Wireless Networks

Assignment-1

Submitted By

Arnav Singh
2021019

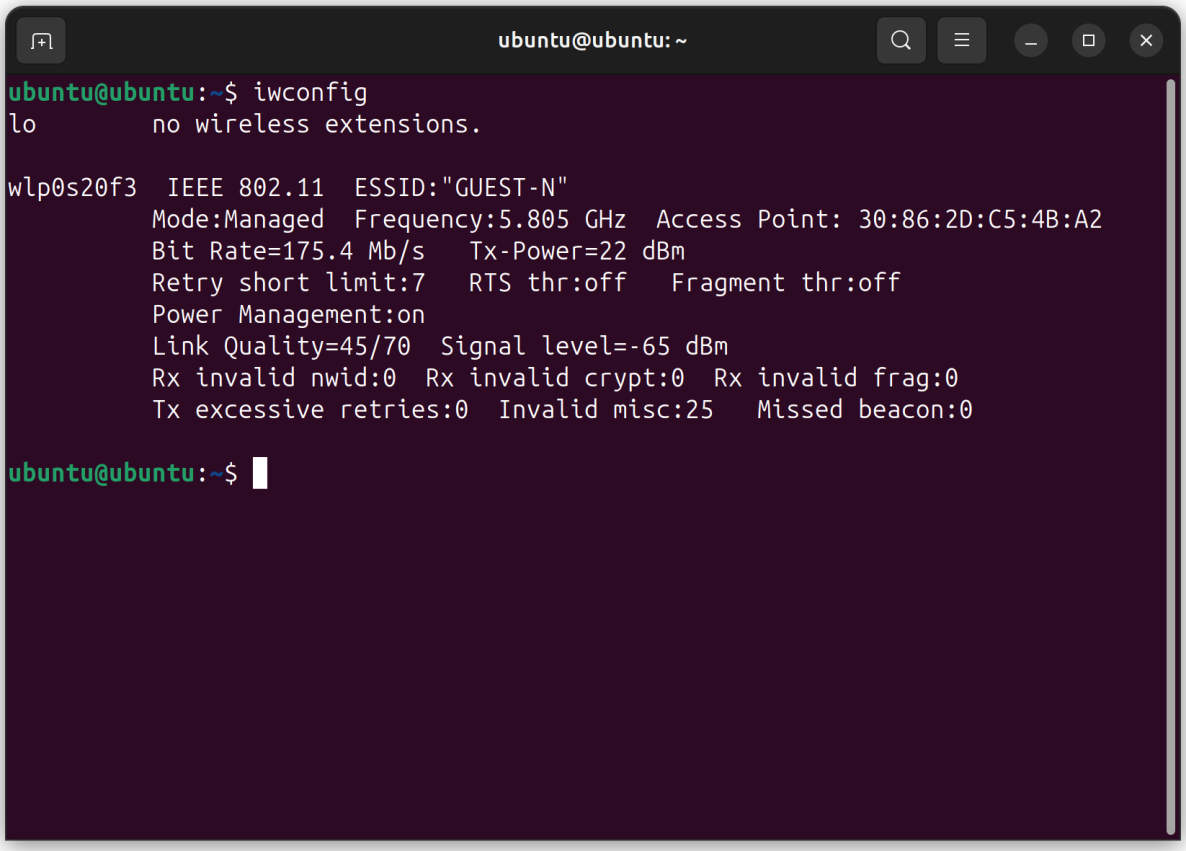
1. Connect your laptop to IIITD access point. Identify the SSID and BSSID of the AP connected to. Take measurements of your current received signal strength, bit rate, transmission power, and operating frequency band. Now, take your laptop and walk for 2 min, all this time, get the above measurement for every 10 sec (through a script). Plot how your signal strength and bitrate vary while you walk. [1+2+1+2]

