The Effect of Human Movement, Security, and Shadowing on Latest Wireless LAN Standard (IEEE802.11ac)

By

Abdulbasit Almatrook

A thesis submitted in partial fulfilment of the requirements for the degree of Master of Computing

Unitec Institute of Technology, 2016

ABSTRACT

This thesis focuses on the evaluation of IEEE 802.11ac WLAN performance using TCP and UDP for both versions of the Internet Protocol (IPv4, IPv6) in three scenarios, namely, the effect of implementing WPA2 security encryption, the impact of shadowing (walls) and distance in laboratory environment, and human movement effects in indoor environmental conditions. This thesis will also provide knowledge about the behaviour of commonly used protocols on a new wireless standard (802.11ac) in real network environments. The performance metrics of wireless network test-beds such as throughput, round trip time, and CPU utilisation are gathered and analysed.

The findings of this study concludes that the shadowing environment and distance have a severe impact of 802.11ac WLAN performance. Applying WPA2 security also reduces the performance metrics measurement. The presence of human movement has an insignificant impact of the 802.11ac WLAN performance. IPv4 outperforms IPv6 on different levels, depending on the network environment. TCP provides lower performance than UDP.

This thesis will be beneficial to academic researchers and to businesses wanting to get the best performance out of IEEE 802.11ac standard.

ACKNOWLEDGEMENTS

I would like to thank my family for believing in me to go further studies and their encouragement. I would like to express my heartfelt thanks for my beloved mom who never stop praying for me to get a highest levels of my life.

I would like to express my gratitude to my supervisor Dr. Samad Kolahi, for giving me the opportunity to work with you, your valuable pieces of advice, and for your guidance and patience.

I would like to thank all my friends who kindly shared their good and bad time with me.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLS

LIST OF ABBREVIATIONS

ACI	Adjacent Channel Interfering
AP	Access Point
BSS	Basic Service Set
BYOD	Bring Your Own Device
CCA	Clear Channel Assessment
CGA	Cryptographic Generated Address
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DS	Distribution System
ESS	Extended Service Set
FSPL	Free Space Loss
GUI	Graphical User Interface
IBSS	Independent Basic Service Set
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
LDPC	Low-Density Parity Check
LOS	Line Of Sight
MAC	Media Access Control
MIMO	Multiple-Input and Multiple-Output
MIPv6	Mobile IPv6
MOV	human movement
MPDU	MAC Protocol Data Unit
MSS	Maximum Segment Size
MU-MIMO	Multi-user MIMO (MU-MIMO)
OFDM	Orthogonal Frequency Division Multiplexing
OS	Open System
PDA	Personal Digital Assistant
PHY	Physical Layer
QAM	Quadrature Amplitude Modulation
RF	Radio Frequency
RTS/CTS	Request to Send / Clear to Send
RTT	Round Trip Time
RX	Receiver
SCTP	Stream Control Transmission Protocol
SISO	Single Input, Single Output
SNR	Signal-to-Noise Ratio
SS	Spatial Stream
STA	Station
TCP	Transmission Control Protocol
TX	Transmitter
UDP	User Datagram Protocol
WEP	Wired Equivalent Privacy

WFA	Wi-Fi Alliance
WLAN	Wireless Local Area Network
W-MOV	Without human movement
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access II

CHAPTER 1

INTRODUCTION

One of the fastest growing sectors of the telecommunication industry is wireless communication. Having a Wi-Fi network simply creates new possibilities. It provides a cheap and stress-free way to connect more than one device with a single Internet connection and allows mobility while using an Internet connection. Wireless network has the ability to expand easily by adding extra new devices without the mess of more wires and with little additional cost. The systems that offer wireless communication include cellular phones, cordless, satellites and Wireless Local Area Networks (WLANs). These systems have recently become a part of day-to-day life of almost everyone and a favourable choice for communicating. Wi-Fi network provides access from anywhere at anytime. It is not only being used as a substitute to wired systems, but it is also preferred over wired communication systems. Statistics revealed that in 2014 almost 10 billion devices were connected through wireless communication, and this figure is expected to rise to 50 billion by 2020 [1]. In 2011, shipments of Wi-Fi certified microchips surpassed one billion units and are expected to be more than 2.5 billion units per year by 2016 [2].

The IEEE 802.11 standard is commonly used for Wi-Fi communications. All the latest Internet devices including smartphones, laptops, and PDAs (personal digital assistant) have WLAN chipsets built-in to support this standard. The latest standard IEEE 802.11ac provides significantly higher data rates, client capacity, and density than previous standards and directly addresses the user demands generated by the explosion of mobile and Bring Your Own Device (BYOD) [3].

The existing methods used for securing wireless networks are based on modern cryptography techniques. Issues with the initial WEP encryption led to the introduction of new encryption technology to enhance the security from wireless penetration including WPA and WPA2. However, the implementation of these security methods has had a negative effect on the WLAN performance. The security encryption adds extra bits on the packet size that can reduce the data transfer rate [4].

Wireless networks have the capability to sense radio signals as long as they are in the range of radio signals' coverage. One of the essential factors that impacts on the performance on Wireless LANs is the radio propagation environment. Shadowing takes place when there is some obstruction between a transmitter and the receiver [5]. Signals can be either attenuated

from propagation through walls or distorted from dispersion wall materials. Strong signal and data transmission rates can be significantly decreased when radio waves are refracted by different objects in a propagation environment. Interference of radio waves occurring in a dense environment can cause network issues, where increasing packets drop and delay over a Wi-Fi network. Human shadowing has a negative impact on WLAN performance in an indoor environment. Receiving signal strength is even influenced by the human body in some cases where the receiver gains the signals from multiple transmitters [5].

Recently, IPv4 is the most extensively adopted network layer protocol in WLANs. IPv4 provides 2^{32} addresses, which cause a shortage in address space leasing. IPv6 is the latest technology and is claimed to outperform IPv4 by allowing 2^{128} addresses. IPv6 is advantageous over IPv4 in many aspects; it provides more effective routing, better packet processing, better mobility, improved network autoconfiguration and more security [6].

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are used at transport layer. TCP establish a connection between two nodes before sending any data to ensures the secure and organised streaming of Bytes from a server to the receiver and the other way around. UDP is Connectionless, which delivers packets to another node even if there is no connection. Hence, the service provided by UDP is unreliable and it is possible that while using this service, the datagrams can get out of order or even go missing without one's knowledge [7].

In this thesis, the performance of IEEE 802.11ac (Windows 8.1 - Windows Server 2012) WLAN was evaluated using TCP and UDP for both versions of the Internet Protocol (IPv4, IPv6). Performance experiments were conducted in three different network scenarios, namely, shadowing (walls) and distance effects in laboratory environment, the impact of implementing WPA2 security encryption, and the effect of human movement in an indoor environment. In each of the three contexts, various networks have been implemented on test-beds and then performance-related metrics (throughput, round trip time, CPU utilisation) were measured and analysed. It was envisaged that this undertaking would lead to a better understanding of 802.11ac network performance behaviours in a new IPv6 environment.

1.1 Thesis Objectives

The primary focus of this thesis is to evaluate the new IEEE 802.11ac WLAN's performance characteristics and produce new results. In each of the three scenarios explained above, various network test-beds have been implemented to evaluate protocol behaviour with regard

to throughput, round trip time (RTT) and CPU utilisation. Thus, the core objectives of this thesis are:

1. To quantify the impact of implementing WPA2 encryption on the performance of wireless networks 802.11ac, taking the measurement for throughput, round trip time, and CPU utilisation.
2. To investigate the impact of shadowing (walls) and distance on 802.11ac WLAN link in an obstructed environment. We evaluate the relationship between shadowing and Wi-Fi link throughput, delay, and CPU utilisation through measurements. This information will help with identifying the optimal locations for APs placement.
3. To investigate the impact of human movement on 802.11ac Wi-Fi link throughput, delay, and CPU utilisation in an indoor propagation environment and provide a comparative analysis to identify if there is any the significant difference in Wi-Fi performance compared to no human obstacle.
4. To examine the performance of 802.11ac WLANs in IPv6 vs IPv4 environment.
5. To examine the performance of 802.11ac WLANs in TCP vs UDP environment.

The thesis evaluation will enhance knowledge related to IEEE 802.11ac WLAN's performance. This will be very useful for expert practitioners who may be determining the best choice to select of this technology they are to implement in their network infrastructures.

1.2 Related Work

In this section, a brief review of the existing literature on the evaluation of 802.11ac wireless networks is presented. However, some research that is relevant to the thesis objectives from IEEE 802.11 g and n are added as related work, especially where 802.11ac data was not available.

In 2015, S. Narayan, et al. [8] carried out a comparative peer-to-peer performance evaluation in 802.11ac and 802.11n WLANs for both versions of the Internet Protocol on Windows 7 operating system. Router channel width settings were configured at 20MHz and 40MHz to 2.4GHz and 5GHz bands respectively in 11n, whereas 11ac located at 80MHz channel width. The outcomes noted that on average, 802.11ac provides a higher throughput than WLAN counterpart (802.11n) for both versions of the Internet Protocol. TCP throughput for 11n in 2.4GHz bands outperforms 11n in the 5GHz bands for both IPv4 and IPv6. On the contrary, 11n in the 5GHz bands has a higher UDP data rate than 11n in the 2.4GHz band for both IPv4

and IPv6. Both WLAN (11ac, 11n) have a highest jitter values by applying IPv4 compared with applying IPv6.

In 2015, Y. Zeng, et al. [9] measured the performance of 802.11ac networks. The impact of various parameters including distance, power consumption, and interference on throughput was measured with varied packet sizes in indoor environments. UDP throughput declined significantly by 91% (585 Mbps) when the receiver was located 90 metres away from the Access Point (AP) in denser network (contains 5 AP and 13 clients) with fixed location to achieve the maximum distance in indoor environments. The experiment was replicated for 802.11n, which was operating in the 5GHz band. Results showed that on the average the UDP throughput is almost doubled on 802.11ac compared with 802.11n. Increasing the number of Spatial Stream (SS) from 1 to 6 provides a lower power consumption by 40% (20 Milliwatt) and increases the throughput to 350 Mbps, which can be achieved by doubling the channel width from 40MHz to 80MHz. 802.11ac channel widths should be selected wisely because the capability of 802.11a/n to operate at 40/20 MHz in the 5GHz band, causes interference to an 802.11ac Access Point.

In 2015, R. S. Cheng, et al. [10] investigated the performance of the emerging communication protocol called Stream Control Transmission Protocol (SCTP) over 802.11ac WLANs by implementing analytical modelling. The protocol has been developed to improve the communication quality in Wi-Fi networks. The results showed that the SCTP outperforms the Transmission Control Protocol (TCP). SCTP offers higher throughput because it utilises a higher number of streams by reducing the delay time. SCTP over the 802.11ac network has faster and more stable performance compared with previous IEEE 802.11 standards.

In 2015, F. Siddiqui et al. [11] addressed the issues that restrict IEEE 802.11ac from achieving the maximum throughput beyond 1Gbps. The study focused on the performance of several 11ac new features by implementing a test-bed of devices supporting 802.11ac draft. The results showed that to obtain the highest data rates, all the spatial streams that are installed at the Access Point should be utilised by the client device. Also, use of 80MHz and 160MHz channel widths is more susceptible to radio frequency interference than 20/40MHz. In addition, advanced modulation formats (256-QAM) can be utilised in a situation that has a high Signal-to-Noise ratio (SNR), or low radio frequency interference. Finally, beamforming technology can work well when AP is close to the client device area.

In 2014, M. D. Dianu, et al. [12] examined the effect of distance, propagation environments, and Wi-Fi interference on 802.11ac WLANs performance in an indoor environment. It was concluded that the maximum UDP throughput achievable in the typical environment was 700

Mbps at channel width 80MHz. However, the throughput dropped significantly by 87.12% (90.1 Mbps) when the receiver (RX) was placed 24.3 metres away from the transmitter (TX) and environmental obstructions were a supporting concrete wall and three soft partitions. To measure the impact of legacy standard interference, IEEE 802.11n WLAN was set up and placed close to the TX or on the RX. Results showed that the UDP data rate of the 802.11ac WLAN is significantly reduced when 11n network sends and receives the packet size simultaneously at a same 11ac channel width (40MHz).

In 2014, M. O. Demir, et al. [13] carried out a comparative examination of IEEE 802.11ac WLANs with regards to the power consumption of the access point during transfer data in server-client LANs test-bed. Data was gathered by considering various parameters like packet size, bandwidth channel and transmit energy level. Results showed that the highest throughput was achieved when all packet sizes (64 Byte to 1470 Byte) were sent in channel width at 80 MHz, which also the highest energy consumed. The energy efficiency was achieved when short packet lengths (64 Byte to 256 Byte) were sent in channel width at 20MHz, and long packets (1024 Byte to 1470 Byte) were sent in channel width at 80MHz. The transmit power level configuration has a tiny effect in terms of power consumption.

In 2014, G. Patwardhan, et al. [14] evaluated the vulnerability of IEEE 802.11ac beamforming by a new type of jamming attacks. The authors conducted the experiment by using jammer and sniffer devices, which were installed between client and access point in 802.11ac draft. Results showed that jamming attack has a remarkable effect on beamforming in terms of throughput degradation with 90.62% (724.5Mbps). Also, the attack reduced data rate transferred to 55.03% (478Mbps) on 802.11ac Multiple-Input and Multiple-Output (MU-MIMO) feature.

In 2014, A. Stelter, et al. [15] offered a new dynamic channel access method that increases the throughput by utilising 80/160MHz channel widths over 802.11ac WLANs. The legacy 802.11a/n signals located at 20/40MHz channels can occupy a non-primary 20MHz channel width over 80MHz 802.11ac station during the clear channel assessment (CCA). The proposed method has the ability to remove the adjacent channel interfering (ACI) signal from the received 11ac signal, which enhances throughput increment.

In 2011, M. Park, et al. [16] carried out a simulation experiment to study the effect of using the primary and secondary channel bandwidths between 20, 40, and 80MHz for the first wave of 802.11ac (draft). The results of the experiment showed that 20MHz channel width throughput was better than the static 80MHz by 85% when the secondary channels are operated by 20MHz IEEE 802.11a/n. The study concluded that dynamic bandwidth channel access was a

recommended option to access point configuration. The secondary channel plays an important role in reducing collisions between the 802.11ac and IEEE 802.11a and 11n.

In 2011, E. H. Ong, et al. [17] carried out a comparative evaluation of IEEE 802.11ac draft and IEEE 802.11n WLANs at three channel widths (40/80/160MHz) in terms of higher data rates. The performance analysis showed that 11ac at 80MHz channel width with single input, single output (SISO) outperforms 802.11n configured at 40MHz with 2×2 multiple-input and multiple-output (MIMO) by 28% higher throughput. Maximum throughput in 160MHz channel widths with SISO does not measure well with the bandwidth increment.

IEEE 802.11 n and g are presented as related works in the following part of the literature review because there is no research that covers the effect of people movement and implementing WPA2 security mechanisms on the 802.11c WLANs.

In 2013, N. I. Sarkar, et al. [18] carried out an investigation of people movement effectiveness against Wi-Fi link throughput using IEEE802.11g in various indoor environments by using radio propagation measurements. The measurements considered both the random and straight line patterns of people movement. Findings of this investigation showed that the human movement had a negative impact on transfer data rate on WLANs. The average of fixed human and random human movement throughput in different obstruction environments decreased to 7.88% and 8.82% respectively compared to non-human shadowing. The pattern of people movement has a tiny impact on throughput degradation over Wi-Fi network.

In 2012, S. Japertas, et al. [19] conducted the experimental study of the IEEE 802.11g and n signal propagation in an indoor environment. The results showed that 802.11n has stronger waveguide effect than the 802.11g in free-space with no obstacles. Single strength for 11n and 11g were spotted at 23dBm and 8dBm respectively when the receiver was located 37 metres away from the transmitter. The partition wall significantly impacted on signals level. The result showed that when the wall is present, the signal power is much lower for 11g than 11n. The average of 11n and 11g signal absorption increased to 21.2dBm and 24dBm respectively when the receiver was located 30 metres away from the transmitter.

In 2011, S.S. Pang et al. [20] conducted a peer-to-peer performance evaluation for 802.11n Wi-Fi network for versions of Internet Protocol by applying WPA2 security mechanism. Results showed that the TCP throughput WPA2 encryption enabled for Windows 7 decreased by 6.21% and 3.11% for IPv4 and IPv6 respectively compared with disabling WPA2 security on WLAN. In contrast, the TCP throughput with WPA2 encryption enabled for Fedora 12 operating system

declined by 5.55% and 3.8% for IPv4 and IPv6 respectively compared to the open system network.

In 2011, Kolahi et al. [21] examined the effect of applying WPA2 encryption on UDP (throughput, RTT) on 802.11n WLANs for both versions of the Internet Protocol. Client-server network (Windows 7-Windows Server 2008) were installed as operating systems. Implementing WPA2 for IPv4 decreased UDP throughput an average of approximately 24.33% (29.4Mbps) less than open systems. For IPv6, UDP throughput dropped at least 10.14% (11.15Mbps), compared to no security enabled.

In 2009, Kolahi et al. [22] analysed the effect of enabling WPA2 encryption on TCP throughput for both versions of the Internet Protocol on 802.11n Wi-Fi network. Three Windows operating systems were installed into two client-server networks (Vista - Server 2008 and XP - Server 2008). XP WLAN with no security implementing gained in an average about 7.07% more TCP throughput than enabling WPA2 for IPv4, and 5.42% more TCP throughput for IPv6. Implementing WPA2 security has more influence over Vista compared to XP. In Vista WLAN with WPA2 encryption enabled reduced the TCP throughput for IPv4 and IPv6 by an average to 9.39% and 17.02% less than applying these protocols on WLAN without WPA2 encryption enabled.

In 2007, Filho et al. [23] carried out a performance evaluation of IEEE 802.11g WLANs by using two security mechanisms with different cryptographic key lengths. Their results showed that WEP-128 has a significant effect on TCP in terms of throughput degradation with 20% whilst applying WEP-64 decreased UDP throughput to 8%. WPA encryption has the lowest level of influence with 14% and 6% for TCP and UDP throughput.

In 2006, Ezedin et al. [24] investigated the effect of security encryption on IEEE 802.11g WLANs performance by implementing different WEP encryption keys on TCP and UDP protocols. Results showed that implementing WEP security for key size 64-bit and 128-bit increased the TCP throughput degradation from 1.9% to 4.5% respectively. The degradation of the throughput for UDP increased slightly with WEP 64-bit by 0.23% compared to 6% with WEP 128-bit.

1.3 Thesis Contributions

This thesis is part of the ongoing works undertaken in the arena of network performance over previous decades. This research aims to produce new results on the latest wireless LAN (802.11ac) that no other researchers have found before. These new results are obtained on:

1. The comparison between the actual achievable throughput in the test-bed and the theoretical maximum throughput of 802.11ac.
2. The effect of obstructed environment and distance in an office environment on the performance of 802.11ac.
3. The effect of implementing WPA2 encryption on the performance of 802.11ac WLANs.
4. The effect of human movement on 802.11ac WLANs performance in Indoor propagation environments.
5. The performance of 802.11ac WLAN in IPv6 compared to IPv4.
6. The performance of 802.11ac WLAN in TCP compared to UDP.

The presented contents will be beneficial to academic researchers and to businesses wanting to get the best performance out of IEEE 802.11ac standard.

1.4 Structure of the Thesis

The thesis is organised as follows:

- Chapter one contains an introduction, which briefly mentions the importance of wireless and issues that confront this technology, and the objectives behind this study. This is followed by the contributions of this research and concludes by highlighting other research works with a similar focus.
- Chapter two provides background information on key concepts relating to the topic.
- Chapter three covers the details of an IEEE 802.11ac standard. This chapter explains the core technology and features of 802.11ac.
- Chapter four covers the methodologies that were employed for this thesis. This chapter also displays the methods of gathering data in laboratory experiments.
- Chapter five includes a detailed explanation of the network diagram and the specification of all hardware and software used in the test bed. It also contains hardware and software configurations, commands and monitoring tools used during the test.
- Chapters six, seven and eight cover the performance evaluation of 802.11ac WLANs in three scenarios, namely, the impact of implementing WPA2 encryption and the effect of shadowing in a laboratory environment, and the effects of human movement in an indoor environment. Each chapter analyses the results with regards to the performance of TCP and UDP for both IPv4 and IPv6 protocol mechanisms.
- Chapter nine is the final chapter, which covers the conclusion, discussion, and directions for future works.

1.5 Chapter Summary

This chapter provided an introduction to the thesis. Thesis objectives, contributions, and related works were presented. It highlighted areas where new results were obtained to get better understanding of 802.11ac standard. In this thesis, new results were obtained on the effect of IPv6, WPA2 security, shadowing, and human movement in Windows 8.1- Server 2012 environment WLAN.

The next chapter provides background information on key concepts relating to the research.

CHAPTER 2

BACKGROUND TECHNOLOGIES

This chapter provides a background of wireless technology features. Section 2.1 gives an overview of IEEE 802.11 standards. Section 2.2 provides the details of the different types of 802.11 architecture. Section 2.3 describes the internet model more focused on data communication and internet protocols. Section 2.4 describes physical and MAC layers of 802.11ac. Section 2.5 covers wireless security protocols. Final section describes wireless radio propagation characteristics.

2.1 An Overview of IEEE 802.11

The WLAN has experienced an exponential growth in the last decade with the increasing number of devices that support different 802.11 standards. The technology development of microchip and IEEE 802.11 standards have led to decreasing the cost dramatically, which has boosted user adoption of Wi-Fi network technology. In 1999, due to the increasing commercial demand, Wi-Fi Alliance (WFA) was founded. It certifies interoperability among IEEE 802.11 devices from various producers through testing [3]. The vigorous upsurge in the data rate with the modification is shown in Figure 2.1.

In October 1997, the IEEE 802.11 standard was published. The published standard covers MAC protocol as well as the physical layer. The initially published standard provided low data rates only comprising of a speed between 1 and 2 Mbps at 2.4GHz ISM band [25].

In October 1999, both IEEE 802.11a and 802.11b modifications were sanctioned by the IEEE 802.11 committee. The IEEE 802.11a functions at 5 GHz unlicensed band and allows a speed of up to 54 Mbps. 802.11a get frequency less prone to interference because it operates at 5GHz band, which has uncrowded frequencies and a shorter coverage range compared to 2.4GHz. IEEE 802.11b has a maximum throughput to 11Mbps, where it operates at 2.4GHz band. 802.11b covers more transfer range than 802.11a but it suffers from high Wi-Fi interference [26].

In June 2003, due to high demand for using different wireless technologies, the 802.11g emerged to improve data transfer speed (54Mbps), where it has enabled backward compatibility with 802.11b. But a major downfall to this protocol is that it experiences the same

interference problems as 802.11b where devices operate at a much crowded band (2.4GHz) [27].

The signal strength and speed of the wireless connections is very important in large growing companies. For this reason, in 2009 IEEE improved wireless standards and produced 802.11n. The 802.11n protocol involves modifications in the standard like adding a multi-input-multi-output antenna (MIMO), which allows the receiver antennas to combine data streams that arrive from different paths at the same time. 802.11n operates in both 2.4GHz and 5GHz frequencies bands. Using 5GHz band has improved a great deal providing a higher throughput due to less crowded frequencies, whereas 2.4GHz extends Wi-Fi range more. One of the major advancements in the new protocol is its enhanced capability of handling data as bandwidth was increased theoretically up to 600Mbps in case of using 4x4 MIMO at 40 MHz channel [28].

With the goal of increasing the performance of WLANs compared to wired networks, in December 2013 the IEEE 802 standards committee formed two new Task Groups (TGs), namely 11ac and 11ad. The 11ac standard functions in the band of 5GHz only and does not support the band of 2.4GHz. Theoretically, it is capable of allowing a speed up to1.3 Gbps. The new provisions were assembled on the 11n standard. The bandwidth of 802.11ac channel was increased from 40MHz to 80 or even 160MHz. It also involves the advanced order of modulation system (256-QAM) and other improved features such as Beamforming, Multi-User Multiple Input Multiple Output (MU-MIMO) with up to 8 spatial streams, etc. [29]. All features will be discussed in details on the next chapter. IEEE 802.11ac is recognised as the most modern wireless standard; this thesis attempts to investigate the different WLANs performance actors based on this latest standard.

IEEE 802.11ad is also emerging technology and an improvement to the 802.11n WLAN standard. It operates in the unlicensed and globally accessible 60GHz band. 802.11ad consumes a low power, and produces very high throughput, up to 7Gbps. The standard has a very short distance of about 1 to 10 metres. At 60GHz, the propagation behaviour increases signal attenuation and leads to difficulty penetrating walls [30].

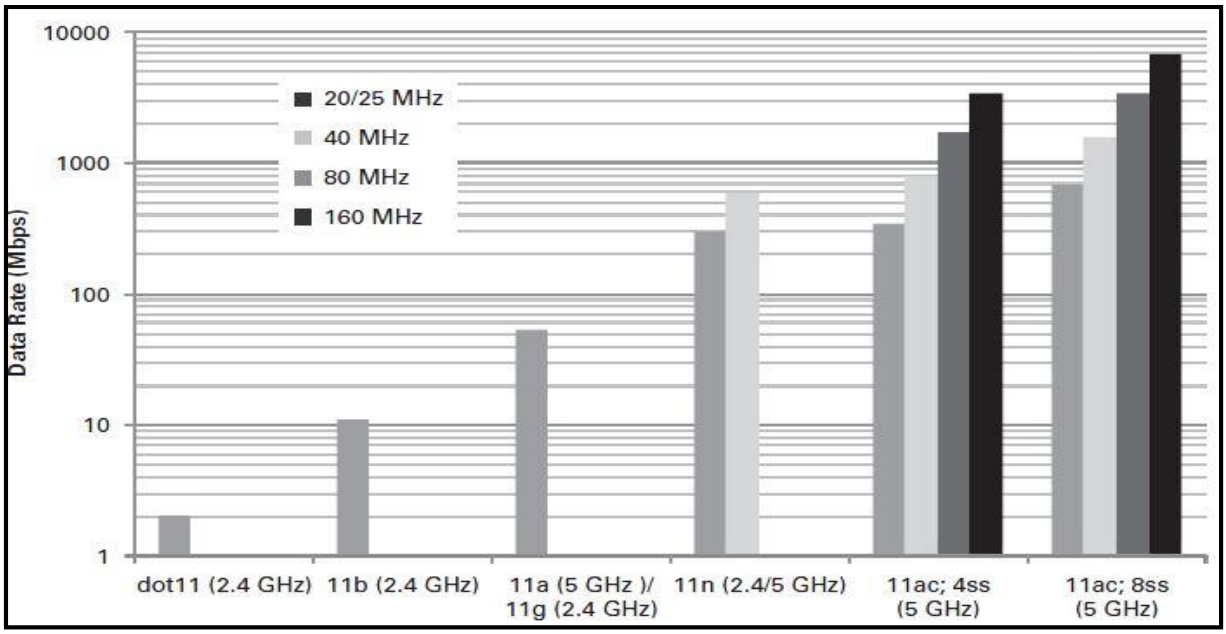

Figure 2.1: Increase in 802.11 Physical data rate [31]

2.2 IEEE 802.11 Architecture

Basic Service Set (BSS) is more than one 802.11 devices (stations) that communicate with each other by connecting to a single access point. The simplest form of BSS is called Independent Basic Service Set (IBSS), where stations can communicate with each other without using an access point. A BSS is built around an access point, which is known as an infrastructure BSS (Figure 2.2). These Infrastructure BSSs can be interconnected through their access points via a Distribution System (DS). Extended Service Set (ESS) is an interconnection of BSSs, which is connected via a DS. The stations within the ESS are able to access each other directly through the MAC layer [32].

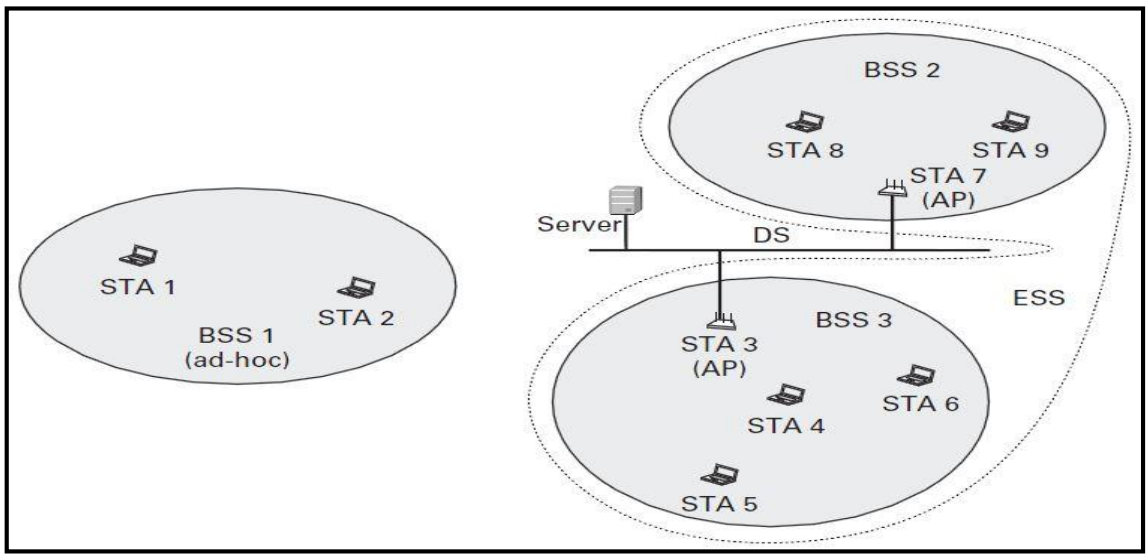

Figure 2.2: BSS, DS, and ESS concepts [31]

2.3 Internet Model (TCP/IP protocol)

Internet Protocol (IP) or Transmission Control Protocol (TCP) is the most commonly used protocol suite for Internet. TCP/IP offers end-to-end connectivity protocol. It specifies the packaging, addressing, transition, route and receiving of the data at the end. As per the scope of networking, four abstraction layers are used to perform all these functions by sorting out the protocols as per requirement. From the highest to lower, the layers are the application layer, which is responsible for the process-to-process application data exchange; the transport layer which mainly handles host-to-host communications; the Internet layer is responsible for connecting the hosts across different networks; and the link layer, which contains the communication technology required for a single network segment [33].

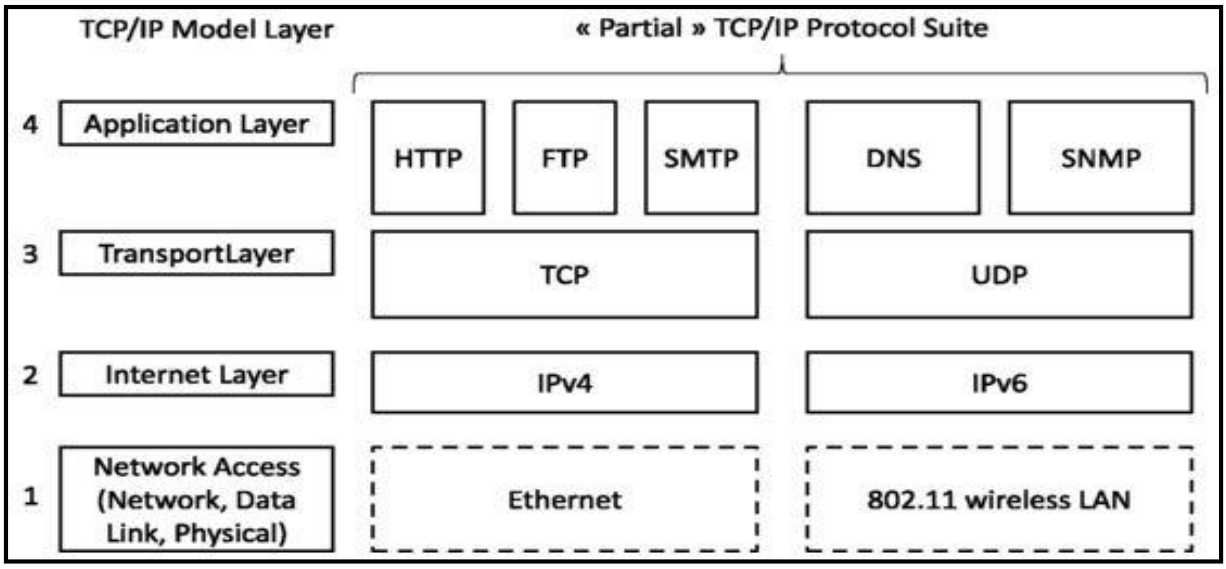

Figure 2.3: TCP/IP protocol structure [34]

2.3.1 Transport Layer

Transport Layer Protocol is an important part of the protocol hierarchy, which is necessary for the provision of end-to-end communication between the hosts over the network. Several features offers by Transport Layer Protocols are: congestion control, reliability, in-sequence delivery, control of flow, etc. These features ensure efficient performance and high quality services for the communication network [35]. It is important to make the correct choice of transport layer protocol for multimedia communication as this can significantly improve the quality requirements of multimedia, i.e. jitter rate, reduced delay, packet loss, efficient throughput, etc. [36]. Following are some of the widely used transport layer protocols:

User Datagram Protocol (UDP)

UDP is the most basic form of transport layer with no reliability for efficient and secure transmission of the packets. However, it is capable of multitasking and broadcasting. UDP provides the best choice when caring about the transmission time rather than reliable transmission. Additionally, there is no congestion control mechanism offers by UDP. The congestion control is important to prevent the network from being congested, which leads to reduced efficiency and performance [37].

Transmission Control Protocol (TCP)

TCP is connection-printed that offers an efficient congestion control mechanism as well as a positive acknowledgment system [37]. It is an extensively used protocol because of the capability of ensuring the reliability regardless of the type of lower layer of network. TCP is stream-oriented, which means the TCP protocol entities exchange streams of data. When transmitting using the TCP protocol, each byte in the communication process has its own sequence number to ensure that all data in motion arrives at the destination intact. TCP is also known as robust protocol because of its adaptability in various networking conditions. However, there are certain reasons that can lead to a drop in the TCP packets over the wireless network. Some of these factors are: higher rate of error, and frequent disconnection of the network [38].

Comparison of TCP and UDP

All transport protocols have overheads. The overhead is information that is encapsulated with transmitted data and contains sources and destinations of the packet. The header format for UDP protocol contains 4 fields; each of them is 2 Bytes in the length (8 Bytes overhead per segment). These fields represent a Protocol Control Information (PCI), which includes [39]:

- Source Port: specify the station (STA) port (Optional).
- Destination Port: specify the client port (Required).
- UDP length: identify the entire datagram length.
- UDP Checksum: check and correct the errors for the header and transmitted data, it is optional in IPv4 and required in IPv6.

The header format for TCP protocol contains 9 fields with a total length of 20 Bytes. Source port, destination port and TCP Checksum are functionally similar to UDP header fields; each of them has 2 Bytes. Sequence number field (4 Bytes length) ensures the reliable connection.

The 2 Bytes window field accommodates the length of Bytes that the client can receive. The remaining fields include Hlen, Flags, Acknowledgment number, and Urgent pointer [39].

Table 2.1 gives an overview of TCP and UDP protocols and Figure 2.3 illustrates a comparison between data packets.

TCP	UDP
The protocol is connection-oriented, which creates a virtual connection between transmitter and receiver.	There is no virtual connection (connectionless).
TCP packets are called segments.	UDP packets are called datagrams.
Virtual: the application layer “thinks” that a single path has been created; in reality packets can travel different physical paths: reliable connection.	The protocol is used when the application needs to send one packet quickly without the overhead of connection creation and termination: unreliable connection.
20 Bytes IP overhead.	8 Bytes IP overhead.
Data packets are rearranged in the order specified.	Due to all transferred packets are independent, there is no inherent order.
The data delivery is slower and more complicated, and most application protocols like SMTP, HTTP, FTP and TELNET use TCP.	UDP is designed for speed and is suitable for applications like video-conferencing and ping.

Table 2.1: comparison between TCP and UDP

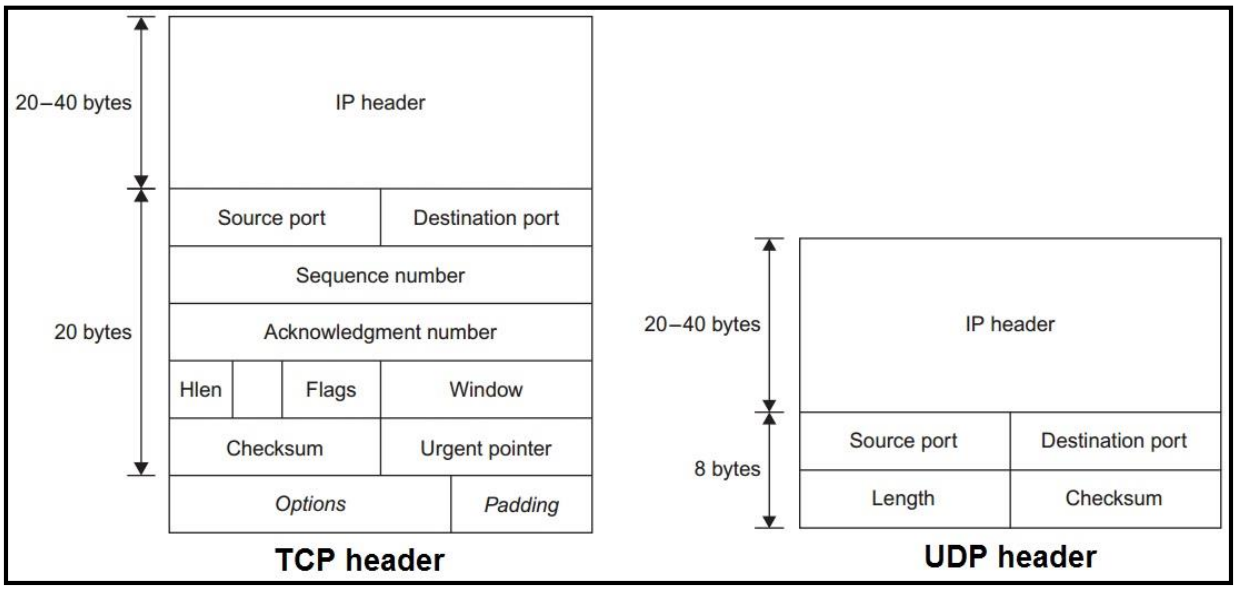

Figure 2.4: Comparison between TCP segment and UDP datagram [40]

2.3.2 IP Header

"Next Node" is determined by the information extracted from the IP datagram through the forwarding protocol of the router. Selected fields of the header of IP datagram hold the required information. IP header information is combined with the routing table in order to extract meaningful information by the router [41]. Currently, two versions of IP Protocols are being used extensively, i.e. IPv4 (version 4) and IPv6 (version 6).

Internet Protocol Version 4 (IPv4)

Amongst TCP/IP Protocol Suite, Internet Protocol (IP) is considered one of the essential protocols. In Open Systems Interconnection Model (OSI Model), this protocol is implemented at the Network Layer, while in the TCP/IP model it works at the Internet Layer. In both of these models, this protocol is responsible for identifying the authorised hosts on the basis of their logical addresses [41]. IPv4 provides 2^{32} addresses containing both network and host identifier. IP Payload is the encapsulated data, whereas IP header contains all information that important for the data packet being transmitted [42].

Internet Protocol Version 6 (IPv6)

Compared to header of IPv4, the IPv6 is less complex. Several fields and fragments have been removed from the IPv6 header while an extension has been made with addition of fields for fragmentation and Checksum. With these modifications, the IPv6 Header now has a fixed length of 40 bits. The header size is increased because the addressing mechanism rose to 2^{128} addresses. Overall, the IPv6 header is comparatively simple, and is, in theory, much more efficient than its counterpart [42].

Comparison of IPv4 and IPv6

IPv6 is an evolved version of IPv4 that focuses on the shortcomings and limitations of IPv4. The following section will present an overview of some of the key features of IPv6 that help overcome the issues of IPv4.

The IP Headers

The increase of IPv6 header size is mainly due to the movement away from 32-bit to 128-bit addressing. The number of fields has reduced to 8 in the IPv6 header instead of 12 in the IPv4 header. The source and destination addresses in the IPv6 header are 4 times longer than the IPv4 header. IPv6 contains one or more extension header to provide both flexibility and

efficiency by providing information that is needed for common functions such as fragmenting. There are a number of fields that have been eliminated in the IPv6 header such as Internet Header Length and Header Checksum, or replaced such as Type of Service to Traffic Class field. The entire IPv6 overhead is of 40 Bytes fixed length compared to 20 Bytes long for IPv4 packet overhead [42].

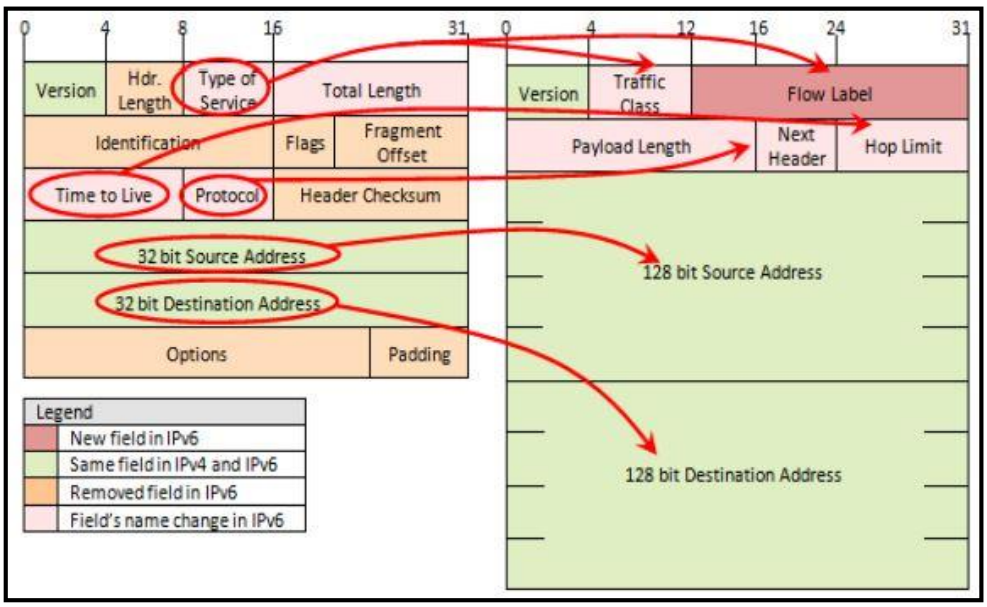

Figure 2.5: Changes and relationship between IPv4 and IPv6 header [41]

Extended Address Space

IPv6 has a hexadecimal address structure that allows it to have almost 7.9x1028 more unique addresses as compared to IPv4. The extended addresses is a crucial feature considering the exponential growth of the Internet as new online products are increasingly used such as mobile platforms, tablets, etc. These demands require more efficient IP referencing embedded models. Thus, IPv6 address space will be needed to establish a sufficiently efficient Internet gateway [43].

Efficient Routing

IPv6 shrinks the size of routing tables and promotes routing efficiency. IPv6 provides Internet Service Providers (ISPs) to combine the prefixes that belong of their clients' network into one prefix and advertise this prefix to the IPv6 Internet [43].

Better Mobility

Mobile IPv6 (MIPv6) is developed to enhance mobility connection. It aims to ensure connections between node mobility without losing their communication [44].

Improved Security

IPv6 offers several security enhancements that were not offers by IPv4. The first action made by the network attackers is to observe the ports in order to collect all possible information related to the network that has to be attacked. Since there were very limited ports in IPv4, this was done by attackers very easily. However, IPv6 has made this network sniffing more difficult because of increased time required for scanning or sniffing a huge number of ports. Thus, reducing the security risks significantly. IPv6 also creates the Cryptographic Generated Address (CGA) for better security. According to the mechanism of CGA, a public signature key is assigned to each IPv6 address. This public key can be used by the authorised user as proof of being the authorised owner of a respective address [43].

