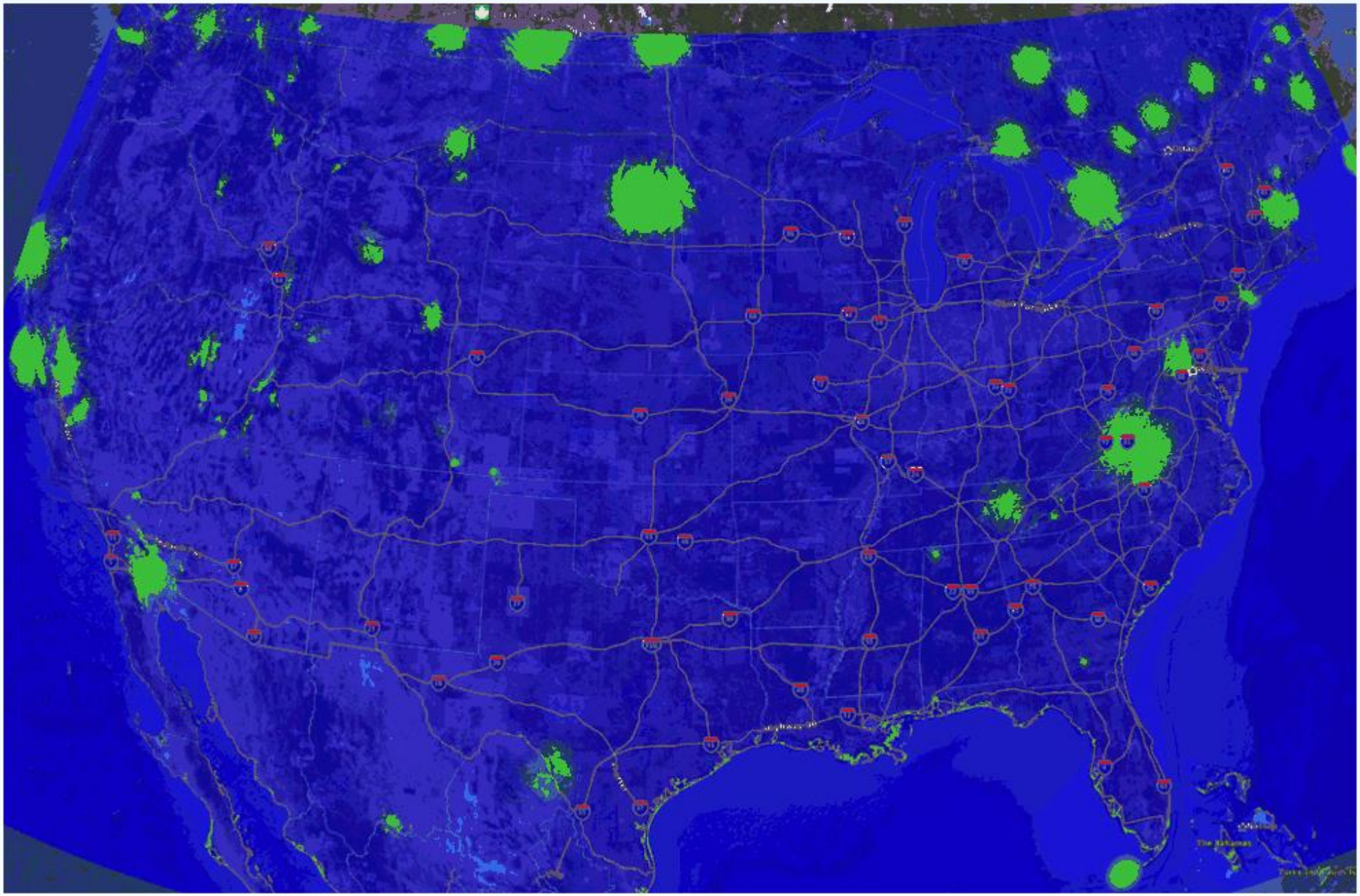
Encryption algorithm

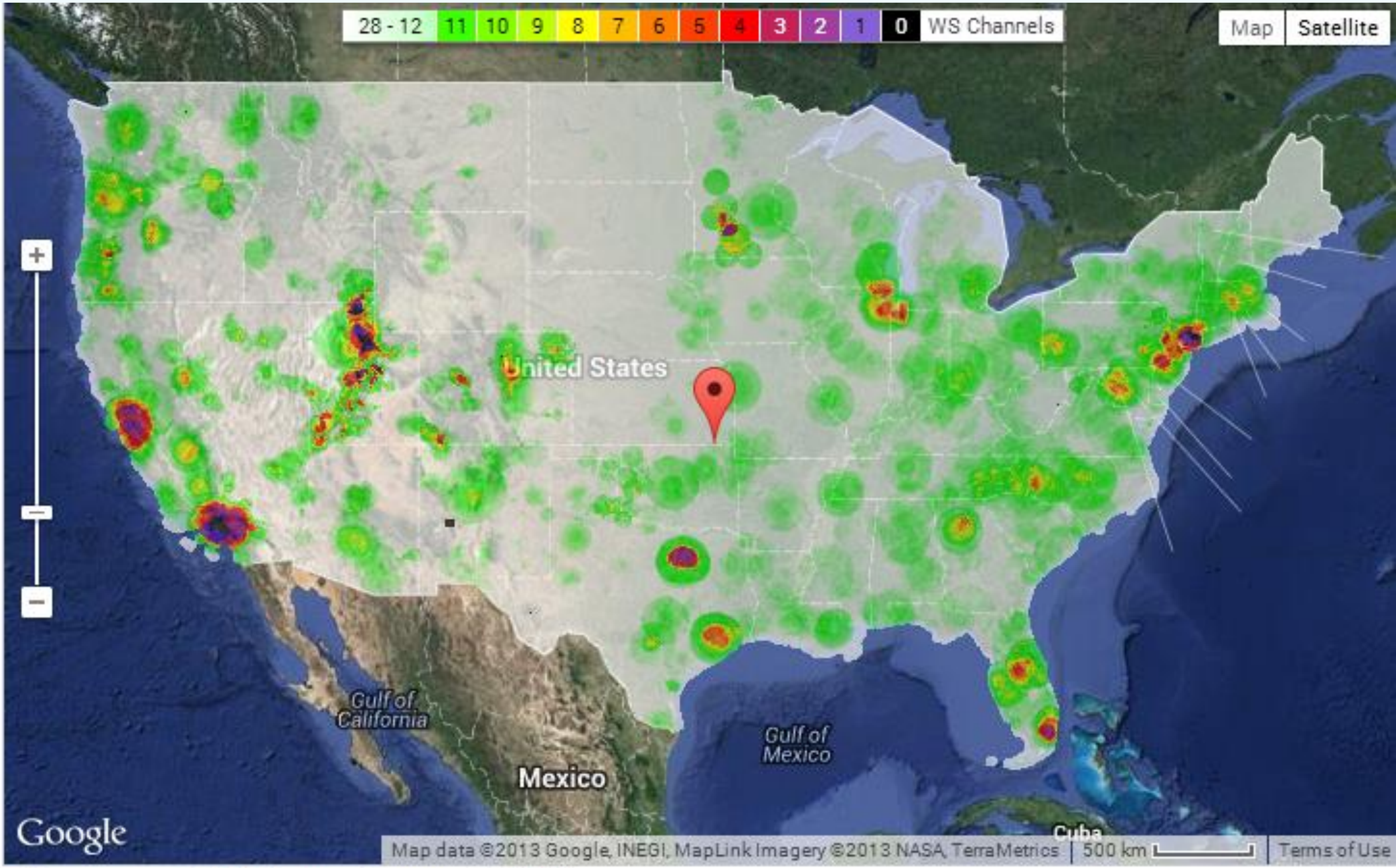
Frame size


1.5
1
0.5
0
-0.5
-1
-1.5
2
1.5
1
0.5
0
-0.5
-1
-1.5
-2
-2
-1.5
-1
-0.5
0
0.5
1
1.5
2


Google



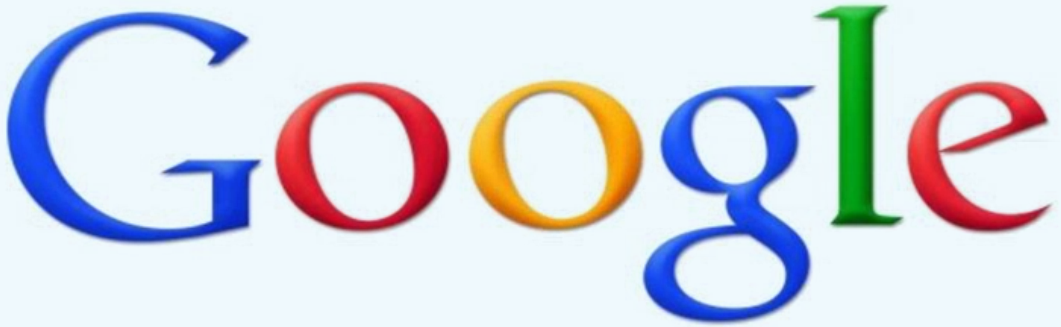




☑ **Spectrum availability** (as of January 29, 2013)


Microsoft


SPECTRUM
BRIDGE


Google


SIGFOX
One network A billion dreams


WEIGHTLESS™

ASSOCIATE MEMBERS

Full access to Weightless & Test specification

A way to “test the water” at low cost

Access to Weightless SIG marketing services

Clear link to the standard

Fee: GBP£650 p.a.

CORE MEMBERS

Full access to Weightless & Test Specification

Able to influence the direction and details of the specification

Able to work in sub-groups including taking key positions

Able to participate in Plenary Conferences

Advance sight of working documents and proposed changes to the specification

Clear link to the standard at a high level

Fee: GBP£3,250 p.a.
for companies with an annual turnover of less than GBP£1m p.a.

GBP£6,500 p.a.
for companies with an annual turnover of greater than GBP£1m p.a..

ASSOCIATE MEMBERS

Full access to Weightless & Test specification

A way to “test the water” at low cost

Access to Weightless SIG marketing services

Clear link to the standard

Fee: GBP£650 p.a.

CORE MEMBERS

Full access to Weightless & Test Specification

Able to influence the direction and details of the specification

Able to work in sub-groups including taking key positions

Able to participate in Plenary Conferences

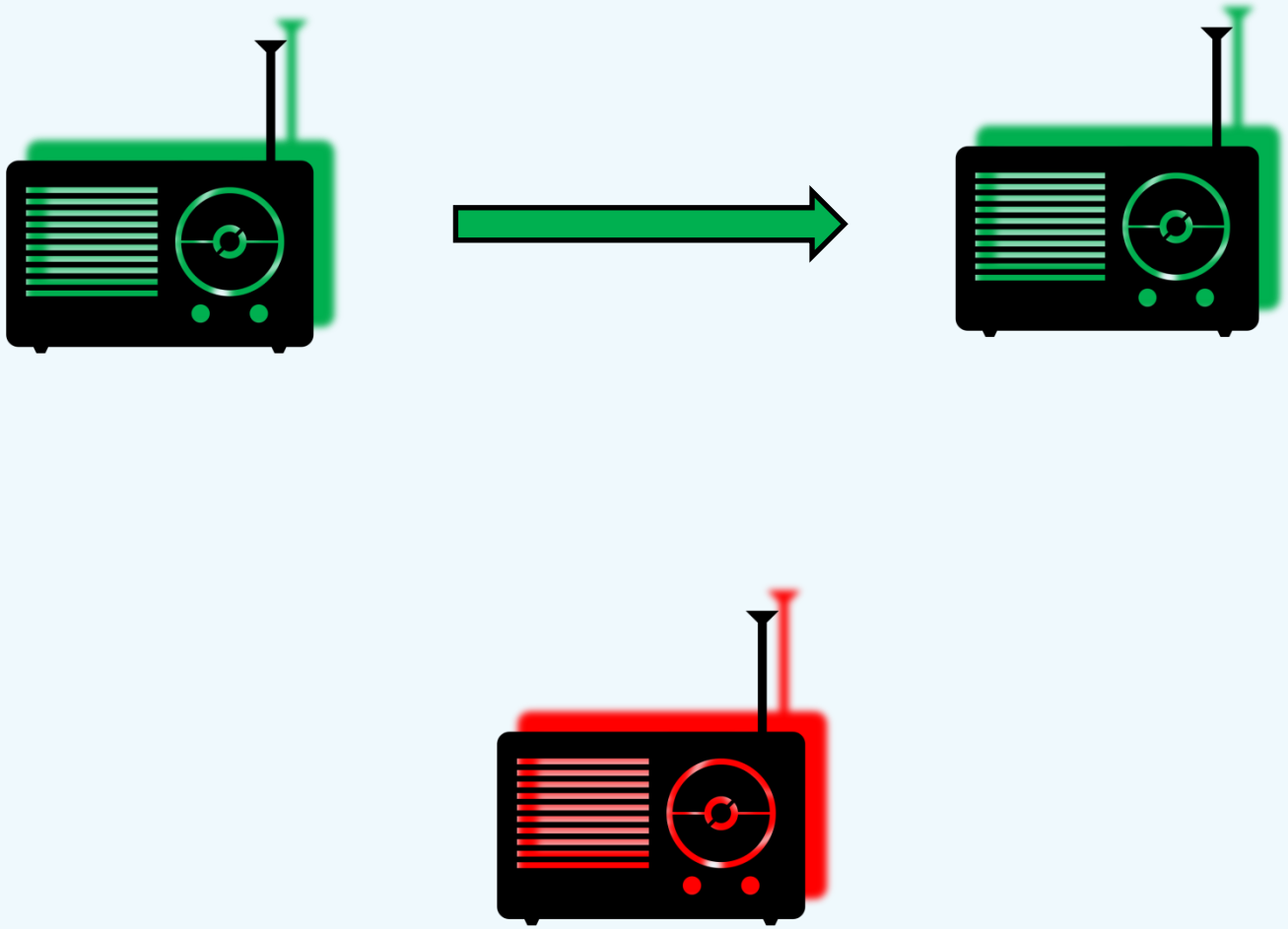
Advance sight of working documents and proposed changes to the specification

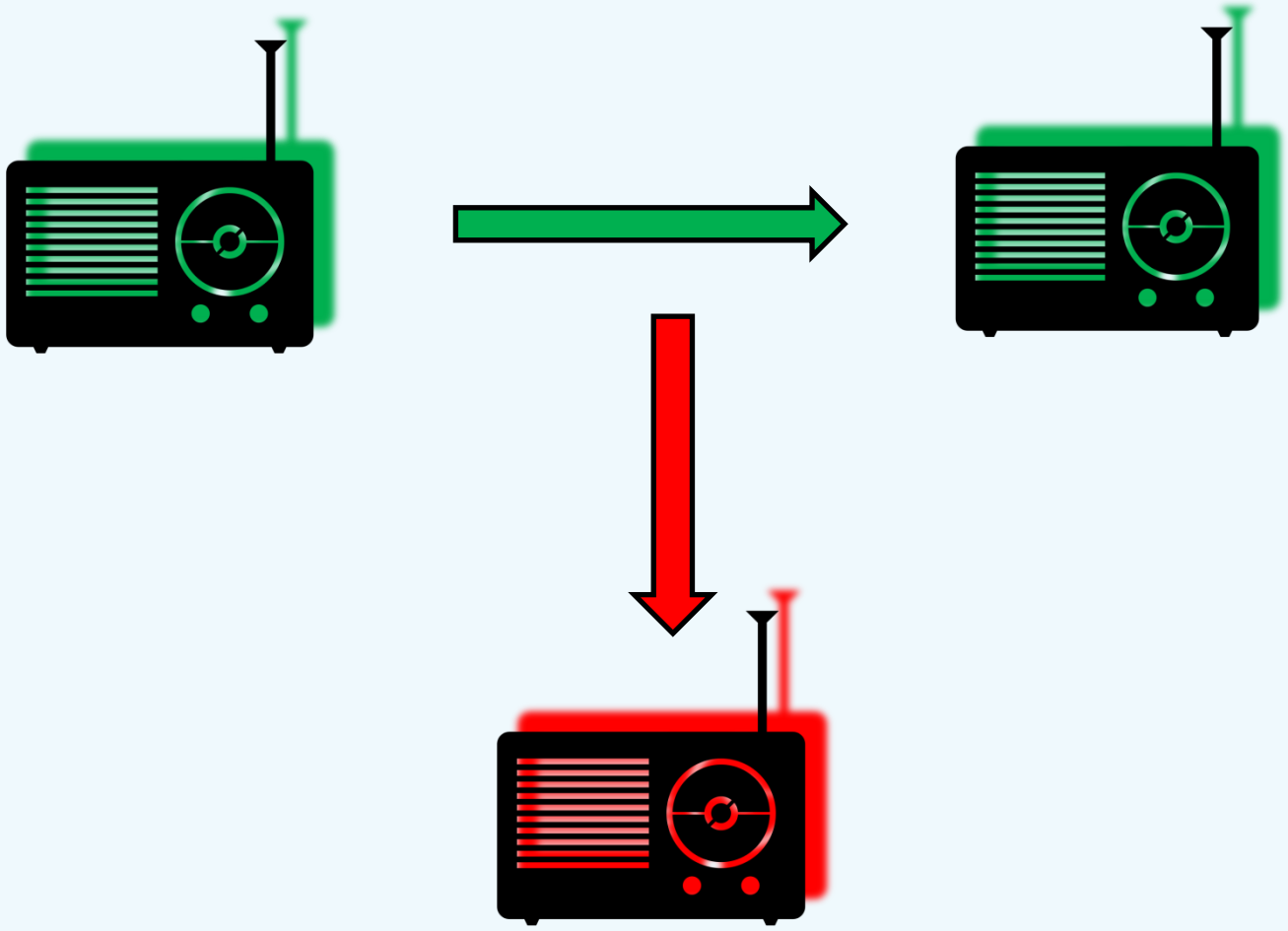
Clear link to the standard at a high level

