# *Assignment 1: Hands-on with Wi-Fi*

**Individual Assignment**

*You need to work on Linux platform (not on VM) 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, data packets on Wi-Fi channel.

**sudo iw dev wlan0 interface add mon0 type**

**monitor sudo ifconfig mon0 up sudo wireshark** and select

mon0 to capture in wireshark interfaces list.

Help:
https://wireless.wiki.kernel.org/en/users/documentation/iw

### 1. Wireshark assignment on Wi-Fi:

Answer queries given in *Kurose and Ross textbook wireshark assignment on Wi-Fi (Wireshark_802.11.pdf, attached on GC), using* Wi-Fi trace available at http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip with the name Wireshark_802_11.pcap as TRACE1.

Collect your own Wi-Fi traffic trace (TRACE2: YourRollNo_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 any in 5.2GHz ISM bands for this trace collection (**preferably one that is having a lot of user traffic in peak time from Acad Block-A/C**).

### Answer the following questions as well 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). b. Answer the following from traces:

1. No. of different APs visible to device which collected the trace?

2. Minimum size of MAC frame for which RTS/CTS exchanged?
3. What fraction of MAC frames are protected (encrypted)?

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.

**2. Configure your Linux laptop as a Wi-Fi hotspot with WPA2 or you can use external Wi-Fi USB dongle for doing this part of the asg.**

a. Write a script which estimates channel utilization on each of 11 Wi-Fi channels in 2.4 GHz ISM band and then configures operating channel of your AP to the one of 3 orthogonal channels (1,6,11) that is having the least channel utilization. In other words, your AP is set to operate on the least loaded orthogonal Wi-Fi channel in 2.4 GHz.

b. One should be able to connect to Internet through this AP. Clients of your AP should be 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 instead of hostapd.

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.

**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 PDF Report summarizing your design and explaining/analyzing your results/plots and screen shots.**

**PLAGIARISM STATEMENT <Include it in your report>**

*I certify that this assignment/report is my own work, based on my personal study and/or research and that I have acknowledged all material and sources used in its preparation, whether they be books, articles, reports, lecture notes, and any other kind of document, electronic or personal communication. I also certify that this assignment/report has not previously been*

*submitted for assessment in any other course, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that I have not copied in part or whole or otherwise plagiarised the work of other students and/or persons. I pledge to uphold the principles of honesty and responsibility at CSE@IITH. In addition, I understand my responsibility to report honour violations by other students if I become aware of it.*

Name:

Date:

Signature: <keep your initials here>

Late Policy:

10% cut in marks for each late day