Neighbor Discovery

MAC address is required whenever a system sends IPv6 packet to another system that is associated with the same subnet. Mechanism for Neighbor discovery is capable of letting the systems identify the MAC addresses of each other. Neighbor solicitation is sent to the solicited node address that refers to the targeted IPv6 address [45].

Duplicate Address Detection

A Duplicate Address Detection mechanism is introduced for IPv6 addresses in order to avoid assigning the same address to two different systems [44].

Autoconfiguration

In a large network environment, autoconfiguration simplifies the network node configuration by automating the process. Stateless host automatic configuration is embedded in the new version and this simplifies the Dynamic Host Configuration Protocol (DHCP) configuration, which assigns IP addresses to each host [43].

2.3.4 The Data Link Layer

The main tasks of this layer are: division of the data stream into small data frames, addition of physical addresses on these frames, imposition of a flow control procedure that tends to protect the overwhelming of the receiver, making the data transmission reliable by detecting the lost and damaged data, and also controlling the access on those links in which two or more devices are associated to the same link [46].

2.4 The IEEE 802.11 Standard

The IEEE 802.11 standard features multiple physical layers referred as PHYs and for wireless local area networking, it has a common medium access control (MAC) layer [47].

2.4.1 802.11 MAC Layer

Medium Access Control (MAC) mechanism protects the multiple nodes from accessing the same channel at the same time. Every node starts listening on a desired channel to detect whether the channel is ideal or busy before it transmits a packet. If the channel is idle during the back-off time, the node transmits the packet and resets the back-off window size to minimum. Otherwise, it doubles the back-off window size, waits until the channel is idle [47].

2.4.2 802.11 Physical Layer (PHY)

Modulation techniques and data coding are the most important parts of the 802.11 physical layer. During the modulation process, digital information symbol turns into a steadily low-frequency signal form. Later on, low frequency signal is transmitted over the high frequency. Design of Modulation Schemes focuses on the implementation complexity and bandwidth efficiency. Bandwidth directly affects the function of a wireless communication system [48].

2.5 Wireless Security Protocols

Wireless communication security is more of a concern than wired since there is no inherent physical protection between communicating devices. The physical connection is replaced by logical associations using radio frequency, which by nature uses broadcast for transmission. In such an environment common security threats, such as eavesdropping, injecting bogus messages, jamming, and Denial of Service (DoS) can be easily mounted. For protection, it is important to ensure confidentiality, authenticity and integrity of the data transmitted through wireless mediums. For this purpose, special wireless security protocols were established [49].

2.5.1 Wired Equivalent Privacy (WEP)

IEEE 802.11 attempted to secure wireless transmission by creating WEP encryption. Its primary objective was to make wireless transmission as secure as wired transmission. WEP is essentially aimed at network access control, ensuring confidentiality for data transmission, and integrity. The shared key is used to authenticate data being transmitted from access point by

only authorised users on the network. This authentication was done through a challenge-response protocol that involved very simple processing [50]. The WEP supports two keys of length (64-bit and 128-bit). The 128-bit WEP key is a more sophisticated encryption compared with 64-bit WEP. It uses a 104-bit as a secret key, and 24-bit Initialization Vector (IV), which is not under user control whereas 64-bit WEP use a 40-bit as a secret key, and 24-bit IV. The main problems with WEP are having weak encryption keys that can be broken by a passive attack, and it also provides a single-way authentication, which can be easily intercepted by a rogue station [50].

2.5.2 Wi-Fi Protected Access (WPA)

WPA encryption method was emerged to handle the WEP vulnerabilities. WPA was enhanced and modified to overcome these issues. For instance, Encrypted Message Integrity Checks (MIC) were integrated within the WPA to restrict any attacker from capturing or altering any data packet being transmitted. MIC further reduces the threat of DoS and spoofing. Despite significant improvements in WPA over WEP, the new WLAN security protocol has already been exploited. Different methods have been developed to crack a WPA encryption. Finally it was confirmed that almost all data packet transmitting towards a WPA security enabled on WLAN client could be decrypted by using spoofing packets in the data stream [50].

2.5.3 Wi-Fi Protected Access 2

WPA2 have been introduced with efficient wireless encryption algorithms. It is capable of providing a better data protection and enhanced access control for the network layers compared to WEP and WPA [50]. WPA2 also supports WPA along with several other features and benefits. WPA2 ensures stronger authentication and processes of encryption for ad-hoc and infrastructural implementations. On the other hand, WPA only supported encryption for infrastructural implementation. Key catching mechanism is also implemented by WPA2 that helps in reducing the overhead of network nodes between the access points. It also supports pre-authentication required for authenticated exchange between the wireless node and the access point [51].

2.5.4 Security Overheads

The protocol overhead is the necessary information that additionally attached to the payload to successfully exchange data packages in a communication system. This information may contain the source and destination of a message or determine the beginning and end of a

message. Any WEP frame has a constant 8 Bytes and followed by the payload. The further fields contain required information to decrypt the message at the receiver side. Whenever body frame size is shorter, the WEP overload becomes a significant weight. The WPA overheads have 20 Bytes occupied, which are 2.5 times more than classical WEP, whereas the total overhead of WPA2 is 16 Bytes [52]. In this thesis, WPA2 was selected in WLAN test-bed.

2.6 Wireless Radio Propagation Characteristics

It is important to understand the propagation of radio waves in order to empathise how physical environment affects the wireless transmission. Environment for the radio propagation is a significant factor that can impact the throughput performance over the Wi-Fi networks. Therefore, it is important to research these factors in order to design and deploy an efficient transmission mechanism for WLANs. Radio propagation in an indoor environment is influenced by building walls and floors, and modelling these factors presents an image of how interference might be attenuated via planning service deployments or even infrastructure modifications [53].

In such a model, a signal is transmitted through an antenna for three distinct routes i.e. ground waves, sky waves, and line of sight (LOS). One of these three transmissions will dominate the remaining based on their frequencies. However it must be understood that the received signal in any form is always different from the signal sent due to various impairments [54]. Following are some of the transmission impairments that are most likely to impact LOS transmission:

2.6.1 Attenuation

Attenuation is referred to any loss of signal power (strength), which can be influenced by the distance over any wave propagate. A logarithmic calculation (path loss) is a standard way to measure signal strength [54].

2.6.2 Free Space Loss

This is the dispersion of the signals over the distance during any wireless communication. A reduction of signal power that will be received by the antenna at reception is based on how far the reception is. Free Space Loss (FSPL) occurs when the transmitting signals are ideally a radiating point source in space without obstacles nearby that might cause reflection or diffraction [54].

2.6.3 Fading

Fading is described as variation in the time of received signal power due to the changes in the medium or path of the transmission. During the designing of the communication system, fading is considered the most challenging technical issue. Generally, it is atmospheric conditions that influenced the fading in a fixed environment. However, in the case of the mobile environment, the impacting factors tend to change with time and motion of the reception and sending antennas, which as a result, becomes even more complex [55].

2.6.4 Multipath

Multipath is referred to as the propagation in which the reception antenna receives the signal from two or more different paths. One of these signals is direct while the others are reflected with an opposite phase. This can lead to mutual cancellation of signals, therefore, causing significant loss of signals. Based on the path and distance of the direct and reflected waves, the composite signal can either be amplified or smaller than the actual signal [55].

Multipath is commonly observed in indoor areas where several metallic surfaces are present. The following figure shows the mechanisms that can result in multipath propagation:

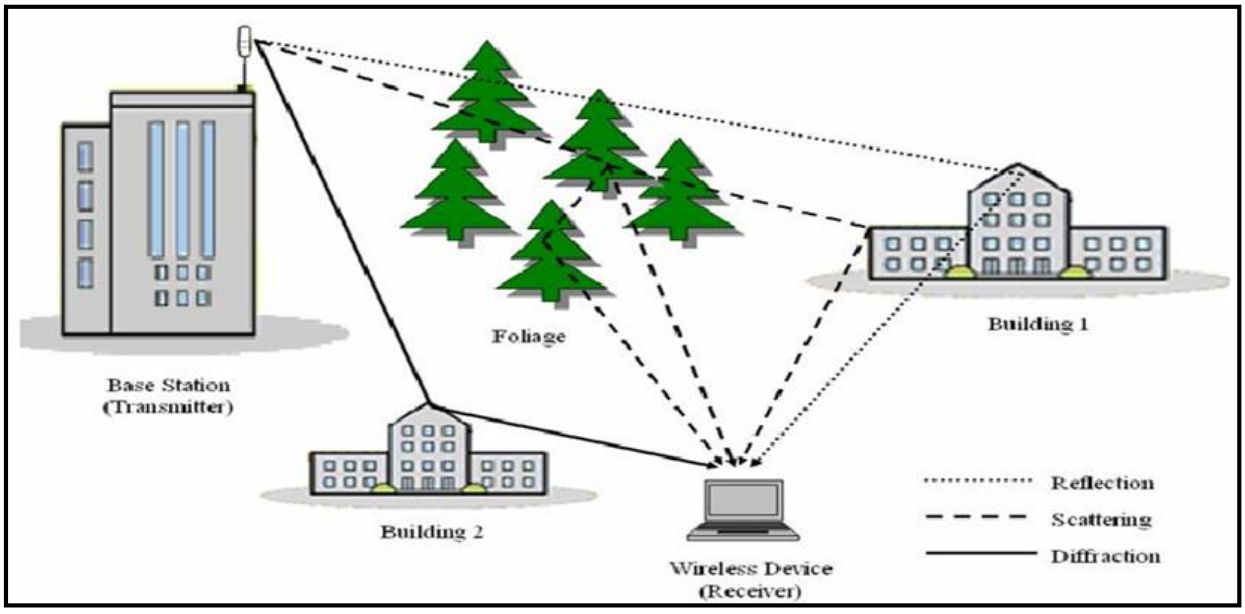

Figure 2.6: Types of propagation mechanism [53]

Reflection

Reflection usually takes place when a large dimensional object becomes an obstacle during the transmission. Such objects can be walls, cabinets, furniture, etc. These mediums tend to

absorb some of the signals that were being transmitted, while the remaining are reflected off the surface [53].

Scattering

Scattering occurs when several small sized objects become an obstacle for the transmitted signals. These objects can be bushes, cabinets, trees, etc. These objects tend to scatter the reflected energy in several directions before they are received by the receiver [53].

Diffraction

Diffraction takes place when the obstacles have sharp edges that can produce a secondary wave, which may bend around the obstruction. Similar to the reflection, the phenomenon of diffraction is also influenced by the physical features of the hurdles. In case of several obstructions, the waves are diffracted. However, they may still have enough strength to combine into a meaningful signal [53].

The above stated effects of propagation can have a significant impact on the performance of the system based on various medium and condition related features. Usually, diffraction and scattering are not major issues with respect to a sufficient LOS distance between the transmission and reception antenna. However, reflection can be a major issue in this case. Furthermore, in the absence of LOS, diffraction and scattering becomes the basic method of reception of the signals [56].

Refraction

Refraction is described as the variation in the direction of the electromagnetic waves that results in the variations in velocity of propagative mediums through which the signals are passing. This can create a condition where very little or no signal reaches the reception antenna [56].

Noise

In a case of any transmission, a transmitted signal will be delivered with a sort of distortion that is enforced by wave propagation, these undesired signals are known noise or interference, which is considered a significant factor limiting the performance of communications systems [56].

Absorption

Absorption occurs when signal is lost while passing through different obstacles or mediums. During absorption, the form of some signals turns into another form of energy, which is mostly heat (thermal energy). Any material that is not transparent to the electromagnetic signals can result in absorption of the transferred signal. The strength of signal mainly depends on characteristics of a medium that the transmitted signal can pass through [57].

Materials	Degree of attenuation	Examples
Air	None	Open space, inner courtyard
Wood	Low	Door, floor, partition
Plastic	Low	Partition
Glass	Low	Untinted windows
Tinted glass	Medium	Tinted windows
Water	Medium	Aquarium, fountain
Living creatures	Medium	Crowds, animals, people, plants
Bricks	Medium	Walls
Plaster	Medium	Partitions
Ceramic	High	Tiles
Paper	High	Rolls of paper
Concrete	High	Load-bearing walls, floors, pillars
Bulletproof glass	High	Bulletproof windows
Metal	Very high	Reinforced concrete, mirrors, metal cabinet, elevator cage

Table 2.2: level of attenuation of different materials [57]

2.7 Chapter Summary

This chapter covered the background on wireless technology. It also spotlighted the issues that influenced of the performance WLANs, which are radio propagation characteristics and packet overheads. It also provided information about IPv4, IPv6, TCP, UDP, and WPA2.

The next chapter provides the details of IEEE 802.11ac, which is the wireless LAN standard used to evaluate in this study.

CHAPTER 3

IEEE 802.11ac WLAN

This chapter covers the details of IEEE 802.11ac standard. Section 3.1 gives the overview of IEEE 802.11ac standard. Section 3.2 covers the core technologies used in 802.11ac.

3.1 An Overview of IEEE 802.11ac

To meet the exponential growth in the WLAN demands, the IEEE released 802.11ac, which can be seen as the finest evolved form of wireless networks. When IEEE 802.11n provides in the theoretical limited of 600Mbps but in practice reality up to 180Mbps [22], IEEE 802.11ac supports a theoretical throughput of 1.3 Gbps [29]. According to ABI research [58] access points shipments that support IEEE 802.11ac standard rose remarkably in 2014, which represents more than 11% of entire devices shipments.

The majority of the techniques used in 11ac are just refined forms of 802.11n. 802.11ac increases channel width from a maximum of 40MHz with 802.11n up to 80 or even 160MHz at 5GHz band. More differences between 802.11ac and 802.11n are shown in the table 3.1 [59].

802.11n	802.11ac
Supports 20 and 40 MHz channels	Adds 80 and 160 MHz channels
Supports 2.4 GHz and 5 GHz frequency bands	Supports 5 GHz only
Supports BPSK, QPSK, 16-QAM, and 64-QAM	Adds 256-QAM
Supports many types of explicit beamforming	Supports only null data packet (NDP) explicit beamforming
Supports up to four spatial streams	Supports up to eight spatial streams (AP); client devices up to four spatial streams
Supports single-user transmission only	Adds multi-user transmission
Includes significant MAC enhancements (A-MSDU, A-MPDU)	Supports similar MAC enhancements, with extensions to accommodate high data rates

Table 3.1: Differences between 802.11n and 802.11ac [59]

802.11ac outperforms 802.11n by many features (using new 80 and 160MHz channels at 5 GHz band, adds 256-QAM, using multi-user transmission, and efficient beamforming, etc.), and this will be discussed in next section.

3.2 The Core Technology of 802.11ac

802.11ac technology stipulates MAC (Medium Access Control) as well as PHY (Physical Layers). The correct modulation scheme is selected by the PHY layer provided by the channel conditions and delivers the essential bandwidth, while the MAC layer selects in a distributed way on how the accessible bandwidth is being shared between all the stations (STAs) [60].

3.2.1 The Physical (PHY) Layer

To increase raw speed of the PHY layer in 802.11ac, many enhancements have been done:

More spatial streams and multi-user MIMO (MU-MIMO)

Prior to 802.11n, the previous standards are known as Single Input Single Output (SISO), which means that every transmitted signal reaches a single destination (single antenna). Multiple input, multiple output (MIMO) technology was introduced in 802.11n. MIMO is a wireless multiple antennas technology, it makes the receiver antennas operate in a smarter way and they become capable of combining data streams that arrive from different paths (multiple transmitter antennas) at the same time, and eventually increase the signal-capturing power of the receiver [61].

Multi user transmission is an advanced characteristic of 802.11ac. A transmitter can simultaneously send separate groups of streams to multiple receivers (antennas) and hence utilise one channel access to transfer a packet data to a group of stations [62]. As shown in figure 3.1 (b), at the time the Access Point transmits, both the smartphone and the laptop transfer radio energy, and channel access can be utilised to connect to only one of the devices at any point in time.

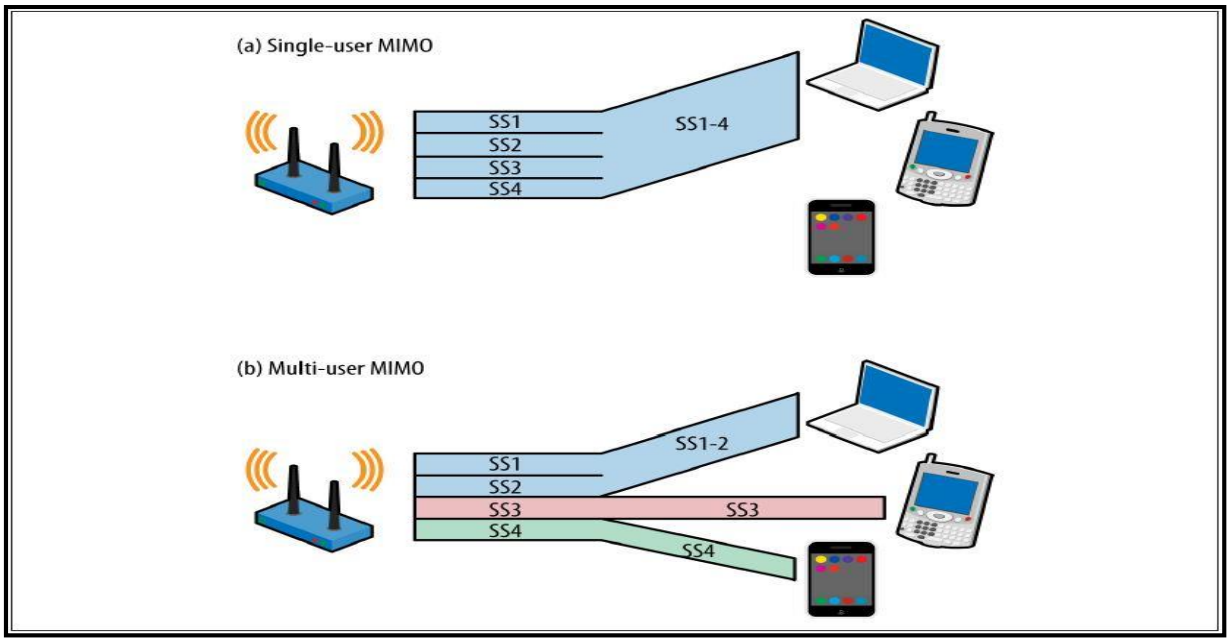

Figure 3.1: Single- and multi-user MIMO comparison [59]

Up to 8 special streams can be specified in 802.11ac while 802.11n can utilise up to 4 spatial streams at the Access Point. More spatial streams mean more clients can be served at the same time. Transmitting high speed for many clients at one time makes 802.11ac capable of working at much faster rates than anticipated by the data rate [63].

Uses Wider Channels

A wider channel enables more data throughput in a wireless system. For this purpose, the 5GHz band in 802.11ac has higher throughputs in 80-160MHz channel width compared to 40MHz in 802.11n [17]. The 802.11ac brings two new channel sizes, 80MHz and 160MHz and uses Orthogonal Frequency Division Multiplexing (OFDM) based transmission. The main advantage of OFDM is the ability to reduce the interference by dividing a high data stream into multiple slow signals. The 80MHz channels are contiguous blocks of spectrum, whereas, due to the difficulty of finding a 160MHz contiguous channel, the 160MHz block can be split if required into two 80MHz non-contiguous blocks of spectrum. In OFDM, not all subcarriers are used for carrying data. Some of the subcarriers are used for equalising the gain as well as determining the phase shift at the receiver's side [29].

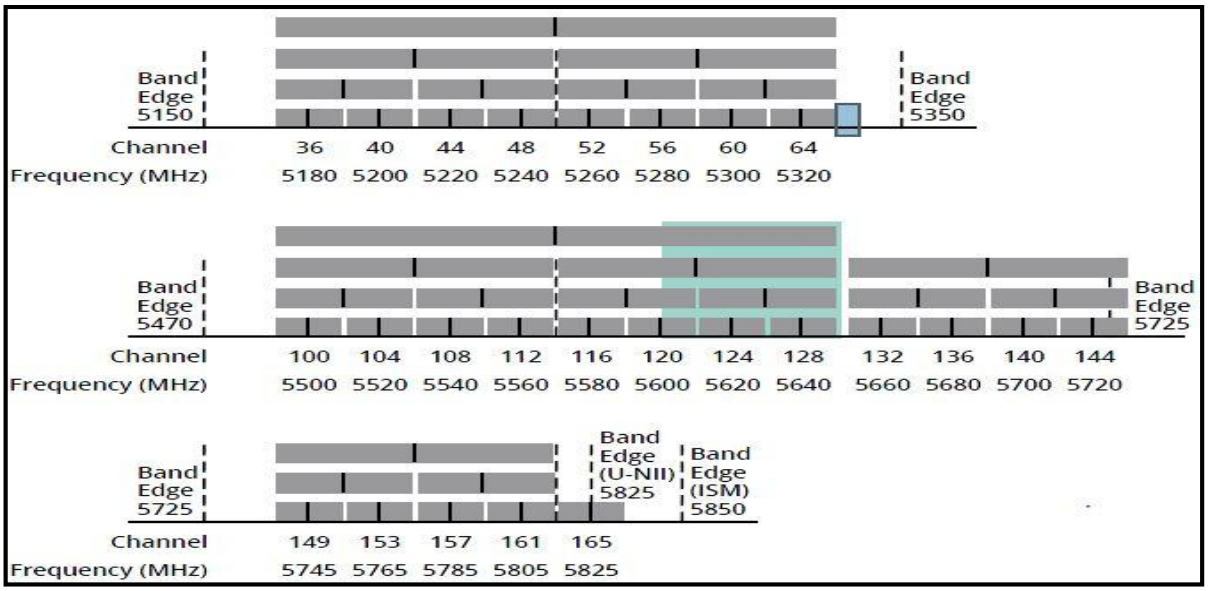

Figure 3.2: The available channel widths in 5GHz band [63]

Primary and Secondary Subchannels

A primary 20MHz wide subchannel is always required to any channel width at 40MHz or wider. 80MHz channels consist of primary and secondary 40MHz subchannels. In the same way, 160MHz channels have a primary 80MHz subchannel and a secondary 80-MHz subchannel. The purpose of the primary subchannel is carrier sensing that ensures the transmission for only a single device. 20-MHz subchannel makes the coexistence and reverse compatibility with devices using a legacy 802.11 standards. The primary subchannel has the ability to make a full clear channel assessment (CCA), which examines the signal energy over the channel before transferring data packets. Whereas the process of CCA is not required to fully perform in the secondary subchannel [63].

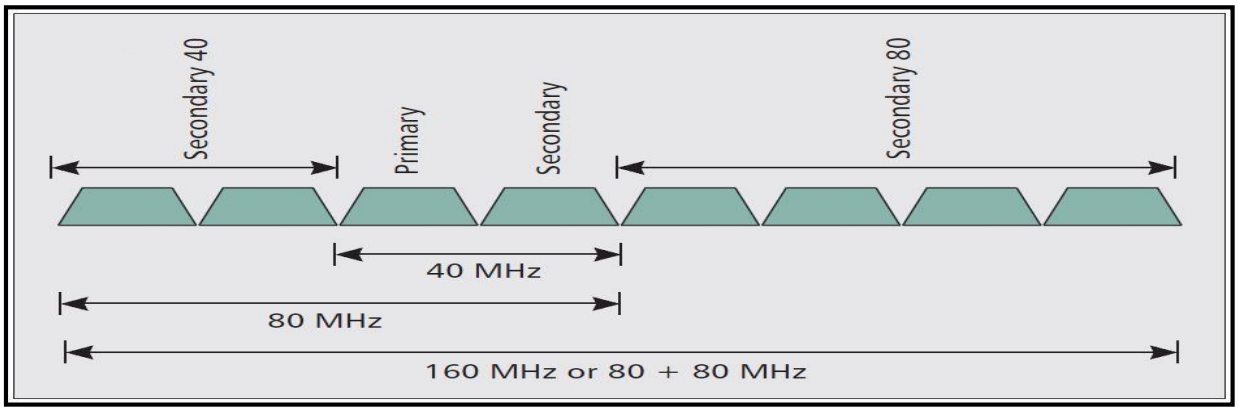

Figure 3.3: Primary and secondary channel selection [63]

Static and Dynamic Channel Access

- Static channel access

In case the secondary sub channel is busy during packets transmitted at 80MHz channel in 802.11ac station, the station will randomly wait for an amount of time before trying to re-transmit until no interferer exists in any of the subchannels [63].

- Dynamic channel access
  The station at 80MHz channel will try to transmit packet by using 20/40MHz narrower channel instead of spending time waiting for an appropriate condition to transmit. This approach allows efficient resource allocation, as the station is capable of transmitting signals over a fraction of the original bandwidth [63].

Better Modulation Technique

One of the important things that improved the 802.11ac throughput is 256-QAM modulation technology. With this technology, each carrier has increased by two more bits compared to 64-QAM modulation, which in turn has raised the capacity by a third [64].

256-QAM Modulation

This is quadrature amplitude modulation (QAM), which combines the two AM (amplitude-modulated) channels to make a single channel that selects the constellation symbols and hence doubles the active bandwidth. Previously used 64-QAM modulation allowed the transmission symbol to take any of the 64 values involving 8 in phase levels (phase shift) and 8 quadrature levels (amplitude of a wave). Every time a symbol transmission occurs it can take one of the 8 in phase shifts and one if the 8 amplitude levels. Instead of an 8 by 8 constellation, the 256-QAM provides 16 in phase shifts as well as 16 amplitude levels. The following figure 2-4 exhibits a comparison among the 64-QAM and 256-QAM constellations [65].

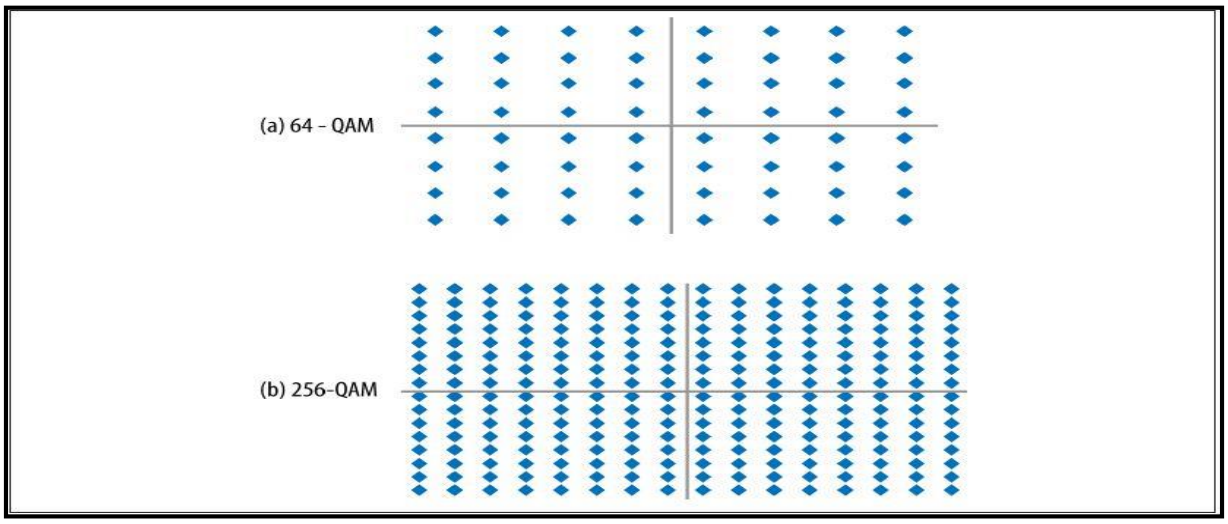

Figure 3.4: Comparison of modulations [59]

802.11ac introduces 256-QAM that increases the PHY layer link speed by 33% over its nearest equivalent rate in 802.11n. But, to achieve this speed there should be much higher Signal-to-Noise Ratio (SNR) (about 5dB more) than what is required for 64-QAM. This gap is bridged using a number of different techniques. One of them is the introduction of a new error correcting code mechanism called Low-Density Parity Check (LDPC) that can gain up to 1-2dB. Also, some Radio Frequency (RF) front-end techniques may be used to increase the SNR at the receiver's antennas [59].

Physical Layer Framing

The 802.11ac Physical (PHY) is designed in such a way that it is compatible with previous 802.11 PHYs. When a frame is transmitted, the frame format of 11ac and 11n has been kept similar. However, a difference between the two is that 11ac has a single frame format in order to simplify implementation of physical layer [66].

3.2.2 The MAC Layer

The MAC layer enhancements in 802.11ac are mostly driven from the 802.11n and their function in order to support the new PHY layer features. The MAC layer, which also caters to channel access methods, has undergone large changes to accommodate sharing of radio resources in channels for different sizes [66].

There are many improvements are offers by 802.11ac besides a few MAC amendments that principally present a faster Physical layer.

Frame Aggregation

MAC Protocol Data Unit (MPDU) aggregates more than one frame into a single frame transmission. The resulting frame comprises of less header overhead as compared to what it is prior to the combining of layers. This is due to the sending of fewer but larger frames that reduces the contention time in the wireless system [17].

Medium Access Mechanisms

With newly introduced channel bandwidths in 802.11ac, new rules which determine whether the channel is clear or not are also established. For this purpose, 802.11ac standard has also added new rules which let the other devices read their targeted consumption of the bandwidth in RTS/CTS (Request to Send / Clear to Send) exchanges. The Clear Channel Assessment (CCA) of 802.11n was less in the secondary channels and organising two 802.11n networks

required having two identical primary channels. Whereas 802.11ac has idle CCA capabilities in their secondary channels, which makes the deployment of two networks easy as large fractions can be transmitted on the parallel level. This solitary refinement in the specification of the system makes a wide range of deployment possible for 802.11ac standard networking systems [16].

3.2.3 Beamforming

Traditionally, the Access Point antennae are omnidirectional; i.e. these are capable of sending energy in all directions. This omnidirectional coverage of an antenna is shown as a circle in the map, which is centered on the Access Point. These are cheap and as they spread the signals in every direction, Access Point does not have to keep a track of the signals transmitted to each client. As result, if the client in a reachable range, the signals will reach them. A drawback of this is that the radio channels stays busy in all the possible directions [67].

Beamforming is an alternative approach to provide sufficient information to the Access Point in order to send a preferential radio energy. It focuses on the signal in one destination, hence the transmission of the signal to reach farther. At medium ranges, beamforming plays a role in enhancing the wireless performance whereas at the short ranges, the high signal power increases the Signal-to-Noise Ratio (SNR) so that it supports maximum data rate of data 1.36 Gbps. At long ranges, data rates will remain the same as in the absence of beamforming. In the beamforming process, both the Access Point and the client workstation are beamformed. So, in the long distance with higher processing power within antennae in access points, it is expected to downlink transmit beamforming occurrence between the Access Point and client [59].

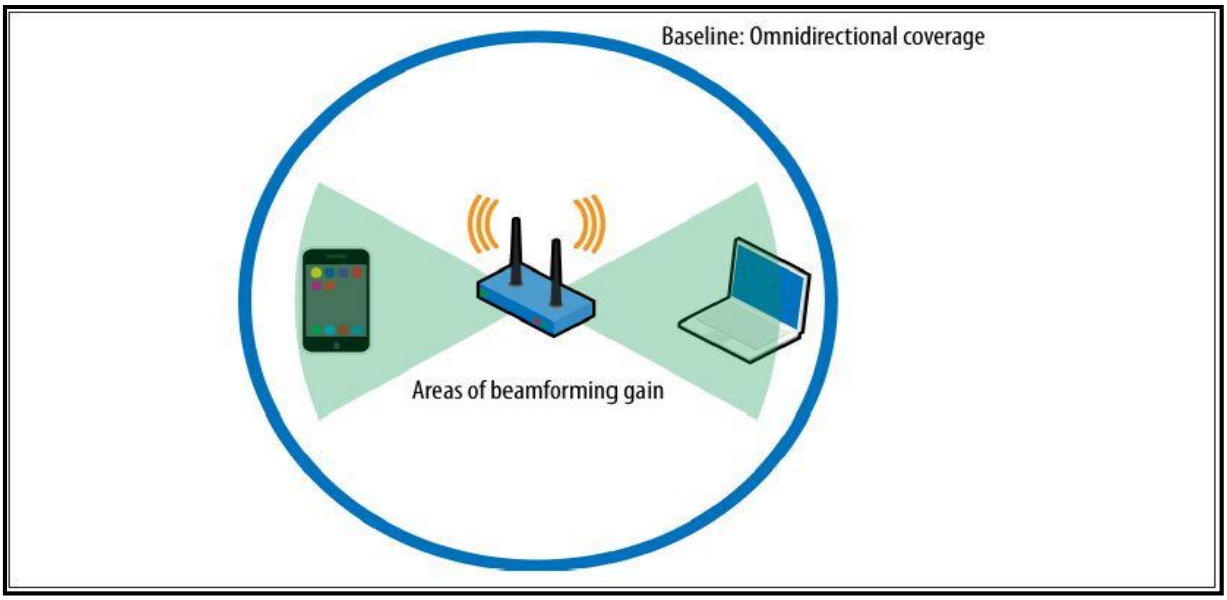

Figure 3.5: Beamforming basics [59]

The 802.11n standard has multiple methods of beamforming and implementing them in hardware was not chosen by vendors, but some proprietary solutions were seen in the real world. However, 802.11ac has defined only one type of beamforming, explicit beamforming. It is normally done for the traffic from the AP (beamformer) to the client (beamformee), only in the downlink direction. This has advantages when using a MU-MIMO system considering the fact that the Access Point is a stationary entity that can have multiple antennae [59].

3.3 Chapter Summary

This chapter covered the details of IEEE 802.11ac standard. We detailed 802.11ac technologies that were either developed from the previous standards or new technologies were introduced such as QAM modulation, Beamforming, using biggest channels in the 5GHz band, and MU-MIMO.

The next chapter covers the methodologies that were employed in this study.

CHAPTER 4

METHODOLOGY

This chapter provides details about the methodologies employed in this thesis. Section 4.1 covers the methods used to fulfil this research. Section 4.2 presents the common approaches used to measure the performance of wireless LANs. Section 4.3 covers the data collection process.

4.1 Method of Study

The quantitative approach was chosen in this study rather than the qualitative approach. The quantitative method deals with numbers that can be measured such as speed, time, height, etc. Qualitative methods rely on descriptions when data is gathered from the observation like tastes, smells, etc. [68]. Quantitative data are crucial and required for this research, where the data are gathered from test-beds and employed to analyse the outcome. The test-bed method was used to evaluate the performance of 802.11ac WLAN in different scenarios. Many researchers have chosen test-bed approach [20, 21, 22, 23].

The data obtained from test-beds are displayed in a numeric way and analysed using statistical methods.

4.2 Performance of a Network

Networking is about devices connecting to each other in such way to transfer and receive data with the purpose of sharing information, resources, and services. Data transfer rate, round trip time, and CPU usage are the most significant components that determine the network efficiency. The essential issue for network communication is the ability to transmit and receive data between two nodes within a specific time [69].

4.2.1 Performance Evaluation Methods

A number of methodologies can be used to examine wireless networks under different conditions. Each of these methodologies has strengths and weaknesses. However, selecting one of methodology relies on the nature of the network being studied.

Analytical Modeling

The analytical model is one of the evaluation tools that uses mathematical formulas to analyse or predict the system behaviour. The computational knowledge is required to conduct this method. The level of computational complexity depends on the size and nature of the network [70].

Simulation

The simulation method is always a favourable selection to test many aspects of network performance. It tends to offer a great set of features by presenting a realistic representation of network components. By implementing this method, researchers can evaluate characteristics of the network infrastructure in a controlled manner, which help to create many types of network topology, customise the pattern of traffic transmitted, and gather data for analysis. Simulators offer a suitable environment giving many benefits to researchers, such as validation of network components, a platform to test new developments, and an opportunity to study a large network infrastructure [70].

However, simulators might have a high consumption of time and memory in the case of applying the simulation method in a large network, and its outcomes mostly relies on some modelling assumptions that may provide limited information in real life environment. Thus, most studies based on simulation are used for qualitative purposes only [71].

Emulation

Emulation allows researchers to carry out experiments by a combination of some real components of the network and simulations. For instance, researchers intend to evaluate a large network but they have a limited resource. So, it is a good way to replace a real hardware like a router with emulation software [72].

However, the emulation approach is not a complete alternative to real world evaluation. Emulation provides inaccurate results in a situation where functionality of hardware is required to change, such as firmware settings [73].

Test-bed

Test-bed is the evaluation method used in this study. Simulation and emulation try to represent a real network environment, but the produced result from these methods can reduce the level of realism. The physical test-bed attempts to fill the gap between these approaches and real

deployment. The test-bed is a real hardware-based network environment, which can be a costly alternative depending on the level of the network complexity [74].

However, test-bed gives realistic results under real world conditions, which generate and measure real parameters such as throughput, delay, and CPU utilisation. The test-bed was chosen because of the features mentioned above and also the small size of the network environment that was tested.

4.2.2 Performance Metrics

Network performance was tested by different network parameters. These parameters are called performance metrics that can be measured to evaluate the performance of a network. Throughput, CPU utilisation and Round Trip Time (RTT) are the most interesting parameters for evaluating the network performance [75] [76].

Throughput

The most widely metrics used to evaluate the network performance is the throughput [77]. It counts the amount of transmitting packets within a specific period of time. These data can be delivered over physical link, logical link, and certain network nodes. Throughput can be influenced by many factors such as hardware processor speed and capacity of wireless networks, which cause network congestion problems. Throughput on a network is controlled by the available bandwidth, Signal-to-Noise Ratio (SNR), and the available hardware and software. It is measured in by Megabits per second (Mbps) [69].

CPU utilitization

CPU utilisation refers to the percentage amount of task processing managed by a CPU. The usage of CPU increases when a system process needs more time or there are more network packets being transmitted and received. In the wireless network, packet length plays a vital role in determining the percentage of CPU utilisation. The packet will be broken up into smaller packets, which increase the length of time of data sending and raise the CPU usage percentage as well [78].

Round Trip Time (RTT)

RTT is the required time for a packet to deliver to a node destination and back to its source for informing that signal has reached its destination. RTT is commonly measured in milliseconds.

There are many factors that can increase RTT such as network congestion, queuing, and the distance between the nodes [79].

4.3 Data Collection Process

Information was collected by two different approaches in this study. The first phase was conducted by carrying out the literature review and then by collecting the actual experimental data.

4.3.1 Literature Review Process

All the information gathered from resources such as, books, articles and conference proceedings was taken from sources like IEEE, Google Scholar, and ACM Journals and was retrieved from credible web sources that are reviewed to build a better understanding of the research area. Also, the knowledge gained from the literature review revealed whether experiments had been done in this research area. The gaps that were identified formed a guide to conduct this research.

4.3.2 Experimental Data Gathering Process

In this research, data was collected in laboratory experiments. These experiments aimed to evaluate the performance of IEEE 802.11ac WLANs under various conditions in an indoor environment. Two operating systems were installed over client and server workstations with different protocol settings. Test-beds examined transmission protocols (TCP and UDP) for both versions of the Internet Protocol (IPv4 and IPv6) with the same dependent variables.

The data gathering stage was carried out in a computer lab environment. Jperf and Netperf were tools used to collect the data by generating and measuring both the bandwidth and RTT respectively, whereas CPU utilisation was measured by using a built-in tool (Typeperf). More details about the three measurement tools will be described in detail in the next chapter. The gathered data were entered into an Excel spreadsheet and the extracted values were graphed to use in the analysis phase.

There were a number of test-beds that were implemented in the process of this research, and consequently a great deal of primary data was generated. Due to the chosen method of data collection (test-bed), it was necessary to ensure that all results reported in the thesis were accurate and free from anomalies. That is, a high degree of accuracy was necessary and this was achieved by ensuing that multiple runs (number depending on the actual context in which

TCP/UDP and IPv4/IPv6 was tested) of JPerf with the same parameters were performed for each value reported in this work. Due to the nature of the technology, wireless-based network analysis required a number of repeat runs in spite of taking all necessary precautions to minimise the effects of external factors like signal interference. Overall, ten to fifteen repeat runs were necessary (to attain 95% confidence interval) for each value reported in this thesis. The reported value was the average of the readings taken after filtering any outliers.

In this process, there were three different types of data used to measure networks performance. They were CPU utilisation, round-trip time, and throughput, all of which were collected by using appropriate tools. Table 4.2 shows metrics and the tools used in the data gathering process. In addition, the process of collecting this data will be explained in the next section.

Metrics	Tools Used For Collecting Data
CPU utilisation	TYPEPERF.EXE (Windows CMD)
Round-trip time	Netperf
User throughput	Jperf

Table 4.1: Metrics and tools used for collecting data

Results Analysis

The results obtained from the three tools mentioned above were converted into Excel spreadsheets and line charts were produced for conducting the comparison and analysis stage. The results are discussed in chapters 6 to 8 including their graphs.

4.4 Chapter Summary

This chapter summarised the research method approaches, the methodology and how the data collection was carried out to complete the study. This chapter further explained the reason for using a quantitative approach and test-bed experimental study for this research. The research describes the methodology of conducting experiments and collecting data and finally analysing the collected data by plotting the graphs in Microsoft Excel.

Chapter five presents the experimental design for this research.

CHAPTER 5

EXPERIMENTAL DESIGN

This chapter provides details about the experimental network design used in this thesis to gain the results. Section 5.1 covers the hardware and software that was used in test-beds, including their specifications. Section 5.2 covers the experimental set-up of different scenarios, which are: implementing WPA2 security algorithm, human movement in indoor environmental conditions, and shadowing (walls) and distance in a laboratory environment.

5.1 Test-bed

As mentioned in the previous chapter, the experiment was carried out in a computer laboratory. This section gives the details of the resources used in the experimental setup. Data was collected using a number of different experimental scenarios by changing the various parameters.

5.1.1 Hardware

The hardware used and their configurations were kept identical in all experiment scenarios in order to produce accurate and consistent data for this study. The hardware contains an Intel Core i5 CPU 2.80 GHz processor with 24.0 GB RAM for the efficient operation of Windows Server 2012 and an Intel 82578DC Gigabit Network Connection on the server workstation, and an Intel Core i7-2600 CPU 3.40 GHz processor with 8.0 GB RAM for the efficient operation of Windows 8.1 Pro and an AC1750 Wireless Dual Band PCI Express Adapter on the client workstation. The client was connected to the server wirelessly by a Linksys lapac1750pro business Access Point. For more details about hardware specifications, see Appendix A.

Access Point Configurations

Several settings on the Access Point had to be re-configured to ensure the maximum throughput possible. These settings were used for all the three different scenarios to ensure consistency. Unitec's IT Support center has provided a heat map of channels and power levels used in the area of conducting the experiments (Figure 5.1). The heat map gives important information that makes sure the channel used for the tests does not overlap with the channels used by the Unitec wireless networks. It also determined which was the best setting of AP power level used during the experiments. According to the heat map figure 5.1, there were 9

wireless (5GHz & 2.4GHz) Access Points deployed. At 5 GHz band, two APs occupied 36 and 44 channel widths in building 182, floor 2.

The area covered by wireless network can be influenced by the amount of power an Access Point. The higher the power level on Access Points, the larger the coverage area of a wireless network, but with minimal overlap between Access Points that share the same channel—this minimises co-channel interference [80]. The following table describes the most significant settings and configurations for the Access Point [81].

AP Settings	Configuration
Channel Bandwidth	There are three options available 20 MHz, 40 MHz and 80 MHz. Set at 80 MHz to utilise the full bandwidth.
Wireless Channel	Channel 40 was selected due to interference from other Unitec's Access Points in the surrounding area.
Beacon Interval	Beacon frame carries regulatory and capability information at regular intervals to inform the nearby wireless devices of its existence. Beacon Interval has an effect on signal stability and battery life. Due to our concern for the signal stability, setting was left on default at 100ms, which gives more signal stability, but at the same time will increase the battery drain [82].
Protection	This setting was disabled to make sure the data transmission did not produce an interference with legacy devices or applications that within the range of the Access Point.
RTS Threshold	RTS threshold helps to control traffic flow over the Access Point, especially dealing with a number of clients. Putting the maximum value of RTS Threshold (2347) can increase the throughput of the packet, and reduce bandwidth consumption.
Security	"Disabled" or "WPA2-Personal" was selected depending on the test-bed scenario. Security was only disabled in the first phase of studying, which was the effect of implementing WPA2 security on the performance compared to no encryption applied scenario.
Transmit Power	This setting was left at the default value which is 100%. The maximum transmit power value provides the Access Point a highest broadcast range.