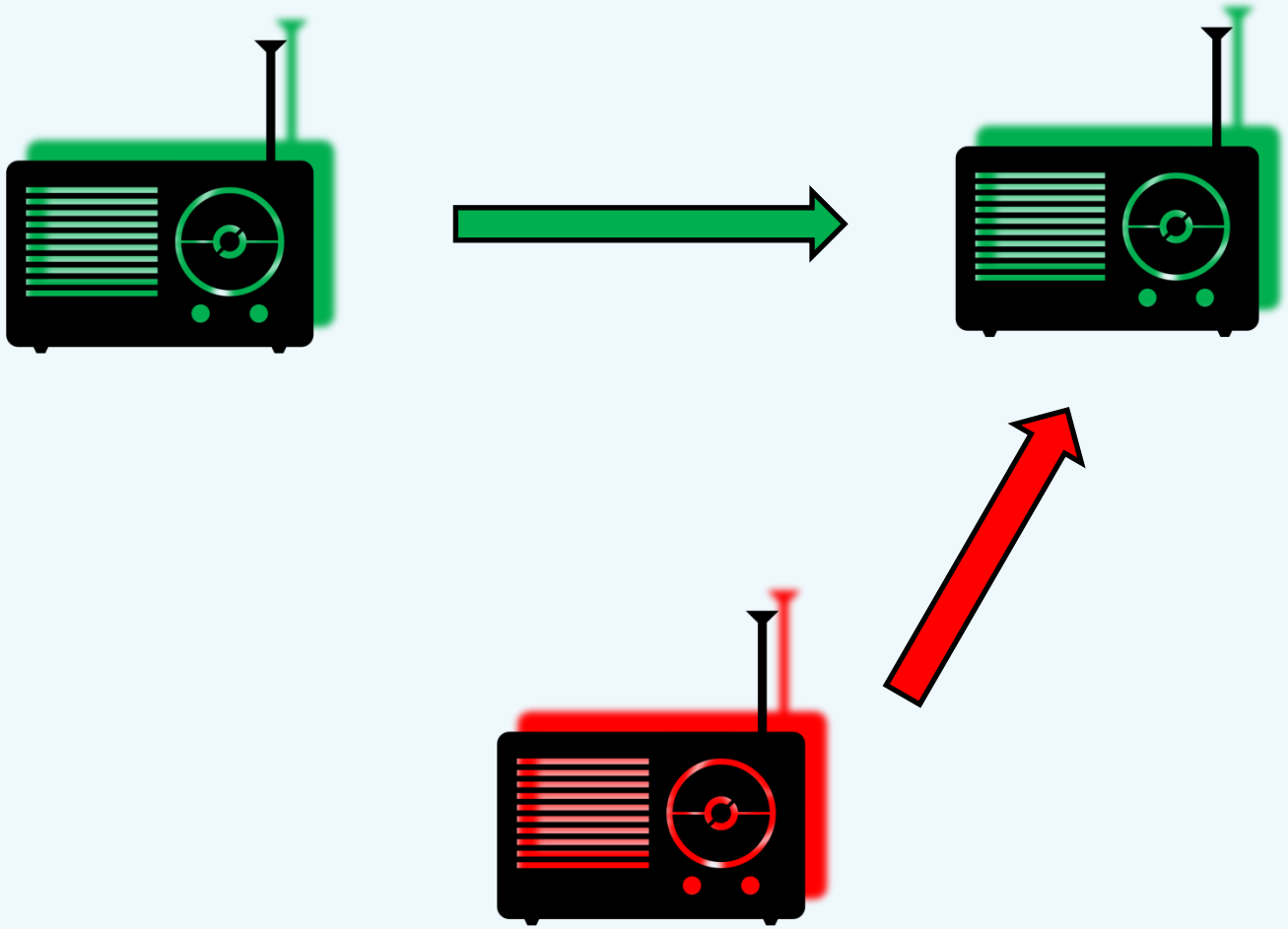
Fee: GBP£3,250 p.a.
for companies with an annual turnover of less than GBP£1m p.a.

GBP£6,500 p.a.
for companies with an annual turnover of greater than GBP£1m p.a..

Attacks specific to cognitive radio networks

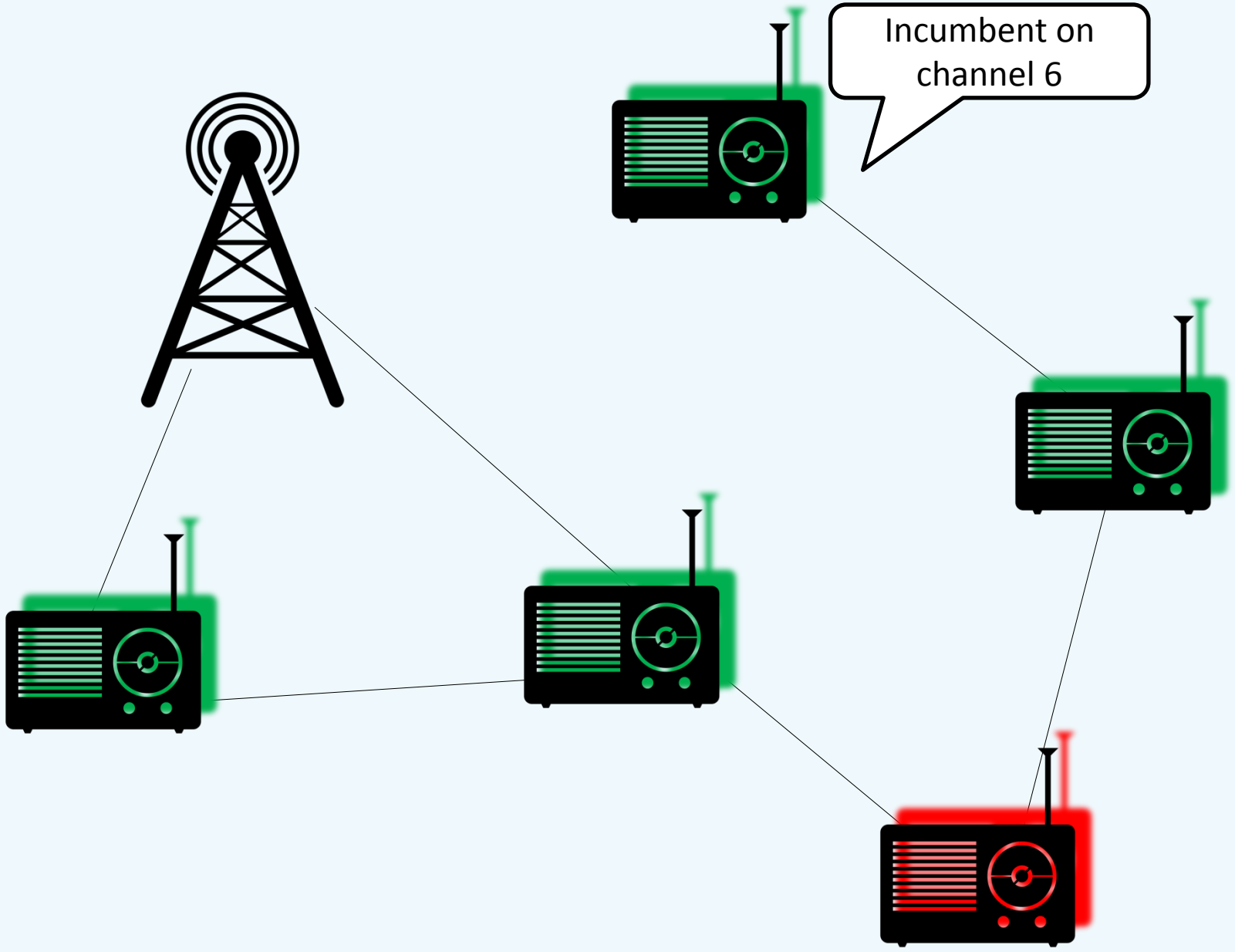




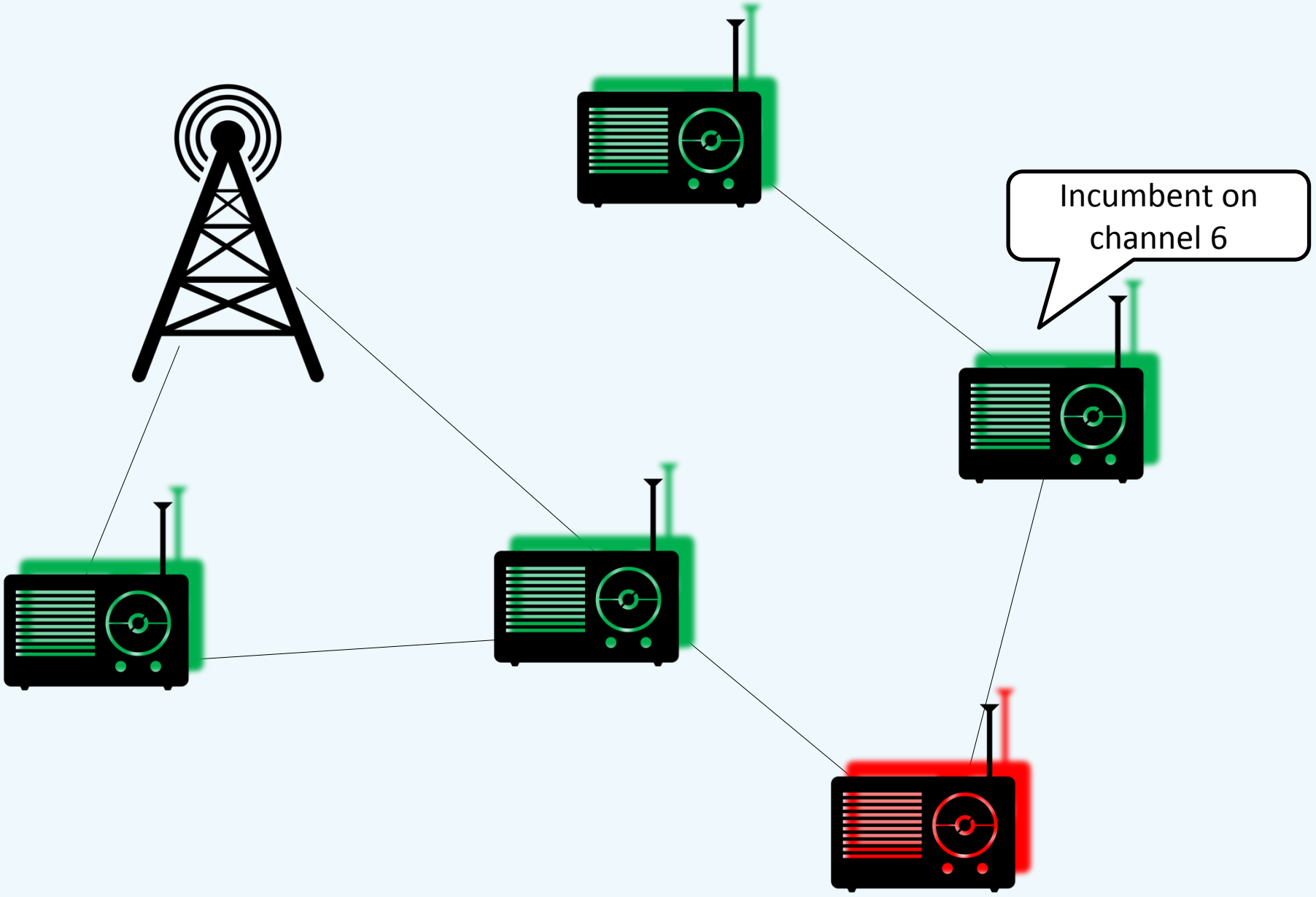


Change cognitive messages being sent through network

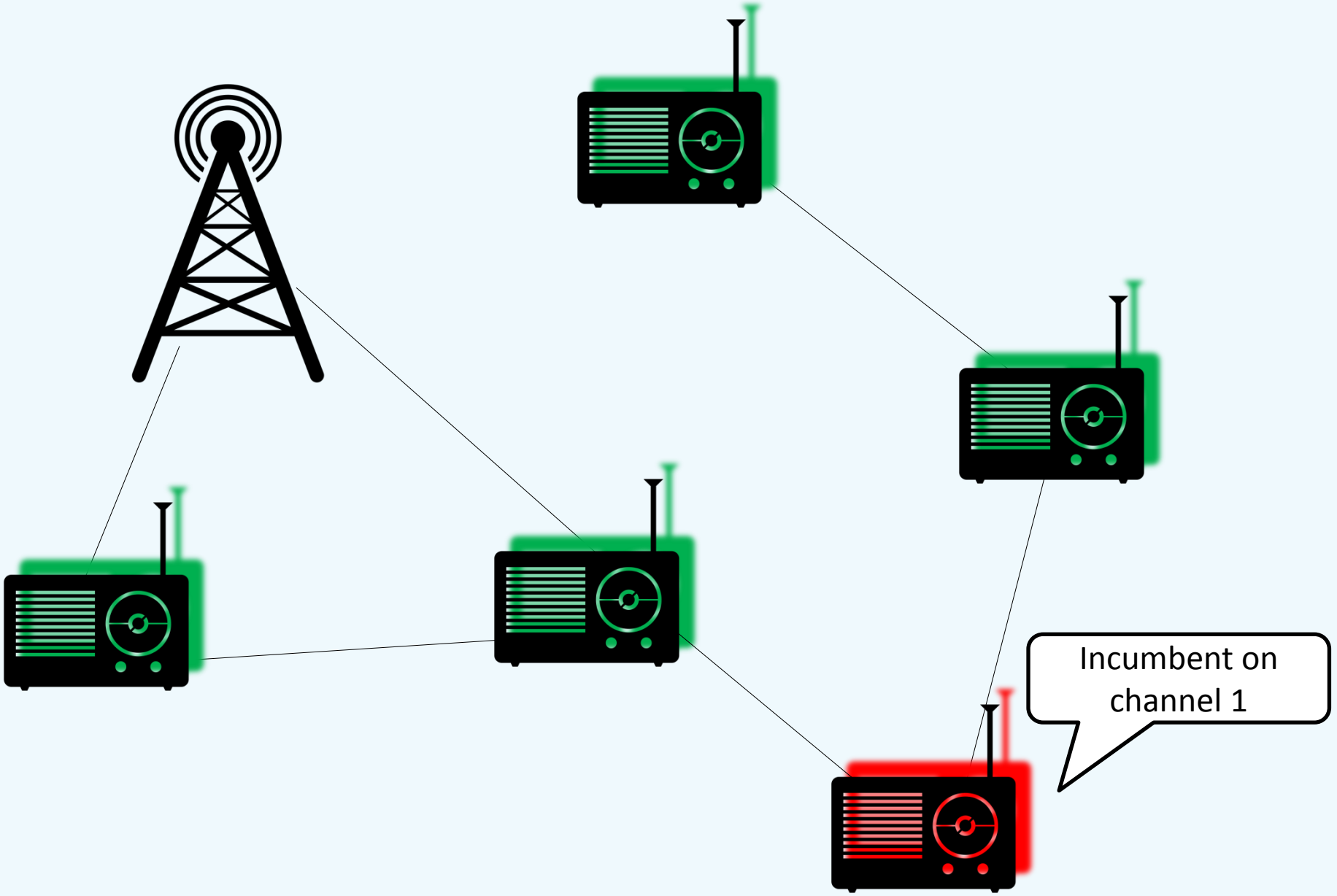
Change cognitive messages being sent through network



