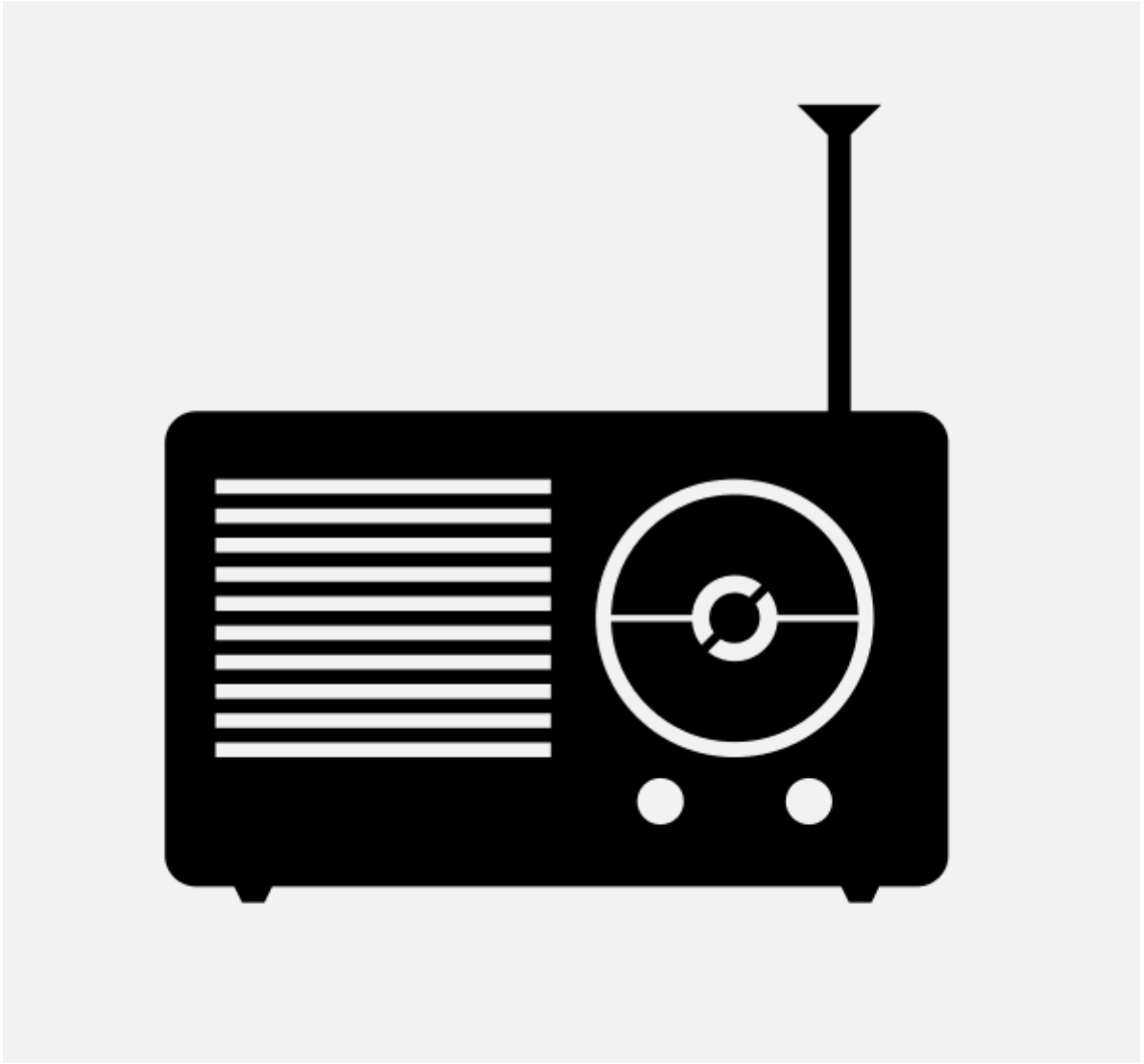
Security in Cognitive Radio Networks

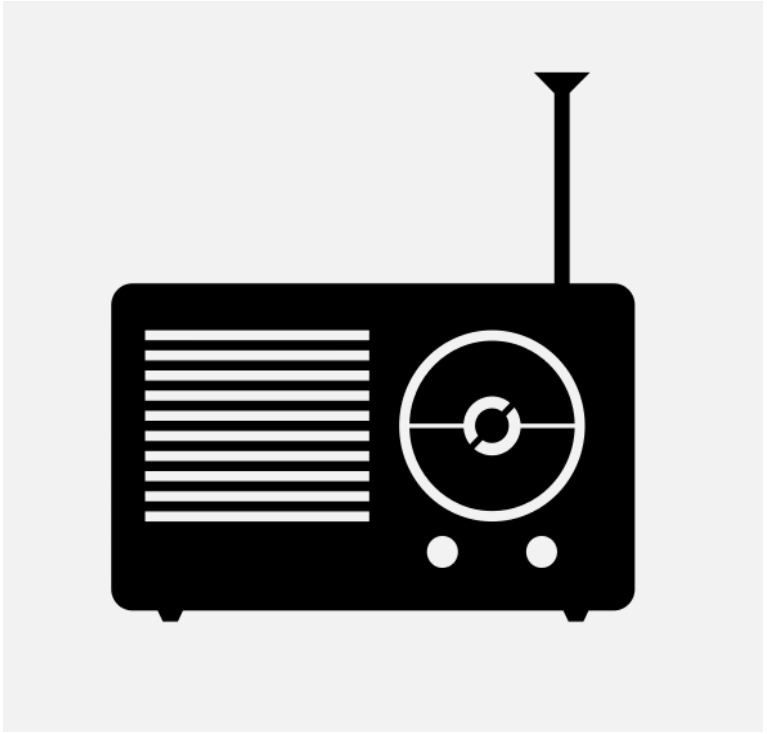
Hunter Scott

Latest version of these slides:

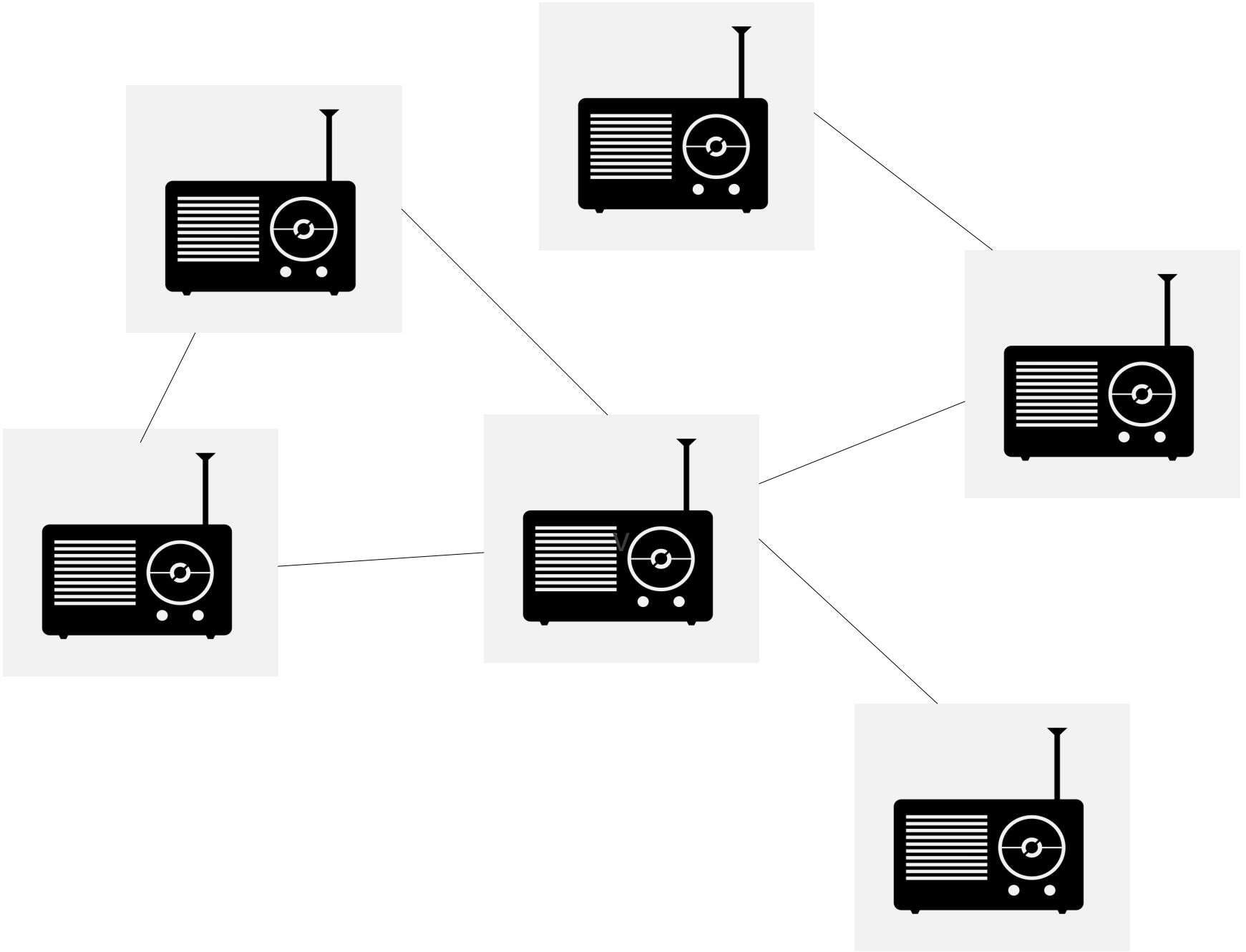
defcon21.hscott.net



```
void link_changed_callback(int speed);
static volatile bool link_is_up = false;     // eth handler sets this


void
start_rx_streaming_cmd(const u2_mac_addr_t *host, op_start_rx_streaming_t *p)
{
 host_mac_addr = *host;        // remember who we're sending to

 /*
  * Construct  ethernet header and word0 and preload into two buffers
  */
 u2_eth_packet_t    pkt;
 memset(&pkt, 0, sizeof(pkt));
 pkt.ehdr.dst = *host;
 pkt.ehdr.ethertype = U2_ETHERTYPE;
 u2p_set_word0(&pkt.fixed, 0, 0);
 // DSP RX will fill in timestamp

 memcpy_wa(buffer_ram(DSP_RX_BUF_0), &pkt, sizeof(pkt));
 memcpy_wa(buffer_ram(DSP_RX_BUF_1), &pkt, sizeof(pkt));


 if (FW_SETS_SEQNO)
  fw_seqno = 0;

 // setup RX DSP regs
 dsp_rx_regs->clear_state = 1;                  // reset

 if (1){                  // we're streaming
  streaming_p = true;
  streaming_frame_count = FRAMES_PER_CMD;
  dsp_rx_regs->rx_command =
   MK_RX_CMD(FRAMES_PER_CMD * p->items_per_frame, p->items_per_frame,
          1, 1);                  // set "chain" bit

  // kick off the state machine
  dbsm_start(&dsp_rx_sm);
  dsp_rx_regs->rx_time = 0;         // enqueue first of two commands

  // make sure this one and the rest have the "now" and "chain" bits set.
  dsp_rx_regs->rx_command =
   MK_RX_CMD(FRAMES_PER_CMD * p->items_per_frame, p->items_per_frame,
          1, 1);
  dsp_rx_regs->rx_time = 0;               // enqueue second command
}
```