Table 5.1: Access point configuration for the test-bed

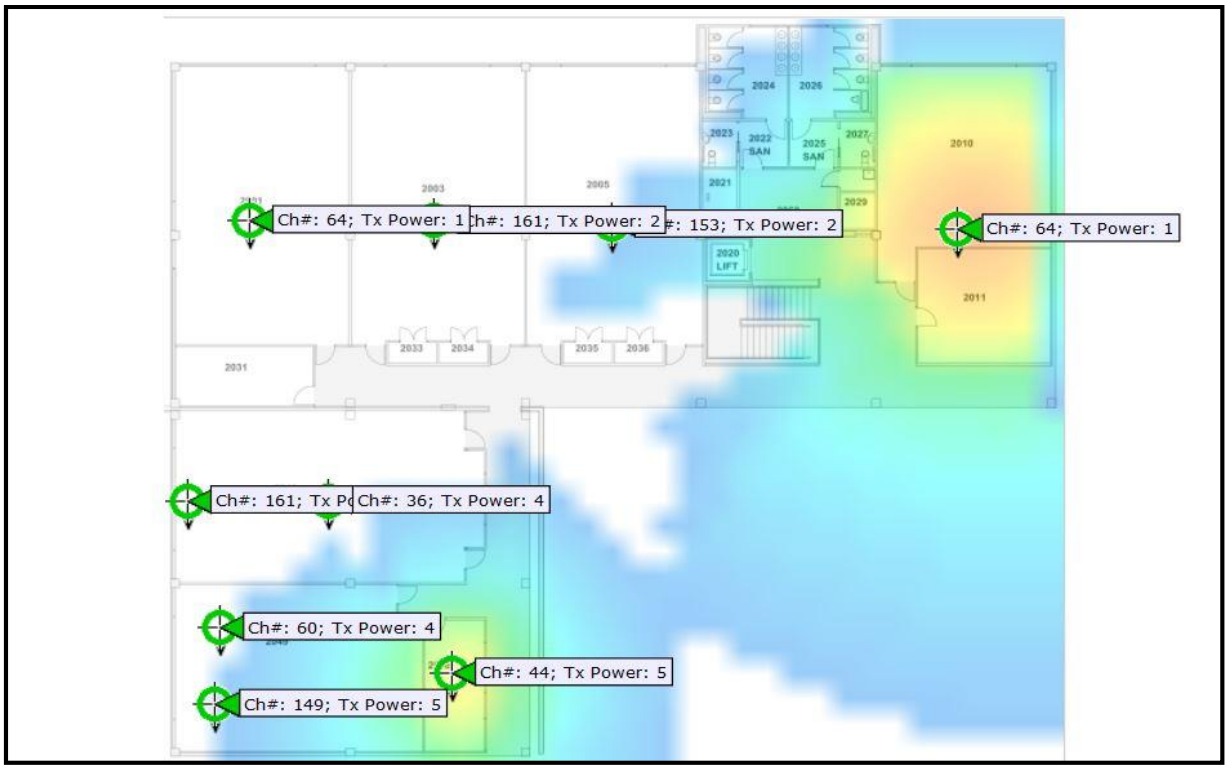

Figure 5.1: Unitec wireless channels and power levels for building 182, floor 2

5.1.2 Software

In terms of software specification, two operating systems were involved in this study; one of them was Windows 8.1 operating system and the other was Windows server operating system. Table 5.5 describes the operating systems, roles, and software installed on the system.

Operating System	Role	Software installed
Windows Server 2012 r2	Server	JPerf and Netperf
Windows 8.1 Pro	Client	JPerf, Netperf, and inSSIDer

Table 5.2: Software specifications

Network Performance Measurements Tools

There are many networks benchmarking tools available. The selecting tools for this experiment based on the similar tools that have been used in the earlier studies in the area.

Jperf

Jperf 2.0.2 [83] is a package that runs as a graphical user interface (GUI) over Iperf. It performs all tests that are executed by Iperf, and generates the same output results as well. The Jperf front end has various text boxes and radio buttons, each of them related to one Iperf command-line [69].

The same Iperf software executes for both client and server workstations. It produces and measures the transmitted packet for TCP and UDP by applying either IPv4 or IPv6 protocols. Delay, jitter and packet loss can only be measured in the UDP network [69]. IPerf has been found to have a higher bandwidth measurement compared to other popular traffic generators in a laboratory environment [84]. In this research, Jperf was the primary tool used for generating and measuring throughputs. To run JPerf, it needed to be installed on two computers, a server computer and a client computer. The former would act as a JPerf client, while the latter would act as the JPerf server.

After operating the trial tests and examining the outcome, it can be determined that the best settings employed for this study were the following:

Options	TCP	UDP
Report Interval	Between 60 to 300 seconds	
Testing Mode	Unchecked option	
Buffer Length	64 KBytes	X
TCP Windows Size	128, 384, 640, 896, 1152, 1408 Bytes (256, 512, 768, 1024, 1280 additional packets for scenario 1)	X
Max Segment Size	1460 Bytes	X
TCP No Delay	Checked option	X
UDP Bandwidth	X	900 MBytes/sec
UDP Buffer Size	X	128, 384, 640, 896, 1152, 1408 Bytes (256, 512, 768, 1024, 1280 additional packets for scenario 1)
UDP Packet Size	X	Default (1500 Bytes)

Table 5.3: Jperf optimal values

The 60 seconds duration on different packets displayed a very stable setting to measure the effect of implementing WPA2 scenario. In contrast, the 300 seconds was a suitable duration to measure the effect of shadowing and human movement scenarios. Testing Mode was unchecked because the experiment focused on evaluation the traffic that was sent in one side (Client) to the other (Server). It is possible to have traffic in both directions by choosing Dual. If Trade option is selected, traffic will be sent in both directions but the tests will be performed one after another. The TCP buffer length is the amount of traffic that can be queued for transmission. The default value is 8 Kb, but in the practical assessment the 64 Kb was found to be the best setting to get a highest throughput. The packet sizes mentioned on the table are

usually selected to measure network performance in the vast majority of previous researches. The 1460 Bytes value was selected in TCP Maximum Segment Size (MSS) setting. MSS is the largest amount of data, in Bytes, that a computer can support in a single, un-fragmented TCP segment. This leaves 1460 Bytes of the payload that can be transmitted in one frame without any possible chance of packet drop [85]. By selecting "TCP No Delay", the software will disable Nagle's algorithm. This algorithm is responsible for reducing network overhead by delaying the transmission of a small packet until all previously transmitted packets are acknowledged [86]. UDP Packet Size was kept as default (1500 Bytes). The MSS option does not work for UDP applications because UDP is a connectionless protocol. Notice that the 1470 Bytes is actually the UDP packet payload and does not include the 8 bytes for UDP header nor the 20 bytes IP header for IPv4 or 40 bytes for IPv6. With IPv6 the total packet size is 1470+8+40=1518 Bytes, which is more than 1500 Bytes and has to be fragmented [42].

Netperf

The Netperf [87] programme was used to measure Round Trip Time (RTT) over the Wi-Fi network. Netperf can either work as a client or a server application. On the server side, the programme can listen for connections from a remote host, while the programme can initiate the wired/wireless network test with the server on the client side. Netperf can be used for both TCP and UDP evaluations with IP versions 4 and 6. Netperf can be used on various operating systems such as Windows, Linux, and UNIX. Netperf uses the command-line below to calculate RTT:

netperf -l 30 -H *server IP address* -v 2 -f x -t TCP_RR -- -r 128 -s 512K -S 512K

Notice that the reading of the round trip time is in microseconds, which need to be converted to milliseconds (10^{-3}).

Typeperf

The primary tool used to collect the CPU utilisation was Typeperf [88], which is a Windows built-in tool that measures the percentage of CPU usage and exports the data to the command window screen or to a log file. The CPU usage was collected during the generator tool sending the traffic from the server to the client. The utilisation of CPU was recorded on the client workstation for 1 to 5 minutes (10-15 runs) depending on the test-bed scenario. It is important to synchronise the Typeperf with traffic generator during the test and disable unnecessary running software over the Microsoft Resource Monitoring tool. The results output present the percentage of consuming the CPU every single second in an exported Excel file. Figure 4.2 illustrates the CPU utilisation code and output.

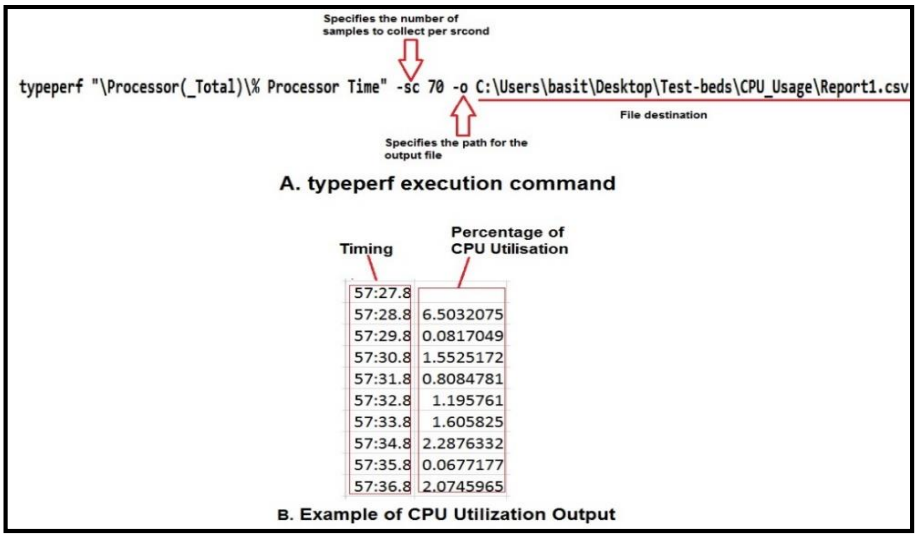

Figure 5.2: Example of CPU Utilisation execution command and output

InSSIDer

InSSIDer [89] is used to measure the signal strength. The software has the capability to identify hardware vendor of Access Points, channels used, name of the network, security protocol used and frequency of the Access Point. InSSIDer is used to determine a suitable place for deploying an Access Point, or for tweaking the existing range on a Wi-Fi network. In this research, inSSIDer was used to detect the channels used for surrounding APs in the area of conducting the experiments. It ensures the conducting tests do not overlap with the channels used by the Unitec wireless networks.

5.2 Experimental Scenarios

Three different network scenarios were carried out, namely, implementing WPA2 security algorithm, examining human movement in indoor environmental conditions, and shadowing (walls) and distance in a laboratory environment. The objective of conducting these scenarios is to study their impact on the performance of the 802.11 ac WLANs.

For all scenarios, two machines and an 802.11ac wireless Access Point (Linksys lapac1750pro) were required. One machine was a server Operating System (Windows Server 2012) while the other machine was a client Operating System (Windows 8.1). The client was equipped with an 802.11ac wireless NIC, which was connected wirelessly to Access Point (AP). The Access Point was connected to the server via Category 5e cabling. Throughput, delay, and CPU usage were measured by using JPerf, Netperf, and Typeperf respectively and were sent from the client to the server. To perform these experiments, traffic was generated from the PC client (Windows 8.1) to the server (Windows Server 2012).

All the experimental scenarios mentioned previously have the same existing hardware setups and settings. Parameters that were tested were the transport protocols (TCP and UDP), IP protocols (IPv4 and IPv6), and wireless security protocols (WPA2 or no security). Each of the parameters mentioned were tested on different packet sizes. The packet sizes are 128, 256, 384, 512, 640, 768, 896, 1024, 1152, 1280, 1408 Bytes, and the duration of each test on each packet was 1 to 5 minutes and was run 10 to 15 times. The results were captured and recorded on a Microsoft Excel spreadsheet. The average of these tests had to be under 0.05 in standard deviation ratio. Any irrelevant result was eliminated and the test run was repeated until it matched the criteria of under 0.05. The average figure was used for creating the comparison line graphs and the standard deviation was also calculated and compared.

5.2.1 Implementing WPA2 security encryption

Two phases of this scenario were carried out, for the purpose of establishing a baseline and to help in analysing the impact of adding a WPA2 encryption on the UDP and TCP traffic for both IPv4 and IPv6 over 802.11ac WLANs. The first phase of the experiment was for measuring the throughput, RTT, and CPU utilisation under normal conditions (no security applied in AP), which aimed at achieving a highest throughput in typical conditions. The second phase of the experiment was to analyse these matrices when WPA2 encryption was applied in order to measure the impact of WPA2 encryption over an 802.11ac Wi-Fi network.

The packet sizes (Bytes) that were tested for this scenario are 128, 256, 384, 512, 640, 768, 896, 1024, 1152, 1280, and 1408. The duration of each test on each packet was 60 seconds (consistent result) and was run between 10 to 15 times. The distance between the Access Point and the client was set closely to keep the signal strength very high.

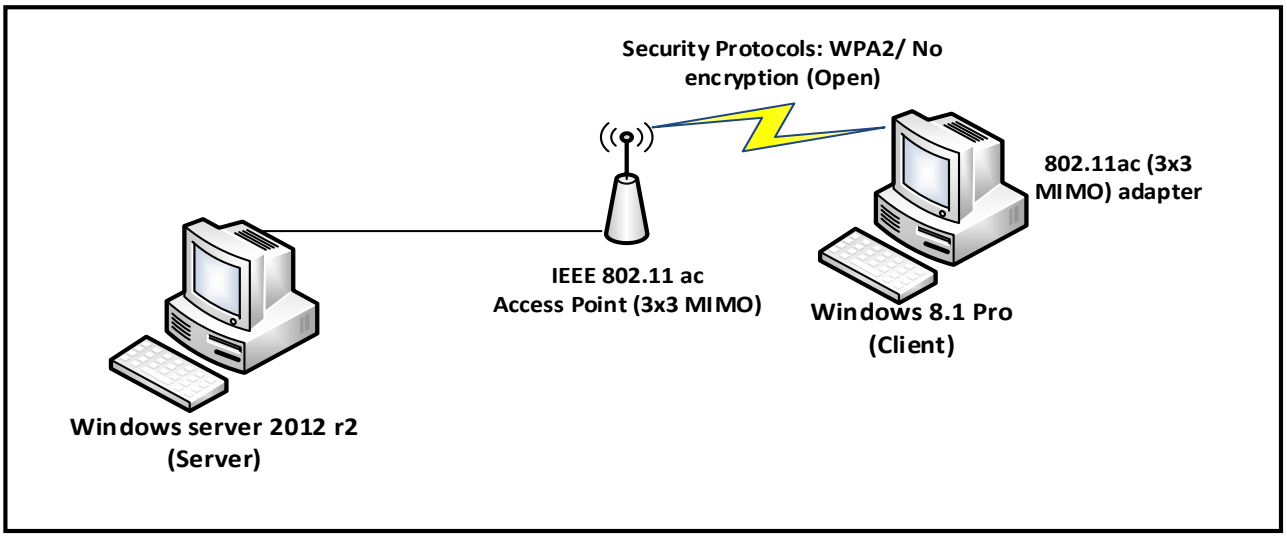

Figure 5.3: Client-Server WLANs diagram

5.2.2 Human movement in an indoor environmental conditions

In this scenario, two phases were conducted for the purpose of comparing the performance of the 802.11ac WLANs in the presence of human movement and normal conditions (no human movement) in an indoor environment. Test-beds were carried out inside the lab room, which has an exit door located at each end of the room. All computers were fixed in the centre of the room and along the wall. The pair of PCs was placed near the back end of the room, which gives a highest throughput result. The packet sizes (Bytes) that were tested for each scenario are 128, 384, 640, 896, 152, and 1408. The duration of each test on each packet was 300 seconds (consistent result) and was run between 10 and 15 times. The distance between the Access Point and the client was set to 3 metres to give a suitable space for body movement while the experiment was conducted. WPA2 encryption was selected in the Access Point security setting. Throughput, RTT, and CPU usage were parameters that tested for transport protocols (TCP and UDP), and IP protocols (IPv4 and IPv6).

No human obstruction

The purpose of conducting these test-beds was to establish a baseline data that compared with the presence of human movement data under the same environmental conditions. Test-beds consist of a space with no human movement between the pair of nodes.

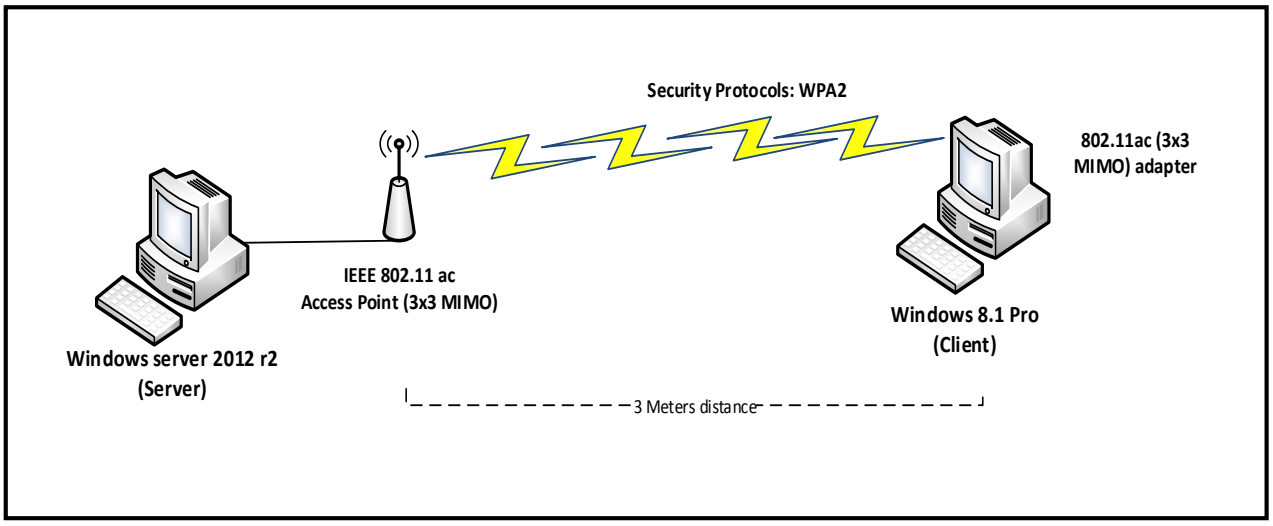

Figure 5.4: No human movement WLANs diagram

Human movement

During test-beds, three participants were standing side-by-side as a barrier (wall) in front of the Access Point and the client PC, while another participant was walking horizontally alongside the standing participants with steady movement backwards and forwards. Participants were located in the middle (1.5 metres) between the Access Point and the client PC. The movement continued until the data had completed transmitting to the client workstation. Figure 5.4 below illustrates human obstruction between a pair of nodes.

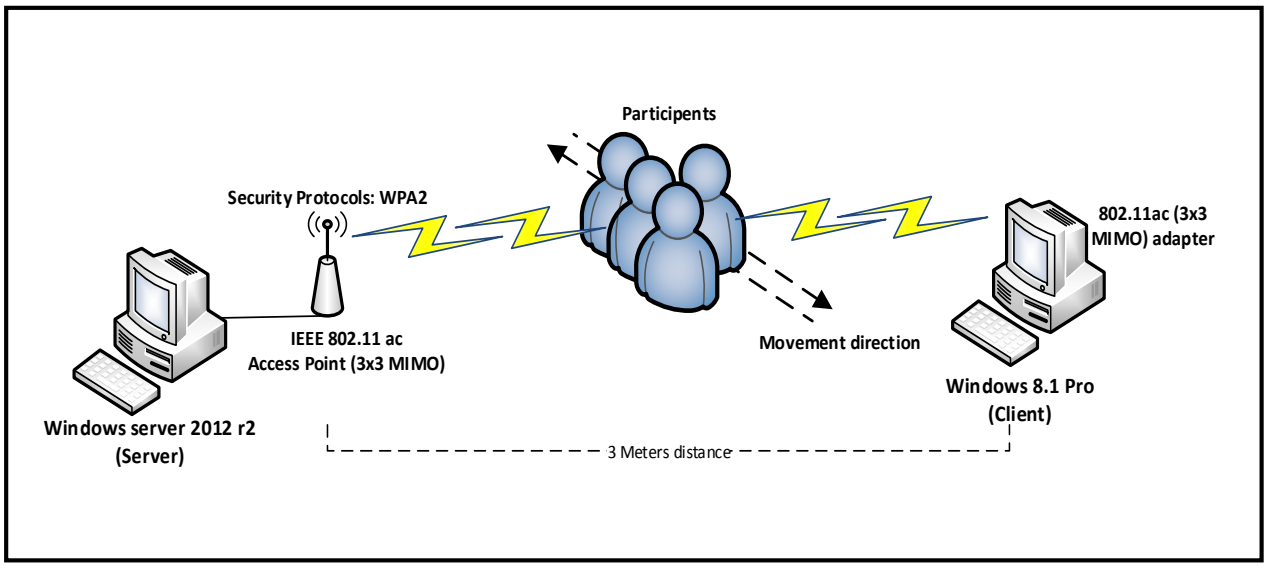

Figure 5.5: Human movement WLANs diagram

5.2.3 Shadowing in a laboratory environment

This scenario aims to study the impact of radio propagation in an indoor environment, which is influenced by building walls and by distance. The experiment was held at Unitec Institute of

Technology, on the second floor of 182 building. Test-beds were conducted at three different locations, with the Access Point being placed in one location during all tests. As mentioned before, only one Access Point was placed in lab 2010, where the client workstation has a different place for each scenario (see Figure 5.6). The first place for location of the client PC was in lab 2005, 5 metres away from the Access Point (lab 2010). In the second scenario, the client PC was moved to lab 2003, which is located 10 metres away from the Access Point. The client PC was moved to lab 2001, which is located 15 metres away from the Access Point in the third scenario. The exterior walls and flooring of the entire building are made of concrete. The internal walls and ceilings of labs are plastered. There are two hung windows for each lab. The labs have three common layouts: computers around the walls (lab 2010), computers in rows with all students facing the front (lab 2003); and a cluster of round tables with computers set up on them (lab 2005 & 2001). Facilities for all labs are: between 24-30 PCs, electronic whiteboard (lab 2005, l2003, and 2001), several chairs and wooden tables to study on. There is a one rubbish bin and one metal locker near the entrance door for each lab.

The packet sizes (Bytes) that were tested for each scenario are 128, 384, 640, 896, 152, and 1408. The duration of each test on each packet was 300 seconds (consistent result) and was run between 10 and 15 times. WPA2 encryption was selected in the Access Point security setting. Parameters that were tested are the transport protocols (TCP and UDP), and IP protocols (IPv4 and IPv6).

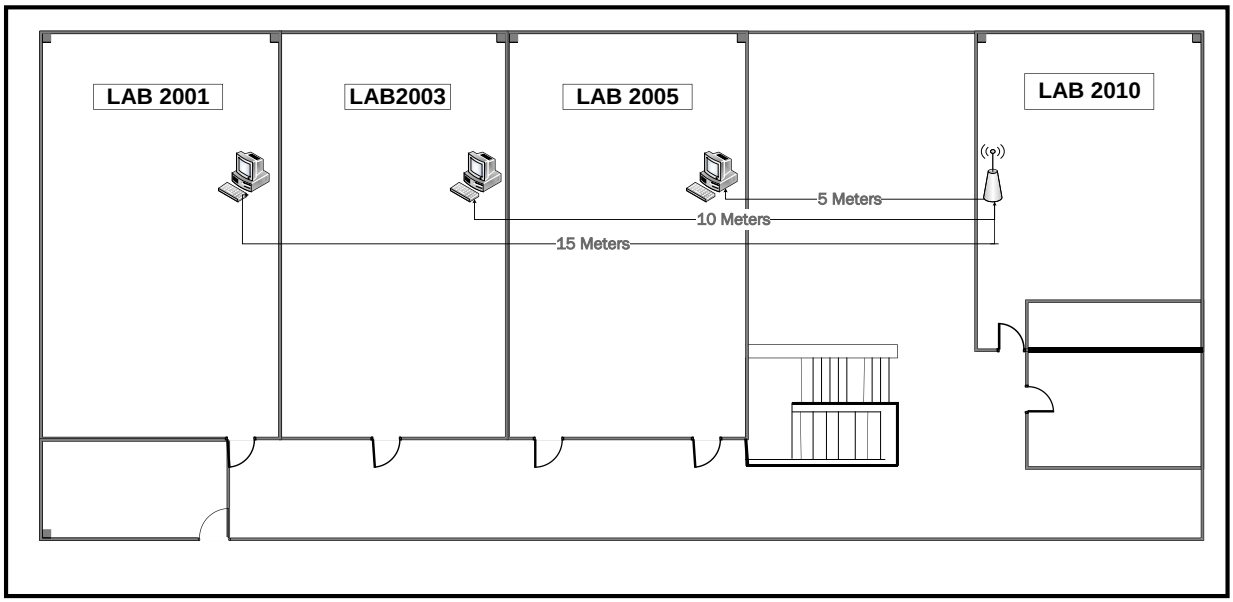

Figure 5.6: 182 Building 2nd Floor experiment area map

5.3 Chapter Summary

This chapter covered the experimental network set-up designs and network test-bed diagrams. There were two workstations used in this study, the server computer (traffic receiver), and the client computer (traffic transmitter). This chapter also covered the experimental set-up and best configuration software settings. Scenarios were described in detail.

The next chapter provides the details of evaluating the impact of implementing WPA2 encryption on 802.11ac WLAN performance.

CHAPTER 6

IMPACT OF WPA2 SECURITY ON 802.11ac WLAN PERFORMANCE

In this chapter, the data gathered from the first experimental scenario is analysed. The purpose of the analysis is to evaluate the effect of implementing WPA2 encryption on the performance of 802.11ac (Windows 8.1 - Windows Server 2012) WLAN using TCP and UDP for both versions of the Internet Protocol by conducting a comparison between open systems and implementing WPA2 security. Section 4.3.2, section 5.2, and section 5.2.1 (Figure 5.3) described in details the experimental data gathering process and experimental design for this scenario. Section 6.1 presents the throughput analysis. The round trip time analysis is discussed in section 6.2. Section 6.3 shows the CPU utilisation analysis. Section 6.4 shows comparison summary of the three metrics. Section 6.5 summarises the scenario outcomes.

6.1 Throughput Analysis

Figures 6.1 and 6.2 show the TCP and UDP throughput for IPv4 and IPv6 on Windows 8.1 with Windows Server 2012 running over 802.11ac WLANs, in environments where no security was enabled and in WPA2 security enabled environments. In all scenarios, as the packet size increased, the throughput of TCP and UDP increased consistently along with them. OS is an abbreviation for open system (no security enabled), while WPA2 is an abbreviation for implementing WPA2 security.

6.1.1 Comparison of TCP throughput

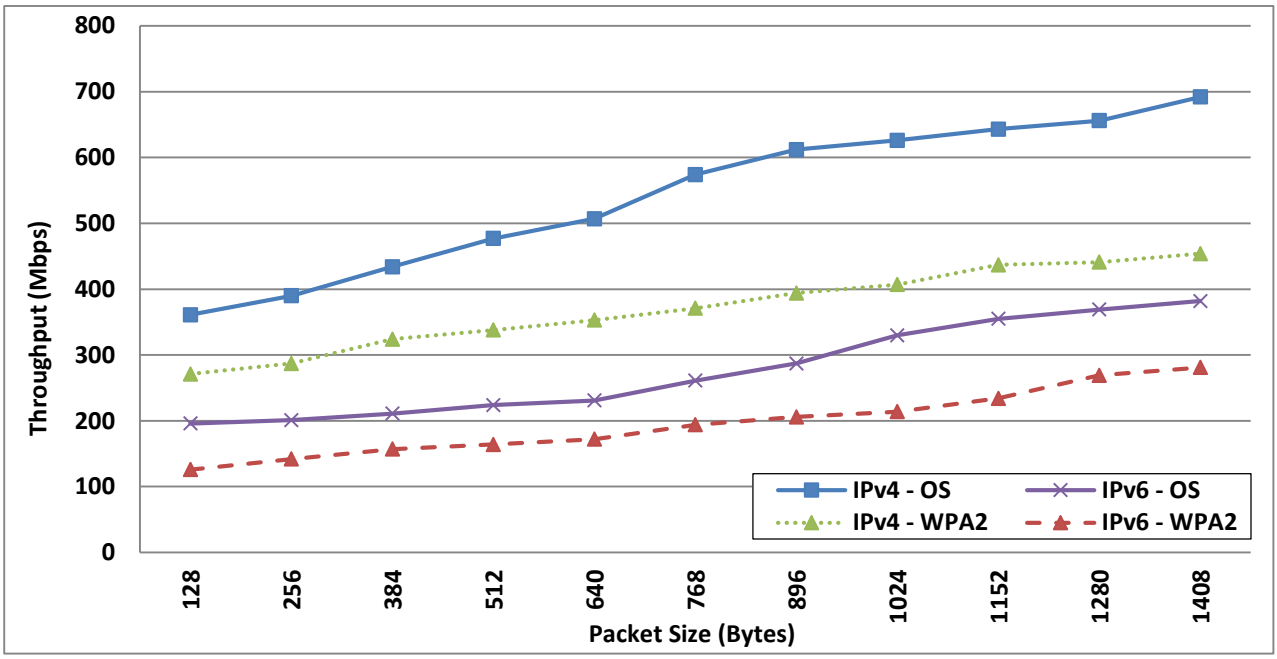

Figure 6.1: Comparison of TCP throughput for both versions of the Internet Protocol in 802.11ac WLAN, Open System vs. WPA2 security

Both with and without WPA2 encryption enabled, IPv4 outperforms IPv6 considerably for TCP throughput on all tested packet sizes. Without security enabled, the greatest improvement is observed at 896 Bytes packet size, where IPv4 outperforms IPv6 by 53.1% (612 Mbps for IPv4; 287 Mbps for IPv6), or higher by 325 Mbps. With WPA2 encryption enabled, the maximum difference in throughput is observed at 1152 Bytes packet size, where IPv4 outperforms IPv6 by 46.45% (437 Mbps for IPv4; 234 Mbps for IPv6), or higher by 203 Mbps.

Running 802.11ac WLAN without security enabled also provides higher throughput for TCP. The maximum improvement in TCP throughput for IPv4 is observed at packet size 1408 Bytes, where it outperforms IPv4 with WPA2 encryption enabled by 34.39% (692 Mbps for OS; 454 Mbps for WPA2), or higher by 238 Mbps. IPv6 without security enabled shows peak improvement at packet size 1152 Bytes, outperforming IPv6 with implementing WPA2 encryption by 34.1% (355 Mbps for OS; 234 Mbps for WPA2), or higher by 121 Mbps.

6.1.2 Comparison of UDP throughput

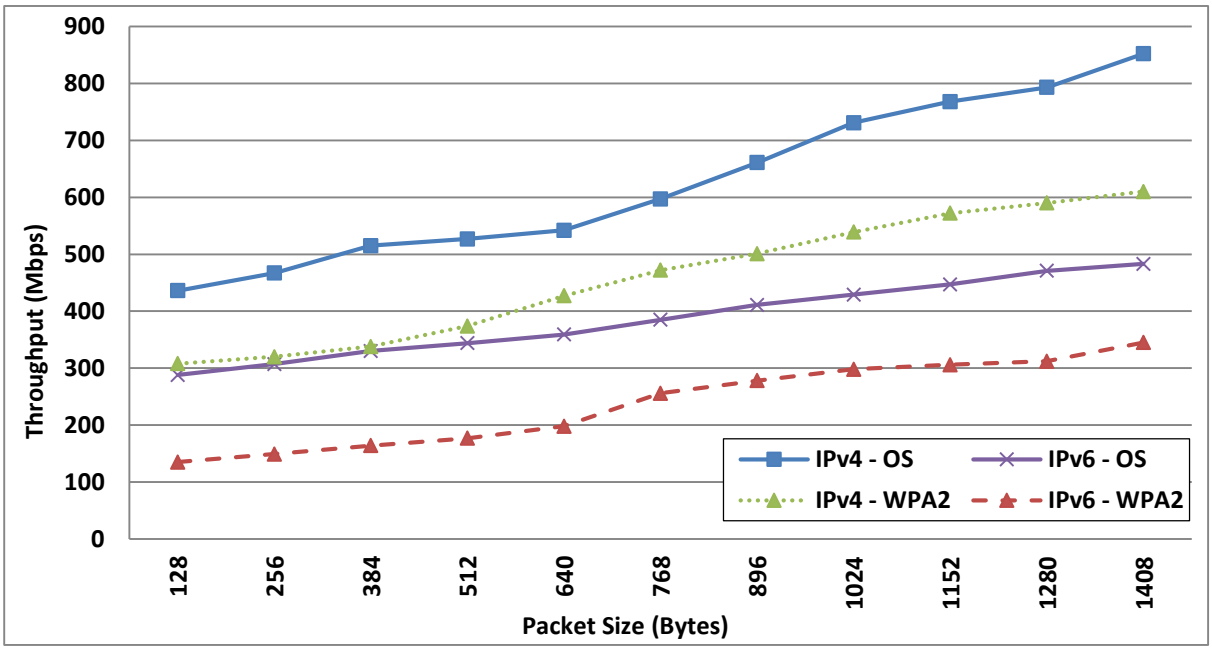

Figure 6.2: Comparison of UDP throughput for both versions of the Internet Protocol in 802.11ac WLAN, Open System vs. WPA2 security

Again, both with and without WPA2 encryption enabled, IPv4 significantly outperforms IPv6 for UDP throughput on all tested packet sizes. Without encryption enabled, the greatest improvement is observed at packet size 1408 Bytes, where IPv4 outperforms IPv6 by 43.31% (852 Mbps for IPv4; 483 Mbps for IPv6), or higher by 369 Mbps. With WPA2 encryption enabled, the highest throughput variation is observed at packet size 1280 Bytes, where IPv4 outperforms IPv6 by 47.12% (590 Mbps for IPv4; 312 Mbps for IPv6), or higher by 278 Mbps.

UDP throughput is also higher without security enabled. For IPv4, the maximum improvement appears at packet size 1408 Bytes, where it outperforms IPv4 with WPA2 encryption enabled by 28.40% (852 Mbps for OS; 610 Mbps for WPA2), or higher by 242 Mbps. The peak improvement for IPv6 without security enabled is observed at 512 Bytes, where it outperforms IPv6 with WPA2 encryption enabled by 48.55% (344 Mbps for OS; 177 Mbps for WPA2), or higher by 167 Mbps.

The results showed that implementing WPA2 security has a negative impact on the network throughput. This is because the WPA2 adds extra overhead (16 Bytes) [52]. Furthermore, IPv6 adds extra overhead (40 Bytes) compared to 20 Bytes extra overhead for IPv4 [42], so using IPv6 provides lower throughput for both UDP and TCP than IPv4.

6.1.3 Comparison of TCP and UDP throughput

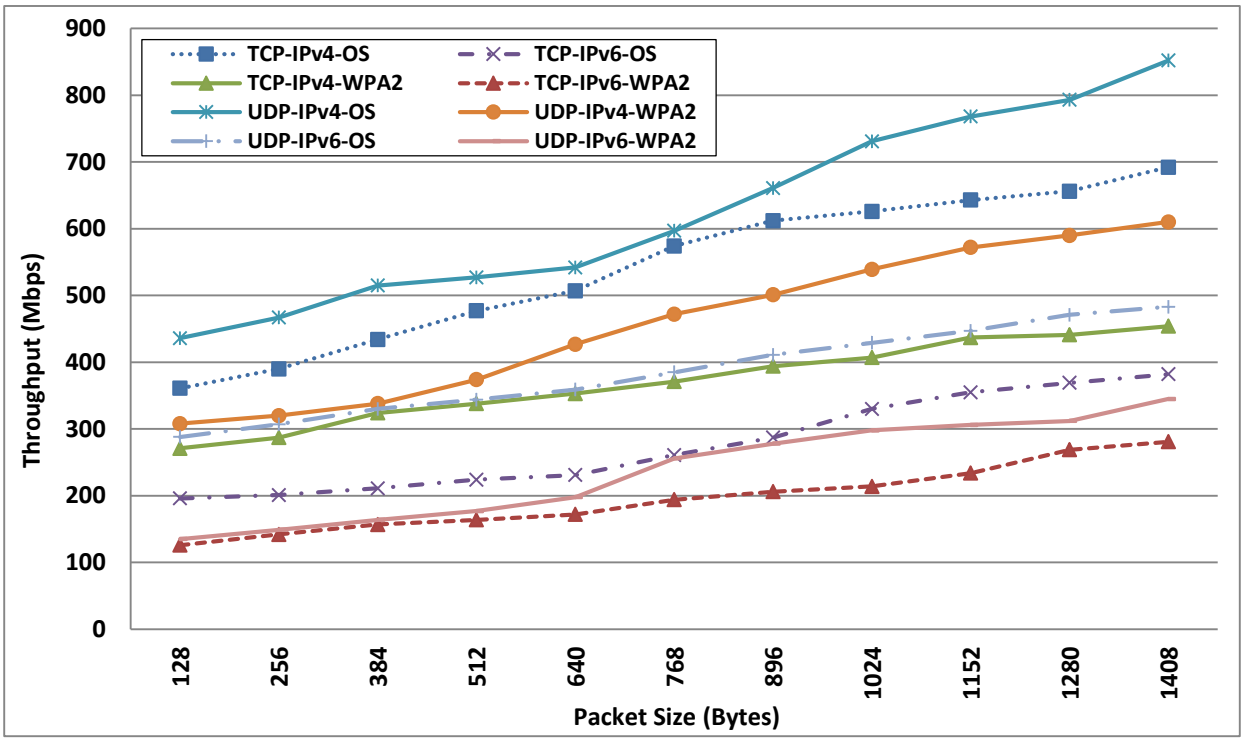

Figure 6.3: Comparison of TCP and UDP throughput for both versions of the Internet Protocol in 802.11ac WLAN, Open System vs. WPA2 security

All the throughput combined show that UDP with or without WPA2 encryption enabled has a greater throughput than TCP for both versions of the Internet Protocol on all tested packet sizes.

Without security enabled, the highest variation between UDP and TCP throughput for IPv4 appears at packet size 1408 Bytes, with an improvement of 18.78% (692 Mbps for TCP; 852Mbps for UDP), or 160 Mbps higher. For IPv6, the maximum difference is at 640 Bytes packet size, with an improvement of 35.65% (231 Mbps for TCP; 359 Mbps for UDP), or higher by 128 Mbps.

With WPA2 encryption enabled, the greatest improvement between UDP and TCP throughput for IPv4 appears at 1408Bytes packet size, with an increase of 25.57% (454 Mbps for TCP; 610 Mbps for UDP), or 156 Mbps higher. For IPv6, the maximum difference in throughput appears at 1024 Bytes, an increases of 28.19% (214 Mbps for TCP; 298 Mbps for UDP), or higher by 84 Mbps.

The reason for the overall superiority of the throughput results for UDP is that UDP has a lower overhead (8 Bytes) than TCP overhead (20 Bytes) [39].

6.1.4 Comparison of TCP and UDP throughput between 802.11ac and 802.11n

TCP throughput

Authors [22] evaluated the effect of enabling WPA2 encryption on TCP throughput for both versions of the Internet Protocol on 802.11n Wi-Fi network. Three Windows operating system were installed on two client-server networks (Vista - Server 2008 and XP - Server 2008).

In 802.11n WLAN (XP - Server 2008), IPv4 with WPA2 security enabled decreases TCP throughput by an average of approximately 7.07% (6.83 Mbps) less than IPv4 in open system. This is more than four times less than implementing WPA2 for IPv4 on the 802.11ac WLAN, which decreases TCP throughput by an average of about 31.73% (172.27 Mbps) less than IPv4 in open system. In 802.11n WLAN, TCP throughput for IPv6 drops of at least 5.42% (4.71 Mbps) compared to IPv6 without implementing WPA2, when 802.11ac Wi-Fi networks decreases TCP throughput for IPv6 to 29.14% (80.73 Mbps) by enabling WPA2 compared with IPv6 in open system. Overall, 802.11ac has the highest TCP throughput degradation values for both versions of the Internet Protocol by implementing WPA2 encryption compared to 802.11n that used the same security mechanism.

UDP throughput

Authors [21] evaluated the impact of implementing WPA2 security on UDP throughput over 802.11n WLANs for both versions of the Internet Protocol. Windows 7 and Windows Server 2008 were installed as operating systems on the Client-Server network.

In 802.11n WLAN (Windows 7 - Server 2008), IPv4 with WPA2 security enabled decreases UDP throughput by an average of approximately 24.33% (29.4 Mbps) less than IPv4 in open system. 802.11ac WLAN has slightly the higher UDP throughput degradation values for IPv4 with WPA2 enabled. It reduces the data rate by an average of about 26.68% (167.09 Mbps) less than IPv4 in open system. In 802.11n WLAN, UDP throughput for IPv6 drops of at least 10.14% (11.15 Mbps) compared to IPv6 without implementing WPA2, when 802.11ac Wi-Fi networks decreases UDP throughput for IPv6 to 38.46% (148.73 Mbps) by enabling WPA2 compared with IPv6 in open system. Overall, implementing WPA2 security over both standards showed that 802.11ac has the highest UDP throughput degradation values for both versions of the Internet Protocol by implementing WPA2 security compared to 802.11n that used the same security mechanism.

6.2 Round Trip Time (RTT) Analysis

Figures 6.4 and 6.5 show TCP and UDP RTT for both versions of the Internet Protocol on Windows 8.1 with Windows Server 2012 running over 802.11ac WLANs in environments where no security is enabled and in WPA2 security enabled. In all scenarios, as the packet size increases, the TCP and UDP RTT increase consistently along with them. OS is an abbreviation for open system (no security enabled), WPA2 is an abbreviation for implementing WPA2 security.

6.2.1 Comparison of TCP RTT

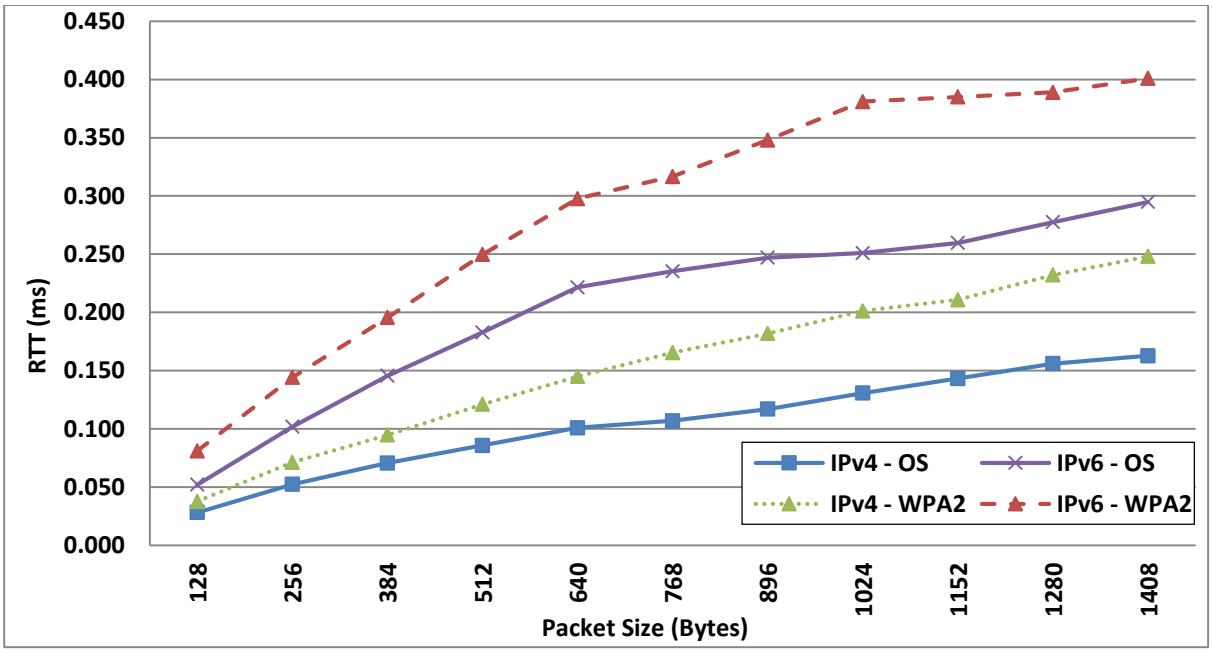

Figure 6.4: Comparison of TCP RTT for both versions of the Internet Protocol in 802.11ac WLAN, Open System vs. WPA2 security

With or without WPA2 encryption enabled, IPv4 performs better than IPv6 on all tested packet sizes. Without security enabled, the peak improvement between both versions of the Internet Protocol in RTT for TCP is observed at 1408 Bytes packet size, with an improvement of 53.23% (0.163 ms for IPv4; 0.295 ms for IPv6), or 0.132 ms faster. With WPA2 encryption enabled, the maximum improvement for IPv4 is at 1024 Bytes packet size, a difference of 47.24% (0.201ms for IPv4; 0.381 ms for IPv6), or 0.18 ms faster.