Part-1

BSSID (Access Point):- **30:86:2D:C5:4B:A2**
SSID: **“GUEST-N”**

Part-2

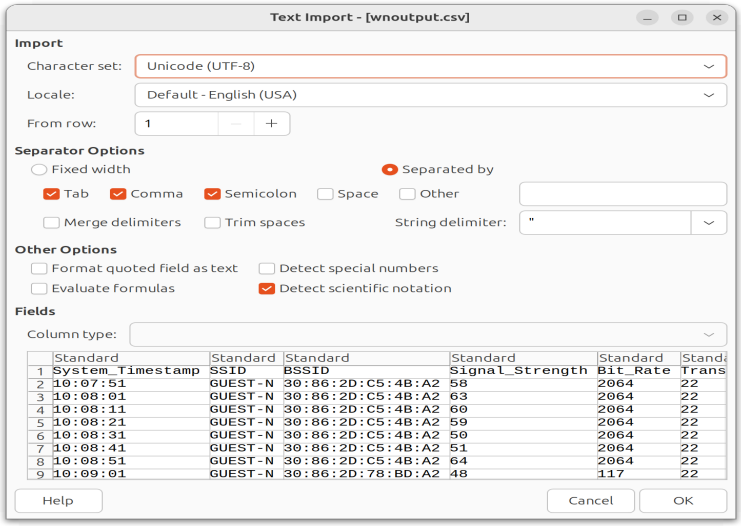
Signal Strength:- **-65dBm**
Bit Rate: **175.4 Mb/s**
Transmission Power:- **22 dBm**
Operating Frequency Band: **5.805 GHz**



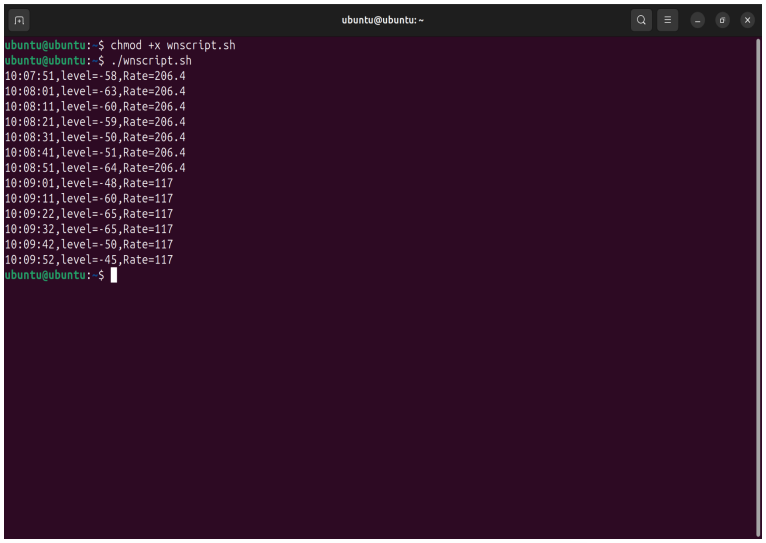
Procedure: Use the ‘iwconfig’ command in a Linux Terminal

