Delft University of Technology

Wireless Networking
ET4394

Wireshark Sniffing Assignment

W14 Measure frame content to over head

Samyuktha Sivaram (4723716)
Swarna Narayanan (4719905)

March 6, 2018

Introduction

We aim to capture the different types of WiFi frames and measure the ratio of the overhead to that of actual data being transmitted. Overheads are the management and the control frames. Frame type and length of each frame in bytes are extracted from TShark for further analysis.For this purpose we use TShark, the command line counterpart of Wireshark. Wireshark is a packet sniffing GUI application that captures and analyzes traffic that passes through the network interface card.

Frame type and subtypes

The data packets obtained during sniffing can be of three types: Management frames, Control frames and Data frames. The management frames are used to establish connection in the network.The management frames have the following subtypes: Assosiation Request, Assosiation Response, Reassosiation Request, Reassosiation Response, Probe request, Probe Response, Beacon, Announcement Traffic Indication Message(ATIM), Disassosiation, Authentication, Deauthenication and Action frames. A control frame helps with the delivery of data and management frames over the network. The subtypes of these frames are: Power Save(PS) Poll, Request to Send (RTS), Clear to send (CTS), Acknowledgement(ACK), Contention-Free(CF)-End (PCF only), CF-End+CF-ACK (PCF only), Block-ACK(HCF) and Block Ack Request(HCF) frames. The data frames carry the actual data.

Results and Analysis

To extract as much as information possible, the network traffic was captured at the University library on Friday (1/3/2018) from 11:20-12:20. And later the traffic was captured at home in the evening from 19:00-20:00. A python script was written to run TShark in monitor mode, capture the packets and save it as CSV file. The number of different frame types and its length were measured and a bar graph was plotted to give an overview of the frame distribution during the capture period.

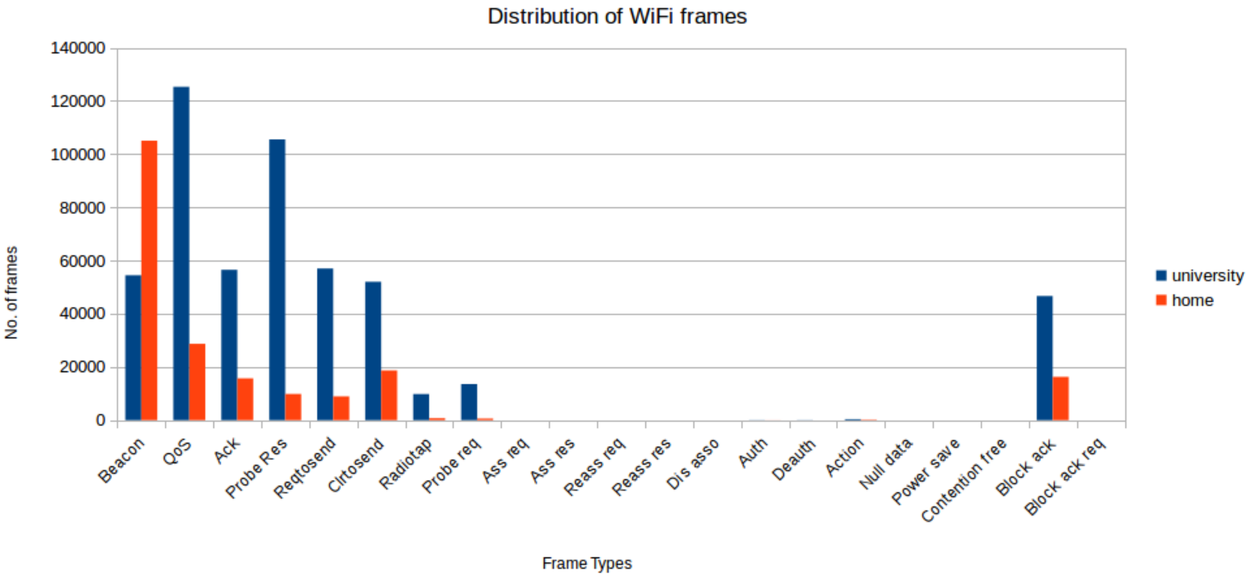

Figure 1: Frame Distribution

From the plot for university, we can see that the management frames mainly beacon, probe response and probe requests are 33% of the total frames captured. The data frames constitute only 24% of the frames while the control frames occupy 41.4%. Traffic captured at home shows that there is very little data transmission and increased number of beacon frames as compared to those captured at the university. At home, data is just 14% of the total frames whereas the management frames make up 56.4%. We can see that the management frames dominate the overhead. Radiotap headers though not part of the standard 802.11 frame format, provides additional information such as received signal level, current channel in use, etc. The overview of the number of frames along with the frame length is tabulated below for the home scenario.

Frame Type	**Frames**	**Size(Bytes)**
Data	28689	19166109
Control	59504	3299826
Ack	15706	785300
RTS	8897	498232
CTS	18663	933150
Block Ack	16238	1083144
PS Poll	0	0
Management	115668	35208232
Action	184	13312
Authentication	14	1123
Beacon	105029	31207652
Probe Request	610	85143
Probe Response	9831	3601002
Radiotap	708	142868

Table 1: Frame type and subtype breakdown(Home)

Conclusion

Overheads hinder the effectiveness of data transmission. The throughput of the network is degraded due to increased overhead transmission. For every SSID on the network, corresponding beacon frames are sent every second. Hence more the SSIDs, more airtime spent in the transmission of beacon frames. Due to increased overhead transmission, the channel capacity for the transmission of data frames is reduced significantly. One of the problems we encountered during traffic capture was that the WiFi kept disconnecting and reconnecting after a certain number of packets have been transmitted. This led to the increase in number of management frames which are responsible for nodes joining and leaving the network. Hence the total number of frames are dominated by the management frames thus hindering with the data transmission.