Virtualized Wireless Networking with WELLED

Adam Welle

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

DM18-1104

Virtualized Wireless Networking

Benefits

Implementation

Screenshots

Future Work

Benefits

Permit centralized, wireless exploitation training/evaluation on virtual machines (without transmission of radio frequencies):

- All virtual -- no real wireless devices (cost effective)
- Enable use inside secure facilities (flexible)
- Eliminate interference from other RF devices (repeatable)
- Function like real Linux wireless interfaces (realistic)

Implementation

- Linux hardware simulation driver – MAC80211_HWSIM
- User space application on host – WMASTERD
- User space application on host – WELLED
- User space application on host – GELLED

Implementation – MAC80211_HWSIM

- Linux hardware simulation driver:
  - Included in the Linux source tree (MAC80211_HWSIM)
  - Simulates one or more 802.11 radios on a single virtual machine
  - Provides wireless API to user space applications for the purpose of software testing
  - Transmits frames to user space applications on virtual machine via netlink

Implementation - WMASTERD

- User space application on host:
  - Wireless Master Daemon (WMASTERD)
  - Can apply signal strength modifications to frames
  - Transfers frames to all guest VMs running WELLED via VSOCK
  - Tracks latitude and longitude for each virtual machine
  - Generates NMEA data for GPS simulation

Implementation - WELLED

- User space application on virtual machines:
  - Wireless Emulation Link Layer Exchange Daemon (WELLED)
  - Receives frames from WMASTERD via VSOCK
  - Sends frames to MAC8011_HWSIM via netlink

Implementation - GELLED

- User space application on virtual machines:
  - GPS Emulation Link Layer Exchange Daemon (GELLED)
  - Receives NMEA sentences from WMASTERD via VSOCK
  - Writes NMEA sentences to a simulated serial device

Wireless Simulation for Wi-Fi and GPS – Functionality

Benefits

- Wireless training does not require the purchase of hardware
- Wireless training can be conducted inside secure facilities
- Wireless training can be predictable and repeatable