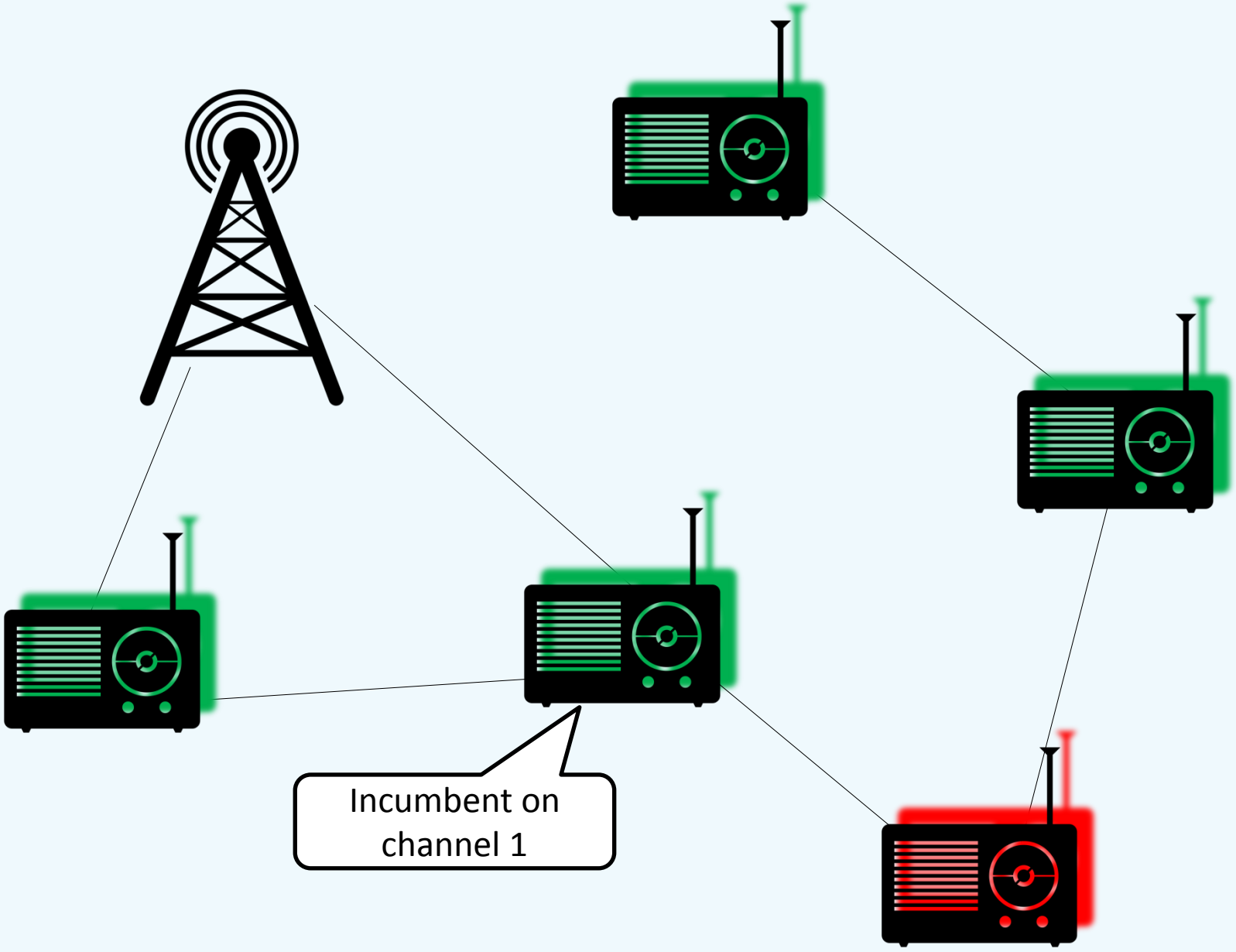
Change cognitive messages being sent through network



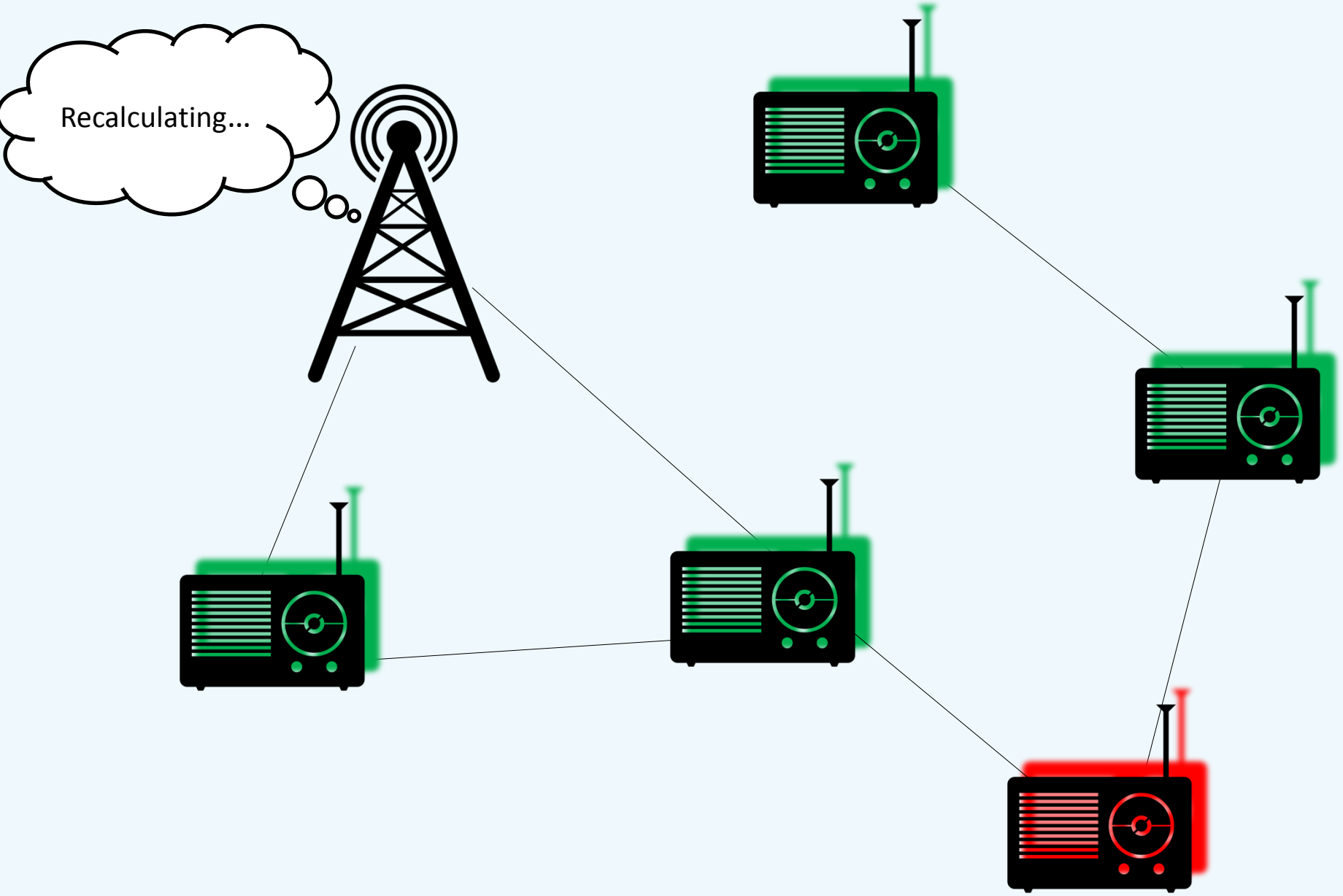
Change cognitive messages being sent through network



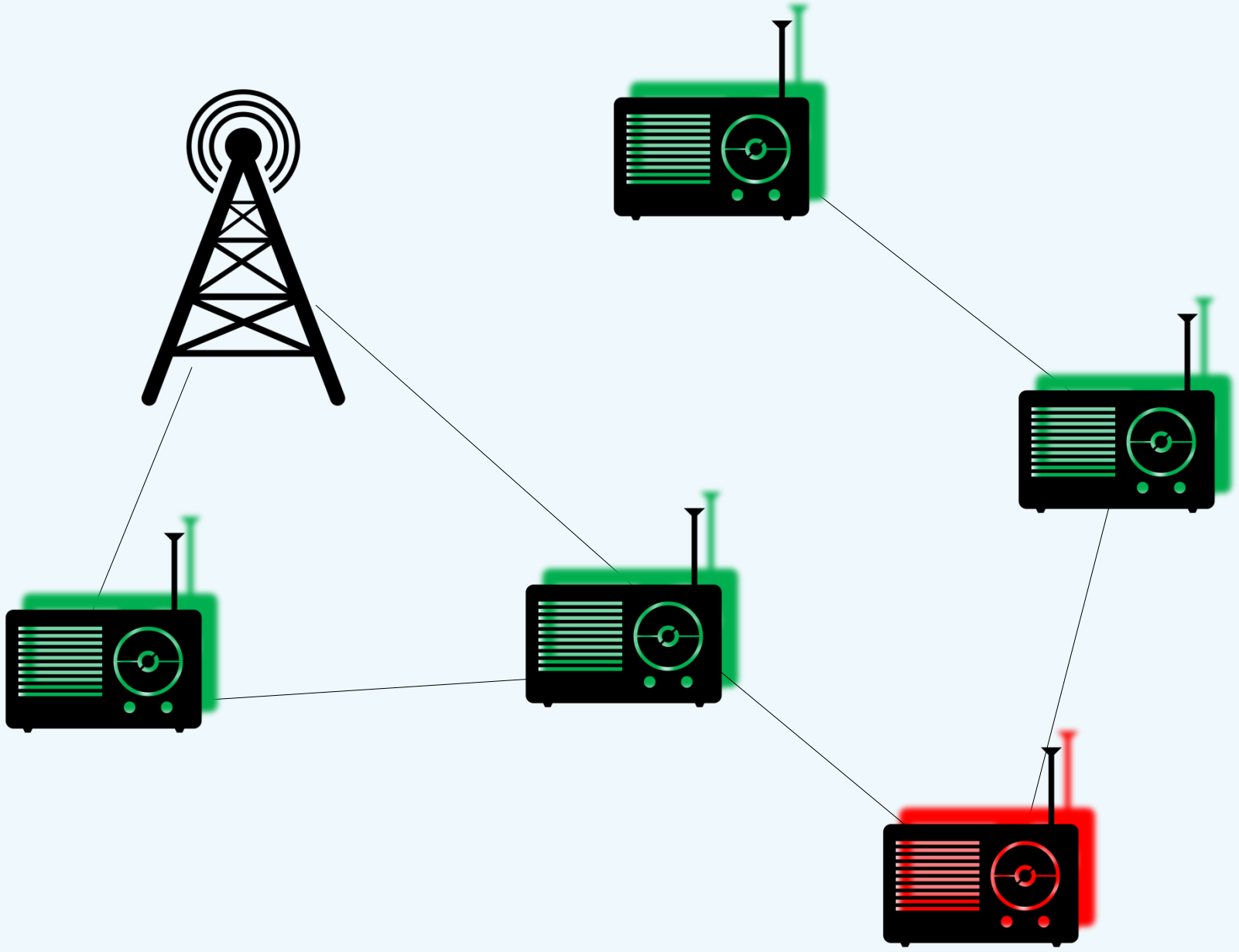
Change cognitive messages being sent through network



