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

Hunter Scott / August 3, 2013
Software Defined Radio

```c
// 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);
}
```
Cognitive Radio
Cognitive Engine
<table>
<thead>
<tr>
<th>Center Frequency</th>
<th>Coding rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth</td>
<td>Channel access protocol</td>
</tr>
<tr>
<td>Transmit power</td>
<td>Encryption algorithm</td>
</tr>
<tr>
<td>Type of modulation</td>
<td>Frame size</td>
</tr>
</tbody>
</table>
**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.
Fee: 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

Incumbent on channel 6
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
Priority Attack
Attacks on Crypto
Attacks on Data Privacy
Primary User Emulation
Primary User Emulation
Primary User Emulation

Primary user on channel 4

Primary user on channel 4

Primary user on channel 4

Primary user on channel 4
Primary User Emulation

Primary user on channel 4
Primary User Emulation

Recalculating...
Countermeasures
Cooperative Intrusion Detection
Device Reputation
Device Location
Why this matters
Industry Forecasts of Mobile Data Traffic

Traffic Relative to 2009

- Cisco
- Coda
- Yankee Group
- Average

Tools
Level

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


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