mapping wifi networks and triggering on interesting traffic patterns

Caleb Madrigal
Website: http://calebmadrigal.com/
Twitter: @caleb_madrigal
Ham call sign: w0hak
I like fuzzy things
I was into "IoT" before I knew it was called IoT

(http://calebmadrigal.com/raspberry-pi-home-security-system/)
Wireless hacking is really interesting
OSI Layer 4/3 (TCP/IP packets): Fun stuff, but less fun with ssl
OSI Layer 1 (802.11 modulation): Suddenly accessible with SDR
OSI Layer 2 (802.11 data frames): Data link - Less fun with good, ubiquitous wireless encryption (boring ! ?)
802.11 - Data Link Layer (OSI layer 2) data

- Explicit data in data frames
  - Source MAC
  - Destination MAC
  - Network SSID and BSSID (MAC)
  - Frame type (management, data, etc)
  - Encrypted data :(
802.11 - Data Link Layer (OSI layer 2) data

- Explicit data in data frames
  - Source MAC
  - Destination MAC
  - Network SSID and BSSID (MAC)
  - Frame type (management, data, etc)
  - Encrypted data

- Inferred data
  - Power level
  - Time
  - Manufacturer (via IEEE OUI)
  - Network/SSID (not always present, but inferable from history)
I had a problem...
I'VE GOT A FEVER

AND THE ONLY PRESCRIPTION IS MORE PYTHON
the solution?

trackerjacker
trackerjacker

- [https://github.com/calebmadrigal/trackerjacker](https://github.com/calebmadrigal/trackerjacker)
- [https://pypi.python.org/pypi/trackerjacker](https://pypi.python.org/pypi/trackerjacker)
- Install: `pip3 install trackerjacker`
Demo 1: Inferring Wireless Camera Motion Detection

- Video
Demo 2: Tracking smartphones

- `trackerjacker --track -m 3c:2e:ff:25:30:61 --log-level=DEBUG --channel-switch-scheme=round_robin`
Demo 3: Mapping

- trackerjacker --map
How wifi works (from a radio perspective)
### 2.4 GHz Channels

<table>
<thead>
<tr>
<th>CHANNEL NUMBER</th>
<th>LOWER FREQUENCY MHZ</th>
<th>CENTER FREQUENCY MHZ</th>
<th>UPPER FREQUENCY MHZ</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2401</td>
<td>2412</td>
<td>2423</td>
</tr>
<tr>
<td>2</td>
<td>2406</td>
<td>2417</td>
<td>2428</td>
</tr>
<tr>
<td>3</td>
<td>2411</td>
<td>2422</td>
<td>2433</td>
</tr>
<tr>
<td>4</td>
<td>2416</td>
<td>2427</td>
<td>2438</td>
</tr>
<tr>
<td>5</td>
<td>2421</td>
<td>2432</td>
<td>2443</td>
</tr>
<tr>
<td>6</td>
<td>2426</td>
<td>2437</td>
<td>2448</td>
</tr>
<tr>
<td>7</td>
<td>2431</td>
<td>2442</td>
<td>2453</td>
</tr>
<tr>
<td>8</td>
<td>2436</td>
<td>2447</td>
<td>2458</td>
</tr>
<tr>
<td>9</td>
<td>2441</td>
<td>2452</td>
<td>2463</td>
</tr>
<tr>
<td>10</td>
<td>2446</td>
<td>2457</td>
<td>2468</td>
</tr>
<tr>
<td>11</td>
<td>2451</td>
<td>2462</td>
<td>2473</td>
</tr>
<tr>
<td>12</td>
<td>2456</td>
<td>2467</td>
<td>2478</td>
</tr>
<tr>
<td>13</td>
<td>2461</td>
<td>2472</td>
<td>2483</td>
</tr>
<tr>
<td>14</td>
<td>2473</td>
<td>2484</td>
<td>2495</td>
</tr>
</tbody>
</table>
## 5 GHz Channels