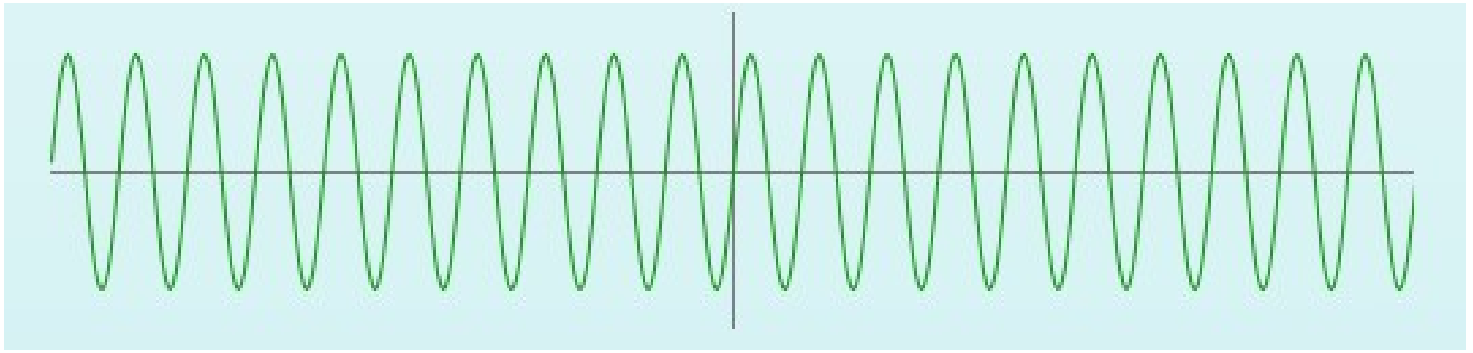


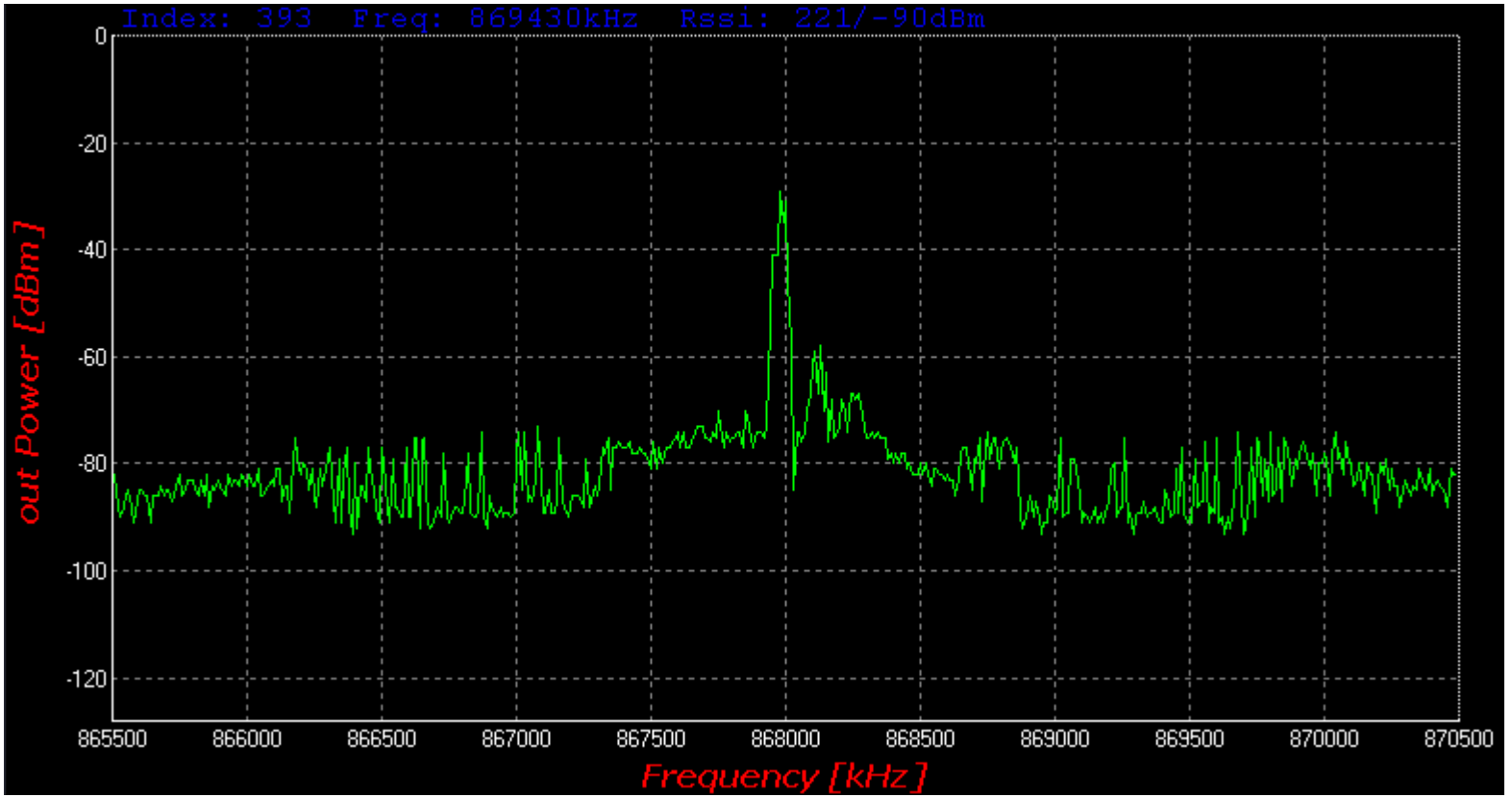
+



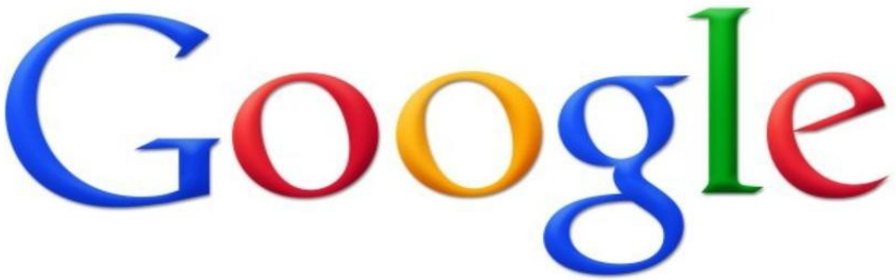
RF Engineering 101

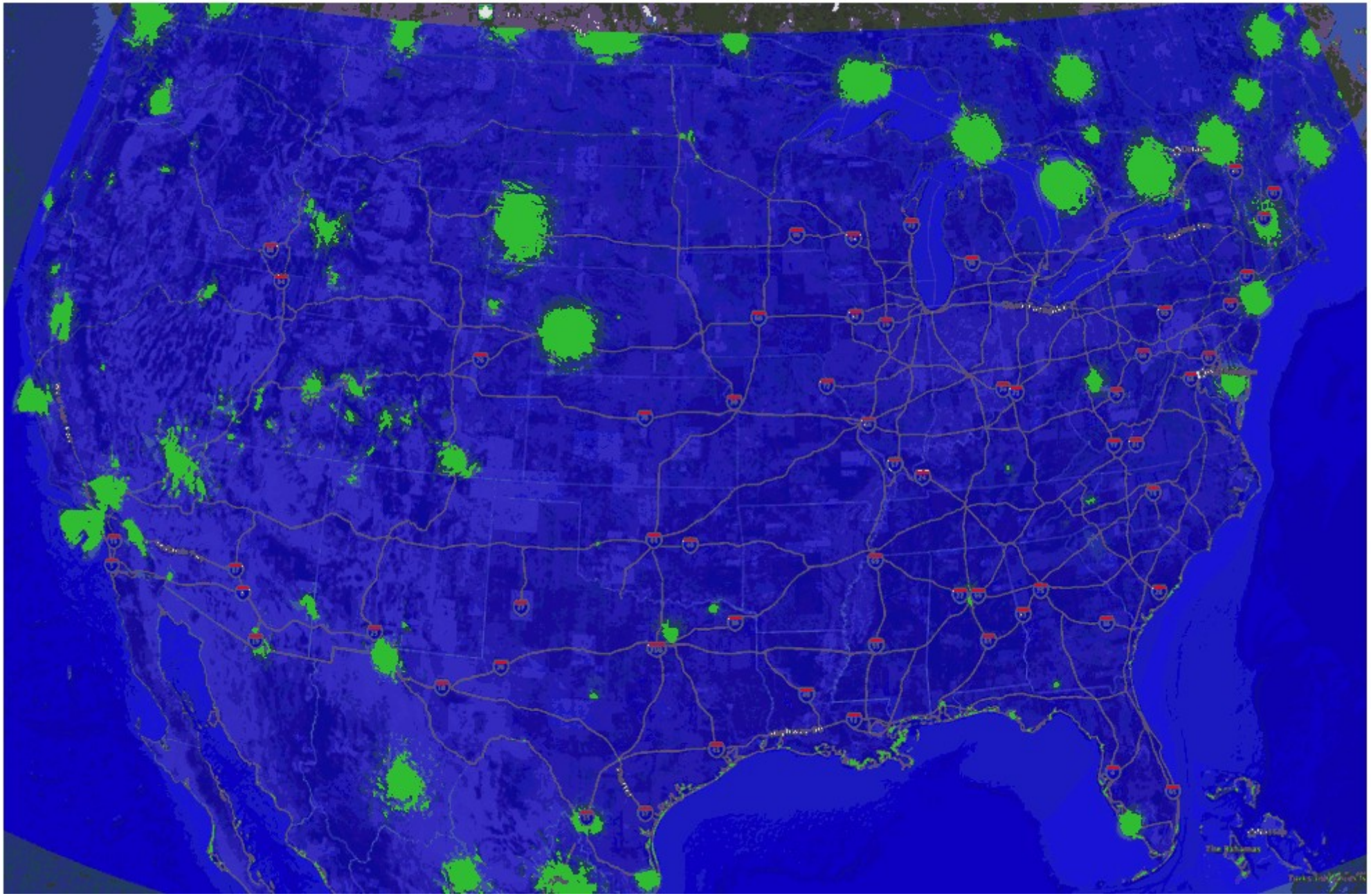
$$A_c \cos(2\pi f_c t + \phi)$$

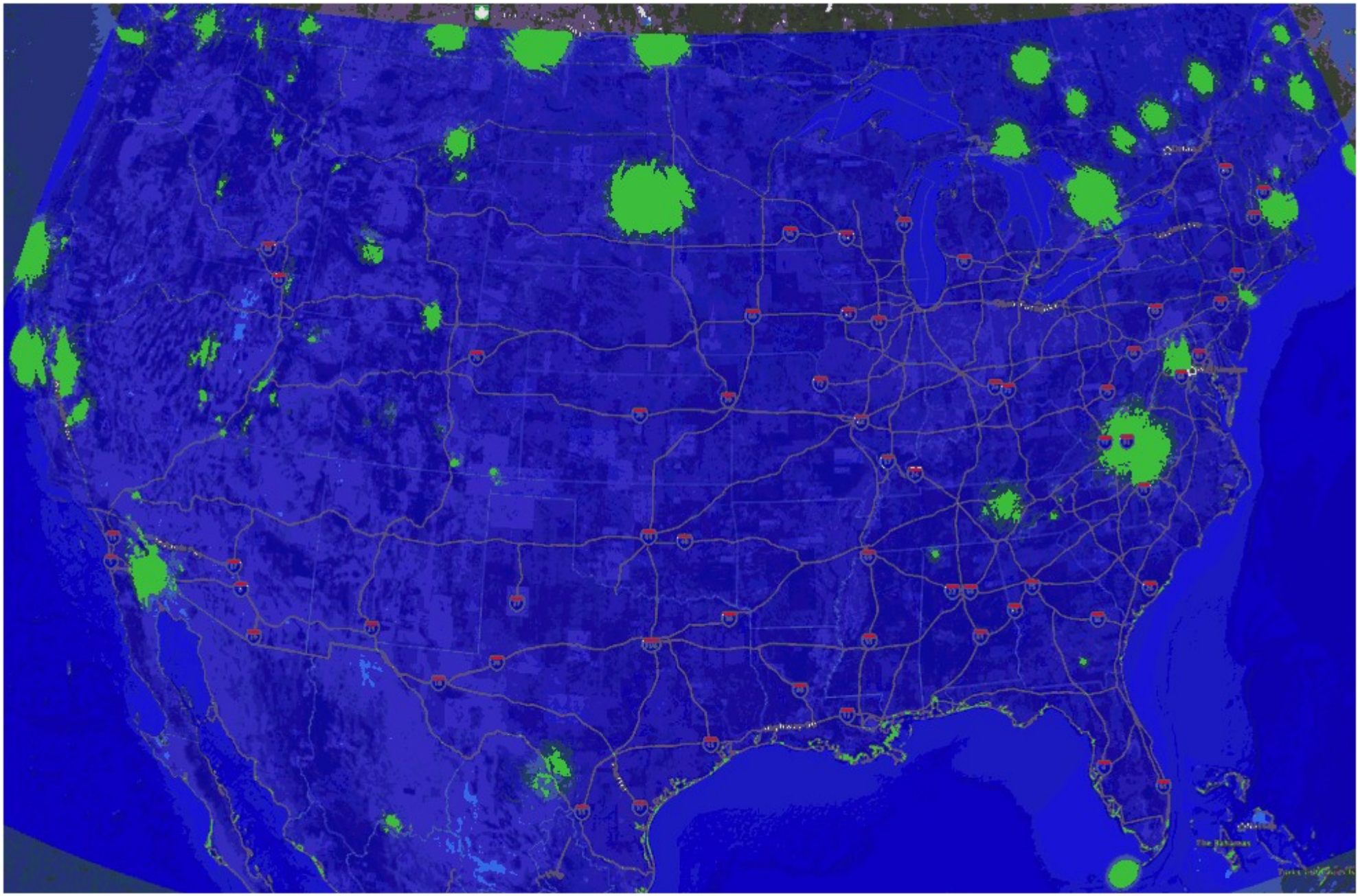



Index: 393 Freq: 869430kHz Rssi: 221/-90dBm
0
-20
-40
-60
-80
-100
-120
out Power [dBm]
865500
866000
866500
