Performance Evaluation of Wi-Fi Networks

Nima Eivazzadeh Kaljahi

Specialization

Cloud-based Services and Operations

Thesis submitted for the degree of
Master in Applied Computer and Information Technology (ACIT)
30 credits

May 2021

Performance Evaluation of Wi-Fi Networks

Nima Eivazzadeh Kaljahi

Performance Evaluation of Wi-Fi Networks

http://www.oslomet.no/

Printed: Oslo Metropolitan University

Abstract

Given the number of wireless devices in use is growing drastically, the bands are going increasingly congested. Asking home users in that developed world about their wireless connection, they are likely arguing that it seems to be getting worse not better. Access Points chooses a radio channel randomly and therefore causes interfere the other wireless networks, while the wireless traf c grows. The objective of this thesis is to examine what happens when two networks disturb each other and discuss this phenomena. Performance measurements of wireless networks will be carried out. Throughput testing when two wireless networks working at the same channel at the same time and interfering each other will be measured. In addition, the measurement of single wireless network will be evaluated to produce different result in a condition without the presence of interfering network to compare results.

Acknowledgements

I wish to thank all the people whose assistance was a milestone in the completion of my Master education and this thesis project:

- I wish to express my sincere gratitude to my supervisor, Madeleine Rønning, who has the substance of a genius: she convincingly guided and encouraged me to be a professional and do the right thing even when the road got tough.

- My appreciation to Torleiv Maseng my other supervisor for all his effort and support. For his helps, insightful comments and suggestions.

- My deep gratitude to my internal supervisor, H arek Haugerud, for his kindness support and encouragement during the dif cult conditions in this thesis.

- My very special thanks to Kyrre Begnum as a brilliant and wonderful teacher of mine. During these two years of study he always supported me in all situation and dif cult conditions.

- I would like to extend my sincere thanks to the Oslo Metropolitan University for offering me my desired Master education and all the facilities they provided throughout the journey of my education.

- I would like to offer my special thanks to the University of Oslo for offering me the education to learn more about Norwegian history, culture, society and language.

- I would like to express my sincere gratitude to my lovely family, my father and my mother whom supported me throughout this journey everyday, every time.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Today, wireless technologies has increased speed, enhanced capabilities and expanded to deliver peer-to-peer connectivity with high speed performance, smart and secure home network services[1]. Wireless communication has opened vast new avenues for entertainment. Devices such as smartphones are equipped with applications for downloading and reading books, newspapers, streaming games, movies, television and live sporting events. People with smartphones now have a way keep themselves almost endlessly entertained while on the go or to ll the time between appointments and classes.

Wi-Fi ® 6 is the latest generation of wireless network technologies offering great capacity, eciency, and performance for advanced connectivity due to [2]. According to Wi-Fi Alliance, Wi-Fi 6 will observe strong global adoption across PCs, access points, smartphones as well as IoT devices in enterprise, homes and public areas with almost nearly 2 billion Wi-Fi 6 devices shipments in 2021 .

In wireless technology wireless devices communicate by radio frequency band. Frequency bands in 2.4, 5 as well as newly emerged 6 GHz, (Wi-Fi 6E)[1] are available for wireless communication at the time of writing the report. The 802.11 standard de nes fourteen channels for use by 2.4 GHz. Each channel is 20 MHz wide with an additional 1 MHz on the low and high end of the channel for inter-channel spacing. This result in each channel requiring 22 MHz of bandwidth according to [3]. Channels are spaced 5 MHz apart. Since of this spacing it is not possible to actually use 11 channels in the same location since the 22 MHz width would overlap and cause interference [3].

In the 5GHz band, channels are ranging from 36 up to 165 MHz wide [4]. Same as the 2.4 GHz wireless channels, each 5GHz channel is 5 MHz wide. There are 23 channels speci ed for 802.11 wireless network, unlike the 2.4 GHz channel de nitions, only non-overlapping channel numbers are used for device con guration according to [3].

[1] https : // www.wi fi.org/ countries enabling wi fi 6e

A question arises as to how interference problem occurs generally? Interference can cause from our own network or neighbor's wireless devices if they are working in the same channel, microwaves or may a radar systems. Signal to noise ratio is one factor affects the interference problem in wireless networks due to [5]. In general, SNR compares the level of a desired signal to the level of background noise. SNR is de ned as the ratio of signal power to the noise power measured in decibels according to [6]. For instance, a client can be right next to an access point with excellent signal, but unable to keep a connection if the signal from another wireless network or any other type of radio-frequency device is too high, meaning that signals from other devices are just noise to your device.

By the given information in mind the importance of wireless network is more serious in the society so therefore it plays an important role in people's daily activities.

As more wireless devices are connected and wireless access points are densely deployed in the scarce frequency spectrum, the failure probability of packet transmission is expected to increase due to interference from other devices. This is because the the 2.4 Ghz band is already congested and the 5 Ghz band will be congested soon, the wireless environment might suffer severe interference from unintentional wireless devices.

The increasing deployment of access points for wireless services result in more interference from neighboring access points, thus noticeably degrading the wireless network performance and damaging the network security as well as quality of service.

1.1 Motivation

In home environment users use various type of devices such as portable computers, mobile phones, tablet computers, intelligent televisions, intelligent fridges and IoT systems which all requires to have Internet connectivity via home-based wireless network settings. By this assumption in mind, the quality of service in home-based wireless networks is a signi cant factor for home users who prefer to use wireless network technologies at home.

Access to various type of devices through a cable connection would not be ef cient and possible at home environment. Therefore, wireless technologies can bridge the gap through its outstanding services allow users to connect themselves to those devices without any computer network cables. This feature is a positive point of wireless network technologies so therefore, it plays a positive role in people's daily life as it makes connectivity simple and more convenient for them. The motivation behind this project is to analyze wireless network performance speci cally in home environment with the presence of controlled and not controlled interfer-

ing wireless networks to observe the behaviour of the network. More speci cally to acquire the better understanding of the factors in place which affect the performance of wireless network.

Home users use wireless routers to connect their own devices to the Internet. There are different type of access points working in the apartment buildings almost near to each other with different distances and different radio frequencies and channels.

In general, there are some parameters affect the performance of the wireless networks. For example, transmit power, received signal from access point (signal strength), distance between access point and clients, busy channel, external heavy noise comes from neighboring wireless devices and a very close distance between a pair of wireless networks.

In wired network carrier-sense multiple access with collision detection is a media access control method was used in early Ethernet technology for local area network. It uses carrier-sensing to defer transmissions until no other stations are transmitting [7]. In wireless network this method is carrier-sensing multiple access with collision avoidance.

In wireless network, nodes have random access to a channel. This means they can transmit whenever they need to, but they can interfere with other nodes transmitting data, causing data loss. CSMA listens to the shared channel, in case the medium is not idle (someone else transmitting), it waits for transmission to become complete. Then, start transmitting data to avoid collision. It is possible to mention that collisions can still occur if two nodes transmit at the same time. Collision Avoidance waits for a random amount of time when the channel is busy to avoid collision. Figure 1.1 illustrates the process.

Figure 1.1: Collision Avoidance

In wireless network, sender expects an acknowledgment message (ACK) back from the receiving device to con rm it arrived correctly. Therefore, if it has not arrived in a set amount of time, the data is re-transmitted.

A problem of CSMA for wireless networks is the hidden nodes problem. For instance, as figure 1.2 illustrates node B and node C can sense each other as they are in the same range of each other. In addition, they can communicate with the router since they are all in the same range. On the other hand, Node A is communicating with access point at the same time as well, but B and C cannot see that node. This is because Node A is far enough and it is not on the same range of B and C. This adaptation requires a node to send a Request to Send message and receive back a Clear to Send message from access point before transmitting. Therefore, to overcome the hidden node problem, RTS/CTS mechanism is implemented at access point in conjunction with the CSMA/CA scheme according to [8]. With RTS/CTS mechanism packet can send with less risk of collision, but it adds overhead to each packet, and will worsen congestion. Therefore, it might be deactivated for small packets. Figure 1.3 illustrates process of CSMA/CA with RTS mechanism.

Figure 1.2: Hidden nodes

Figure 1.3: CSMA/CA with RTS
[8]

Since this research study tries to evaluate performance of home-based wireless networks as well as measuring interfering problems in home environment. Therefore, it tries to use real wireless network devices instead of using simulated software such as NS3 or Mininet to observe the real behaviour of the wireless network performance. Thus, as these simulation tools simplify the wireless medium and the result obtained from these environments is not correctly translatable to real-life environment problems, Raspberry Pie devices is used to make a real wireless network with real devices rather than simulated environment to observe the performance in real environment.

1.2 The problem statement

In IEEE 802.11 the channel access is controlled by a carrier sense procedure. This includes the clear channel assessment (CCA) which is a function with CSMA/CA and performs the channel access by observing the channel for ongoing transmissions. It prevents the node form sending if transmissions of other networks are sensed on the same channel. The following two cases result in reducing rates due to [9]:

- Any energy above a certain threshold triggers the channel as busy and the channel will wait. This causes the rate to be reduced.
- On the other hand, if no signal is detected, transmission starts. It is possible that it should not have started and failed to detect that the channel was busy. This would result in many faults in the frames. This will result in re-transmission of frames.

The objective of this thesis is to examine what happens when two networks disturb each other and discuss this phenomena.

Performance measurement with the presence of single wireless network as well as two pair of wireless networks will be conducted through a throughput testing application. For instance,

when one single pair of wireless network works stand-alone in two certain distances. Moreover, when two pair of wireless networks work beside each other horizontally on the same channel with the same con guration at the same environment. The purpose of measurement is to observe the behaviour of the network, variations and numbers.

The approach chapter will explain clearly the project's testbed architectures through different type of visual illustrations and gures. Subsequently, the result of measurements relevant for each architecture introduced in the approach chapter will be reported in result chapter.

Chapter 2

Background and Research Work

In order to understand the interference problems in home-based wireless networks, it is crucial to have adequate understanding of the problem domain. This chapter explain interference problems, medium access, career sensing as well as RTS/CTS mechanism obtained from scienti c papers as well as online resources. Moreover, it would be a comparison between the work has been developed and implemented in this project and other research work de ned by other researchers regarding the problem domain. Moreover, this chapter tries to present knowledge in data link layer and connect them to the work accumulated in the approach chapter by reviewing scienti c paper.

2.1 Factors affecting wireless network performance

Wireless interference occurs when something disrupts or weakens the signal coming from an access point. The most typical channel for wireless connection is in the 2.4 GHz band. This channel is shared with other devices in home environment, the limited channel in 2.4 GHz increases the interference further. Interference from other radio signals can affect network performance. The higher interference between neighbors the more congestion and low speed throughput occurs in a wireless networks.

Due to [10] there are some factors affects the performance of wireless networks. Below are a few example of them .

- Antennas:

  Wireless network performance can be affected by the antennas in an environment service equipment. Antennas has a signi cant impact on network coverage. For instance, if antennas are near some sort of structure, such as a metal grid or cement beam, this can affect wireless transmissions and subsequently reduce the performance.

