Passive sniffing for analysis of channel distribution

Kaustubh Agarwal

Student No. - 4823168
Delft University of Technology
Delft, The Netherlands
Email: K.Agarwal-1@student.tudelft.nl

Maria Teresa Blanco Abad

Student No. - 4935829
Delft University of Technology
Delft, The Netherlands
Email: M.T.BlancoAbad@student.tudelft.nl

***Abstract*—This report provides an analysis of the utilization of the ISM frequency bands in addition to providing insights in Wi-Fi usage. After processing the data gathered by passively sniffing packets from different locations, conclusions such as the popularity of a particular channel, evolution of spectrum usage based on users of a network and a comparison between Access Points supporting 2.4GHz and 5GHZ are drawn.**

I. Introduction

In this report we document the channel distribution of ISM bands at different locations in Deflt, The Netherlands. We find out the number of Access Points (AP) supporting 2.4 GHZ as well as 5GHz band and find out the PHY type associated with these Access Points. We provide our inferences on the different patterns of channel distribution observed for these different locations.

The report is divided into sections where section II mentions the different locations of interest for the experiment. In section III, we provide the detail of the hardware used and it's capabilities. Section IV describes the software setup used to sniff the packets and their post processing for further investigation. We illustrate our observations with the help of graphs. Section V documents the results and our inferences from the observed data. The final Section VI describes our conclusions from the experiment.

II. Experimental Setup

As the radio propagation environment varies greatly at different places such as a business park, city center and at residential complexes, we decided to record wireless channel information at multiple varying locations. These locations include Delft city center, Educational buildings- Pulse and EWI at the TU Delft campus, a Residential complex and a hospital. We discuss in detail on the collected data from these locations in the results section.

III. Hardware Setup

For capturing the wireless data We used our personal computers which has - Intel(R) Dual Band wireless-AC 8265 card- which supports 2x2 11ac Wi-Fi and has backward compatibility with 802.11 a/b/g/n standards. It supports monitor mode which allows a computer to monitor all traffic received on a wireless channel without having to associate with an Access Point first.

For a given area and channel, the number of Wi-Fi devices currently being used can be discovered. This helps to create a better Wi-Fi network that reduces interference with other Wi-Fi devices by choosing the least used Wi-Fi channels.

IV. Software Setup

Since wireshark does not support channel hopping by default we used a tool called "Airodump-ng" [1] and kismet[2] along with Tshark to capture raw 802.11 frames. We first check the available interfaces for our device and then select the wireless interface. Additionally, airodump-ng writes out several files containing the details of all Access Points and clients seen. We focus only on the the Probe request/response and beacon frames as they contain the necessary 802.11 frame data. Airodump-ng also outputs a CSV file containing the information of the Access Points and the 802.11 frame information and a Pcap file for further investigation. We used the following script for capturing the required data as shown-

```
#!/bin/bash
#Check for available interfaces
tshark –D
# Check which channel is selected
iwlist wlp2s0 channel
# kill other processes
sudo airmon–ng check kill
# start monitor mode!
sudo airmon–ng start wlp2s0
mkdir drive
cd drive
#Monitor 2.4 and 5 GHz channels with time
#interval 0.2 sec and write data to file
sudo airodump–ng –f 200 ––band abg ––write
data wlp2s0mon
```

Since by default, airodump-ng hops only in 2.4GHz channels, we monitor both 2.4 and 5GHz channels by using the band option. The output csv file contains the list of unique Access Points with their selected channel and supported data rates. A pcap file also found in the output contains the raw capture with IEEE 802.11 frames header data.

In addition, to provide contrast to the gathered data, Kismet [2] was used in order to visualize the packets captured since kismet decodes WEP packets at runtime. After an AP is detected, its GUI allow to see which clients are connected to that particular AP. This feature is useful to correlate to the data processed using methods in section below IV-A. In addition, Kismet supports channel hopping, and it can hop 1-10 channels per second.

A. Processing of extracted files

Once the correct files were created, python was used to parse the .pcap output from tshark in order to obtain relevant graphs showing SSID of senders, channel distribution, PHY types. In order to handle .pcap fields, the scapy library [3] provides methods to filter packets or access .pcap fields. In addition, to extract the manufacturer of an AP by parsing the first three octets of the MAC address (OUI of vendor), manuf library [4] was used.

V. Results

A. Channels used in ISM band

By convention in Europe, for 2.4 GHz band only channels (1-13) are allowed to be used in the ISM band as also depicted in the following figures. We collected data from different places and extracted the Operating frequency of each Access Point and plotted the number of Access Points against the operating channel. As we can see from Figure 2 the maximum Access Points are operating in channel 1,5,9,13 and in Figure 1 on channels 1,9,11,13 to reduce the interference and keep the connection at a good quality level. Also compared to a university building, the number of Access Points operating on 5GHz in a residential area is considerably low as the major concern of a user in a home is connectivity(2.4 GHz) and not higher throughput(5 GHz).

