NWS Assignment 4: Hands-on with Wi-Fi

Group Assignment

*You need to work on Linux platform for doing the following assignment. You need to know UNIX shell scripting. Use GNUPLOT tool for generating plots. Read **man** pages of the following commands: iw, hostapd, ifconfig, iptables, apt-get; which are useful for doing this assignment.*

How to capture Wireless frames in monitor mode?

One approach: create monitor interface to capture management,control,wif data packets.

sudo iw dev wlan0 interface add mon0 type monitor

sudo ifconfig mon0 up

sudo wireshark

and select mon0 to capture in wireshark interfaces list.

1. Wireshark assignment on Wi-Fi:

Answer queries given in *Kurose and Ross textbook wireshark assignment on Wi-Fi (Wireshark_802.11.pdf available in Assignment Files folder in GC),* Call the trace, External_802_11.pcap, available at http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip as TRACE1.

Collect your own Wi-Fi traffic trace (TRACE2: GroupID_IITH_802_11.pcap) for at least 10 minutes from your laptop with built-in Wi-Fi radio or USB dongle in ***Monitor mode***. Select one of the orthogonal channels (1, 6, 11) in 2.4 GHz or 5.2GHz ISM bands for this trace collection (**preferably one that is having lot of user traffic in in peak time**).

Answer the following also by using the traces TRACE1 and TRACE2:

a. Pie chart of MAC Management, Control, Data Traffic. Further division in Management and control frames (i.e., probe reqs, association reqs, RTS/CTS, power-saving, etc). Which MAC frame appeared the most in the trace and its percentage?
b. Bar graph/pie chart for different Application/network layer protocol traffic (i.e., http, ftp, smtp, dns, dhcp, arp, etc). You may need to supply encryption key in wireshark to first decrypt packets.

c. Plot avg packet size vs Time (1-minute resolution), Plot avg PHY data rate vs Time, Plot RSSI (received signal strength) vs Time and Plot Packet rate (pkts/sec) vs Time (1-minute resolution). You need to count total no. of packets received in each 1-min interval and divide that with 60 to get Packet rate. For other plots, you need to take avg of packets received in each 1-min interval. List out main observations in each plot.
d. Histograms of packet sizes and PHY data rates. List out main observations in each plot.
e. Display beacon important information (all capabilities of AP, number of stations connected, channel utilization, rate supported etc) broadcasted by various APs (IITH, IITH-GUEST)

2. Configure your Linux laptop as a Wi-Fi hotspot with WPA2. Contact TAs and borrow Wi-Fi USB dongle for doing this part of the asg.

a. One should able to connect to Internet through this AP. Clients of your AP should able to connect to Internet. Your AP should give out IP addresses dynamically by using DHCP. Describe the whole procedure involved in setting up of your custom AP in the design document. Refer man pages of iw, iptables, hostapd and dhcpd. You get grace marks if you accomplish this using iw commands w/o hostapd.
b. Compare security features of your **AP SSID, IITH-GUEST and IITH SSIDs.** Write all messages exchanged during station association with above mentioned SSIDs. And comment on security messages exchange.
c. Write a script for wireless clients to know about Number of stations connected to each SSID (IITH, IITH-Guest, Your AP) and connect to the SSID, which is having least number of clients. (You can connect to wireless AP using iw command from CLI)

Deliverables in a tar ball on GC:

- **All trace files, scripts (to setup AP, to connect to best AP, analyze results, plotting results, etc)**
- **Readable Report in Word or Latex summarizing your design and explaining/analyzing your results/plots.**

Late Policy:
7 slip days overall
10% cut in marks for each day beyond slip dates.