- Power Level:

Power level of wireless equipment also in uence speed. Power level is transmitted by an access point is considered as wireless coverage. The transmit power of an access point radio is proportional to its effective range. The higher the transmit power, the farther a signal can travel, and the more obstructions it can effectively penetrate. Stefan [11] argues that a common approach to assess the quality of the network is the received signal strength indicator (RSSI). The RSSI corresponds to the signal strength at the receiving antenna. Duo to [12], it has been widely realized that the link reliability has signi cantly related to received signal strength indicator known as RSSI(Received Signal strength Indicator) or signal-to-interference-plus-noise ratio known as SINR. In addition, external interference makes it unpredictable which is different from the previous understanding that there is no tight relationship between the link reliability and RSSI or SINR.

To reduce interference, maximum transmit power is reduced. In addition, observing that nodes should not adapt their rates due to losses during congestion (channel busy time() the fraction of time the medium is utilized) can be used as metric. Noting that in this case, the evaluation of channel busy time has dependency on the underlying assumption that physical carrier sense mechanisms, which play an important role in avoiding packet collision [13].

Woo [12] argues that, both the link distance and Signal-to-Interference Ratio(SINR) are not strongly correlated with frame loss rates. Woo et al. They also claim that received signal strength indicator (RSSI) is a good indicator to predict link performance in (rural) mesh network that barely have external interference.

- Interference:

Woo et al [12], in wireless networks, links usually do not permanently stay at the state of link reliability 1.0 or at the opposite state of link reliability 0.0 because of external interference, multi-path fading, where the link reliability is explained in terms of frame delivery rate (FDR). Also , each wireless link rate additionally turns out to have an intermediate range of link reliability in between 0.0 and 1.0. This means that links do not always successfully transmit data or do not successfully drop data in a given interval.

Hwangnam et al [12]. Understanding of irregular variation of wireless links enables network protocols or systems to use optimal link or different classes of wireless link according to the current link state or required link quality. Moreover, Woo et al [12] claims that, link performance can be predicted by RSSI which can be easily translated to SINR with a

constant noise oor in rural mesh networks without having a external interference.

Due to [14] powerful signal can interfere with neighboring devices even if they are on different channels (frequencies). Access points can interfere with each other, even if there is enough space distance between them. Interference can also emanate from adjacent channels. Thus, in this case the design of an 802.11 system's, RF sub-system and digital ltering can greatly affect the performance of the wireless network. Also, the physical design of a wireless network can overcome many of the consequences of in-band interference. The performance of wireless network is determined by the signal - to interference ration (S/I or SIR), which is de ned as the ratio of the data signal to the interference signal. The signal-to-interference ratio (SIR) measures the aireless signal in comparison with how much co-channel [1] interference is present from other radio transmitters due to [15]. SIR is usually more critical to WLAN performance than the signal-to-noise (SNR). Figure 2.1 illustrates the mentioned concept [16].

[16]

Figure 2.1: Interference Pattern

According to [17] IEEE 802.11 uses many mechanisms to mitigate noise and interference, thus it is natural to ask whether 802.11 links are already as robust to interference as can reasonably be expected. Those mechanisms are as follows:

1. A MAC protocol that avoids collision.
2. lower transmission rates that accommodate lower. signal-to-interference-plus-noise ratios (SINR).
3. signal spreading that tolerates narrow-band fading and interference.
4. PHY layer coding for error correction.
5. RTS/CTS mechanism to reduce the risk of collision in wireless network.

[1]co-channel interference or CCI is cross-talk from two different radio transmitters using the same channel.

2.2 Fragmentation and Aggregation:

Fragmentation aims to improve wireless performance in a cluttered environment due to [18]. Fragmentation break up packets into smaller pieces, for a higher chance of successful transmission. A receiver has to put all these fragments back together to form the original packet. Moreover, aggregation is used to acknowledge blocks or groups of packets, which cuts down the requirement to acknowledge every single packet, enhancing ef ciency and performance. Due to [19] frame aggregation is a function that combines several frames into a single large frame for transmission. Frame aggregation has many bene ts: rst, transmitting large frame leads to higher throughput than transmitting small frames. Second and most important bene t is the reduction of timing and header overheads that are required to transmit a frame by the MAC distribution coordination function. Therefore, by using frame aggregation, these overheads are squeezed and only few overheads have been used to transmit the aggregated frame. Aggregation can be performed either at the packet level or at the frame level. It is called packet aggregation of it is performed at higher layers such as IP and application layers. However, it is called frame aggregation if it is performed at the lower layers such as PHY and MAC layer. The frame level aggregation provides more control over the transmitted frames and exhibits an ef cient partial re-transmission. Moreover, aggregation at the MAC level is the widely used aggregation where the MAC headers overhead can be squeezed or even removed. Also, the channel access can be optimized by reducing the timing overhead such as backoff and message exchange overhead such as ACKs.

2.3 Carrier Sensing

According to [20] carrier sense is the fundamental part of most wireless networking stacks in wireless local area and sensor networks. As growing number of users and more demanding applications uses wireless networks to their capacity limits, the ef cacy of the carrier sense mechanism is a key factor in determining wireless network capacity.

A question arises as to what is the basic idea of carrier sensing? due to [20] in career sensing before transmitting a packet a sender listens to the channel and evaluates whether a nearby node is transmitting a packet or not. Therefore, if no nearby node is transmitting a packet the sender transmits a packet immediately. If a nearby node is transmitting, the sender defers and it waits for a few time after the end of the intervening transmission.

Carrier sense is a part of the medium access control MAC layer of the radio stack. Well-informed MAC decisions are crucial for maximizing the capacity of a broadcast radio medium. Failed transmissions not only waste energy, but also have potential to corrupt other transmissions in the network, reducing aggregate capacity. Deferring a transmission has the potential of wasting a good transmission opportunity, therefore reducing capacity. Due to [20] in carrier

sensing the sender and receiver are in different locations, and the sender makes the carrier sense decision based on local information .

Contention Window(CW) is related to idle channel availability by using Clear Channel Assessment (CCA). Initial value of CW is 2, that is a node needs to pass the channel availability for two successive times before declaring the channel idle according to [21]. Figure 2.2 illustrates the detailed ow diagram of CSMA/CA.

[21]

Figure 2.2: Flow diagram of slotted CSMA/CA

Jamieson et a[20]. Although carrier sense improves link qualities at all traf c loads, but it leaves room for performance improvements. In addition, they claim that carrier sense can actually reduce capacity under extreme loads. Jamieson claim that carrier sense is not always a good predictor of transmission success since it relies on channel measurements at the sender to infer the probability of reception at the receiver. However, in many cases, no correlation exists between channel conditions at the sender and at the receiver. Thus, this lack of correlation is often because of exposed terminals, the aggregate effect of distant nodes raising the noise oor. In addition, they claim that local level carrier sense may perform poorly when exposed terminals are present.

The IEEE802.11 specify two mechanisms for sensing whether a medium is busy or not, those are as follows:

- Virtual carrier sensing
- Physical carrier sensing

In virtual carrier sensing the medium is de ned busy by reading the Network Allocation Vector (known as NAV) eld present in the MAC frame. This led can be read when using RTS/CTS control frames.

The physical CS (PHY) is a different mechanism. In IEEE 802.11 networks, physical carrier sensing is de ned by the clear channel assessment (CCA) function monitor the channel to de- ne whether the channel is free or is in use.

Regarding RTS mechanism Jamieson et al [20]. Represented that imagine two transmitters, for instance node A and B, are both within radio range of each other. The intended recipients of their transmissions, nodes A' and B' respectively are within range of only one transmitter, and thereby could simultaneously receive a packet from the intended transmitter. In this environment carrier sense would only allow one transmission to take place. Whichever node lost the CSMA contention period would sense a busy channel and wait for the other nodes's transmission to complete. In addition , carrier sense may be a poor predictor of transmission success if interference comes from large number of distant nodes rather than a few local neighbors nodes. He claims that when interference is local and nodes are within each other's transmission range, carrier sense or RTS/CTS exchange may be a good method of contending for the channel.

There are three different methods that can be considered to see whether a channel is busy or not.

1. Energy detection.
2. High rate PHY signal.
3. Direct sequence spread spectrum (DSSS) signal.

DSSS signal looks at an actual DSSS signal and report the medium as busy if a signal is detected regardless of the received energy. DSSS signal is widely used both in military and commercial communication. This is because of the low power spectrum density, it is very dif cult to detect in non-cooperative communication. It has very low power signal spectral density, which result in the transmission below the noise level [22].

Huehn et al [13]. In CSMA wireless networks several mechanism are exists, mechanisms such as transmit rate, transmit power control. According to Huehn carrier sense aim is to maximize throughput performance, while these presented mechanisms operate independently, they present high dependency affects the optimum of transmission decision . For instance, A packet can be transmitted at a high rate in case the SNR (Signal to Noise Ratio) at receiver is

high. Otherwise, a lower transmit rate achieves more robust communication.

2.4 IEEE 802.11 MAC Frame:

The MAC layer frame consist of nine elds due to [23]. Figure 2.3 illustrates the basic structure of an IEEE 802.11 MAC data frame along with the content of the frame control led.

[23]

Figure 2.3: IEEE 802.11 MAC Frame structure

Typeis a two bits long led which determines the function of frame, i.e management (00), control(01) or data(10), the value 11 is reserved due to [23].

Sub-typeis a four bits long led which indicates sub-type of the frame. For example, 0000 for association request, 1000 for beacon.

To DSis a one bit long eld indicates that destination frame is for DS (distribution system).

From DSis a one bit long led indicates frame coming from destination.

Retry bit is one bit long eld. It represents if the current frame is a re-transmission of an earlier frame, then this led is set to 1. This means that when client transmit a frame to its access point, but didn't received acknowledge message from its access point, then client assumes frame was lost in between of transmission so therefore re-transmits frame again. This research study will look into Retry eld through the measurements to observe the probability and number of frames re-transmitted from client to its access point in different measurements. This is to observe if channel is busy or if client received weak signal or signal is lost, then how many error and re-transmission of frames occurs. For instance, how many Retry bit are exist when a Pair of wireless network works stand-alone and how many are exist when two Pairsof wireless network work beside each other and result in interference Approach chapter will explain the matter more in detail.

2.5 The MAC sublayer :

IEEE 802.11 de nes two MAC sub-layers due to [24]:

- The distribution coordination function (DCF).
- Point coordination function (PCF).

Figure 2.4 illustrates MAC sub layers and physical layer standards for IEEE 802.11.

[24]

Figure 2.4: MAC sub-layer and the related physical layer standards for IEEE 802.11

2.5.1 Distributed Coordination Function

In IEEE 802.11 family of standards DCF protocol, controls access to the physical medium. A station must sense the status of the wireless medium before transmitting.