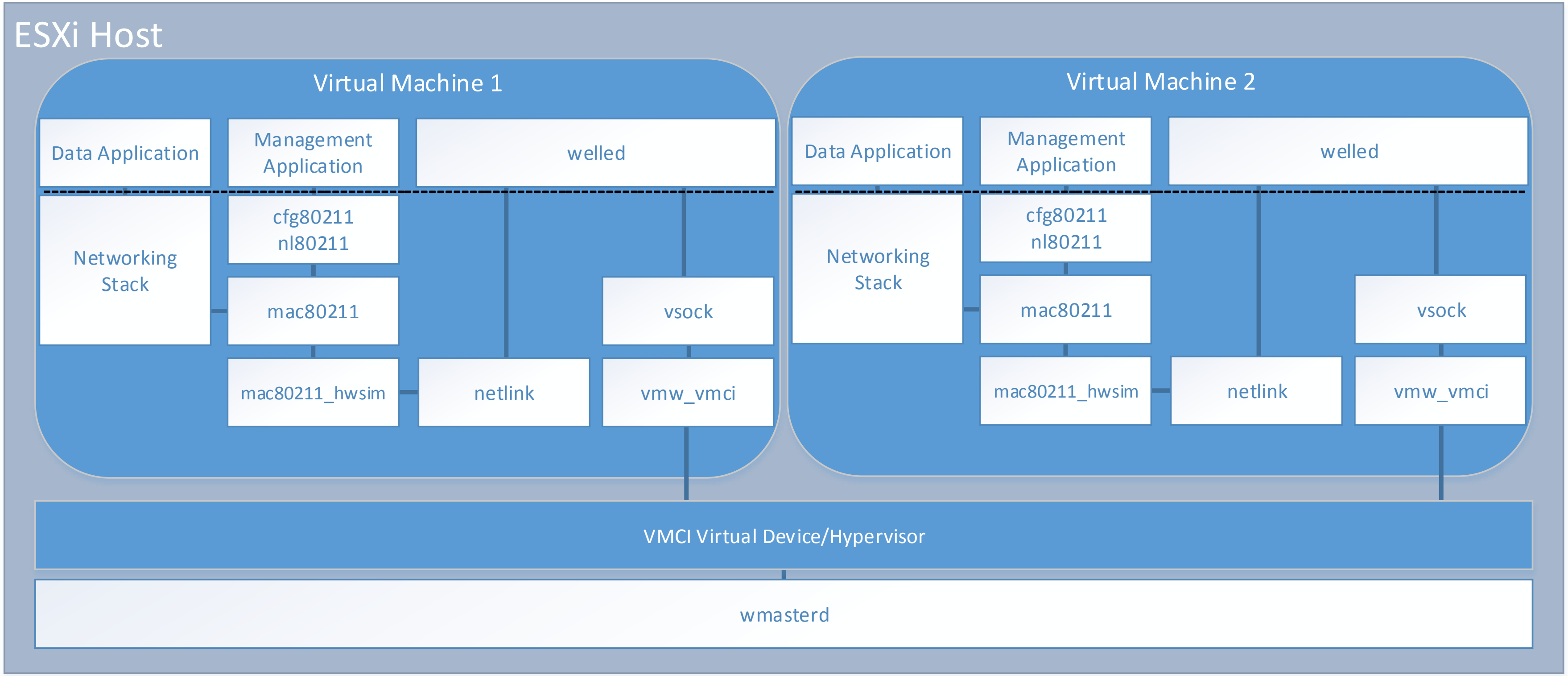
Wi-Fi Simulation with WELLED

- Standard tools such as hostpad, wpa_supplicant, and aircrack-ng can be used
- Enables the training of wireless penetration testing

GPS Simulation with GELLED

- Virtual machines can “move” throughout their virtual world
- Enables the simulation of vehicle control systems
- Enables the simulation of tracked mobile assets: convoys, ships, airplanes

Diagram


ESXi Host
Virtual Machine 1
Data Application
Management Application
welled
Networking Stack
cfg80211
nl80211
mac80211
vsock
mac80211_hwsim
netlink
vmw_vmci
Virtual Machine 2
Data Application
Management Application
welled
Networking Stack
cfg80211
nl80211
mac80211
vsock
mac80211_hwsim
netlink
vmw_vmci
VMCI Virtual Device/Hypervisor
wmasterd

Guest Operating Systems

Example applications used in training scenarios to date:

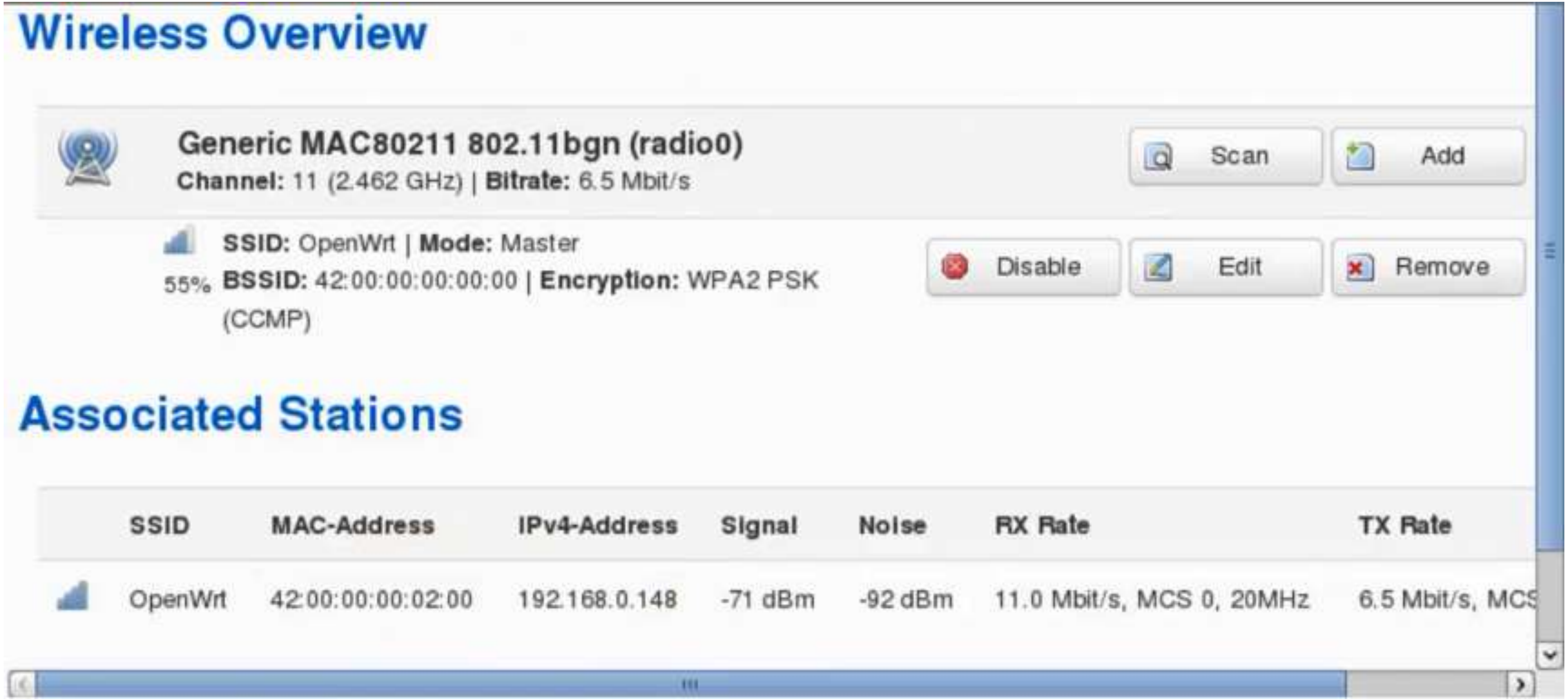
- Kali
  - kismet
  - aircrack-ng
  - gpsd
- OpenWrt
  - hostapd
- Ubuntu
  - wpa_supplicant
- Fedora
  - wpa_supplicant
  - gpsd
- android
  - wpa_supplicant

Host Operating Systems

Operating systems used to host virtual machines running wireless simulation:

- Windows
- ESXi

OpenWrt Access Point



Wireless Overview

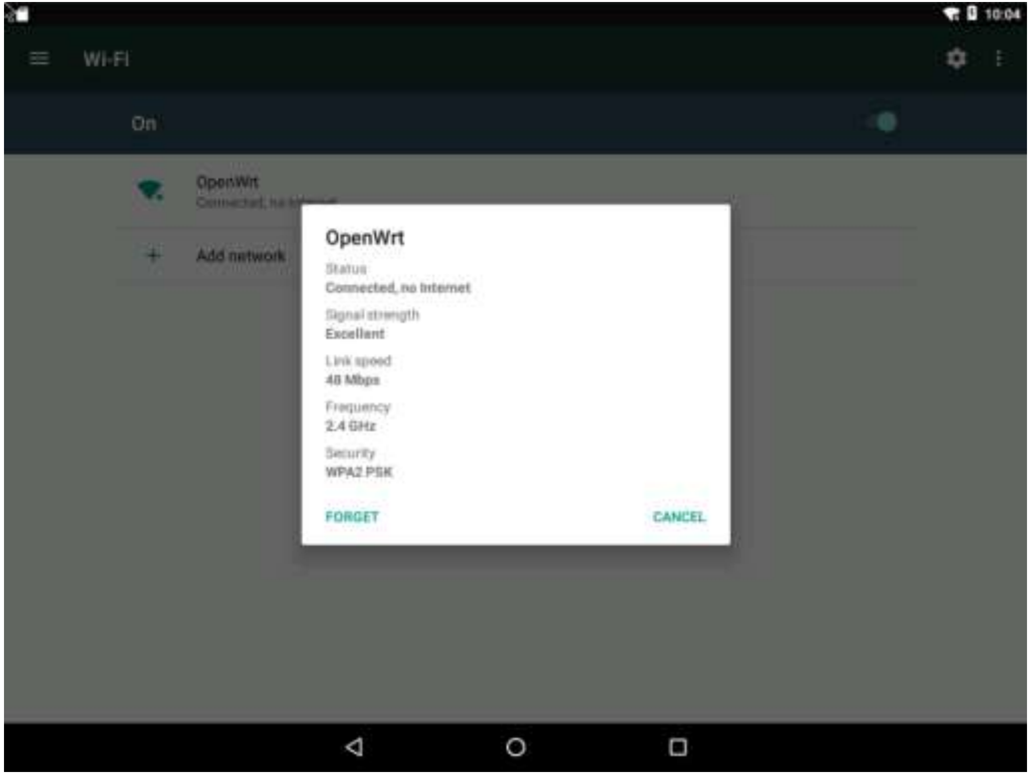
Generic MAC80211 802.11bgn (radio0)
Channel: 11 (2.462 GHz) | **Bitrate:** 6.5 Mbit/s