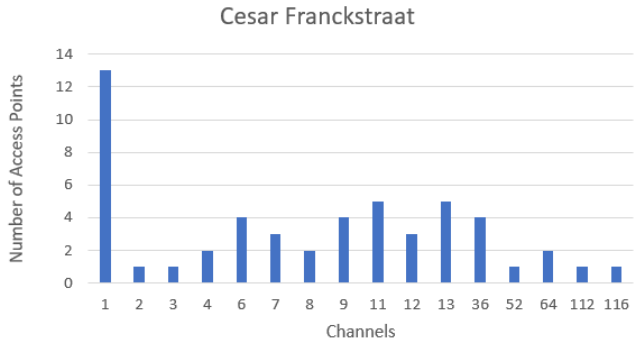

Fig. 1. Channel distribution in a residential area

Since the channels are overlapping, an Access Point tries to connect to those channel which are far off from each other to reduce interference as much as possible. Since the number of Access Points in a market area is expected to be high(shops,cafes,gov buildings,offices) the operating channels are also distributed over a wide range as also depicted from

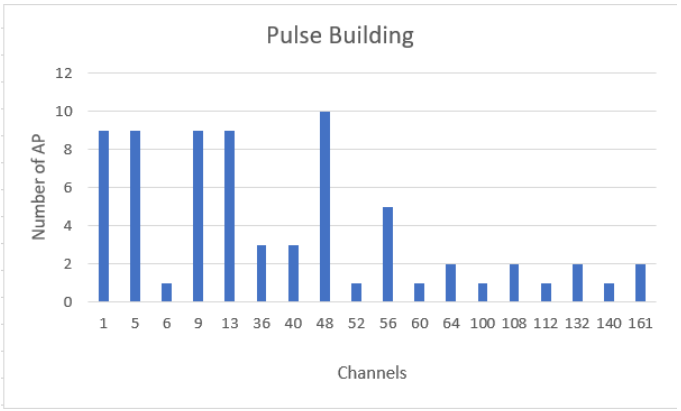

Fig. 2. Channel distribution in PULSE

Figure 3. Also a high number of Access Points operating on 5GHz frequency can be accounted for different shops as they want to reduce the interference from nearby shops(since 5GHz has a shorter range than 2.4 GHz band). Also in most access Points channels in the lower frequency range of 5GHz are more popular such as channel 36. Also we see there are less Access Points operating on channels 52,56,60 and 64 as these are DFS channels. If radar signals are detected on current channel(DFS), the devices will vacate that channel and switch to another channel which will lead to interruption in the current transmission and reduces the QOS of the system.

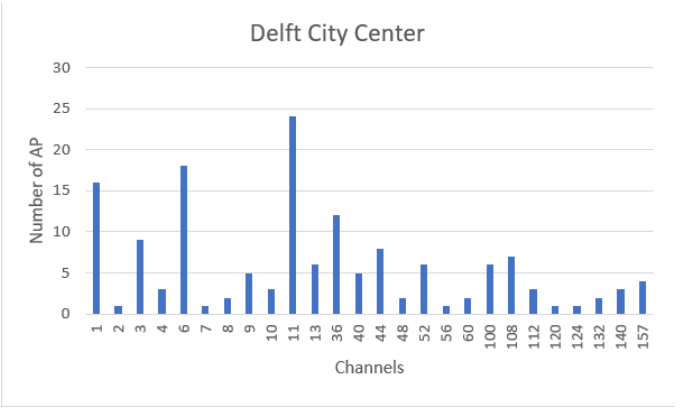

Fig. 3. Channel distribution in Delft City Center

B. Correlation between Access Point type and the selected channel

Throughout the development of the experiment at different locations, several conclusions were drawn regarding the AP type and the channel selected by the AP. The used packets to identify AP are beacons and therefore a dedicated tshark filter for beacon frames is needed: wlan.fc.type_subtype=0x08. The implementation code is found below:

```
sudo ifconfig wlp2s0 down
sudo iwconfig wlp2s0 mode monitor
```

```
sudo kismet

#after pcapdump file, filtering frames
tshark -r Kismet-20190303-17-57.pcapdump
-Y "wlan.fc.type_subtype==0x08"
-w outputINDUS_beacon.pcap

tshark -r outputINDUS_beacon.pcap
-Y "wlan.fc.type_subtype==0x08" -T fields
-e frame.time_epoch -e wlan.sa -e
wlan_radio.signal_dbm -e wlan_radio.channel
-e wlan_radio.phy >> output_beacon.csv
```

Firstly a definition of AP types is needed, therefore an Access Point will be considered either professional solution AP or consumer grade AP. The first type, a professional solution refers to an Access Point that could be installed in an industrial,hospital or university network such as Eduroam. In order to determine AP of these type, the manufacturer "Cisco systems" and BSSIDS as "Eduroam" were filtered in wireshark and compared to the rest of Access Points. On the other hand, the consumer grade AP is considered as the Access Points used in commercial establishments or private properties. Again, to differentiate consumer grade APs, an analysis in manufacturers such as "Ubiquiti" or "Zte" or "RuckusWi" or BSSIDS containing words such as "guest" "free wifi" helped to classify AP of consumer grade.