Change cognitive messages being sent through network

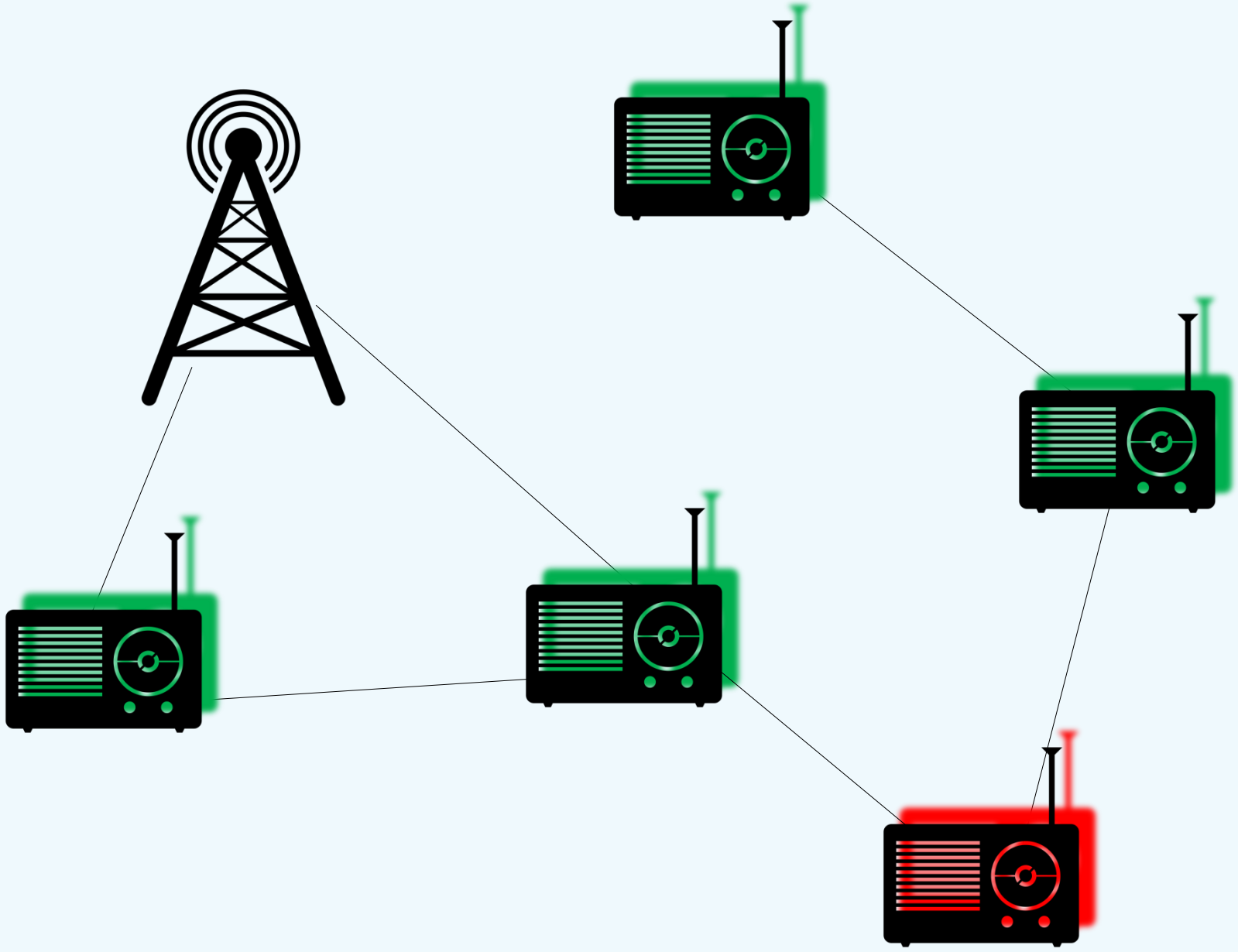


Routing Disruption

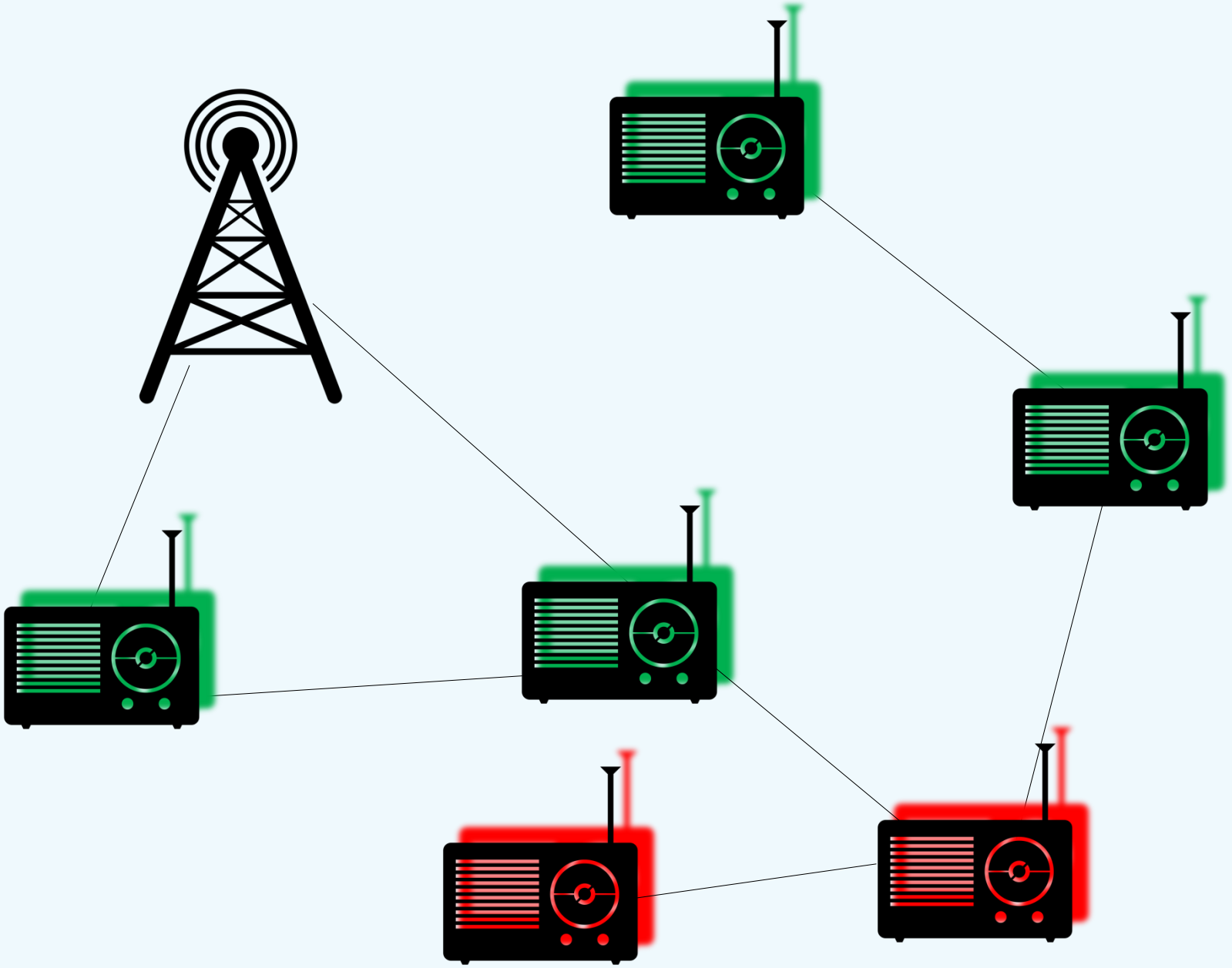


Sybil Attack

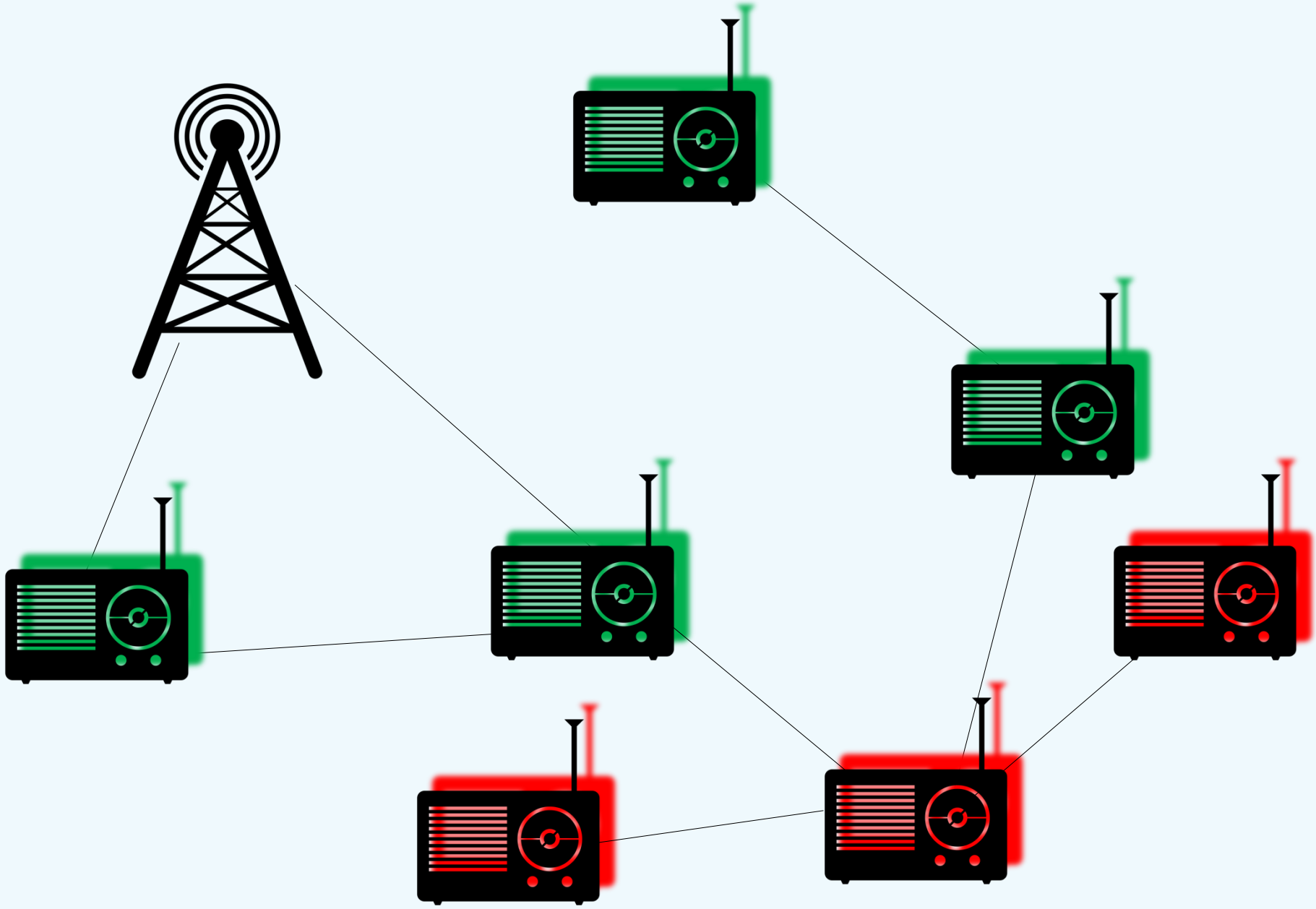
Sybil Attack



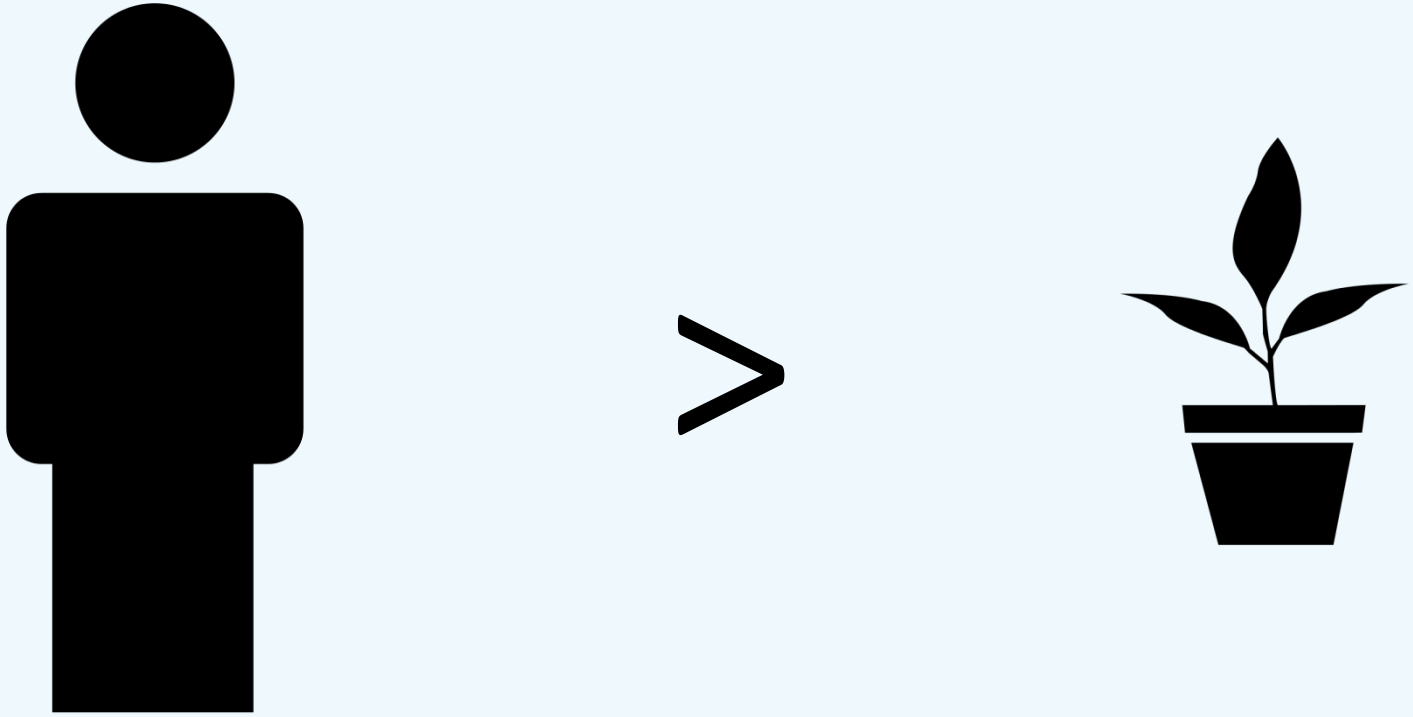
Sybil Attack



Sybil Attack

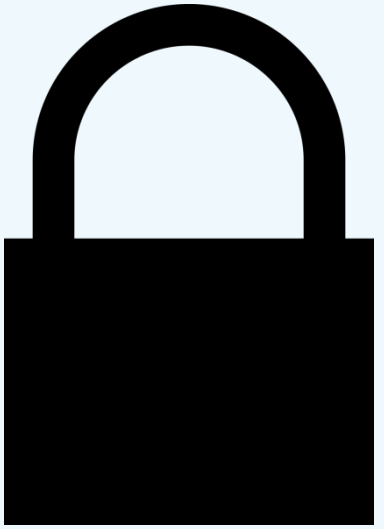


Priority Attack



Attacks on Crypto

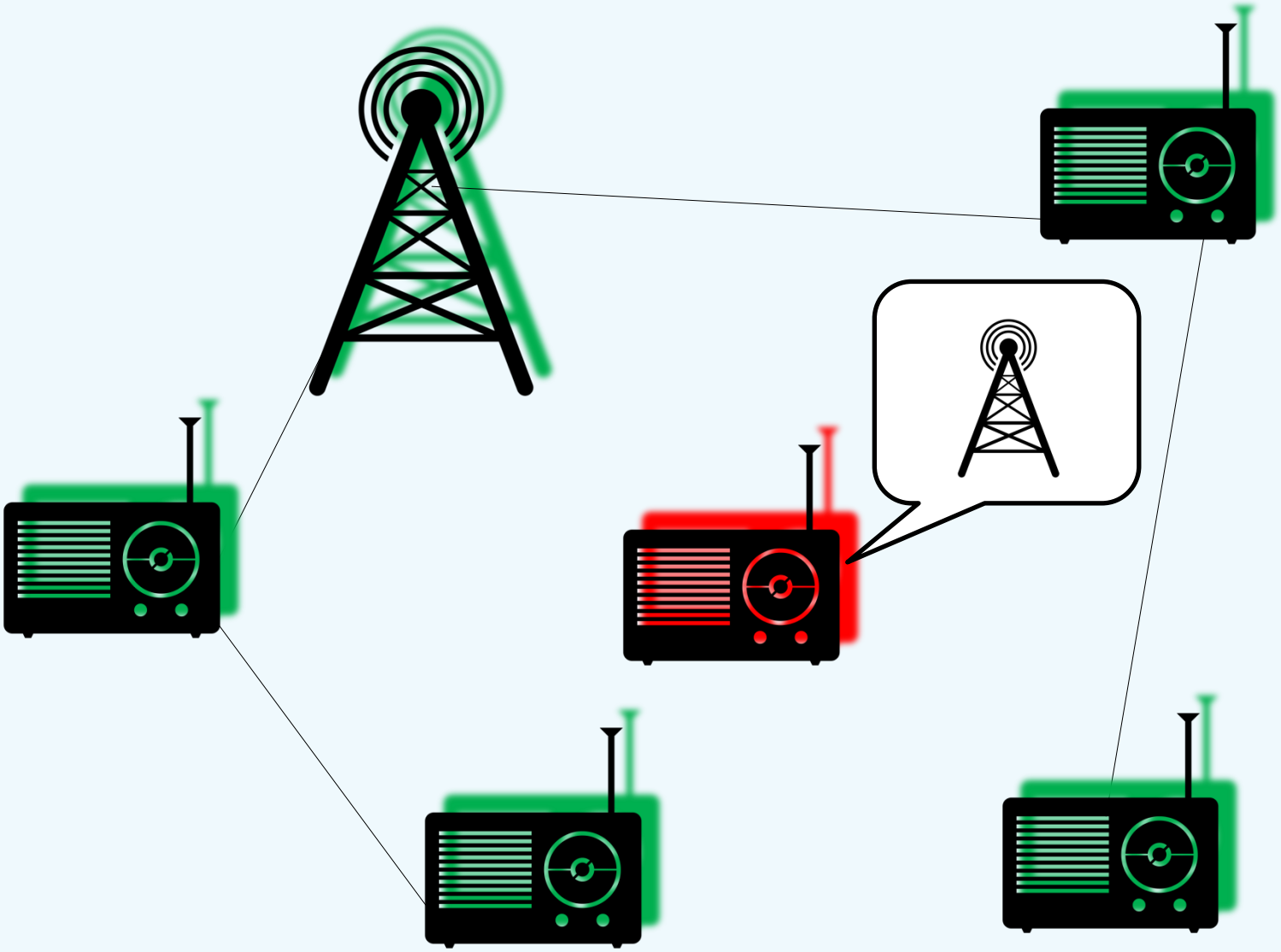
VS



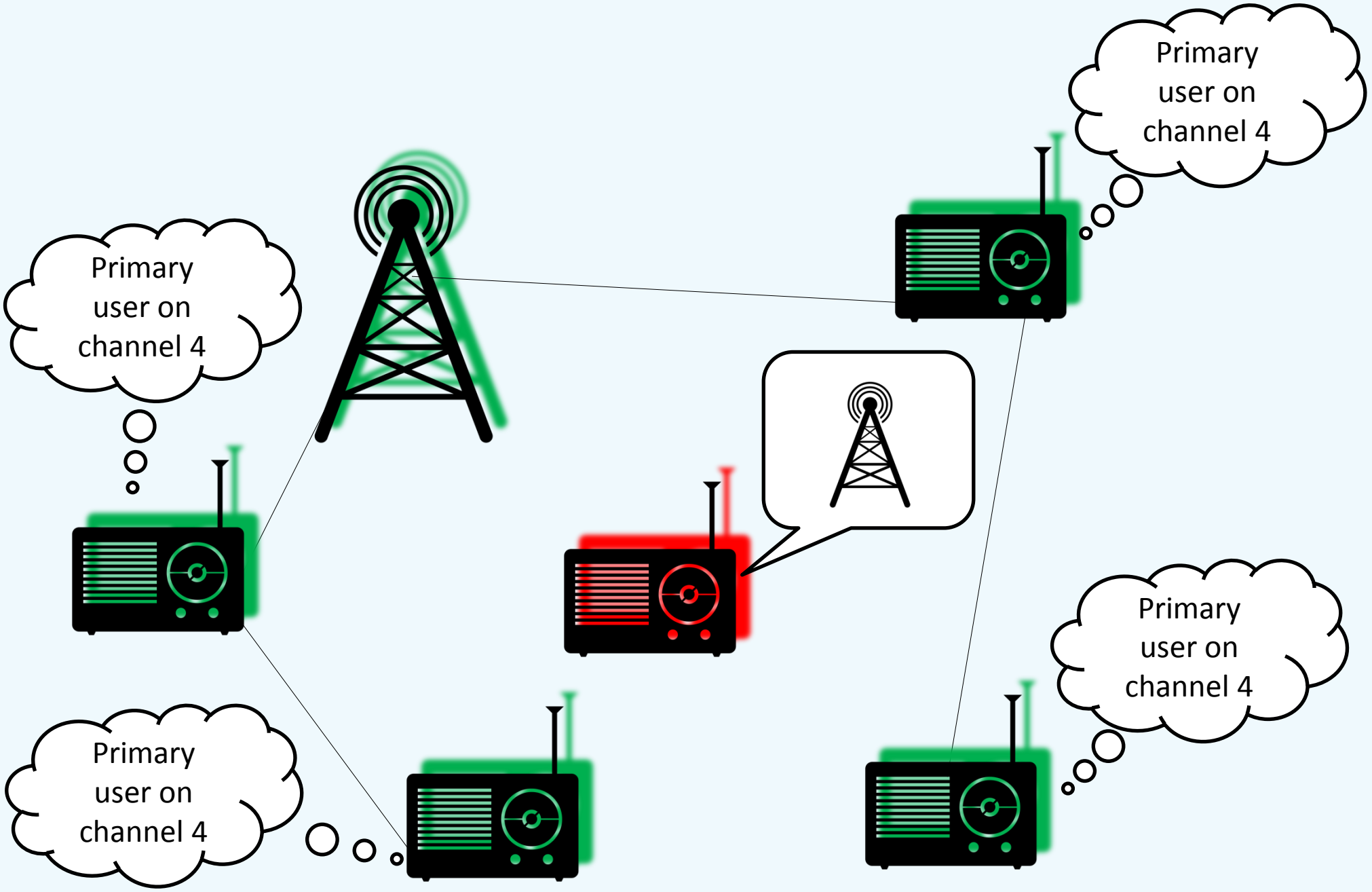
Attacks on Data Privacy

Primary User Emulation

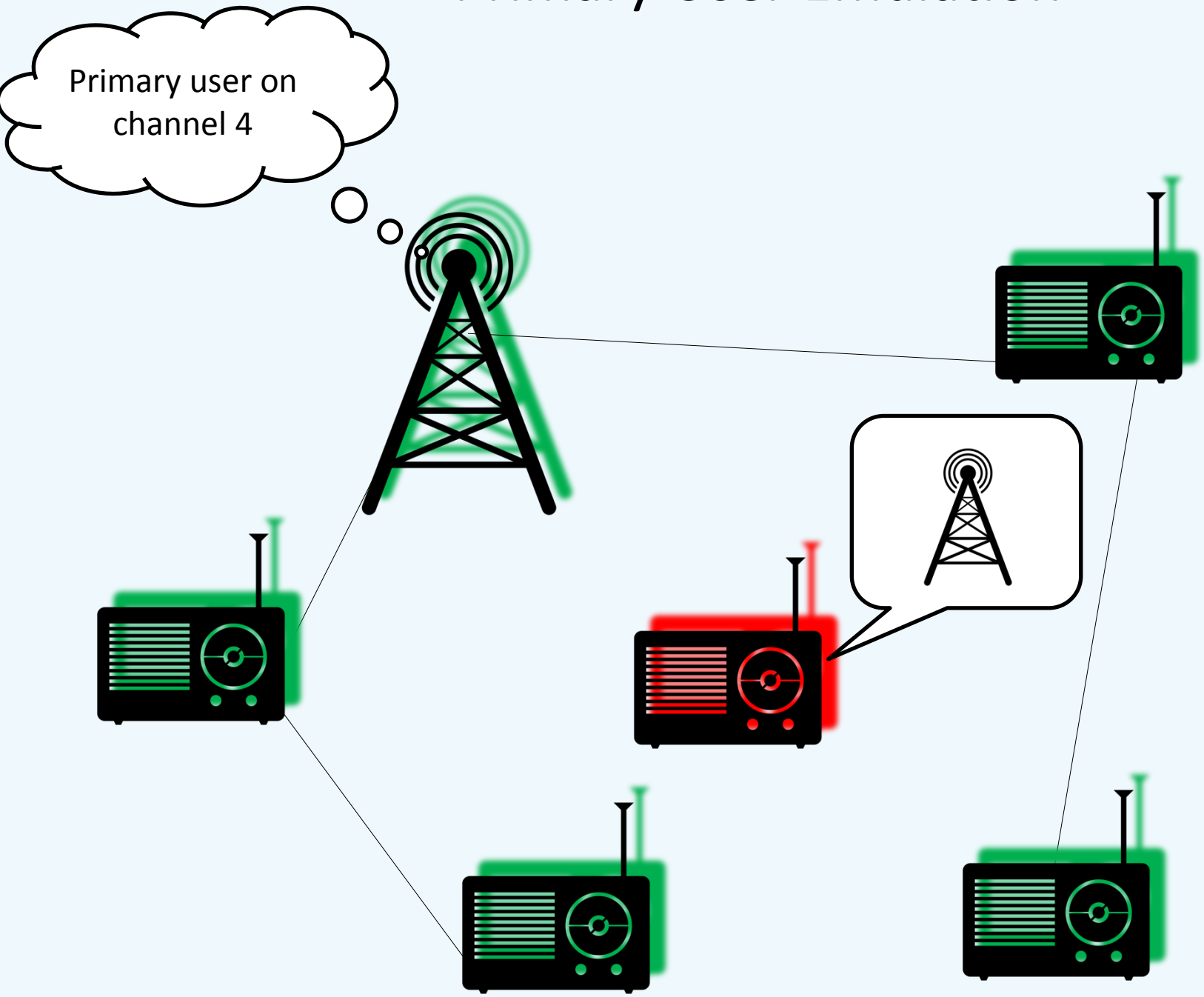
Primary User Emulation