The results showed that without implementing WPA2 security, the TCP RTT is significantly faster for both versions of the Internet Protocol. The highest TCP RTT improvement between with and without of WPA2 encryption enabled is observed at packet size 1408 Bytes for IPv4, with an improvement of 34.27% (0.163 ms for OS; 0.248 ms for WPA2), or a 0.085 ms shorter

RTT. At packet size 1024 Bytes, applying IPv6 without encryption enabled results in a difference of 34.12% (0.251 ms for OS; 0.381 ms for WPA2), or a 0.13 ms shorter RTT.

6.2.2 Comparison of UDP RTT

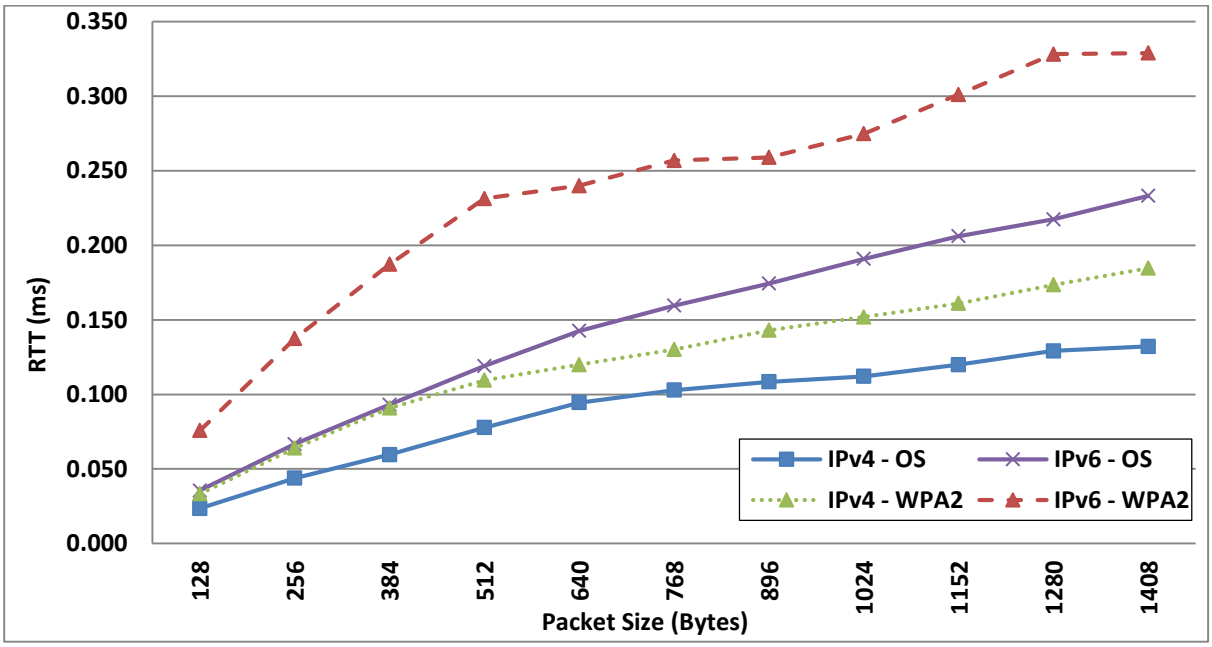

Figure 6.5: Comparison of UDP RTT for both versions of the Internet Protocol in 802.11ac WLAN, Open System vs. WPA2 security

For UDP RTT, IPv4 outperforms IPv6 on different packet sizes, with or without implementing WPA2 security. With no security enabled, the maximum UDP RTT difference is at 1408 Bytes packet size, with an improvement of 43.35% (0.132 ms for IPv4; 0.233 ms for IPv6), or a 0.101 ms shorter RTT. With WPA2 encryption enabled, the peak difference is at 1280 Bytes, where IPv4 outperforms IPv6 by 47.26% (0.174 ms for IPv4; 0.328 ms for IPv6), or a 0.155 ms faster rate.

The results also showed that implementing WPA2 significantly slows the RTT for both versions of the Internet Protocol. The peak UDP RTT difference between with and without of WPA2 encryption enabled is captured at packet size 1408 Bytes for IPv4, with an improvement of 28.11% (0.132 ms for OS; 0.185 ms for WPA2), or a 0.052 ms faster rate. At packet size 512 Bytes, applying IPv6 with no security enabled improves by 48.48% (0.119 ms for OS; 0.231 ms for WPA2), or a 0.112 ms faster rate.

In both scenarios, as the packet size increases from 128 to 1408 Bytes, the RTT consistently growing. Implementing WPA2 encryption has a negative impact on WLAN RTT, for TCP and UDP with both versions of the Internet Protocol. IPv6 adds extra overhead (40 Bytes); 20 Bytes

extra overhead by IPv4 [42], so that using IPv6 results in a longer RTT for both UDP and TCP than IPv4.

6.2.3 Comparison of TCP and UDP RTT

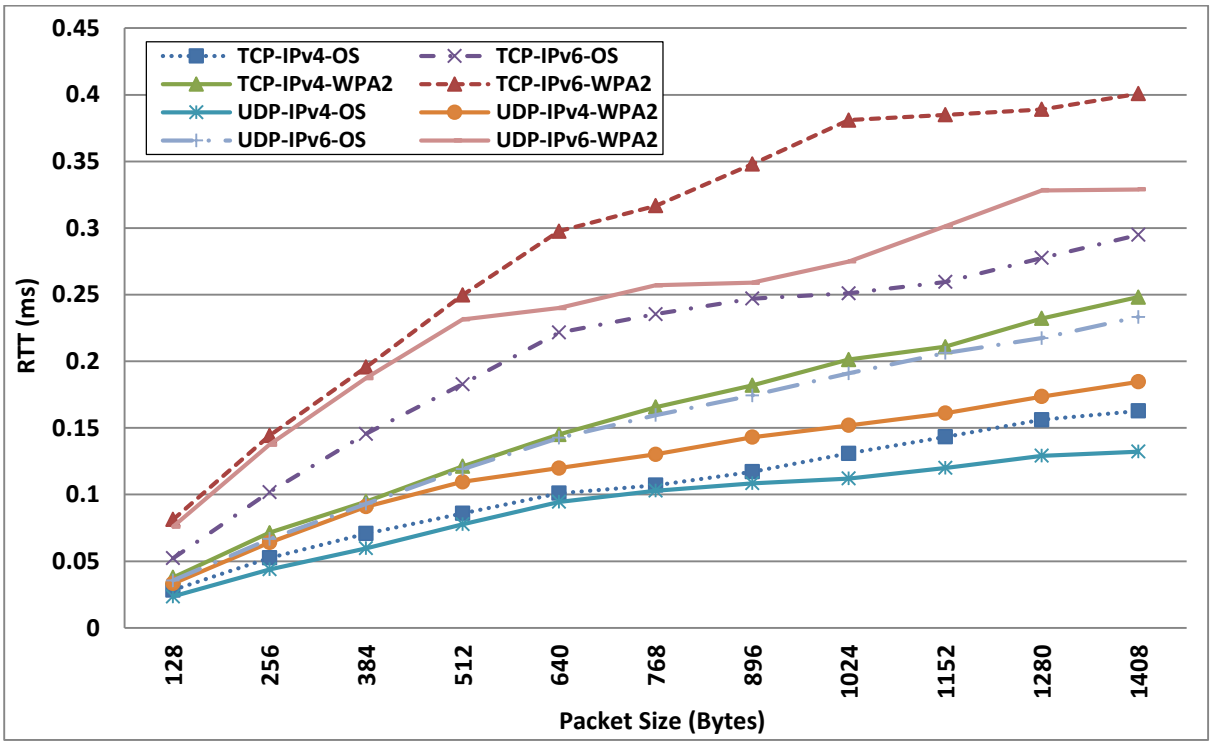

Figure 6.6: Comparison of TCP and UDP RTT for both versions of the Internet Protocol in 802.11ac WLAN, Open System vs. WPA2 security

The results showed that UDP with or without WPA2 encryption enabled achieves a faster RTT than TCP for both versions of the Internet Protocol on all tested packet sizes.

With no security enabled, the peak difference between UDP and TCP RTT for IPv4 is observed at packet size 1408 Bytes, where UDP is lower by 19.02% (0.163 ms for TCP; 0.132 ms for UDP), or a 0.031 ms shorter RTT. For IPv6, the maximum RTT difference between TCP and UDP is at 640 Bytes with an improvement of 35.59% (0.222 ms for TCP; 0.143 ms for UDP).

With WPA2 encryption enabled, the peak difference between UDP and TCP RTT for IPv4 appears at packet size 1408 Bytes, where UDP is lower by 25.4% (0.248 ms for TCP; 0.185 ms for UDP), or a 0.063 ms faster. For IPv6, the maximum RTT difference is at 1024 Bytes, where UDP outperforms TCP by 27.53% (0.381 ms for TCP; 0.275 ms for UDP).

UDP returns consistently faster results because UDP has a lower overhead (8 Bytes) than TCP (20 Bytes) [39].

6.3 CPU Utilisation Analysis

Figures 6.7 and 6.8 show the CPU utilisation on TCP and UDP protocols for both versions of the Internet Protocol on Windows 8.1 with Windows Server 2012 running over 802.11ac WLANs in environments where no security is enabled and in WPA2 encryption enabled environments. In all scenarios, as the packet size increases the TCP and UDP CPU utilisation decrease consistently along with them. OS is an abbreviation for open system (no security enabled), WPA2 is an abbreviation for implementing WPA2 security.

6.3.1 Comparison of TCP CPU Utilisation

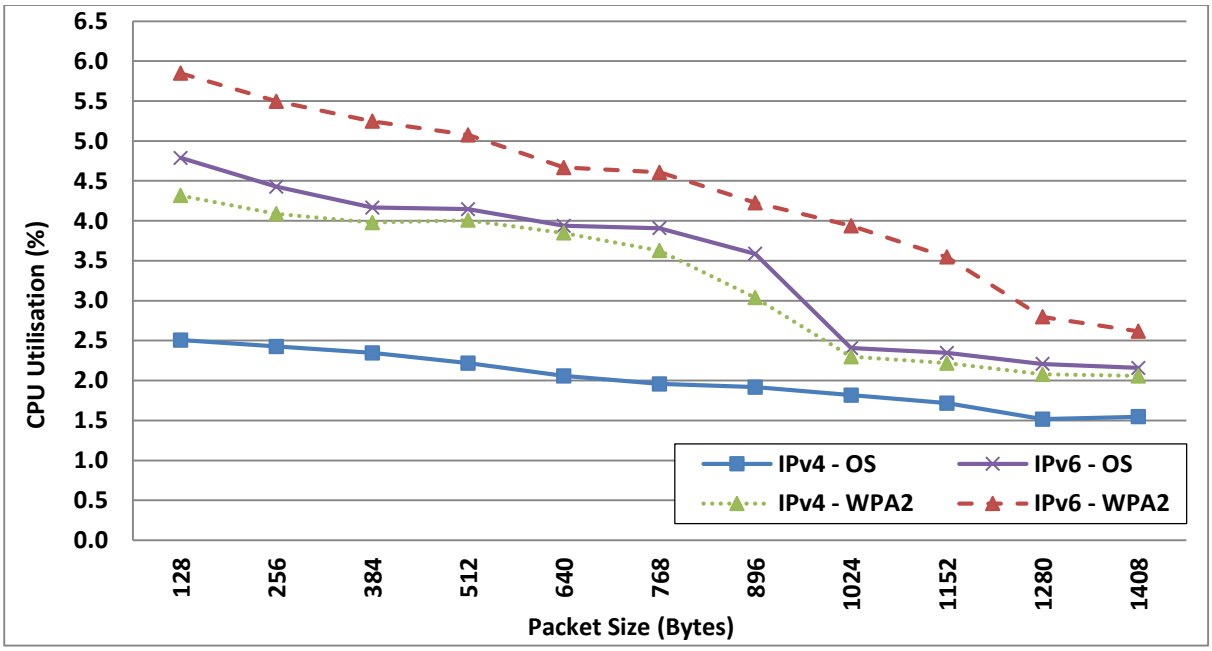

Figure 6.7: Comparison of TCP CPU Utilisation for both versions of the Internet Protocol in 802.11ac WLAN, Open System vs. WPA2 security

IPv4 consumes less TCP CPU resource than IPv6 on different packet sizes, with or without implementing WPA2 security. Without encryption enabled, the maximum improvement is at packet size 128 Bytes, where IPv4 is lower by 2.28% (2.51% for IPv4; 4.79% for IPv6). With WPA2 encryption enabled, the maximum improvement between IPv4 and IPv6 appears at 1024 Bytes, where IPv4 outperforms IPv6 by 1.64% (2.3% for IPv4; 3.94% for IPv6).

Comparing TCP CPU utilisation shows the usage is significantly lower for both IPv4 and IPv6 without implementing WPA2 encryption. At packet size 128 Bytes, applying IPv4 with no security enabled consumes less CPU resource by 1.81% (2.51% for OS; 4.32% for WPA2). At packet size 1024 Bytes, applying IPv6 with no security enabled consumes less CPU resource by 1.53% (2.41% for OS; 3.94% for WPA2).

6.3.2 Comparison of UDP CPU Utilisation

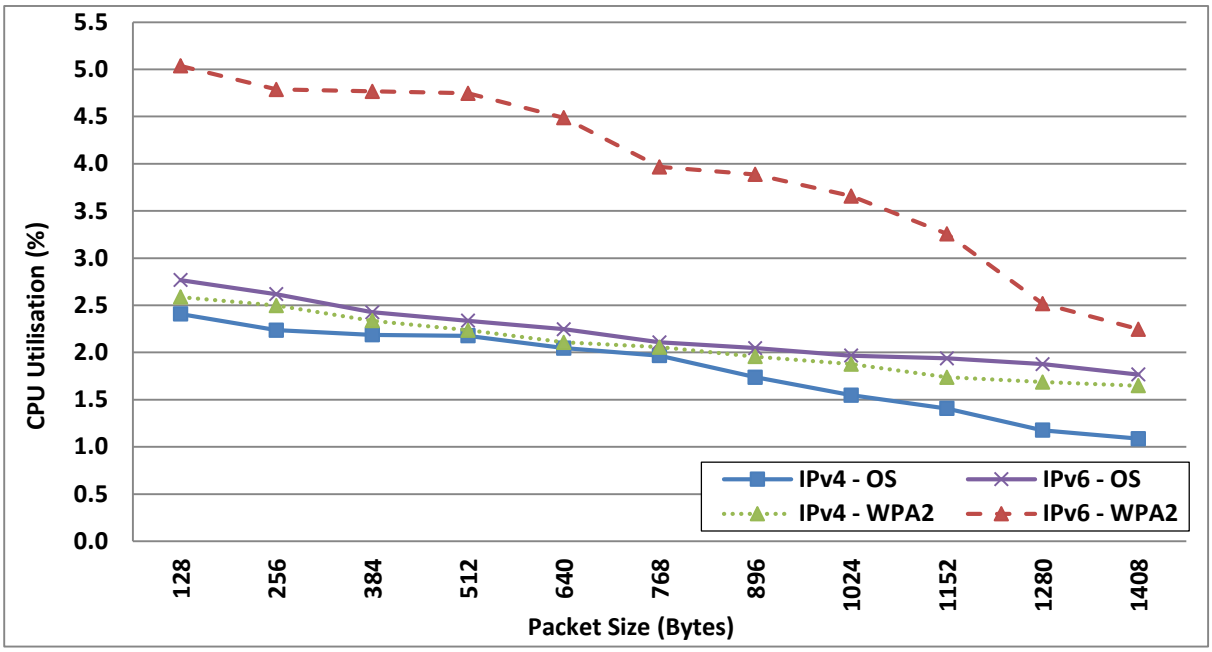

Figure 6.8: Comparison of UDP CPU Utilisation for both versions of the Internet Protocol in 802.11ac WLAN, Open System vs. WPA2 security

With or without security enabled, applying IPv4 consumes less UDP CPU resource than IPv6 on different packet sizes. Without security enabled, the peak improvement between IPv4 and IPv6 appears at packet size 1280 Bytes, with IPv4 consuming 0.7% less (1.18% for IPv4; 1.88% for IPv6). With implementing WPA2 encryption, the greatest improvement is at 512 Bytes, where IPv4 outperforms IPv6 by 2.51% (2.24% for IPv4; 4.75% for IPv6).

The results shows that without security enabled, the CPU usage is consistently lower for both versions of the Internet Protocol. The highest UDP CPU usage difference is observed at packet size 1408 Bytes for IPv4, with a 0.56% lower CPU utilisation rate (1.09% for OS; 1.65% for WPA2). For IPv6, the peak appears at 512 Bytes, achieving a 2.41% lower rate (2.34% for OS; 4.75% for WPA2).

In both scenarios, as the packet size increases from 128 to 1408 Bytes, CPU utilisation generally decreases. Implementing WPA2 security has a negative impact on CPU usage, both using TCP and UDP and for both IPv4 and IPv6. IPv6 adds extra overhead (40 Bytes) compared to 20 Bytes for IPv4 [42], with the result that IPv6 uses more CPU resources for both UDP and TCP than IPv4.

6.3.3 Comparison of TCP and UDP CPU Utilisation

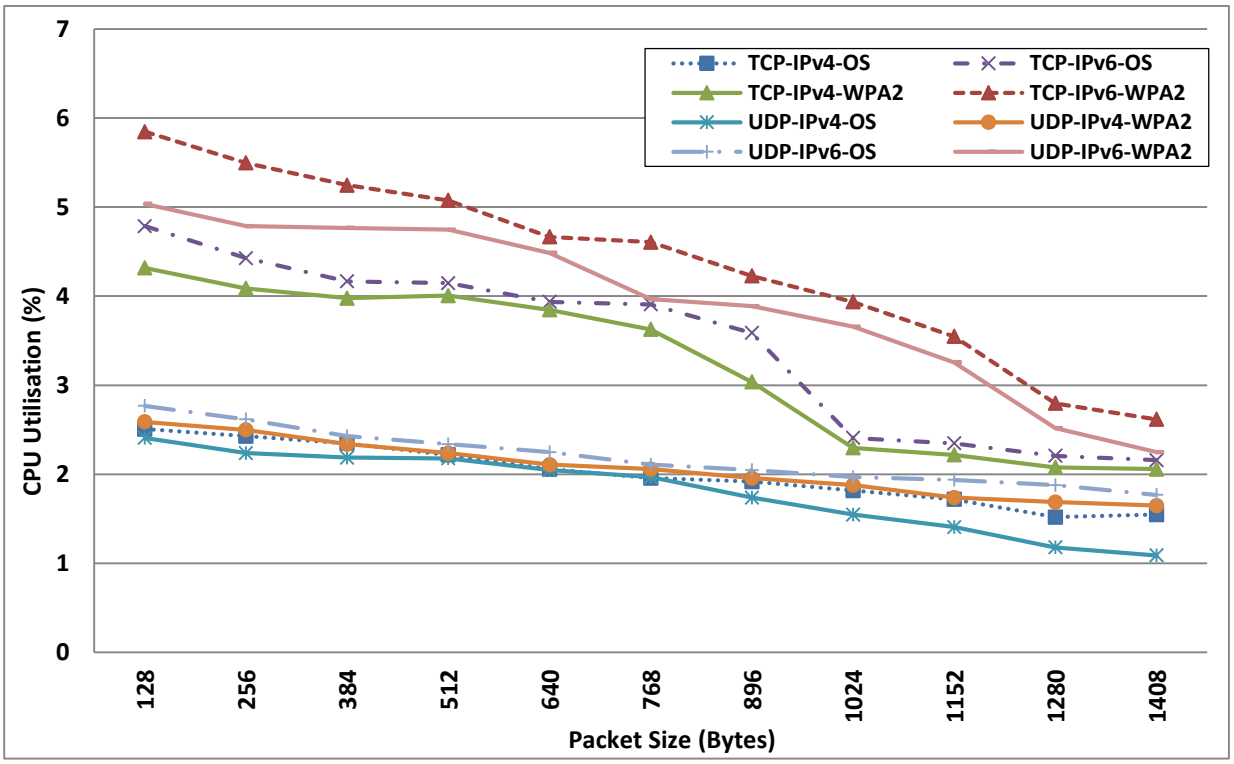

Figure 6.9: Comparison of TCP and UDP CPU Utilisation for the Internet Protocol in 802.11ac WLAN, Open System vs. WPA2 security

The results showed that UDP with or without WPA2 encryption enabled has a lower CPU usage than TCP for both IPv4 and IPv6 on all packet sizes.

With no security enabled, the maximum difference between UDP and TCP CPU usage for IPv4 is at packet size 1408 Bytes, where UDP has 0.46% lower CPU usage (1.55% for TCP; 1.09% for UDP). For IPv6, the peak CPU usage difference was also at 128 Bytes, where UDP outperforms TCP by 2.02% (4.79% for TCP; 2.78% for UDP).

With WPA2 encryption, the maximum difference between UDP and TCP for IPv4 is observed at packet size 512 Bytes, where UDP has 1.77% lower CPU usage (4.01% for TCP; 2.24% for UDP). For IPv6, the maximum CPU utilisation difference is at 128 Bytes, where UDP outperforms TCP by 0.81% (5.85% for TCP; 5.04% for UDP).

UDP has a consistently lower CPU usage because it has a lower overhead (8 Bytes) than the overhead for TCP (20 Bytes) [39].

6.4 Comparison Summary of Throughput, RTT, and CPU Usage

The overall results showed that on average, WLAN with WPA2 encryption enabled returned a lower throughput, longer RTT, and higher CPU usage for both TCP and UDP when implementing both versions of the Internet Protocol (IPv4 and IPv6).

Throughput comparison between with and without WPA2 encryption enabled

The results showed that on the average, the TCP and UDP on WLAN with WPA2 encryption enabled has a lower throughput than open system for both versions of the Internet Protocol. For IPv4, implementing WPA2 encryption decreased TCP throughput by 31.73% and UDP throughput by 26.68%. Implementing WPA2 encryption with IPv6, TCP and UDP throughput reduced about 29.14% and 38.46% respectively.

Throughput comparison between IPv4 and IPv6 with and without WPA2 encryption enabled

On average, throughput for IPv4 outperformed throughput for IPv6 when implementing TCP and UDP with or without WPA2 encryption enabled. With no security enabled, applying IPv6 decreased TCP throughput by 48.98% and UDP throughput by 38.25% compared to IPv4. With WPA2 security enabled, the TCP throughput for IPv6 dropped by 47.04% whereas UDP throughput for IPv6 decreased by 48.17%.

Throughput comparison between TCP and UDP with and without WPA2 encryption enabled

On average, UDP throughput outperformed TCP throughput when implementing IPv4 and IPv6 with or without WPA2 security enabled. Without security enabled, UDP achieved a higher throughput than TCP by 13.31% for IPv4 and 28.37% for IPv6. With WPA2 encryption enabled, UDP achieved a higher throughput than TCP by 19.28% for IPv4 and 17.53% for IPv6.

RTT comparison between with and without WPA2 encryption enabled

On average, the shortest TCP and UDP RTT for both IPv4 and IPv6 when no security enabled. With WAP2 security enabled, TCP RTT increased for IPv4 by 32.42% and UDP RTT by 26.30%. For IPv6 with implementing WPA2 encryption, TCP and UDP RTT rose about 28.83% and 37.48% respectively.

RTT comparison between IPv4 and IPv6 with and without WPA2 encryption enabled

On average, RTT for IPv4 outperformed RTT for IPv6 when applying TCP and UDP with or without implementing WPA2 security. For IPv6 with no security enabled, TCP had a longer RTT than IPv4 by 49.1% and UDP by 38.74%. With WPA2 encryption enabled, the TCP and UDP for IPv6 had a longer RTT than IPv4 by 46.37% and 48.04% respectively.

RTT comparison between TCP and UDP with and without WPA2 sec encryption enabled

On average, RTT for UDP outperformed RTT for TCP by implementing IPv4 and IPv6 with or without WPA2 encryption enabled. With no security enabled, UDP achieved a shorter RTT than TCP by 13.13% for IPv4 and 27.79% for IPv6. With WPA2 encryption enabled, UDP provided a shorter RTT than TCP by 20.35% for IPv4 and 17.80% for IPv6.

CPU utilisation comparison between with and without WPA2 encryption enabled

On average, the highest TCP and UDP CPU usage for both IPv4 and IPv6 were measured on WLAN with WPA2 security enabled. IPv4 with WPA2 encryption enabled rose the CPU usage by 1.23% for TCP and 0.25% for UDP. The TCP and UDP CPU usage increased by 0.91% and 1.75% respectively by applying IPv6 with WPA2 security enabled.

CPU utilisation comparison between IPv4 and IPv6 with and without WPA2 encryption enabled

On average, CPU usage for IPv4 outperformed CPU usage for IPv6 by applying TCP and UDP without or with implementing WPA2 security. With no security enabled, IPv6 had higher CPU usage than IPv4 by 1.46% for TCP and 0.38% for UDP. With WPA2 security enabled, IPv6 had higher CPU usage than IPv4 by 1.14% for TCP and 1.88% for UDP.

CPU utilisation comparison between TCP and UDP with and without WPA2 encryption enabled

On average, CPU usage for UDP outperformed CPU usage for TCP when implementing IPv4 and IPv6 with or without WPA2 security enabled. With no security enabled, UDP achieved a lower CPU usage than TCP by 0.19% for IPv4 and 1.27% for IPv6. With WPA2 encryption enabled, UDP achieved a lower CPU usage than TCP by 1.17% for IPv4 and 0.43% for IPv6.

6.5 Chapter Summary

In this chapter, it was demonstrated that with WPA2 encryption enabled, there was a negative impact on the throughput, RTT and CPU usage over 802.11ac WLANs. Both TCP and UDP had the shortest RTT and lowest CPU usage and highest throughput with no security enabled for both versions of the Internet Protocol. Moreover, implementing IPv6 had the lowest throughput and longest RTT and highest CPU usage compared with IPv4 for both TCP and UDP. Also, applying UDP outperformed TCP for both versions of the Internet Protocol. The results showed that on average, the highest throughput (626.27 Mbps), shortest RTT (0.91 ms) and lowest CPU usage (1.82%) were measured in the open system and applied IPv4 for the UDP protocol, whereas the lowest throughput (196.27 Mbps), longest RTT (0.29 ms) and highest CPU usage (4.37%) were measured in the implementation of WPA2 encryption and applied IPv6 for the TCP protocol.

The next chapter provides the details of evaluating the effect of human movement on 802.11ac WLAN performance.

CHAPTER 7

EFFECT OF HUMAN MOVEMENT ON 802.11ac WLAN

In this chapter, the data gathered from the second experimental scenario is analysed. The purpose of the analysis is to evaluate the effect of human movement on 802.11ac WLAN in indoor propagation environment (laboratory) in Unitec building 182, floor 2. Section 4.3.2, section 5.2, and section 5.2.2 (Figures 5.4 & 5.5) described in details the experimental data gathering process and experimental design for this scenario. Section 7.1 presents the TCP and UDP throughput analysis for both versions of the Internet Protocol. Section 7.2 covers the TCP and UDP round trip time analysis. Section 7.3 shows the TCP and UDP CPU utilization analysis for IPv4 and IPv6. Section 7.4 shows comparison summary of the three metrics. Section 7.5 summarises the scenario outcomes.

7.1 Throughput Analysis

Figures 7.1 and 7.2 show the throughput on TCP and UDP protocols for both versions of the Internet Protocol on Windows 8.1 with Windows Server 2012 running over 802.11ac WLANs in the presence of human movement and in non-human shadowing environments (i.e., without human movement). In all scenarios, as the packet size increases, so does the throughput of TCP. W-MOV is an abbreviation for without human movement; MOV is an abbreviation for human movement.

7.1.1 Comparison of TCP throughput

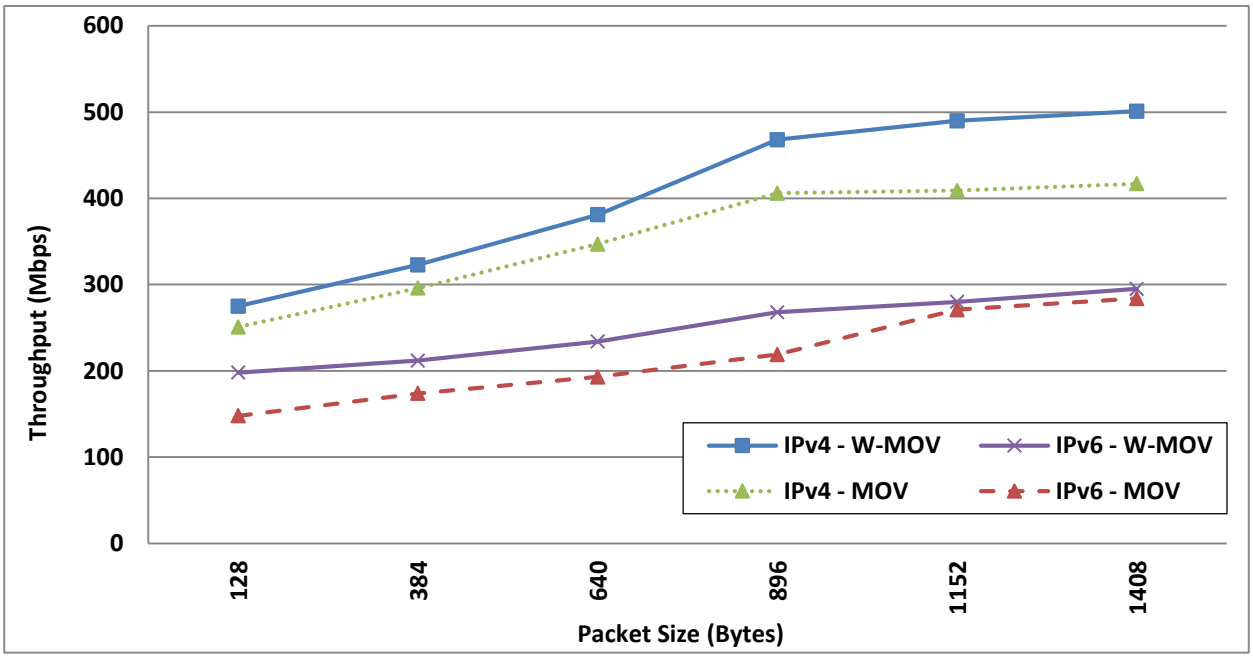

Figure 7.1: Comparison of TCP throughput for both versions of the Internet Protocol in 802.11ac WLAN, without human movement vs. with human movement

Both with and without human movement, IPv4 outperforms IPv6 considerably for TCP throughput on different packet sizes. Without human movement, the maximum difference is observed at 1152 Bytes packet size, where IPv4 outperforms IPv6 by 42.86% (490 Mbps for IPv4; 280 Mbps for IPv6), or higher by 210 Mbps. With human movement, the maximum difference in throughput is observed at 896 Bytes packet size, where IPv4 outperforms IPv6 by 45.72% (406 Mbps for IPv4; 219 Mbps for IPv6), or higher by 187 Mbps.

Running 802.11ac WLAN without human movement also provides higher TCP throughput. The maximum improvement in TCP throughput for IPv4 is observed at packet size 1408 Bytes, where it outperforms IPv4 with human movement by 16.77% (501 Mbps for W-MOV; 417 Mbps for MOV), or higher by 84 Mbps. IPv6 without human movement shows peak improvement at packet size 128 Bytes, outperforming IPv6 with human movement by 25.25% (198 Mbps for W-MOV; 148 Mbps for MOV), or higher by 50 Mbps.

7.1.2 Comparison of UDP throughput

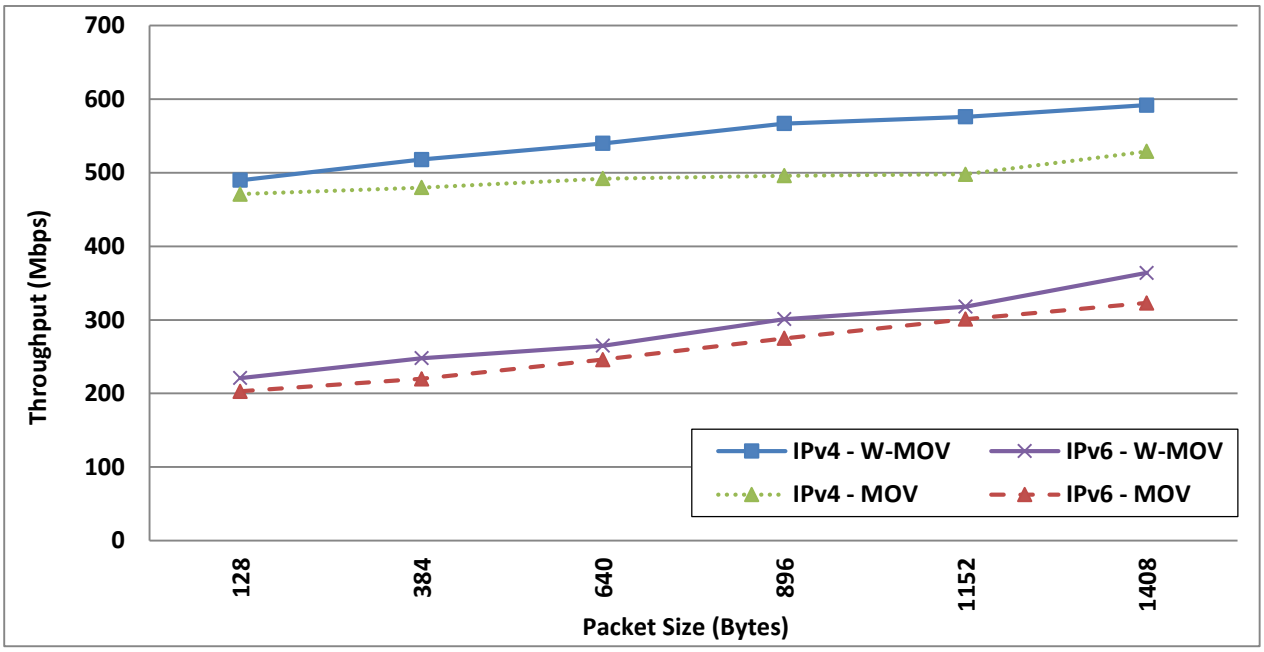

Figure 7.2: Comparison of UDP throughput for both versions of the Internet Protocol in 802.11ac WLAN, without human movement vs. human movement

Again, both with and without human movement, IPv4 significantly outperforms IPv6 for UDP throughput on different packet sizes. Without human movement, the greatest improvement is observed at packet size 640 Bytes, where IPv4 outperforms IPv6 by 50.93% (540 Mbps for IPv4; 265 Mbps for IPv6), or higher by 275 Mbps. With human movement, the greatest throughput improvement is observed at packet size 128 Bytes, where IPv4 outperforms IPv6 by 56.90% (471 Mbps for IPv4; 203 Mbps for IPv6), or higher by 268 Mbps.

UDP throughput is also higher without human movement. For IPv4, the maximum improvement appears at packet size 1152 Bytes, where it outperforms IPv4 with human movement by 13.54% (576 Mbps for W-MOV; 498 Mbps for MOV), or higher by 78 Mbps. The peak improvement for IPv6 without human movement is observed at 1408 Bytes, where it outperforms IPv6 with human movement by 11.26% (364 Mbps for W-MOV; 323 Mbps for MOV), or higher by 41 Mbps.

The results showed that human movement has a negative impact on the network throughput. This is because the human movement acts as a shadowing obstacle with a strongly adverse effect on the signal, thus decreasing throughput [5]. Furthermore, IPv6 adds extra overhead (40 Bytes) compared to 20 Bytes extra overhead for IPv4 [42], so using IPv6 provides lower throughput for both UDP and TCP than IPv4.

7.1.3 Comparison of TCP and UDP throughput

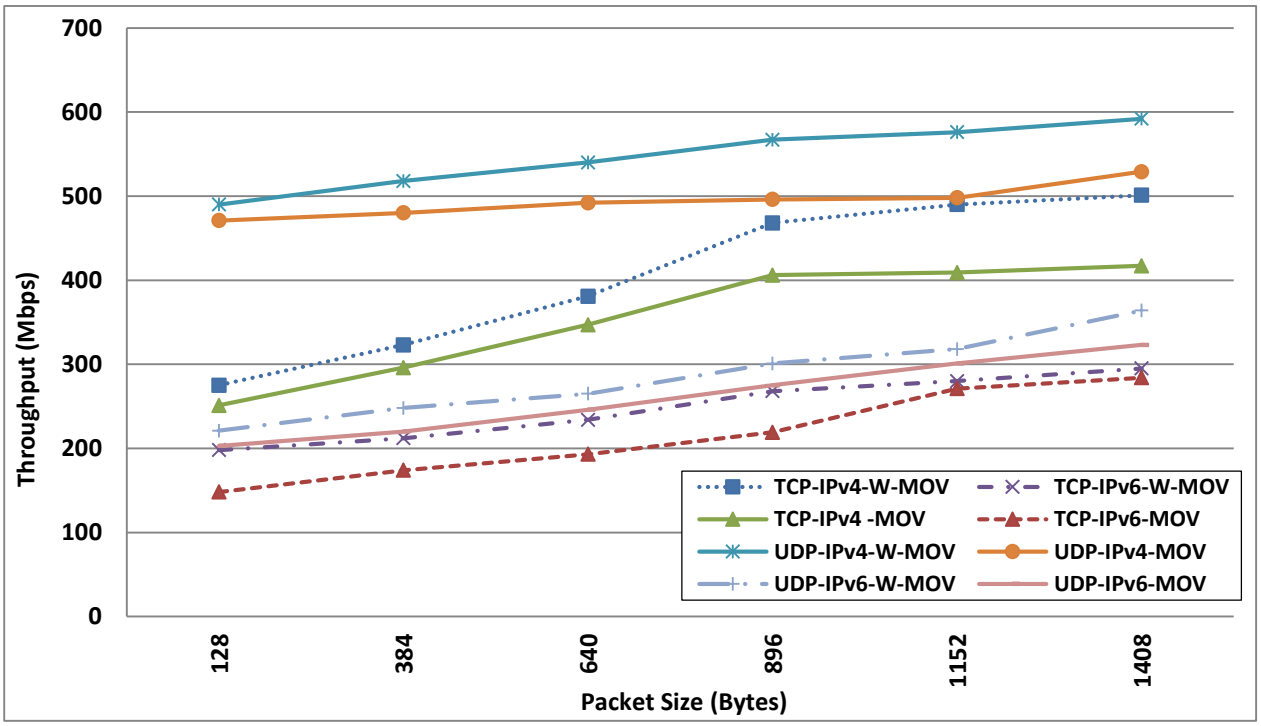

Figure 7.3: Comparison of TCP and UDP throughput for both versions of the Internet Protocol in 802.11ac WLAN, without human movement vs. human movement

All the throughput combined show that UDP with or without human movement has a greater throughput than TCP for both versions of the Internet Protocol on different packet sizes.

Without human movement, the peak improvement between UDP and TCP throughput for IPv4 appears at packet size 128 Bytes, with an improvement of 43.88% (275 Mbps for TCP; 490 Mbps for UDP), or 215 Mbps higher. For IPv6, the highest improvement is at 1408 Bytes packet size, with an improvement of 18.96% (295 Mbps for TCP; 364 Mbps for UDP), or higher by 69 Mbps.

With human movement, the maximum difference between UDP and TCP throughput for IPv4 appears at 128 Bytes packet size, with an increase of 46.71% (251 Mbps for TCP; 471 Mbps for UDP), or 220 Mbps higher. For IPv6, the greatest improvement in throughput appears at 896 Bytes, an increase of 20.36% (219 Mbps for TCP; 275 Mbps for UDP), or higher by 56 Mbps.

The reason for the overall superiority of the throughput results for UDP is that UDP has a lower overhead (8 Bytes) than TCP overhead (20 Bytes) [39].

7.2 Round Trip Time (RTT) Analysis

Figures 7.4 and 7.5 show the RTT on TCP and UDP for both versions of the Internet Protocol on Windows 8.1 with Windows Server 2012 running over 802.11ac WLANs in the presence of human movement and without human movement. In all scenarios, as the packet size increases, so does the TCP RTT. W-MOV is an abbreviation of without human movement; MOV is an abbreviation for human movement.

7.2.1 Comparison of TCP RTT

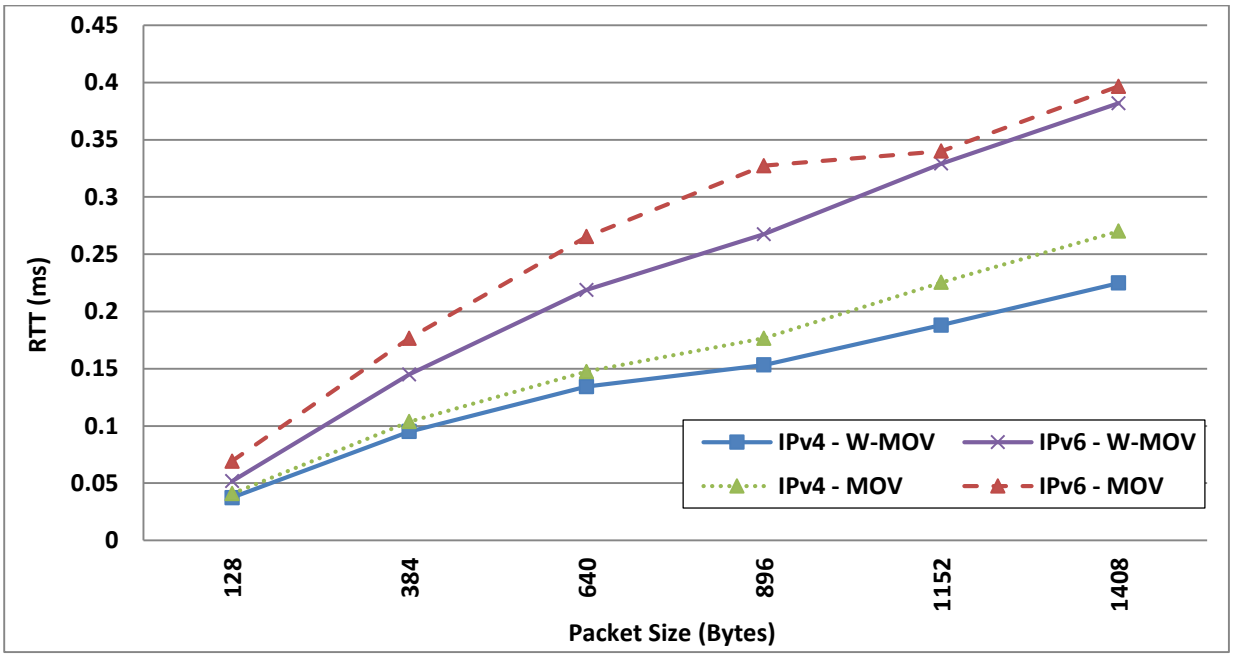

Figure 7.4: Comparison of TCP RTT for both versions of the Internet Protocol in 802.11ac WLAN, without human movement vs. human movement

With or without human movement, IPv4 outperforms IPv6 on all tested packet sizes. Without human movement, the peak improvement between IPv4 and IPv6 in RTT for TCP is observed at packet size 1408 Bytes, with an improvement of 41.10% (0.225 ms for IPv4; 0.382 ms for IPv6), or 0.157 ms faster. With human movement, the maximum improvement for IPv4 is at 896 Bytes packet size, a difference of 46.18% (0.177 ms for IPv4; 0.327 ms for IPv6), or 0.151 ms faster.

