CS5553: Wireless Network & Security

Assignment 2: Hands-on with Wi-Fi (Part-A)

Ganesh Vernekar - CS15BTECH11018

Questions from Wireshark_802.11_v7.0.pdf

1. 30 Munroe St, linksys12

2. 0.1024 sec for both linksys_SES_24086 and 30 Munroe St.

3. Source address: 00:16:b6:f7:1d:51

4. Destination address: ff:ff:ff:ff:ff:ff (its a broadcast)

5. BSS ID: 00:16:b6:f7:1d:51

6. Supported Rates: 1, 2, 5.5, 11 [Mbit/sec]
Extended Supported Rates: 6, 9, 12, 18, 24, 36, 48, 54 [Mbit/sec]

7. SYN sent from wireless host to the server.

Packet Info:
Packet No. 474, time=24.811093,
192.168.1.109->128.119.245.12, TCP,
length=110 B, PORT 2538->80,
Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1

Wireless host: 00:13:02:d1:b6:4f (Transmitter)
Access Point: 00:16:b6:f7:1d:51 (Receiver)
First Hop Router: 00:16:b6:f4:eb:a8 (Destination)

Wireless host IP: 192.168.1.109
Destination IP: 128.119.245.12

Destination IP corresponds to the *actual server* which is serving the file alice.txt.

8. SYNACK sent from server to the wireless host.

Packet Info:
Packet No. 476, time=24.827751,

128.119.245.12->192.168.1.109, TCP,
length=110 B, 80->2538,
Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1

Wireless host: 91:2a:b0:49:b6:4f (Destination/Receiver)
Access Point: 00:16:b6:f7:1d:51 (Transmitter)
First Hop Router: 00:16:b6:f4:eb:a8 (Source)

FCS was wrong, hence there must error in Wireless Host MAC address if we compare it with other frames.

No, Sender MAC address (Transmitter) corresponds to the Access Point. IP address corresponds to the actual server whose MAC address is not there in the frame.

9. DHCP Release (Packet 1733) and Deauthentication (Packet 1735).

What feels missing is Disassociation frame.

10. 6 Authentication message sent to linksys_ses_24086 starting at around t=49 (Packet 1740,1741,1742,1744,1746,1749).

11. It requires a key.

12. No

13. Host sends AUTHENTICATION frames at t=63.168087 (Packet 2156) and t=63.169707 (Packet 2160).
It receives reply AUTHENTICATION from AP at t=63.169071 (Packet 2158) and t=63.170692 (Packet 2164)

14. ASSOCIATION REQUEST: t=63.169910 (Packet 2162)
ASSOCIATION RESPONSE: t=63.192101 (Packet 2166)

15. Host supports:
1, 2, 5.5, 11, 6, 9, 12, 18 [Mbit/sec]
Extended: 24, 36, 48, 54 [Mbit/sec]

AP supports:
1, 2, 5.5, 11 [Mbit/sec]
Extended: 6, 9, 12, 18, 24, 36, 48, 54 [Mbit/sec]

16. Probe Request:

It is a broadcast message. Hence receiver and BSS ID are ff:ff:ff:ff:ff:ff. Whereas the sender MAC address is that of the host which is broadcasting.

Probe Response:

It is a message from AP to Host. Hence receiver MAC address is that of the Host. The packets originates from AP, hence sender and BSS ID MAC address are that of AP.

These packets are used in *Active Scanning* to join a wireless network. The host broadcasts *Probe Request* saying that it wants to know all the AP present in the network. And all the APs which receive this message responds as *Probe Response* containing its info.

From the Doc

TRACE 2 was taken in mess during lunch, for Channel 11 of 2.4GHz spectrum.
(All values are from the script and not from wireshark, hence no screenshots)

a.

Main Type

There were 5 packets with Unknown type (unused *11*) in Trace 1. Maybe due to corruption of packet.

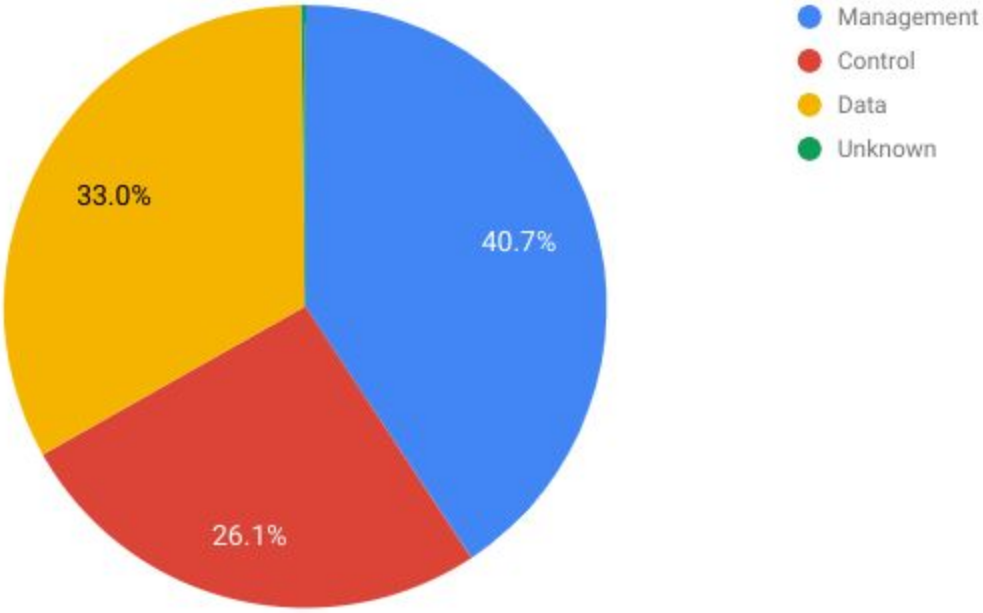
Trace 1:

Total: 2,364
Management: 962
Control: 617
Data: 779

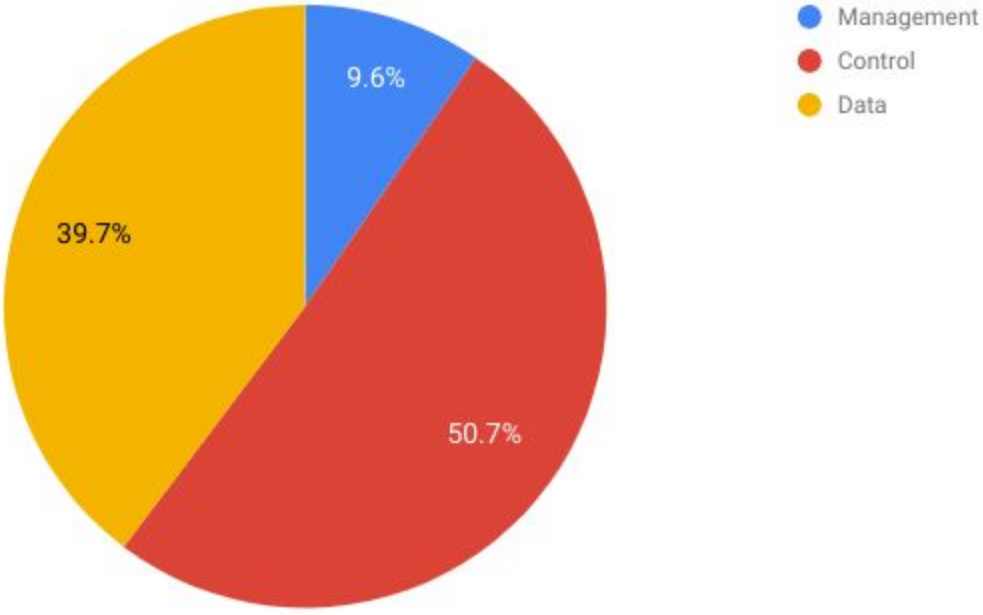
Trace 2:

Total: 1,222,842
Management: 117,280
Control: 620,038
Data: 485,524

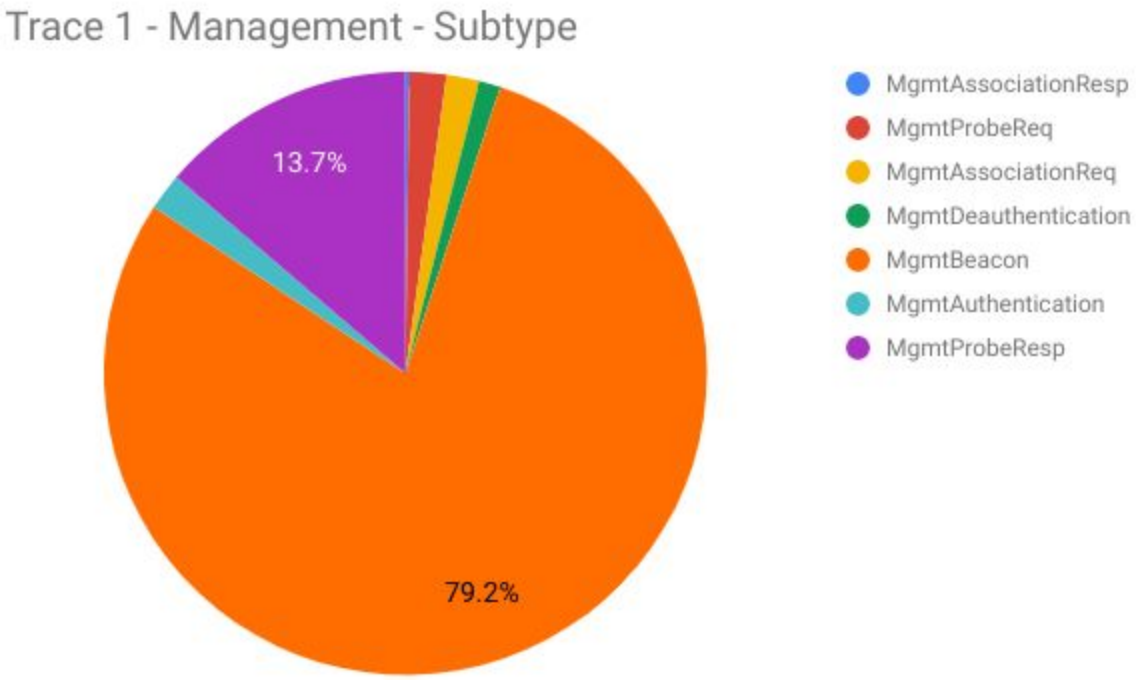
Trace 1 - Type Division

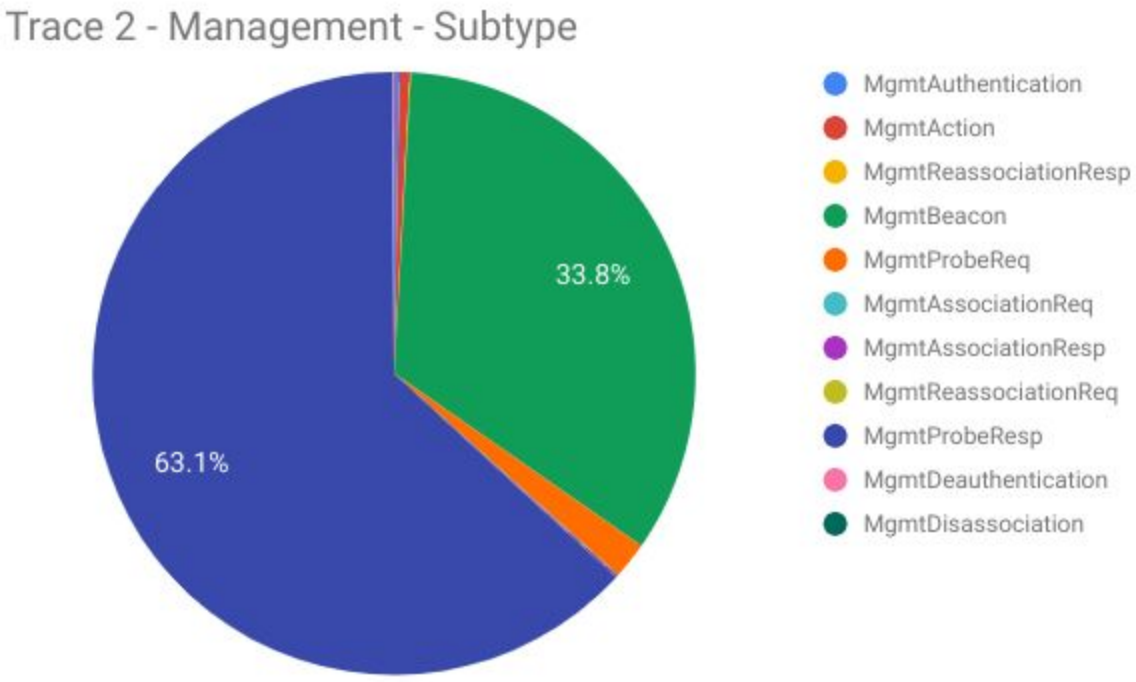


Trace 2 - Type Division

