WNGP02

Simone Orru'- Hiram Rayo Torres

March 2018

1 Introduction

This report aims to present the results of project number 14: "Measure frame content to overhead".

2 Project description

This project consists in sniffing Wi-Fi packets using tshark to make an assessment on the amount of Data Frames that are sent over the network compared to Management and Control frames and to measure the airtime of these frames. Initially we understood this project as just measuring the amount of overhead in a Data Frame compared to the actual data that was sent on the Data packet. However, this was later clarified by the teaching assistant.

Our approach consisted in measuring and acquiring data on 3 different locations over an approximate duration of 2 hours at each spot in order to acquire enough data for our analysis.

3 Data collection

In order to gather the most possible quantity of information we chose locations which we considered to be crowded or that would most likely provide a high amount of data traffic. For this analysis we chose the following locations: IDE Faculty, EWI Faculty, Home Residence(Appartment Building).

Once the locations were decided we chose to make our measurements starting from 11:40 in the morning till 13:40 for both faculties and from 7:22 until 9:13 for the home residence in order to provide a contrast between these.
To be able to capture through every Wi-fi channel we used the Aircrack-ng software suit to enable our network cards to work in monitor mode.
For data collection we developed a python script, which used pyshark, a python wrapper for tshark. The purpose of this script was to capture the data packets being sent over the wi-fi network over a fixed period of time in order to later

parse them to get the specific information regarding the frame type, subtype and duration of each packet to make our analysis.

```
#Live capture
cap = pyshark.LiveCapture(interface='mon0',
      output_file="/home/simone/Documents/Wireless_Networking/Sniffing/live_capture1.pcap")
cap.sniff(timeout=t_cap)
#cap.sniff(timeout=30*60) #Specify the amount of time you want to capture (s)
count = len(cap)
print(cap)

t_end = time.strftime("%H:%M:%S",time.gmtime());

workbook = xlsxwriter.Workbook('live_capture1.xlsx')
worksheet = workbook.add_worksheet()

worksheet.write('A1', "Frame Type")
worksheet.write('B1', "Frame SubType")
worksheet.write('C1', "Wifi Frame type")
worksheet.write('D1', "Wifi Frame subtype")
worksheet.write('E1', "Duration wlan_radio")
worksheet.write('F1', "Length")
```

Figure 1: Part of the python script Live_Capture

Furthermore we utilized the xlsxwriter library to write the information into a simple excel sheet.

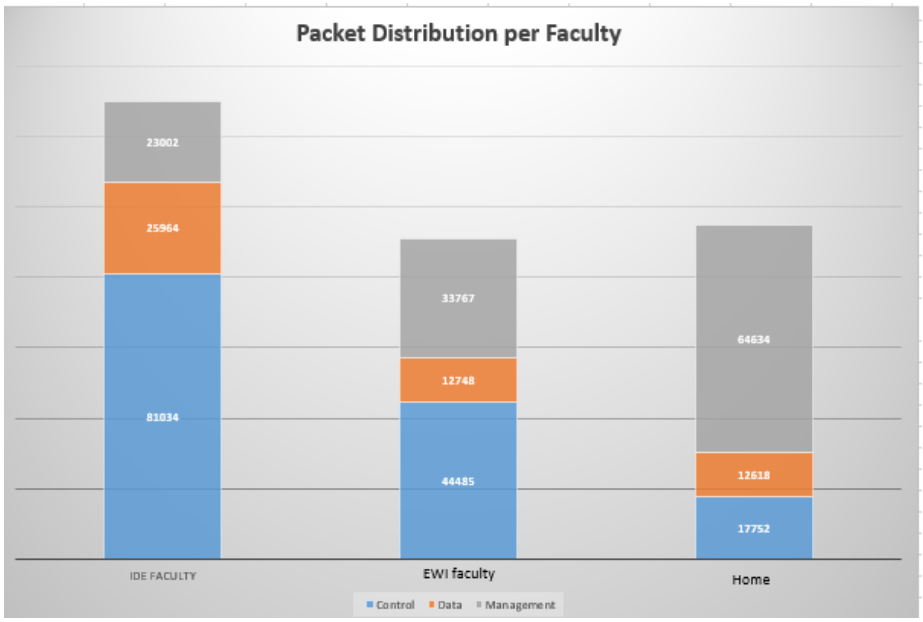
4 Data Analysis

Once the excel files with parsed information were generated, we created some graphs to facilitate the analysis. The table below presents the condensed information shown by this study.
Note: The full data and graphs presenting the information below can be found in the excel file at the repository.

Location	Data Packets	Management Packets	Control Packets	Airtime of Data packets	Airtime of Management Packets	Airtime of Control Packets
EWI Faculty	12,748	33,767	44,485	2.098s	3.64s	1.32s
IDE Faculty	25,964	23,002	81,034	4.16s	2.59s	2.59s
Home	12,618	64,634	17,752	6.30s	169.83s	3.25s

Regarding the EWI faculty, we observed that only 14 % of the packets corresponded to actual Data frames, accounting to only 12,748 packets. We can possibly explain this by taking in consideration the time at which the data was acquired. During this time, lectures were still in place, hence, students were not using their smartphones/computers as much as they would in their free time. In contrast, we observe that over the same period of time, twice the amount of Data Frames were transmitted at the IDE faculty, representing 20 % of the data transmitted. However, to compare these 2 results, we must also take into account the number of students that were

online at the capture locations as well as the possible missed captures due to channel hoping in monitoring mode. Also, taking into account the reported quantity of students enrolled at both faculties(according to TU Delft website) we could possible make assumptions regarding studying habits between them. In addition, we can also observe that the amount of Data packets sent over the network at Home location over the course of one hour and a half are approximately the same as the EWI faculty. One more fact that we can get from the table is how not always a higher number of packets correspond to a higher complessive airtime. This is the case of the EWI capture, where 50% of the packets were of the control type, but took up only 18% of the total airtime.



5 Conclusions

With this project we learned about the huge overhead represented by the control information that has to be sent over the wireless network compared to the actual Data. In addition, we got to understand the amount of information that is sent over the Wi-Fi channels and the insights that can be obtained by analyzing it. However, even though we captured over long periods of time, some of the data collected cannot be considered statistically significant, especially regarding the ratio control-management over data packets. This because we observed too much variation over these captures, so more data would be required in order to provide an accurate insights.