

ET4394 Wireless Networking

Experimental Evaluation of Interference Impact on WiFi Packet corruption

by

Group Name: JMDB

Anup Bhattacharjee	4738845	A.K.Bhattacharjee@student.tudelft.nl
Rahul Vyas	4747798	r.r.vyas@student.tudelft.nl

Contents

1	Theory	2
2	Objectives.	2
3	Relating RSSI and CRC errors	3
4	Results	3
	4.1 CASE 1:	3
	4.2 CASE 2:	3
	4.3 CASE 3:	3
5	Conclusion	4
6	Figures	4

1. Theory

Cyclic Redundancy Check (CRC) is used to indicate whether the received data is valid or not. In our project we have used Field Check Sum (FCS), which is the data link layer implementation of CRC. The errors on the receiver side packets are generally indicated by a term called bit error rate (BER), which defines the number of errors in our data packets (headers inclusive), hence implying the probability of having error bits in received packets. BER improves depending on the coding used. In case of CRC,

$$BER_{CRC8} > BER_{CRC16} > BER_{CRC32} > BER_{CRC64}$$

In all the readings that have been taken, CRC32 is used (inferred from the 32bit hex FCS field). This can be seen in Fig. 1,

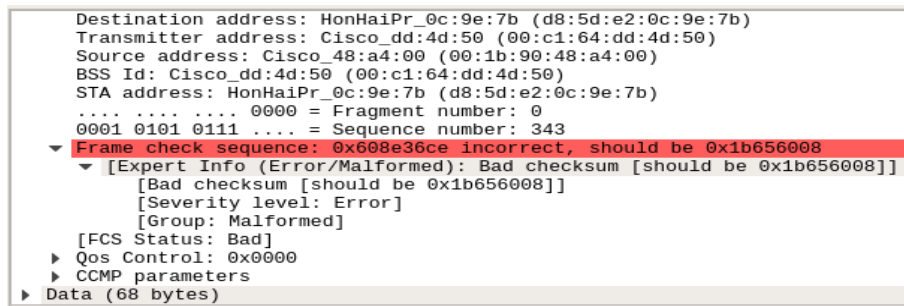


Figure 1: CRC Length

It should also be noted that the obtained values and the obtainable values will strictly depend on the Network Interface Card being used.

2. Objectives

The aim of this project is to show the inter relation between interference and packet corruption of WiFi packets in real life scenarios. To fulfill this purpose, Wireshark, tshark are used for packet sniffing. Bash script is used for automating the whole process of packet collection and processing. MATLAB has been used for processing the data obtained into meaningful insights.

The Fig.2 shows a bad FCS packet with relevant information such as Signal strength (RSSI),