According to [25] The DCF uses CSMA/collision avoidance mechanism to control access to the shared wireless medium. This is because collisions are dif cult to detect in wireless environment, therefore, a backoff-based collision avoidance technique, rather than the collision detection technique which is common in Ethernet standard is used. Each wireless station/user rst listens to the wireless medium to detect transmissions. If medium is sensed to busy, the station waits until the ongoing transmission is over. If the medium is detected to be idle for a distributed inter-frame space (DIFS) interval, user enters a backoff procedure. In the backoff procedure, user selects a random backoff time (in slots) from a contention window, and starts decreamenting a backoff counter for each slot that is sensed to be idle, while counting down, another user begins transmitting. User in backoff mode suspends its counting, until the transmitting user nishes and the medium is sensed to be idle for a DIFS duration, and resumes its countdown thereafter. Once the backoff interval expires, the user begins transmission. The value of the random backoff interval is chosen from an interval called the contention window CW which lies between two pre-con gured values, CW_{min} and CW_{max} . The contention window is set to (CW_{min}) at the rst transmission attempt, and doubles after each unsuccessful attempt, until it reaches (CW_{max}). The contention window is reset to (CW_{min}) after every successful transmission. This procedure illustrated in gure 2.5 as well as gure 2.6.

[25]

Figure 2.5: Event sequence in DCF CSMA/CA

[26]

Figure 2.6: Basic access mode of DCF

In DCF con guration, a contention window is set after a frame is transmitted. This is considered to avoid collision. The window de nes the contention time of various stations who contend with each other for access to channel. Thus, each of the stations cannot garb the channel immediately, rather the

MAC protocol uses a randomly chosen time period for each station after that channel has undergone transmission [27]. For CSMA/CA medium access, a backoff mechanism with a contention window comparable to IEEE 802.11 is used in order to reduce the collision probability. As collisions cannot be avoided completely, the receiver of a frame sends an acknowledgment in order to enable the transmitter to detect transmission errors.

Cheng et al [26] argue that CSMA/CA in IEEE 802.11 provides con rmation frame ACK to ensure the check of frame lost and re-sent. For further avoiding con ict, RTS/CTS + ACK four handshakes protocol is imported. RTS/CTS protocol is a common mechanism to reserve channel by the way of handshakes between sender node and receiver node. Figure 2.7 shows the process of data transmission between the sender and the receiver by use of RTS/CTS + ACK + DATA, called handshakes protocol and the situation of other nodes setting NAV. Other nodes renew the value of NAV by use of the led duration of RTS/CTS frame after receiving this frame. The node could not send frame before the value of NAV equal zero. When only the value of NAV equal zero, the node could send data frame by the way of DCF.

[26]

Figure 2.7: Principle of RTS/CTS

2.5.2 Backoff algorithm BEB

Due to [26] In IEEE802.11 WLAN, all nodes can carry out carrier sense. Each node operates sending action according to backoff counter when data packets are trying to send at the rst time. The contention window CW is set to the minimum CW_{min} before sending, and transmission is carrying out in equal probability at a choice time between 0 , CW_{min} . Therefore, when a channel is free for an interval, the backoff counter would decrease 1. So, when the channel is sensed busy, the backoff couner would be freeze until the channel is sensed free for DIFS time, and then the backoff counter would be unfreeze and continue to sense the channel. According to gure 2.8 node A and node B are share the channel.

[26]

Figure 2.8: Schematic of BEB algorithm

In BEB algorithm, backoff window CW of a node increase redouble until maximum CW_{max} when con ict occurred, backoff window CW decrease until minimum CW_{min} when sending is successfull. Below formula (2.1) explains the renew regular of CW in BEB algorithm.

$$\begin{cases} Finc = Min(2 \quad CW, CW_{max}) \\ Fdec = \quad CW \end{cases} \tag{2.1}$$

CW is the value of backoff window, CW_{min} and CW_{max} are set according to the channel load. According to [26] typically CW_{max} = 1024 , and CW_{min} = 2.

Taijun li et al [26] claims that the size of backoff window depends on the times of experienced con icts. Contention window increases drastically with the increasing of re sending times, reducing the con ict probability. However, this leads to the node which is the last one sending successful has the smallest backoff time, while is at a disadvantage in next contention, and the probability of the node sending failure access channel again is signi cant decreasing. Therefore, BEB algorithm always gives the node which is the last one sending successfull the greatest priority.

2.6 RTS/CTS

Due to [28] Request to send / clear to send is the optional mechanism used by the 802.11 wireless networking protocol to reduce frame collision introduced by the hidden node problem. Hidden nodes are the nodes that are not in the range of other nodes or a group of nodes. Each node is within communication range of the access point, but the nodes cannot communicate with each other as they do not have physical connection to each other. For instance, in a wireless network, it is possible that the node at the far edge of the access points' range, known asr, can see the access point, but it is unlikely that the same node can see a node on the opposite end of the access point's ranger2. Thus, these nodes are known as hidden

Figure 2.9 illustrates the hidden nodes problems.
Kanapi et al [28]. The problem is when nodes r and r2 start to send packets simultaneously to the access point. Since noder and r2 cannot sense the carrier, Carrier Sense Multiple Access with Collision Avoidance does not work. To solve this problem, handshaking is implemented in conjunction with the CSMA/CA scheme.

[28]

Figure 2.9: Hidden Node

2.6.1 RTS/CTS handshake in action

- A is the source which is in the range of B, D and C.
- B is the destination which is in the range of A, D and E.
- A is the source which is in the range of B, D and C.
- B is the destination which is in the range of A,D and E.
- B sends ACK after receiving one data packet.
- Improves link reliability using ACK show in the below gure.

[28]

Figure 2.10: RTS/CTS handshaking with ACK

IEEE 802.11 uses RTS/CTS acknowledgment and handshake packets partly overcome the hidden node problem. RTS/CTS is not a complete solution and may reduce throughput even further, adaptive acknowledgment from the base station can help too.

Due to [29] the sender rst sends the RTS frame to reserve the channel before its transmission, and upon receiving the CTS frame from the receiver, the normal packet transmission and the ACK response proceeds.

2.6.2 Exposed Terminals

Kanapi et al [28]. In wireless networks, the exposed node problem occurs when a node is prevented from sending pakcets to other nodes due to a neighbouring transmitter. For instance, consider 4 nodes labaled R1, S1, S2 and R2, where the two receivers are out of range of each other, the two transmitters in the middle are in range of each other as it presents in gure 2.11. If a transmission between node S1 and node R1 is taking place, node S2 is preventing from transmitting to node R2 as it concludes after carrier sense that it will interfere with the transmission by its neighbor node S1. Due to [28] node

R2 could still receive the transmission from node S2 without interference since it is out of range from S1.

[28]

Figure 2.11: Exposed Terminal Problem

2.7 Experimental platform developed by other researchers

Michael et al [9] prepared the experimental architecture with the presence of two pair of networks which they call pair 1 and pair 2. In order to evaluate the in uence of adjacent interference on 802.11 throughput they prepared two competing pairs. Figure 2.12 illustrates the scenario:

[9]

Figure 2.12: Measurement setup

AP and client in each pair are placed side by side to achieve the maximum SNR (Signal to Noise ration). In addition, in order to generate traf c and maximize the throughput between pairs and ood the channel they used iperf throughput tester application. In addition, UDP packet with the default length 1470 bytes sent to the link to transmit traf c between client and its AP's. In order to avoid the in uence of rate adaption schemes in all experiments the transmission rate is xed. In addition, based on the fact that APs and clients in typical residential deployments are not communicating in such a close proximity Michael et al performed measurements for different distances d between the interfering pairs, while the distance B between AP and client in each pair was increased to three meter. Michael argues that the distance between competing access point and client pairs is crucial for the interference between them. Therefore, they argue that a higher distance between adjacent WLAN links result in a higher signal attenuation (weaker) and therefore to a better SINR. The same transmission power is used during the measurement.

They argue that for different distances between the pairs it can be discovered that even very short links are affected from adjacent channel. In addition Michael et al [9] claim that the interference generated by one pair has only a minor in uence on the other. They claim that in the real life it is very unlikely that a client and an access point are placed directly side by side, so the inter-link distance B between access point and client increased to 3 meter. Therefore, the measurement setup they implement is based on assumption of general WLAN use case which often applied in residential or of ce environment. Also, based on the result they accomplished they claim that the distance d has almost no in uence on the achievable link throughput. Therefore, for the purpose of clarity only the throughput of one link pair 1 is given.

According to Michael et al [9] results they stated that the usage of Partially overlapping channel (POC) in 802.11g will not automatically lead to improvement in the cumulative throughput. Also, they cliam that concerning the channel access scheme the adjacent channels have limited scope of application. So,

this behaviour makes the practical implementation of POC in 802.11 g pointless. They summarized and concluded that the POC has an advantage in 802.11 b, but the restricted application of CSMA/CA and the different PHY makes POC in 802.11 gnot recommendable any more.

Chapter 3

Approach

This chapter provides an overview of the techniques used in this research. It covers the considered ways that tries to answer the problem statement followed by design of experiments. Moreover, the different type of testbed architectures will be shown in this chapter in order to interpret the different con gurations setup for devices used for the measurements of this research study. In it worth noting that the idea behind designing the testbed used to run the experiments is a consultation between the author and supervisors as well as scienti c paper such as [9].

Based on a discussion author had with supervisors regarding the studying and analyzing measurement of performance of wireless networks, those agreed that to work on data link layer rather than network layer for measurement and capture frames through Wireshark. Therefore, result of the measurements produced in result chapter is a result measured by Wireshark.

In order to properly answer the problem statement a proper experimental design should be considered.

3.1 Experiments design

There are different strategies doing the measurement which those are as follows:

- First and second measurement consisting of one access point and one client. An access point and client in rst measurement has one meter distance from each other. In addition, in the second measurement access point and client has ve meter distance from each other. This measurement has completed in a channel which observed is least busy in the test environment. This means that there are a few not controlled access points working on that channel. In the time of testing channel 108 in 5 GHz frequency band observed a least busy channel.
- Third and forth measurements consist of two wireless networks (networks such as Client1 and AP1 as well as Client2 and AP2). Distance between wireless networks are one and ve meters. In the third measurement Client1 and AP1 network has static distance which is one meter between client and access point. Also, the interfere network Client2 and AP2 has two certain distances such as one and ve meter from Client1 and AP1 network. The reason why two wireless networks has two distances from each other is to observe results when Client2 and AP2 interfere Client1 and AP1 in different distances.

- Fifth and sixth measurements were completed by single Pair of network (Client1 and AP1) in one and ve meter distances between client and access point, but in a clearchannel. clearchannel is a channel that there are not any access points working on that channel in the environment test has been completed. WiFi Analyzer mobile application was used to de ne the the channel in the environment.
- In seventh and eight measurement the interference Client2 and AP2network works beside Client1 and AP1. This means that two wireless networks working beside each other in a clearchannel. Same as third measurement the interference wireless network which is Client2 and AP2works in one and ve meter distance from Client1 and AP1network.

3.1.1 Testbed design and hardware used for the measurement

In this project ve Raspberry Pi devices are used. Two Raspberry Pi's are working as access points and two others are working as clients. In addition, one Raspberry Pi works in Monitor mode to capture the MAC Frame elds in the data link layer.