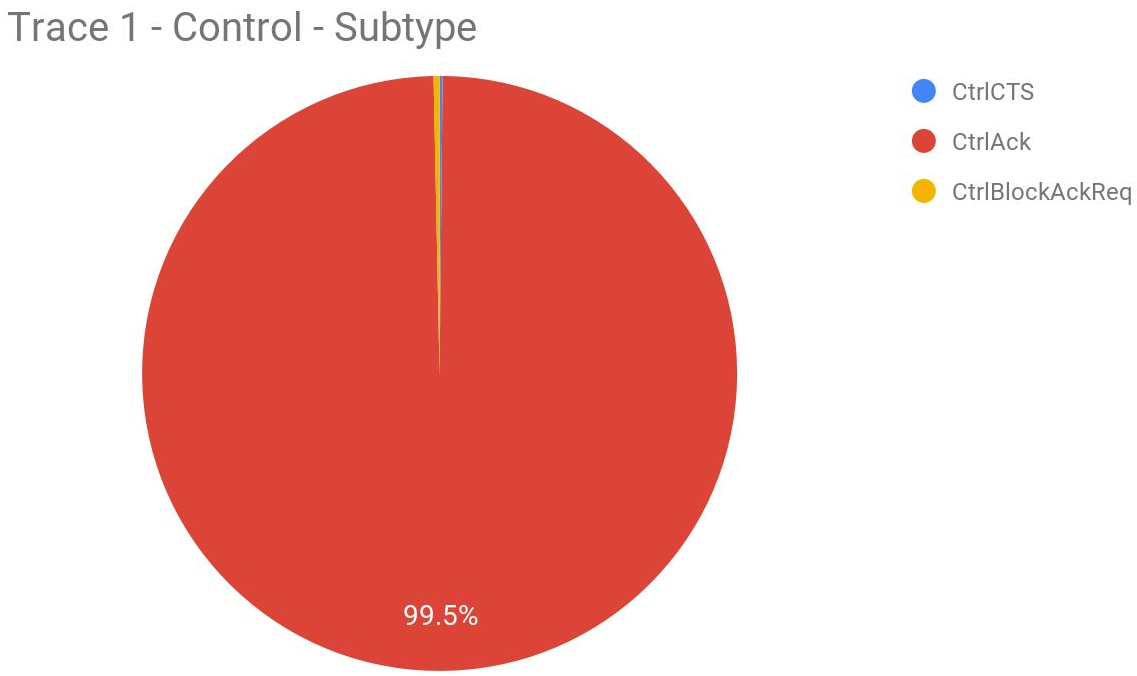


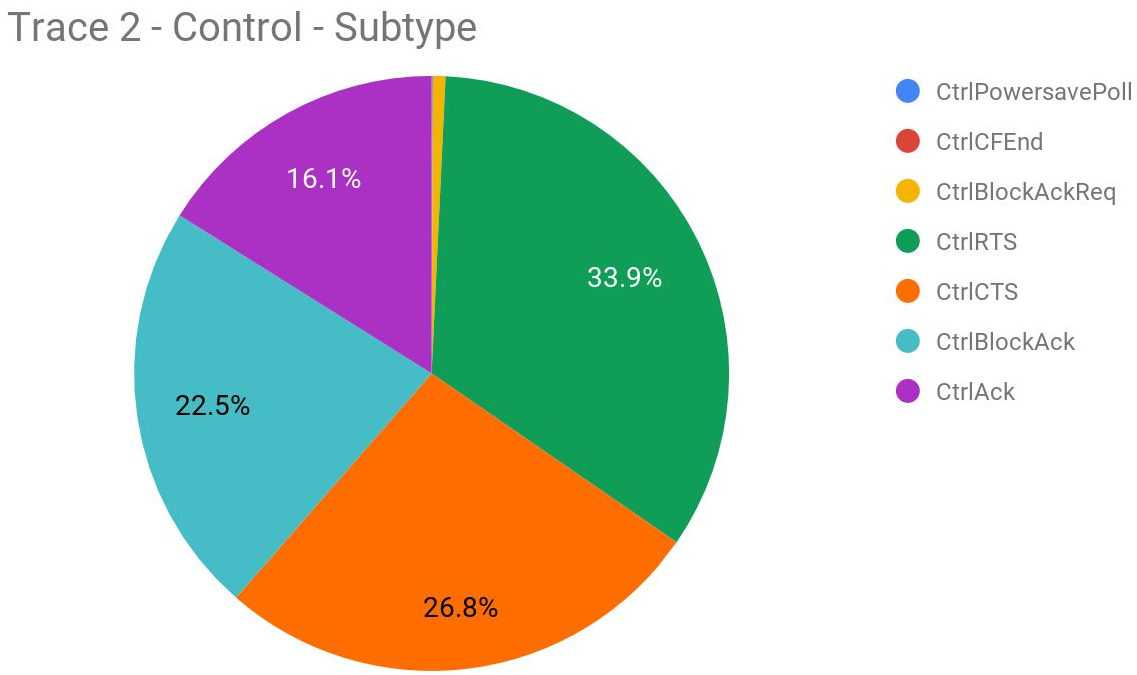
Subtype - Management





Subtype - Control





b.

(2) is the number of unique MAC addresses of AP (and not unique SSID, as SSID can be shared by multiple AP)