55% **SSID:** OpenWrt | **Mode:** Master
BSSID: 42:00:00:00:00:00 | **Encryption:** WPA2 PSK (CCMP)

Associated Stations

	SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
	OpenWrt	42:00:00:00:02:00	192.168.0.148	-71 dBm	-92 dBm	11.0 Mbit/s, MCS 0, 20MHz	6.5 Mbit/s, MCS

Android Client



OpenWrt

Status
Connected, no Internet

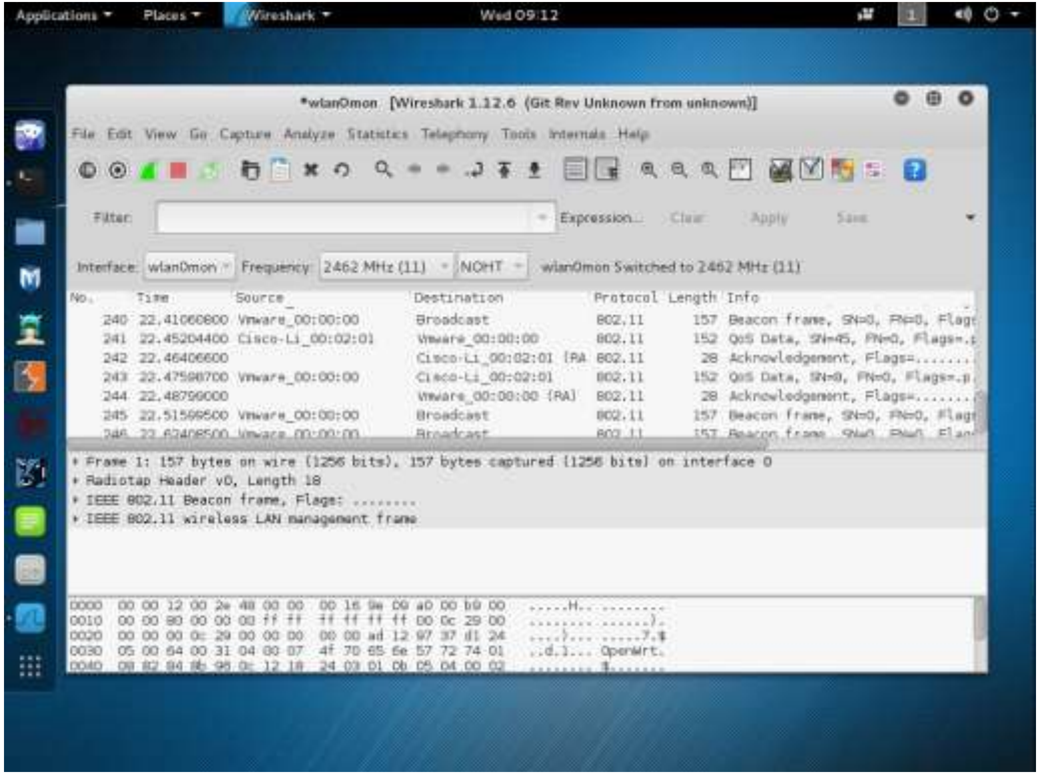
Signal strength
Excellent

Link speed
48 Mbps

Frequency
2.4 GHz

Security
WPA2 PSK

Packet Capture with Wireshark



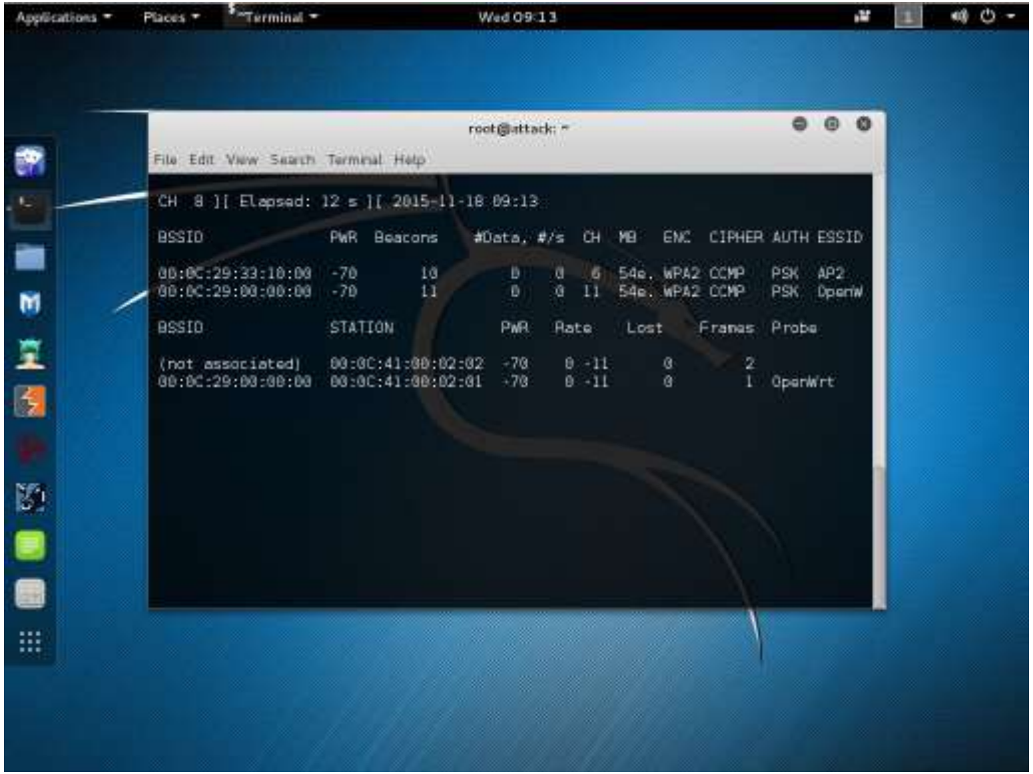
Interface: wlan0mon Frequency: 2462 MHz (11) NOHT wlan0mon Switched to 2462 MHz (11)

```
No.    Time         Source                 Destination              Protocol Length Info
   240 22.41060800 Vmware_00:00:00        Broadcast                802.11      157 Beacon frame, SN=0, FN=0, Flag
   241 22.45204400 Cisco-Li_00:02:01      Vmware_00:00:00          802.11      152 QoS Data, SN=45, FN=0, Flags=.p
   242 22.46406600                        Cisco-Li_00:02:01 (RA    802.11       28 Acknowledgement, Flags=.......
   243 22.47598700 Vmware_00:00:00        Cisco-Li_00:02:01        802.11      152 QoS Data, SN=0, FN=0, Flags=.p.
   244 22.48799000                        Vmware_00:00:00 (RA)     802.11       28 Acknowledgement, Flags=.......
   245 22.51599500 Vmware_00:00:00        Broadcast                802.11      157 Beacon frame, SN=0, FN=0, Flag
   246 22.62408500 Vmware_00:00:00        Broadcast                802.11      157 Beacon frame, SN=0, FN=0, Flag
```

```
▸ Frame 1: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface 0
▸ Radiotap Header v0, Length 18
▸ IEEE 802.11 Beacon frame, Flags: ........
▸ IEEE 802.11 wireless LAN management frame
```

