ET4394 Wireless Networking
Wireshark Report: Distribution of Frame Types
Group ALGG1

Alexios Lyrakis (4735811)
Georgios Giannakaras (4747046)

March 6, 2018

1 Introduction

During this project we had the opportunity to work with the most widely-used network protocol analyzers, Wireshark and Tshark. Our main goal was to make measurements and gather information about the wireless traffic, using the WIFI chips of our laptops, in various places. With the acquired data we plotted and observed the distribution of the involved frame types and other corresponding details for their transmission. In the second section of this report the methodology of work and plan of action are mentioned, in the third we refer to the main frame types and to some of the subtypes, while in the fourth one we describe the conducted experiments and present graphs of frame types distributions and comparisons between different cases.

2 Methodology of Work and Plan of Action

The experiments were conducted with the use of the WIFI chips of our laptops. For this to be accomplished the chips had to be set in 'monitor mode'. We worked on the operating system Kali Linux, which offers the ability of changing the mode of the WIFI chips. Here we have to mention that this is also possible with the use of Kali Linux with a live usb.

For every experiment before recording the traffic information we scanned for all the available Access Points and the corresponding channels. In every different case we chose the channel with the most APs featuring a strong transmitting signal. For the experiments that took place in different locations of the TUDelft campus we set the channel in which the AP 'eudoram' had the strongest signal.

While we initially used Wireshark to get familiar with a network protocol analyzer, we finally used Tshark for the experiments, because it was more handy into extracting specific information and compressing the total size of the final exported files. We managed a significant compression by exporting only the desired numbers in .txt files and by extracting the information with scripts written in Python. The scripts are available in Github. A file of one hour recorded data had approximately the size of 50mB. For every location we gathered the following information: the subtype of frames, their length, the corresponding data rate, their duration and their FCS status.

3 Frame Types and Subtypes

In this section we briefly mention and describe the three main frame types and the subtypes that most frequently occurred in our experiments, so we can assess the results and graphs in section 4. The main frame types are:

- Management Frames: They enable stations to establish and maintain communications, i.e. join and Leave the Basic Service Set.
- Control Frames: Control frames assist in the delivery of data frames. They administer access to the wireless medium (but not the medium itself) and provide MAC-layer reliability functions.
- Data Frames: Data frames carry higher-level protocol data in the frame body.

The most frequently observed management frame subtypes in our experiments are:

- Probe Request: Mobile stations use Probe Request frames to scan an area for existing 802.11 networks. In Active scanning, stations still go through each channel in turn, but instead of passively listening to the signals on that frequency, station send a Probe Request management frame asking what network is available on that channel.

- Probe Response: An access point will send out a probe response when it hears a probe request frame, either directed at the specific access point or to all stations in the area using the broadcast SSID, and the parameters are compatible.

- Beacon: It contains all the information about the network. Beacon frames are transmitted periodically, they serve to announce the presence of a wireless LAN and to synchronize the members of the service set. Beacon frames are transmitted by the access point (AP) in an infrastructure basic service set (BSS).

The most frequently observed control frame subtypes in our experiments are:

- RTS/CTS: It is possible for a client station to be able to communicate with an AP, but not able to hear or be heard by any of the other client stations. This will lead to possible collisions when a station transmits. RTS/CTS is a mechanism used to reduce frame collisions introduced by the hidden node problem and when is enabled on a STA, every time the STA wants to transmit a frame, it must perform RTS/CTS exchange prior to the normal data transmission.

- ACK: An acknowledgement is a signal passed between communicating computers, or devices to signify acknowledgement, or receipt of message, as part of a communications protocol.

- Block ACK: The Block Ack mechanism improves channel efficiency by aggregating several acknowledgments into one frame, and acknowledging with a single BA multiple frames.

The most frequently observed data frame subtypes in our experiments are:

- QOS Data: Data frames with a value of 1 in the QoS subfield of the Subtype field (Bit7) are collectively referred to as QoS data frames. A QoS STA always uses QoS data frames for data transmissions to other QoS STAs. The goal of QoS is to provide preferential delivery service for the applications that need it by ensuring sufficient bandwidth, controlling latency and jitter, and reducing data loss.

- Null Data: No data frame. In this case this frame is used to indicate that client is going to Power Save mode. This frame is sent to the AP by the client.