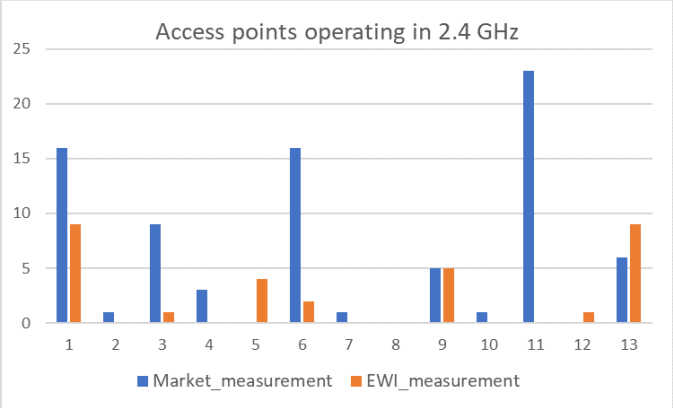

Fig. 4. Channel distribution depending on AP type. The blue distribution correlates to consumer grade AP. The orange distribution relates to professional solution.

Secondly, after drafting the classification of AP, differences between measurements in an university setting and a commercial area were compared in figure 4. The conclusion extracted is that an area where reliable wireless connectivity should be guaranteed (industrial area, university) skilled networking personnel would configure the AP to use non interfering channels leading to an efficient use of the radio spectrum. The reason is that it is ensured that less users will be using those channels (1, 3, 5, 13). On the other hand, the city center (market) is characterized by Access Points for commercial use or private individual networks. Therefore, more standard practices are followed leading to exploitation of the well known non-colliding channels (1, 6, 11) even though they may be more saturated by users.

C. PHY types

For describing the distribution of PHY types, we sniffed data in the TU Delft campus as shown in figure 5, since nowadays almost all devices have hardware supporting the latest PHY type: 802.11n (2.4 GHz) or 802.11ac (5 GHz). Even though more devices (around 10 times more) were accessing the 2.4 GHz band, we notice that also the PHY types using 5 GHz band are more and more supported nowadays. Moreover we still see a considerable amount of 802.11a as the beacon frames are transmitted at the lowest data rate in order to support the devices which only use low data rates. Although it is was not expected to detect a large number of 802.11n frames they are attributed to the large number of QOS frames being transmitted during the capture period.

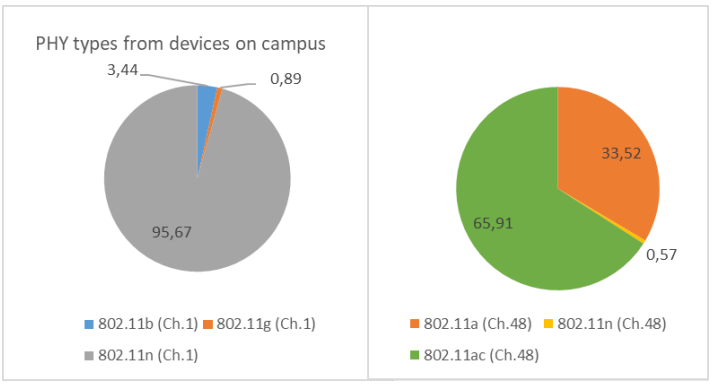

Fig. 5. Distribution of PHY types in TU Delft

D. Number of Access Points supporting 5GHz

We also did a comparison of the number Access Points operating at 5GHz against the total number of Access Points and also evident from Figure 6 -

- About 47% AP support 5 GHz band in educational buildings like Pulse, EWI and city center.
- About 15 % AP support 5 GHz band in hospital and residential areas
- We expect this number to be slightly higher as the range of 5GHz is considerably lower than 2.4GHz band

E. Channel hopping

Access Points have a centered frequency that can be configured by specifying a static channel of use. In addition, some enterprise Access Points have optional mechanisms where an automatic change of channel is performed whenever there is traffic congestion in a specific set channel. This feature called adaptive mode in a highly dynamic environment, especially in congested areas such as universities. This phenomena was observed in V-B where on campus, not that used channels such as 5, 13 were used and we think that is because the AP may have the adaptive mode enabled. After analyzing figure7 we can see the router representing the blue line is a dual band