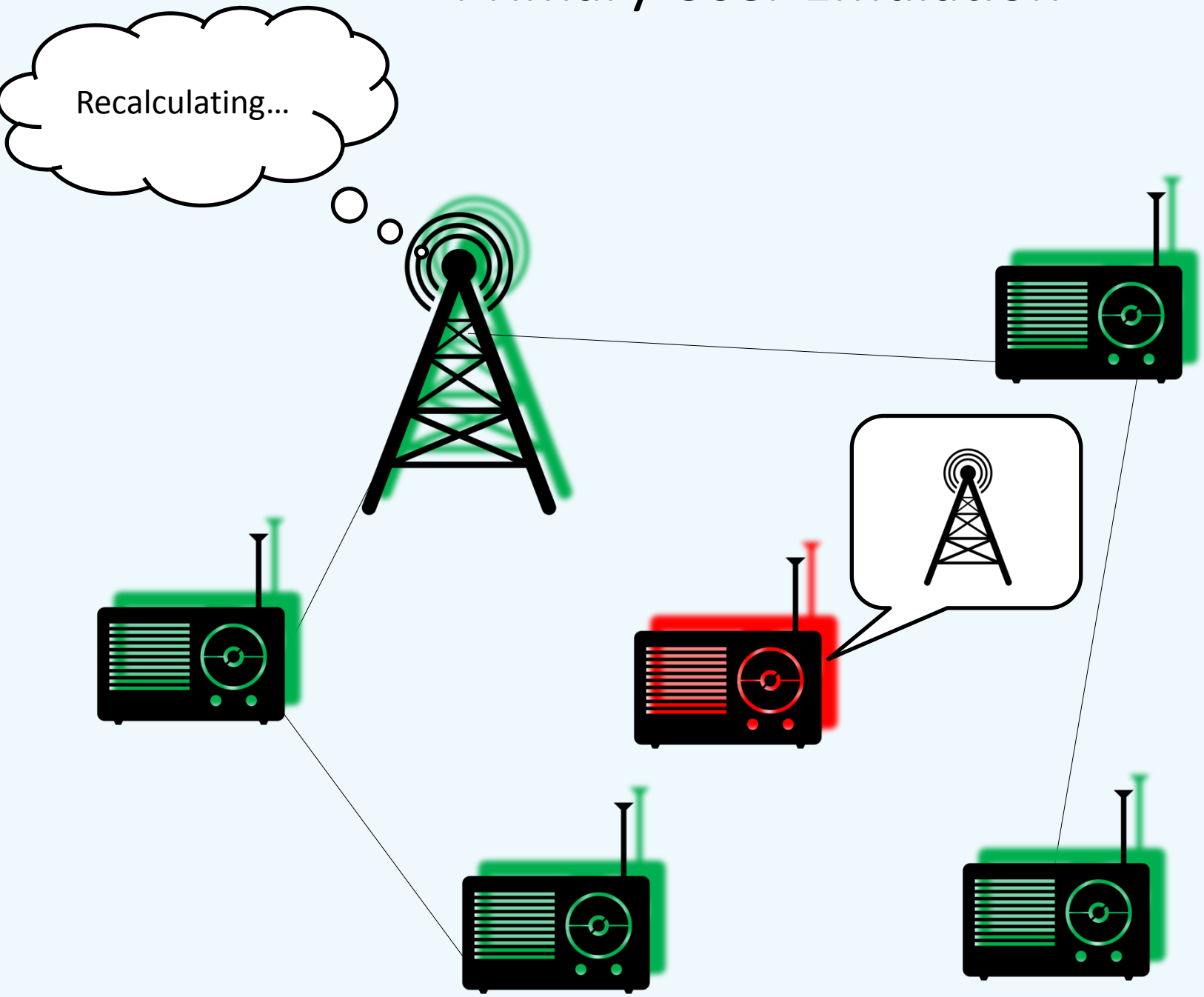
Primary User Emulation



Primary User Emulation

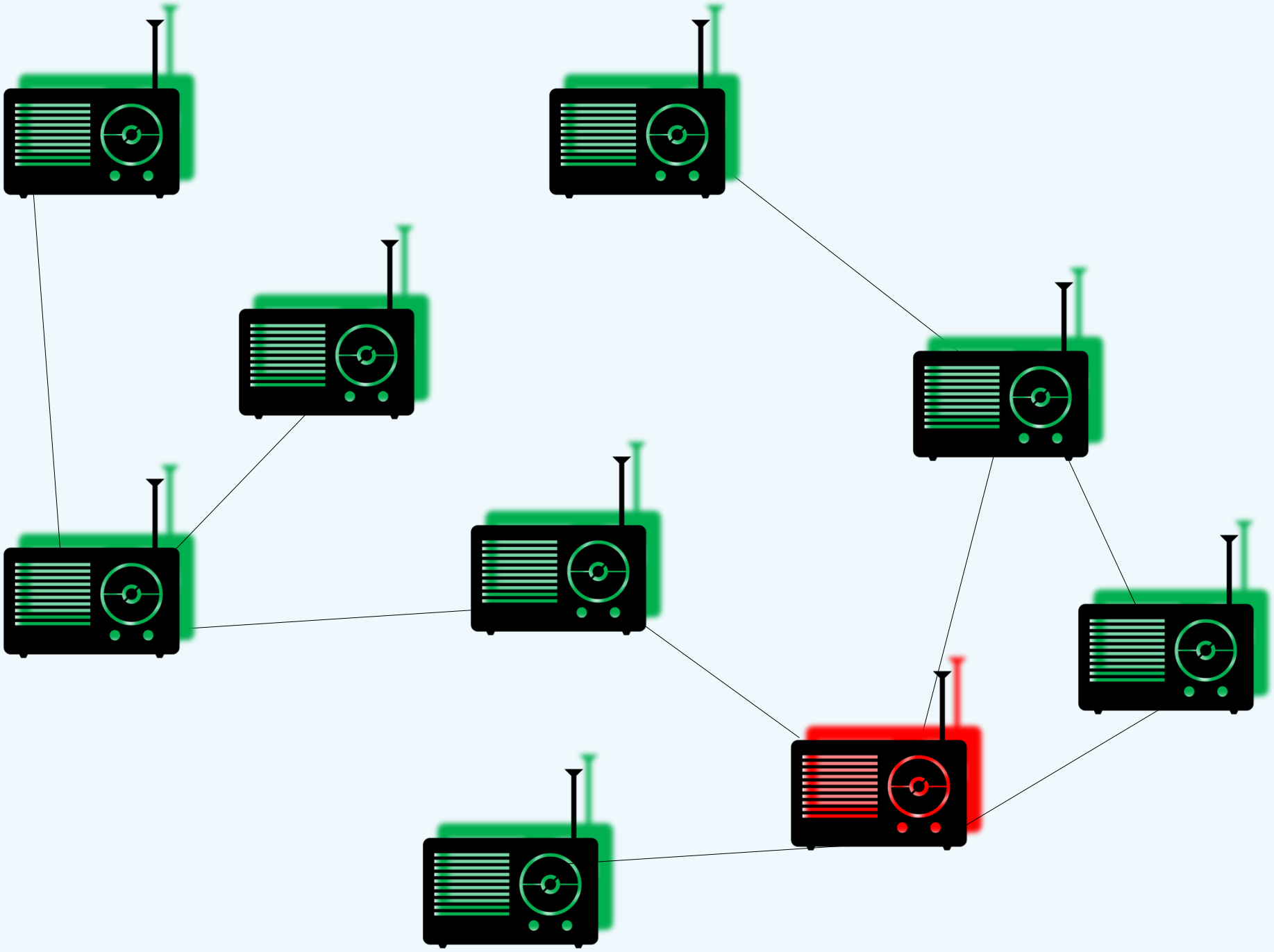


Primary User Emulation



Countermeasures

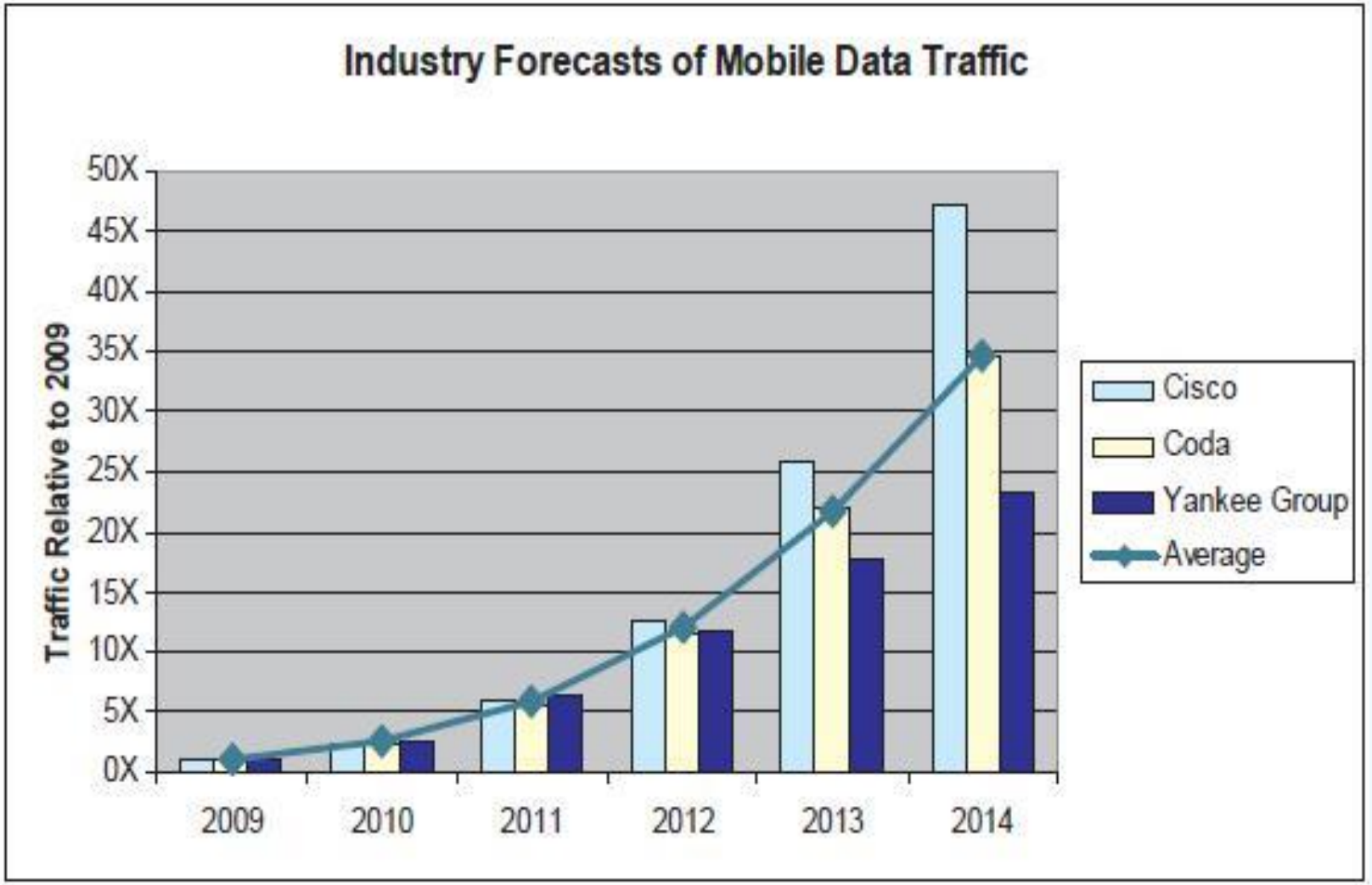
Cooperative Intrusion Detection



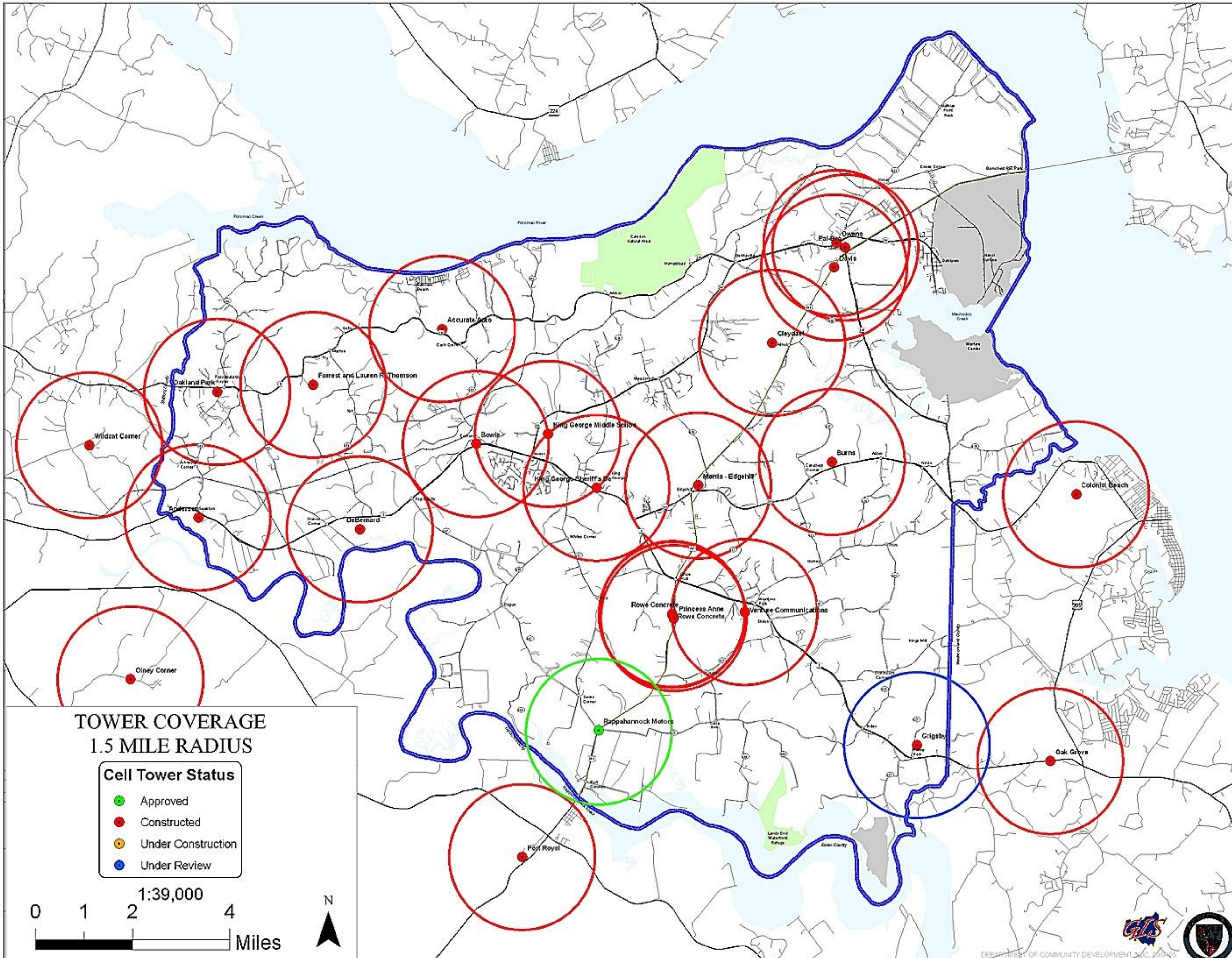
Device Reputation

Device Location

Why this matters


Industry Forecasts of Mobile Data Traffic
Traffic Relative to 2009
50X
45X
40X
35X
30X
25X
20X
15X
10X
5X
0X
2009
2010
2011
2012
2013
2014
Cisco
Coda
Yankee Group
Average


NOT ALLOCATED
RADIONAVIGATION
MARITIME MOBILE
FIXED
Radiolocation
AERONAUTICAL RADIONAVIGATION
Aeronautical Mobile
3 kHz
300 kHz
3 MHz
30 MHz
300 MHz
3 GHz
30 GHz
300 GHz


TOWER COVERAGE
1.5 MILE RADIUS
Cell Tower Status
Approved
Constructed
Under Construction
Under Review
1:39,000
0 1 2 4
Miles
N
Accurate Auto
Forrest and Lauren R. Thomson
Oakland Park
Wildcat Corner
Bowie
King George Middle School
King George Sheriff's Of
Morris - Edgehill
Claydael
Pal-Bro
Owens
Davis
Burns
Colonial Beach
Anderson
DeBernard
Rowe Concrete
Princess Anne
Rowe Concrete
Venture Communications
Olney Corner
Rappahannock Motors
Grigsby
Oak Grove
Port Royal