Trace 1

1. Management - 40.7%
2. 10
3. 54 Bytes (including the frame headers)
4. 8

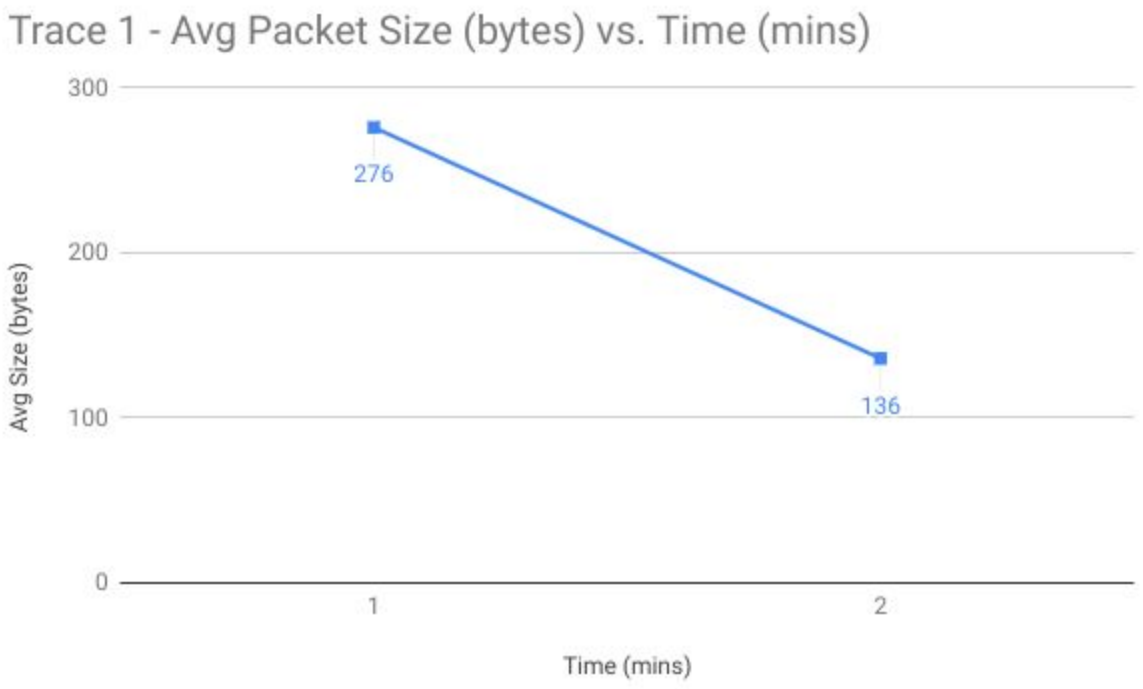
Trace 2

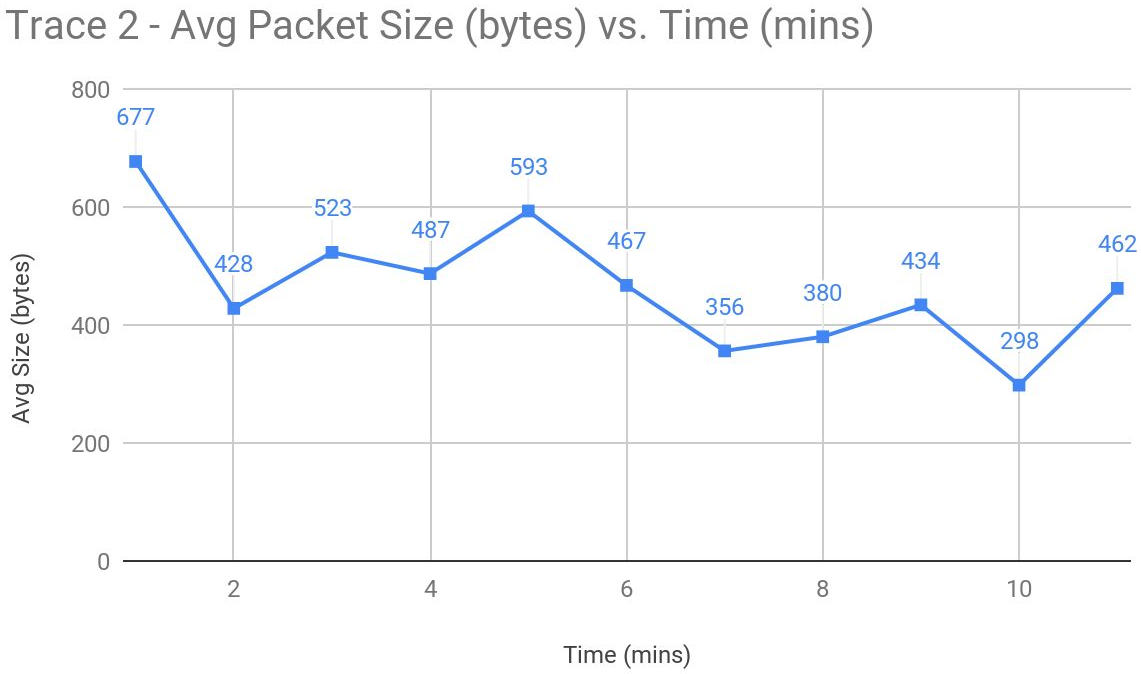
1. Control - 50.7%
2. 16
3. 78 Bytes (including the frame headers)
4. 238387

d.

NOTE: (1) As Trace 1 spanned only for ~74s, observations can be imprecise.
(2) Plot for Trace is not for entire 2 mins, the values for T=2min corresponds to 60s-74s.

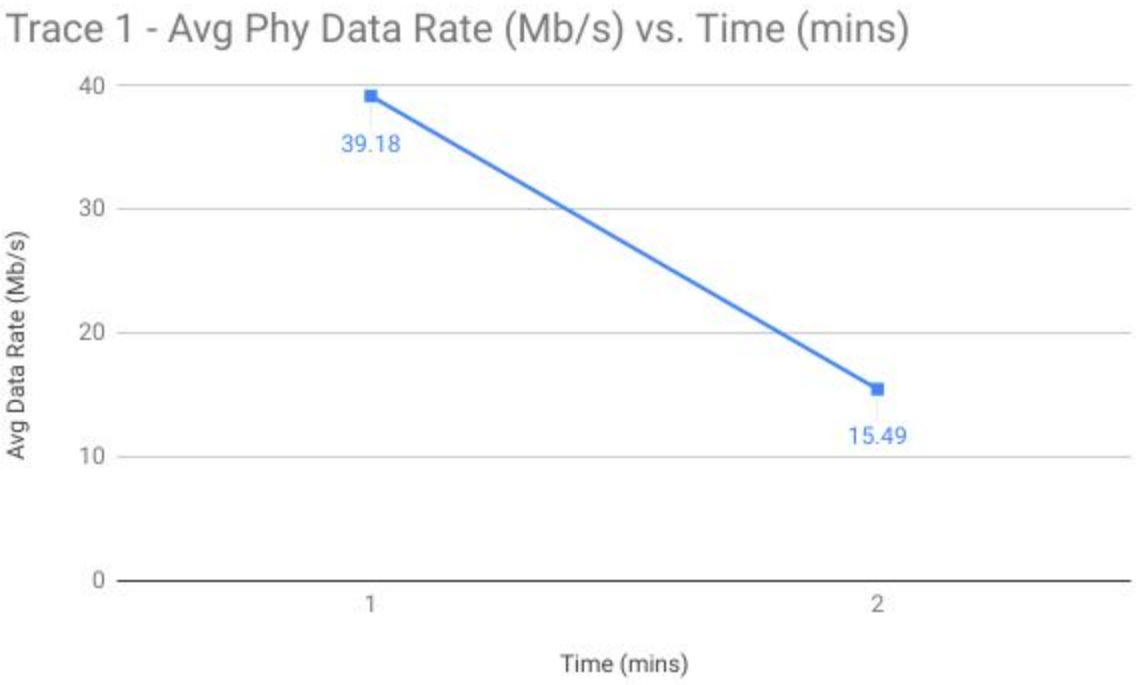
Avg packet size vs Time (1-minute resolution)