4 Experimental Results and Conclusions

In figure 1 the total distribution of frame types of all the conducted experiments is presented. In total 25 hours of wireless traffic was recorded in six different places, which are two dorms, the TUDelft Library, EWI, 3mE building and a Cafe in Rotterdam. The experiments took place in various hours along the days.

As we notice the biggest amount of frames consists of management frames. As we expected the most frequently shown frames are the Probe Request, Probe Response and Beacons, which are used for establishing a wireless connection between a client and an AP. Also, we notice that the expected frame types, Block ACK, RTS/CTS and ACK occupy the largest part of control frames. The significant amount of RTS/CTS frames implies that most of the stations had the RTS/CTS mechanism enabled. A worth mentioning point is that the majority of data frames consists of QoS Data and not Data. This indicates that most of STAs support the QoS feature for preferential delivery service and uses it for data transmission.

In figure 2 a comparison between our recorded data (left table) and the data from [1] (right table) is presented.We observe that in both cases the results are quite similar in proportions.The amount of frames in a decreasing order is management, control and finally data types. Furthermore, we notice that in both tables the data frames have the majority of bytes, followed by the management and control frames. Finally, we see a similar pattern also for the average data rates.

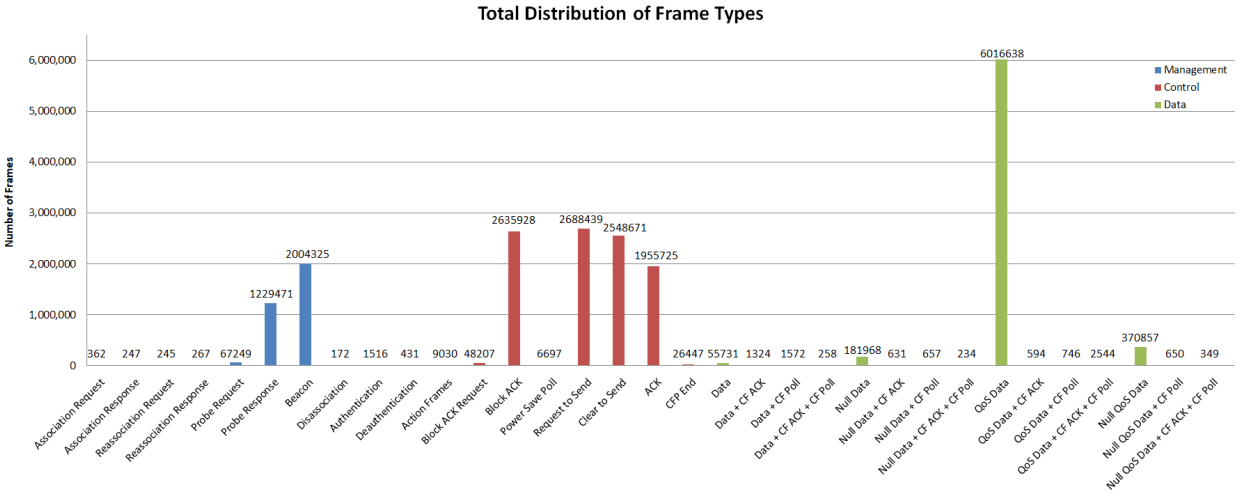

Figure 1: Total distribution of frame types of all the conducted experiments.

Frame Type	Management	Control	Data
Number of Frames	3313315	9910114	6634753
Min Length (Bytes)	78	62	76
Max Length (Bytes)	3326	88	4150
Average Length (Bytes)	339.04	76.47	928.24
Min Data Rate (Mb/s)	1	1	1
Max Data Rate (Mb/s)	48	54	173.33
Average Data Rate (Mb/s)	10.02	22.2	73.64
Min Duration (μs)	32	24	28
Max Duration (μs)	3808	448	12624
Average Duration (μs)	1593.2	34.09	240.78
Status: Good	3313315	9910114	5133389
Status: Bad	0	0	1501364

Frame type and subtype	Airtime (secs)	Bits (MB)	Frames (1000s)	Avg. Rate (Mbps)
Data	6802	1884	5540	6.46
Originals	3616	1276	3988	7.30
Retransmits	3185	608	1552	4.31
Control	1418	74	5442	1.89
Ack.	1332	69	5135	1.90
RTS	42	3	142	1.69
CTS	40	2	155	1.75
PS poll	2	0	10	1.60
Management	878	82	1098	1.12
Assoc. Req.	1	0	2	1.42
Assoc. Res.	1	0	3	1.08
Authentication	6	0	13	1.13
Beacon frame	412	39	428	1.00
Deauth.	0	0	0	1.30
Dissassoc.	6	0.40	13794	1.00
Probe Req.	177	16.07	333707	1.35
Probe Res.	270	25.44	296250	1.00
Reassoc. Req.	0	0.03	2727	1.00
Reassoc. Res.	0	0.03	621	1.00
Totals	9098	2040	12080	3.92

Figure 2: The left table lists information for the main frame types of the conducted experiments. The right table is taken from [1], lists similar information and is presented for comparison purpose.