The results showed that without human movement, the TCP RTT is faster for both versions of the Internet Protocol. The highest TCP RTT improvement between absence and presence of human movement is observed at packet size 1408 Bytes for IPv4, with an improvement of 16.67% (0.225 ms for W-MOV; 0.270 ms for MOV), or a 0.045 ms shorter RTT. At packet size

896 Bytes, implementing IPv6 without human movement results in a difference of 18.35% (0.267 ms for W-MOV; 0.327 ms for MOV), or a 0.060 ms shorter RTT.

7.2.2 Comparison of UDP RTT

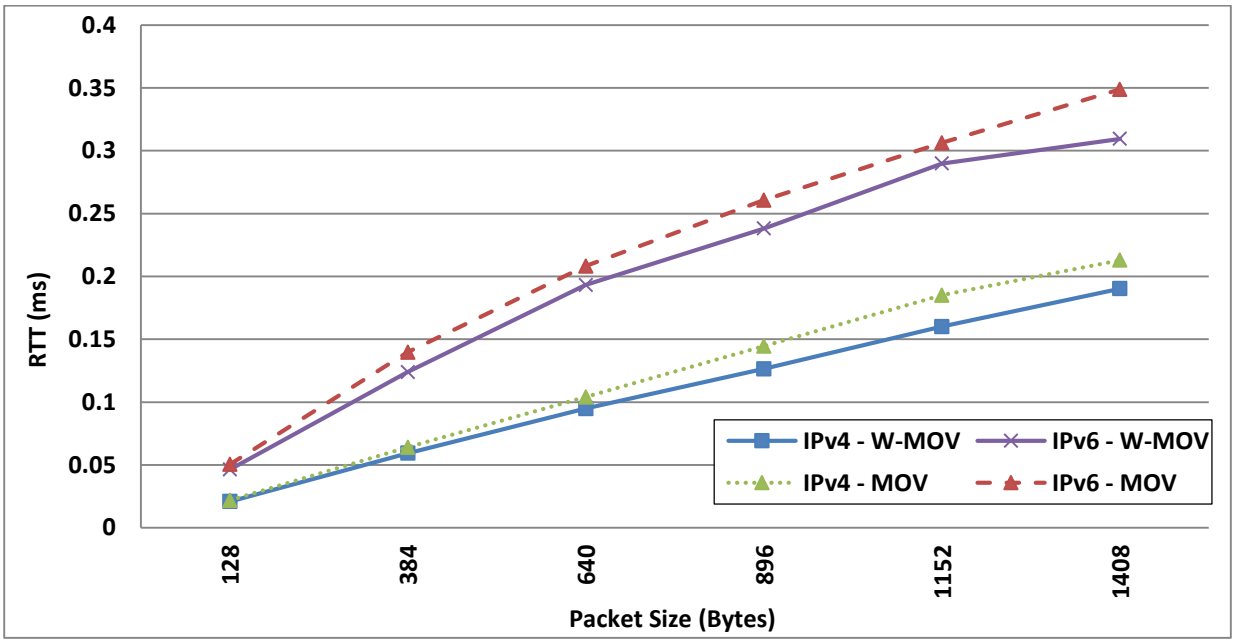

Figure 7.5: Comparison of UDP RTT for both versions of the Internet Protocol in 802.11ac WLAN, without human movement vs. human movement

For UDP RTT, IPv4 outperforms IPv6 on different packet sizes, with or without human movement. With no human movement, the maximum UDP RTT difference is at packet size 1152 Bytes, with an improvement of 44.83% (0.16 ms for IPv4; 0.29 ms for IPv6), or a 0.13 ms shorter RTT. With human movement, the peak difference is at 1408 Bytes, where IPv4 outperforms IPv6 by 38.97% (0.213 ms for IPv4; 0.349 ms for IPv6), or a 0.136 ms faster rate.

The results also showed that human movement significantly slows the RTT for both versions of the Internet Protocol. The peak UDP RTT improvement between absence and presence of human movement is captured at packet size 1152 Bytes for IPv4, with an improvement of 13.51% (0.16 ms for W-MOV; 0.185 ms for MOV), or a 0.025 ms faster rate. At packet size 1408 Bytes, applying IPv6 without human shadowing improves by 11.17% (0.309 ms for W-MOV; 0.349 ms for MOV), or a 0.039 ms faster rate.

In both scenarios, as the packet size increases from 128 to 1408 Bytes, the RTT consistently growing. Human movement has a negative impact on RTT, for TCP and UDP with both IPv4 and IPv6. IPv6 adds extra overhead (40 Bytes); 20 Bytes extra overhead by IPv4 [42], so that using IPv6 results in a longer RTT for both UDP and TCP than IPv4.

7.2.3 Comparison of TCP and UDP RTT

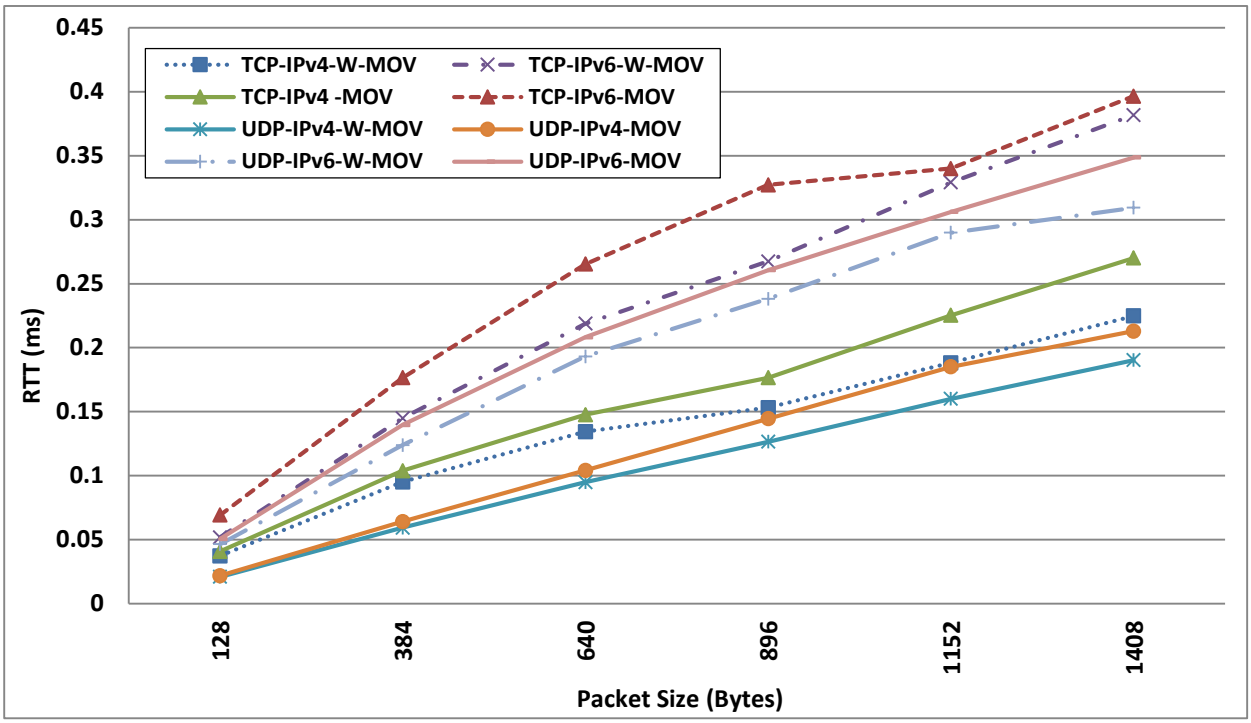

Figure 7.6: Comparison of TCP and UDP RTT for both versions of the Internet Protocol, without human movement vs. human movement

The results showed that UDP with or without human movement achieves a faster RTT than TCP for both versions of the Internet Protocol on all tested packet sizes.

Without human movement, the greatest improvement between UDP and TCP RTT for IPv4 is observed at packet size 640 Bytes, where UDP is lower by 29.85% (0.134 ms for TCP; 0.095 ms for UDP), or a 0.04 ms shorter RTT. For IPv6, the maximum RTT difference between TCP and UDP is at 1408 Bytes with an improvement of 18.85% (0.382 ms for TCP; 0.309 ms for UDP), or a 0.072 ms shorter RTT.

With human movement, the peak difference between UDP and TCP RTT for IPv4 appears at packet size 1408 Bytes, where UDP is lower by 21.11% (0.27 ms for TCP; 0.213 ms for UDP), or a 0.057 ms faster rate. For IPv6, the maximum RTT difference is at 896 Bytes, where UDP outperforms TCP by 20.49% (0.327 ms for TCP; 0.261 ms for UDP).

UDP returns consistently faster results because UDP has a lower overhead (8 Bytes) than TCP (20 Bytes) [39].

7.3 CPU Utilisation Analysis

Figures 7.7 and 7.8 show the CPU utilisation on TCP and UDP protocols for both versions of the Internet Protocol on Windows 8.1 with Windows Server 2012 running over 802.11ac WLANs in the presence of human movement and in non-human shadowing environments. In all scenarios, as the packet size increases, the TCP and UDP CPU utilisation decrease consistently along with them. W-MOV is an abbreviation for without human movement, MOV is an abbreviation for human movement.

7.3.1 Comparison of TCP CPU Utilisation

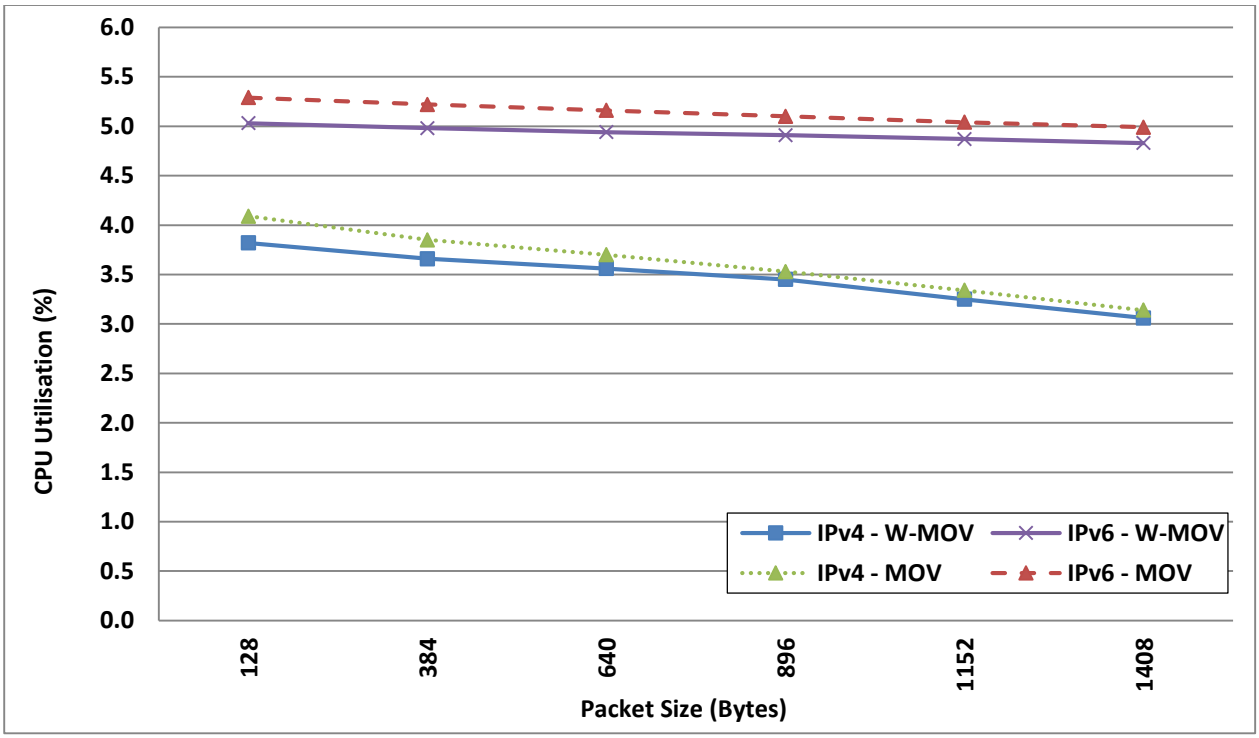

Figure 7.7: Comparison of TCP CPU Utilisation for both versions of the Internet Protocol in 802.11ac WLAN, without human movement vs. human movement

IPv4 consumes less TCP CPU resource than IPv6 on all packet sizes, with or without human movement. Without human movement, the greatest improvement is at packet size 1408 Bytes, where IPv4 is lower by 1.77% (3.06% for IPv4; 4.83% for IPv6). With human movement, the maximum improvement between IPv4 and IPv6 appears at 1408 Bytes, where IPv4 outperforms IPv6 by 1.85% (3.14% for IPv4; 4.99% for IPv6).

Comparing TCP CPU utilisation shows the usage is lower for both versions of the Internet Protocol without human movement. The maximum improvement is observed at packet size 128

Bytes. IPv4 achieves an improvement of 0.27% (3.82% for W-MOV; 4.09% for MOV). A 0.26% lower CPU usage rate is observed for IPv6 (5.03% for W-MOV; 5.29% for MOV).

7.3.2 Comparison of UDP CPU Utilisation

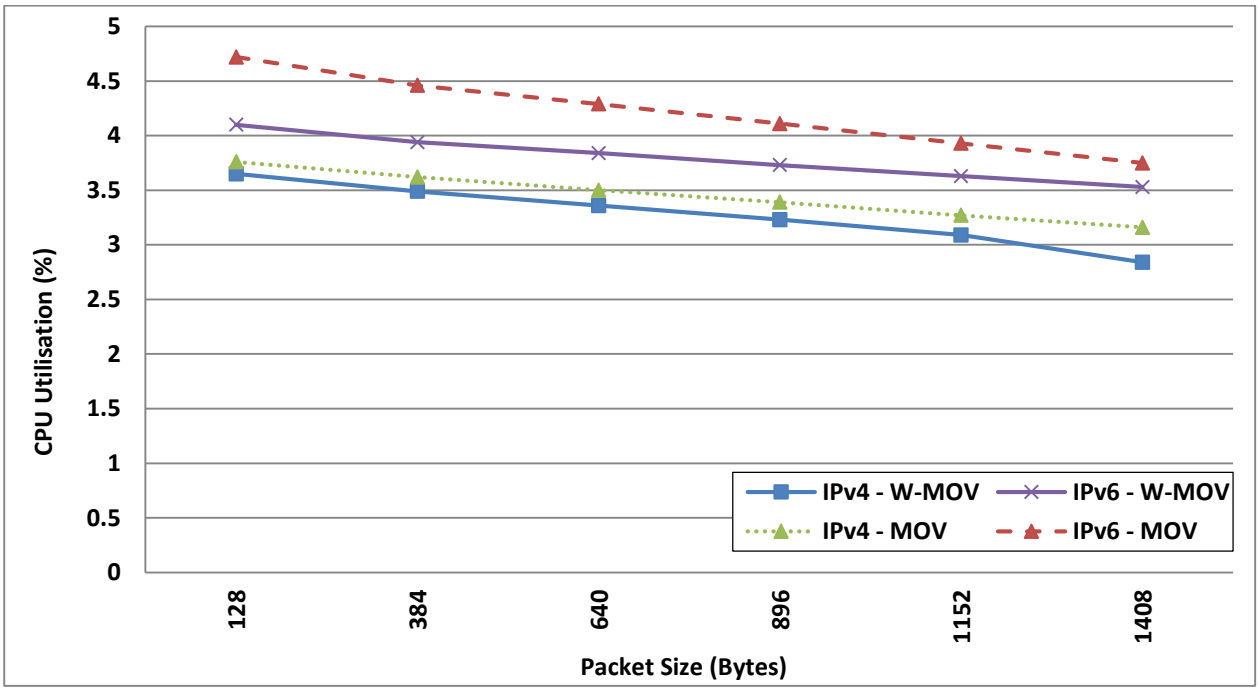

Figure 7.8: Comparison of UDP CPU Utilisation for both versions of the Internet Protocol in 802.11ac WLAN, without human movement vs. human movement

With or without human movement, applying IPv4 consumes less UDP CPU resource than IPv6 on different packet sizes. Without human movement, the greatest improvement between IPv4 and IPv6 appears at packet size 1408 Bytes, with IPv4 consuming 0.69% less (2.84% for IPv4; 3.53% for IPv6). With human movement, the maximum difference is at 128 Bytes, where IPv4 outperform IPv6 by 0.96% (3.76% for IPv4; 4.72% for IPv6).

The results shows that with no human movement, the CPU usage is consistently lower for both versions of the Internet Protocol. The maximum UDP CPU usage improvement is observed at packet size 1408 Bytes for IPv4, with a 0.32% lower CPU utilisation rate (2.84% for W-MOV; 3.16% for MOV). For IPv6, the peak appears at 128 Bytes, achieving a 0.62% lower rate (4.1% for W-MOV; 4.72% for MOV).

In both scenarios, as the packet size increases from 128 to 1408 Bytes, CPU utilisation generally decreases. Human movement has a negative impact on network CPU usage, both using TCP and UDP and for both IPv4 and IPv6. IPv6 adds extra overhead (40 Bytes) compared to 20 Bytes for IPv4 [42], with the result that IPv6 uses more CPU resources for both UDP and TCP than IPv4.

7.3.3 Comparison of TCP and UDP CPU Utilisation

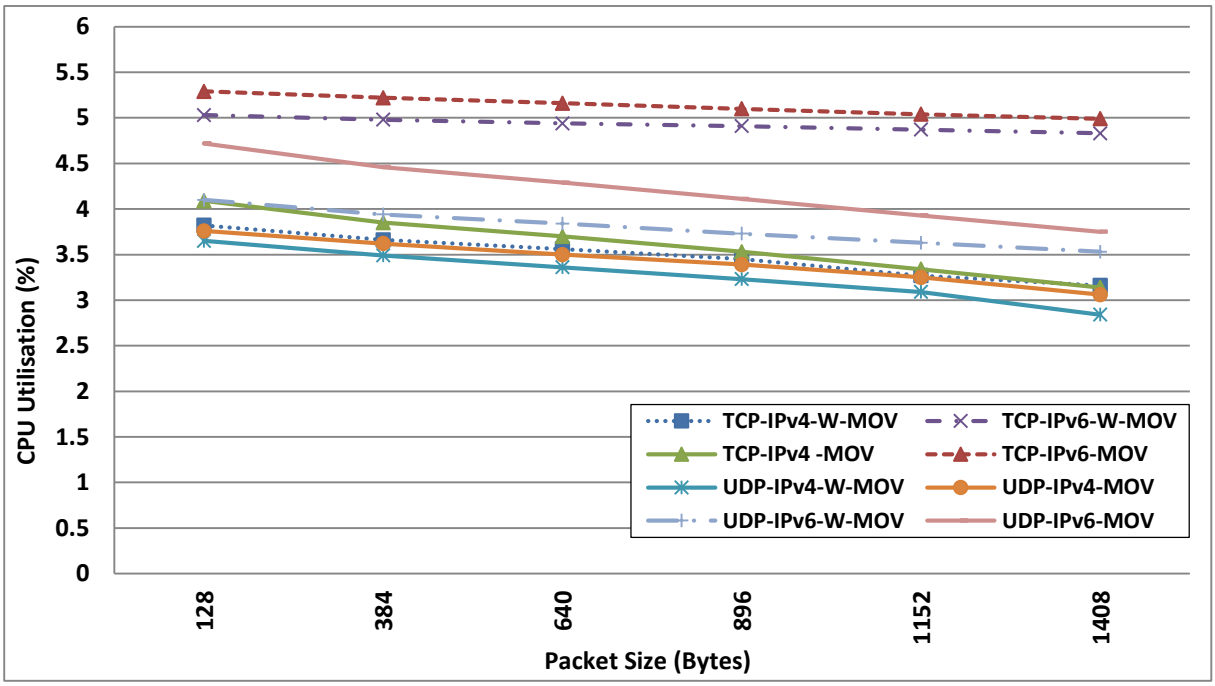

Figure 7.9: Comparison of TCP and UDP CPU Utilisation for both versions of the Internet Protocol, without human movement vs. human movement

The results showed that UDP with or without human movement has a lower CPU usage than TCP for both versions of the Internet Protocol on all tested packet sizes.

In the absence of human movement, the maximum difference between UDP and TCP CPU usage for IPv4 is at packet size 1408 Bytes, where UDP has 0.32% lower CPU usage (3.16% for TCP; 2.84% for UDP). For IPv6, the peak CPU usage difference was also at 1408 Bytes, where UDP outperforms TCP by 1.3% (4.83% for TCP; 3.53% for UDP).

In the presence of human movement, the maximum difference between UDP and TCP for IPv4 is observed at packet size 128 Bytes, where UDP has 0.33% lower CPU usage (4.09% for TCP; 3.76% for UDP). For IPv6, the maximum CPU utilisation difference is at 1408 Bytes, where UDP outperforms TCP by 1.24% (4.99% for TCP; 3.75% for UDP).

UDP has a consistently lower CPU usage because it has a lower overhead (8 Bytes) than the overhead for TCP (20 Bytes) [39].

7.4 Comparison Summary of Throughput, RTT, and CPU Usage

The overall results showed that on average, human movement returned a lower throughput, longer RTT, and higher CPU usage for both TCP and UDP when implementing both versions of the Internet Protocol (IPv4 and IPv6).

Throughput comparison between absence and presence of human movement

On average, the TCP and UDP on WLAN with human movement had a lower throughput than non-human shadowing for both IPv4 and IPv6. For IPv4, the presence of human movement decreased TCP throughput by 12.76% and UDP throughput by 9.66%. For IPv6 with human movement, TCP and UDP throughput reduced about 13.38% and 8.74% respectively.

Throughput comparison between IPv4 and IPv6 with and without human movement

On average, throughput for IPv4 outperformed throughput for IPv6 when implementing TCP and UDP without or with human movement. Without human movement, applying IPv6 decreased TCP throughput by 39.01% and UDP throughput by 47.7% compared to IPv4. With human movement, the TCP throughput for IPv6 dropped by 39.37% whereas UDP throughput for IPv6 decreased by 47.13%

Throughput comparison between TCP and UDP with and without human movement

On average, UDP throughput outperformed TCP throughput when implementing IPv4 and IPv6 with or without human movement. In the absence of human movement, UDP achieved a higher throughput than TCP by 25.74% for IPv4 and 13.40% for IPv6. In the presence of human movement, UDP achieved a higher throughput than TCP by 28.32% for IPv4 and 17.79% for IPv6.

RTT comparison between absence and presence of human movement

On average, the shortest TCP and UDP RTT for both IPv4 and IPv6 were measured in the absence of human of movement. With human movement, TCP RTT increased for IPv4 by 13.62% and UDP RTT by 11.01%. For IPv6 with human movement, TCP and UDP RTT rose about 11.5% and 8.6% respectively.

RTT comparison between IPv4 and IPv6 with and without human movement

On average, RTT for IPv4 outperformed RTT for IPv6 when implementing TCP and UDP without or with human movement. For IPv6 without human movement, TCP had a longer RTT than IPv4 by 40.25% and UDP by 45.73%. With human movement, the TCP and UDP for IPv6 have a longer RTT than IPv4 by 38.79% and 44.26% respectively.

RTT comparison between TCP and UDP with and without human movement

On average, RTT for UDP outperformed RTT for TCP by implementing IPv4 and IPv6 with or without human movement. In the absence of human movement, UDP achieved a shorter RTT than TCP by 21.75% for IPv4 and 13.85% for IPv6. In the presence of human movement, UDP provided a faster RTT than TCP by 24.04% for IPv4 and 16.59% for IPv6.

CPU utilisation comparison between absence and presence of human movement

On average, the lowest TCP and UDP CPU usage for both IPv4 and IPv6 were measured in the absence of human of movement. The presence of human movement increased TCP and UDP CPU usage for IPv4 by 0.14% and 0.17% respectively compared to IPv4 in the absence of human shadowing. For IPv6 with human movement, TCP and UDP CPU usage increased by 0.2% and 0.41% respectively compared to IPv6 without human shadowing.

CPU utilisation comparison between IPv4 and IPv6 with and without human movement

On average, CPU usage for IPv4 outperformed CPU usage for IPv6 by implementing TCP and UDP without or with human movement. In non-human shadowing, IPv6 had higher CPU usage than IPv4 by 1.45% for TCP and 0.52% for UDP. In the presence of human movement, IPv6 had higher CPU usage than IPv4 by 1.52% for TCP and 0.76% for UDP.

CPU utilisation comparison between TCP and UDP with and without human movement

On average, CPU usage for UDP outperformed CPU usage for TCP when implementing IPv4 and IPv6 without or with human movement. In the absence of human movement, UDP achieved a lower CPU usage than TCP by 0.21% for IPv4 and 1.13% for IPv6. In the presence of human movement, UDP achieved a lower CPU usage than TCP by 0.18% for IPv4 and 0.92% for IPv6.

7.5 Chapter Summary

In this chapter, it was demonstrated that with human movement, there was a negative impact on the throughput, RTT and CPU usage over 802.11ac WLANs. Both TCP and UDP had the

shortest RTT and lowest CPU usage and highest throughput with non-human shadowing for both versions of the Internet Protocol. Moreover, implementing IPv6 had the lowest throughput and longest RTT and highest CPU usage compared with IPv4 for both TCP and UDP. Also, applying UDP outperformed TCP for both versions of the Internet Protocol. The results showed that on average, the highest throughput (547.17 Mbps), shortest RTT (0.109 ms) and lowest CPU usage (3.277%) were measured in the absence of human movement and implemented IPv4 for the UDP protocol, whereas the lowest throughput (214.67 Mbps), longest RTT (0.263 ms) and highest CPU usage (5.13%) were measured in the presence of human movement and implemented IPv6 for the TCP protocol.

The next chapter provides the details of evaluating the effect of shadowing on 802.11ac WLAN in laboratory environment.

CHAPTER 8

EFFECT OF SHADOWING ON 802.11ac WLAN IN LABORATORY ENVIRONMENT

In this chapter, the data gathered from the third experimental scenario is analysed. The purpose of the analysis is to evaluate the impact of shadowing (walls) and distance on the performance of 802.11ac WLANs in an obstructed environment. TCP and UDP protocols are tested by conducting comparisons on data sent between a client PC placed in test locations lab 2001, lab 2003, and lab 2005 (later abbreviated to LAB001, LAB003, and LAB005) and an access point in one location (lab 2010) during all tests (Figure 5.6). Section 4.3.2, section 5.2, and section 5.2.3 described in detail the experimental data gathering process and experimental design for this scenario. Section 8.1 covers the throughput analysis. The round trip time analysis is discussed in section 8.2. Section 8.3 shows the CPU Utilisation analysis. Section 8.4 shows comparison summary of the three metrics. Section 8.5 summarises the scenario outcomes.

8.1 Throughput Analysis

Figures 8.1 and 8.2 show the TCP and UDP throughput for both versions of the Internet Protocol on Windows 8.1 with Windows Server 2012 running over 802.11ac WLANs, in environments where the PC client and server are placed as described at the start of this chapter. To perform this experiment, traffic was generated from the PC client (Windows 8.1) to the server (Windows Server 2012). In all scenarios, as the packet size increased, the throughput of TCP and UDP also increased consistently.

8.1.1 Comparison of TCP throughput

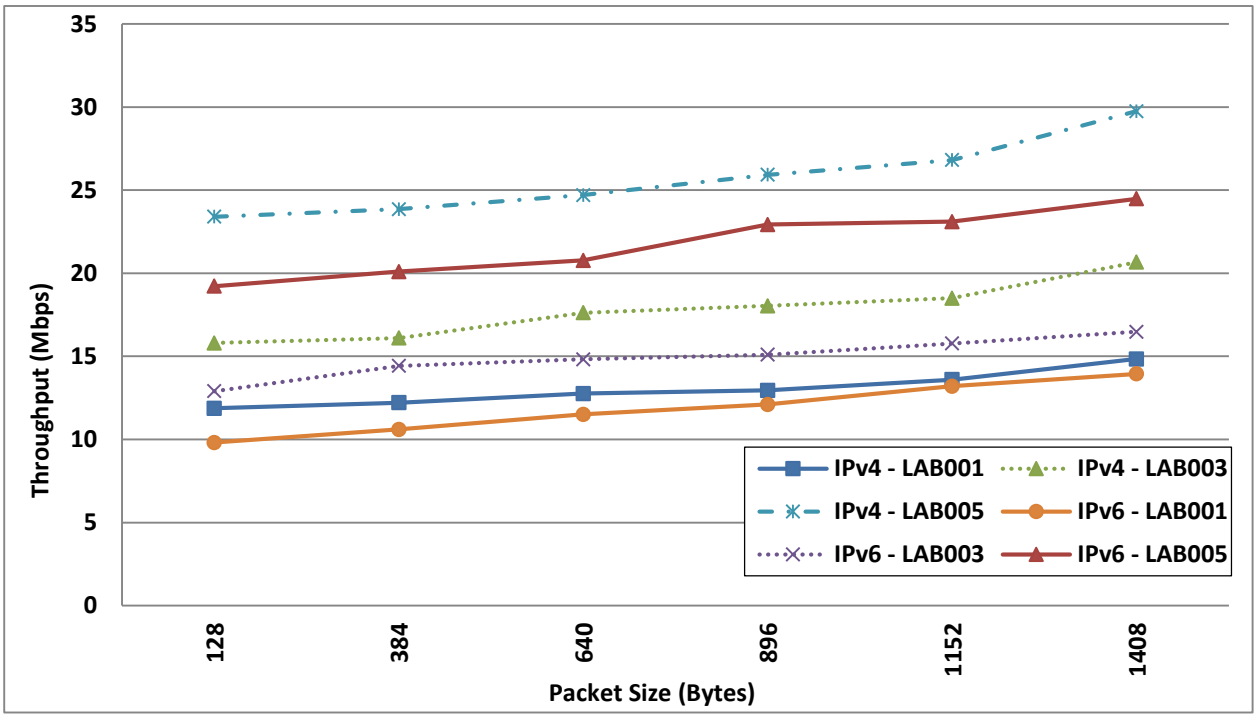

Figure 8.1: Comparison of TCP throughput for both versions of the Internet Protocol in 802.11ac WLAN, LAB005 vs. LAB003, LAB005 vs. LAB001, and LAB003 vs. LAB001

At all three lab locations, IPv4 performs better than IPv6 for TCP throughput for all tested packet sizes. For LAB005, the highest TCP throughput variation is observed at packet size 1408 Bytes, where IPv4 outperforms IPv6 by 17.71% (29.75 Mbps for IPv4; 24.48 Mbps for IPv6), or a throughput higher by 5.27 Mbps. At LAB003, the maximum difference was also at 1408 Bytes, with IPv4 results higher by 20.27% (20.67 Mbps for IPv4; 16.48 Mbps for IPv6), or by 4.19 Mbps. At LAB001, the highest variation appears at 128 Bytes, where IPv4 outperforms IPv6 by 17.35% (11.87 Mbps for IPv4; 9.81 Mbps for IPv6), or higher by 2.06 Mbps.

Comparing the three locations, running 802.11ac WLAN in LAB005 provides a higher TCP throughput than LAB003, which in turn is higher than LAB001. The maximum difference between LAB005 and LAB003 is captured at packet size 1408 Bytes for both versions of the Internet Protocol: IPv4 in the LAB005 results in an 30.52% increase (29.75 Mbps for IPv4 LAB005; 20.67 Mbps for IPv4 LAB003), or 9.08 Mbps higher throughput, and IPv6 LAB005 is higher by 32.68% (24.48 Mbps for IPv6 LAB005; 16.48 Mbps for IPv6 LAB003), or 3.06 Mbps higher.

Between LAB005 and LAB001, the maximum difference in TCP throughput appears at packet size 1408 Bytes for IPv4 and 896 Bytes for IPv6. IPv4 in the LAB005 outperforms LAB001 by 50.12% (29.75 Mbps for IPv4 LAB005; 14.84 Mbps for IPv4 LAB001), or higher by 14.91 Mbps.

IPv6 LAB005 achieves an increase of 47.23% (22.93 Mbps for IPv6 LAB005; 12.1 Mbps for IPv6 LAB001), or 10.83 Mbps higher throughput.

The maximum improvement between LAB003 and LAB001 is at packet size 1408 Bytes for IPv4 and 384 Bytes for IPv6. At its peak, IPv4 in the LAB003 increases throughput by 28.21% (20.67 Mbps for IPv4 LAB003; 14.84 Mbps for IPv4 LAB001), or higher by 5.83 Mbps. IPv6 LAB003 is higher by 26.54% (14.43 Mbps for IPv6 LAB003; 10.6 Mbps for IPv6 LAB001), or by 3.83 Mbps.

8.1.2 Comparison of UDP throughput

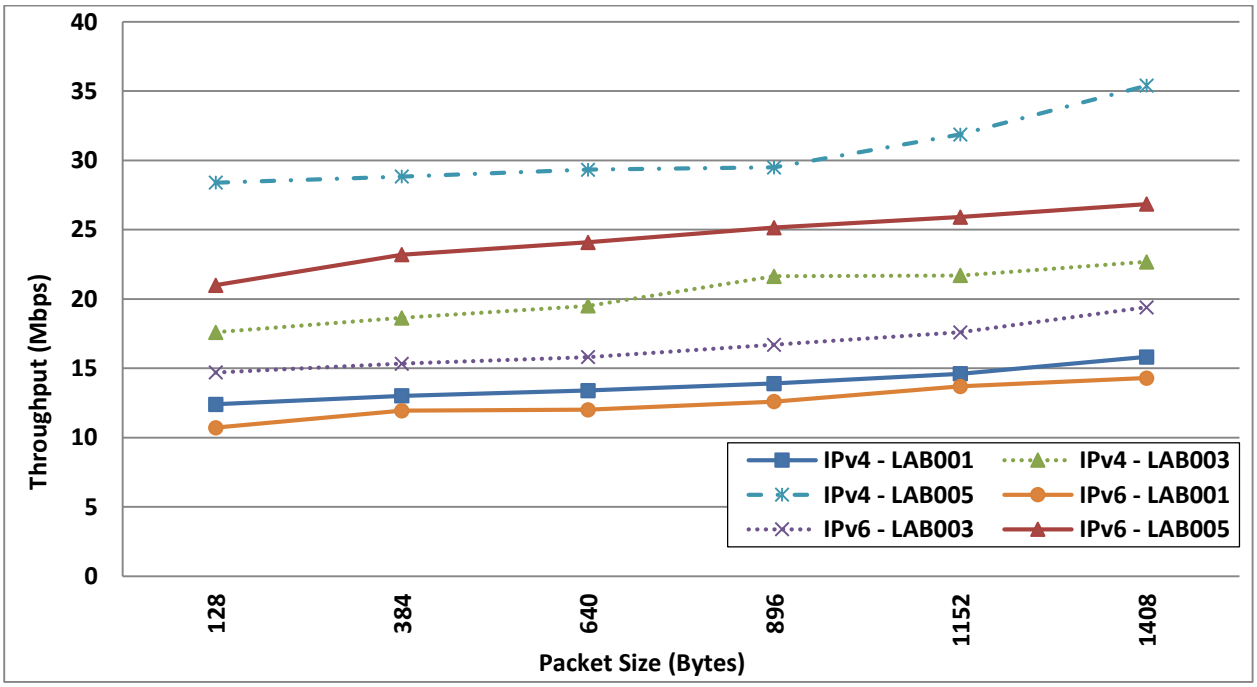

Figure 8.2: Comparison of UDP throughput for both versions of the Internet Protocol in 802.11ac WLAN, LAB005 vs. LAB003, LAB005 vs. LAB001, and LAB003 vs. LAB001

At all three locations, IPv4 performs better than IPv6 for UDP throughput for all tested packet sizes, with the maximum variation appearing at packet size 1408 Bytes. At LAB005, IPv4 increases throughput by 24.15% (35.4 Mbps for IPv4; 26.85 Mbps for IPv6), or an increase of 8.55 Mbps. At LAB003, the greatest improvement is at 896 Bytes, where IPv4 outperforms IPv6 by 22.83% (21.64 Mbps for IPv4; 16.70 Mbps for IPv6), or higher by 4.94 Mbps. At LAB001, the peak is observed at 128 Bytes, with an increase for IPv4 of 13.63% (12.40 Mbps for IPv4; 10.71 Mbps for IPv6), or 1.69 Mbps higher throughput.

Among the locations, running this WLAN in LAB005 delivers the best UDP throughput, then LAB003, and last LAB001. Between LAB005 and LAB003, the greatest increase appears at packet size 1408 Bytes for IPv4 and 896 Bytes for IPv6. Applying IPv4 in the LAB005 results

in a peak 35.93% increase (35.4 Mbps for IPv4 LAB005; 22.68 Mbps for IPv4 LAB003), or higher by 12.72 Mbps. IPv6 LAB005 outperforms LAB003 by 33.6% (25.15 Mbps for IPv6 LAB005; 16.7 Mbps for IPv6 LAB003), or 8.45 Mbps higher throughput.

Between LAB005 and LAB001, the highest improvement is observed at packet size 1408 Bytes for both versions of the Internet Protocol. Using IPv4 in the LAB005 increases throughput by 55.31% (35.4 Mbps for IPv4 LAB005; 15.82 Mbps for IPv4 LAB001), or a 19.58 Mbps increase. At peak, IPv6 LAB005 outperforms LAB001 by 46.74% (26.85 Mbps for IPv6 LAB005; 14.3 Mbps for IPv6 LAB001), or higher by 12.55 Mbps.

The greatest improvement between LAB003 and LAB001 is captured at packet size 896 Bytes for IPv4 and 1408 Bytes for IPv6. IPv4 in LAB003 outperforms LAB001 by 35.77% (21.64 Mbps for IPv4 LAB003; 13.9 Mbps for IPv4 LAB001), or 7.74 Mbps higher throughput. IPv6 LAB003 also increases output by 26.29% (19.4 Mbps for IPv6 LAB003; 14.3 Mbps for IPv6 LAB001), or 5.1 Mbps higher.

LAB005 has a superior throughput compared to the other two lab locations because of the number of obstructions and distance between the access point and client PC. In addition, IPv6 adds extra overhead in its header size (40 Bytes) compared to 20 Bytes extra overhead by IPv4 [42], and therefore applying IPv6 provides lower throughput for both UDP and TCP than applying IPv4.

8.1.3 Comparison of TCP and UDP throughput

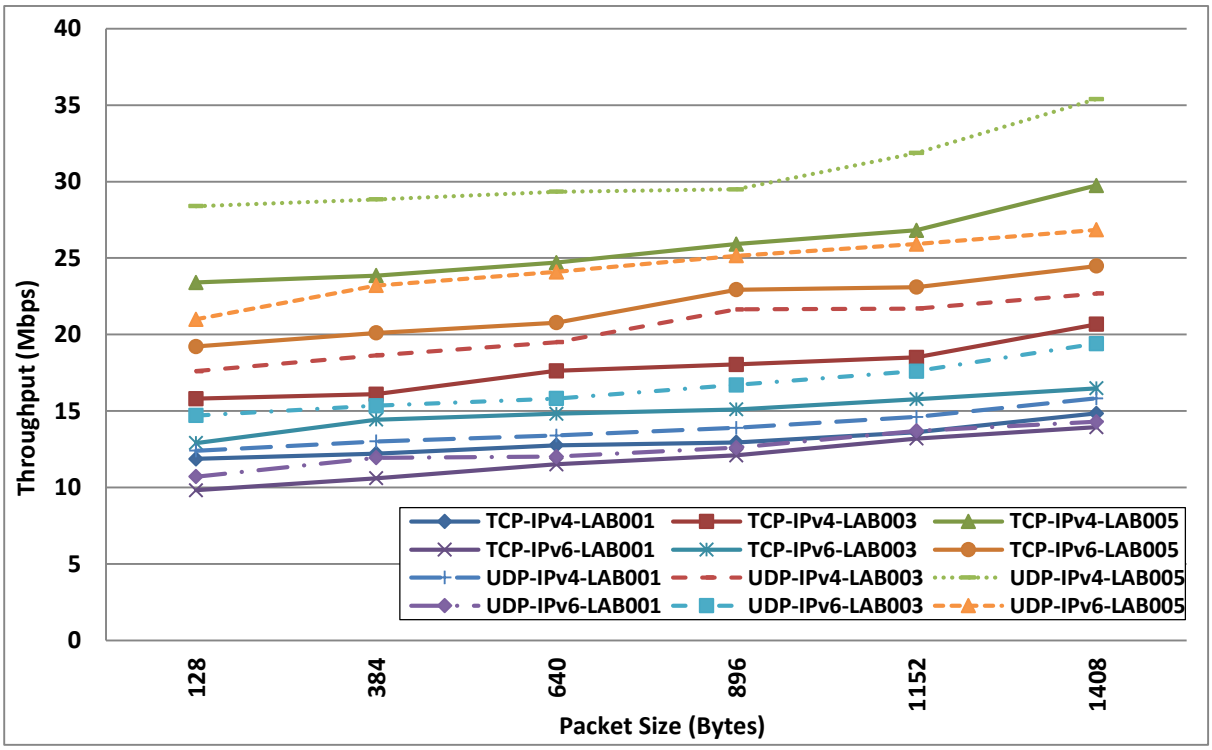

Figure 8.3: Comparison of TCP and UDP throughput for both versions of the Internet Protocol on LAB005, LAB003, and LAB001

At all three labs, UDP outperforms TCP for both IPv4 and IPv6 on all the tested packet sizes. For LAB005 with IPv4, the highest variation is observed at packet size 1408 Bytes, where UDP shows an increase of 15.96% (29.75 Mbps for TCP; 35.4 Mbps for UDP), or higher by 5.65 Mbps. For IPv6, UDP increases throughput by 13.78% (20.77 Mbps using TCP; 24.09 Mbps using UDP) at packet size 640 Bytes, a 3.32 Mbps increase.

At LAB003 with IPv4, the highest throughput variation is at 896 Bytes, with UDP providing 16.64% higher values (18.04 Mbps for TCP; 21.64 Mbps for UDP), or a 3.6 Mbps higher throughput. At 1408 Bytes, UDP for IPv6 performs15.05% better (16.48 Mbps using TCP; 19.4 Mbps using UDP), or 2.29 Mbps higher.

At LAB001 for IP4, the highest throughput variation between UDP and TCP is at 1152 Bytes, with UDP giving a throughput 6.91% higher (13.6 Mbps for TCP; 14.61 Mbps for UDP), or higher by 1.01 Mbps. For IPv6, at 384 Bytes, UDP increases throughput by 11.22% (10.6 Mbps for TCP; 11.94 Mbps for UDP) or higher by 1.34 Mbps.

UDP's faster results are due to its lower overhead (8 Bytes) compared to TCP (20 Bytes) [39].

8.2 Round Trip Time (RTT) Analysis

Figures 8.4 and 8.5 show the TCP and UDP RTT for IPv4 and IPv6 on Windows 8.1 with Windows Server 2012 running over 802.11ac WLANs, in environments where the PC client and the server are placed as described at the start of this chapter. To perform this experiment, traffic was generated from the PC client (Windows 8.1) to the server (Windows Server 2012). In all scenarios, as the packet size increases, the RTT of TCP and UDP increase consistently along with them.