867000
867500
868000
868500
869000
869500
870000
870500
Frequency [kHz]

TV Whitespace

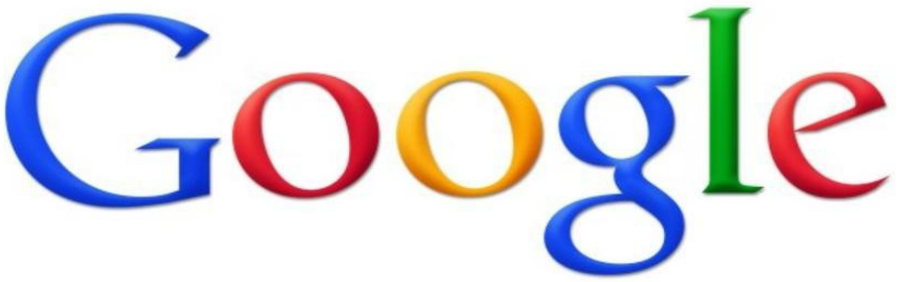

Google






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..

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.

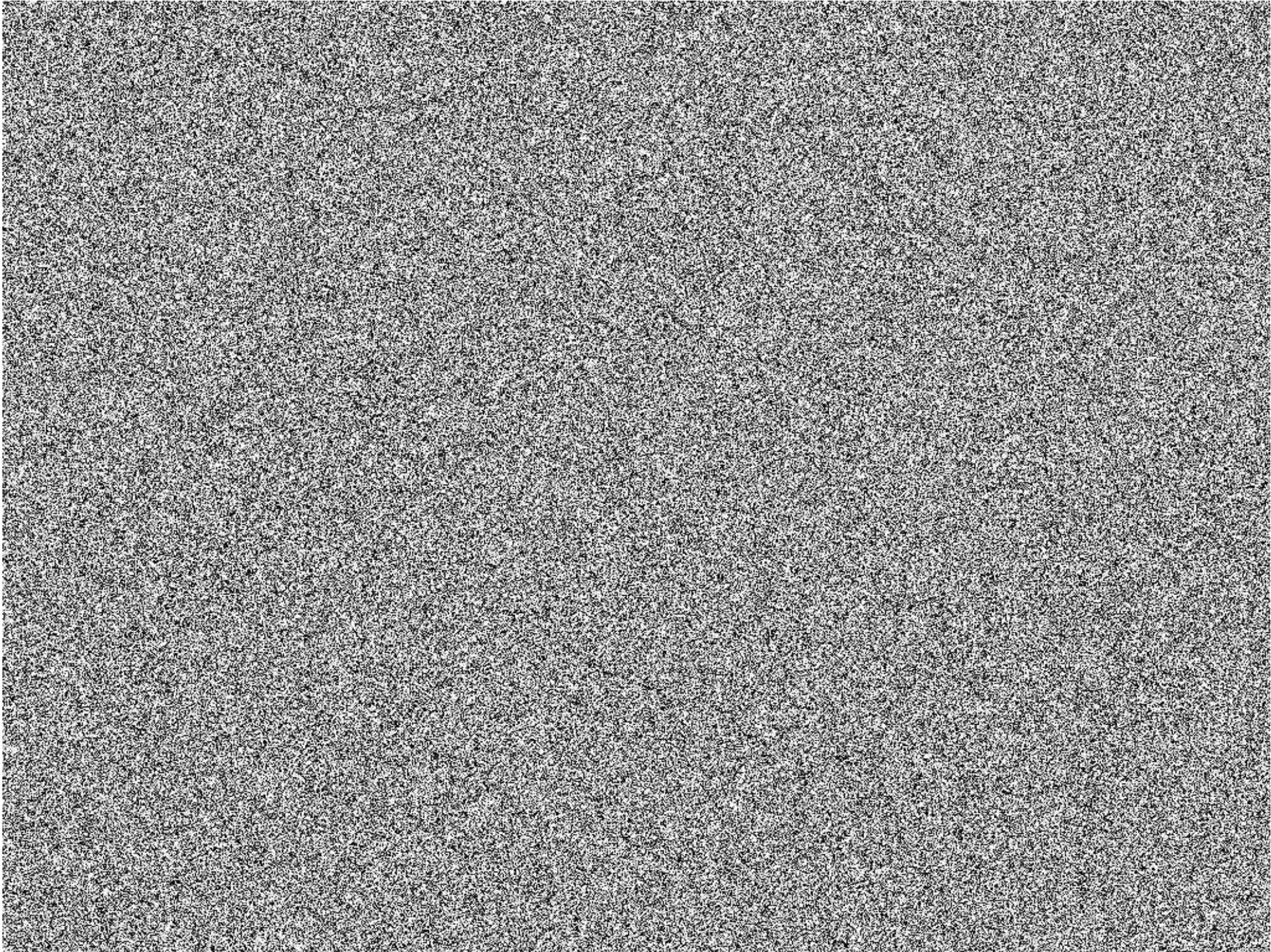
GBP£6,500 p.a.
for companies with an annual turnover of greater than GBP£1m p.a..