In the following experiments we observe the same frequently occurred frame subtypes as the total distribution in figure 1. Despite the similarities among them, the depicted distributions for each experiment depend also on the corresponding conditions and the utilization of the network while we were recording the wireless traffic. All the following wireless traffic recordings were executed for 1 hour long each.

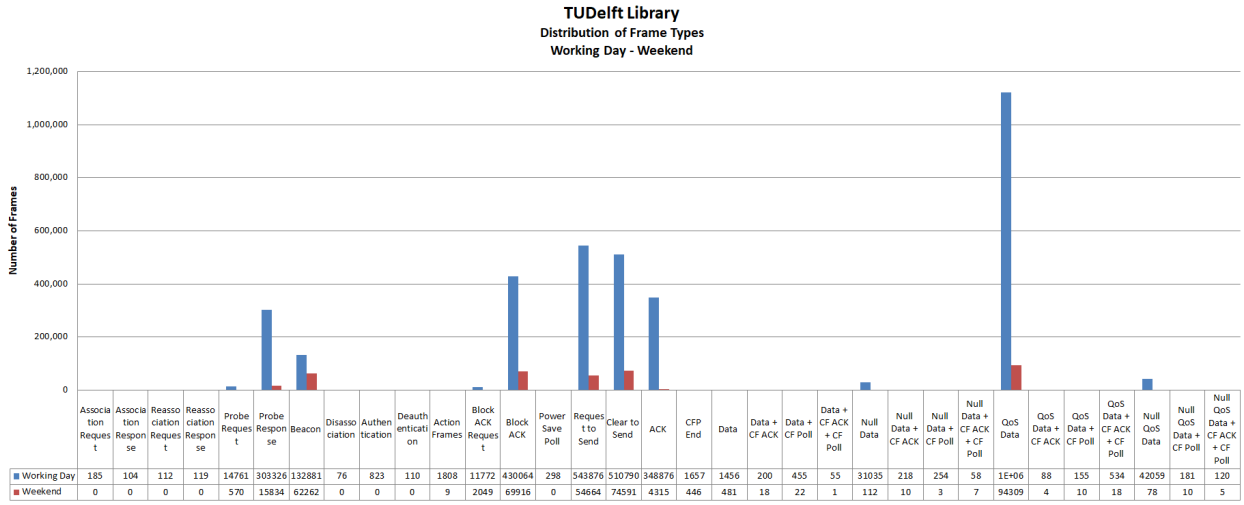

Figure 3: Frame types distribution in TUDelft library on a working day and on a weekend day.

In figure 3 we notice that during a working day in TUDelft library there is much more wireless traffic than during a weekend day. In figure 4 we observe that in the midday there is more intense traffic in contrast to after midnight hours, as expected. Finally, in figure 5 is depicted that in both 3mE and EWI buildings similar frame type distributions takes place in midday, while in EWI a significantly more intense wireless traffic is observed.