No.	Time	Source	Destination	Protocol	Length	Info	RSSI	Channel	Data rate
1549	3.114227433	Cisco_dd:4d:50 (00:c1:64:dd:4d:50)	HonHaiPr_0c:9e:7b (d8:5d:e2:0c:9e:7b)	802.11	46	Request-to-send, Flags=.....C	-31 dBm		1.24
1550	3.114232321	Cisco_dd:4d:50 (00:c1:64:dd:4d:50)	HonHaiPr_0c:9e:7b (d8:5d:e2:0c:9e:7b)	802.11	151	QoS Data, SN=1543, FN=0, Flags=p....F..	-25 dBm		1.1
1551	3.114248974	Cisco_48:a4:00 (00:1b:90:48:a4:00)	HonHaiPr_0c:9e:7b (d8:5d:e2:0c:9e:7b)	802.11	120	QoS Data, SN=1543, FN=0, Flags=p....F..	-25 dBm		1.1
1552	3.115541842	Cisco_dd:4d:50 (00:c1:64:dd:4d:50)	Broadcast	802.11	307	Beacon frame, SN=1690, FN=0, Flags=.....C	-32 dBm		1.24
1553	3.115561884	Cisco_dd:4d:50 (00:c1:64:dd:4d:50)	HonHaiPr_0c:9e:7b (d8:5d:e2:0c:9e:7b)	802.11	58	802.11 Block Ack, Flags=.....C	-31 dBm		1.24
1554	3.115570811	HonHaiPr_0c:9e:7b (d8:5d:e2:0c:9e:7b)	All-MSRP-routers_...	802.11	93	QoS Data, SN=485, FN=0, Flags=p....T			
1555	3.115573365	HonHaiPr_0c:9e:7b (d8:5d:e2:0c:9e:7b)	All-MSRP-routers_...	802.11	93	QoS Data, SN=486, FN=0, Flags=p....T			
1556	3.116320821	Cisco_dd:4d:50 (00:c1:64:dd:4d:50)	HonHaiPr_0c:9e:7b (d8:5d:e2:0c:9e:7b)	802.11	58	802.11 Block Ack, Flags=.....C	-31 dBm		1.24
1557	3.122175135	Cisco_dd:4d:50 (00:c1:64:dd:4d:50)	HonHaiPr_0c:9e:7b (d8:5d:e2:0c:9e:7b)	802.11	46	Request-to-send, Flags=.....C	-30 dBm		1.24
1558	3.122193919	Cisco_48:a4:00 (00:1b:90:48:a4:00)	HonHaiPr_0c:9e:7b (d8:5d:e2:0c:9e:7b)	802.11	120	QoS Data, SN=1544, FN=0, Flags=p....F..	-25 dBm		1.1
1559	3.135951977	Cisco_27:d3:70 (00:13:72:d3:70)	Broadcast	802.11	297	Beacon frame, SN=2747, FN=0, Flags=.....C	-60 dBm		1.24
1560	3.148808774	HonHaiPr_ca:d4:d5 (00:0c:29:d4:d5)	Cisco_dd:4d:50 (00:c1:64:dd:4d:50)	802.11	46	Request-to-send, Flags=.....C	-23 dBm		1.24

Frame 1550: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits) on interface 0
Ethernet II Header, Length 26
802.11 radio information
PHY type: 802.11b (4)
Short preamble: False
Data rate: 1.0 Mb/s
Channel: 1
Frequency: 2412MHz
Signal strength (dBm): -25dBm
TSF timestamp: 2184195329
[Duration: 1192us]
IEEE 802.11 QoS Data, Flags: p....F..
Type/Subtype: QoS Data (0x0028)
Frame Control Field: 0x8842
000000000100000 = Duration: 48 microseconds
Receiver address: HonHaiPr_0c:9e:7b (d8:5d:e2:0c:9e:7b)
Destination address: HonHaiPr_0c:9e:7b (d8:5d:e2:0c:9e:7b)
Transmitter address: Cisco_dd:4d:50 (00:c1:64:dd:4d:50)
Source address: Cisco_48:a4:00 (00:1b:90:48:a4:00)
BSS Id: Cisco_dd:4d:50 (00:c1:64:dd:4d:50)
STA address: HonHaiPr_0c:9e:7b (d8:5d:e2:0c:9e:7b)
... .. 0000 = Fragment number: 0
0110 0000 0110 ... = Sequence number: 1542
Frame check sequence: 0x32a7a821 incorrect, should be 0x78413ba5
[FCS Status: Bad]

Figure 2: Wireshark GUI with error packet selected

3. Relating RSSI and CRC errors

RSSI - Received Signal Strength indicator($Signallevel + Noiselevel$) represents the signal strength calculated by the network card at particular frequency band. In our analysis we use RSSI values as representation of interference in the specific frequency band. We represent the corrupted packets whose FCS is corrupted.

4. Results

4.1. CASE 1:

Case 1 shows the results of experimentation conducted at home and Delft station (at night).

This case represents two scenarios with low interference. In fig.3 (blue - good packets, Red - corrupted Packets), the plots show the corruption of packets w.r.t to RSSI over 15 minutes time period. Both the plots indicate that the chances of packet loss increases with increase in RSSI values i.e increase in interference, while in the second plot the interference leads to packet corruption (red marks) in the beginning. This is being caused by us with the help of a mobile which is later removed(WiFi switched off on mobile) and the effect is seen with improve in good packets (blue marks).