8.2.1 Comparison of TCP RTT

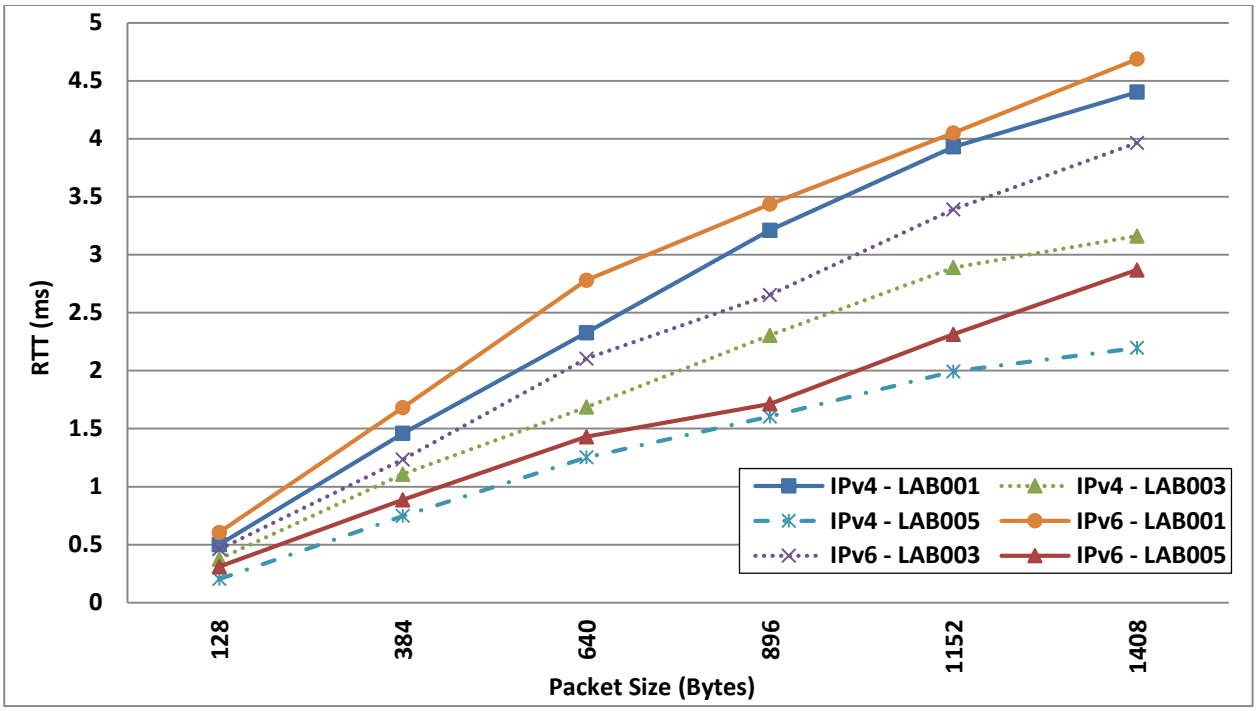

Figure 8.4: Comparison of TCP RTT for both versions of the Internet Protocol in 802.11ac WLAN, LAB005 vs. LAB003, LAB005 vs. LAB001, and LAB003 vs. LAB001

At all three locations, IPv4 outperforms IPv6 on all packet sizes tested for TCP RTT. For LAB005, the highest variation appears at 1408 Bytes, where IPv4 outperforms IPv6 by 23.34% (2.2 ms for IPv4; 2.87 ms for IPv6), or faster by 0.67 ms. At LAB003, the maximum difference is also at 1408 Bytes, where IPv4 is shorter by 20.2% (3.16 ms for IPv4; 3.96 ms for IPv6), or 0.8 ms faster RTT. At LAB001, the highest TCP RTT variation is at 640 Bytes, where IPv4 outperforms IPv6 by 16.19% (2.33 ms for IPv6; 2.78 ms for IPv6), or 0.45 ms faster.

Among the locations, running the WLAN in LAB005 provides the best TCP RTT, then LAB003, and last LAB001.

The maximum difference in TCP RTT between LAB005 and LAB003 is captured at packet size 1408 Bytes for both versions of the Internet Protocol. For IPv4, LAB005 outperforms LAB003 by 30.38% (2.2 ms for IPv4 LAB005; 3.16 ms for IPv4 LAB003), or an RTT rate 0.96 ms lower. For IPv6, LAB005 outperforms LAB003 by 27.78% (2.87 ms for IPv6 LAB005; 3.96 ms for IPv6 LAB003), or a 1.09 ms lower rate.

The maximum improvement between LAB005 and LAB001 appears at packet size 1408 Bytes for both IPv4 and IPv6. IPv4 in the LAB005 results in a variation of 50.22% over LAB001 (2.2 ms for IPv4 LAB005; 4.4 ms for IPv4 LAB001), or faster by 2.21 ms. IPv6 LAB005 is shorter than IPv6 LAB001 by 38.81% (2.87 ms for IPv6 LAB005; 4.69 ms for IPv6 LAB001), or 1.82 ms faster.

The maximum difference in TCP RTT between LAB003 and LAB001 is at packet size 1408 Bytes for IPv4 and 896 Bytes for IPv6. IPv4 at LAB003 is shorter than LAB001 by 28.18% (3.16 ms for IPv4 LAB003; 4.4 ms for IPv4 LAB001), or 1.24 ms faster RTT. IPv6 LAB003 outperforms IPv6 LAB001 by 22.67% (2.65 ms for IPv6 LAB003; 3.44 ms for IPv6 LAB001), or lower by 0.78 ms.

The results showed that that the client PC at the LAB005 location achieves a fastest TCP RTT for both IPv4 and IPv6 compared to LAB003 and LAB001.

8.2.2 Comparison of UDP RTT

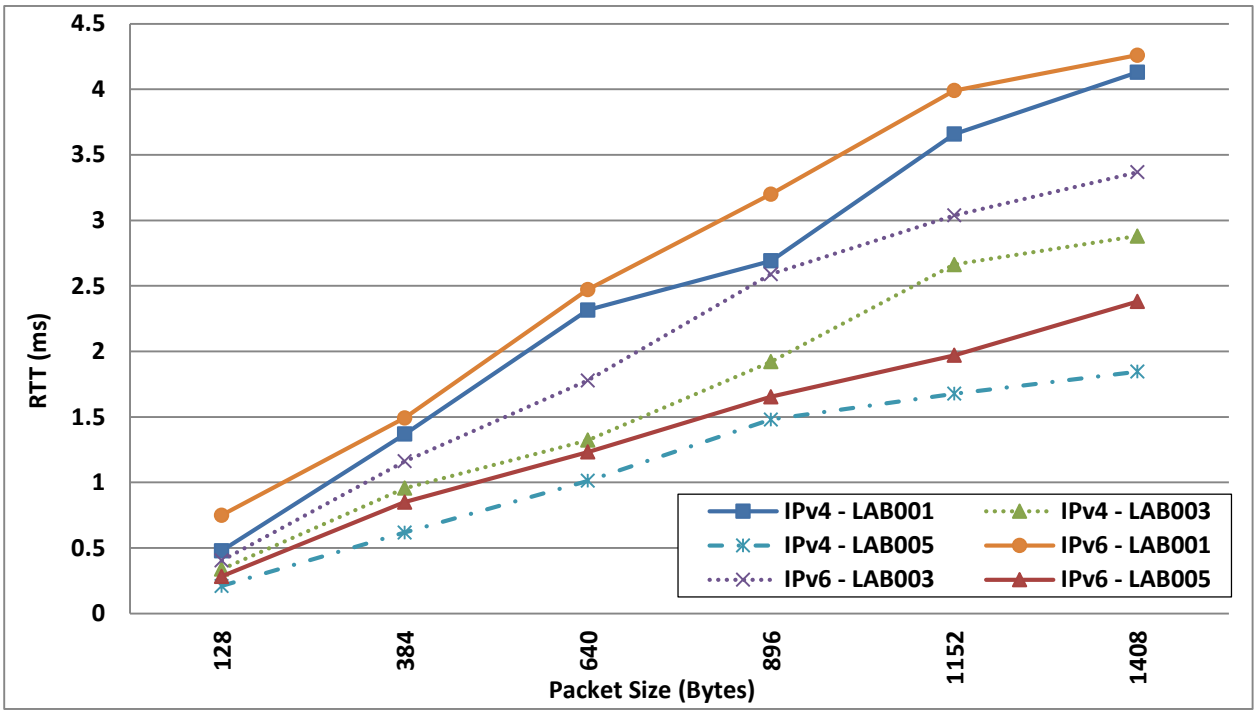

Figure 8.5: Comparison of UDP RTT for both versions of the Internet Protocol in 802.11ac WLAN, LAB005 vs. LAB003, LAB005 vs. LAB001, and LAB003 vs. LAB001

At the three lab locations, IPv4 performs better than IPv6 on different packet sizes. For LAB005, the highest UDP RTT variation is observed at packet size 1408 Bytes, where IPv4 outperforms IPv6 by 22.27% (1.85 ms for IPv4; 2.38 ms for IPv6), achieving an RTT rate 0.53 ms lower. At LAB003, the maximum difference in RTT was at 896 Bytes, with an improvement for IPv4 by 25.87% (1.92 ms for IPv4; 2.59 ms for IPv6), or faster by 0.67 ms. At LAB001, the greatest variation is at 896 Bytes, where IPv4 outperforms IPv6 by 15.94% (2.69 ms for IPv4; 3.2 ms for IPv6), an RTT rate lower by 0.51 ms.

Comparing the locations, running 802.11ac WLAN in LAB005 outperforms LAB003 which in turn was faster than LAB001 for UDP RTT. The maximum difference between LAB005 and LAB003 is observed at packet size 1408 Bytes for IPv4 and 1152 Bytes for IPv6. IPv4 in the LAB005 outperforms LAB003 by 48.61% (1.85 ms for IPv4 LAB005; 2.88 ms for IPv4 LAB003), or lower by 1.04 ms. IPv6 LAB005 returns a 35.2% faster rate than LAB003 (1.97 ms for IPv6 LAB005; 3.04 ms for IPv6 LAB003), or a 1.07 ms lower RTT rate .

The maximum difference between LAB005 and LAB001 is at 1408 Bytes for IPv4 and 1152 Bytes for IPv6. IPv4 in the LAB005 achieves an improvement of 55.21% over LAB001 (1.85 ms for IPv4 LAB005; 4.13 ms for IPv4 LAB001), or lower by 2.28 ms. For IPv6, LAB005 returns

50.63% faster results (1.97 ms for IPv6 LAB005; 3.99 ms for IPv6 LAB001), or a 2.02 ms lower rate.

The greatest improvement in UDP RTT between LAB003 and LAB001 is at 1408 Bytes for IPv4 and 1152 Bytes for IPv6. IPv4 in the LAB003 provides an improvement of 30.27% (2.88 ms for IPv4 LAB003; 4.13 ms for IPv4 LAB001), or lower by 1.25 ms. IPv6 LAB003 outperforms IPv6 LAB001 by 23.81% (3.04 ms for IPv6 LAB003; 3.99 ms for IPv6 LAB001), or a 0.95 ms lower RTT rate.

The round trip time consistently growing as the packet size increases from 128 to 1408 Bytes for both scenarios. Increasing the number of obstructions and distance between the access point and client PC have a negative impact on the WLAN round trip time. TCP and UDP for RTT performs better in LAB005 than LAB003 and LAB001 for both IPv4 and IPv6.

8.2.3 Comparison of TCP and UDP RTT

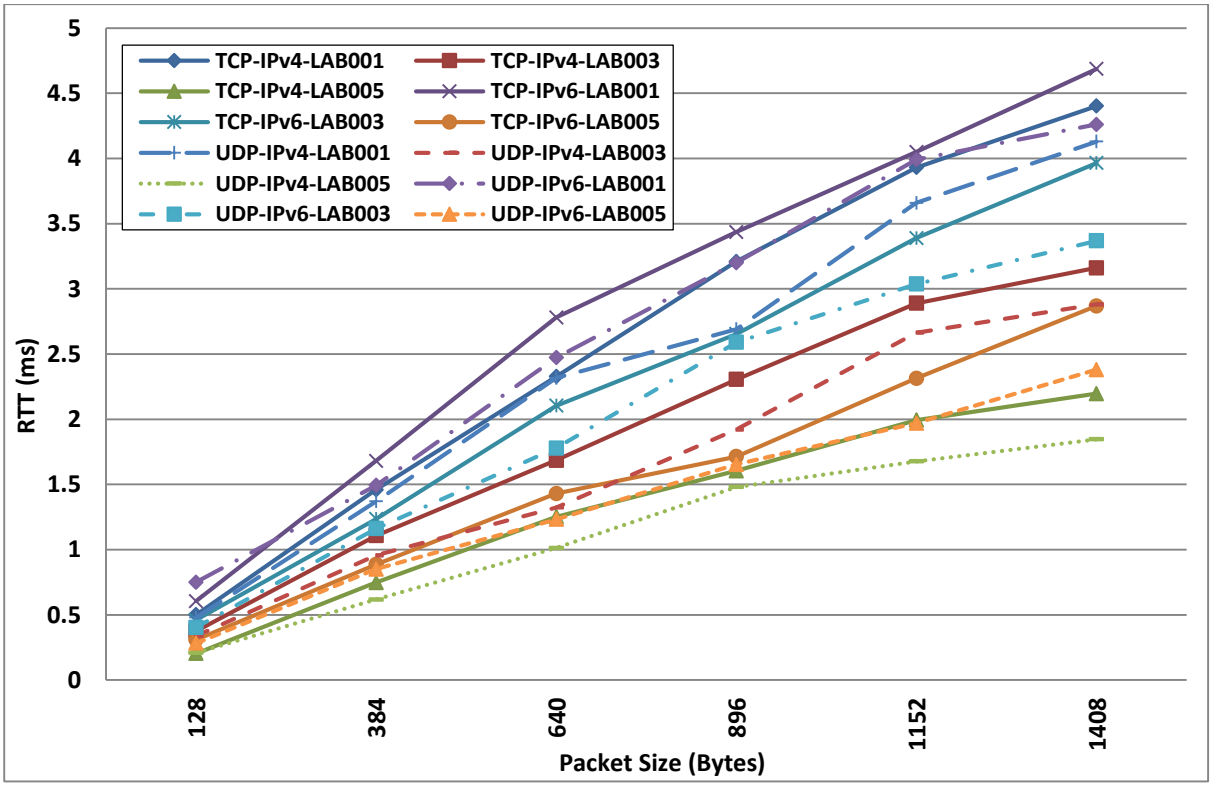

Figure 8.6: Comparison of TCP and UDP RTT for both versions of the Internet Protocol on LAB005, LAB003, and LAB001

At all locations, TCP has a longer RTT than UDP in almost all packet sizes for both versions of the Internet Protocol. For LAB005, the greatest improvement for IPv4 is observed at packet size 1408 Bytes, where UDP is faster by 15.91% (2.196 ms for TCP IPv4; 1.846 ms for UDP

IPv4), or by 0.35 ms. For IPv6, also at 1408 Bytes, UDP decreases RTT by 17.07% (from 2.869 ms by using TCP to 2.38 ms by using UDP), an RTT of 0.489 ms lower.

At LAB003, the highest RTT variation between UDP and TCP for IPv4 is at packet size 896 Bytes. UDP returns a lower RTT by 16.52% (2.305 ms for TCP IPv4; 1.921 ms for UDP IPv4). At packet size 1408 Bytes, UDP for IPv6 is shorter by 15.15% (3.964 ms for TCP IPv4; 3.368 ms for UDP IPv4) or 0.597 ms faster.

At LAB001, the greatest RTT improvement between UDP and TCP for IPv4 is at 896 Bytes. UDP outperforms TCP by 16.2% (3.21 ms for TCP IPv4; 2.691 ms for UDP IPv4). At packet size 1408 Bytes, UDP for IPv6 is faster by 9.17% (4.687 ms for TCP IPv4; 4.26 ms for UDP IPv4) or 0.427 ms decreased RTT.

The results showed that UDP has greater RTT than TCP for both versions of the Internet Protocol on all packet sizes. The reason for this is that UDP has a lower overhead (8 Bytes) than TCP (20 Bytes) [39].

8.3 CPU Utilisation Analysis

Figures 8.7 and 8.8 show the CPU utilisation on TCP and UDP protocols for both IPv4 and IPv6 on Windows 8.1 with Windows Server 2012 running over 802.11ac WLANs, in environments where the PC client and the server are placed as described at the start of this chapter. To perform this experiment, traffic was generated from the PC client (Windows 8.1) to the server (Windows Server 2012). In all scenarios, as the packet size increases, the TCP and UDP CPU utilisation decrease consistently along with them.

8.3.1 Comparison of TCP CPU Utilisation

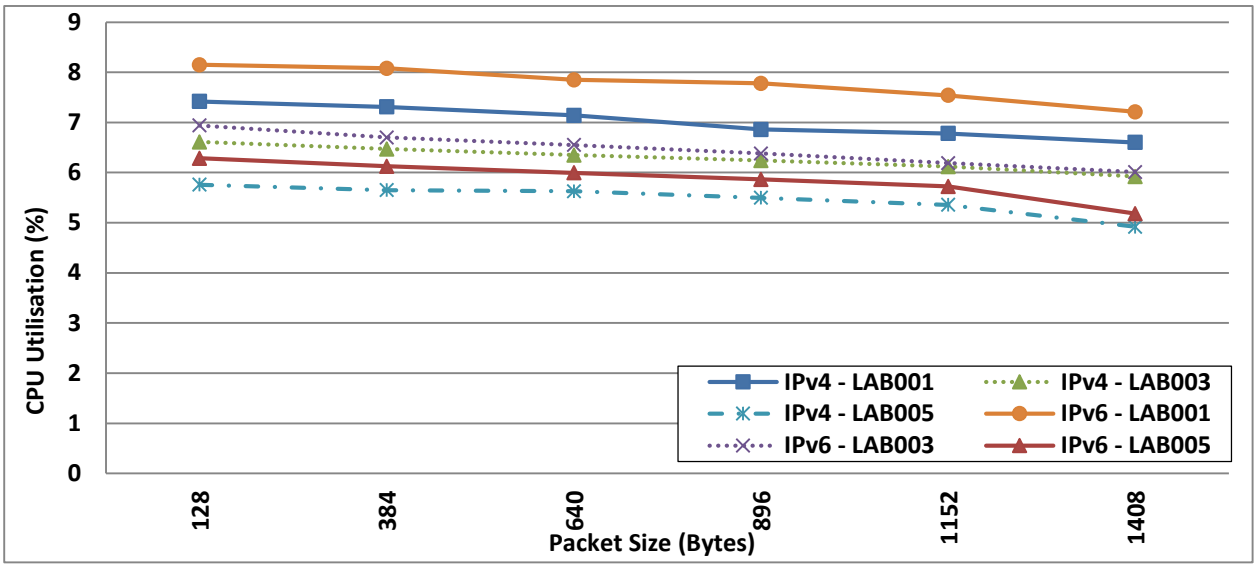

Figure 8.7: Comparison of TCP CPU Utilisation for both versions of the Internet Protocol in 802.11ac WLAN, LAB005 vs. LAB003, LAB005 vs. LAB001, and LAB003 vs. LAB001

At all lab locations, IPv4 outperforms IPv6 for TCP CPU utilisation on all tested packet sizes. At LAB005, the highest variation is observed at packet size 128 Bytes, with IPv4 lower by 0.53% (5.76% for IPv4; 6.29% for IPv6). At LAB003, the maximum improvement appears at 128 Bytes, where IPv4 is lower by 0.33% (6.61% for IPv4; 6.94% for IPv6). For LAB001, the peak improvement is at 896 Bytes, where IPv4 outperforms IPv6 by 0.92% (6.86% for IPv4; 7.78% for IPv6).

Comparing all locations, running 802.11ac WLAN in LAB005 results in lower CPU usage for TCP than LAB003, and the highest usage is in LAB001. Between LAB005 and LAB003, the highest improvement is captured at packet size 1408 Bytes for both versions of the Internet Protocol. IPv4 in the LAB005 is reduced the CPU usage by 1% (4.92% for IPv4 LAB005; 5.92% for IPv4 LAB003). IPv6 LAB005 is lower by 0.83% (5.18% for IPv6 LAB005; 6.01% for IPv6 LAB003).

The greatest improvement in TCP CPU utilisation between LAB005 and LAB001 is at 1408 Bytes for both versions of Internet Protocol. Applying IPv4 in the LAB005 results in a 1.68% improvement (4.92% for IPv4 LAB005; 6.6% for IPv4 LAB001). IPv6 LAB005 outperforms IPv6 LAB001 by 2.03% (5.18% for IPv6 LAB005; 7.21% for IPv6 LAB001).

Between LAB003 and LAB001, the maximum difference in CPU utilisation for TCP appears at packet size 384 Bytes for IPv4 and 896 Bytes for IPv6. For IPv4, LAB003 outperforms LAB001

by 0.84% (6.47% for IPv4 LAB003; 7.31% for IPv4 LAB001). At IPv6, LAB003 is lower than LAB001 by 1.4% (6.38% for IPv6 LAB003; 7.78% for IPv6 LAB001).

8.3.2 Comparison of UDP CPU Utilisation

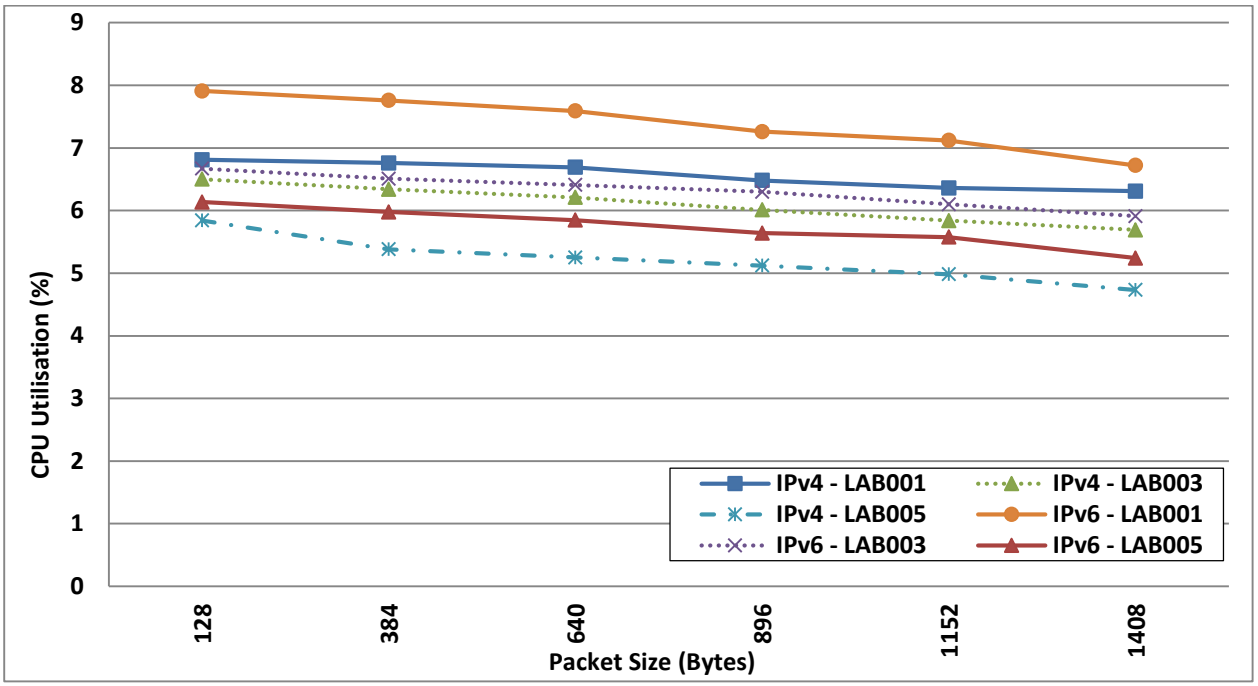

Figure 8.8: Comparison of UDP CPU Utilisation for both versions of the Internet Protocol in 802.11ac WLAN, LAB005 vs. LAB003, LAB005 vs. LAB001, and LAB003 vs. LAB001

At all locations, IPv4 outperforms IPv6 for UDP CPU utilisation on all packet sizes tested. For LAB005, the highest variation is observed at packet size 1152 Bytes, where IPv4 is lower by 0.59% (4.98% for IPv4; 5.58% for IPv6). At LAB003, the maximum difference is at 896 Bytes, where IPv4 outperforms IPv6 by 0.29% (6.01% for IPv4; 6.3% for IPv6). At LAB001, the greatest improvement is at 128 Bytes, where IPv4 is lower by 1.1% (6.81% for IPv4; 7.91% for IPv6).

Among the locations, running 802.11ac WLAN in LAB005 results in lower CPU usage for UDP than in LAB003, with the highest being LAB001. The maximum difference between LAB005 and LAB003 is captured at packet size 1408 Bytes for both versions of the Internet Protocol. IPv4 in the LAB005 outperforms IPv4 in the LAB003 by 0.96% (4.73% for IPv4 LAB005; 5.69% for IPv4 LAB003). IPv6 LAB005 is lower by 0.67% (5.24% for IPv6 LAB005; 5.91% for IPv6 LAB003).

Between LAB005 and LAB001, the maximum difference in UDP CPU utilisation appears at 384 Bytes for IPv4 and 1408 Bytes for IPv6. For IPv4, LAB005 outperforms LAB001 by 1.58%

(4.73% for IPv4 LAB005; 6.31% for IPv4 LAB001). For IPv6, LAB005 is lower by 1.78% (5.98% for IPv6 LAB005; 7.76% for IPv6 LAB001).

The greatest improvement in CPU utilisation for UDP between LAB003 and LAB001 is at packet size 1408 Bytes for IPv4 and 384 Bytes for IPv6. With IPv4, LAB003 consumed less 0.62% (5.69% for IPv4 LAB003; 6.31% for IPv4 LAB001. For IPv6, LAB003 outperforms LAB001 by 1.25% (6.51% for IPv6 LAB003; 7.76% for IPv6 LAB001).

In both scenarios, as the packet size increases from 128 to 1408 Bytes, the CPU utilisation generally decreases. Increasing the number of obstructions and distance between the access point and client PC have a negative impact on the WLAN CPU usage. CPU usage for TCP and UDP performs better in LAB005 than either LAB003 or LAB001 for both versions of the Internet Protocol.

8.3.3 Comparison of TCP and UDP CPU utilisation

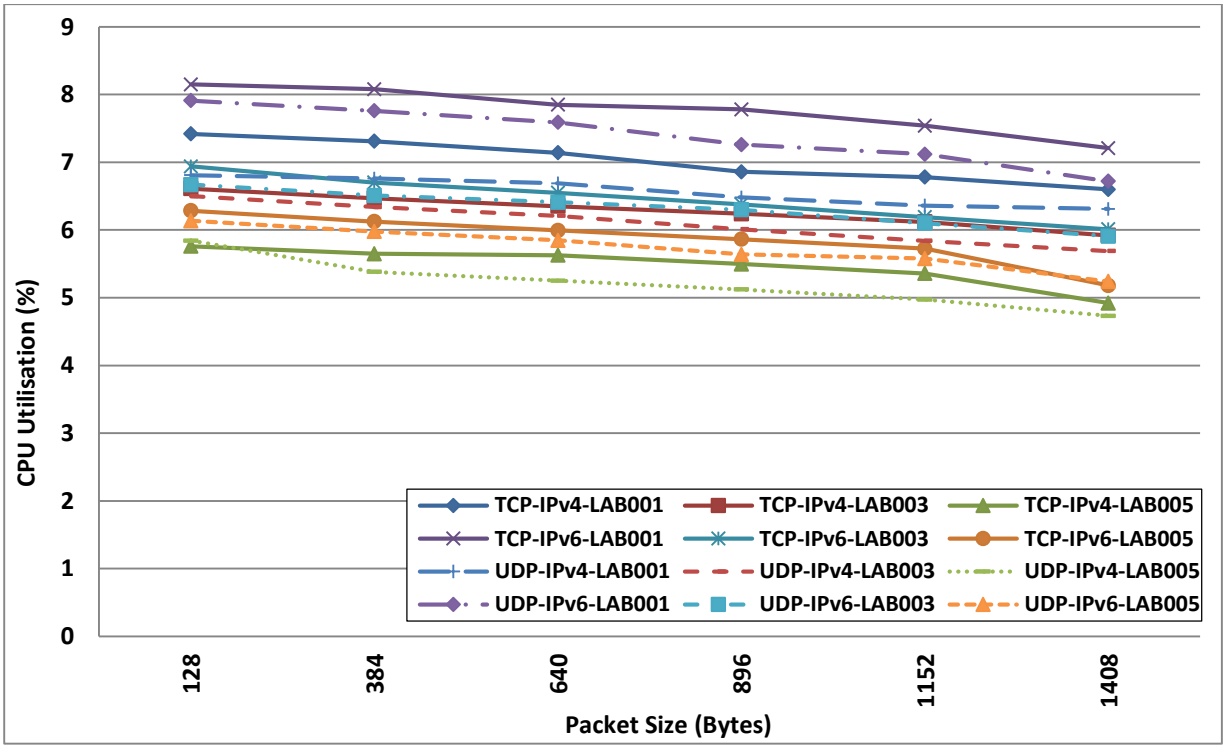

Figure 8.9: Comparison of TCP and UDP CPU Utilisation for both versions of the Internet Protocol in 802.11ac WLAN, LAB005, LAB003, and LAB001

At all three lab locations, UDP consumes less CPU resource than TCP in almost all packet sizes for both versions of the Internet Protocol. In LAB005, the peak difference between UDP and TCP for IPv4 is observed at packet size 1152 Bytes, with UDP outperforming TCP by 0.385% (5.36% for TCP; 4.97% for UDP). For IPv6, UDP decreases CPU usage to 0.225% (from 5.87% by using TCP to 5.64% by using UDP) at 896 Bytes packet size.

At LAB003, the maximum improvement between UDP and TCP for IPv4 is at 1152 Bytes, where UDP has lower CPU usage by 0.28% (6.12% for TCP; 5.84% for UDP). For IPv6, the greatest difference between TCP and UDP is at 128 Bytes, where UDP outperforms TCP by 0.27% (6.94% for TCP; 6.67% for UDP).

At LAB001, the highest variation between UDP and TCP for IPv4 is at packet size 128 Bytes, where UDP consumes less CPU resource than TCP by 0.61% (7.42% for TCP; 6.81% for UDP). At packet size 896 Bytes, UDP for IPv6 returns lower CPU usage than TCP by 0.52% (7.78% for TCP; 7.26% for UDP).

Overall, UDP has the minimum CPU utilisation for both versions of the Internet Protocol on almost all packet sizes. This is because UDP has a lower overhead (8 Bytes) than TCP (20 Bytes) [39].

8.4 Comparison of throughput, RTT, and CPU utilisation

The overall results showed that on average, when the client PC moved away from the access point and the number of obstacles increased, the impact of shadowing results in a lower throughput, longer RTT and higher CPU usage for both TCP and UDP when implementing both Internet Protocols (IPv4 and IPv6).

Throughput comparison between LAB005 vs. LAB003, LAB005 vs. LAB001, and LAB003 vs. LAB001

On average, the highest TCP and UDP throughput for both versions of the Internet Protocol were measured at LAB005 (5 meters away from AP), then at LAB003 (10 meters away from AP), followed by LAB001 (15 meters away from AP). TCP and UDP throughput for IPv4 decreased by 30.89% and 33.59% respectively at LAB003 compared with applied IPv4 in LAB005. TCP and UDP throughput for IPv4 at LAB001 went down to 49.34% and 54.66% respectively compared with applied IPv4 in LAB005. At LAB003, TCP and UDP throughput for IPv4 decreased by 26.7% and 31.72% respectively compared with applied IPv4 in LAB001. At LAB003, the TCP and UDP throughput for IPv6 reduced by 31.47% and 31.91% respectively compared with applied IPv6 in LAB005. At LAB001, IPv6 decreased the throughput to 45.51% for TCP and 48.53% for UDP compared with implemented IPv6 in LAB005. TCP and UDP for IPv6 in LAB001 returned lower throughput by 20.49% and 24.4% respectively than IPv6 in the LAB003.

Throughput comparison between IPv4 and IPv6 on LAB005, LAB003, and LAB001

On average, throughput for IPv4 outperformed throughput for IPv6 when implementing TCP and UDP in all lab locations (LAB005, LAB003, and LAB001).

At LAB005, the TCP and UDP throughput for IPv6 decreased to 15.43% and 20.26% respectively compared to IPv4. At LAB003, the TCP and UDP throughput for IPv6 decreased to 16.14% and 18.24% respectively compared to IPv4. At LAB001, the TCP and UDP throughput for IPv6 decreased to 9.04% and 9.48% respectively compared to IPv4.

Throughput comparison between TCP and UDP on LAB005, LAB003, and LAB001

On average, throughput for UDP outperformed throughput for TCP by implementing IPv4 and IPv6 at all labs (LAB005, LAB003, and LAB001).

At LAB005, UDP throughput for IPv4 and IPv6 increased to 15.77% and 10.67% respectively compared with applying TCP for both versions of the Internet Protocol. At LAB003, UDP throughput for IPv4 and IPv6 increased to 12.34% and 10.10% respectively compared with TCP for both protocols (IPv4, IPv6). At LAB001, UDP throughput for IPv4 and IPv6 increased to 5.91% and 5.45% respectively compared with TCP for both protocols (IPv4, IPv6).

RTT comparison between LAB005 vs. LAB003, LAB005 vs. LAB001, and LAB003 vs. LAB001

On average, the lowest TCP and UDP RTT for both IPv4 and IPv6 were measured at LAB005, then at LAB003, followed by LAB001.

The client PC at LAB005 decreased the TCP and UDP RTT for IPv4 by 30.60% and 32.13% respectively compared with applied IPv4 in LAB003. RTT for IPv4 reduced by 49.48% or TCP and 53.28% for UDP at LAB005 compared with applied IPv4 in LAB001. Implementing IPv4 decreased RTT to 27.21% for TCP and 31.16% for UDP at LAB003 compared with applied IPv4 in LAB001. The client PC at LAB005 decreased the TCP and UDP RTT for IPv6 by 31.04% and 32.17% respectively compared with applied IPv6 in LAB003. At LAB005, RTT for IPv6 reduced by 44.77% for TCP and 48.23% for UDP compared with applied IPv6 in LAB001. At LAB003, implementing IPv6 decreased RTT to 19.91% for TCP and 23.67% for UDP compared with applied IPv6 in LAB001.

RTT comparison between IPv4 and IPv6 on LAB005, LAB003, and LAB001

On average, RTT for IPv4 outperformed RTT for IPv6 by implementing TCP and UDP at all labs (LAB005, LAB003, and LAB001).

At LAB005, the TCP and UDP RTT for IPv6 increased by 16.1% and 18.24% respectively compared to IPv4. At LAB003, the TCP and UDP RTT for IPv6 rose by 16.54% and 18.29% respectively compared to IPv4. At LAB001, the TCP and UDP RTT for IPv6 increased by 8.17% and 9.41% respectively compared to IPv4.

RTT comparison between TCP and UDP on LAB005, LAB003, and LAB001

On average, RTT for UDP outperformed throughput for TCP by implementing IPv4 and IPv6 at all labs (LAB005, LAB003, and LAB001).

At LAB005, UDP decreased RTT to 14.44% for IPv4 and 12.1% for IPv6 compared with TCP for both protocols (IPv4, IPv6). At LAB003, UDP decreased RTT by 12.51% for IPv4 and 10.63% for IPv6 compared with TCP. At LAB001, UDP had a shorter RTT by 7.49% for IPv4 and 6.23% for IPv6 than TCP.

CPU Utilisation comparison between LAB005 vs. LAB003, LAB005 vs. LAB001, and LAB003 vs. LAB001

On average, the lowest TCP and UDP CPU usage for both IPv4 and IPv6 were measured at LAB005, then at LAB003, followed by LAB001.

Applying IPv4 for TCP and UDP reduced the CPU usage by 0.82% and 0.88% at LAB005 compared with applying IPv4 for TCP and UDP in LAB003. IPv4 for TCP and UDP consumed less CPU resource by 1.55% and 1.35% at LAB005 than in LAB001. IPv4 for TCP and UDP reduced the CPU usage by 0.73% and 0.47% at LAB003 compared with LAB001. Applying IPv6 for TCP and UDP reduced the CPU usage by 0.6% and 0.58% at LA005 compared with LAB003. IPv6 for TCP and UDP consumed a lower CPU resource by 1.91% and 1.66% at LAB005 than in LAB001. IPv6 for TCP and UDP reduced the CPU usage by 1.31% and 1.08% at LAB003 compared with LAB001.

CPU utilisation comparison between IPv4 and IPv6 on LAB005, LAB003, and LAB001

On average, CPU usage for IPv4 outperformed CPU utilisation for IPv6 when applying TCP and UDP at all labs (LAB005, LAB003, and LAB001).

At LAB005, the TCP and UDP CPU usage for IPv6 increased by 0.39% and 0.52% respectively compared to IPv4. At LAB003, the TCP and UDP CPU usage for IPv6 rose by 0.18% and 0.22% respectively compared to IPv4. At LAB001, the TCP and UDP CPU usage for IPv6 increased by 0.75% and 0.82% respectively compared to IPv4.

CPU utilisation comparison between TCP and UDP on LAB005, LAB003, and LAB001

On average, UDP consumed less CPU resource than TCP by implementing IPv4 or IPv6 at all labs (LAB005, LAB003, and LAB001).

At LAB005, UDP decreased CPU usage by 0.25% for IPv4 and 0.13% for IPv6 than TCP for both protocols (IPv4, IPv6). At LAB003, UDP decreased CPU usage by 0.19% for IPv4 and 0.14% for IPv6 than TCP for both protocols (IPv4, IPv6). At LAB001, UDP decreased CPU usage by 0.45% for IPv4 and 0.38% for IPv6 than TCP.

8.5 Chapter Summary

In this chapter, an inverse relationship was demonstrated between (the number of obstructions, and distance) and (the throughput, RTT, and CPU usage). When the client moved away from the access point and increased the number of obstacles, the throughput was decreased, while RTT and CPU usage were increased. Moreover, implementing IPv6 had a lower throughput, longer RTT and higher CPU usage than IPv4 for both TCP and UDP laboratories testing. Also, applying UDP outperformed TCP for both IPv4 and IPv6. The results showed that on average, the highest throughput (30.56 Mbps), shortest RTT (1.85 ms) and lowest CPU usage (5.22%) were measured with the client located 5 meters away from the Access Point (LAB005) and implementing IPv4 for UDP protocol, whereas the lowest throughput (11.86 Mbps), longest RTT (2.87 ms) and highest CPU usage (7.77%) were measured with the client located 15 meters away from the Access Point (LAB001) and implementing IPv6 for TCP protocol.

The next chapter covers the summary, conclusions, and future works.

CHAPTER 9

SUMMARY, CONCLUSIONS, AND FUTURE WORKS

This chapter summarises the experimental results and thesis contribution. Suggested future work in the same arena is also presented.

This study evaluated the performance of 802.11ac WLAN in three different scenarios, namely, the impact of implementing WPA2 security encryption, the effect of human movement, and the shadowing effects. In order to fulfill the objects of this research, experiments have been employed to collect data in a laboratory environment. Two operating systems were installed over client and server workstations (Windows 8.1 Pro and Server 2012) with different protocol settings. Test-beds examined transmission protocols (TCP and UDP) for both versions of the Internet Protocol (IPv4 and IPv6) with the same dependent variables. The performance metrics measured and analysed were throughput, round trip time, and CPU utilisation.

This thesis produced much interesting information about the IEEE 802.11ac standard that will contribute to knowledge related to its performance characteristics in different environmental conditions. The data in various rooms, effect of security, human movement, will help network designer to finds out the number of access points required to achieve a certain throughput. It also helps to decide where to put the access points. An appropriate AP placement is required to obtain greater performance of WLANs.

IEEE 802.11ac is better than the previous standard technologies such as 11g, 11b and 11a, as far as protocol overheads are concerned. This is because 802.11ac uses Frame aggregation (section 3.2.2), which similar to 802.11n to reduce overheads. As chapter 2 explained in detail, the overhead provides information that is encapsulated with transmitted data and which contains the sources and destinations of the packet. It adds extra bytes to the data packet. It was noticed that the most significant increases in throughput degradation, CPU consumption, and round trip time occurred when TCP was applied for IPv6 with WPA2 encryption enabled over the Wi-Fi LAN in all experimental scenarios. The reason for this is that the selection of protocol mechanisms (mentioned above) adds 76 Bytes overhead (16 Bytes by WPA2, 20 Bytes by TCP, and 40 Bytes by IPv6) into the data packet, which may lead to the packet breaking up into several smaller packets, thus leading to reduced throughput and increased CPU usage and round trip time.

The key issues investigated and new results obtained and these are the following:

9.1 Open System vs. WPA2 Security Encryption

In all the test-bed evaluations, the TCP and UDP on WLAN in an open system had a higher throughput and shorter round trip time and lower CPU usage than the WPA2 encryption enabled for both versions of the Internet Protocol. The results showed that on average, the most significant differences with regard to higher throughput, shorter RTT, and lower CPU usage between the open system and the WPA2 security enabled system was captured when UDP throughput for IPv6 went up to 38.46% (from 238 Mbps for UDP WPA2 to 386.73 Mbps for UDP OS), and UDP RTT for IPv6 reduced to 37.48% (from 0.238 ms for UDP WPA2 to 0.149 ms for UDP OS), whereas UDP CPU usage for IPv6 decreased by 1.75% (from 3.94% for UDP WPA2 to 2.19% for UDP OS).

Moreover, the smallest differences with regard to higher throughput, shorter RTT, and lower CPU usage between with and without WPA2 encryption enabled system was captured when UDP throughput for IPv4 went up to 26.68% (from 459.18 Mbps for UDP WPA2 to 626.27 Mbps for UDP OS), and UDP RTT for IPv4 reduced to 26.3% (from 0.124 ms for UDP WPA2 to 0.091 ms for UDP OS), whereas UDP CPU usage for IPv4 decreased by 0.25% (from 2.06% for UDP WPA2 to 1.82% for UDP OS).

The maximum achievable throughput was spotted at packet size 1408 Bytes where UDP throughput for IPv4 provided 852 Mbps in the open system environment. This throughput value is less than the theoretical maximum throughput of 802.11ac (1.3 Gbps) by 34.46% (448 Mbps).

9.2 No Human Shadowing vs. Human Movement

In all the test-bed evaluations, the performance of 802.11ac WLAN without human shadowing outperformed the performance of this network in the presence of human movement. In the absence of human movement, the TCP and UDP had a higher throughput and shorter round trip time and lower CPU usage than in the presence of human movement for both IPv4 and IPv6.

The results showed that on average, the most significant differences between the absence and the presence of human movement was spotted when the TCP throughput for IPv6 went up to 13.38% (from 214.67 Mbps for TCP MOV to 247.83 Mbps for TCP W-MOV), and TCP RTT for IPv4 reduced to 13.62% (from 0.161 ms for TCP MOV to 0.139 ms for TCP W-MOV), and UDP CPU usage for IPv6 decreased by 0.415% (from 4.12% for UDP MOV to 3.78% for UDP W-MOV).

Moreover, the smallest differences between the absence and presence of human movement were spotted when the UDP throughput for IPv6 went up to 8.74% (from 261 Mbps for UDP MOV to 286 Mbps for UDP W-MOV), and UDP RTT for IPv6 reduced to 8.6% (from 0.219 ms for UDP MOV to 0.2 ms for UDP W-MOV), and TCP CPU usage for IPv4 decreased by 0.142% (from 3.61% for TCP MOV to 3.47% for TCP W-MOV).

As shown from the results above, the presence of human movement has an insignificant impact of 802.11ac WLAN performance compared with the absence of a human shadowing environment.

9.3 The Effect of Shadowing in Laboratory Environment (lab 2005, lab 2003, and lab 2001)

There was a reverse relation between the number of obstructions, the distance and the throughput. When the client moved away from the access point and increased the number of obstacles, the throughput was decreased. In all the test-bed evaluations, the performance of 802.11ac WLAN was influenced by the placement of the client (receiver). When the client moved away from the access point then the number of obstacles was increased, the impact of shadowing provided a lower throughput and longer round trip time and lower CPU usage for both TCP and UDP by implementing both the Internet Protocols (IPv4 and IPv6). The results showed that on average, the most significant differences between three obstructed environments was spotted at lab 2001. Lab 2001 has more walls and distance than other two rooms between wireless client and server (Figure 5.6) so the bandwidth has dropped much further. As a result of that the UDP throughput for IPv4 went down to 54.66% (from 30.56 Mbps for UDP lab 2005 to 13.86 Mbps for UDP lab 2001), and UDP RTT for IPv4 increased to 53.28% (from 1.14 ms for UDP lab 2005 to 2.44 ms for UDP lab 2001) and TCP CPU usage for IPv6 increased by 1.91% (from 5.86% for TCP lab 2005 to 7.77% for TCP lab 2001) compared to the receiver at lab 2005.