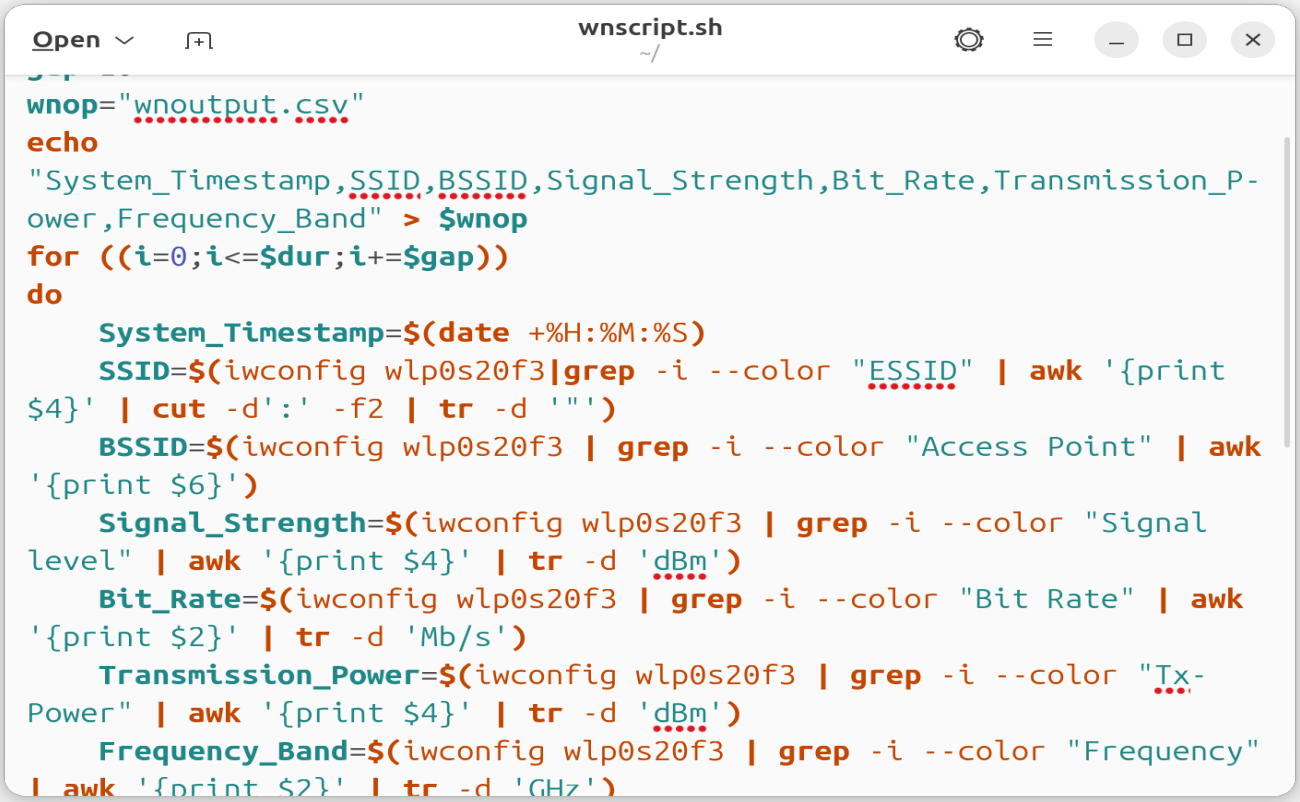
Part-3

I took my laptop and walked around in the C-wing OBH for 2 minutes, collecting the aforementioned network data, every 10 seconds, essentially collecting 13 data points in the CSV file. The BASH script for the same is attached in the folder. It is to be noted that since I formatted all the collected values as numbers, disregarding other symbols, the values are missing decimal points, but since it is pretty intuitive to spot the error(s) if any, it's rather harmless, nonetheless, necessary corrections were made in the graphing code, in accordance with the values echo-ed in the terminal.



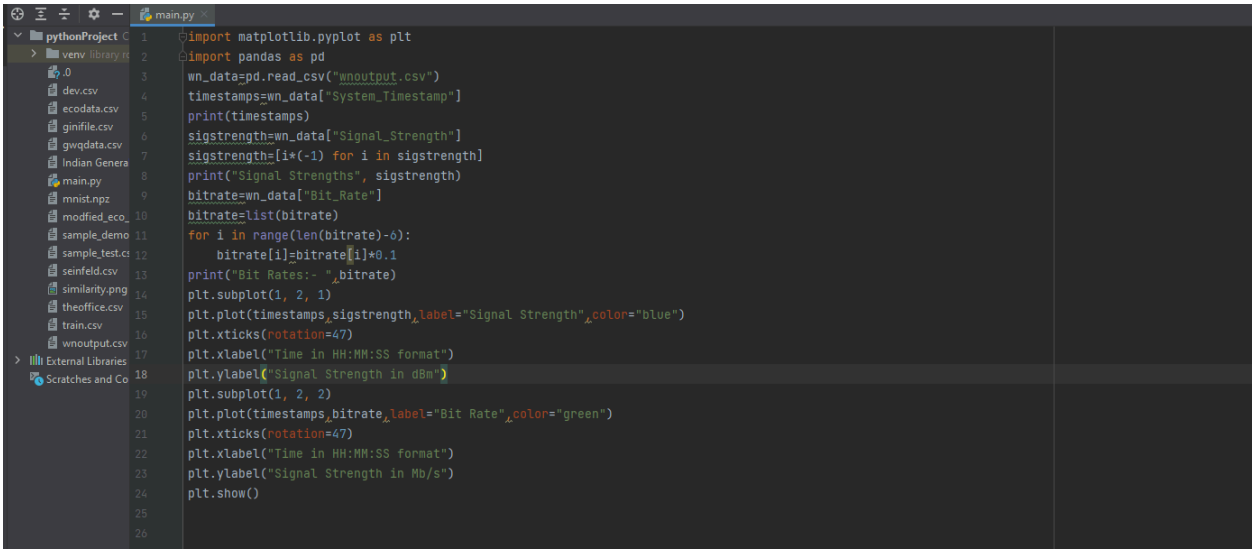
	Standard	Standard	Standard	Standard	Standard	Standa
1	System_Timestamp	SSID	BSSID	Signal_Strength	Bit_Rate	Trans
2	10:07:51	GUEST-N	30:86:2D:C5:4B:A2	58	2064	22
3	10:08:01	GUEST-N	30:86:2D:C5:4B:A2	63	2064	22
4	10:08:11	GUEST-N	30:86:2D:C5:4B:A2	60	2064	22
5	10:08:21	GUEST-N	30:86:2D:C5:4B:A2	59	2064	22
6	10:08:31	GUEST-N	30:86:2D:C5:4B:A2	50	2064	22
7	10:08:41	GUEST-N	30:86:2D:C5:4B:A2	51	2064	22
8	10:08:51	GUEST-N	30:86:2D:C5:4B:A2	64	2064	22
9	10:09:01	GUEST-N	30:86:2D:78:BD:A2	48	117	22