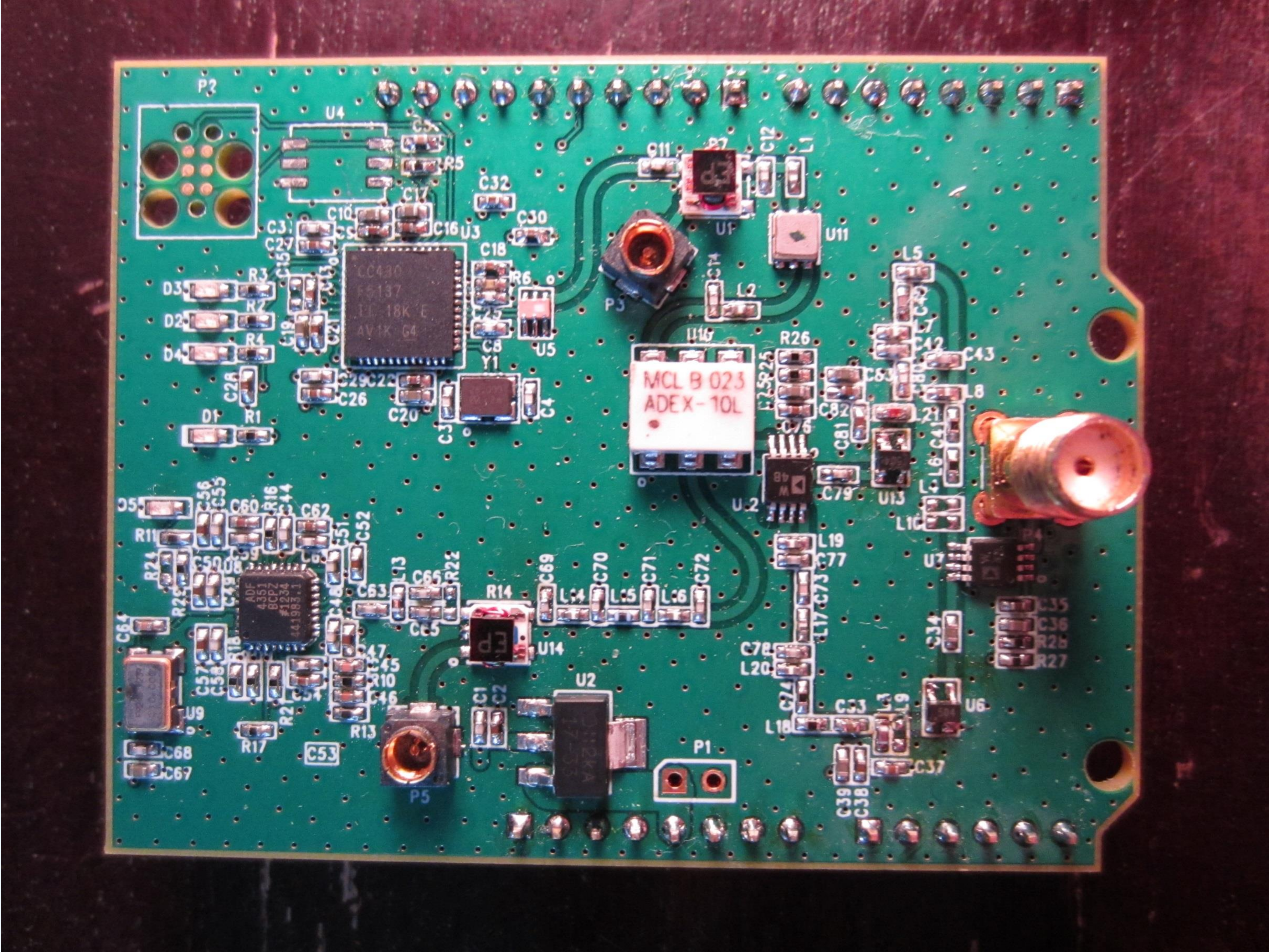
Tools


Ettus Research
USRP E100

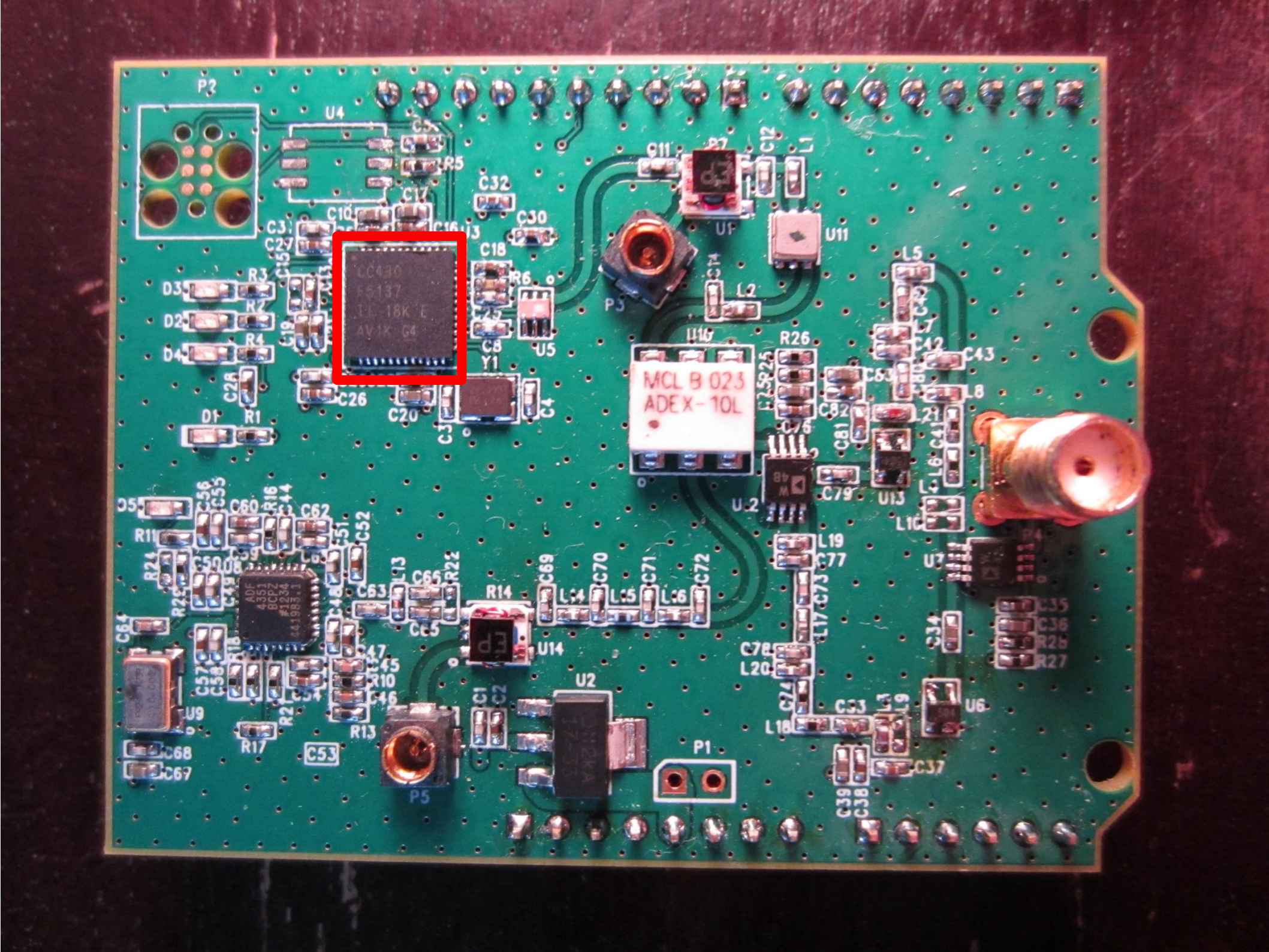

MaxStream™
XBee™
FCC ID: OUR-XBEE
IC ID: 4214A-XBEE
www.maxstream.net
1
20

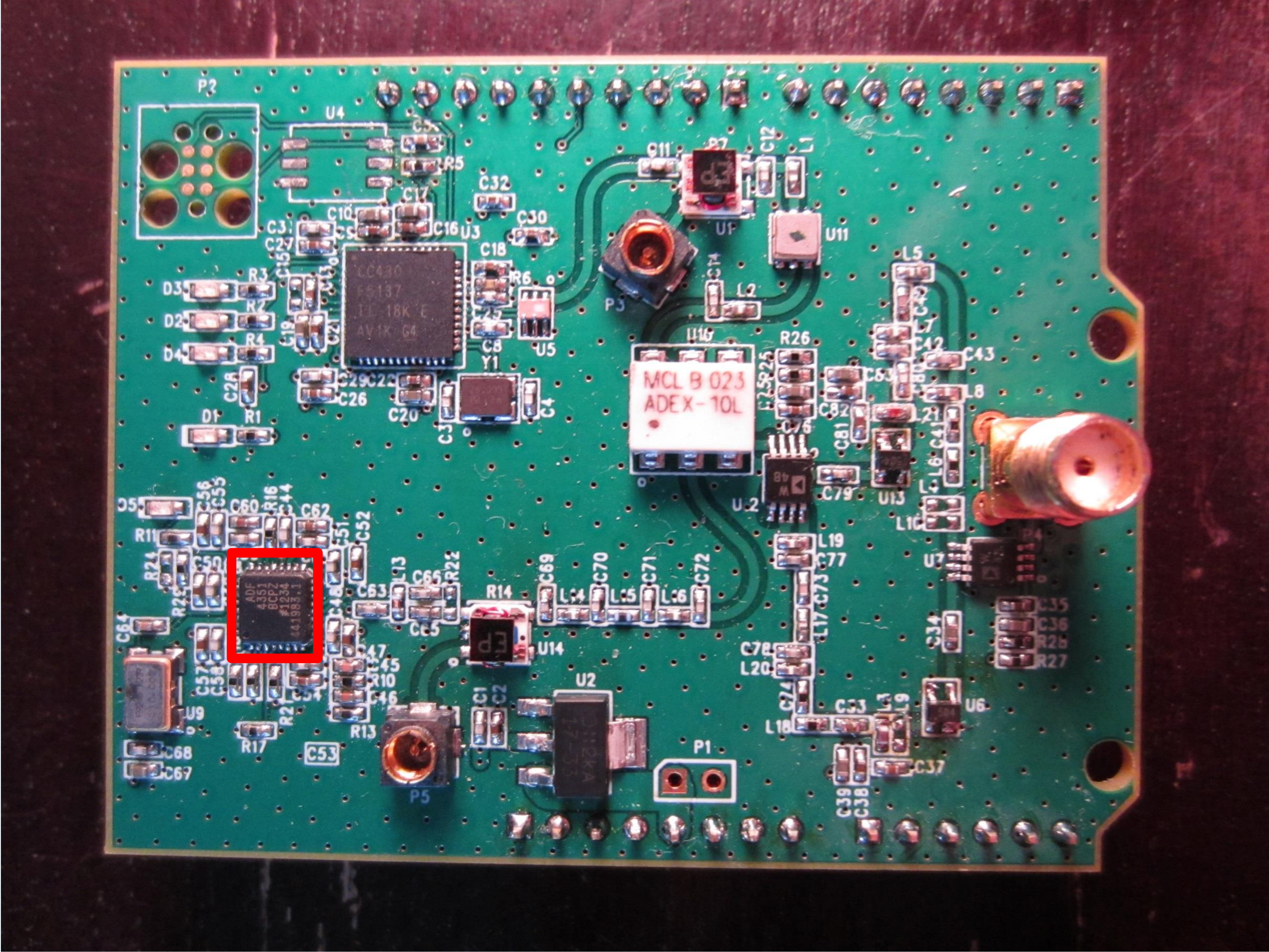
Level

30 MHz to 4.4 GHz
60 mW
SimpliciTI
Fits Arduino shields
~$100 in quantity

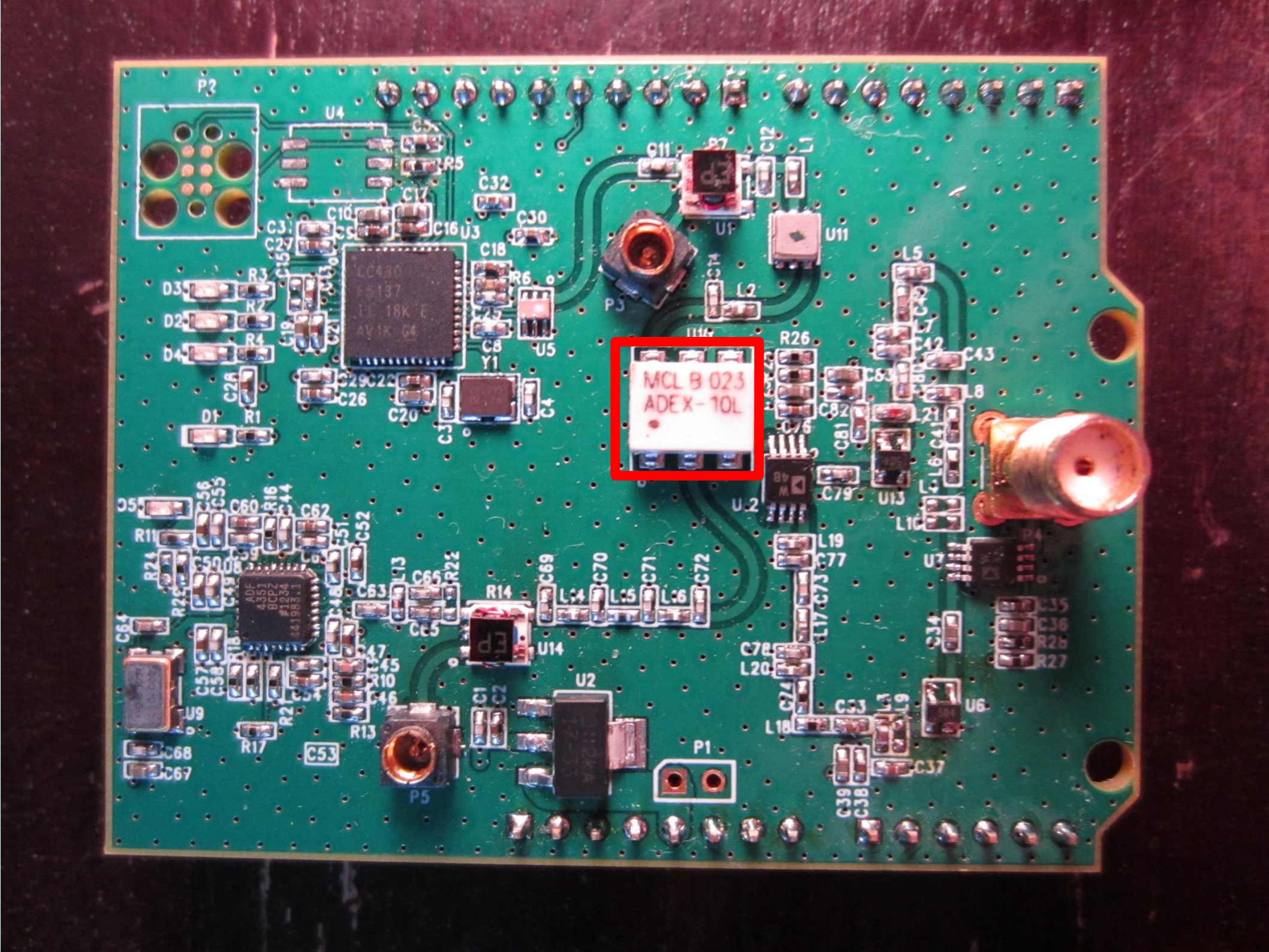


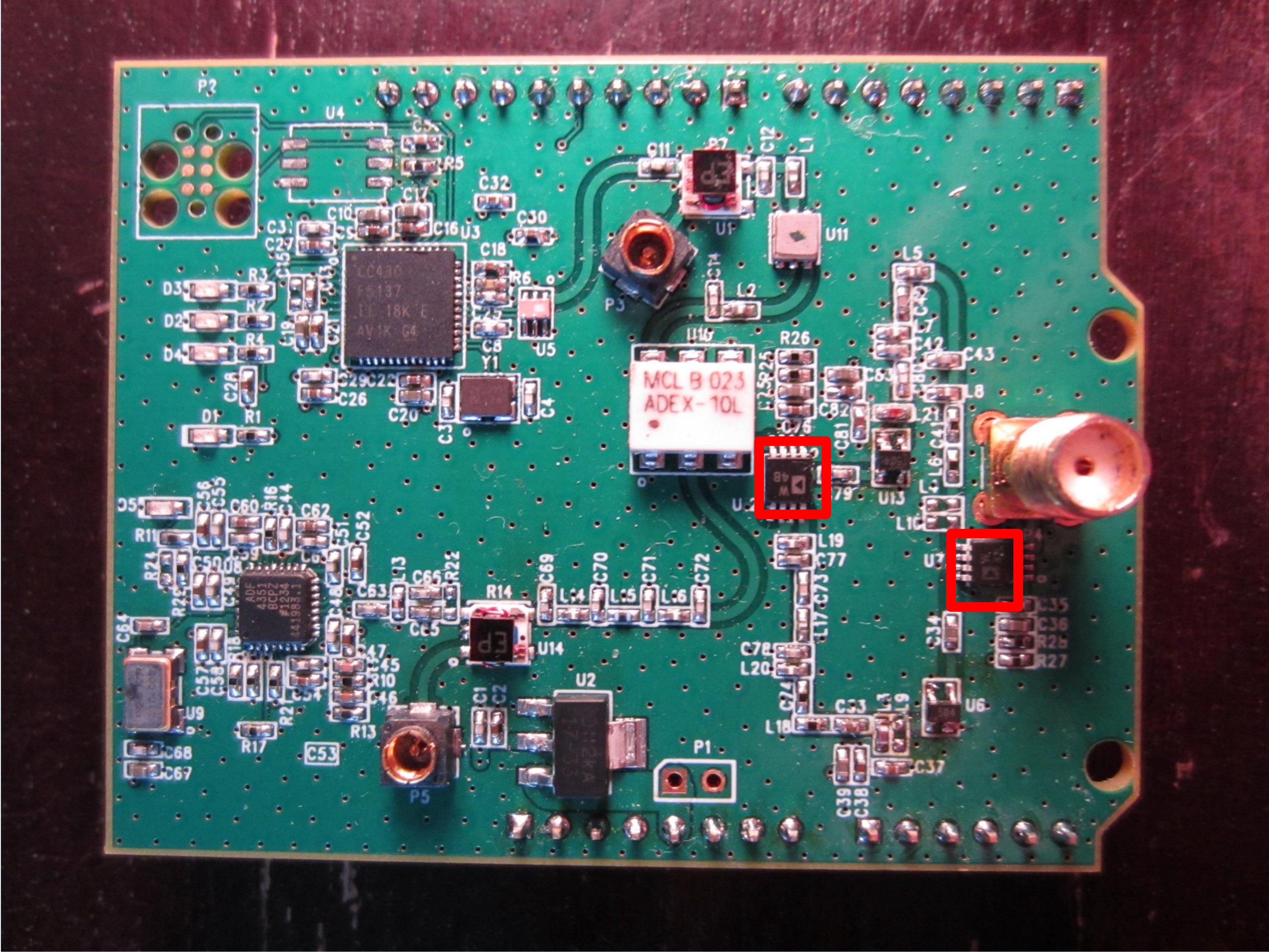
P2
U4
U3
U1
U11
P3
U10
MCL B 023
ADEX-10L
Y1
U5
U8
ADF
4351
BCPZ
U14
R14
U2
U9
U7
U6
U13
P1
P5

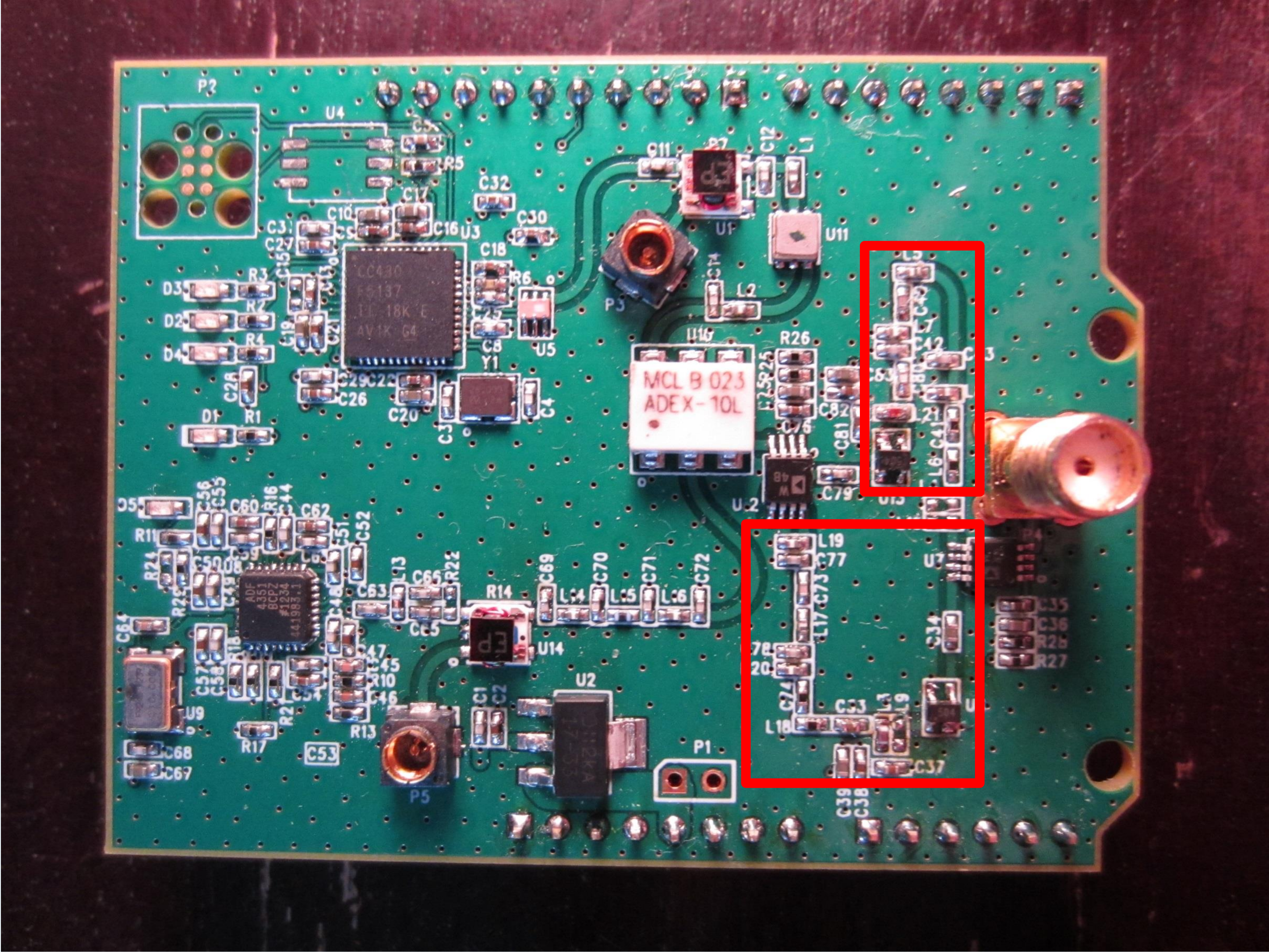

P2
U4
C5
R5
C32
C17
C10
C16
U3
C30
C18
C3
C27
C15
C13
R3
D3
R2
D2
R4
D4
C19
C28
D1
R1
CC430
F6137
18K E
AV1K G4
C26
C20
C8
Y1
C4
C3
R6
U5
P3
C11
D7
C12
L1
U1
U11
L5
C14
L2
U10
MCL B 023
ADEX-10L
R26
R25
C25
C76
U12
C79
C81
C82
C63
C42
C43
C7
L8
L21
C41
L6
U13
L10
C5
R11
C56
C55
C60
R16
C44
C62
C51
C52
R24
C50
C59
C49
R23
C64
C48
C63
L13
C65
R22
C66
R14
C69
C70
C71
C72
L14
L15
L16
U14
ADF
4351
BCPZ
%1234
4419B3.1
C57
C58
C47
C45
X10
C46
C54
R18
R2
U9
R17
R13
C53
C68
C67
P5
C1
C2
U2
P1
C39
C38
L19
C77
C73
L17
C78
L20
C24
C33
L3
L18
U6
C37
U7
C34
C35
C36
R28
R27