Moreover, the smallest differences between three obstructed environments was spotted at lab 2001 when TCP throughput for IPv6 went down to 20.49% (from 14.92 Mbps for TCP lab 2003 to 11.86 Mbps for TCP lab 2001), TCP RTT for IPv6 increased to 19.91% (from 2.3 ms for TCP lab 2003 to 2.87 ms for TCP lab 2001), and UDP CPU usage for IPv4 increased by 0.47% (from 6.1 % for UDP lab 2003 to 6.57% for UDP lab 2001) compared to the receiver at lab 2003.

The shadowing (walls) environment and distance had a much greater impact on 802.11ac WLAN performance than that observed when comparing the effects of applying IPv6, WPA2 encryption and the presence of human movement. It reduced the throughput by figures as large as 98% (11.86 Mbps for TCP-IPv6 at lab 2001 compared to 626.27 Mbps for UDP-IPv4 OS) for a minimum average of throughput compared with the maximum average of throughput in typical environmental conditions (the impact of implementing WPA2 security scenario).

9.4 IPv4 vs. IPv6

The difference between IPv4 and IPv6 over WLAN performance was mostly large. In all the test-bed evaluations, IPv4 outperformed IPv6 in different levels, depending on the network environment. The results showed that, on average, the most significant differences with regard to throughput degradation, as well as the highest RTT and CPU usage between IPv4 and IPv6 were spotted in implementing the WPA2 security scenario. The TCP throughput for IPv6 reduced by 48.99% (from 542.91 Mbps for IPv4 OS to 277 Mbps for IPv6 OS) and TCP RTT for IPv6 increased by 49.08% (from 0.105 ms for IPv4 OS to 0.206 ms for IPv6 OS) compared with applying IPv4 in the open system environment. The UDP usage for IPv6 rose by 1.88% (from 2.07% for IPv4 WPA2 to 3.94% for IPv6 WPA2) compared to IPv4 in the WPA2 security enabled environment.

Moreover, the smallest differences related to throughput degradation, RTT length, and CPU consumption between IPv4 and IPv6 were captured during the shadowing effects scenario. The TCP throughput for IPv6 reduced by 9.04% (from 13.04 Mbps for IPv4 to 11.86 Mbps for IPv6), and the TCP RTT for IPv6 increased by 8.17% (from 2.64 ms for IPv4 to 2.87 ms for IPv6) compared with applying IPv4 in the lab 2001 (15 meters away from AP). IPv6 for TCP increased by 0.18% (from 6.29% for IPv4 to 6.46% for IPv6) compared with applying IPv4 in the lab 2003 (10 meters away from AP).

9.5 TCP vs. UDP

The variation between TCP and UDP was mostly significant. In all the test-bed evaluations, UDP outperformed TCP at different levels, depending on the network environment and conditions. The results showed that on average, the most significant differences with regard to higher throughput, shorter RTT, and lower CPU usage between TCP and UDP were spotted when studying the impact of implementing the WPA2 security scenario. In the open system for this scenario, the UDP throughput for IPv6 increased by 28.37% (from 277 Mbps for TCP OS to 386.73 Mbps for UDP OS), and the UDP RTT for IPv6 decreased by 27.79% (from 0.206 ms

for TCP OS to 0.149 ms for UDP OS), whereas the UDP CPU usage for IPv6 reduced by 1.27% (from 3.46% for TCP OS to 2.19% for UDP OS).

Moreover, the smallest differences related to higher throughput, shorter RTT, and lower CPU usage between TCP and UDP were captured during the shadowing effects scenario. In this scenario, the TCP throughput for IPv6 went down about 5.45% (from 12.54 Mbps for UDP to 11.86 Mbps for TCP) and TCP RTT for IPv6 increased by 6.23% (from 2.69 ms for UDP to 2.87 ms for TCP) in the lab 2001 (15 meters away from AP), whereas UDP CPU usage for IPv6 increased by 0.145% (from 6.32% for UDP to 6.46% for TCP) in the lab 2003 (10 meters away from AP).

9.6 Future Work

9.6.1 The Impact of the Number of Nodes on 802.11ac WLAN Performance

In a large-scale network that contains multiple numbers of wireless nodes, when the number of wireless nodes increases, throughput decreases and delay increases [90].

The main objective of this experiment will be to analyse the effect that connecting a single access point to multiple clients (receivers) on the performance of the 802.11ac WLAN, by applying the experimental scenarios that are evaluated in this thesis.

9.6.2 The Effect of Implementing Virtualisation on 802.11ac WLAN Performance

Virtualisation is a fast-growing technology and an important part of modern computing, with more businesses implementing it, due to its many benefits including cost savings and its ability to consolidate network servers. However, the virtualisation architecture has a complicated process that can degrade the wireless network performance by limiting the bandwidth [91].

The main objective of this experiment will be to analyse the effect of implementing virtualisation on the performance of the 802.11ac WLAN by applying the experimental scenarios that are evaluated in this thesis.

9.6.3 The Impacts of Shadowing on the 802.11ac WLAN Performance In an Outdoor Environment

The outdoor environment has a different penetration loss compared to the indoor environment. There are many outdoor factors that can affect penetration loss, such as the position of the building and building materials near the experimental location, and also by effective illumination of these buildings, trees, etc. [92].

These factors can be considered in studying the 802.11ac WLAN performance by applying the experimental scenarios that are evaluated in this thesis in an outdoor environment.

9.6.4 The Impact of Laptop and Smartphone Motion on the 802.11ac WLAN performance

The purpose of studying the performance of the 802.11ac WLANs in the case of user motion (laptop, smartphone) in an indoor environment. There are many factors can be considered in this study such as the increment of user motion speed, rate of packet loss, voice quality, etc. [93].

APPENDICES

APPENDIX A

Hardware Spesfications

Hardware		Server Specification	Client Specification
PC	Processor	Intel® Core™ i5 CPU 2.80 GHz	Intel® Core™ i7-2600 CPU 3.40 GHz
	RAM	24.0 GB RAM	8.0 GB
	LAN Card (NIC) /Ethernet Card	Intel® 82578DC Gigabit Network Connection	AC1750 Wireless Dual Band PCI Express Adapter
Network Connect Device	Cable	CAT5e	
	Access Point	Linksys lapac1750pro business	

Table A-1: Hardware specifications of stations and network connection device

Model	Linksys lapac1750pro business
Network Standards	IEEE 802.11a, b, g, n, and ac
Radio Frequency Bands	2.4 GHz and 5 GHz
Radio Frequency Channels	2.412 to 2.462 GHz: 11 channels 5.180 to 5.240 GHz: 4 channels 5.745 to 5.825 GHz: 5 channels
MIMO	3x3
Data Rates	Up to 1750 Mbps
Access Control	IPv4, IPv6, and MAC-based
Maximum Power Consumption	24W

Table A-2: Access point specifications [94]

Model	AC1750 Wireless Dual Band PCI Express Adapter
Network Standards	IEEE 802.11a, b, g, n, and ac
Radio Frequency Bands	2.4 GHz and 5 GHz
MIMO	3x3
Data Rates	Up to 1300 Mbps at 5 GHz band using 11ac AP
Transmit Power	<20dBm (EIRP)

Table A-3: NIC card specifications [95]

APPENDIX B

The Impact of Implementing WPA2 Security on 802.11ac WLAN Performance

The following tables show the results of TCP and UDP throughput for the first experimental scenario. The results are represented in megabit per second.

TCP throughput

Packet Size (Bytes)	128	256	384	512	640	768	896	1024	1152	1280	1408	AVR
IPv4 - OS	361.00	390.00	434.00	477.00	507.00	574.00	**612.00**	626.00	643.00	656.00	**692.00**	**542.91**
IPv4 - WPA2	271.00	287.00	324.00	338.00	353.00	371.00	394.00	407.00	**437.00**	441.00	454.00	**370.64**
IPv6 - OS	196.00	201.00	211.00	224.00	231.00	261.00	287.00	330.00	**355.00**	369.00	382.00	**277.00**
IPv6 - WPA2	126.00	142.00	157.00	164.00	172.00	194.00	206.00	214.00	234.00	269.00	281.00	**196.27**

The maximum differences												MAX	Percentage	
IPv4 Vs. IPv6	165.00	189.00	223.00	253.00	276.00	313.00	**325.00**	296.00	288.00	287.00	310.00	325.00	**53.10%**	OS
IPv4 Vs. IPv6	145.00	145.00	167.00	174.00	181.00	177.00	188.00	193.00	**203.00**	172.00	173.00	203.00	**46.45%**	WPA2
OS Vs. WPA2	90.00	103.00	110.00	139.00	154.00	203.00	218.00	219.00	206.00	215.00	**238.00**	238.00	**34.39%**	IPv4
OS Vs. WPA2	70.00	59.00	54.00	60.00	59.00	67.00	81.00	116.00	**121.00**	100.00	101.00	121.00	**34.10%**	IPv6

Comparesion between OS vs. WPA2				Comparesion between ipv4 vs. ipv6			
OS vs. WPA2	172.27	31.73	IPv4	IPv4 vs. IPv6	265.91	48.979	OS
OS vs. WPA2	80.73	29.14	IPv6	IPv4 vs. IPv6	174.36	47.044	WPA2

UDP throughput

Packet Size (Bytes)	128	256	384	512	640	768	896	1024	1152	1280	1408	AVR
IPv4 - OS	436.00	467.00	515.00	527.00	542.00	597.00	661.00	731.00	768.00	793.00	**852.00**	**626.27**
IPv4 - WPA2	308.00	320.00	338.00	374.00	427.00	472.00	501.00	539.00	572.00	**590.00**	610.00	**459.18**
IPv6 - OS	288.00	307.00	330.00	**344.00**	359.00	385.00	411.00	429.00	447.00	471.00	483.00	**386.73**
IPv6 - WPA2	135.00	149.00	164.00	177.00	198.00	256.00	278.00	298.00	306.00	312.00	345.00	**238.00**

The maximum differences												MAX	Percentage	
IPv4 Vs. IPv6	148.00	160.00	185.00	183.00	183.00	212.00	250.00	302.00	321.00	322.00	**369.00**	369.00	**43.31%**	OS
IPv4 Vs. IPv6	173.00	171.00	174.00	197.00	229.00	216.00	223.00	241.00	266.00	**278.00**	265.00	278.00	**47.12%**	WPA2
OS Vs. WPA2	128.00	147.00	177.00	153.00	115.00	125.00	160.00	192.00	196.00	203.00	**242.00**	242.00	**28.40%**	IPv4
OS Vs. WPA2	153.00	158.00	166.00	**167.00**	161.00	129.00	133.00	131.00	141.00	159.00	138.00	167.00	**48.55%**	IPv6

Comparesion between OS Vs. WPA2				Comparesion between ipv4 vs. ipv6			
OS vs. WPA2	167.09	26.68	IPv4	IPv4 vs. IPv6	239.55	38.249	OS
OS vs. WPA2	148.73	38.46	IPv6	IPv4 vs. IPv6	221.18	48.169	WPA2

TCP vs. UDP throughput

Packet Size (Bytes)	128	256	384	512	640	768	896	1024	1152	1280	1408	AVR
TCP-IPv4-OS	361.00	390.00	434.00	477.00	507.00	574.00	612.00	626.00	643.00	656.00	**692.00**	542.91
TCP-IPv4-WPA2	271.00	287.00	324.00	338.00	353.00	371.00	394.00	407.00	437.00	441.00	454.00	370.64
TCP-IPv6-OS	196.00	201.00	211.00	224.00	231.00	261.00	287.00	330.00	355.00	369.00	382.00	277.00
TCP-IPv6-WPA2	126.00	142.00	157.00	164.00	172.00	194.00	206.00	214.00	234.00	269.00	281.00	196.27
UDP-IPv4-OS	436.00	467.00	515.00	527.00	542.00	597.00	661.00	731.00	768.00	793.00	**852.00**	626.27
UDP-IPv4-WPA2	308.00	320.00	338.00	374.00	427.00	472.00	501.00	539.00	572.00	590.00	610.00	459.18
UDP-IPv6-OS	288.00	307.00	330.00	344.00	**359.00**	385.00	411.00	429.00	447.00	471.00	483.00	386.73
UDP-IPv6-WPA2	135.00	149.00	164.00	177.00	198.00	256.00	278.00	**298.00**	306.00	312.00	345.00	238.00

The maximum differences											MAX	Percentage	
UDP-OS vs. TCP-OS	75.00	77.00	81.00	50.00	35.00	23.00	49.00	105.00	125.00	137.00	**160.00**	160.00	**18.78%**	IPv4
UDP-WPA2 vs. TCP-WPA2	37.00	33.00	14.00	36.00	74.00	101.00	107.00	132.00	135.00	149.00	**156.00**	156.00	**25.57%**	IPv4
UDP-OS vs. TCP-OS	92.00	106.00	119.00	120.00	**128.00**	124.00	124.00	99.00	92.00	102.00	101.00	128.00	**35.65%**	IPv6
UDP-WPA2 vs. TCP-WPA2	9.00	7.00	7.00	13.00	26.00	62.00	72.00	**84.00**	72.00	43.00	64.00	84.00	**28.19%**	IPv6

Comparesion between TCP vs. UDP			
UDP-OS vs. TCP-OS	83.36	13.31	IPv4
UDP-WPA2 vs. TCP-WPA2	88.55	19.28	
UDP-OS vs. TCP-OS	109.73	28.37	IPv6
UDP-WPA2 vs. TCP-WPA2	41.73	17.53	

The following tables show the results of TCP and UDP round trip time for the first experimental scenario. The results are represented in milliseconds.

TCP RTT

Packet Size (Bytes)	128	256	384	512	640	768	896	1024	1152	1280	1408	AVR
IPv4 - OS	0.028	0.053	0.071	0.086	0.101	0.107	0.117	0.131	0.143	0.156	0.163	0.105
IPv4 - WPA2	0.038	0.071	0.095	0.121	0.145	0.166	0.182	0.201	0.211	0.232	**0.248**	0.155
IPv6 - OS	0.052	0.102	0.146	0.183	0.222	0.235	0.247	0.251	0.260	0.278	**0.295**	0.206
IPv6 - WPA2	0.081	0.144	0.196	0.250	0.298	0.317	0.348	**0.381**	0.385	0.389	0.401	0.290

The maximum differences											MAX	Percentage	
IPv4 Vs. IPv6	-0.024	-0.049	-0.075	-0.097	-0.121	-0.128	-0.130	-0.120	-0.116	-0.121	**-0.132**	-0.132	**53.23%**	OS
IPv4 Vs. IPv6	-0.043	-0.073	-0.101	-0.129	-0.153	-0.151	-0.166	**-0.180**	-0.174	-0.157	-0.153	-0.180	**47.24%**	WPA2
OS Vs. WPA2	-0.009	-0.019	-0.024	-0.035	-0.044	-0.059	-0.065	-0.070	-0.068	-0.076	**-0.085**	-0.085	**34.27%**	IPv4
OS Vs. WPA2	-0.029	-0.042	-0.050	-0.067	-0.076	-0.081	-0.101	**-0.130**	-0.125	-0.111	-0.106	-0.130	**34.12%**	IPv6

Comparesion between OS Vs. WPA2				Comparesion between ipv4 vs. ipv6			
OS vs. WPA2	-0.050	-32.42	IPv4	IPv4 vs. IPv6	-0.101	-49.078	OS
OS vs. WPA2	-0.084	-28.83	IPv6	IPv4 vs. IPv6	-0.134	-46.374	WPA2

UDP RTT

Packet Size (Bytes)	128	256	384	512	640	768	896	1024	1152	1280	1408	AVR
IPv4 - OS	0.023	0.044	0.060	0.078	0.094	0.103	0.108	0.112	0.120	0.129	0.132	0.091
IPv4 - WPA2	0.033	0.064	0.091	0.110	0.120	0.130	0.143	0.152	0.161	0.174	**0.185**	0.124
IPv6 - OS	0.036	0.067	0.093	0.119	0.143	0.160	0.174	0.191	0.206	0.217	**0.233**	0.149
IPv6 - WPA2	0.076	0.137	0.187	**0.231**	0.240	0.257	0.259	0.275	0.301	**0.328**	0.329	0.238

The maximum differences											MAX	Percentage	
IPv4 Vs. IPv6	-0.012	-0.023	-0.033	-0.041	-0.048	-0.057	-0.066	-0.079	-0.086	-0.088	**-0.101**	-0.101	**43.35%**	OS
IPv4 Vs. IPv6	-0.043	-0.073	-0.096	-0.122	-0.120	-0.127	-0.116	-0.123	-0.140	**-0.155**	-0.144	-0.155	**47.26%**	WPA2
OS Vs. WPA2	-0.010	-0.020	-0.031	-0.032	-0.025	-0.027	-0.035	-0.040	-0.041	-0.044	**-0.052**	-0.052	**28.11%**	IPv4
OS Vs. WPA2	-0.040	-0.071	-0.094	**-0.112**	-0.097	-0.097	-0.085	-0.084	-0.095	-0.111	-0.096	-0.112	**48.48%**	IPv6

Comparesion between OS Vs. WPA2				Comparesion between ipv4 vs. ipv6			
OS vs. WPA2	-0.033	-26.30	IPv4	IPv4 vs. IPv6	-0.058	-38.739	OS
OS vs. WPA2	-0.089	-37.48	IPv6	IPv4 vs. IPv6	-0.114	-48.037	WPA2

TCP and UDP RTT

Packet Size (Bytes)	128	256	384	512	640	768	896	1024	1152	1280	1408	AVR
TCP-IPv4-OS	0.028	0.053	0.071	0.086	0.101	0.107	0.117	0.131	0.143	0.156	**0.163**	0.105
TCP-IPv4-WPA2	0.038	0.071	0.095	0.121	0.145	0.166	0.182	0.201	0.211	0.232	**0.248**	0.155
TCP-IPv6-OS	0.052	0.102	0.146	0.183	**0.222**	0.235	0.247	0.251	0.260	0.278	0.295	0.206
TCP-IPv6-WPA2	0.081	0.144	0.196	0.250	0.298	0.317	0.348	**0.381**	0.385	0.389	0.401	0.290
UDP-IPv4-OS	0.023	0.044	0.060	0.078	0.094	0.103	0.108	0.112	0.120	0.129	0.132	0.091
UDP-IPv4-WPA2	0.033	0.064	0.091	0.110	0.120	0.130	0.143	0.152	0.161	0.174	0.185	0.124
UDP-IPv6-OS	0.036	0.067	0.093	0.119	0.143	0.160	0.174	0.191	0.206	0.217	0.233	0.149
UDP-IPv6-WPA2	0.076	0.137	0.187	0.231	0.240	0.257	0.259	0.275	0.301	0.328	0.329	0.238

The maximum differences											MAX	Percentage	
UDP-OS vs. TCP-OS	-0.005	-0.009	-0.011	-0.008	-0.007	-0.004	-0.009	-0.019	-0.023	-0.027	**-0.031**	-0.031	19.02%	IPv4
UDP-WPA2 vs. TCP-WPA2	-0.005	-0.007	-0.004	-0.012	-0.025	-0.035	-0.039	-0.049	-0.050	-0.059	**-0.063**	-0.063	25.40%	IPv4
UDP-OS vs. TCP-OS	-0.017	-0.035	-0.053	-0.064	**-0.079**	-0.076	-0.073	-0.060	-0.053	-0.060	-0.062	-0.079	35.59%	IPv6
UDP-WPA2 vs. TCP-WPA2	-0.005	-0.007	-0.008	-0.018	-0.058	-0.060	-0.089	**-0.106**	-0.084	-0.061	-0.072	-0.106	27.53%	IPv6

Comparesion between TCP vs. UDP			
UDP-OS vs. TCP-OS	-0.014	-13.13	IPv4
UDP-WPA2 vs. TCP-WPA2	-0.032	-20.35	
UDP-OS vs. TCP-OS	-0.057	-27.79	IPv6
UDP-WPA2 vs. TCP-WPA2	-0.052	-17.80	

The following tables show the results of TCP and UDP CPU usage for the first experimental scenario. The results are represented in percentage.

TCP CPU usage

Packet Size (Bytes)	128	256	384	512	640	768	896	1024	1152	1280	1408	AVR
IPv4 - OS	2.51	2.43	2.35	2.22	2.06	1.96	1.92	1.82	1.72	1.52	1.55	2.002
IPv4 - WPA2	4.32	4.09	3.98	4.01	3.85	3.63	3.04	2.30	2.22	2.08	2.06	3.232
IPv6 - OS	4.79	4.43	4.17	4.15	3.94	3.91	3.59	2.41	2.35	2.21	2.16	3.462
IPv6 - WPA2	5.85	5.50	5.25	5.08	4.67	4.61	4.23	3.94	3.55	2.80	2.62	4.370

The maximum differences												MAX	
IPv4 Vs. IPv6	**-2.280**	-2.000	-1.820	-1.930	-1.880	-1.950	-1.670	-0.590	-0.630	-0.690	-0.610	-2.280	OS
IPv4 Vs. IPv6	-1.530	-1.410	-1.270	-1.070	-0.820	-0.980	-1.190	**-1.640**	-1.330	-0.720	-0.560	-1.640	WPA2
OS Vs. WPA2	**-1.810**	-1.660	-1.630	-1.790	-1.790	-1.670	-1.120	-0.480	-0.500	-0.560	-0.510	-1.810	IPv4
OS Vs. WPA2	-1.060	-1.070	-1.080	-0.930	-0.730	-0.700	-0.640	**-1.530**	-1.200	-0.590	-0.460	-1.530	IPv6

Comparesion between OS Vs. WPA2				Comparesion between ipv4 vs. ipv6			
OS vs. WPA2	-1.229	-38.03	IPv4	IPv4 vs. IPv6	-1.459	-42.151	OS
OS vs. WPA2	-0.908	-20.78	IPv6	IPv4 vs. IPv6	-1.138	-26.047	WPA2

UDP CPU usage

Packet Size (Bytes)	128	256	384	512	640	768	896	1024	1152	1280	1408	AVR
IPv4 - OS	2.41	2.24	2.19	2.18	2.05	1.97	1.74	1.55	1.41	1.18	1.09	1.816
IPv4 - WPA2	2.59	2.50	2.34	2.24	2.11	2.06	1.96	1.88	1.74	1.69	1.65	2.066
IPv6 - OS	2.77	2.62	2.43	2.34	2.25	2.11	2.05	1.97	1.94	1.88	1.77	2.191
IPv6 - WPA2	5.04	4.79	4.77	4.75	4.49	3.97	3.89	3.66	3.26	2.52	2.25	3.942

The maximum differences												MAX	
IPv4 Vs. IPv6	-0.360	-0.380	-0.240	-0.160	-0.200	-0.140	-0.310	-0.420	-0.530	**-0.700**	-0.680	-0.700	OS
IPv4 Vs. IPv6	-2.450	-2.290	-2.430	**-2.510**	-2.380	-1.910	-1.930	-1.780	-1.520	-0.830	-0.600	-2.510	WPA2
OS Vs. WPA2	-0.180	-0.260	-0.150	-0.060	-0.060	-0.090	-0.220	-0.330	-0.330	-0.510	**-0.560**	-0.560	IPv4
OS Vs. WPA2	-2.270	-2.170	-2.340	**-2.410**	-2.240	-1.860	-1.840	-1.690	-1.320	-0.640	-0.480	-2.410	IPv6

Comparesion between OS Vs. WPA2				Comparesion between ipv4 vs. ipv6			
OS vs. WPA2	-0.250	-12.10	IPv4	IPv4 vs. IPv6	-0.375	-17.098	OS
OS vs. WPA2	-1.751	-44.42	IPv6	IPv4 vs. IPv6	-1.875	-47.582	WPA2

TCP and UDP CPU usage

Packet Size (Bytes)	128	256	384	512	640	768	896	1024	1152	1280	1408	AVR
TCP-IPv4-OS	2.507	2.427	2.347	2.217	2.057	1.957	1.917	1.817	1.717	1.517	1.547	**2.002**
TCP-IPv4-WPA2	4.317	4.087	3.977	4.007	3.847	3.627	3.037	2.297	2.217	2.077	2.057	**3.232**
TCP-IPv6-OS	4.787	4.427	4.167	4.147	3.937	3.907	3.587	2.407	2.347	2.207	2.157	**3.462**
TCP-IPv6-WPA2	5.847	5.497	5.247	5.077	4.667	4.607	4.227	3.937	3.547	2.797	2.617	**4.370**
UDP-IPv4-OS	2.407	2.237	2.187	2.177	2.047	1.967	1.737	1.547	1.407	1.177	1.087	**1.816**
UDP-IPv4-WPA2	2.587	2.497	2.337	2.237	2.107	2.057	1.957	1.877	1.737	1.687	1.647	**2.066**
UDP-IPv6-OS	2.767	2.617	2.427	2.337	2.247	2.107	2.047	1.967	1.937	1.877	1.767	**2.191**
UDP-IPv6-WPA2	5.037	4.787	4.767	4.747	4.487	3.967	3.887	3.657	3.257	2.517	2.247	**3.942**

The maximum differences											MAX	
UDP-OS vs. TCP-OS	-0.100	-0.190	-0.160	-0.040	-0.010	0.010	-0.180	-0.270	-0.310	-0.340	**-0.460**	-0.460	**IPv4**
UDP-WPA2 vs. TCP-WPA2	-1.730	-1.590	-1.640	**-1.770**	-1.740	-1.570	-1.080	-0.420	-0.480	-0.390	-0.410	-1.770	**IPv4**
UDP-OS vs. TCP-OS	**-2.020**	-1.810	-1.740	-1.810	-1.690	-1.800	-1.540	-0.440	-0.410	-0.330	-0.390	-2.020	**IPv6**
UDP-WPA2 vs. TCP-WPA2	**-0.810**	-0.710	-0.480	-0.330	-0.180	-0.640	-0.340	-0.280	-0.290	-0.280	-0.370	-0.810	**IPv6**

Comparesion between TCP vs. UDP			
UDP-OS vs. TCP-OS	**-0.186**	**-9.31**	**IPv4**
UDP-WPA2 vs. TCP-WPA2	**-1.165**	**-36.06**	
UDP-OS vs. TCP-OS	**-1.271**	**-36.72**	**IPv6**
UDP-WPA2 vs. TCP-WPA2	**-0.428**	**-9.80**	

APPENDIX C

Effect of Human Movement on 802.11ac WLAN

The following tables show the results of TCP and UDP throughput for the second experimental scenario. The results are represented in megabit per second.

TCP throughput

Packet Size (Bytes)	128	384	640	896	1152	1408	AVR
IPv4 - W-MOV	275.00	323.00	381.00	468.00	490.00	501.00	**406.33**
IPv4 - MOV	251.00	296.00	347.00	406.00	409.00	418.00	**354.50**
IPv6 - W-MOV	198.00	212.00	234.00	268.00	280.00	295.00	**247.83**
IPv6 - MOV	148.00	174.00	193.00	219.00	271.00	283.00	**214.67**

The maximum differences							MAX	Percentage	
IPv4 Vs. IPv6	77.00	111.00	147.00	200.00	**210.00**	206.00	210.00	**42.86%**	W-MOV
IPv4 Vs. IPv6	103.00	122.00	154.00	**187.00**	138.00	135.00	187.00	**45.72%**	MOV
W-MOV vs. MOV	24.00	27.00	34.00	62.00	81.00	**83.00**	83.00	**16.77%**	IPv4
W-MOV vs. MOV	**50.00**	38.00	41.00	49.00	9.00	12.00	50.00	**25.25%**	IPv6

Comparesion between W-MOV vs. MOV				Comparesion between ipv4 vs. ipv6			
W-MOV vs. MOV	**51.83**	**12.76**	**IPv4**	IPv4 vs. IPv6	**158.50**	**39.007383**	**W-MOV**
W-MOV vs. MOV	**33.17**	**13.38**	**IPv6**	IPv4 vs. IPv6	**139.83**	**39.445228**	**MOV**

UDP throughput

Packet Size (Bytes)	128	384	640	896	1152	1408	AVR
IPv4 - W-MOV	490.00	518.00	540.00	567.00	576.00	592.00	**547.17**
IPv4 - MOV	471.00	480.00	492.00	496.00	498.00	529.00	**494.33**
IPv6 - W-MOV	221.00	248.00	265.00	301.00	318.00	363.00	**286.00**
IPv6 - MOV	203.00	220.00	246.00	275.00	301.00	321.00	**261.00**

The maximum differences							MAX	Percentage	
IPv4 Vs. IPv6	269.00	270.00	**275.00**	266.00	258.00	229.00	275.00	**50.93%**	W-MOV
IPv4 Vs. IPv6	**268.00**	260.00	246.00	221.00	197.00	208.00	268.00	**56.90%**	MOV
W-MOV vs. MOV	19.00	38.00	48.00	71.00	**78.00**	63.00	78.00	**13.54%**	IPv4
W-MOV vs. MOV	18.00	28.00	19.00	26.00	17.00	**42.00**	42.00	**11.26%**	IPv6

Comparesion between W-MOV vs. MOV				Comparesion between ipv4 vs. ipv6			
W-MOV vs. MOV	**52.83**	**9.66**	**IPv4**	IPv4 vs. IPv6	**261.17**	**47.730734**	**W-MOV**
W-MOV vs. MOV	**25.00**	**8.74**	**IPv6**	IPv4 vs. IPv6	**233.33**	**47.201618**	**MOV**

TCP and UDP throughput

Packet Size (Bytes)	128	384	640	896	1152	1408	AVR
TCP-IPv4-W-MOV	275.00	323.00	381.00	468.00	490.00	501.00	406.33
TCP-IPv4 -MOV	251.00	296.00	347.00	406.00	409.00	417.00	354.33
TCP-IPv6-W-MOV	198.00	212.00	234.00	268.00	280.00	295.00	247.83
TCP-IPv6-MOV	148.00	174.00	193.00	219.00	271.00	284.00	214.83
UDP-IPv4-W-MOV	490.00	518.00	540.00	567.00	576.00	592.00	547.17
UDP-IPv4-MOV	471.00	480.00	492.00	496.00	498.00	529.00	494.33
UDP-IPv6-W-MOV	221.00	248.00	265.00	301.00	318.00	364.00	286.17
UDP-IPv6-MOV	203.00	220.00	246.00	275.00	301.00	323.00	261.33

The maximum differences							MAX	Percentage	
UDP-W-MOV vs. TCP-W-MOV	**215.00**	195.00	159.00	99.00	86.00	91.00	215.00	**43.88%**	IPv4
UDP-MOV vs. TCP-MOV	**220.00**	184.00	145.00	90.00	89.00	112.00	220.00	**46.71%**	IPv4
UDP-W-MOV vs. TCP-W-MOV	23.00	36.00	31.00	33.00	38.00	**69.00**	69.00	**18.96%**	IPv6
UDP-MOV vs. TCP-MOV	55.00	46.00	53.00	**56.00**	30.00	39.00	56.00	**20.36%**	IPv6

Comparesion between TCP vs. UDP			
UDP-W-MOV vs. TCP-W-MOV	140.83	25.74	IPv4
UDP-MOV vs. TCP-MOV	140.00	28.32	
UDP-W-MOV vs. TCP-W-MOV	38.33	13.40	IPv6
UDP-MOV vs. TCP-MOV	46.50	17.79	

The following tables show the results of TCP and UDP round trip time for the second experimental scenario. The results are represented in milliseconds.

TCP RTT

Packet Size (Bytes)	128	384	640	896	1152	1408	AVR
IPv4 - W-MOV	0.037	0.095	0.134	0.153	0.188	0.225	0.139
IPv4 - MOV	0.041	0.104	0.148	0.177	0.225	0.270	0.161
IPv6 - W-MOV	0.052	0.145	0.219	0.267	0.329	0.382	0.232
IPv6 - MOV	0.069	0.177	0.265	0.327	0.340	0.397	0.263

The maximum differences							MAX	Percentage	
IPv4 Vs. IPv6	-0.014	-0.050	-0.084	-0.114	-0.141	**-0.157**	-0.157	**41.10%**	W-MOV
IPv4 Vs. IPv6	-0.028	-0.073	-0.118	**-0.151**	-0.115	-0.126	-0.151	**46.18%**	MOV
W-MOV vs. MOV	-0.004	-0.009	-0.013	-0.023	-0.037	**-0.045**	-0.045	**16.67%**	IPv4
W-MOV vs. MOV	-0.017	-0.032	-0.046	**-0.060**	-0.011	-0.015	-0.060	**18.35%**	IPv6

Comparesion between W-MOV vs. MOV				Comparesion between ipv4 vs. ipv6			
W-MOV vs. MOV	-0.022	-13.62	IPv4	IPv4 vs. IPv6	-0.094	-40.25	W-MOV
W-MOV vs. MOV	-0.030	-11.50	IPv6	IPv4 vs. IPv6	-0.102	-38.79	MOV

UDP RTT

Packet Size (Bytes)	128	384	640	896	1152	1408	AVR
IPv4 - W-MOV	0.021	0.059	0.095	0.126	0.160	0.190	0.109
IPv4 - MOV	0.022	0.064	0.104	0.145	0.185	0.213	0.122
IPv6 - W-MOV	0.046	0.124	0.193	0.238	0.290	0.309	0.200
IPv6 - MOV	0.050	0.140	0.208	0.261	0.306	0.349	0.219

The maximum differences							MAX	Percentage	
IPv4 Vs. IPv6	-0.025	-0.065	-0.098	-0.112	**-0.130**	-0.119	-0.130	**44.83%**	W-MOV
IPv4 Vs. IPv6	-0.029	-0.076	-0.104	-0.116	-0.121	**-0.136**	-0.136	**38.97%**	MOV
W-MOV vs. MOV	-0.001	-0.005	-0.009	-0.018	**-0.025**	-0.023	-0.025	**13.51%**	IPv4
W-MOV vs. MOV	-0.004	-0.016	-0.015	-0.023	-0.016	**-0.039**	-0.039	**11.17%**	IPv6

Comparesion between W-MOV vs. MOV				Comparesion between ipv4 vs. ipv6			
W-MOV vs. MOV	-0.013	-11.01	IPv4	IPv4 vs. IPv6	-0.092	-45.72786	W-MOV
W-MOV vs. MOV	-0.019	-8.60	IPv6	IPv4 vs. IPv6	-0.097	-44.25889	MOV

TCP and UDP RTT

Packet Size (Bytes)	128	384	640	896	1152	1408	AVR
TCP-IPv4-W-MOV	0.037	0.095	0.134	0.153	0.188	0.225	0.139
TCP-IPv4 -MOV	0.041	0.104	0.148	0.177	0.225	0.270	0.161
TCP-IPv6-W-MOV	0.052	0.145	0.219	0.267	0.329	0.382	0.232
TCP-IPv6-MOV	0.069	0.177	0.265	0.327	0.340	0.397	0.263
UDP-IPv4-W-MOV	0.021	0.059	0.095	0.126	0.160	0.190	0.109
UDP-IPv4-MOV	0.022	0.064	0.104	0.145	0.185	0.213	0.122
UDP-IPv6-W-MOV	0.046	0.124	0.193	0.238	0.290	0.309	0.200
UDP-IPv6-MOV	0.050	0.140	0.208	0.261	0.306	0.349	0.219

The maximum differences							MAX	Percentage	
UDP-W-MOV vs. TCP-W-MOV	-0.016	-0.036	**-0.040**	-0.027	-0.028	-0.035	-0.040	**29.85%**	IPv4
UDP-MOV vs. TCP-MOV	-0.019	-0.040	-0.043	-0.032	-0.040	**-0.057**	-0.057	**21.11%**	IPv4
UDP-W-MOV vs. TCP-W-MOV	-0.005	-0.021	-0.026	-0.029	-0.039	**-0.072**	-0.072	**18.85%**	IPv6
UDP-MOV vs. TCP-MOV	-0.019	-0.037	-0.057	**-0.067**	-0.034	-0.048	-0.067	**20.49%**	IPv6

Comparesion between TCP vs. UDP			
UDP-W-MOV vs. TCP-W-MOV	-0.03	-21.75	IPv4
UDP-MOV vs. TCP-MOV	-0.04	-24.04	
UDP-W-MOV vs. TCP-W-MOV	-0.03	-13.85	IPv6
UDP-MOV vs. TCP-MOV	-0.04	-16.59	

The following tables show the results of TCP and UDP CPU usage for the second experimental scenario. The results are represented in percentage.

TCP CPU usage

Packet Size (Bytes)	128	384	640	896	1152	1408	AVR
IPv4 - W-MOV	3.820	3.660	3.560	3.450	3.250	3.060	3.47
IPv4 - MOV	4.090	3.850	3.700	3.530	3.340	3.140	3.61
IPv6 - W-MOV	5.030	4.980	4.940	4.910	4.870	4.830	4.93
IPv6 - MOV	5.290	5.220	5.160	5.100	5.040	4.990	5.13

The maximum differences							MAX	Percentage	
IPv4 Vs. IPv6	-1.210	-1.320	-1.380	-1.460	-1.620	**-1.770**	-1.770	36.65%	W-MOV
IPv4 Vs. IPv6	-1.200	-1.370	-1.460	-1.570	-1.700	**-1.850**	-1.850	37.07%	MOV
W-MOV vs. MOV	**-0.270**	-0.190	-0.140	-0.080	-0.090	-0.080	-0.270	6.60%	IPv4
W-MOV vs. MOV	**-0.260**	-0.240	-0.220	-0.190	-0.170	-0.160	-0.260	4.91%	IPv6

Comparesion between W-MOV vs. MOV				Comparesion between ipv4 vs. ipv6			
W-MOV vs. MOV	-0.142	-3.93	IPv4	IPv4 vs. IPv6	-1.460	-29.63464	W-MOV
W-MOV vs. MOV	-0.207	-4.03	IPv6	IPv4 vs. IPv6	-1.525	-29.70779	MOV

UDP CPU usage

Packet Size (Bytes)	128	384	640	896	1152	1408	AVR
IPv4 - W-MOV	3.650	3.490	3.360	3.230	3.090	2.840	3.277
IPv4 - MOV	3.760	3.620	3.500	3.390	3.270	3.160	3.450
IPv6 - W-MOV	4.100	3.940	3.840	3.730	3.630	3.530	3.795
IPv6 - MOV	4.720	4.460	4.290	4.110	3.930	3.750	4.210

The maximum differences							MAX	Percentage	
IPv4 Vs. IPv6	-0.450	-0.450	-0.480	-0.500	-0.540	-0.690	-0.690	19.55%	W-MOV
IPv4 Vs. IPv6	-0.960	-0.840	-0.790	-0.720	-0.660	-0.590	-0.960	20.34%	MOV
W-MOV vs. MOV	-0.110	-0.130	-0.140	-0.160	-0.180	-0.320	-0.320	10.13%	IPv4
W-MOV vs. MOV	-0.620	-0.520	-0.450	-0.380	-0.300	-0.220	-0.620	13.14%	IPv6

Comparesion between W-MOV vs. MOV				Comparesion between ipv4 vs. ipv6			
W-MOV vs. MOV	-0.173	-5.02	IPv4	IPv4 vs. IPv6	-0.518	-13.65832	W-MOV
W-MOV vs. MOV	-0.415	-9.86	IPv6	IPv4 vs. IPv6	-0.760	-18.05226	MOV

TCP and UDP CPU usage

Packet Size (Bytes)	128	384	640	896	1152	1408	AVR
TCP-IPv4-W-MOV	3.820	3.660	3.560	3.450	3.270	3.160	3.49
TCP-IPv4 -MOV	4.090	3.850	3.700	3.530	3.340	3.140	3.61
TCP-IPv6-W-MOV	5.030	4.980	4.940	4.910	4.870	4.830	4.93
TCP-IPv6-MOV	5.290	5.220	5.160	5.100	5.040	4.990	5.13
UDP-IPv4-W-MOV	3.650	3.490	3.360	3.230	3.090	2.840	3.28
UDP-IPv4-MOV	3.760	3.620	3.500	3.390	3.250	3.060	3.43
UDP-IPv6-W-MOV	4.100	3.940	3.840	3.730	3.630	3.530	3.80
UDP-IPv6-MOV	4.720	4.460	4.290	4.110	3.930	3.750	4.21

The maximum differences							MAX	
UDP-W-MOV vs. TCP-W-MOV	-0.170	-0.170	-0.200	-0.220	-0.180	-0.320	-0.320	IPv4
UDP-MOV vs. TCP-MOV	-0.330	-0.230	-0.200	-0.140	-0.090	-0.080	-0.330	IPv4
UDP-W-MOV vs. TCP-W-MOV	-0.930	-1.040	-1.100	-1.180	-1.240	-1.300	-1.300	IPv6
UDP-MOV vs. TCP-MOV	-0.570	-0.760	-0.870	-0.990	-1.110	-1.240	-1.240	IPv6

Comparesion between TCP vs. UDP			
UDP-W-MOV vs. TCP-W-MOV	-0.21	-6.023	IPv4
UDP-MOV vs. TCP-MOV	-0.18	-4.942	
UDP-W-MOV vs. TCP-W-MOV	-1.13	-22.970	IPv6
UDP-MOV vs. TCP-MOV	-0.92	-17.987	

APPENDIX D

EFFECT OF SHADOWING ON 802.11ac WLAN IN LABORATORY ENVIRONMENT

The following tables show the results of TCP and UDP throughput for the third experimental scenario. The results are represented in megabit per second.