The aim of the measurement is to capture the low level data packet which is called frames on the MAC layer to observe MAC frame elds most speci cally Retry bit. This work is possible when the state of the wireless card changes from Manage mode to Monitor mode. The wireless card in Monitor mode can capture every packets travels on the air, but wireless card in Manage mode can only capture packets that have device's MAC address in network layer. Therefore, it can capture speci c type of packets which is understandable by the MAC address of a device.

Through Monitor mode it is possible to observe the number of Retry bit in order to understand that how many data packet has been transmitted more than once from client to access point. This means that this type of frames transmitted once, but server could not interpret the packet. Therefore, client assume that the packet lost in between and requires re-transmission to server again. For this purpose the rst experiment consists of Client1 and AP1network with Raspberry Pi devices was completed and Wireshark application captured those required information independently through the Monitor mode wireless card.

It is worth nothing that the Raspberry Pi's wireless card by default has set up to work in managed/operationalmode. Therefore, in manage mode setup client can connect to an access point through SSID name and pre-shared password key which is the common way for all wireless devices to make a connection from client to access point. Otherwise, in monitor mode wireless connection between client and access point disconnect, this means that it is not possible for a client to have connection to an access point when the wireless card is in monitor mode status. This is because monitor mode only capture radio-layer information about packets. Therefore, connection between client and access point terminates in that situation (discussion chapter explains more in detail about that problem). For the mentioned reason, one Raspbery Pi's wireless card is con gured to work stand-alone in monitor mode so therefore this card is responsible to capture data-link layer.

Steps presented in (3.1 and 3.2 below) required to set the wireless card to monitor mode in Kali Linux which customized for Raspberry Pi. The reason why it requires to use this speci c Kali Linux distribution is that it can set the wireless card from manage mode to monitor mode through a speci c

driver called NEXMON due to [30]. In addition, the command airmong-ngcan be used to enable the monitoring mode on that device in desired channel which requires to capture. Commands enabled monitor mode in two different channels such as 108 and 140 in 5 GHz frequency band are as follow: [31]

airmon-ng start wlan0 108 —— to observe traf c on channel 108 . (3.1)

airmon-ng start wlan0 140 —— to observe traf c on channel 140 . (3.2)

To switch from monitor to manage mode steps (3.3) and (3.4) are required.

airmon-ng stop wlan0mon 108 —— stop monitor mode capturing traf c on channel 108 . (3.3)

airmon-ng stop wlan0mon 140 —— stop monitor mode capturing traf c on channel 140 . (3.4)

When commands such as 3.1 and 3.2 are executed in the Raspebbry Pi who has a role of monitoring the status of wlan0 interface changes towlan0mon Then, through this interface traf c can be captured through Wireshark Rasbperry Pi device who is reponsible to capture air traf c has always x place in the environment test were performed. The position of Monitor card has shown in gures 3.1 as well as 3.2.

The complete information about the difference between Manage mode and Monitor mode has been discussed in the discussion chapter of the report.

3.2 Throughput testing

The purpose of doing experiments with a single and two pair of networks is to observe how many frames transmits from client to access point, how many received by access point, the number of pkt send by client and received by access point in different certain distances when the channel is busy and when the channel is not in use. Therefore, when the Client 2 and AP2work as an interfering network beside Client1 and AP1result is comparable for further analysis. This means to observe when channel is corrupted by other nodes to measure the throughput and network performance. In addition, to observe how RTS/CTS mechanism acts in a measurement when RTS is under control by access point and when it is off. Moreover, how many frame loss produces when received signal in client is weak and strong when a channel is busy or free. Also, to observe how CSMA/CA behaviour in a case channel is idle or free to measure throughput when two nodes transmitting frame at the same time in a channel and how they reduce the performance of network.

3.2.1 The mechanisms of the throughput testing

The server application runs in server side which is access point. After execution it waits to answer to the client request.

3.2.2 Theory of operation

The measure of successfulness of packet transmission is the throughput which is the number of bits transmitted due to [32].

$$\text{Throughput} = \frac{\text{Prob success transmission Mega bits transmitted}}{\text{Time for 1 try of 1 packet to be sent on the air}}.$$

The test was accomplished in a same time frame for the entire type of test which is 100 seconds. traf c generated through iperf3 throughput tester application which is a well-known tool according to [9]. To run the throughput testing commands is used on both sides on the server and on the client. So those are as follows:

- Server: iperf3 -s -p 2323
- Client: iperf3 -u -c ”server IP address” -p 2323 -t 100

The server side command run iperf3 in server mode and it listens to port 2323, -s run iperf3 in server mode. Command runs in client side speci es the UDP packet through -u command and -c speci es the current machine is a client. In addition, -t decides for timeframe which test should be completed. Therefore, tests setup to run in 100 seconds for the measurements. It is worth mentioning that when those command runs iperf3 maximize the throughput by ooding the channel with 1470 Bytes long UDP packet by default. In order to decide the length of the packet size the –lengthparameter is used to observe the result when the size of the packet is higher than default. command are as follows:

- Client: iperf3 -u -c ”server IP address” -p 2323 –length 2100 -t 100
- Client: iperf3 -u -c ”server IP address” -p 2323 –length 6560 -t 100

Therefore, through the mentioned steps throughput testing has been conducted and result has shown in the result chapter of the report.

channels such as 108 and 140 were assigned to the access points to work on those channels. Traf c sent on the air on Client2 and AP2network with the goal of ooding channel and making a pair of interfere network for pair one network. In this situation (when two pairs of network working beside each other) both APs working in the same channel, either 108 (busy) or 140 (free) in different tests. In addition, the wireless monitor card work in monitor mode to capture data link layer information and record them in a le. The number of pcap les are generated through Wireshark which sniffed data link layer traf c during measurement.

One meter and ve meter distances between client and access point has been considered for the rst and second measurement. Figure 3.1 and the subsequent table illustrates the measurement setup and

the con guration of devices used during measurement. According to the document of the hostapd [33] supported rates are varied and it depends on which hardware can support what rate. The rate 240 equal to 24 Mbit/s showed it works stable in Raspberry Pi device after con guration was completed. Therefore, rate xed in 24 Mbit/s on both access points in con guration le of hostapd

Figure 3.1: Single network, One and Five meter distances between client and access point.

RF interface type	Broadcom Wi-Fi network interface (Raspberry Pi Wi-Fi interface)
Frequency	5540 and 5700 (5GHz)
Channel	108 and 140
Bitrare	Fixed (24 MBit/s)
Nodes	2
Access Points	1
Client	1

Table 3.1: The measurement architecture with one network

In the second measurement, the distance between client and access point increased by five meters. This distance is the most far distance exist in the test environment (the authors apartment building). First Laptop computer is connected through RJ-45 cable to the Raspberry Pi device who has role of monitoring and Wireshark started to capture the air traffic. Then, the same cable unplugged from Laptop and plugged to the Client1 device to start throughput testing on the channel. Server must start first before client can start.

At this stage the measurement with single network in two different certain distances has completed and the Monitor wireless card captured required data from air. The third measurement is the measurement with the presence of the controlled interfering network which is Client2 and AP2 As figure 3.2 illustrates not controlled neighboring access points are working in the same environment. To complete the test first the Monitor wireless card started, then the traffic sent to the Client2 and AP2network to flood the channel in order to make an interfering network for Client1 and AP1 Finally, traffic sent on the Client1 and AP1network. Test has been accomplished in two different certain distances such as one and five meter distances between two wirelessnetworks (Client1 and AP1 and Client2 and AP2). Figure 3.2 shows two networks including two access points and two clients working beside each other in the same test environment. Table illustrates the configuration on both devices in two different measurements in channels 108 and 140.

Figure 3.2: Controlled and uncontrolled interfering networks are available and they are working in the same environment. One and Five meter distances d (distance)between two wireless networks.

RF interface type	Broadcom Wi-Fi network interface (Raspberry Pi Wi-Fi interface)
Frequency	5540 and 5700 (5GHz)
Channel	108 and 140 in both APs
Bitrare	Fixed (24 Mbit/s)
Nodes	4
Access Points	2
Client	2

Table 3.2: The measurement architecture with two networks

3.3 Tools used for capturing data

To do the measurement, the following tools has been used:

- Throughput tester application used during measurement to sent traf c on the air on both links.
- hostapd [1] has been used to con gure access points with desired radio band and channel frequency in the Raspberry Pies.
- Kali Linux operating system customized for Raspberry Pi device who is responsible to capture air traf c. The Monitor modedevice operating system [2]
- Rasperian OS 32-bit Debian-based Raspberry Pi's recommended OS on both clients and access points.
- External RJ-45 connector located in Laptop to connect the raspberry Pi to the Laptop and access to the console of Raspberry Pi devices.
- Ethernet cable to connect Laptop to the Raspberry Pi devices and read collected data.
- Wireshark to sniff the low level data frames in data link layer.

3.4 Wireshark Filtering feature

The number of frame transmitted to the access point has been measured through the Python script. In addition, this script calculates how much data frame send to the desired access point in Byte. Transmitted frames to access point observed and reported in the result chapter. It is possible to observe numbers through Wiresharkapplication as well. In order to access to Wiresharkstatistics a few steps should be done. For instance, in Wiresharkin the menu bar there is an item is called wireless after clicking on wireless item the WLAN Traf c items should be triggered. Therefore, it is possible to observe desired statistics. For example, how many data packet sent from client to access point and how many received through the based station (AP). In addition, it is possible to read the Retry bit number, the percentage of re-transmitted frames and other statistics regarding speci c measurements. The number of Retry bit which is desired number for this project obtained form Wiresharkstatistics.

[1] hostapd is a user space daemon software enabling a network interface card to act as an access point and authentication server.

[2] Kali-linux-2021.1-rpi4-nexmon-64 [34]

3.5 Operating system of Raspberry Pie

Two Raspberry Pies con gured as access point and they uses a Rasbian operating system which is Debian-based Linux operating system. In addition, the both clients uses the same Linux operating system as access points use during the measurement. The *hostapd* software used to make two Raspberry Pis as access points. Through *hostapd* software the wireless network interface card is enabled to act as access point and authentication server for the clients during the measurement. Kali Linux (Customized for Raspberry Pi) is used to use the monitoring feature of WiFi interface card to observe traf c on the air and to capture frames in data link layer.

3.5.1 Rasspbery Pi's MAC address

Clients and access points Media Access Control addresses are shown below. Those address are required to have access to related data captures by *Monitor mode* Wireless card. This is because to exclude traf c traveled between

$$(dc:a6:32:32:40:45 == > Client1) \quad (dc:a6:32:32:3f:fa == > AccessPoint1) \tag{3.5}$$

$$(dc:a6:32:32:3f:d0 == > Client2) \quad (dc:a6:32:32:40:42 == > AccessPoint2) \tag{3.6}$$

Chapter 4

Results and Analysis

This chapter explains the results of the measurements in which the testbed devices are used for the throughput testing and performance evaluation. As explained in the approach chapter each measurement has been carried out in two different distances; one meter is the closest distance possible and ve meter is the largest possible distance in the lab the experiments were performed.