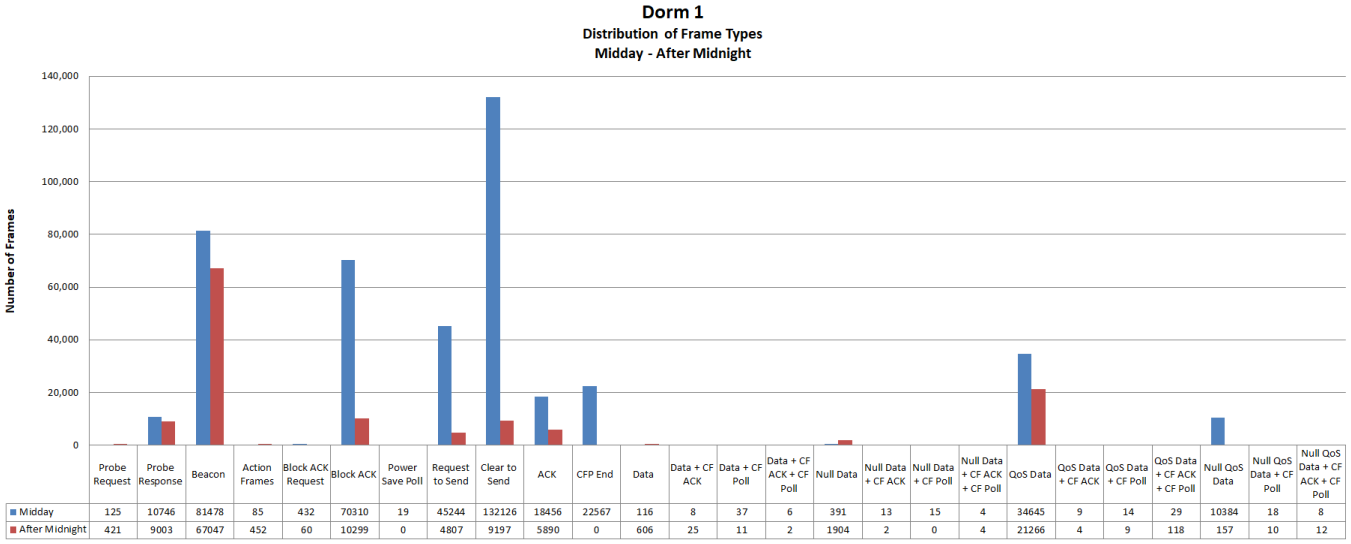

Figure 4: Total distribution of frame types in a dorm during midday and after midnight.

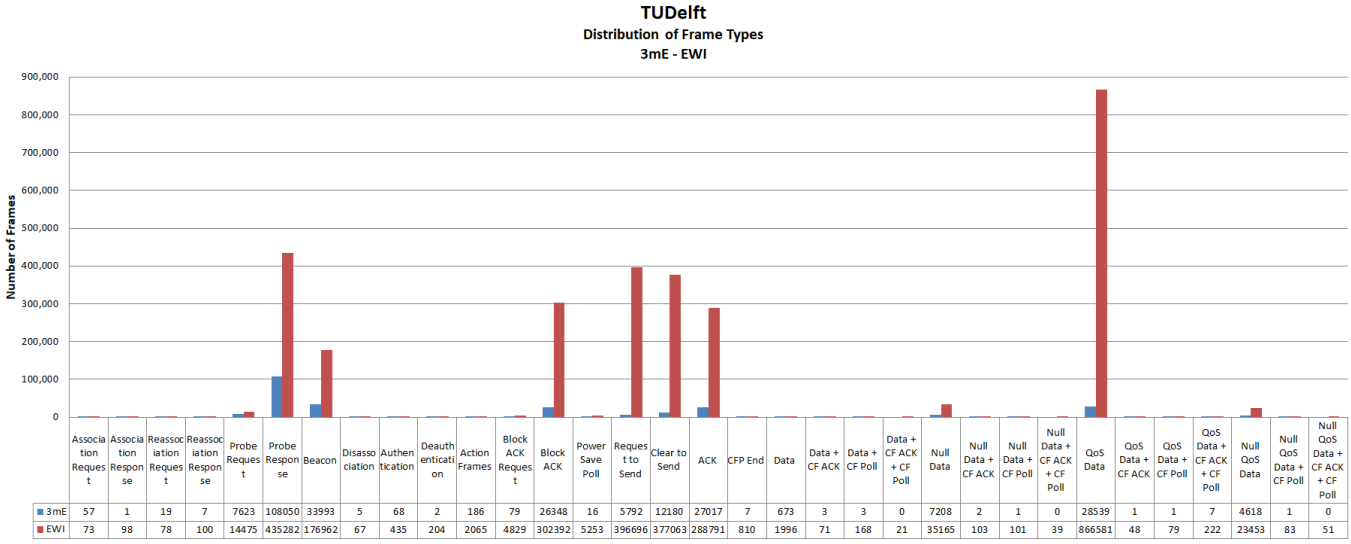

Figure 5: Total distribution of frame types in 3mE and EWI buildings in midday.

References

[1] Rodrig et al. Measurement-based Characterization of 802.11 in a Hotspot Setting, ACM SIGCOMM'05 Workshop, Aug. 22–26, 2005, Philadelphia, PA, USA