4.2. CASE 2:

Case 2 shows the results of experimentation conducted at Aula centre TU Delft in evening when there are lots of people nearby, leading to high interference. Hence, with increasing interference (increasing RSSI), the probability or the chances of packet being corrupted increases(BER will increase) which can be clearly seen in the stacked bar graph of fig.4 and fig.5 . Both the figures represent the same scenario but the network cards used for reception of WiFi signals are different, which causes varied results.

4.3. CASE 3:

Case 3 shows the results of experimentation conducted at study centre. In the beginning there are few students but later on lots of students enter the area, leading to high increase in interference levels. This can be seen in fig.6.

5. Conclusion

The above results clearly show the relation between Chances of Packet corruption w.r.t interference indicating that the chances of a WiFi packet being corrupted increases with increase in RSSI levels.

6. Figures

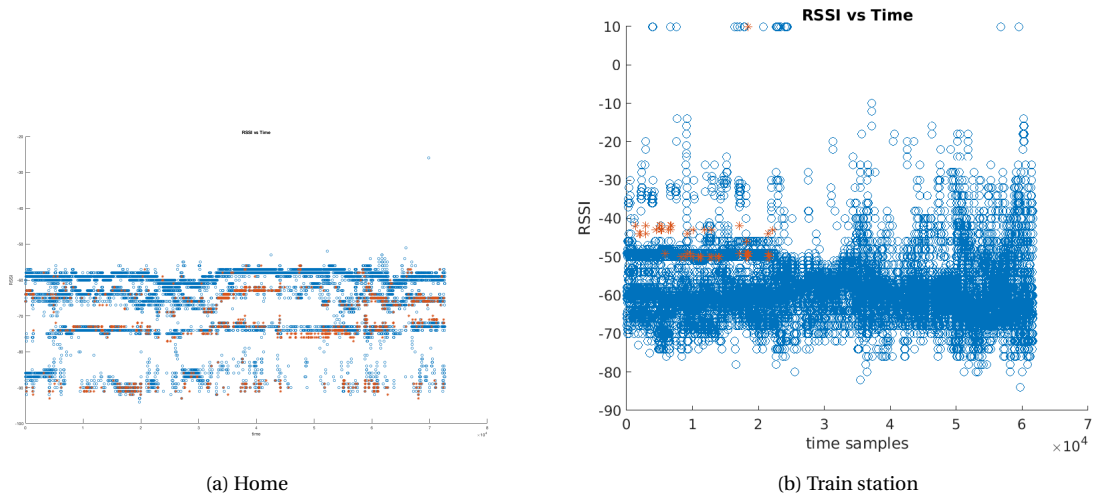


Figure 3: Scenario: Home(AirPort) and Train Station(RTL8723BE)