It is important to mention that the Client2 and AP2network has the role of interfering network for the Client1 and AP1network. Therefore, with the presence of the interfering network, distance between two wireless networks is one and ve meter(the horizontal distance).

The distance between clients and its access point is always one meter (the vertical distance) without the presence ofClient2 and AP2

4.1 Range limitations

The tests were carried out in a small lab limited the range available for tests. The distances for the interference measurements where limited to $d_1 = 1$ and $d_2 = 5$ meters distances between the two interfering networks. The path loss in dB is given by

$$L = 10 \log_{10}(d/ l)^h \quad (4.1)$$

where h is the propagation exponent and l is the wavelength. The difference in path loss between these two distances is therefore:

$$L_d = 10 h \log_{10}(d_1/ d_2) \quad (4.2)$$

For h = 2, corresponding to free space propagation, the difference of only 12 dB.

4.2 Result of experiments

Result of the experiment with two different channels such as 108 as well as 140 will be illustrated in a form of gures and tables. In channel 108 there are a few access points working in the lab environment which they are not controlled (meaning that we do not have access to them). Also, channel 140 was observed free of use by other access points. The reason is that it was used two different channels is to

observe different results. WiFi Analyzer mobile application was used to to observe channels.

Figures illustrates result of experiments without presence of controlled interfering network (only single network with different pkt size). Tables demonstrates all results more in detail and exact numbers accumulated from measurement pcap file.

In order to observe the behavior of throughput with different pkt size, the length of the pkt increased from default value (1470 bytes) to 2100 and 6560 bytes in different measurements. The length decided through TP tester application and explained in approach chapter through Linux command. In the measurement when the pkt size 2100 (bytes) it was observed that the first frame was transmitted to its access point has a length of 138 bytes. As it is not possible to transmit a packet more that 1500 bytes cause it goes over maximum transmission unit size. Therefore, the TP tester fragmented pkt size to smaller size and transmitted frames. Numbers such as 700 and 1500 were most likely observed as the length of frames in the related pcap file.

To observe the length of frames a Wireshark filter is required. As Monitor card captures all wireless traffic on the air (related or not related to the link you are working on). Therefore, a filter is required to exclude frames transmitted to its access point. Therefore, filters were used to filter traffic are as follows: (4.4 is used in addition to 4.3)

$$(wlan.addr == dc:a6:32:32:40:45 \&\& (wlan.addr == dc:a6:32:32:3f:fa) \&\& \quad (4.3)$$

$$[35]wlan.fc.type_subtype == 40) \quad (4.4)$$

$$(wlan.addr == dc:a6:32:32:40:45) == > Client\ MAC\ address \quad (4.5)$$

$$(wlan.addr == dc:a6:32:32:3f:fa) == > Access Point\ MAC\ address \quad (4.6)$$

As table 4.12 illustrates when the interfering network is not present beside Client 1 throughput is higher than 100 MBit/s stay at 103.69 MBit/s. In contrast, in the same measurement when the interfering network is present throughput is under 100 MBit/s stay at 89.29 MBit/s. (Table 4.3 and 4.12 compares). The reason is the channel they used is free of use without the presence of interfering network so therefore medium is idle since there is no access point working in the same channel. Therefore, throughput without the presence of interfering network is better (table 4.12). In addition, distance between client and access point without the presence of interfering network is one meter. So, received signal by client is more reasonable in one meter distance. As Eric [5] claims the best signal is -30 dBm and least signal is -90 dBm. In this measurement when we remove interfering network received signal by client is -46 dBm. Therefore, this is the second reason shows throughput is better.

As the introduction chapter explained the RTS/CTS is implemented in access point in conjunction with CSMA/CA to reduce the risk of collision. Due to [8] RTS/CTS as a virtual career sensing is not a complete solution to improve throughput and it may reduce throughput even further, but adaptive acknowledgment from the base station can help to reduce the risk of re-transmission. This is because client send request to send message to access point and ask if the medium is idle, then transmits frame,

but if the medium is busy then it wait until to receive CTS message from access point for transmission. Table 4.2 illustrates when the RTS mechanism is under control by access point the number of re-transmission is under 5 stay at 4 on both clients. Also, the percentage of re-transmission is 0. In contrast, in the measurement when the RTS mechanism is not controlled by access point the number of re-transmission is higher than 200 stay at 223 number in client 1 and 538 in client 2. (Tables 4.2 and 4.3 compares).

Result in the measurement with larger pkt size shows a little bit higher throughput. For instance, in the measurement when pkt size is 2100. This is because the larger pkt size do not need to have access to the medium as the smaller pkt size required. This is because the smaller pkt size has more overhead than larger so therefore it needs to have more access to the medium to send the same number of bytes which the larger packet size send. Table 4.8 represents the transmitted frames is 14,082,704 bytes when pkt size is 2100 compared with the measurement when the pkt size is 1470 the transmitted frames is 13,443,593 bytes (tables 4.8 and 4.10 shows the matter). Therefore, throughput in the former is 112.66 MBit/s, while throughput in the latter is 107.54 MBit/s . During the TP testing when the pkt size was decided to send with the length of 2100 there was a fragmentation occured through the TP tester application. After investigating in the measurement le it was observed that frames transmitted to the corresponding access point has a length of 1578 and 746 bytes with the same header length of 24 bytes. As it it not possible to transmit a packet more than 1500 byte since MTU size is 1518 bytes (1500 packet and 18 bytes for header) due to [36] . Then, fragmentation occured in application layer. Therefore, the fragmented length of packet was observed in data link layer in pcaps .

Tables 4.4 illustrates throughput when two wireless networks have one meter distance from each other is under 100 MBit/s stay at 89.92 MBit/s in Client 1 and 86.82 MBit/s in client 2. In contrast, when they have ve meter distance from each other they have a better throughput which is 106.32 MBit/s in Client 1 and 105.31 MBits/ in client 2 (table 4.5). This is noticeable that as they have a one meter distance from each other they should shared medium in halve equal so therefore 50 percent reduction in throughput is expected, but result shows only 10 to 20 percent reduction in throughput. A few probability are exists in this condition. One reason is that there is a little bit delay starting the TP testing in Client 1 . This is because it was one Laptop and one cable available and it required to switch between three different devices (Two networks (Client1 and Client2) as well as one monitor card) at the same time to start TP testing. Therefore, it could mention that channel is not busy for at least 5 - 10 seconds in the beginning of test.

Result shows when distance increases gradually throughput goes down increasingly. The reason is the power transmitted by access point decreases in larger distance. Therefore, RSSI or received signal from client reduces subsequently and result in the lower throughput and re-transmission of frames. Therefore, throughput form 103.69 MBit/s in one meter distance reaches to 88.46 MBit/s in ve meter distance. This would be a one example explained in problem statement which claims when signal is not detected transmission start and result in re-transmission and more Retry bit. Moreover, the percentage of re-transmission goes up from 1.2 to 2.9 percent (tables 4.12 and 4.13 demonstrates the matter). In addition, in the measurement when pkt size is 2100 when client and access point have one meter distance throughput is 112.66 MBit/s a little bit above 103.69 MBit/s (in pkt size 1470 shows in table 4.12), while distance increases and reaches to ve meter throughput goes down reaches at 95.10 MBit/s this is also a bit over 88.46 MBit/s (in pkt size 1470 table 4.13). Tables 4.8 and 4.9 illustrate when pkt size is 2100.

As the introduction chapter explained regarding career sensing with collision avoidance for wireless network gure in 1.3, it was observed and analysed when channel is busy by interfering network, and RTS is not under control by access point throughput is low. This can be shown in table 4.4. Also, interference is high in one meter distance between two wireless networks as well. On the other hand, results shows the same measurement when distance is ve meter between networks throughput is better (table 4.5). This is because two networks are far away from each other and interference is less since channel is not more in use. In addition, result shows when RTS in under control by access point throughput is 109,26 and 103.89 MBit/s in Client 1 and Client 2 (Table 4.1). Compared with the measurement when the RTS is not under control throughput is 89,29 and 99,41 MBit/s in Client 1 and Client 2 respectively in one meter distance. Tables such as 4.1 and 4.3 illustrate the matter. Also, the percentage of re-transmission is 2.1 and 0.1 in Client-1 and Client-2 when the RTS is under control compared with the measurement when RTS is not under control re-transmission percentage is 2.8 and 6.4 in Client-1 and Client-2 (Tables such as 4.1 and 4.3) shows the matter. Also, it is possible to refer to the Jamieson [20] et al which they claim that "when interference is local and nodes are within each other's transmission range, carrier sense andRTS/CTS exchange may be a good method of contending for the channel".

In single network measurements without the presence of interfering network with different pkt size results represented when the pkt size is larger re-transmission is higher compared with the measurement when the pkt size is smaller. Tables such as 4.8 and 4.12 illustrates the matter. This is because the smaller pkt needs more access to medium than larger packet therefore less transmission occurs when pkt size is smaller. On the other hand, larger pkt has fewer overhead so less access to medium is required therefore more frames transmits in bytes. But it is noticeable that different measurement with different pkt size represents different results. For instance, in a measurement when pkt size decided 2100 without presence of interfering network the percentage of re-transmission is over 4.5 stay at 4.7 percent (shows in table 4.8). But in the measurement with the same distance when the pkt size is 1470 the percentage of re-transmission is under 0.5 stay at 0.4. Tables such as 4.8 and 4.16 represents the matter. This is because it takes more time for larger pkt to be sent than the smaller when they are transmitting in the same time-frame.

The RTS/CTS feature in the measurements without presence of interfering network shows different results. For instance, Tables such as 4.11 and 4.16 shows although RTS is under control by access point in the former (table 4.11), but the percentage of re-transmission is higher compared with the measurement when the RTS feature is not under control by access point. Therefore, the former has 7.4 (table 4.11) percent of re-transmission and the latter has the 0.4 percentage of re-transmission. This is because RTS generally tries to solve the hidden node problem when there are more than one network send a message to access point. This is because to control clients when they try send messages to access point and expect to receive CTS with the goal of reducing collision.

In order to observe frame size in the measurement with pkt size 6560 the same steps (introduced above) are required in the related pcap le. After execution of the mentioned lter 4.3 and 4.4 it was observed that the frames transmitted to the corresponding access point has a length of 1578 and 746 bytes with the same header length of 24 bytes. As explained above fragmentation occured and this is because MTU size is 1500 bytes. Therefore, frames should be transmitted in smaller amount of numbers.

Figure 4.1 illustrates throughput when Client1 and AP1work stand-alone without the presence of Client2 and AP2 The range limitation calculated when Client1 and AP1work stand-alone. Signal in ve meter distance is -58 (dBm), this number deducted with signal accumulated in one meter distance (-46 (dBm)). Therefore, the difference is 12 db. This calculation conducted based on formula (4.1 and 4.2) presented above.

As gure 4.1 illustrates when distance between client and access point is one meter throughput is better compared with the other side when client and access point has ve meter distance from each other. This is because in one meter distance received signal from access point is stronger and in ve meter distance received signal is weaker. But as distance is not exceeds more than ve meter there is not a big differences in one and ve meter distances in throughput variation. In this measurement the controlled interfering network is not present during measurement. The received signal problem introduced in problem statement was showed and compared through different measurements in table format above.