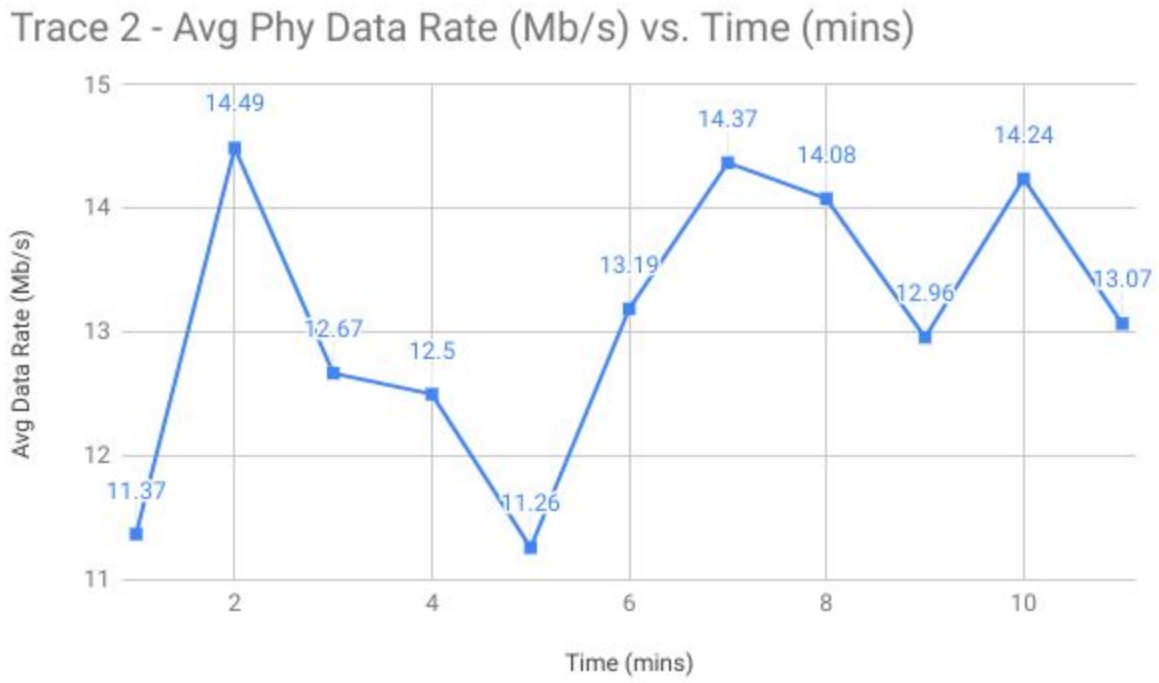




Observation: There were lot more data packets in Trace 2 compared to Trace 1. Hence the size of packets in Trace 2 were a bit higher.
Also in both Traces, bigger packets were being sent in the beginning of monitoring.

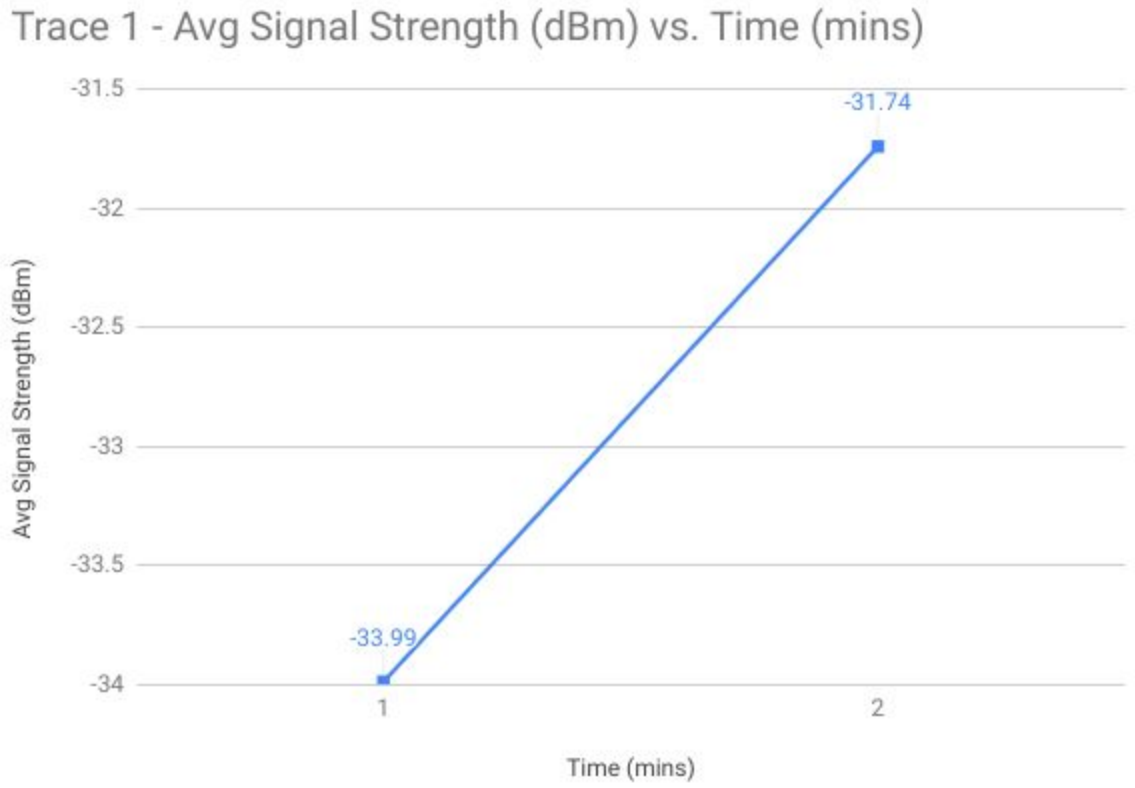
Avg PHY Data rate vs Time (1-minute resolution)

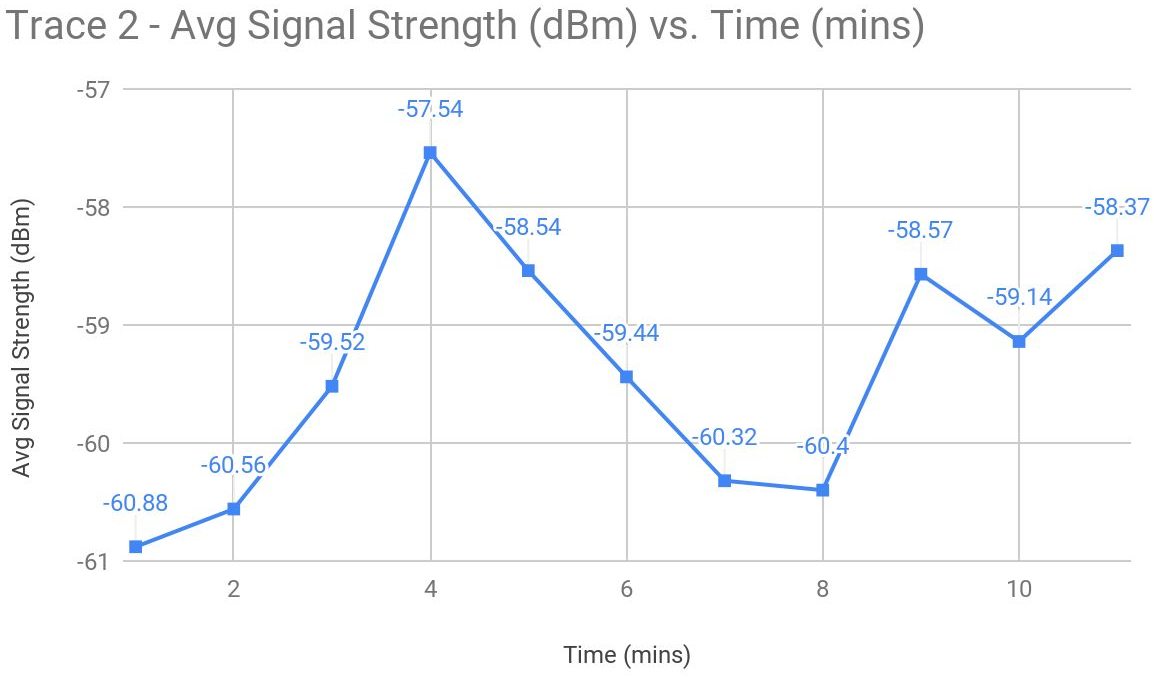




Observation: Lots of data was sent in the first 1 minute of Trace 1. Also as number of packets per minute was very high for Trace 2 compared to Trace 1, we can infer that there was lot of noise in Trace 2, which might have led to decrease of data rate.
It can be also possible that lots of AP in Trace 2 were running in mixed mode, and many devices with lower capacity, hence decreased rate.