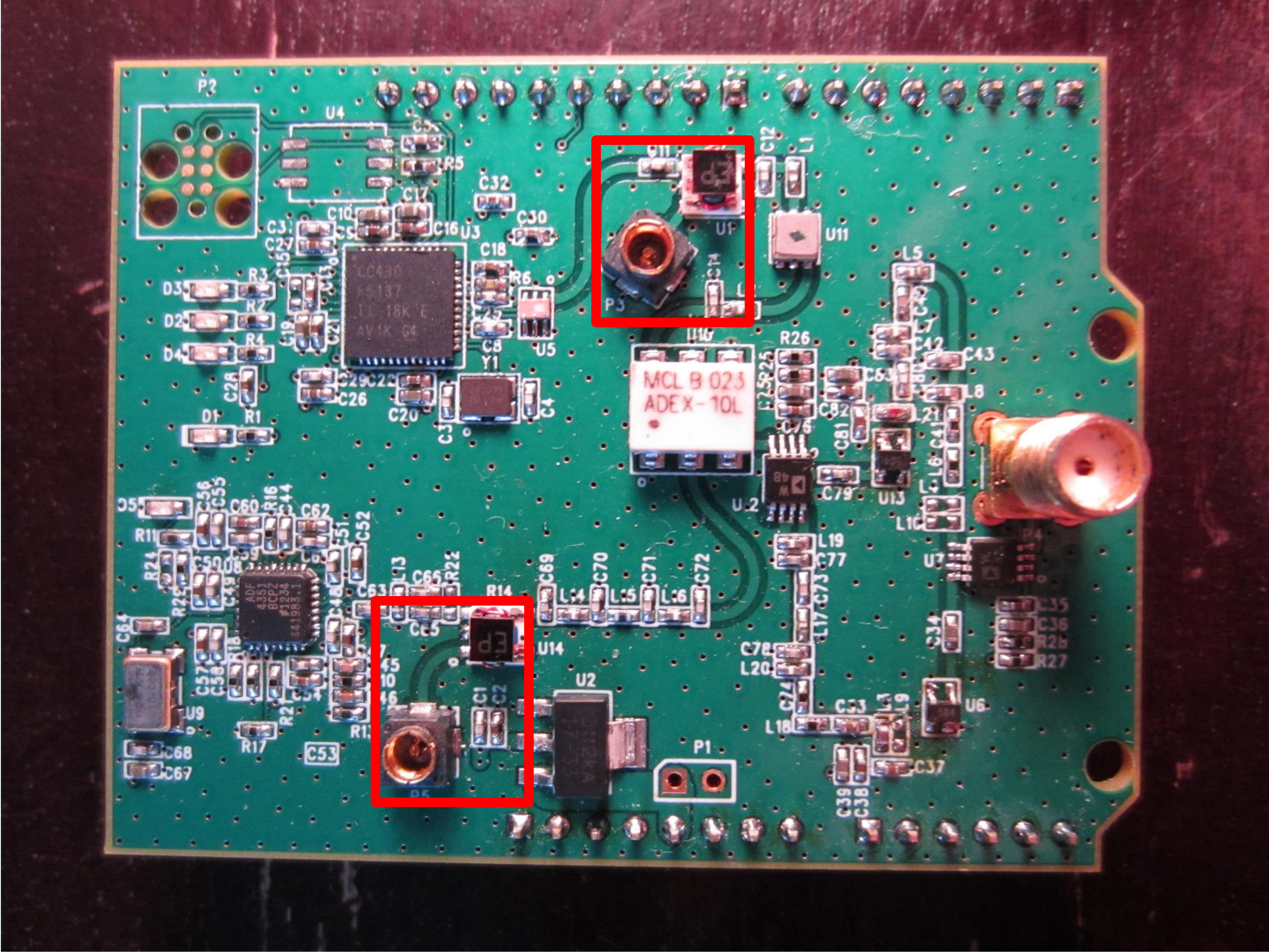


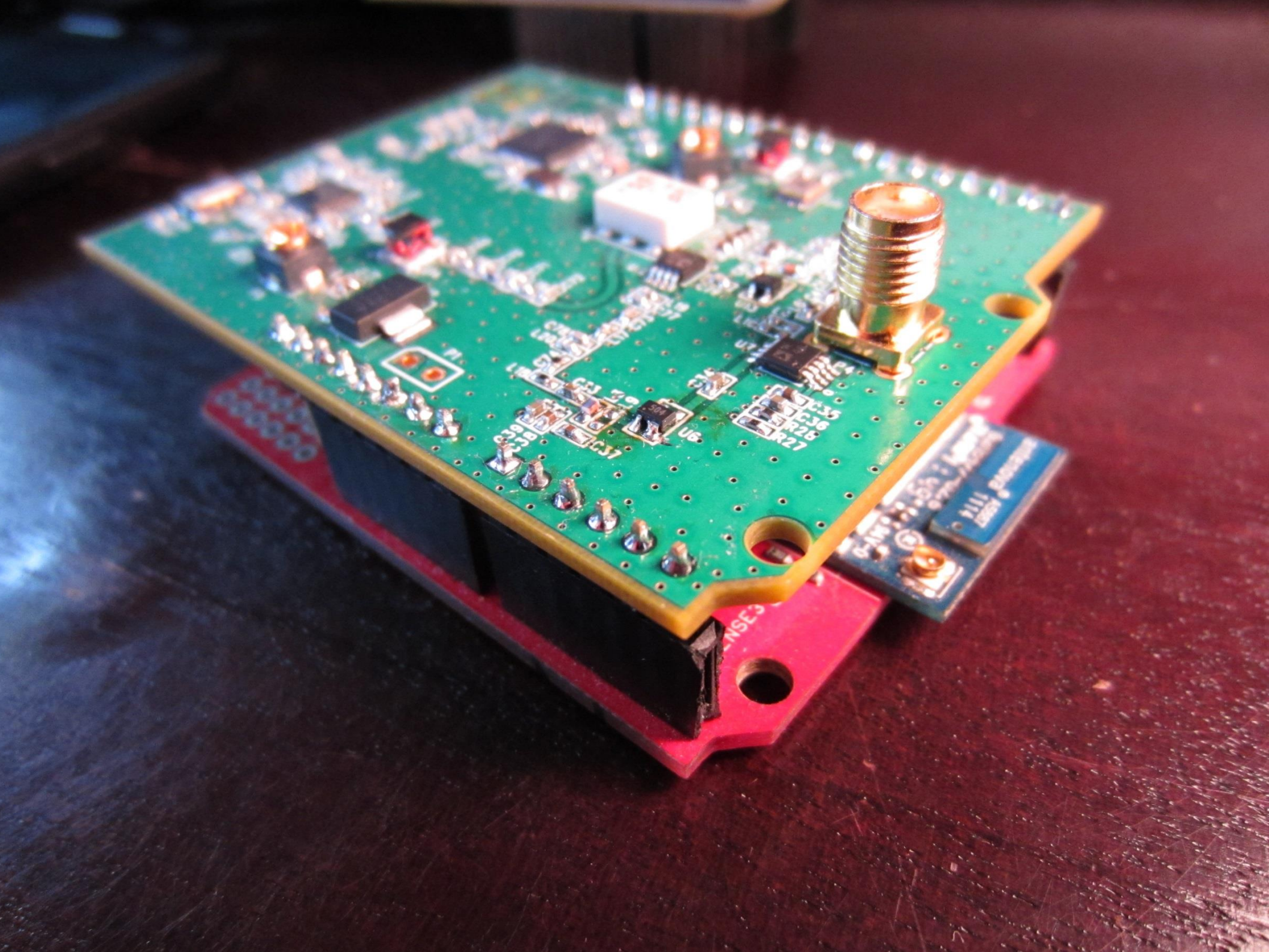
MCL B 023
ADEX-10L
ADF
4351
BCPZ
P2
U4
P3
P5
P1
U2
U14
U11
U7
U6
U9
Y1
R14

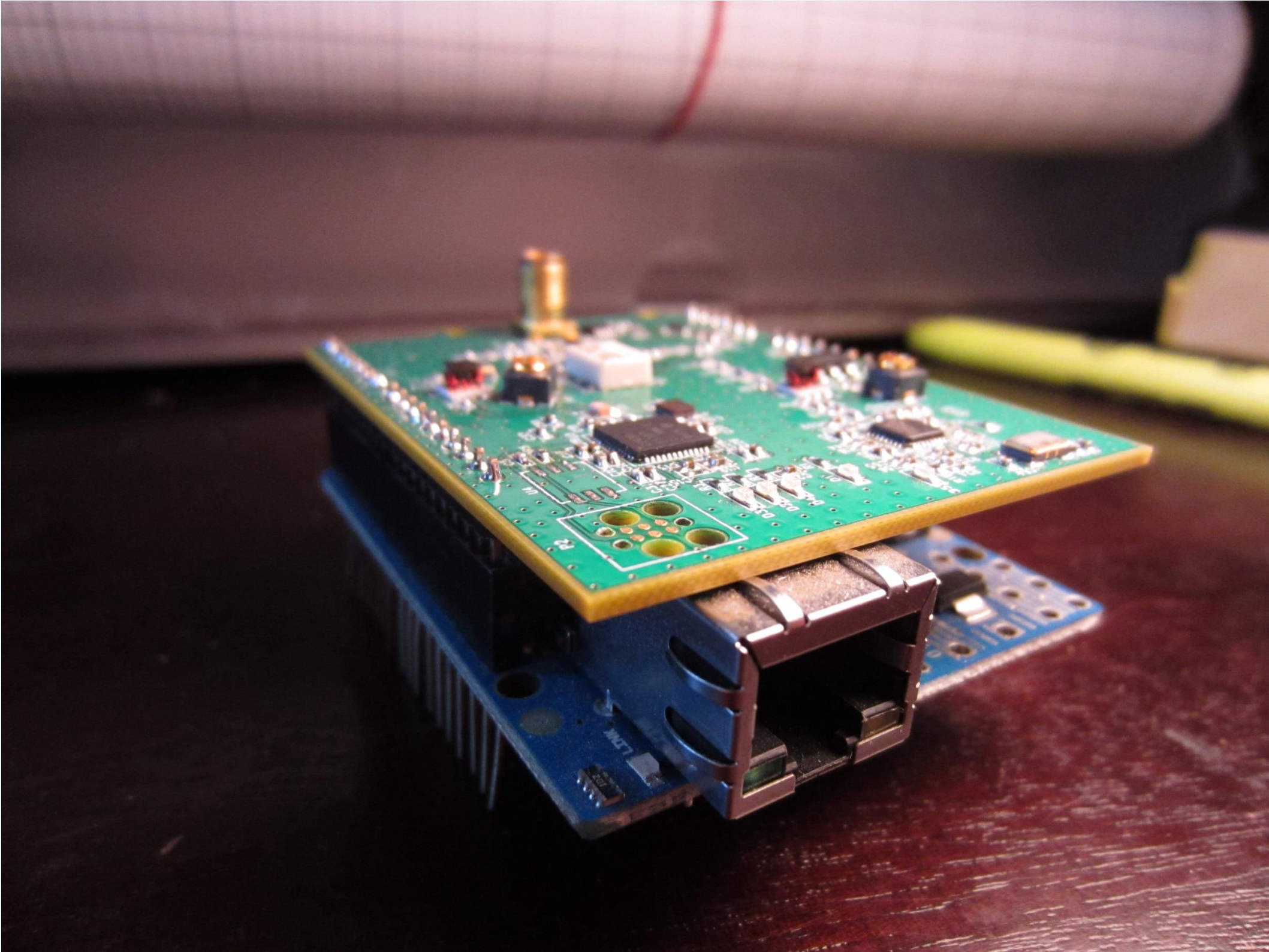

MCL B 023
ADEX-10L


P2
U4
U3
U1
U11
P3
U5
Y1
U10
MCL B 023
ADEX-10L
U13
U7
U14
U2
P1
P5
U9
U6
ADF
4351
BCPZ


MCL B 023
ADEX-10L
U10
U4
U11
P2
P3
P5
P1
U2
U14
R14
U9


P2
U4
R5
C17
C32
C30
C18
U3
R6
U5
Y1
C8
C4
C26
C20
D1
R1
D2
D3
D4
R3
R4
P3
U1
U11
C12
L1
L5
L7
L8
C43
U10
R26
MCL B 023
ADEX-10L
U12
C79
U13
L19
C77
U7
C35
C36
R27
C34
C78
L20
C33
L18
U6
C37
C39
C38
P1
U2
U14
C1
C2
R14
C69
C70
C71
C72
L13
C63
C65
C62
C60
C52
D5
R11
ADF
4351
C64
U9
R17
C53
C68
C67

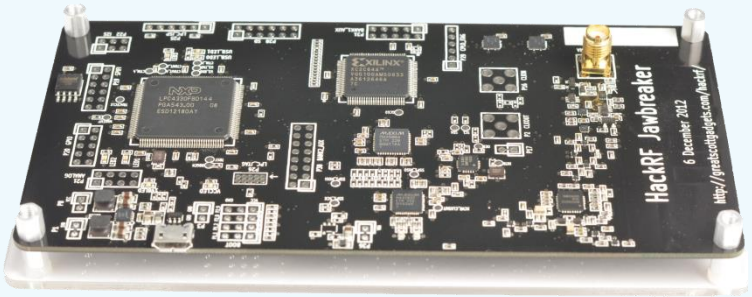

C35
C36
R26
R27
U6
C37



Other tools

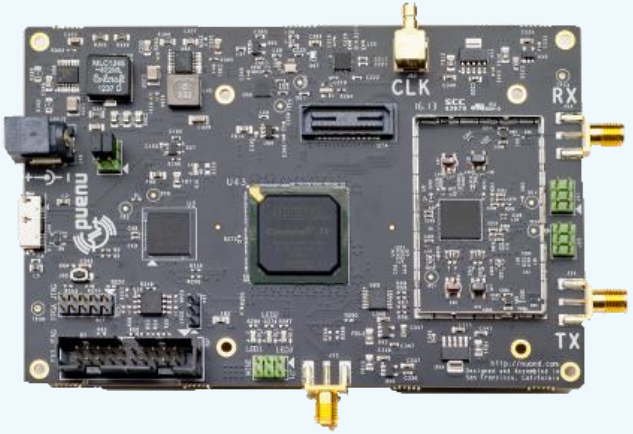
HackRF ($300)

Michael Ossmann



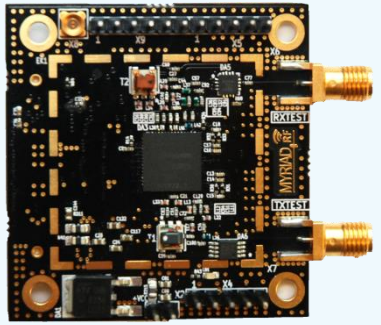
BladeRF ($420)

Nuand



MyriadRF ($300)

Azio



What’s next

Latest version of these slides + code & schematics:

defcon21.hscott.net

Image Credits:

Radio designed by Monika Ciapala from The Noun Project

Radio Tower designed by iconoci from The Noun Project

Brain designed by Samuel Dion-Girardeau from The Noun Project

Person designed by Björn Andersson from The Noun Project

Plant designed by Luke Anthony Firth from The Noun Project

Lock from The Noun Project

Speedometer designed by Volodin Anton from The Noun Project

Location designed by Ricardo Moreira from The Noun Project

Further Reading:

FCC. In the matter of unlicensed operation in the TV broadcast bands: second report and order and memorandum opinion and order., Nov. 2008.

Fadlullah, Zubair Md, et al. "An Intrusion Detection System (IDS) for Combating Attacks Against Cognitive Radio Networks." *IEEE Network* (2013): 52.

Jackson, David. "Exploiting Rogue Signals to Attack Trust-based Cooperative Spectrum Sensing in Cognitive Radio Networks." (2013).

Du, Jiang, Chunjiao Zhu, and Zhaohui Chen. "Security issues in cooperative spectrum sensing for cognitive radio network." *2012 International Conference on Graphic and Image Processing*. International Society for Optics and Photonics, 2013.

For even more readings, see the references of these papers.