Figure 4.2 illustrates the percentage of re-transmitted frames to the corresponding access point with different pkt size. In this measurement the controlled interfering network is not present during measurement. This probability calculated through below formula:

$$100 / [\text{pkt sent}] * \text{retry bit} \tag{4.7}$$

In order to calculate this probability the number of Retry bit is required. It is worth nothing that the Retry bit number observed through Monitor Mode wireless card after measurement was completed through pcap le. Thus, for this purpose all frames re-transmitted should be divided by 100 (this is because all frames are 100 percent of the frames). Then, the accumulated number should be multiplied by Retry bit number. As gure 4.2 illustrates there are variations on re-transmission with different pkt size. The percentage of re-transmission with larger pkt size should be higher than the percentage of re-transmission with smaller pkt size since the larger pkt need less medium access than smaller then the number of Retry bit goes up accordingly. But there is a question why pkt size 6560 has less Retry in this speci c measurement. Figure 4.3 shows the number of Retry instead of percentage .

Table 4.4 and 4.5 illustrates result of throughput testing when they have one and ve meter distance from each other. Based on those statistics throughput when two wireless networks have one meter distance from each other is lower compared with the measurement when they have ve meter distance. This is because in one meter distanceinterferencis high so therefore rate goes down and result in a lower throughput and re-transmission number increases.

Table 4.6 illustrates result of measurement when access points have setup to work in channel 108 which was observed busyin the test environment, but not so busy. It was observed that there are ve other not controlled access points working in the same channel (108). In this measurement the pkt lengthhas decided through TP tester application to be 6560 to observe result when packet has larger size than default size (1470). In this measurement two wireless networks have one meter distance from each other. It is interesting to mention that in this measurement when two wireless networks are far away from ech other they have a better performance shows in table 4.7. For instance, throughput in one meter distance has lower value stay at 87.42 MBit/s in Client 1 as interfering by Client2 and AP2, while when they have ve meter distance throughput is over 100 stay at 105.42 MBit/s table 4.7 represents. This is because

the fewer interfering are exist in ve meter distance between them.

Table 4.10 and 4.11 illustrates result when only Client1 and AP1network works stand-alone in one and ve meter distance. In this measurement access point setup up to work in channel 108 which was observed that four other not controlled access points working on that channel near of test environment. As results represents in this measurements the percentage of re-transmission in the ve meter distance is over 7 percent stay at 7.4 in table 4.11. In contrast, in one meter distance as table 4.10 illustrates the percentage of re-transmission is under 1.5 percents stay at 1.3. One reason is a distance. As distance increases received signal goes increasingly weaker and the number of re-transmission goes up. This is one example of measurement which can be refer to the problem statement introduced in introduction chapter. "if no signal is detected, transmission starts, This would result in many faults in the frames and also result in re-transmission of frame's.

Tables 4.12 and 4.13 are result of measurements when only one wireless network work stand-alone, but in channel 140 which was observed free of use by not controlled nearby access points in the test environment. As channel is free of use it is possible to mention that the re-transmission percentage is lower compared with the measurement when the channel is in use by other access points this is because medium is more in idle when channel is free of use.

Tables 4.16 and 4.17 are repeat measurement. The reason of doing same measurement is to observe the different result and the behaviour of the network.

Figure 4.1: Throughput without the presence of interferenetwork in two different distances.

Figure 4.2: The percentage of frames re-transmitted without the presence of interferenetwork in two different distances.

Figure 4.3: Frame re-transmitted without the presence of interferenetwork in two different distances.

Items	Client 1	Client 2
Throughput (MBit/s)	109.26	103.89
Transmitted frames (bytes)	13,658,141	12,987,469
Pkts Sent(Cli)	9367	8966
Pkts Received (AP)	8531	8157
Retry	183	6
Percent retry	2.1	0.1

Table 4.1: Result of experiment when two wireless networks have One meter distance from each other. Channel 108 pkt size 1470. Frequency 5540MHz (Band 5GHz). RTS threshold 2346 bytes.

Items	Client 1	Client 2
Throughput (MBit/s)	103.59	106.06
Transmitted frames (bytes)	12,949,458	13,258,045
Pkts Sent(Cli)	8936	9056
Pkts Received(AP)	8792	8931
Retry	4	4
Percent retry	0.0	0.0

Table 4.2: Result of experiment when two wireless networks have Five meter distance from each other. Channel 108 pkt size 1470. Frequency 5540MHz (Band 5GHz). RTS threshold 2346 bytes.

Items	Client 1	Client 2
Throughput (MBit/s)	89.29	99.41
Transmitted frames (bytes)	11,161,991	12,426,424
Pkts Sent(Cli)	7701	8420
Pkts Received(AP)	7635	8336
Retry	223	538
Percent retry	2.8	6.4

Table 4.3: Result of experiment when two wireless networks have One meter distance from each other. Channel 140 pkt size 1470. Frequency 5700MHz (Band 5GHz). RTS is Off.

Items	Client 1	Client 2
Throughput (MBit/s)	89.92	86.82
Transmitted frames (bytes)	11,239,696	10,851,960
Pkts Sent(Cli)	7901	7520
Pkts Received(AP)	7741	7361
Retry	196	154
Percent retry	2.4	2.1

Table 4.4: Result of experiment when two wireless networks have One meter distance from each other. Channel 140 pkt size 1470. Frequency 5700MHz (Band 5GHz). RTS is Off. Repeated measurement of table 4.3.

Items	Client 1	Client 2
Throughput (MBit/s)	106.32	105.31
Transmitted frames (bytes)	13,290,610	13,164,902
Pkts Sent(Cli)	9239	8973
Pkts Received(AP)	9099	8868
Retry	7	238
Percent retry	0.1	2.7

Table 4.5: Result of experiment when two wireless networks have Five meter distance from each other. Channel 140 pkt size 1470. Frequency 5700MHz (Band 5GHz). RTS is Off.

Items	Client 1	Client 2
Throughput (MBit/s)	87.42	119.44
Transmitted frames (bytes)	10,928,408	14,930,332
Pkts Sent(Cli)	8183	10036
Pkts Received(AP)	8076	9945
Retry	116	31
Percent retry	1.4	0.3

Table 4.6: Result of experiment when two wireless networks have One meter distance from each other. Channel 108 - pkt size 6560. Frequency 5540MHz (Band 5GHz). RTS is Off.

Items	Client 1	Client 2
Throughput (MBit/s)	105.42	149.35
Transmitted frames (bytes)	13,178,081	18,669,650
Pkts Sent(CLi)	9821	13833
Pkts Received(AP)	9737	13744
Retry	263	190
Percent retry	2.7	1.4

Table 4.7: Result of experiment when two wireless networks have Five meter distance from each other. Channel 108. Pkt size 6560. Frequency 5540MHz (Band 5GHz). RTS is Off.

Items	Client 1
Throughput (MBit/s)	112.66
Transmitted frames (bytes)	14,082,704
Pkts Sent(CLi)	12860
Pkts Received(AP)	12790
Retry	608
Percent retry	4.7
RTS threshold (bytes)	2346

Table 4.8: Result of experiment when only Client1 and AP1wireless network works stand-alone. Distance between client and AP is One meter. Channel 108. Pkt size 2100. Frequency 5540MHz (Band 5GHz).

Items	Client 1
Throughput (MBit/s)	95.10
Transmitted frames (bytes)	11,887,647
Pkts Sent(CLi)	10826
Pkts Received(AP)	10785
Retry	806
Percent retry	7.4
RTS threshold (bytes)	2346

Table 4.9: Result of experiment when only Client1 and AP1wireless network works stand-alone. Distance between client and AP is Five meter. Channel 108. Pkt size 2100. Frequency 5540MHz (Band 5GHz).

Items	Client 1
Throughput (MBit/s)	107.54
Transmitted frames (bytes)	13,443,593
Pkts Sent(CLi)	9144
Pkts Received(AP)	9046
Retry	120
Percent retry	1.3
RTS threshold (bytes)	2346

Table 4.10: Result of experiment when only Client1 and AP1wireless network works stand-alone. Distance between client and AP is One meter. Channel 108. Pkt size 1470. Frequency 5540MHz (Band 5GHz).

Items	Client 1
Throughput (MBit/s)	100.24
Transmitted frames (bytes)	12,530,199
Pkts Sent(CLi)	8521
Pkts Received(AP)	8406
Retry	626
Percent retry	7.4
RTS threshold (bytes)	2346

Table 4.11: Result of experiment when only Client1 and AP1wireless network works stand-alone. Distance between client and AP is Five meter. Channel 108. Pkt size 1470. Frequency 5540MHz (Band 5GHz).

Items	Client 1
Throughput (MBit/s)	103.69
Transmitted frames (bytes)	12,961,709
Pkts Sent(CLi)	8763
Pkts Received(AP)	8653
Retry	102
Percent retry	1.2
RTS/CTS	Off

Table 4.12: Result of experiment when only Client1 and AP1wireless network works stand-alone. Distance between client and AP is One meter. Channel 140. Pkt size 1470. Frequency 5700MHz (Band 5GHz).

Items	Client 1
Throughput (MBit/s)	88.46
Transmitted frames (bytes)	11,058,450
Pkts Sent(CLi)	7470
Pkts Received(AP)	7383
Retry	216
Percent retry	2.9
RTS/CTS	Off

Table 4.13: Result of experiment when only Client1 and AP1wireless network works standalone. Distance between client and AP is Five meter. Channel 140. Pkt size 1470. Frequency 5700MHz (Band 5GHz).

Items	Client 1
Throughput (MBit/s)	105.41
Transmitted frames (bytes)	13,177,100
Pkts Sent(CLi)	9822
Pkts Received(AP)	9719
Retry	165
Percent retry	1.7
RTS/CTS	Off

Table 4.14: Result of experiment when only Client1 and AP1wireless network works standalone. Distance between client and AP is One meter. Channel 108. Pkt size 6560. Frequency 5540MHz (Band 5GHz).

Items	Client 1
Throughput (MBit/s)	45.85
Transmitted frames (bytes)	5,731,370
Pkts Sent(CLi)	4287
Pkts Received(AP)	4232
Retry	151
Percent retry	3.6
RTS/CTS	Off

Table 4.15: Result of experiment when only Client1 and AP1wireless network works standalone. Distance between client and AP is Five meter. Channel 108. Pkt size 6560. Frequency 5540MHz (Band 5GHz).

Items	Client 1
Throughput (MBit/s)	108.62
Transmitted frames (bytes)	13,577,109
Pkts Sent(CLi)	9237
Pkts Received(AP)	9085
Retry	32
Percent retry	0.4
RTS/CTS	Off

Table 4.16: Result of experiment when only Client1 and AP1wireless network works stand-alone. Distance between client and AP is One meter. Channel 108. Pkt size 1470. Frequency 5540MHz (Band 5GHz).