Let's break it.

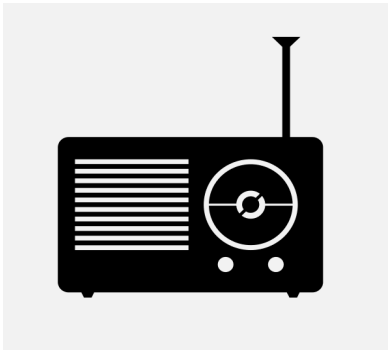
Change (or appear to change) the spectrum to force certain decisions

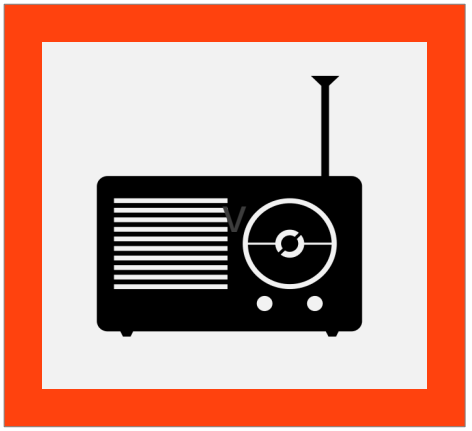
Selfish Attack

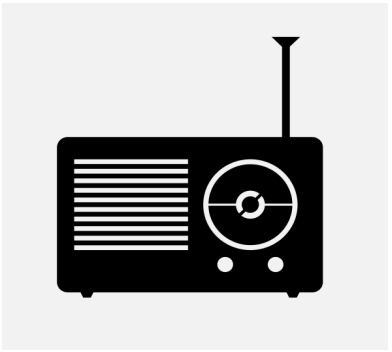
DOS

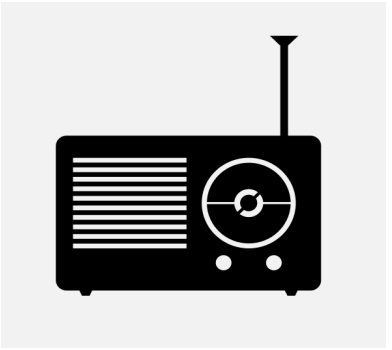


Secondary User Emulation

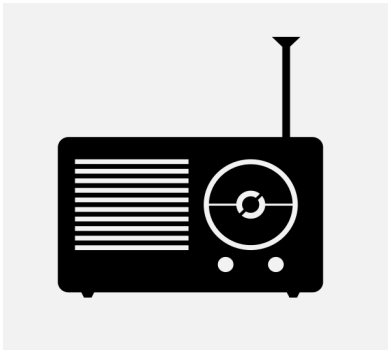


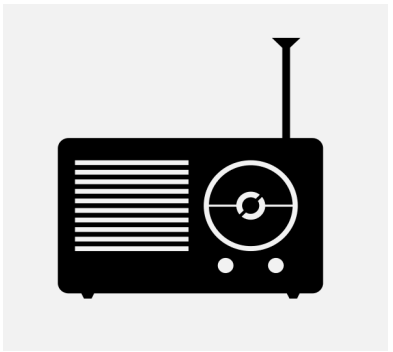


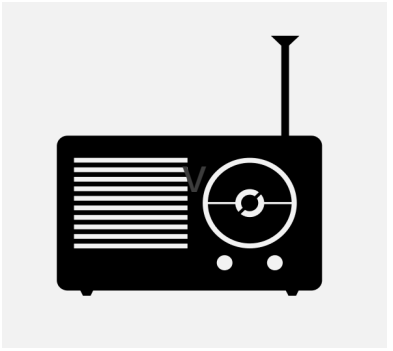


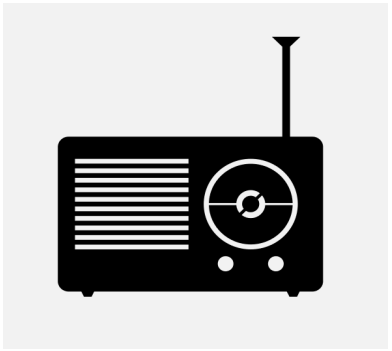


Primary User Emulation

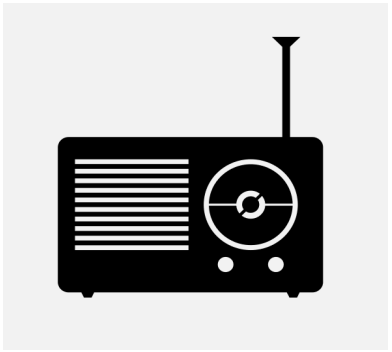


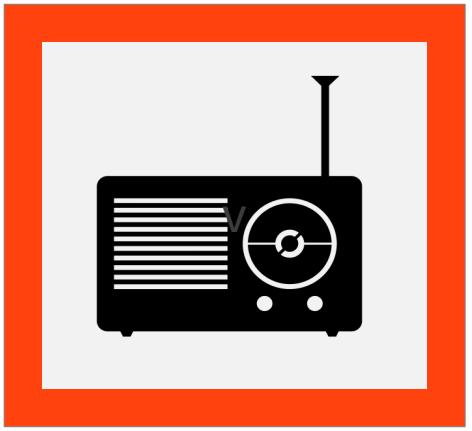


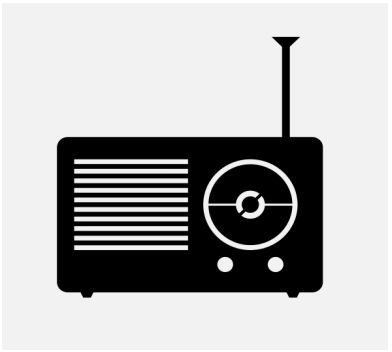


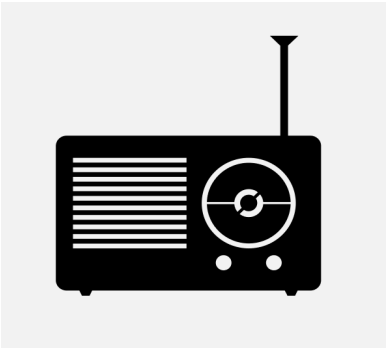


Misbehave Attack

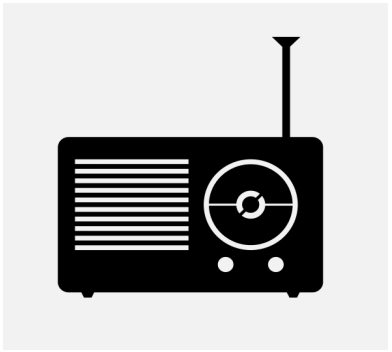


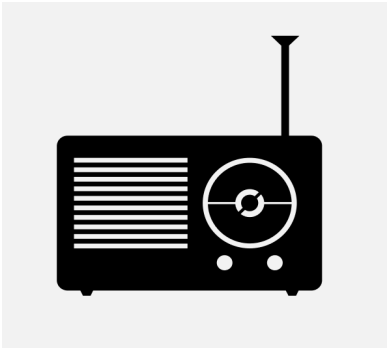


