CS5553: Wireless Network & Security

Assignment 2: Hands-on with Wi-Fi (Part-B)

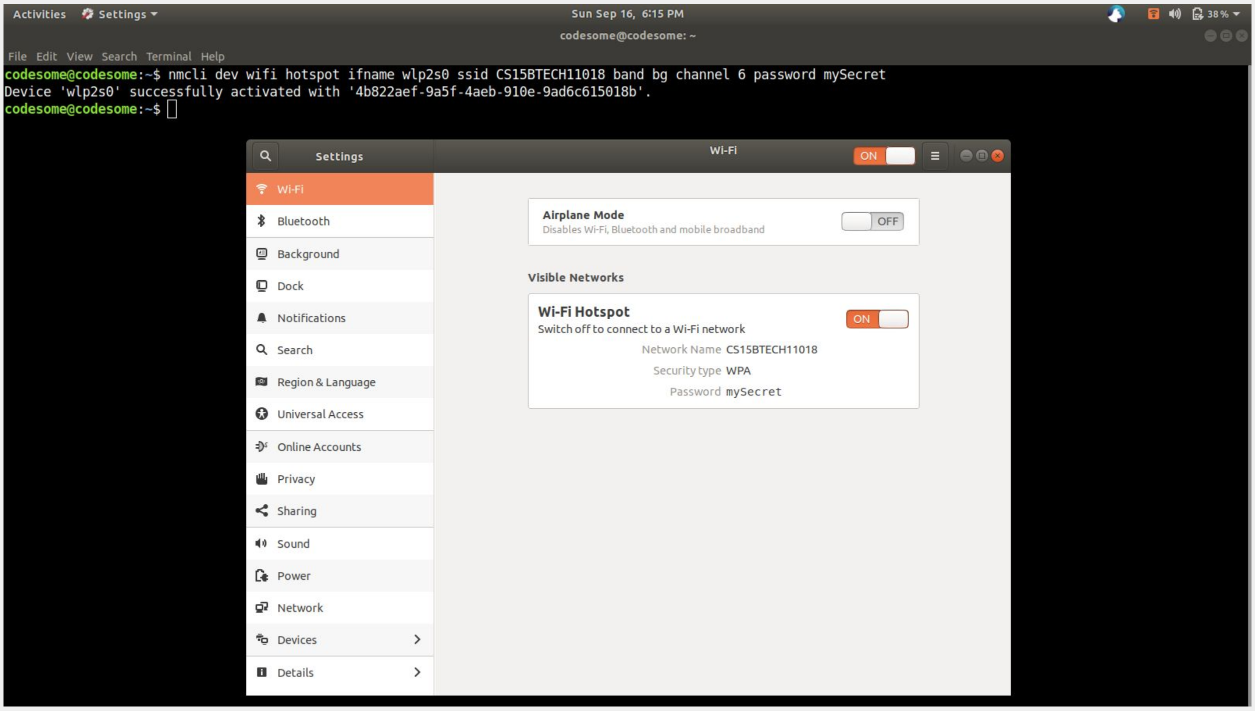
Ganesh Vernekar - CS15BTECH11018

a. Configuring laptop as WiFi hotspot can be done by following command.

```
$ nmcli dev wifi hotspot ifname <interface> ssid <ssid> band <band> channel
<channel> password <password>
```

Example:

```
$ nmcli dev wifi hotspot ifname wlp2s0 ssid CS15BTECH11018 band bg channel
6 password mySecret
```



```
codesome@codesome:~$ nmcli dev wifi hotspot ifname wlp2s0 ssid CS15BTECH11018 band bg channel 6 password mySecret
Device 'wlp2s0' successfully activated with '4b822aef-9a5f-4aeb-910e-9ad6c615018b'.
codesome@codesome:~$
```

Wi-Fi ON

Airplane Mode OFF
Disables Wi-Fi, Bluetooth and mobile broadband

Visible Networks

Wi-Fi Hotspot ON
Switch off to connect to a Wi-Fi network

Network Name CS15BTECH11018
Security type WPA
Password mySecret

b & e.

Both were done in the same code, with small additions for both.

Design

High level design of the code:

1. Start monitor mode.
2. For each channel (1-11 of 2.4GHz band)
    a. Sniff for some time.
    b. For each packet
        i. Gather the statistics required. (more explanation later)
            1. Utilization for b.
            2. Station count for e.
    c. If **b** (creating hotspot) is required
        i. Pick the channel (among 1,6,11) which has least average utilization.
        ii. Print the utilization and other stats for every channel as a table.
        iii. Create hotspot at the picked channel with SSID “`CS15BTECH11018`”.
    d. If **e** (connecting to WiFi) is required
        i. Pick the SSID with least station count.
        ii. Print station counts of all SSID and other stats as a table.
        iii. Take username and password from user for the picked SSID.
        iv. Connect to the AP with picked SSID.
3. Stop monitor mode.

Collecting Stats

1. For every packet, look for all **`802.11 Information Element`**.
2. If the Information Element is **`QBSS Load Element`**, then it contains the channel utilization and station count. More Info.
3. If we don’t find any QBSS Load Element, then we skip that packet (basically no information from that packet).
4. For Utilization
    a. Number of QBSS Load Element received and sum of utilization is noted for each channel.
    b. Number of unique APs is also noted per channel. (Reason is in next section).
        i. This is done using MAC addresses of APs and not SSID.
5. For Station Count
    a. Number of QBSS Load Element received and sum of station counts is noted for each SSID.

Picking Least Utilized Channel

1. It is possible that some APs don’t broadcast QBSS Load Element.
2. If `sum_of_utilization > 0` (atleast 1 AP braodcasted the value) for channels 1, 6, 11,
    a. Then pick the channel with least average utilization (`sum_of_utilization / no_QBSS_Load_Element`).
3. Else
    a. Pick the channel (among 1,6,11) with least number of APs.

Picking SSID with Least Station Count

1. Same as above, it is possible that some APs don’t broadcast QBSS Load Element.
2. We pick an SSID only if it broadcasts station counts.
3. Pick the SSID with least average station count (`sum_of_station_counts / no_QBSS_Load_Element`).

Basic Info about code

- Language: `Go`
- Tool for capturing packets: `tshark`
- Package for parsing packets: https://github.com/google/gopacket

Prerequisite

1. Golang compiler
2. tshark (should be able to run without `sudo`)
3. These Go packages

```
$ go get github.com/google/gopacket
$ go get github.com/olekukonko/tablewriter
```

Build & Run

```
# Build
$ go build main.go sniffer.go
# For creating hotspot (question b)
$ ./main hotspot
# For connecting to WiFi (question e)
$ ./main connect
```