RSSI (received signal strength) vs Time (1-minute resolution)

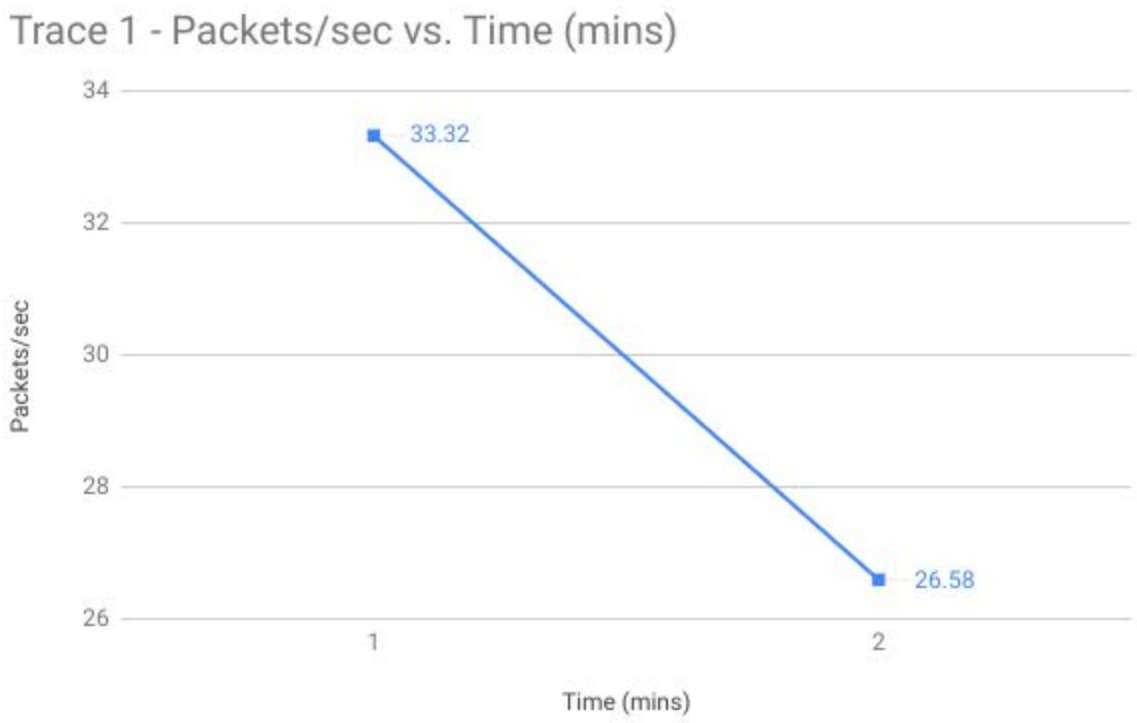


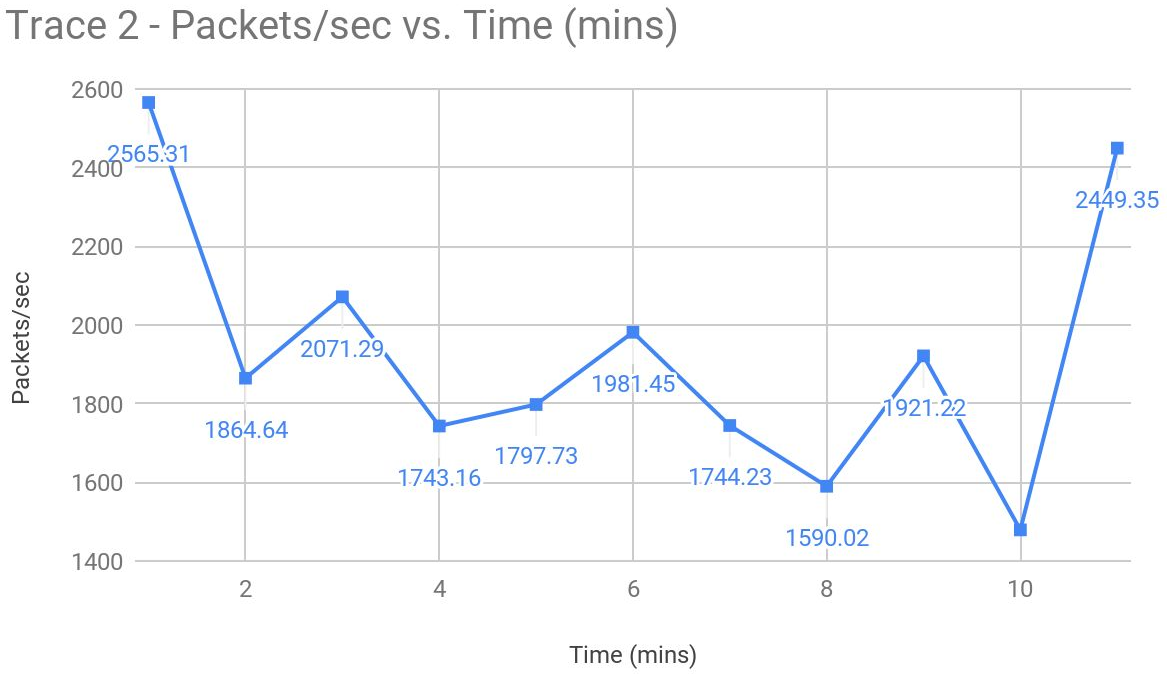


Observation: Very low signal strength in Trace 2 compared to Trace 1. It might be the case that in Trace 1 the distance between AP and host was less, also with less obstacles. The distance and obstacles in mess might have caused effective lowering of average power.

The fluctuation in strength was similar (2-3 dBm).