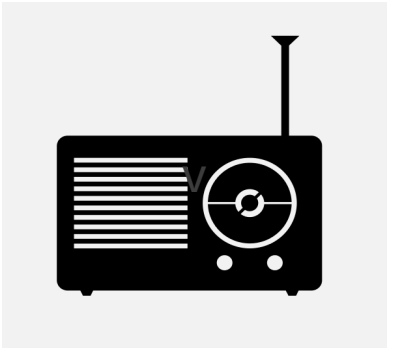


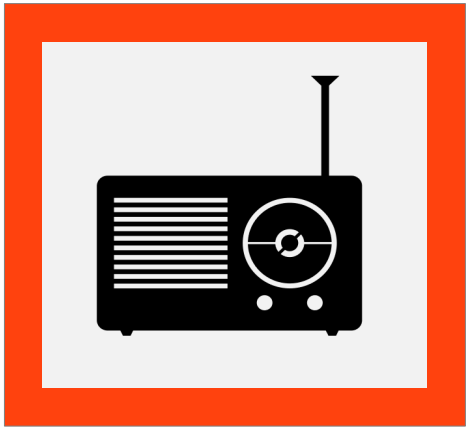


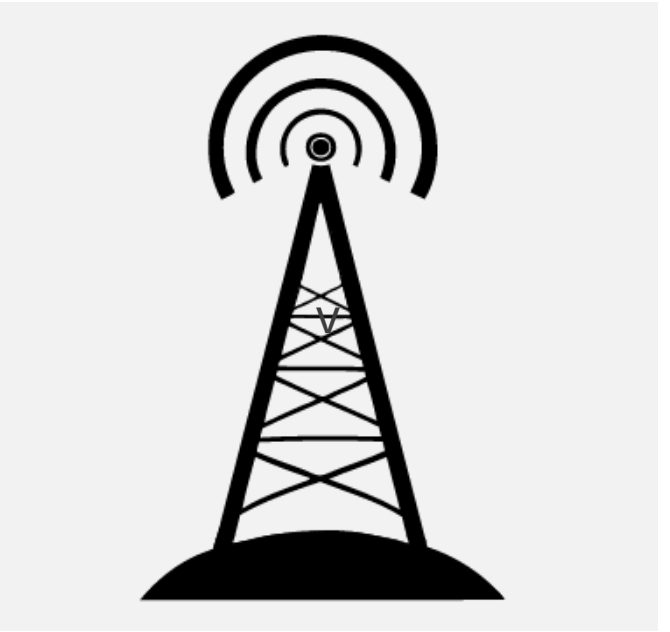
Asynchronous Sensing



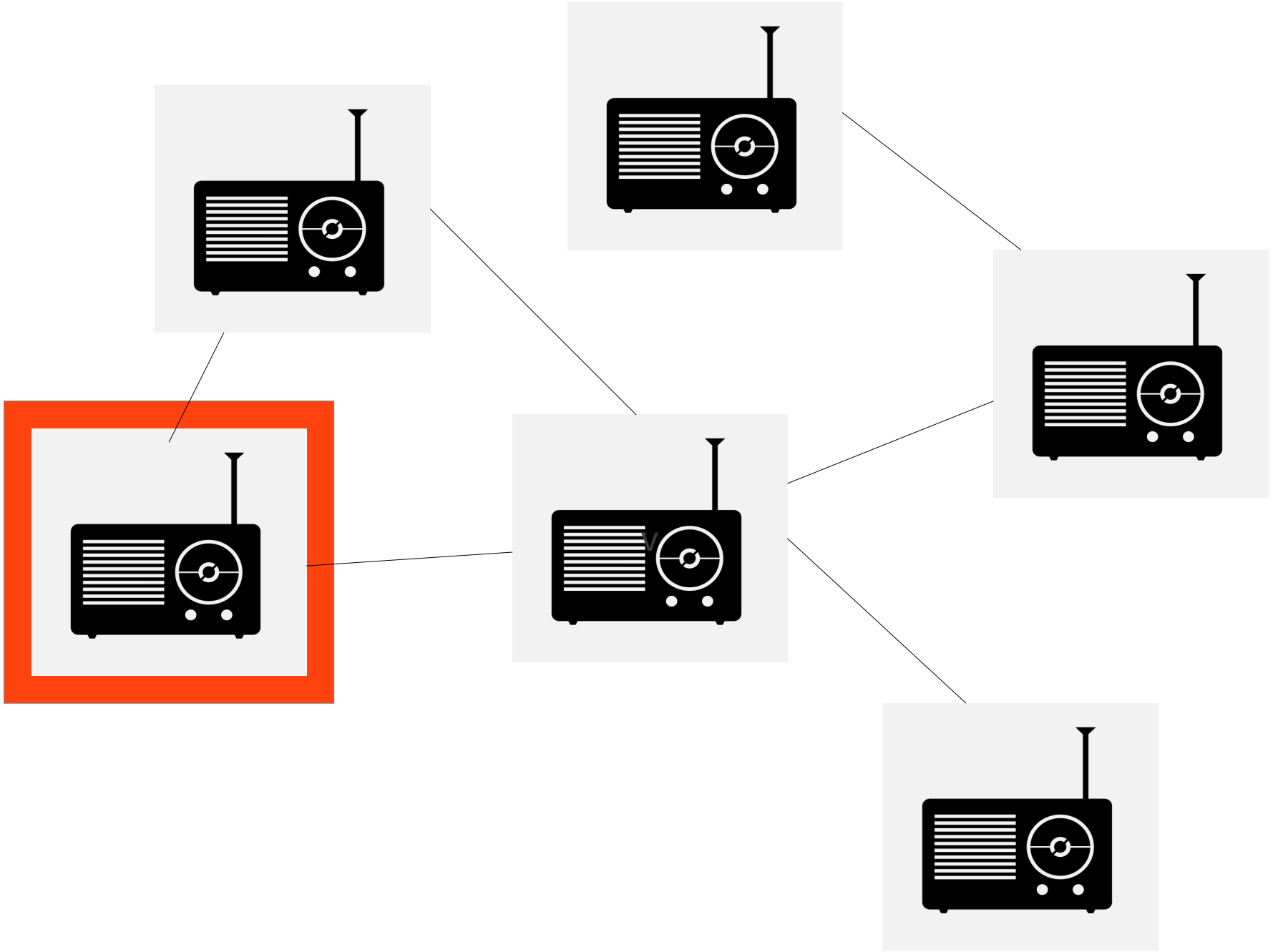




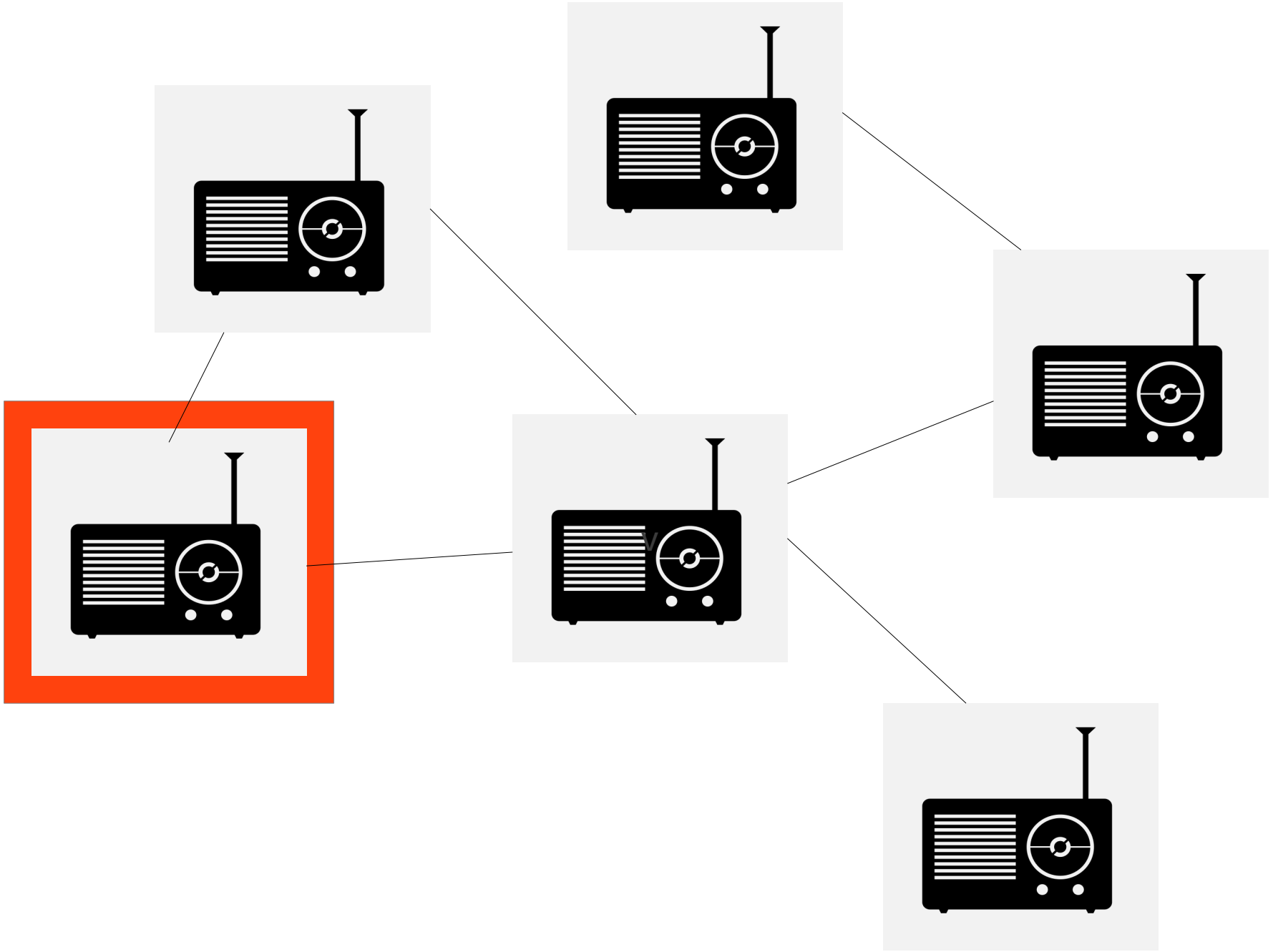




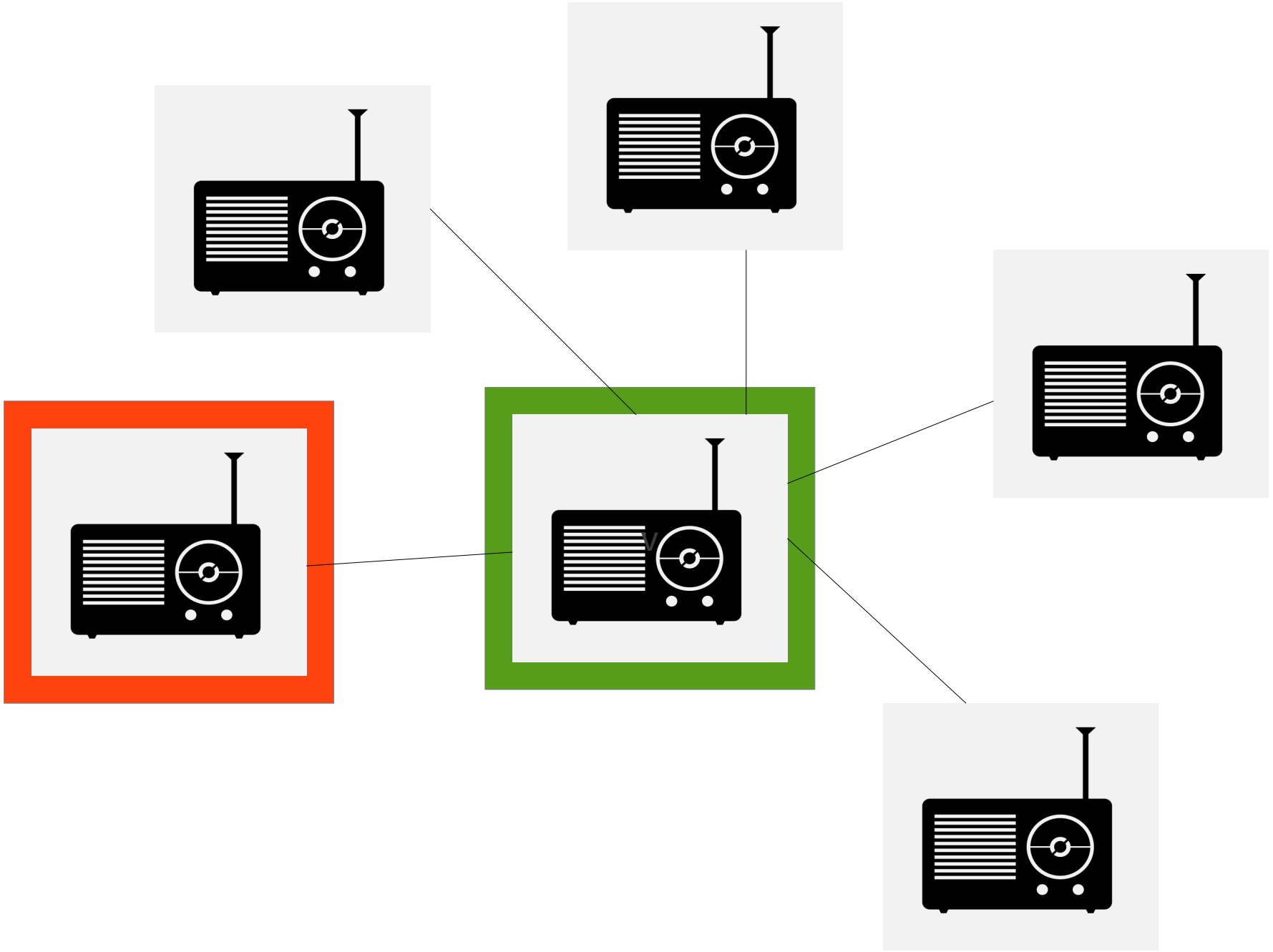
Network Endoparasite



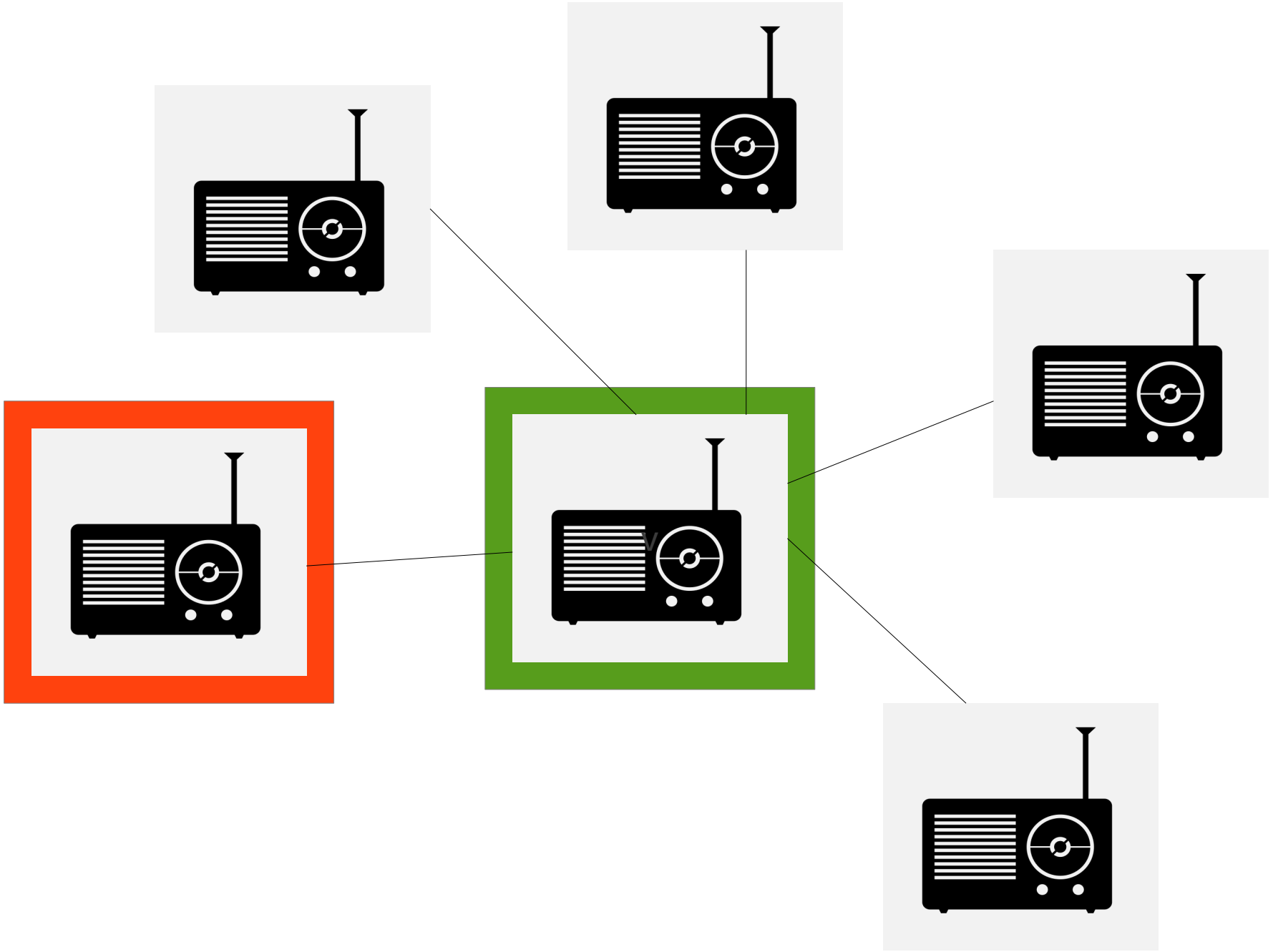
Network Ectoparasite



Fabrication



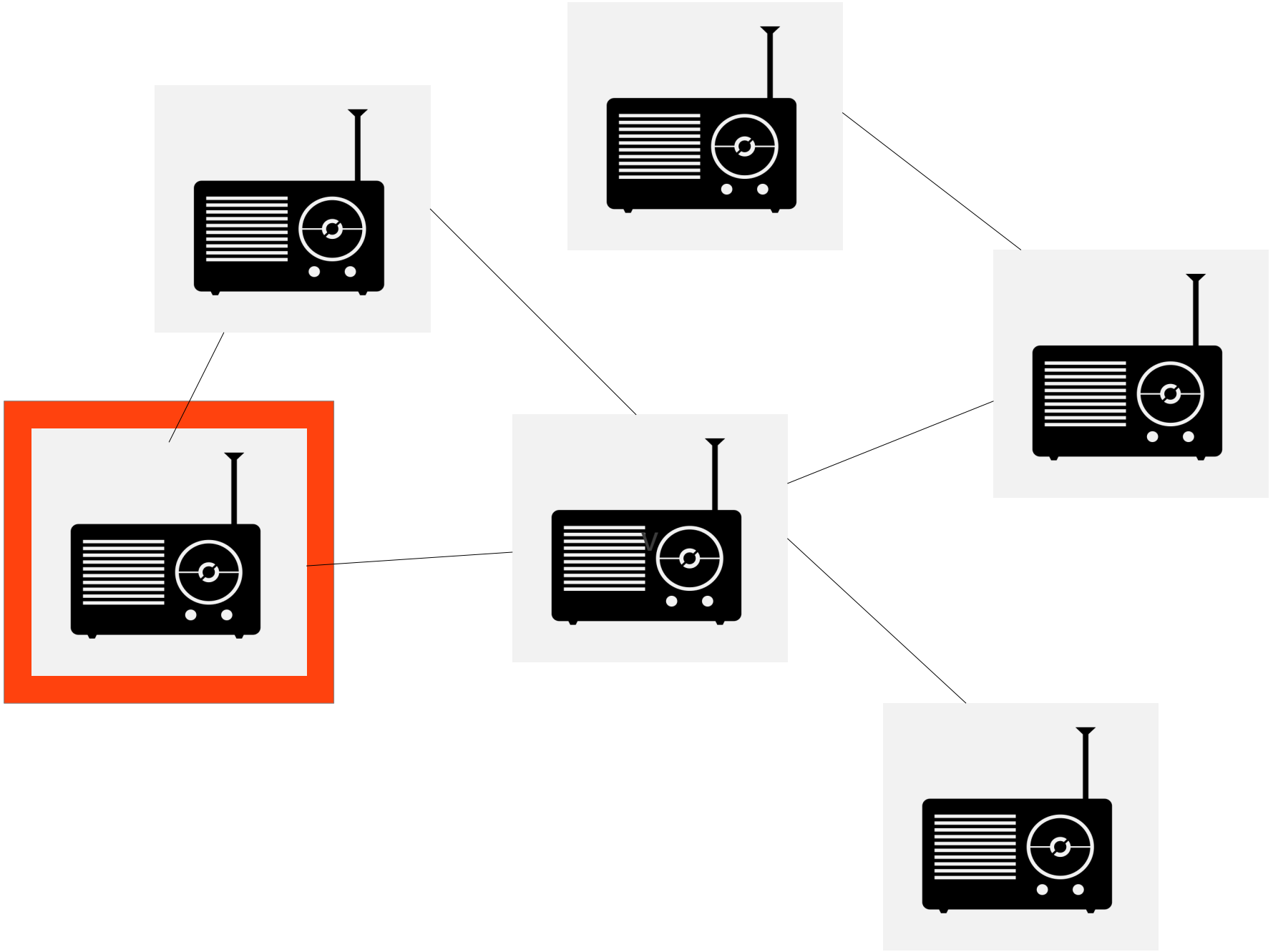
On-Off



Countermeasures

Authenticate devices on the network

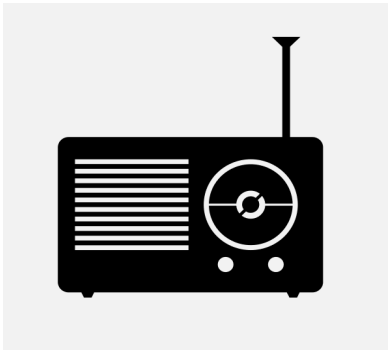
Cooperative Intrusion Detection

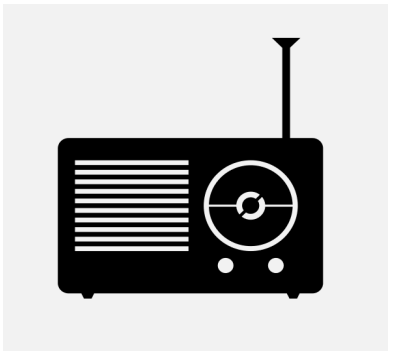


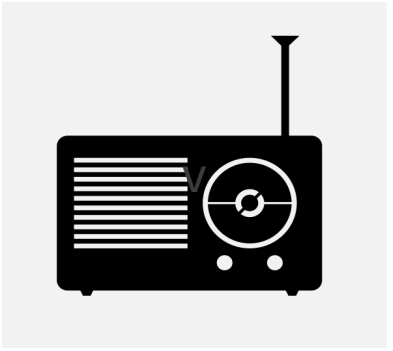
Device Reputation

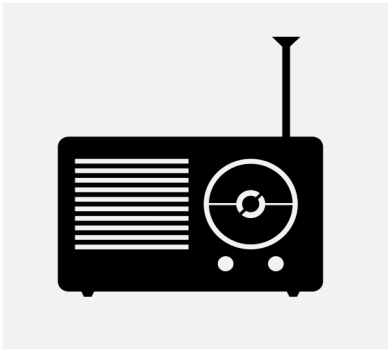
Device Location

Primary User Emulation