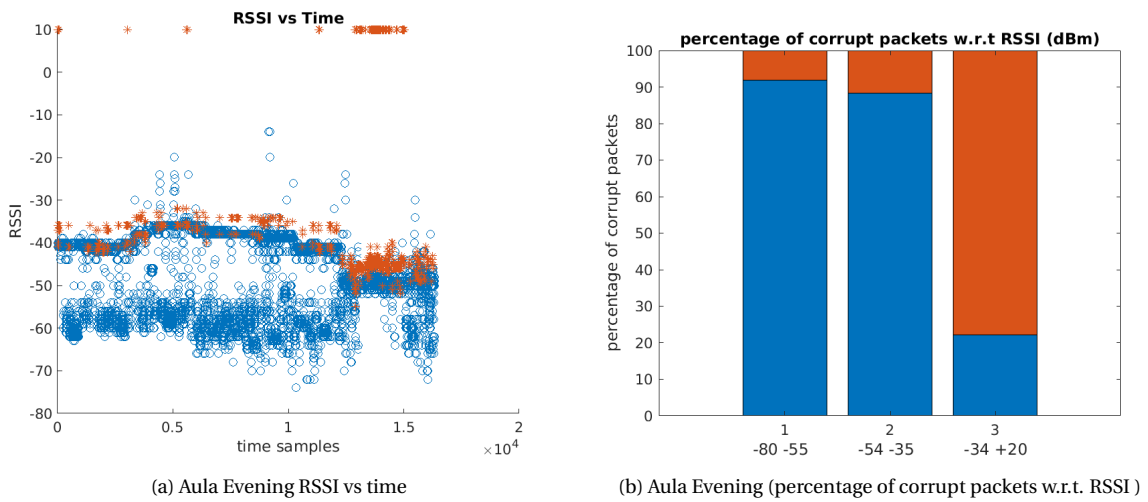
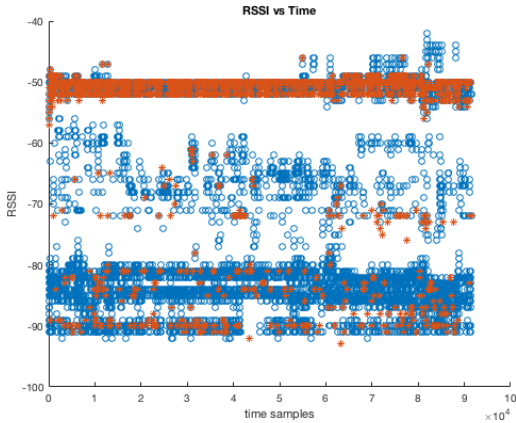
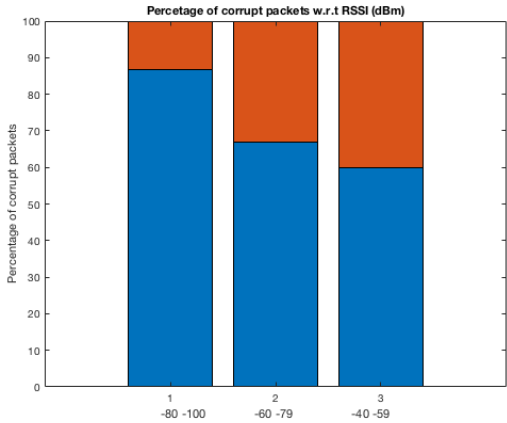


Figure 4: Scenario: Aula Evening (RTL8723BE)

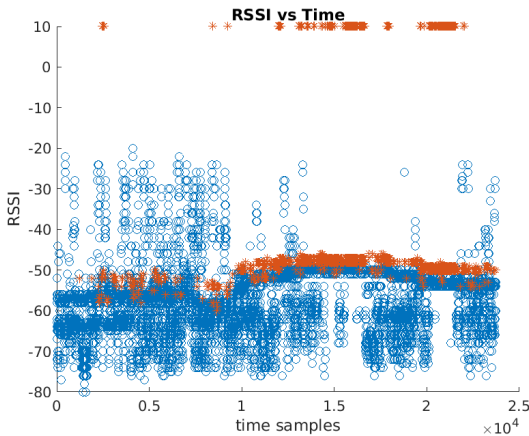


(a) Aula Evening RSSI vs time

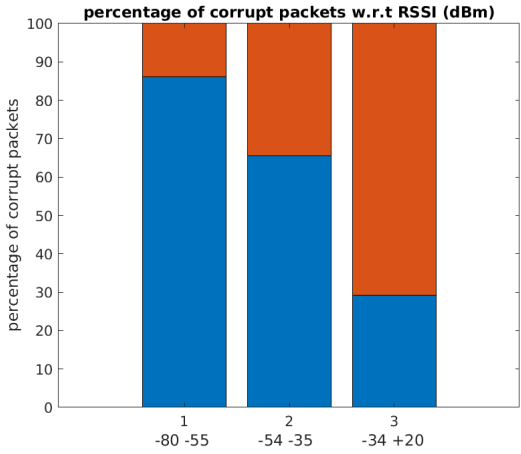


(b) Aula Evening (percentage of corrupt packets w.r.t. RSSI)

Figure 5: Scenario: Aula Evening (AirPort)



(a) Two People RSSI vs time



(b) Two People (percentage of corrupt packets w.r.t. RSSI)

Figure 6: Scenario: Two People (RTL8723BE)