Items	Client 1
Throughput (MBit/s)	28.98
Transmitted frames (bytes)	3,621,915
Pkts Sent(CLi)	2667
Pkts Received(AP)	2441
Retry	21
Percent retry	0.8
RTS/CTS	Off

Table 4.17: Result of experiment when only Client1 and AP1wireless network works stand-alone. Distance between client and AP is Five meter. Channel 108. Pkt size 1470. Frequency 5540MHz (Band 5GHz).

and Analysis

Chapter 5

Discussion and Future Work

In this chapter measurement tools, actions required to do the measurements as well as dif culties and challenges occured during measurements will be discussed. In addition, any probable weakness of the measurement tools and methodology was used for the measurements will be discussed.Issues regarding hardware and software, possible adjustment as well as possible future works will be discussed at the end.

5.1 Problems and challenges occured during measurement

As approach chapter explained the Raspberry Pi devices with a common Debian-based Rasberian operating (32-bit) system was used for client machines during the measurements. By default wireless network interface card is setup to work in promiscuous mode or manage mode. Manage mode is used to make a wireless link to its corresponding access point. Therefore, it is not possible to sniff the data link layer's behaviour when wireless card is in promiscuous mode. It required to understand how it is possible. By this research study the author realized that in order for capture MAC frame elds and access to the required items it is required to set the wireless network interface in the Monitor mode Therefore, it enables thewlan interface to capture/sniff data link layer frames and subsequently to understand how many frames transmitted at once how many re-transmitted. Also, it gives in detail information about WLAN behavior.

Due to [37] in order to capture radio-layer information about packets and observe information in this layer wireless card must change from the state of manage mode to monitor mode. To address the problem the author investigated to understand how this work is possible. Since it is not possible for the Raspberry Pi operating system (Which is recommended by default) to set the card from promiscuous mode to monitor mode other operating system who can support the monitor mode feature was required for the project instead. Thus, after so many research and challenging the author was addressed the problem through an speci c kali Linux operating system customized for Raspberry Pies uses NEXMON rmware. As this rmware is integrated to the kernel of the kali Linux operating system customized for Raspberry Pi it doesn't require to install it afterwards. Due to [30] NEXMON is a C-based rmware patching framework for Broadcom/Cypress Wi-Fi chips enables Monitor mode with radiotap headers and frame injection.

After setting the card from promiscuous mode to monitor mode it was observed that the card in some

measurement do not work 100 percent stable. In this condition, as the card presented it is active, but there was not traf c captured by the card so therefore a reboot for the entire operating system was required to repeat the measurement again.

The second challenge: When the Wi-Fi card is in Monitor mode it is not possible to keep client's connection to the corresponding access point. Therefore, it was required to realize that how it is possible to keep client's connection to access point and have access to Monitor feature to capture air traf c at the same time. It is not possible to have access to both features promiscuous mode to monitor mode at the same time. Therefore, the author had to come up with a solution. To address the problem following alternatives has been considered:

Alternative one: To have an extra USB-based wireless card and make a bridge connection with Raspberry pi's wireless card. Therefore, one card can be in Monitor mode and can capture MAC frame elds and the second card in Manage mode can keep the connection to the access point. Therefore, traf c can be sent on the air and can capture frames from data link layer. This alternative was not successful. The reason was the USB-based card could not be detected though Raspberry Pies OS after so much challenge. Therefore, other solution required to be considered. Figure 5.1 represents the rst architecture which was not successful.

Figure 5.1: Single network with USB wireless card on a client

The second alternative: The second alternative has a different design architecture compared with alternative one. In this solution one client and one access point can make a link through manage/operational mode card. In addition, one Raspberry Pi device can work stand-alone in Monitor mode and can capture radio-layer information. Also, it captures nearby (uncontrolled) wireless network traf c on the air. Figure 5.2 illustrates the second alternative design. This solution was successfully implemented and the desired elds captured through Wiresharkand subsequently the pcap les produced as a result of measurements.

Figure 5.2: Single network and monitor mode device captures traf c information from air.

5.1.1 Equipment problems

It is important to note that with the presence of the second network Client2 and AP2as interferenetwork some dif culties were experienced. For instance, it was required to do actions in three different devices at the same time to start the test. So, those are as follows:

- Step one is to plug the Ethernet cable to Raspberry Pi's Ethernet interface who has a role of Monitor. Then, start Wiresharkand push to start button to start capturing/snif ng air traf c. (This is the place where that it was observed card do not work stable sometimes, therefore reboot in OS and re-con guration on wlan card was required.)
- Step two is to unplug Ethernet cable from Monitor Raspberry Pi device and plug the cable to the Client 2 and start throughput testing in order to send traf c on the link to ood the channel with the purpose of making an interferenetwork for Client1 and AP1
- Step three is to unplug the cable from Client 2 device and plug to Client 1 to start throughput testing on Client1 and AP1

All actions introduced above were required to execute at the same time as fast as possible in order to run test in the same timeframe. Also, only one Ethernet cable was available to use and switch between devices. Therefore, switching between devices to have access to the console of devices and do the action was another challenge which made a bit delay to have access to the console of each device (a delay of 5 to 10 seconds). This is because it took a bit time to connect to the console of device after cable unplugged from one and plugged to another device. It is better to have three Laptops computer so each Laptop can control one device. Figure 5.3 illustrates the steps.

Figure 5.3: Steps to capture air traf c with the presence of Client2 ans AP2as ainterferenetwork.

It is noticeable that the Raspberry Pi device who has a role of capturing data link layer, the Monitor modeinterface showed that it is not working stable and it crashes sometimes during measurements. This is because it seems capturing/ snif ng air traf c is a very heavy process. Therefore, it requires a professional wireless network interface to handle the work (Raspberry Pi Wi-Fi card do not recommended). This is because after each measurement the operating system of Raspberry Pi required reboot.

Figure 5.4 represents steps was required to run TP testing by one Ethernet cable.

5.1.2 The measurement tool used before iperf3

Before using iperf3 for throughput testing, the other TP testing application was used. After doing so many tests, the result showed that the TP tester is not suitable for measurement as it sends data frame from client to access point and reverse back to client and it is not possible to decide for time of throughput testing as well as Pkt size. In addition, it is not possible to control time when throughput testing start. Therefore, this work should be done manually. In order to have control to measurements it was required to go to more professional TP tester. To gure out the matter, iperf3was used. iperf3can cover the required features and it was used by other researchers for throughput testing. For example Michael et al[9].

Figure 5.4: Steps to capture air traf c without the presence of Client2 and AP2as a interfere network.

5.2 Result of measurement accumulated by other researcher

For experiment, Michael et al [9] used their own platform and devices which is different with the devices was used in this project. According to Michael they used Laptops (meaning that more than one) with Netgear WAG511v2 PCMCIA cards 802.11 a/b/g (AR5212 chipset and the Madwi driver). In addition, they claim that they used CORAL testbed which is pretty speci c so the refer explain that testbed. CORAL [38] and [39] is developed by the Communication Research Center (CRC) to provide a reseach study platform for studying interference in WLAN 802.11 b/g networks according to [9]. They claim that the platform itself contains two different parts: a hardware called WIFI-CR and a software for storing obtained interference information and controlling the hardware. The mentioned that the WIFI-CR contains of a common off-the-shelf roruterboard RB433 from Miktotik which is equipped with two Wistron CM9 802.11 a/b/g miniPC cards (AR5212 chipset). The claim that the rst card is set to promiscuous mode and is used to sniff 802.11 b/g packets independently of the second transceiver card. The routerboard is encapsulated by a shell of FPGA and RAdio Front-end (RF) circuitry to control the traf c ows of the routerboard. Also, They mention the shell involves a simple built-in spectrum analyzer for energy detection. So, in this project the author was use WiFi Analyzer which was downloaded form Google play and was the best possible tool available to detect nearby access point and see and analyse

in which channel they work. This work was required to find a most clear channel available in the test environment. They claim the operating system of the routerboard is OpenWRT. Also, they mention that the drawback of the encapsulation approach is a decrease of the maximum throughput by at least 20 percent. Also, only the 2.4 GHz band can be used.

It is noticeable that they have access to the distances form 0 to 18 meter for doing measurements in their Lab and they compare the different throughput result in different distances such as 4, 8, 12, 15 and 18 meters. To summarize the discussion regarding their research work, the result they accumulated is different from result accomplished for this research project as they use different setup, wireless assets as well as the lab environment they used. To detail information refer to [9].

5.3 Future work

For the future work of this project it is recommend to use more professional wireless assets rather than Raspberry Pi devices. For instance, a wireless card can support monitor feature without the help of operating system and a specific firmware in order to be able to handle the heavy process itself and record data in its local memory card. Therefore, result would be more concrete and reliable. As it was introduced above assets which Michael et al [9] used is more professional than Raspberry Pi devices such as finding a reasonable OS to capture data link layer. In addition, distance is another factor which should be take it into account. The longer distance the more diverse results can be obtained for further analysis.

5.4 Challenges occured during special days

It is important to mention that working on the project entirely carried out in the author's small flat which limited the distance variation and affected other things. One reason is that it faced with the pandemic restriction so that the author had to stay home and work alone entirely with the given wireless assets in hand. Therefore, it made the work challenging and increased difficulties for the entire work. Also, specifically when the author had to fix technical problems and challenge happened in devices. Although he supported by his supervisor digitally, but the author believe working in the real lab with more professional devices could be more interesting and reduces challenges specifically in the pandemic days. By the way, the author worked so hard during the difficult days and he tried to produce a project as perfect as possible with the help of his supervisors. The author believe sharing difficulties happened during the work has positive effect on the future work of the project.

Chapter 6

Conclusion

The problem statement for this thesis explained, in IEEE 802.11 accessing to a wireless channel is controlled by the carrier sense mechanism. Also, explained CCA is a function works in conjunction with CSMA/CA to perform the channel access by observing the channel with the purpose of frame transmission.

In this thesis we studied and observed when channel is busy it waits so therefore throughput goes down and result in a low performance of wireless network. The mentioned result was observed and illustrated through different measurements. For instance, when distance between two wireless networks is one meter interference occurs and throughput goes down . In addition, the number of re-transmission increases and produce faults and error. Moreover, we observed when the RTS mechanism in under control by access point a few percentage of re-transmissions occurs.

The second problem was explained in problem statement was when the received signal by client is weak or not detected by client and re-transmission start. Then, the percentage of re-transmission increases so therefore throughput decreases accordingly and result in a weak performance on that network. Through different experiments illustrated that this problem occurs speci cally when there is only single wireless network works stand-alone and when distance between a client and it corresponding access point increase.

It is noticeable that a few experiments are exist which they repeated with the purpose of observing different results for further analysis and future work of this project. Also, the interesting aspect of this work is that it reports network behaviour in the data link layer which is accumulated by the author. It makes possible to observe directly number of re-transmission and percentage of re-transmission of frames in different measurements.

Overall, it is noticeable that the wireless equipment's, measurement tools as well as the environment tests has been carried out are different from equipment's that other researchers used in their research project. This problem was discussed in the discussion chapter in detail. Therefore, in the measurements with the presence of interfering network results showed surprisingly small degradation in throughput compared with other measurements reported in [9].

