Monitoring Network Packets

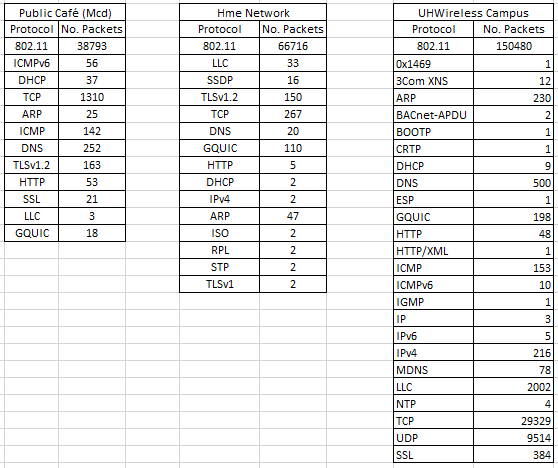
For capturing packets, I have used Wireshark in Ubuntu 18.0 OS. To enable monitor mode I have used following commands.

1. sudo iwlist channels
2. sudo airmon-ng start wlp3s0 <channel number>
3. sudo airmon-ng stop wlp3s0mon

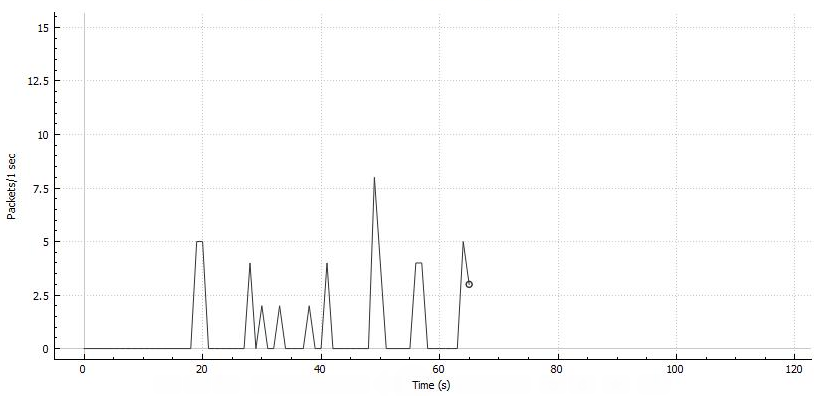
1. I have captured three traces of packets in 1. Home network, 2. Campus network 3.McD cafe with monitor mode enabled in Wireshark for the duration of 2 mins.

Following are my observations.

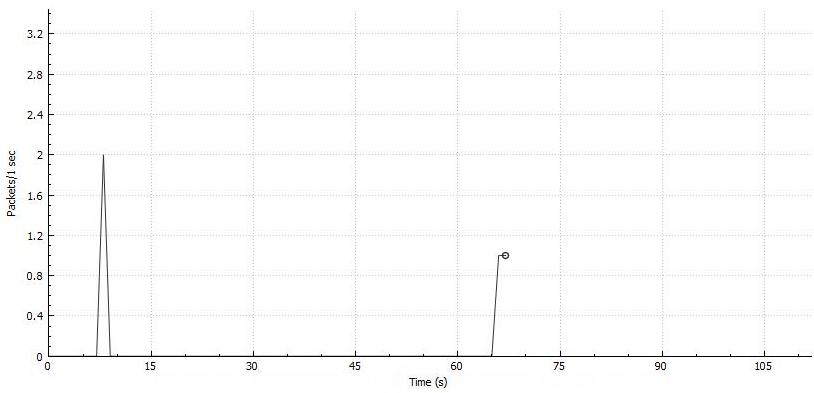
Each trace has captured different types of protocols and have different number of packets transferred. Protocol and No of packets it transferred under the protocol are captured and kept in the following tables.



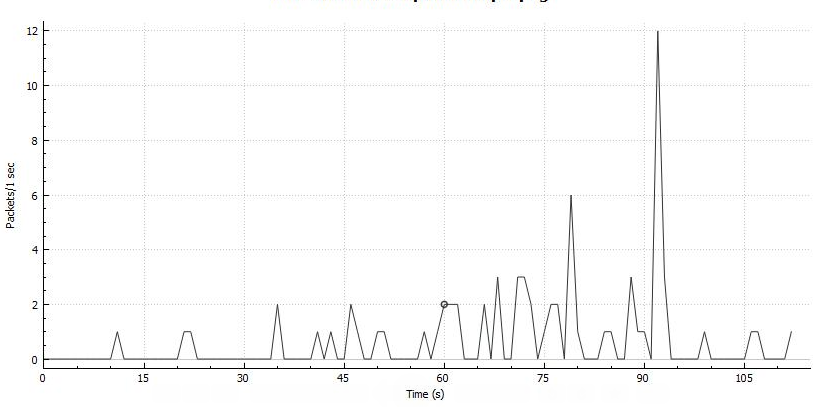
2. I have calculated the total number of HTTP packets per second on Time and recorded on below graphs.



a.Home Network.



b. Public cafe Network



c. UHWireless Network

3. I have counted the number of people in McD café and started capturing the packets in monitor mode. What I observed is number of different MAC addresses show in wireshark is significantly equal to the number of people in the café. There are 2 to 3 other MAC address are shown but I ignored in counting since there may be other entities connected to same network but not present in café.

4. I have took the sample packets captured in campus on UHWireless network and exported the packets in CSV file format. The csv file is the input to my program. Looping through every row in the input I have calculated baseline level by calculating average of total number of packets by total time frame. Then calculated surge levels by calculating sudden increase in the number of packets per second that are greater than pervious time frame. Then recorded the surge start time and surge end time. Recorded the surge level by number of packets in surge by time frame. Then noted the IP address of node that created the surge.