Packet rate (pkts/sec) vs Time (1-minute resolution)

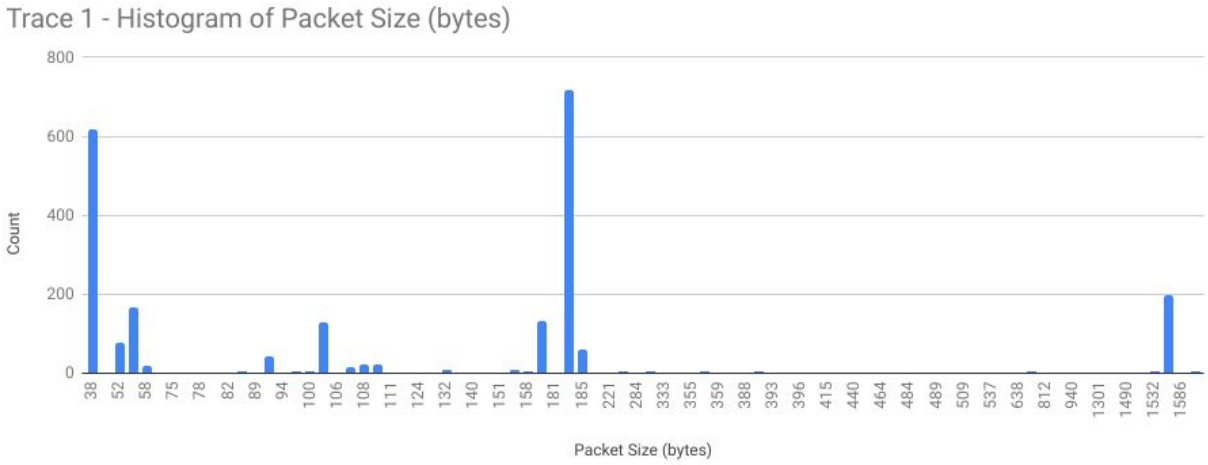




Observation: Both traces had burst of packets in the first minute, later dropped. Though Trace 2 had a burst of packets at the end too. Relating this graph with Packet Size graph, we can infer that most of the data packets in Trace 2 were in the beginning and the end of sniffing (considering *Size x Packets*).

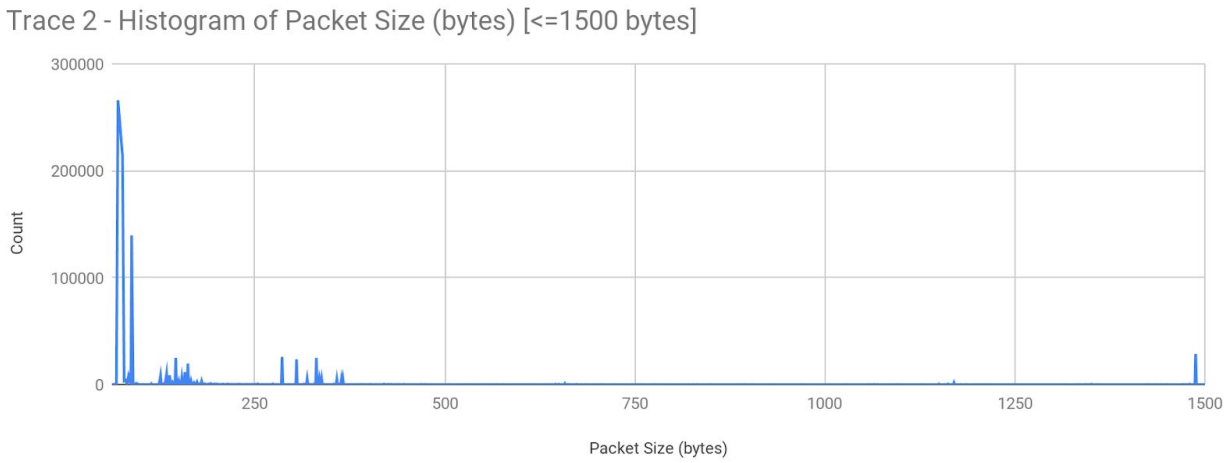
e.

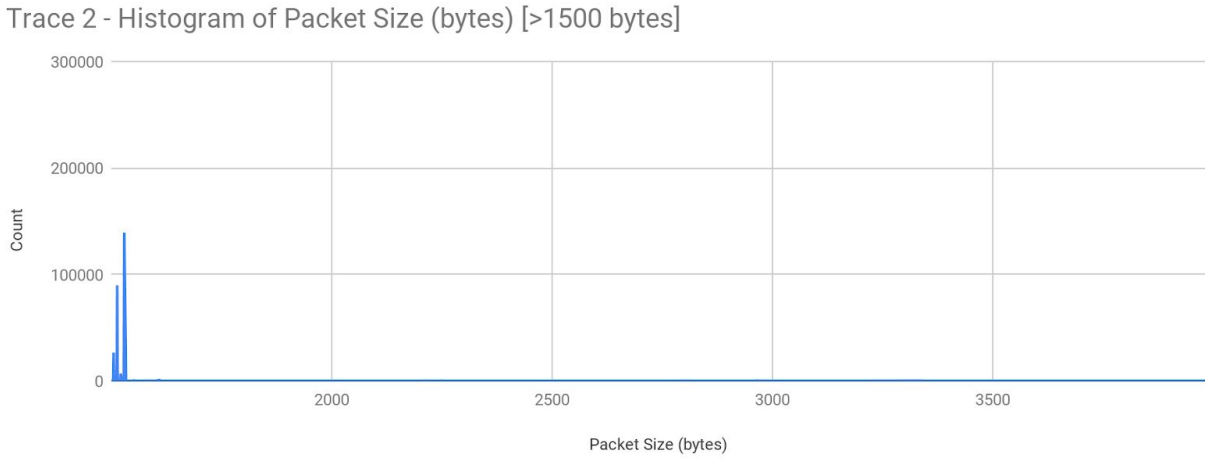
Histogram of Packet Size



Observation: Lots of small sized packets (30-60B) would the control and management packets, especially ACKs, and lots of mid-sized packets (150-200B) are Beacons, Probe, some data packets etc. There are some bigger size packets (1500B+) which will be the data packets. Hence there is a lot of traffic of small size packets than large size packets.

