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_ETHETYPE;
    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
    dsmsm_start(&dsp_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
$A_c \cos(2\pi f_c t + \phi)$
TV Whitespace
### 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

- Cisco
- Coda
- Yankee Group
- Average

Tools
Introducing Level...
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