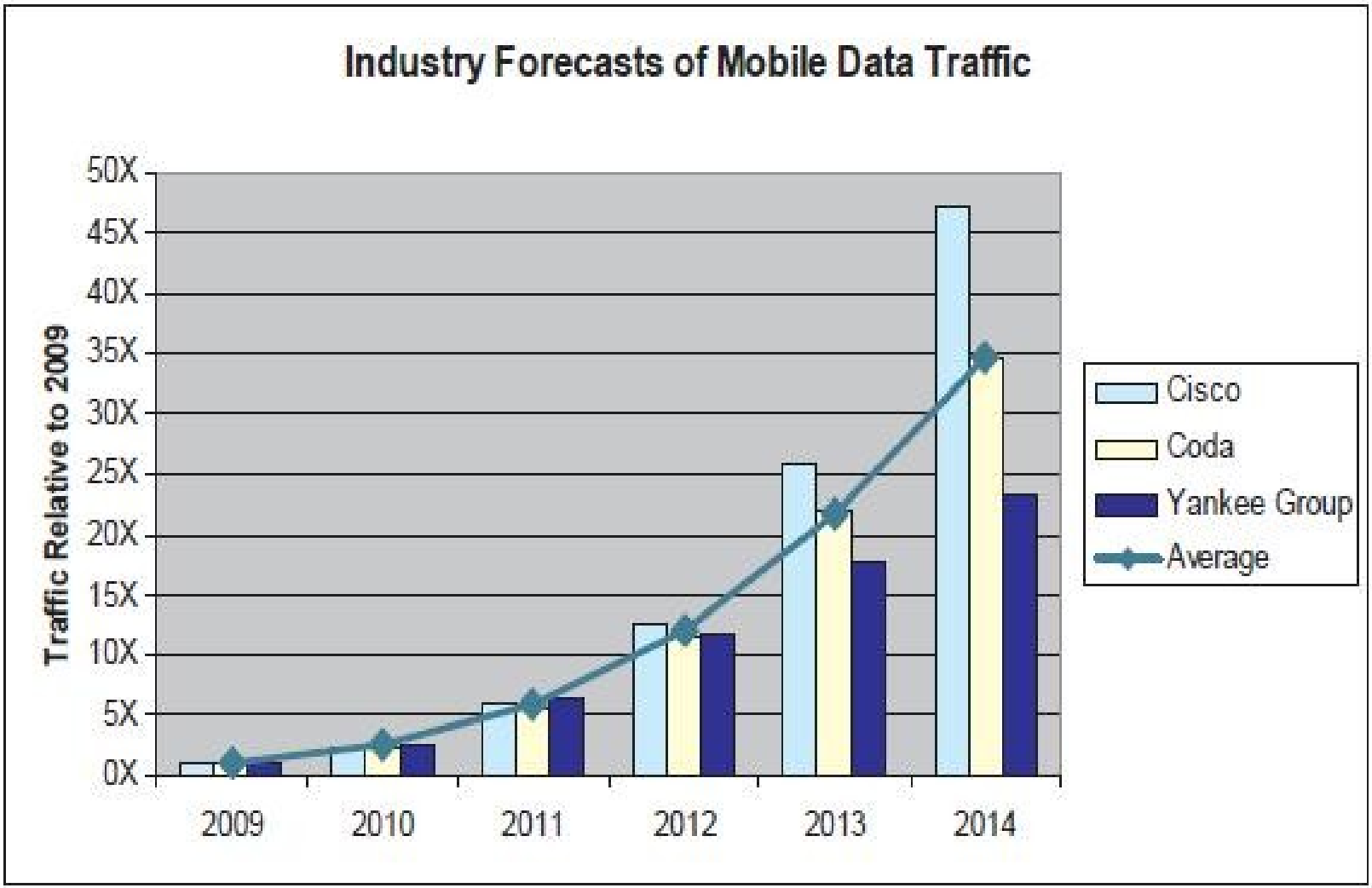








Why this matters


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

UNITED STATES FREQUENCY ALLOCATIONS

THE RADIO SPECTRUM

RADIO SERVICES COLOR LEGEND

- AERONAUTICAL MOBILE
- AERONAUTICAL MOBILE SATELLITE
- AERONAUTICAL RADIONAVIGATION
- AMATEUR
- AMATEUR SATELLITE
- BROADCASTING
- BROADCASTING SATELLITE
- EARTH EXPLORATION SATELLITE
- FIXED
- FIXED SATELLITE
- INTER-SATELLITE
- LAND MOBILE
- LAND MOBILE SATELLITE
- MARITIME MOBILE
- MARITIME MOBILE SATELLITE
- MARITIME RADIONAVIGATION
- METEOROLOGICAL AIDS
- METEOROLOGICAL SATELLITE
- MOBILE
- MOBILE SATELLITE
- RADIO ASTRONOMY
- RADIODETERMINATION SATELLITE
- RADIOLOCATION
- RADIOLOCATION SATELLITE
- RADIONAVIGATION
- RADIONAVIGATION SATELLITE
- SPACE OPERATION
- SPACE RESEARCH
- STANDARD FREQUENCY AND TIME SIGNAL
- STANDARD FREQUENCY AND TIME SIGNAL SATELLITE

ACTIVITY CODE

- GOVERNMENT EXCLUSIVE
- GOVERNMENT/ NON-GOVERNMENT SHARED
- NON-GOVERNMENT EXCLUSIVE

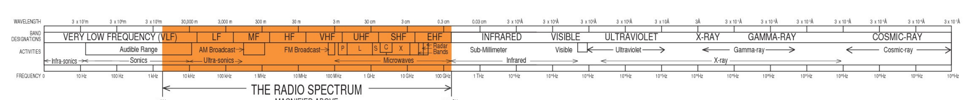
ALLOCATION USAGE DESIGNATION

SERVICE	EXAMPLE	DESCRIPTION
Primary	FIXED	Capital Letters
Secondary	Mobile	1st Capital with lower case letters

This chart is a graphic single-point-in-time portrayal of the Table of Frequency Allocations used by the FCC and NTIA. As such, it does not completely reflect all aspects, i.e., footnotes and recent changes made to the Table of Frequency Allocations. Therefore, for complete information, users should consult the Table to determine the current status of U.S. allocations.