TCP throughput

Packet Size (Bytes)	128	384	640	896	1152	1408	AVR
IPv4 - LAB001	11.87	12.21	12.76	12.95	13.60	14.84	13.04
IPv4 - LAB003	15.80	16.10	17.62	18.04	18.50	20.67	17.79
IPv4 - LAB005	23.40	23.85	24.70	25.92	26.81	29.75	25.74
IPv6 - LAB001	9.81	10.60	11.51	12.10	13.20	13.94	11.86
IPv6 - LAB003	12.90	14.43	14.82	15.10	15.77	16.48	14.92
IPv6 - LAB005	19.22	20.10	20.77	22.93	23.10	24.48	21.77

The maximum differences							MAX	Persentage	
IPv4 vs. IPv6	2.06	1.61	1.25	0.85	0.40	0.90	2.06	17.35%	LAB001
IPv4 vs. IPv6	2.90	1.67	2.80	2.94	2.73	4.19	4.19	20.27%	LAB003
IPv4 vs. IPv6	4.18	3.75	3.93	2.99	3.71	5.27	5.27	17.71%	LAB005
LA005 vs. LAB003	7.60	7.75	7.08	7.88	8.31	9.08	9.08	30.52%	IPv4
LA005 vs. LAB001	11.53	11.64	11.94	12.97	13.21	14.91	14.91	50.12%	
LA003 vs. LAB001	3.93	3.89	4.86	5.09	4.90	5.83	5.83	28.21%	
LA005 vs. LAB003	6.32	5.67	5.95	7.83	7.33	8.00	8.00	32.68%	IPv6
LA005 vs. LAB001	9.41	9.50	9.26	10.83	9.90	10.54	10.83	47.23%	
LA003 vs. LAB001	3.09	3.83	3.31	3.00	2.57	2.54	3.83	26.54%	

Comparesion between lab001-lab003-lab005				Comparesion between ipv4 vs. ipv6			
LA005 vs. LAB003	7.95	30.89	IPv4	IPv4 vs. IPv6	1.18	9.04	LAB001
LA005 vs. LAB001	12.70	49.34		IPv4 vs. IPv6	2.87	16.14	LAB003
LA003 vs. LAB001	4.75	26.70		IPv4 vs. IPv6	3.97	15.43	LAB005
LA005 vs. LAB003	6.85	31.47	IPv6				
LA005 vs. LAB001	9.91	45.51					
LA003 vs. LAB001	3.06	20.49					

UDP throughput

Packet Size (Bytes)	128	384	640	896	1152	1408	AVR
IPv4 - LAB001	12.40	13.01	13.40	13.90	14.61	15.82	13.86
IPv4 - LAB003	17.60	18.64	19.50	21.64	21.70	22.68	20.29
IPv4 - LAB005	28.40	28.84	29.34	29.50	31.87	35.40	30.56
IPv6 - LAB001	10.71	11.94	12.01	12.60	13.70	14.30	12.54
IPv6 - LAB003	14.70	15.34	15.81	16.70	17.60	19.40	16.59
IPv6 - LAB005	21.00	23.20	24.09	25.15	25.92	26.85	24.37

The maximum differences							MAX	Persentage	
IPv4 vs. IPv6	1.69	1.07	1.39	1.30	0.91	1.52	1.69	13.63%	LAB001
IPv4 vs. IPv6	2.90	3.30	3.69	4.94	4.10	3.28	4.94	22.83%	LAB003
IPv4 vs. IPv6	7.40	5.64	5.25	4.35	5.95	8.55	8.55	24.15%	LAB005
LA005 vs. LAB003	10.80	10.20	9.84	7.86	10.17	12.72	12.72	35.93%	IPv4
LA005 vs. LAB001	16.00	15.83	15.94	15.60	17.26	19.58	19.58	55.31%	
LA003 vs. LAB001	5.20	5.63	6.10	7.74	7.09	6.86	7.74	35.77%	
LA005 vs. LAB003	6.30	7.86	8.28	8.45	8.32	7.45	8.45	33.60%	IPv6
LA005 vs. LAB001	10.29	11.26	12.08	12.55	12.22	12.55	12.55	46.74%	
LA003 vs. LAB001	3.99	3.40	3.80	4.10	3.90	5.10	5.10	26.29%	

Comparesion between lab001-lab003-lab005				Comparesion between ipv4 vs. ipv6			
LA005 vs. LAB003	10.27	33.59	IPv4	IPv4 vs. IPv6	1.31	9.48	LAB001
LA005 vs. LAB001	16.70	54.66		IPv4 vs. IPv6	3.70	18.24	LAB003
LA003 vs. LAB001	6.44	31.72		IPv4 vs. IPv6	6.19	20.26	LAB005
LA005 vs. LAB003	7.78	31.91	IPv6				
LA005 vs. LAB001	11.83	48.53					
LA003 vs. LAB001	4.05	24.40					

TCP and UDP throughput

Packet Size (Bytes)	128	384	640	896	1152	1408	AVR
TCP-IPv4-LAB001	11.87	12.21	12.76	12.95	13.60	14.84	13.04
TCP-IPv4-LAB003	15.80	16.10	17.62	18.04	18.50	20.67	17.79
TCP-IPv4-LAB005	23.40	23.85	24.70	25.92	26.81	29.75	25.74
TCP-IPv6-LAB001	9.81	10.60	11.51	12.10	13.20	13.94	11.86
TCP-IPv6-LAB003	12.90	14.43	14.82	15.10	15.77	16.48	14.92
TCP-IPv6-LAB005	19.22	20.10	20.77	22.93	23.10	24.48	21.77
UDP-IPv4-LAB001	12.40	13.01	13.40	13.90	14.61	15.82	13.86
UDP-IPv4-LAB003	17.60	18.64	19.50	**21.64**	21.70	22.68	20.29
UDP-IPv4-LAB005	28.40	28.84	29.34	29.50	31.87	**35.40**	30.56
UDP-IPv6-LAB001	10.71	**11.94**	12.01	12.60	13.70	14.30	12.54
UDP-IPv6-LAB003	14.70	15.34	15.81	16.70	17.60	**19.40**	16.59
UDP-IPv6-LAB005	21.00	23.20	**24.09**	25.15	25.92	26.85	24.37

The maximum differences							MAX	Percentage	
UDP-LA001 vs. TCP-LAB001	0.53	0.80	0.64	0.95	**1.01**	0.98	1.01	6.91%	IPv4
UDP-LA003 vs. TCP-LAB003	1.80	2.54	1.88	**3.60**	3.20	2.01	3.60	16.64%	IPv4
UDP-LA005 vs. TCP-LAB005	5.00	4.99	4.64	3.58	5.06	**5.65**	5.65	15.96%	IPv4
UDP-LA001 vs. TCP-LAB001	0.90	**1.34**	0.50	0.50	0.50	0.36	1.34	11.22%	IPv6
UDP-LA003 vs. TCP-LAB003	1.80	0.91	0.99	1.60	1.83	**2.92**	2.92	15.05%	IPv6
UDP-LA005 vs. TCP-LAB005	1.78	3.10	**3.32**	2.22	2.82	2.37	3.32	13.78%	IPv6

Comparesion between TCP vs. UDP			
UDP-LA001 vs. TCP-LAB001	0.82	5.91	IPv4
UDP-LA003 vs. TCP-LAB003	2.51	12.34	
UDP-LA005 vs. TCP-LAB005	4.82	15.77	
UDP-LA001 vs. TCP-LAB001	0.68	5.45	IPv6
UDP-LA003 vs. TCP-LAB003	1.68	10.10	
UDP-LA005 vs. TCP-LAB005	2.60	10.67	

The following tables show the results of TCP and UDP round trip time for the third experimental scenario. The results are represented in milliseconds.

TCP RTT

Packet Size (Bytes)	128	384	640	896	1152	1408	AVR
IPv4 - LAB001	0.50	1.46	2.33	3.21	3.93	4.40	2.64
IPv4 - LAB003	0.38	1.11	1.69	2.30	2.89	3.16	1.92
IPv4 - LAB005	0.20	0.75	1.25	1.60	1.99	2.20	1.33
IPv6 - LAB001	0.61	1.68	2.78	3.44	4.05	4.69	2.87
IPv6 - LAB003	0.46	1.23	2.10	2.65	3.39	3.96	2.30
IPv6 - LAB005	0.31	0.89	1.43	1.71	2.31	2.87	1.59

The maximum differences							MAX	Persentage	
IPv4 vs. IPv6	-0.11	-0.22	-0.45	-0.23	-0.12	-0.28	-0.45	16.19%	LAB001
IPv4 vs. IPv6	-0.08	-0.13	-0.42	-0.35	-0.50	-0.80	-0.80	20.20%	LAB003
IPv4 vs. IPv6	-0.11	-0.14	-0.18	-0.11	-0.32	-0.67	-0.67	23.34%	LAB005
LA005 vs. LAB003	-0.17	-0.36	-0.43	-0.70	-0.90	-0.96	-0.96	30.38%	IPv4
LA005 vs. LAB001	-0.30	-0.71	-1.08	-1.61	-1.94	-2.21	-2.21	50.22%	
LA003 vs. LAB001	-0.12	-0.35	-0.64	-0.91	-1.04	-1.24	-1.24	28.18%	
LA005 vs. LAB003	-0.15	-0.35	-0.67	-0.94	-1.08	-1.10	-1.10	27.78%	IPv6
LA005 vs. LAB001	-0.30	-0.79	-1.35	-1.72	-1.74	-1.82	-1.82	38.81%	
LA003 vs. LAB001	-0.15	-0.45	-0.68	-0.78	-0.66	-0.72	-0.78	22.67%	

Comparesion between lab001-lab003-lab005				Comparesion between ipv4 vs. ipv6			
LA005 vs. LAB003	-0.59	-30.60	IPv4	IPv4 vs. IPv6	-0.23	-8.17	LAB001
LA005 vs. LAB001	-1.31	-49.48		IPv4 vs. IPv6	-0.38	-16.54	LAB003
LA003 vs. LAB001	-0.72	-27.21		IPv4 vs. IPv6	-0.25	-16.01	LAB005
LA005 vs. LAB003	-0.71	-31.04	IPv6				
LA005 vs. LAB001	-1.29	-44.77					
LA003 vs. LAB001	-0.57	-19.91					

UDP RTT

Packet Size (Bytes)	128	384	640	896	1152	1408	AVR
IPv4 - LAB001	0.48	1.37	2.32	2.69	3.66	4.13	2.44
IPv4 - LAB003	0.34	0.96	1.32	1.92	2.66	2.88	1.68
IPv4 - LAB005	0.21	0.62	1.01	1.48	1.68	1.85	1.14
IPv6 - LAB001	0.75	1.49	2.47	3.20	3.99	4.26	2.69
IPv6 - LAB003	0.40	1.16	1.78	2.59	3.04	3.37	2.06
IPv6 - LAB005	0.28	0.85	1.23	1.65	1.97	2.38	1.39

The maximum differences							MAX	Persentage	
IPv4 vs. IPv6	-0.27	-0.12	-0.16	-0.51	-0.33	-0.13	-0.51	15.94%	LAB001
IPv4 vs. IPv6	-0.07	-0.21	-0.46	-0.67	-0.37	-0.49	-0.67	25.87%	LAB003
IPv4 vs. IPv6	-0.07	-0.23	-0.22	-0.17	-0.29	-0.53	-0.53	22.27%	LAB005
LA005 vs. LAB003	-0.13	-0.34	-0.31	-0.44	-0.99	-1.04	-1.04	48.61%	IPv4
LA005 vs. LAB001	-0.27	-0.75	-1.30	-1.21	-1.98	-2.28	-2.28	55.21%	
LA003 vs. LAB001	-0.14	-0.41	-0.99	-0.77	-1.00	-1.25	-1.25	30.27%	
LA005 vs. LAB003	-0.12	-0.31	-0.55	-0.94	-1.07	-0.99	-1.07	35.20%	IPv6
LA005 vs. LAB001	-0.47	-0.64	-1.24	-1.55	-2.02	-1.88	-2.02	50.63%	
LA003 vs. LAB001	-0.35	-0.33	-0.69	-0.61	-0.95	-0.89	-0.95	23.81%	

Comparesion between lab001-lab003-lab005				Comparesion between ipv4 vs. ipv6			
LA005 vs. LAB003	-0.54	-32.13	IPv4	IPv4 vs. IPv6	-0.25	-9.41	LAB001
LA005 vs. LAB001	-1.30	-53.28		IPv4 vs. IPv6	-0.38	-18.29	LAB003
LA003 vs. LAB001	-0.76	-31.16		IPv4 vs. IPv6	-0.25	-18.24	LAB005
LA005 vs. LAB003	-0.66	-32.17	IPv6				
LA005 vs. LAB001	-1.30	-48.23					
LA003 vs. LAB001	-0.64	-23.67					

TCP and UDP RTT

Packet Size (Bytes)	128	384	640	896	1152	1408	AVR
TCP-IPv4-LAB001	0.500	1.459	2.327	**3.210**	3.930	4.402	2.64
TCP-IPv4-LAB003	0.376	1.107	1.685	**2.305**	2.889	3.161	1.92
TCP-IPv4-LAB005	0.204	0.747	1.252	1.604	1.994	**2.196**	1.33
TCP-IPv6-LAB001	0.605	1.681	2.780	3.436	4.049	**4.687**	2.87
TCP-IPv6-LAB003	0.460	1.235	2.104	2.653	3.390	**3.964**	2.30
TCP-IPv6-LAB005	0.309	0.886	1.430	1.713	2.314	**2.869**	1.59
UDP-IPv4-LAB001	0.479	1.370	2.316	2.691	3.659	4.130	2.44
UDP-IPv4-LAB003	0.337	0.956	1.323	1.921	2.663	2.881	1.68
UDP-IPv4-LAB005	0.209	0.618	1.012	1.480	1.677	1.846	1.14
UDP-IPv6-LAB001	0.750	1.492	2.473	3.200	3.990	4.260	2.69
UDP-IPv6-LAB003	0.404	1.162	1.778	2.589	3.037	3.368	2.06
UDP-IPv6-LAB005	0.283	0.850	1.233	1.653	1.970	2.380	1.39

The maximum differences							MAX	Percentage	
UDP-LA001 vs. TCP-LAB001	-0.021	-0.090	-0.011	**-0.519**	-0.272	-0.273	-0.519	16.20%	IPv4
UDP-LA003 vs. TCP-LAB003	-0.038	-0.151	-0.362	**-0.383**	-0.226	-0.280	-0.383	16.52%	IPv4
UDP-LA005 vs. TCP-LAB005	0.005	-0.129	-0.240	-0.124	-0.317	**-0.350**	-0.350	15.91%	IPv4
UDP-LA001 vs. TCP-LAB001	0.145	-0.189	-0.307	-0.236	-0.059	**-0.427**	-0.427	9.17%	IPv6
UDP-LA003 vs. TCP-LAB003	-0.056	-0.073	-0.325	-0.064	-0.352	**-0.597**	-0.597	15.15%	IPv6
UDP-LA005 vs. TCP-LAB005	-0.026	-0.036	-0.197	-0.060	-0.344	**-0.489**	-0.489	17.07%	IPv6

Comparesion between TCP vs. UDP			
UDP-LA001 vs. TCP-LAB001	-0.20	-7.49	IPv4
UDP-LA003 vs. TCP-LAB003	-0.24	-12.51	
UDP-LA005 vs. TCP-LAB005	-0.19	-14.44	
UDP-LA001 vs. TCP-LAB001	-0.18	-6.23	IPv6
UDP-LA003 vs. TCP-LAB003	-0.24	-10.63	
UDP-LA005 vs. TCP-LAB005	-0.19	-12.10	

The following tables show the results of TCP and UDP CPU usage for the third experimental scenario. The results are represented in percentage.

TCP CPU usage

Packet Size (Bytes)	128	384	640	896	1152	1408	AVR
IPv4 - LAB001	7.42	7.31	7.14	6.86	6.78	6.60	7.02
IPv4 - LAB003	6.61	6.47	6.35	6.24	6.12	5.92	6.29
IPv4 - LAB005	5.76	5.65	5.63	5.50	5.36	4.92	5.47
IPv6 - LAB001	8.15	8.08	7.85	7.78	7.54	7.21	7.77
IPv6 - LAB003	6.94	6.70	6.55	6.38	6.19	6.01	6.46
IPv6 - LAB005	6.29	6.13	6.00	5.87	5.73	5.18	5.86

The maximum differences							MAX	Persentage	
IPv4 vs. IPv6	-0.73	-0.77	-0.71	-0.92	-0.76	-0.61	-0.92	11.83%	LAB001
IPv4 vs. IPv6	-0.33	-0.23	-0.20	-0.14	-0.07	-0.09	-0.33	4.76%	LAB003
IPv4 vs. IPv6	-0.53	-0.48	-0.37	-0.37	-0.37	-0.26	-0.53	8.43%	LAB005
LA005 vs. LAB003	-0.85	-0.82	-0.72	-0.74	-0.76	-1.00	-1.00	16.89%	
LA005 vs. LAB001	-1.66	-1.66	-1.51	-1.36	-1.42	-1.68	-1.68	25.45%	IPv4
LA003 vs. LAB001	-0.81	-0.84	-0.79	-0.62	-0.66	-0.68	-0.84	11.49%	
LA005 vs. LAB003	-0.66	-0.58	-0.56	-0.52	-0.47	-0.83	-0.83	13.81%	
LA005 vs. LAB001	-1.87	-1.96	-1.86	-1.92	-1.82	-2.03	-2.03	28.15%	IPv6
LA003 vs. LAB001	-1.21	-1.38	-1.30	-1.40	-1.35	-1.20	-1.40	17.99%	

Comparesion between lab001-lab003-lab005				Comparesion between ipv4 vs. ipv6			
LA005 vs. LAB003	-0.82	-12.99		IPv4 vs. IPv6	-0.75	-9.65	LAB001
LA005 vs. LAB001	-1.55	-22.08	IPv4	IPv4 vs. IPv6	-0.18	-2.73	LAB003
LA003 vs. LAB001	-0.73	-10.45		IPv4 vs. IPv6	-0.39	-6.72	LAB005
LA005 vs. LAB003	-0.60	-9.27					
LA005 vs. LAB001	-1.91	-24.53	IPv6				
LA003 vs. LAB001	-1.31	-16.82					

UDP CPU usage

Packet Size (Bytes)	128	384	640	896	1152	1408	AVR
IPv4 - LAB001	6.81	6.76	6.69	6.48	6.36	6.31	6.57
IPv4 - LAB003	6.50	6.34	6.21	6.01	5.84	5.69	6.10
IPv4 - LAB005	5.84	5.38	5.25	5.12	4.98	4.73	5.22
IPv6 - LAB001	7.91	7.76	7.59	7.26	7.12	6.72	7.39
IPv6 - LAB003	6.67	6.51	6.41	6.30	6.10	5.91	6.32
IPv6 - LAB005	6.14	5.98	5.85	5.64	5.58	5.24	5.74

The maximum differences							MAX	Persentage	
IPv4 vs. IPv6	-1.10	-1.00	-0.90	-0.78	-0.76	-0.41	-1.10	13.91%	LAB001
IPv4 vs. IPv6	-0.17	-0.17	-0.20	-0.29	-0.26	-0.22	-0.29	4.60%	LAB003
IPv4 vs. IPv6	-0.29	-0.59	-0.59	-0.52	-0.59	-0.51	-0.59	10.57%	LAB005
LA005 vs. LAB003	-0.66	-0.96	-0.96	-0.89	-0.86	-0.96	-0.96	16.87%	
LA005 vs. LAB001	-0.97	-1.38	-1.44	-1.36	-1.38	-1.58	-1.58	25.04%	IPv4
LA003 vs. LAB001	-0.31	-0.42	-0.48	-0.47	-0.52	-0.62	-0.62	9.83%	
LA005 vs. LAB003	-0.53	-0.53	-0.56	-0.66	-0.52	-0.67	-0.67	11.34%	
LA005 vs. LAB001	-1.77	-1.78	-1.74	-1.62	-1.54	-1.48	-1.78	22.94%	IPv6
LA003 vs. LAB001	-1.24	-1.25	-1.18	-0.96	-1.02	-0.81	-1.25	16.11%	

Comparesion between lab001-lab003-lab005				Comparesion between ipv4 vs. ipv6			
LA005 vs. LAB003	-0.88	-14.42		IPv4 vs. IPv6	-0.82	-11.16	LAB001
LA005 vs. LAB001	-1.35	-20.55	IPv4	IPv4 vs. IPv6	-0.22	-3.46	LAB003
LA003 vs. LAB001	-0.47	-7.16		IPv4 vs. IPv6	-0.52	-9.02	LAB005
LA005 vs. LAB003	-0.58	-9.19					
LA005 vs. LAB001	-1.66	-22.41	IPv6				
LA003 vs. LAB001	-1.08	-14.56					

TCP and UDP CPU usage

Packet Size (Bytes)	128	384	640	896	1152	1408	AVR
TCP-IPv4-LAB001	7.42	7.31	7.14	6.86	6.78	6.60	**7.02**
TCP-IPv4-LAB003	6.61	6.47	6.35	6.24	6.12	5.92	**6.29**
TCP-IPv4-LAB005	5.76	5.65	5.63	5.50	5.36	4.92	**5.47**
TCP-IPv6-LAB001	8.15	8.08	7.85	7.78	7.54	7.21	**7.77**
TCP-IPv6-LAB003	6.94	6.70	6.55	6.38	6.19	6.01	**6.46**
TCP-IPv6-LAB005	6.29	6.13	6.00	5.87	5.73	5.18	**5.86**
UDP-IPv4-LAB001	6.81	6.76	6.69	6.48	6.36	6.31	**6.57**
UDP-IPv4-LAB003	6.50	6.34	6.21	6.01	5.84	5.69	**6.10**
UDP-IPv4-LAB005	5.84	5.38	5.25	5.12	4.97	4.73	**5.22**
UDP-IPv6-LAB001	7.91	7.76	7.59	7.26	7.12	6.72	**7.39**
UDP-IPv6-LAB003	6.67	6.51	6.41	6.30	6.10	5.91	**6.32**
UDP-IPv6-LAB005	6.14	5.98	5.85	5.64	5.58	5.24	**5.74**

The maximum differences							MAX	
UDP-LA001 vs. TCP-LAB001	**-0.610**	-0.550	-0.450	-0.380	-0.420	-0.290	-0.610	IPv4
UDP-LA003 vs. TCP-LAB003	-0.110	-0.130	-0.140	-0.230	**-0.280**	-0.230	-0.280	IPv4
UDP-LA005 vs. TCP-LAB005	0.082	-0.268	-0.375	-0.375	**-0.385**	-0.188	-0.385	IPv4
UDP-LA001 vs. TCP-LAB001	-0.240	-0.320	-0.260	-0.520	-0.420	-0.490	-0.520	IPv6
UDP-LA003 vs. TCP-LAB003	-0.270	-0.190	-0.140	-0.080	-0.090	-0.100	-0.270	IPv6
UDP-LA005 vs. TCP-LAB005	-0.148	-0.148	-0.148	-0.225	-0.148	0.060	-0.225	IPv6

Comparesion between TCP vs. UDP			
UDP-LA001 vs. TCP-LAB001	**-0.45**	**-6.41**	IPv4
UDP-LA003 vs. TCP-LAB003	**-0.19**	**-2.97**	
UDP-LA005 vs. TCP-LAB005	**-0.25**	**-4.60**	
UDP-LA001 vs. TCP-LAB001	**-0.38**	**-4.83**	IPv6
UDP-LA003 vs. TCP-LAB003	**-0.14**	**-2.24**	
UDP-LA005 vs. TCP-LAB005	**-0.13**	**-2.15**	

REFERENCES

[1] PR Newswire Association. (2014). *The evolving connected device universe: 12 technology innovations for 2015* [Online]. Available: http://search.proquest.com/docview/1636533029?accountid=142908.

[2] ABI research. (2012). *Wireless connectivity market data* [Online]. Available: https://www.abiresearch.com/market-research/product/1014046-wireless-connectivity/

[3] G.R. Hiertz, D. Denteneer, L. Stibor, Y. Zang, X.P. Costa, B. Walke, "The IEEE 802.11 universe," *IEEE Communications Magazine*, vol. 48, no. 1, pp. 62 - 70, January 2010.

[4] A. H. Lashkari, M. M. S. Danesh, and B. Samadi, "A survey on wireless security protocols (WEP, WPA and WPA2/802.11i)," in 2nd IEEE International Conference on Computer Science and Information Technology (ICCSIT '09), Beijing, China, 8-11 Aug. 2009, 48 - 52.

[5] H. Hongwei, S. Wei, X. Youzhi, and Z. Hongke, "The effect of human activities on 2.4 GHz radio propagation at home environment," in 2nd IEEE International Conference on Broadband Network & Multimedia Technology (IC-BNMT'09), Beijing, China, 18 - 20 Oct. 2009, pp. 95 - 99.

[6] A. N. A. Ali, "Comparison study between IPv4 & IPv6," *International Journal of Computer Science Issues (IJCSI)*, vol. 9, no. 3, pp. 314 - 317, May 2012.

[7] T. A. Radaei, and Z. A. Zukarnain, "Comparison study of Transmission Control Protocol and User Datagram Protocol behavior over Multi-Protocol Label Switching Networks in case of failures," *Journal of Computer Science*, vol. 5, no. 12, pp. 1042 - 1047, 2009.

[8] S. Narayan, C. Jayawardena, Jiaxin Wang, Weizhi Ma, and G. Geetu, "Performance test of IEEE 802.11ac wireless devices," in International Conference on Computer Communication and Informatics (ICCCI'15), Coimbatore, India, 8-10 January 2015, pp. 1 - 6.

[9] Y. Zeng, P. H. Pathak, and P. Mohapatra, "Throughput, energy efficiency and interference characterisation of 802.11ac," Transactions on Emerging Telecommunications Technologies, 13 May 2015, doi: 10.1002/ett.2946.

[10] R. S Cheng, "Performance evaluation of stream control transport protocol over IEEE 802.11ac networks," IEEE Wireless Communications and Networking Conference Workshops (WCNCW'15), New Orleans, LA, 9-12 March 2015, pp. 97 - 102.

[11] F. Siddiqui, S. Zeadally, and K. Salah, "Gigabit Wireless Networking with IEEE 802.11ac: technical overview and challenges," *Journal of Networks*, vol. 10, no. 3, pp. 164 - 171, Apr. 2015.

[12] M. D. Dianu, J. Riihijarvi, and M. Petrova, "Measurement-based study of the performance of IEEE 802.11ac in an indoor environment," in IEEE International Conference on Communications (ICC'14), Sydney, Australia, 10-14 June 2014, pp. 5771 - 5776.

[13] M. O. Demir, G.K. Kurt, and M. Karaca, "An energy consumption model for 802.11ac access points," in 22nd International Conference on Software, Telecommunications and Computer Networks (SoftCOM'14), Split, Croatia, 17-19 Sept. 2014, pp. 67 - 71.

[14] G. Patwardhan, and D. Thuente, "Jamming Beamforming: a new Attack vector in Jamming IEEE 802.11ac Networks," in IEEE Military Communications Conference (MILCOM'14), Baltimore, USA, 6-8 Oct. 2014, pp. 1534 - 1541.

[15] A. Stelter, P. Szulakiewicz, R. Kotrys, M. Krasicki, and P. Remlein, "Dynamic 20/40/60/80MHz Channel Access for 80MHz 802.11ac," *Wireless Personal Communications journal*, vol. 79, no. 1, pp. 235 - 248, November 2014.

[16] P. Minyoung, "IEEE 802.11ac: Dynamic bandwidth channel access," in IEEE International Conference on Communications (ICC'11), Kyoto, Japan, 5-9 June 2011, pp. 1 - 5.

[17] E. H. Ong, J. Kneckt, O. Alanen, Z. Chang, T. Huovinen, and T. Nihtila, "IEEE 802.11ac: Enhancements for very high throughput WLANs," in IEEE 22nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC'11), Toronto, Canada, 11-14 Sept. 2011, pp. 849 - 853.

[18] N. I. Sarkar, and O. Mussa, "The effect of people movement on Wi-Fi link throughput in indoor propagation environments," in IEEE TENCON Spring Conference, Sydney, Australia, 17-19 April 2013, pp. 562 - 566.

[19] S. Japertas, E. Orzekauskas, and R. Slanys, "Research of IEEE 802.11 standard signal propagation features in multi partition indoors," in Second International Conference on Digital Information Processing and Communications (ICDIPC'12), Klaipeda City, Lithuania, 10-12 July 2012, pp. 1 - 4.

[20] S. S. Kolahi, Peng Li, M. Argawe, and M. Safdari, "WPA2 security-bandwith trade-off in 802.11n peer-peer WLAN for IPv4 and IPv6 using Windows XP and Windows 7 operating systems," in IEEE Symposium on Computers and Communications (ISCC'12), Cappadocia, Turkey, 1-4 July 2012, pp. 1530-1346.

[21] S. S. Kolahi, H. Singla, M.N. Ehsan, and C. Dong, " The influence of WPA2 security on the UDP performance of IPv4 and IPv6 using 802.11n WLAN in Windows 7-Windows 2008 environment," in Baltic Congress on Future Internet Communications (BCFIC'11), Riga, Latvia, 16-18 Feb 2011, pp. 50 – 53.

[22] S. S. Kolahi, Zhang Qu, B. K. Soorty, and N. Chand, " The Impact of security on the performance of IPv4 and IPv6 using 802.11n Wireless LAN," in 3rd International Conference on New Technologies, Mobility and Security (NTMS'09), Cairo, Egypt, 20-23 Dec 2009, pp. 1 – 4.

[23] E. J. M. Filho, P. N. L. Fonseca, M. J. S. Leitao, and P. S. F. Barros, " Security versus Bandwidth: the support of mechanisms WEP e WPA in 802.11g Network," in IFIP International Conference on Wireless and Optical Communications Networks (WOCN'07), Singapore, 2-4 July 2007, pp. 1 – 5.

[24] B. Ezedin, M. Boulmalf, A. Alteniji, H. Al Suwaidi, H. Khazaimy, and M. Al Mansouri, "Impact of security on the performance of Wireless-Local Area Networks," in Conference on Innovations in Information Technology, Dubai, AUE, Nov. 2006, pp. 1 – 5.

[25] J. Berg. *The IEEE 802.11 Standardization Its history specifications, implementations, and future* (*Technical report series, George Mason University*) [Online]. Available: http://telecom.gmu.edu/sites/default/files/publications/Berg_802.11_GMU-TCOM-TR-8.pdf

[26] M. J. Ho, M. S. Rawles, M. Vrijkorte, and L. Fei, "RF challenges for 2.4 and 5 GHz WLAN deployment and design," in Wireless Communications and Networking Conference (WCNC'02), Orlando, USA, Mar. 2002, 783 - 788 vol.2

[27] A. Doefexi, S. Armour, L. Beng-Sin, A. Nix, and D. Bull, " An evaluation of the performance of IEEE 802.11a and 802.11g wireless local area networks in a corporate office environment," in IEEE International Conference on Communications (ICC'03) Anchorage, AK, 11 - 15 May 2003, pp. 1196 - 1200 vol.2.

[28] E. Perahia, "IEEE 802.11n development: history, process, and technology," *IEEE Communications Magazine*, vol. 46, no. 7, pp. 48 - 55, July 2008.

[29] Aruba Networks. (2015, Feb. 18). *802.11ac in-depth white paper* [Online]. Available: http://www.arubanetworks.com/pdf/technology/whitepapers/WP_80211acInDepth.pdf?_ga=1.105319942.460286927.1442720395

[30] T. Nitsche, C. Cordeiro, A.B. Flores, E.W. Knightly, E. Perahia, and J.C. Widmer, "IEEE 802.11ad: directional 60 GHz communication for multi-Gigabit-per-second Wi-Fi," *IEEE Communications Magazine*, vol. 52, no. 12, pp. 132 - 141, December 2014.

[31] E. Perahia and R. Stacey, "Next Generation Wireless LANS: 802.11 n and 802.11 ac," vol. 2, London: Cambridge university press, 2013.

[32] B. P. Crow, I. Widjaja, J. G. Kim, and P. T. Sakai, "IEEE 802.11 Wireless Local Area Networks," *IEEE Communications Magazine*, vol. 35, no. 9, pp. 116 - 126, Sep 1997.

[33] T. Socolofsky, and C. Kale. (1991, Jan.). *TCP/IP tutorial, The RFC series (ISSN 2070-1721)* [Online]. Available: https://www.rfc-editor.org/rfc/rfc1180.txt

[34] J. Crenne, B. Pierre, G. Guy and D. J. Philippe, "End-to-end bitstreams repository hierarchy for FPGA partially reconfigurable systems," in *Algorithm-Architecture Matching for Signal and Image Processing*, vol. 73, Springer Netherlands, 2011, pp. 171 - 194.

[35] S. Medidi, J. Ding, and M. Medidi, "Performance of Transport Protocols in Wireless Networks," in Annual Review of Communications vol. 59 , 2007, pp. 295 - 301.

[36] H. M. O. Chughtai, S. A. Malik, and M. Yousaf, "Performance evaluation of transport layer protocols for video traffic over WiMax," in IEEE 13th International Multitopic Conference (INMIC'09), Islamabad, Pakistan, 14-15 Dec. 2009, pp. 1 - 6.

[37] H. RiLi, "Research and application of TCP/IP protocol in embedded system," in IEEE 3rd International Conference on Communication Software and Networks (ICCSN'11), Xi'an, China, 27-29 May 2011, pp. 584 - 587.

[38] T. Nguyen, M. Park, Y. Youn, and S. Jung, "An improvement of TCP performance over wireless networks," in Fifth International Conference on Ubiquitous and Future Networks (ICUFN'13), Da Nang, Vietnam, 2-5 July 2013, pp. 214 - 219.

[39] S. Kumar, and S. Rai, "Survey on Transport Layer Protocols: TCP & UDP," *International Journal of Computer Applications*, vol. 46, no. 7, pp. 20 - 25, May 2012.

[40] P. M. Miller, "TCP/IP - The ultimate protocol guide: complete 2 volume set", vol. 2, USA: Brown Walker Press (FL), 2010.

[41] M. K. Sailan, R. Hassan, and A. Patel, "A comparative review of IPv4 and IPv6 for research test bed," in International Conference on Electrical Engineering and Informatics (ICEEI'09), Selangor, Malaysia, 5-7 Aug. 2009, pp. 427 - 433.

[42] S. Dutta, P. K. Mishra, G. M. Prasad, S. Shukla, and S. K. Chaulya, "Internet Protocols: IPv4 vis a vis IPv6," *Asian Journal of Information Technology*, vol. 11, no. 3, pp. 100 - 107, 2012.

[43] W. Stallings, "IPv6: the new Internet protocol," *IEEE Communications Magazine*, vol. 34, no. 7, pp. 96 - 108, Jul. 1996.

[44] D. Johnson, C. Perkins, and J. Arkko. (2004, Jun.). *Mobility support in IPv6, The RFC series (ISSN 2070-1721)* [Online]. Available: https://www.rfc-editor.org/rfc/pdfrfc/rfc3775.txt.pdf

[45] T. Narten, E. Nordmark, W. Simpson, and H. Soliman. (2007, Sep.). *Neighbor Discovery for IP version 6 (IPv6), RFC 4861* [Online]. Available: http://tools.ietf.org/html/rfc4861

[46] L. Staalhagen, "A comparison between the OSI reference model and the B-ISDN protocol reference model," *IEEE Network Magazine*, vol. 10, no. 1, pp. 24 - 33, Jan/Feb 1996.

[47] P. Chatzimisios, A. C. Boucouvalas, and V. Vitsas, "Performance analysis of the IEEE 802.11 MAC protocol for wireless LANs," *International Journal of Communication Systems*, vol. 18, no. 6, pp. 545–569, August 2005.

[48] H. Manshaei, G. R. Cantieni, C. Barakat, and T. Turletti, " Performance analysis of the IEEE 802.11 MAC and physical layer protocol," in Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM'05), Taormina-Giardini Naxos, Italy, 13-16 June 2005, pp. 88 - 97.

[49] A. Nisbet, "A tale of four cities: Wireless security & growth in New Zealand," in International Conference on Computing, Networking and Communications (ICNC'12), Maui, Hawaii, Jan. 30 2012-Feb. 2 2012, pp. 1167 - 1171.

[50] A. H. Lashkari, M. Mansoor, and A. S. Danesh, "Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA)," in International Conference on Signal Processing Systems, Singapore, 15-17 May 2009, pp. 445 - 449.

[51] S. S. Kolahi, Peng Li, M. Argawe, and M. Safdari, "Effect of WPA2 Security on IEEE 802.11n Bandwith and Round Trip Time in Peer-Peer Wireless Local Area Networks," in IEEE Workshops of International Conference on Advanced Information Networking and Applications (WAINA'11), Biopolis, Singapore, 22-25 March 2011, pp. 777 - 782.

[52] A. D. Potorac, and D. Balan, "The Impact of security overheads on 802.11 WLAN throughput," *Journal of Computer Science and Control Systems*, vol. 1, no. 1, pp. 47 – 52, Jan. 2009.

[53] A. H. Ali, M. R. A. Razak, M. Hidayab, S. A. Azman, M. Z. M. Jasmin, and M. A. Zainol, "Investigation of indoor WIFI radio signal propagation," in IEEE Symposium on Industrial Electronics & Applications (ISIEA'10), Penang, Malaysia, 3-5 Oct. 2010, pp. 117 - 119.

[54] Stein, and C. John. (1998). *Indoor radio WLAN performance part II: Range performance in a dense office environment (Intersil Corporation, 2401, Palm Bay, Florida, pp. 1 – 9)* [Online]. Available: http://erasme.org/IMG/experience_attenuation.pdf

[55] W. Rummler, R. P. Coutts, and M. Liniger, "Multipath fading channel models for microwave digital radio," *IEEE Communications Magazine*, vol. 24, no. 11, pp. 30 - 42, November 1986.

[56] W. C. O'Reilly, and R. T. Guza, "Comparison of spectral refraction and refraction-diffraction wave models," *Journal of Waterway, Port, Coastal, and Ocean Engineering*, vol. 117, no. 3, pp. 30 - 42, May 1991.

[57] ccmbenchmark. (2014, Jun.). *Propagation of radio waves (802.11)* [Online]. Available: http://ccm.net/contents/832-propagation-of-radio-waves-802-11

[58] ABI research. (2015). *802.11ac Wi-Fi CPE shipments to accelerate in 2015 to reach 71 million units (Telecommunications Weekly pp. 49)* [Online]. Available: http://search.proquest.com/docview/1676807618?accountid=142908

[59] Gast, and S. Matthew, "802.11 ac: A survival guide," vol. 1, O'Reilly Media, Inc., 2013.

[60] IEEE 802.11 WG, part 11a/11b/11g, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications,” Standard Specification, IEEE, 1999. Del

[61] V. Valls, and D. J. Leith, "Multipath fading channel models for microwave digital radio," *IEEE Wireless Communications Letters*, vol. 3, no. 2, pp. 221 - 224, April 2014.

[62] G. Redieteab, L. Cariou, P. Christin, and J. -F. Helard, "PHY+MAC channel sounding interval analysis for IEEE 802.11ac MU-MIMO," in International Symposium on Wireless Communication Systems (ISWCS'12), Paris, France, 128-31 Aug. 2012, pp. 1054 - 1058.

[63] O. Bejarano, E. W. Knightly, and M. Park, "IEEE 802.11 ac: from channelization to multi-user MIMO," *IEEE Communications Magazine*, vol. 51, no. 10, pp. 84 - 90, 2013.

[64] R. van Nee, "Breaking the Gigabit-per-second barrier with 802.11AC," *IEEE Wireless Communications Magazine*, vol. 18, no. 2, pp. 4, April 2011.

[65] D. Larsson, J. F. Cheng, Y. Yang, and M. Wang. (2015). *256 Quadrature amplitude modulation user equipment category handling (U.S. Patent No. 20,150,296,503. Washington, DC: U.S. Patent and Trademark Office)* [Online]. Available: http://www.freepatentsonline.com/20150296503.pdf

[66] G. Redieteab, L. Cariou, P. Christin, J.-F. Helard, " SU/MU-MIMO in IEEE 802.11ac: PHY+MAC performance comparison for single antenna stations," in Wireless Telecommunications Symposium (WTS'12), London, UK, 18-20 April 2012, pp. 1 – 5.

[67] M. X. Gong, B. Hart, and S. Mao, "Advanced Wireless LAN technologies: IEEE 802.11 ac and beyond," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 18, no. 4, pp. 48 - 52, 2015.

[68] G. Barczak, "Publishing qualitative versus quantitative research," *Journal of Product Innovation Management*, vol. 32, no. 5, pp. 221 - 224, 26 JUL 2015.

[69] R. Blum, "Network performance open source toolkit: using Netperf, tcptrace, NISTnet, and SSFNet," vol. 2, John Wiley & Sons, 2003.

[70] M. Chen, H. Bai, Y. Zhou, Z. Wang, and P. Jiang, "A novel network performance evaluation method based on maximizing deviations," in Telecommunication Systems, Springer, January 2014, pp. 149 - 158.

[71] E. Goturk, "Emulating ad hoc networks: differences from simulations and emulation specific problems," in New Trends in Computer Networks, imperial college press, January 2005, pp. 329.

[72] E. Göktürk, "A stance on emulation and testbeds, and a survey of network emulators and testbeds", Proceedings of ECMS, 13. Chicago, 2007.

[73] G. Judd, and P. Steenkiste, "Using emulation to understand and improve wireless networks and applications," in 2nd conference on Symposium on Networked Systems Design & Implementation, Berkeley, USA, May 2005, pp. 203 - 216.

[74] M. Imran, A. M. Said, and H. Hasbullah, "A survey of simulators, emulators and testbeds for wireless sensor networks," in International Symposium in Information Technology (ITSim'10), Kuala Lumpur, Malaysia, 15-17 June 2010, pp. 897 - 902. vol.2.

[75] S. K. Tripathi, Y. Huang, and S. Jajodia, "Local Area Networks: software and related Issues," *IEEE Transactions on Software Engineering*, vol. 13, no. 8, pp. 872 - 879, Aug. 1987.

[76] S. Narayan, D. Graham, and R. H. Barbour, "Generic factors influencing optimal LAN size for commonly used operating systems maximized for network performance," *IJCSNS International Journal of Computer Science and Network Security*, vol. 9, no. 6, pp. 63 - 72, June 2009.

[77] L. Isaksson, S. Chevul, and M. Fiedler, "Application-perceived throughput process in wireless systems," in IEEE Systems Communications, 14-17 Aug. 2005, pp. 172 - 177.

[78] Cisco Systems. (2008, Oct. 30). *Troubleshooting high CPU utilization* [Online]. Available: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/troubleshooting/cpu_util.html.

[79] B. Constantine, G. Forget, R. Geib, and R. Schrage. (2011, Aug.). *Framework for TCP throughput testing (The RFC series (6349))* [Online]. Available: http://www.ietf.org/rfc/rfc6349.txt.

[80] Y. Chen, Q. Yang, J. Yin, and X. Chai, "Power-efficient access-point selection for indoor location estimation," *IEEE Transactions on Knowledge and Data Engineering*, vol. 18, no. 7, pp. 877 - 888, July 2006.

[81] Linksys. *LAPAC1750PRO Access Point software user manual (Belkin International)* [Online]. Available: http://downloads.linksys.com/downloads/userguide/1224701939563/MAN_LAPAC1750PRO_LNKPG-00129_RevA00_User_Guide_EN.pdf

[82] Kontakt.io. (2014, Sep. 11). *Beacon Configuration Strategy Guide – Interval* [Online]. Available: http://kontakt.io/blog/beacon-configuration-strategy-guide-interval/

[83] Google code. *Graphical frontend for IPERF written in Java* [Online]. Available: https://code.google.com/p/xjperf/

[84] S. S. Kolahi, S. Narayan, D.D.T. Nguyen, and Y. Sunarto, "Performance monitoring of various network traffic generators," in 13th International Conference on Computer Modelling and Simulation (UKSim'11), Cambridge, March 30 2011-April 1 2011, 501 - 506.

[85] S. Alcock, and R. Nelson. *An analysis of TCP maximum segment sizes* [Online]. Available: http://wand.net.nz/sites/default/files/mss_ict11.pdf

[86] G. Kaiser. (2014, Jul. 24). Understanding application performance on the network – Part VI: The Nagle Algorithm (Dynatrace) [Online]. Available: http://apmblog.dynatrace.com/2014/07/24/understanding-application-performance-on-the-network-the-nagle-algorithm/

[87] R. Jones. (2009). *Welcome to the Netperf homepage* [Online]. Available: http://www.netperf.org/netperf.

[88] J. Gretarsson, F. Li, M. Li, A. Samant, M. Claypool, and R. Kinicki, "Performance analysis of the intertwined effects between network layers for 802.11 g transmissions," in 1st ACM workshop on Wireless multimedia networking and performance modeling (WMuNeP '05), New York, USA, 2005, pp. 123 - 130.

[89] L. Samara. (2013). *inSSIDer for office (PCmag.Com)* [Online]. Available: http://search.proquest.com/docview/1536159649?accountid=142908.

[90] Xiangle Xu. (2012). *Evaluation of wireless network performance in a multi-nodes environment (master's thesis)* [Online]. Available: http://unitec.researchbank.ac.nz/bitstream/handle/10652/1996/Xiangle%20Xu%20MComp.pdf?sequence=1&isAllowed=y.

[91] H. Wen, P. K. Tiwary, and T. Le-Ngoc, "Wireless virtualization," in SpringerBriefs in Computer Science, springer, 29 August 2013.

[92] S. Stavrou, and S. R. Saunders, "Factors influencing outdoor to indoor radio wave propagation," in 12th International Conference on Antennas and Propagation (ICAP' 03), Exeter, UK, 31 March-3 April 2003, pp. 581 – 5852.

[93] C. Hoene, A. Gunther, and A. Wolisz, "Measuring the impact of slow user motion on packet loss and delay over IEEE 802.11b wireless links," in 28th Annual IEEE International Conference on Local Computer Networks (LCN'03), Bonn/Konigswinter, Germany, 20-24 Oct. 2003, pp. 652 - 662.

[94] Linksys. *Linksys LAPAC1750PRO business access point wireless Wi-Fi Dual Band 2.4 + 5GHz AC1750 with PoE (Belkin International)* [Online]. Available: http://www.linksys.com/us/p/P-LAPAC1750PRO/

[95] TP-LINK technologies. *Archer T8E specifications* [Online]. Available:http://www.tp-link.com/lb/products/details/cat-11_Archer-T8E.html#specifications