Part-4

I mailed these files to myself, downloaded them in the PyCharm directory on my PC, imported the CSV file using Pandas, performed the aforementioned corrective actions, and graphed them using matplotlib.



2. Now, create a setup of 3 devices: D1: your phone as the AP, D2: another phone/tablet/laptop as client and D3: your laptop as monitor mode
Keep distance between D1 and D2. Place D3 close to D2.

   D1 make it open (Go to settings->connections->Mobile Hotspot->configure->security->open).
   D2: Forget the D1 credential if stored before, then connect to D1. From the browser, open IIITD webpage.
   D3: Put your laptop in monitor mode and collect a packet trace for 2 min. [2]

   a. Identify the beacon frames, tell the SSID of all the APs you can see [2]
   b. Compute the average signal strength from each AP across all the beacons you have received for 2 min. [2]
   c. Compute the average bitrate from each AP across all the beacons you have received for 2 min [2]
   d. Find out the types of frames exchanged between D1 and D2. Write down all the types of frames, count the number of each type programmitically. Look at this to identify the types of frames [3].
   e. Identify the MAC layer acknowledgment, and identify which types of frames have MAC layer acknowledgements. Compute the bitrate of the MAC layer acknowledgments. [2]
   f. Compute average signal strength and bitrate across all frames between D1 and D2. [2]
   g. Take D2, now move closer to D1. Keep D3 as it is. Open IIITD page once again, take packet trace in monitor mode for 2 min at D3. Compute the average signal strength and bitrate of all frames between D1 and D2. Do you see any difference from f). Explain. [2]

(a) Identified the Beacon Frames using ***wlan.fc.type_subtype == 0x8*** as a filter, there were 679 frames in total, The SSIDs I can see are LAPTOP-S, MOBILE-S, GUEST-N, badabing, “5G” (yep the SSID is called 5G), and MKR-new.
(b) The Average Bit Rate is:- 8.013254786450663 Mb/s, computed this by adding the relevant column to the pcapng file, exporting it in a csv format, opening it in Python, importing it with pandas, summing it up, and dividing it by its length. (Check the code)
(c) The Average Signal Strength is:- -81.9381443298969 dBm, computed this by adding .....[yeah the same stuff as the last question, but it gets more intense since there are 3 Antenna Signals under the Radio Section, so I was a bit confused there, but ultimately found out that there was an actual sigstren column in the IEEE section, and it matches the strengths for Antenna1 (which is actually the 2nd antenna) so, that’s something crazy], exporting it... (refer to the prev part)
(d) (wlan.da == 3c:a6:f6:2c:98:37 && wlan.sa == 2a:b8:02:f0:1e:54) || (wlan.sa == 3c:a6:f6:2c:98:37 && wlan.da == 2a:b8:02:f0:1e:54) (used this to create another pcap). All 16 frames are QoS Data frames (fc.type.subtype==0x28 filter returns the same list, q.e.d.)

(e) Found Acknowledgements using wlan.fc.type_subtype==0x1D, couldn't identify what they were responses to since there were no exact Sequence Numbers listed with individual packets. However, I did list all the destination addresses, so perhaps that's what was being asked. The Average Bit Rate for ACKs is:- 2.5495495495495497 Mb/s, found it by exporting it and repeating prev mentioned steps

(f) The Average Signal Strength is:- -46.3125 dBm, The Average Bit Rate for D1-D2 packets is:- 110.95124999999999 Mb/s

(g) The Average Signal Strength is:- -29.7027027027027 dBm, The Average Bit Rate for D1-D2 packets is:- 104.27716516516517 Mb/s. The Signal Strength has increased which is pretty intuitive, but the bit rate has surprisingly fallen a bit, which seems absurd but since the number of D1-D2 packets in the close distance capture increased dramatically, and there were a lot instances of failed transmissions and spurious retransmissions, which makes the slight fall somewhat explainable.

These assertions can be confirmed by running the attached Python script.