* EXCEPT AERO MOBILE (R)

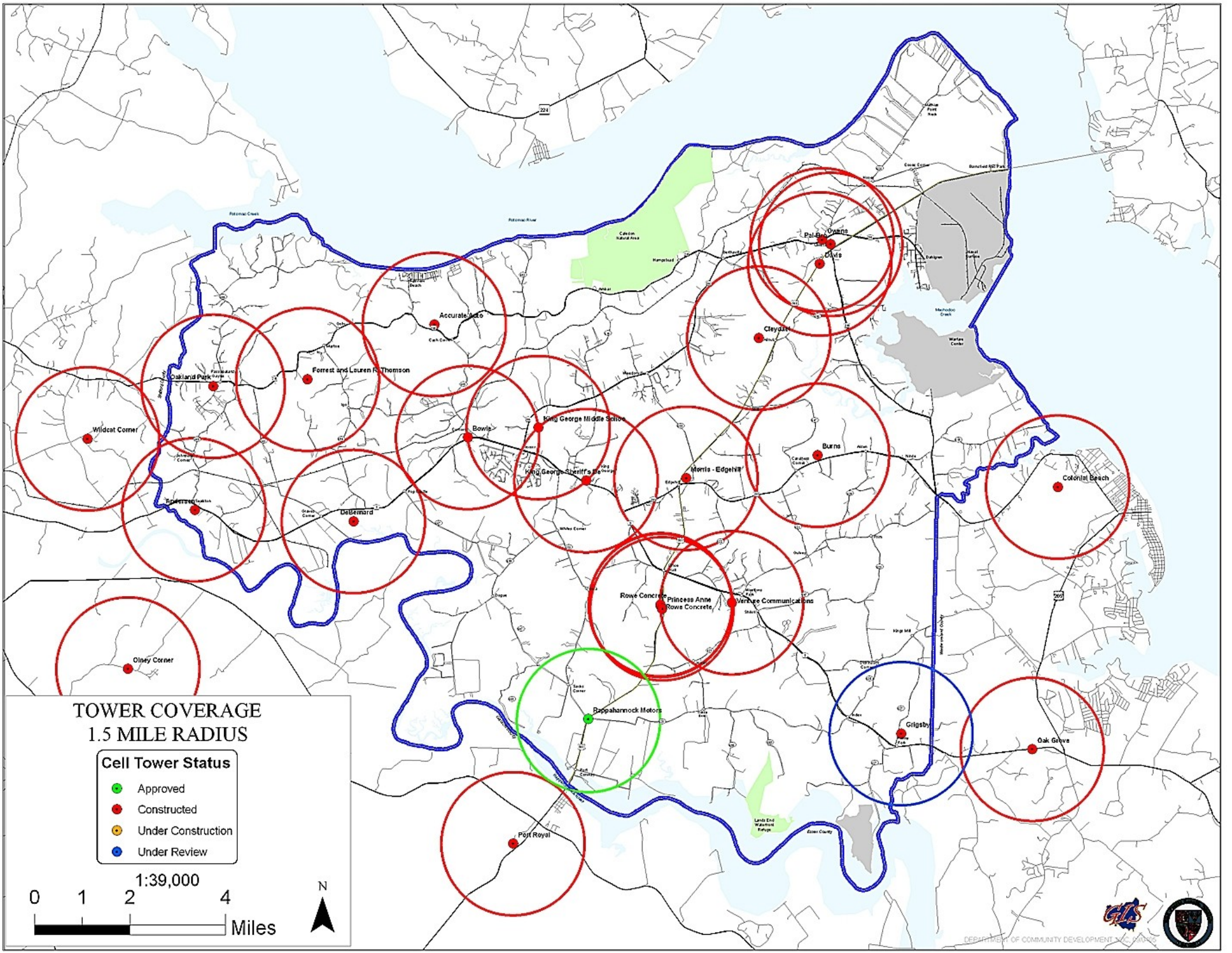
** EXCEPT AERO MOBILE



PLEASE NOTE: THE SPACING ALLOTTED THE SERVICES IN THE SPECTRUM SEGMENTS SHOWN IS NOT PROPORTIONAL TO THE ACTUAL AMOUNT OF SPECTRUM OCCUPIED.

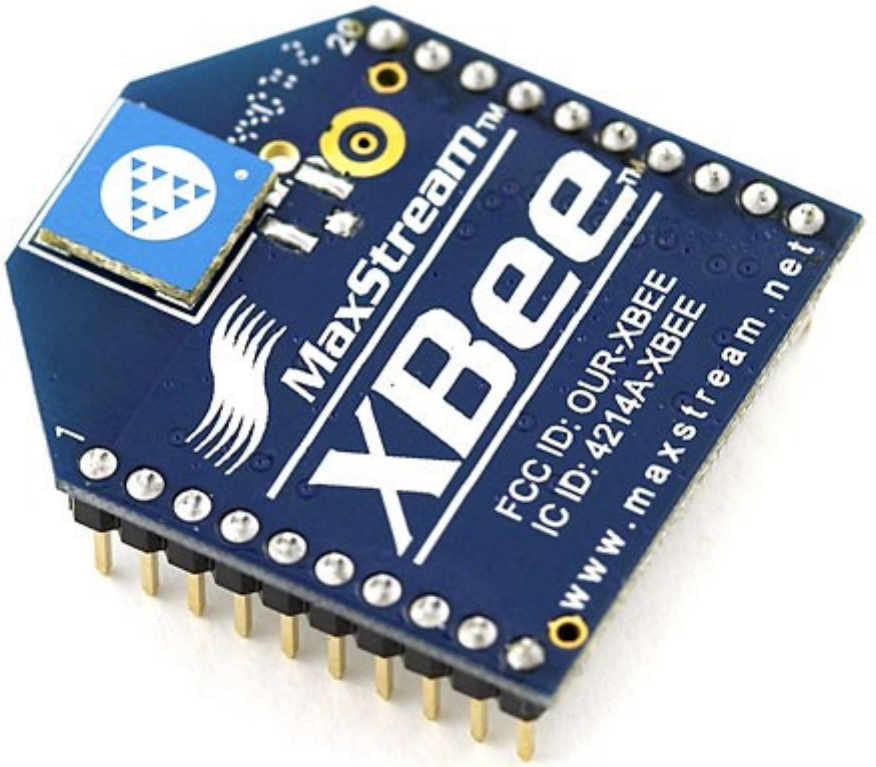
U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Office of Spectrum Management

October 2003

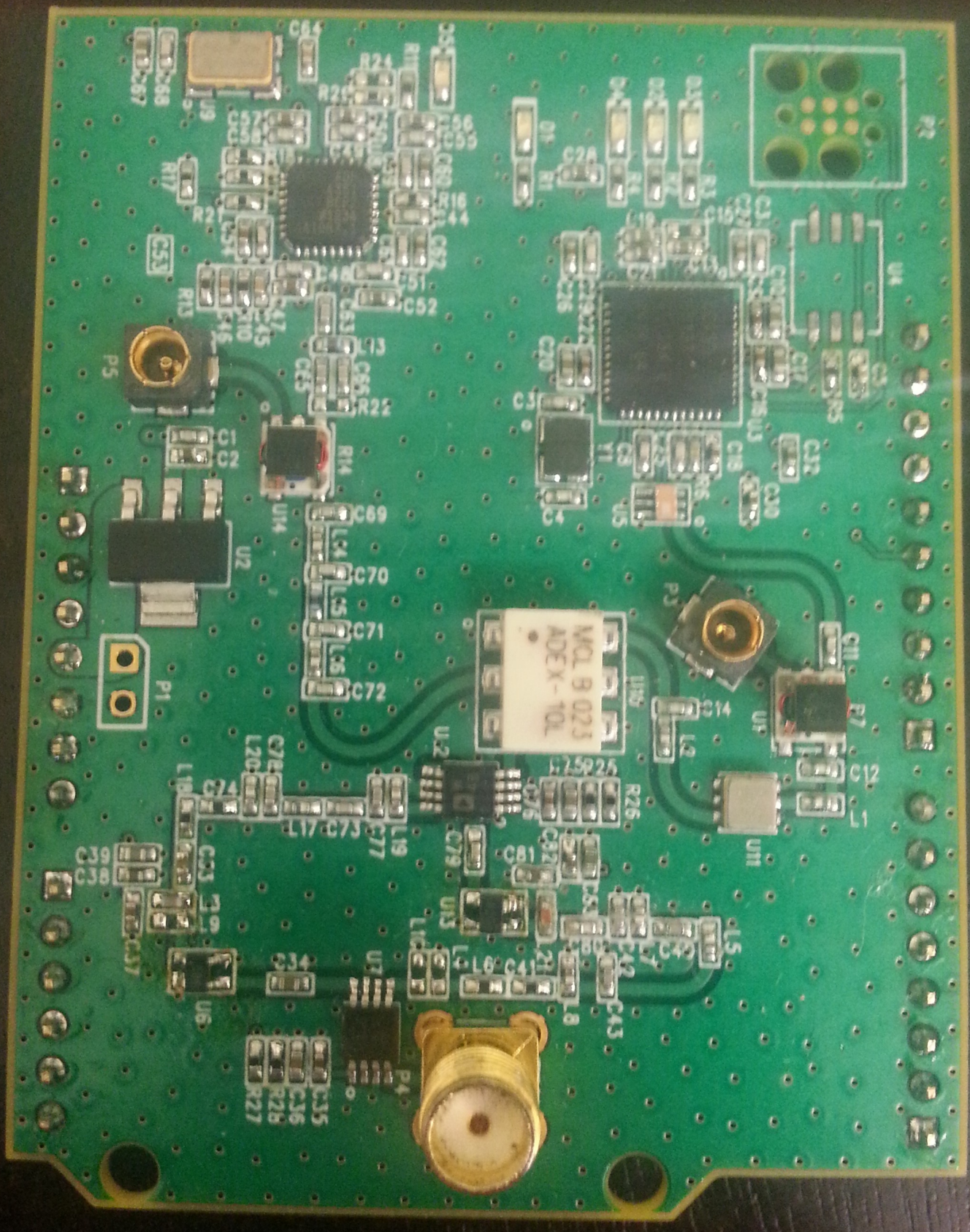

TOWER COVERAGE
1.5 MILE RADIUS
Cell Tower Status
Approved
Constructed
Under Construction
Under Review
1:39,000
0 1 2 4
Miles
N
Accurate Auto
Forrest and Lauren R. Thomson
Oakland Park
Wildcat Corner
Bowie
King George Middle School
King George Sheriff's Office
DeBernard
Olney Corner
Port Royal
Claydan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

Tools


Ettus Research
USRP2
REF CLOCK
PPS IN
SD MEMORY
MIMO EXPANSION
GB ETHERNET
POWER
5V DC 3A


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

Introducing Level...


MCL B 023
ADEX-10L

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

Other tools:

HackRF by Micheal Ossman

MyriadRF

What's next