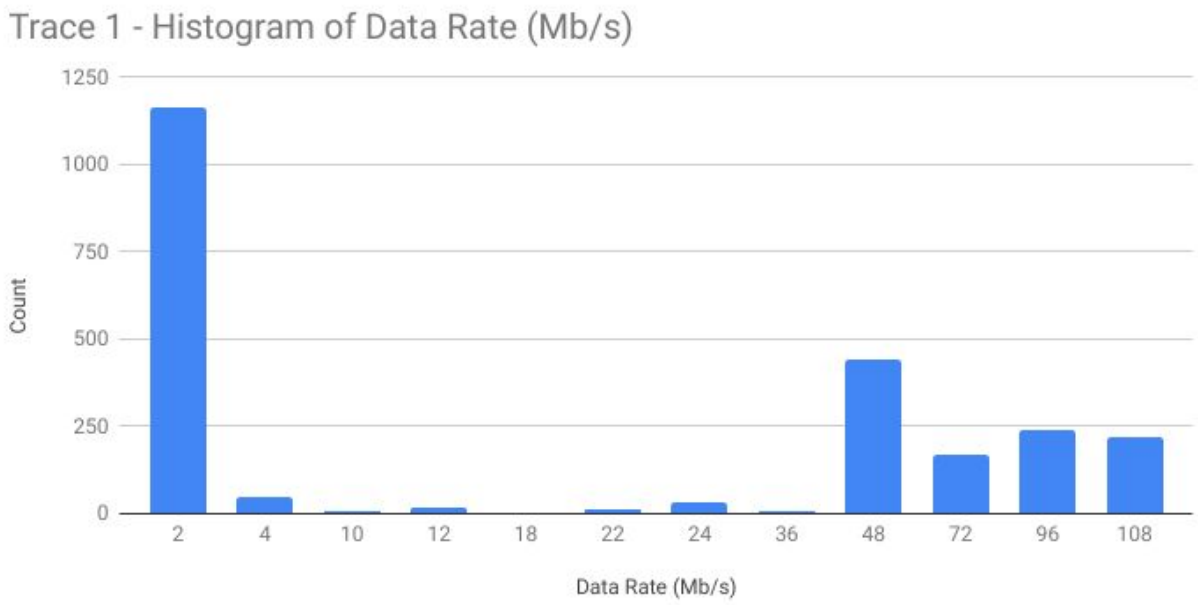
Range of histogram for Trace 2 was very wide, hence its broken into 2 parts (<=1500 bytes, >1500 bytes)



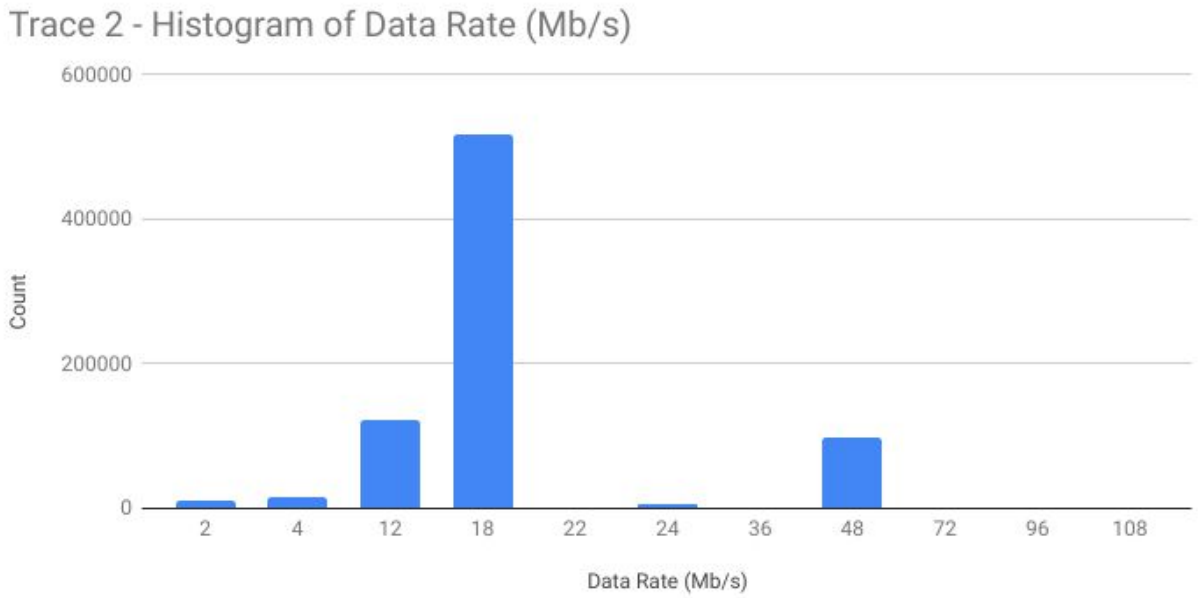


Observation: Same like above, there are a lot of small size packets. The observation for this remains similar as above, but only difference is that the proportion of mid-sized packets is very less. This trace also had some very big packets (upto 3900B+) compared to Trace 1. The number of small sized packets are so huge that, it overshadows the histogram of other sizes.

Histogram of Phy Data Rates



Observation: Many packets were sent a lower rate of 2 Mb/s, so this has to be the management and the control frames which are smaller size, which don't require a lot of bandwidth. Higher sizes were well distributed, and mostly used to data.



Observation: Unlike above, most of the packets were sent at a higher rate of 18 Mb/s. This might be due to the high number of users in Trace 2, which needed higher bandwidth. Some big number of packets were also served at higher speed of 48 Mb/s, which will be mostly for data packets.

f.

(Done in Wireshark)

From Trace 1:

30 Munroe St:

- Supported Rates: 1, 2, 5.5, 11 [Mbit/sec]
- Extended Supported Rates: 6, 9, 12, 18, 24, 36, 48, 54 [Mbit/sec]
- Cannot support WEP
- Automatic Power Save delivery not implemented
- Using short slot time

linksys12:

- Supported Rates: 1, 2, 5.5, 11 [Mbit/sec]
- Extended Supported Rates: 6, 9, 12, 18, 24, 36, 48, 54 [Mbit/sec]
- Cannot support WEP
- Automatic Power Save delivery not implemented
- Not using short slot time

linksys_ses_24086:

- Supported Rates: 1, 2, 5.5, 11 [Mbit/sec]
- Can support WEP
- Automatic Power Save delivery not implemented
- Not using short slot time

From Trace 2:

IITH:

- Supported Rates: 9, 11, 12, 18, 24, 36, 48, 54 [Mbit/sec]
- Can support WEP
- Automatic Power Save delivery not implemented
- Using short slot time
- Channel utilization: 62% (Packet 4830), 77% (Packet 288654)
- Admission capacity: 23437
- Station count: 156 (Packet 999033)

IITH-Guest:

- Supported Rates: 9, 11, 12, 18, 24, 36, 48, 54 [Mbit/sec]
- Cannot support WEP
- Automatic Power Save delivery not implemented
- Using short slot time
- Channel utilization: 76% (Packet 436752)
- Admission capacity: 23437
- Station count: 158 (Packet 833085)

Smart-X:

- Supported Rates: 9, 11, 12, 18, 24, 36, 48, 54 [Mbit/sec]
- Can support WEP
- Automatic Power Save delivery not implemented
- Using short slot time
- Channel utilization: 48% (Packet 574614)
- Admission capacity: 23437
- Station count: 165 (Packet 86191)

eduroam:

- Supported Rates: 9, 11, 12, 18, 24, 36, 48, 54 [Mbit/sec]
- Can support WEP
- Automatic Power Save delivery not implemented
- Using short slot time
- Channel utilization: 51% (Packet 781574)
- Admission capacity: 23437
- Station count: 165 (Packet 325408)