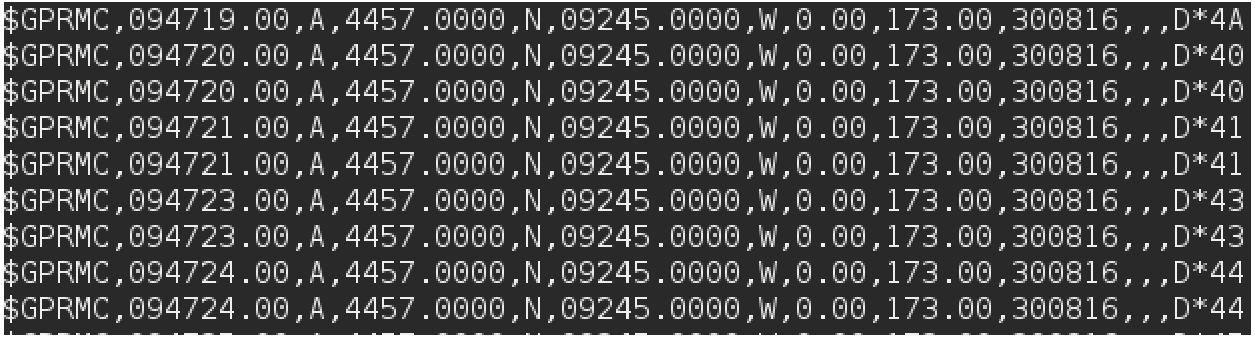
```
0000  00 00 12 00 2e 48 00 00  00 16 9e 09 a0 00 b9 00   ......H.. ........
0010  00 00 80 00 00 00 ff ff  ff ff ff ff 00 0c 29 00   ........ ......).
0020  00 00 00 0c 29 00 00 00  00 00 ad 12 97 37 d1 24   ....)... ......7.$
0030  05 00 64 00 31 04 00 07  4f 70 65 6e 57 72 74 01   ..d.1... OpenWrt.
0040  08 82 84 8b 96 0c 12 18  24 03 01 0b 05 04 00 02   ........ $.......
```

Wireless Survey with airodump-ng



```
CH  8 ][ Elapsed: 12 s ][ 2015-11-18 09:13

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:0C:29:33:10:00  -70       10        0    0   6  54e. WPA2 CCMP   PSK  AP2
00:0C:29:00:00:00  -70       11        0    0  11  54e. WPA2 CCMP   PSK  OpenW

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   00:0C:41:00:02:02  -70    0 -11      0        2
00:0C:29:00:00:00  00:0C:41:00:02:01  -70    0 -11      0        1  OpenWrt
```

NMEA Data for GPS Simulation



```
$GPRMC,094719.00,A,4457.0000,N,09245.0000,W,0.00,173.00,300816,,,D*4A
$GPRMC,094720.00,A,4457.0000,N,09245.0000,W,0.00,173.00,300816,,,D*40
$GPRMC,094720.00,A,4457.0000,N,09245.0000,W,0.00,173.00,300816,,,D*40
$GPRMC,094721.00,A,4457.0000,N,09245.0000,W,0.00,173.00,300816,,,D*41
$GPRMC,094721.00,A,4457.0000,N,09245.0000,W,0.00,173.00,300816,,,D*41
$GPRMC,094723.00,A,4457.0000,N,09245.0000,W,0.00,173.00,300816,,,D*43
$GPRMC,094723.00,A,4457.0000,N,09245.0000,W,0.00,173.00,300816,,,D*43
$GPRMC,094724.00,A,4457.0000,N,09245.0000,W,0.00,173.00,300816,,,D*44
$GPRMC,094724.00,A,4457.0000,N,09245.0000,W,0.00,173.00,300816,,,D*44
```

Limitations and Future Work

Limitations

- Only applies basic signal strength variations according to distance
- Only available for Linux-based guest operating systems

Future Work

- Leverage GPS simulation to develop mobile simulations with vehicle-born networks
- Utilize wireless simulation to develop IoT simulations

Questions