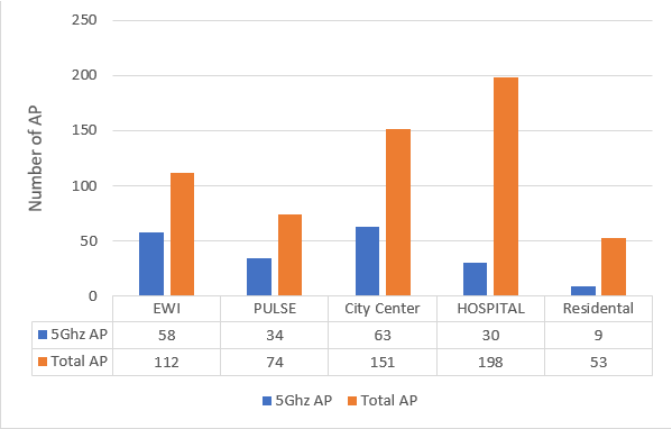

Fig. 6. Comparison of Access Points operating on 5GHz to total Access Points)

router as it switches between both 2.4GHz and 5GHZ bands in order to reduce interference from nearby Access Points. We can also estimate the time between a channel hop for a Access Point located in an industrial setting with the help of Figure 7.

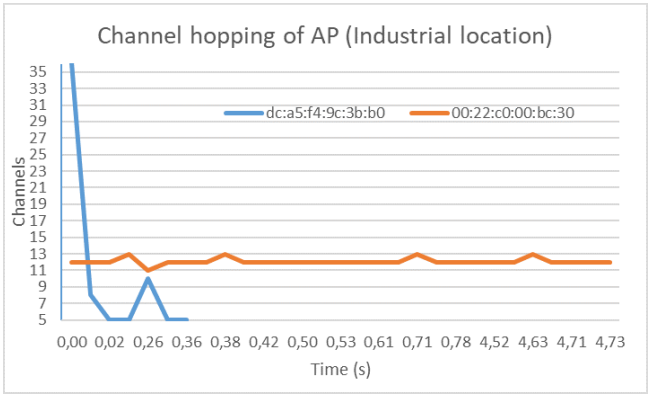

Fig. 7. Channel hopping observed in two AP (manufacturers: Cysco system and Shenzen Inc.)

F. Wigle database comparison

Based on the data collected from all the locations (Total 588 APs) we made a distribution of all the channels as shown in Figure8 and compared it with the data from the Wigle database as shown in Figure 9. Channels 1,6 and 11 are dominant in both data sets while there is increase in the use of 5 GHz bands in our collected data. In the data we collected as shown in Figure 9 there is a certain shift towards 5 Ghz routers as four bands(channel 36,44,48,108) makes to top 10 used bands. Also we can see that the use of 2.4 Ghz bands have reduced and faster 5GHz bands are taking their place. As the data from the Wigle database could be a bit out dated we can see a shift towards 5GHz band maybe because of increasing interference in and the 2.4 GHz band and the increase in number of Access Points.

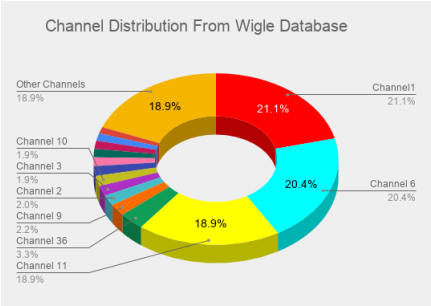

Fig. 8. Distribution of Channels according to Wigle database

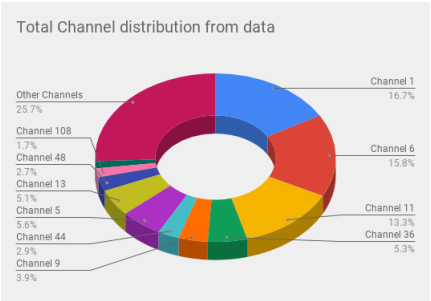

Fig. 9. Distribution of Channels according to collected data

VI. Conclusions

Through capturing and processing of the sniffed packets, we achieved a better understanding about the process of channel selection and distribution for Access Points. The extracted information extracted gave us an idea about which users use with spectrum based on their location. For example, we observed the popularity of specific channels and how the congestion of spectrum is handled (in industrial or university they use configured adaptive mode of AP whereas in commercial or residential areas they use standard configuration).

In addition, we could correlate the switching of users to usage of the 5 GHz band instead of the traditional and saturated 2.4 GHz by comparing historical data from Wigle database and the data collected during this experiment.

References

[1] https://www.aircrack-ng.org/doku.php?id=airodump-ng
[2] https://www.kismetwireless.net/
[3] https://scapy.net/
[4] https://github.com/coolbho3k/manuf
[5] https://www.tp-link.com/us/faq-763.html
[6] https://wigle.net/statsoctetstats