Chapter 7

Appendix

7.1 The Python script

When the measurement of throughput testing has been carried out the pcapwill be generated through Wireshark in Monitor mode card. Therefore, pcap les are calculated to realize that how many data frames transmitted from client to access points and the number of frames. It is possible to obtain the same statistic from Wireshark as well. Written by Madeleine.

```
import argparse
import os
from time import sleep
import sys
from scapy.utils import PcapReader
from scapy.layers.dot11 import *
from scapy.packet import Packet
from scapy.all import *

def get_data_frames():
    myreader = PcapReader(FILE_NAME)
    for pkt in myreader:
        if Dot11 in pkt and pkt[Dot11].type == 2:
            yield pkt

def get_data_frames_from_to(fromNode, toNode):
    for pkt in get_data_frames():
        DS = pkt[Dot11].FCfield & 0x3
        to_DS = DS & 0x1 != 0
        from_DS = DS & 0x2 != 0

        # If data frame going is going from Client ---> AP:
        if to_DS and not from_DS and pkt[Dot11].addr3 == toNode and pkt[Dot11].addr2 == fromNode:
            yield pkt
```

```
def count_all_data_frames():
    count = 0
    for pkt in get_data_frames():
        count = count + 1
    return count

def count_data_frames_from_to(fromNode, toNode):
    count = 0
    frames = get_data_frames_from_to(fromNode, toNode)
    for frame in frames:
        count = count + 1
    return count

def count_all_retry_data_frames():
    count = count_all_data_frames()
    retryCount = 0

    if count == 0:
        return 0

    for pkt in get_data_frames():
        retry_bit = pkt[Dot11].FCfield & 0x8!= 0
        if retry_bit:
            retryCount = retryCount +  1

    if retryCount == 0:
        return 0
    else:
        return retryCount / count

def count_retry_data_frames_from_to(fromNode, toNode):
    count = count_data_frames_from_to(fromNode, toNode)
    frames = get_data_frames_from_to(fromNode, toNode)
    retryCount = 0

    if count == 0:
        return 0

    for pkt in frames:
        retry_bit = pkt[Dot11].FCfield & 0x8!= 0
        if retry_bit:
            retryCount = retryCount + 1

    if retryCount == 0:
        return 0
```

```
        else:
            return retryCount / count

def data_frame_bytes_from_to(fromNode, toNode):
    count_bytes = 0
    frames = get_data_frames_from_to(fromNode, toNode)
    for pkt in frames:
        count_bytes = count_bytes + len(pkt[Dot11].payload)
    return count_bytes

def process_pcap(AP, CLIENT):
    print("All data frames:", count_all_data_frames())
    print("Data frames", CLIENT, (client) ----> , AP, (AP): ,
    print("\nPercentage of re-transmitted data frames:"
    print("Percentage of re-transmitted data frames", CLIENT, (client) ----> , AP,
    print("\nData frame bytes", CLIENT, (client) ----> , AP,

if __name__ == __main__ :
    parser = argparse.ArgumentParser(description= PCAP reader )
    parser.add_argument( --pcap , metavar= <pcap file name> ,
                         help= pcap file to parse , required=True)
    parser.add_argument( --client , metavar= <client MAC address> ,
                         help= The transmitting node , required=True)
    parser.add_argument( --ap , metavar= <AP MAC address> ,
                         help= The receiving node , required=True)
    args = parser.parse_args()

    global FILE_NAME

    FILE_NAME = args.pcap
    AP = args.ap
    CLIENT = args.client


    if not os.path.isfile(FILE_NAME):
        print( "{}" does not exist .format(FILE_NAME))
        sys.exit(-1)

    print("Starting processing of PCAP file", FILE_NAME, "\n")
    process_pcap(AP, CLIENT)
    sys.exit(0)
```

7.2 Wireshark lters

wlan.fc.type_subtype == 40) > to filter QoS Data frames (7.1)

wlan.fc.type_subtype == 2) > to filter all Data frames (7.2)

wlan.fc.tods == 1) > to filter retry bit towards access point (7.3)

wlan.fc.fromds == 1) > to filter retry bit from access point to client (7.4)

[35]

Bibliography

[1] Wi-Fi-Alliance. Wi- alliance® celebrates 20-year milestone, industry momentum continues. [Online]. Available: https://www.wi- .org/news-events/newsroom/wi- -in-2019

[2] Wi-FiAlliance. Wi- alliance® wi- ® predictions for 2021. [Online]. Available: https://www.wi- .org/news-events/newsroom/wi- -alliance-wi- -predictions-for-2021

[3] maui communications. Wi channel description. [Online]. Available: https://www.maui-communications.net/802-11-channel-frequency-allocation

[4] T. O'Brien. Channel planning best practices for better wi- . [Online]. Available: https://www.ekahau.com/blog/channel-planning-best-practices-for-better-wi- /#:~:text=The%202.4GHz%20band%20is,20%20MHz%2D160%20MHz).

[5] E. Geier. signal to noise. [Online]. Available: https://www.networkworld.com/article/2215287/coping-with-wi- -s-biggest-problem-interference.html

[6] WIKI. Snr. [Online]. Available: https://en.wikipedia.org/wiki/Signal-to-noise_ratio

[7] wiki. Csma/cd. [Online]. Available: https://en.wikipedia.org/wiki/Carrier-sense_multiple_access_with_collision_detection

[8] Wiki. Hidden node. [Online]. Available: https://en.wikipedia.org/wiki/Hidden_node_problem

[9] M. Doering, . Budzisz, D. Willkomm, and A. Wolisz, "About the practicality of using partially overlapping channels in ieee 802.11 b/g networks," in 2013 IEEE International Conference on Communications (ICC) IEEE, 2013, pp. 5110–5114.

[10] wiki PIFS. Factor affecting wi performance. [Online]. Available: https://www.fastmetrics.com/blog/wi /factors-affecting-wi -performance/

[11] S. Feirer and T. Sauter, "Seamless handover in industrial wlan using ieee 802.11k," in 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE) 2017, pp. 1234–1239.

[12] S. Woo and H. Kim, "An empirical interference modeling for link reliability assessment in wireless networks," IEEE/ACM Transactions on Networking, vol. 21, no. 1, pp. 272–285, 2012.

[13] T. Huehn, R. Merz, and C. Sengul, "Joint transmission rate, power, and carrier sense settings: An initial measurement study," in 2010 Fifth IEEE Workshop on Wireless Mesh Networks IEEE, 2010, pp. 1–6.

[14] P. Riihikallio. power level. [Online]. Available: https://metis. /en/2017/10/txpower/#:~:text=By%20default%20almost%20all%20WiFi,a%20fraction%20of%20the%20maximum.

[15] NetSpot. Sir. [Online]. Available: https://www.netspotapp.com/help/troubleshooting-sir/#:~:text=The%20signal%2Dto%2Dinterference%20ratio,present%20from%20other%20radio%20transmitters.

[16] "The effective of adjacent channel rejection and adjacent channel interference," in International Conference on Wired/Wireless Internet Communication. Texas-Instruments, 2003, p. 3.

[17] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan, "Understanding and mitigating the impact of rf interference on 802.11 networks," ACM SIGCOMM Computer Communication Review, vol. 37, no. 4, pp. 385–396, 2007.

[18] F. Metrics. affect interference. [Online]. Available: https://www.fastmetrics.com/blog/wi-/factors-affecting-wi-performance/

[19] A. Saif, M. Othman, S. Subramaniam, and N. A. Abdul Hamid, "Frame aggregation in wireless networks: Techniques and issues," IETE Technical Review, vol. 28, no. 4, pp. 336–350, 2011.

[20] K. Jamieson, B. Hull, A. Miu, and H. Balakrishnan, "Understanding the real-world performance of carrier sense," in Proceedings of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis, 2005, pp. 52–57.

[21] A. N. Alvi, S. H. Bouk, S. H. Ahmed, and M. A. Yaqub, "In uence of backoff period in slotted csma/ca of ieee 802.15. 4," in International Conference on Wired/Wireless Internet Communication. Springer, 2016, pp. 40–51.

[22] L. Chang, F. Wang, and Z. Wang, "Detection of dsss signal in non-cooperative communications," in 2006 International Conference on Communication Technology, 2006, pp. 1–4.

[23] hostapd con guration le. Mac frame. [Online]. Available: https://www.geeksforgeeks.org/ieee-802-11-mac-frame/

[24] mac. mac. [Online]. Available: https://www.brainkart.com/article/IEEE-802-11_13458/

[25] D. Sharma and D. A. Karandikar, "Qos in wireless networks," in QoS in Wireless Networks, p. 230.

[26] T. Li, T. Tang, and C. Chang, "A new backoff algorithm for ieee 802.11 distributed coordination function," in 2009 Sixth International Conference on Fuzzy Systems and Knowledge Discovery, vol. 3. IEEE, 2009, pp. 455–459.

[27] A. Malik, J. Qadir, B. Ahmad, K.-L. A. Yau, and U. Ullah, "Qos in ieee 802.11-based wireless networks: a contemporary review," Journal of Network and Computer Applications, vol. 55, pp. 24–46, 2015.

[28] V. V. Kapadia, S. N. Patel, and R. H. Jhaveri, "Comparative study of hidden node problem and solution using different techniques and protocols," arXiv preprint arXiv:1003.4070, 2010.

[29] W. Hneiti and N. Ajlouni, "Performance enhancement of wireless local area networks," in 2006 2nd International Conference on Information & Communication Technologies, vol. 2. IEEE, 2006, pp. 2400–2404.

[30] seemoo. Monitor mode feature. [Online]. Available: https://github.com/seemoo-lab/nexmon

[31] maui communications. monitor mode. [Online]. Available: https://www.aircrack-ng.org/doku.php?id=airmon-ng

[32] throughput. Sniff the mac frames. [Online]. Available: https://wireless.wiki.kernel.org/en/developers/documentation/mac80211/ratecontrol/minstrel

[33] hostapd configuration file. fixed rate. [Online]. Available: https://w1.fi/cgit/hostap/plain/hostapd/hostapd.conf

[34] kali. Kalilinux. [Online]. Available: https://www.offensive-security.com/kali-linux-arm-images/

[35] Wireshark-filter. Sniff the mac frames. [Online]. Available: https://dalewifisec.wordpress.com/2014/04/29/wireshark-802-11-display-filters-2/

[36] networkdirection.net. Mtu. [Online]. Available: https://networkdirection.net/articles/network-theory/mtu-and-mss/

[37] Wireshark. Sniff the mac frames. [Online]. Available: https://wiki.wireshark.org/CaptureSetup/WLAN

[38] J. Sydor, "Coral: A wifi based cognitive radio development platform," in *2010 7th International Symposium on Wireless Communication Systems*. IEEE, 2010, pp. 1022–1025.

[39] R. Ruby, S. Hanna, J. Sydor, and V. C. Leung, "Interference sensing using coral cognitive radio platforms," in *2011 6th International ICST Conference on Communications and Networking in China (CHINACOM)*. IEEE, 2011, pp. 949–954.