<table>
<thead>
<tr>
<th>CHANNEL NUMBER</th>
<th>FREQUENCY MHZ</th>
</tr>
</thead>
<tbody>
<tr>
<td>36</td>
<td>5180</td>
</tr>
<tr>
<td>40</td>
<td>5200</td>
</tr>
<tr>
<td>44</td>
<td>5220</td>
</tr>
<tr>
<td>48</td>
<td>5240</td>
</tr>
<tr>
<td>52</td>
<td>5260</td>
</tr>
<tr>
<td>56</td>
<td>5280</td>
</tr>
<tr>
<td>60</td>
<td>5300</td>
</tr>
<tr>
<td>64</td>
<td>5320</td>
</tr>
<tr>
<td>100</td>
<td>5500</td>
</tr>
<tr>
<td>104</td>
<td>5520</td>
</tr>
<tr>
<td>108</td>
<td>5540</td>
</tr>
<tr>
<td>112</td>
<td>5560</td>
</tr>
<tr>
<td>116</td>
<td>5580</td>
</tr>
<tr>
<td>120</td>
<td>5600</td>
</tr>
<tr>
<td>124</td>
<td>5620</td>
</tr>
<tr>
<td>128</td>
<td>5640</td>
</tr>
<tr>
<td>132</td>
<td>5660</td>
</tr>
<tr>
<td>136</td>
<td>5680</td>
</tr>
<tr>
<td>140</td>
<td>5700</td>
</tr>
<tr>
<td>149</td>
<td>5745</td>
</tr>
<tr>
<td>153</td>
<td>5765</td>
</tr>
<tr>
<td>157</td>
<td>5785</td>
</tr>
<tr>
<td>161</td>
<td>5805</td>
</tr>
<tr>
<td>165</td>
<td>5825</td>
</tr>
</tbody>
</table>
2.4 GHz (802.11b/g/n)

Channels 1, 6, 11

5 GHz (802.11a/n/ac)

Channels 36 to 64, 100 to 149, 149 to 166
Modulation

(http://calebmadrigal.com/digital-radio-signal-generation/, Note: this is a sample of ASK, whereas wireless typically uses FSK, PSK, or QAM)
Monitor vs Promiscuous mode
Promiscuous mode

SSID: Inksys

SSID: ATT993
Monitor mode

channel 1

channel 2

channel 3
Demo: foxhunt plugin

- trackerjacker --track --plugin foxhunt
- https://github.com/calebmadrigal/trackerjacker/blob/master/trackerjacker/plugins/foxhunt.py
Demo: deauth plugin

- trackerjacker --track --plugin plugin_examples/deauth_attack.py --plugin-config "{"vendor_to_deauth": ‘Apple’}"  
- https://github.com/calebmadrigal/trackerjacker/blob/master/plugin_examples/deauth_attack.py
Demo: example plugin

- trackerjacker --track --plugin plugin_examples/count_apples.py
- https://github.com/calebmadrigal/trackerjacker/blob/master/plugin_examples/count_apples.py
Environment

Recommendations

- Linux in a VM
  - I’ve also tested on Ubuntu
  - I’ve also tested in a Raspberry Pi
- An external wireless adapter
  - Especially if running in a VM
- macOS support is pre-alpha
  - (Don’t bother reporting any bugs encountered in macOS)
Wireless Adapters

- Panda PAU07 N600 Dual Band (nice, small, 2.4GHz and 5GHz)
- Panda PAU09 N600 Dual Band (higher power, 2.4GHz and 5GHz)
- Alfa AWUS052NH Dual-Band 2x 5dBi (high power, 2.4GHz and 5GHz, large, ugly)
- TP-Link N150 (works well, but not dual band)
Take-away

- At the physical layer, wifi is just radio
- It is trivial to track Wifi devices with monitor mode
- Interesting information can be obtained just from the raw, encrypted 802.11 packets
  - Good to keep in mind with IoT stuff
- New tool: trackerjacker
- How to not be tracked: turn off wifi when not using (or use MAC randomization)
Thanks!

Questions?

Caleb Madrigal
Website: http://calebmadrigal.com/
Twitter: @caleb_madrigal
Ham call sign: w0hak
https://github.com/calebmadrigal/trackerjacker