Impact of Security on Bandwidth and Latency in IEEE 802.11ac Client-to-Server WLAN

Samad S. Kolahi, A. A. Almatrook
Unitec Institute of Technology
skolahi@unitec.ac.nz
abdulbaset.almtrook@gmail.com

***Abstract*- In this paper, wireless 802.11ac client-server network with open system (no security) and WPA2 (Wi-Fi Protected Access 2) security is investigated. The results shows that, by implementing WPA2 security, TCP throughput of IPv4 and IPv6 on average decreased by 16.79% and 10.22% respectively. Throughput for UDP is decreased by 18.07% and 12.99% for IPv4 and IPv6 respectively. For both IPv4 and IPv6, WPA2 wireless security implementation also increases the round trip time (RTT) and CPU Utilization for both TCP and UDP.**

I. INTRODUCTION

Wireless Networking has increased in popularity in the last decade due to the many advantages wireless networking offers. One main advantage is that the users can connect to the local area network or the internet to share resources from anywhere, and anytime. Wireless networking also allows for data communication at locations where it is impossible, difficult, or expensive to use wired infrastructure.

While wireless networking has its advantages, it is less secure than wired networks because of the fact that the data is transmitted in the air. Thus, encryption and security protocols have been developed to mitigate this drawback of wireless networks.

Over the last decade, many wireless devices and products have been developed based on IEEE 802.11 wireless standards. Previous 802.11a/b/g standards are almost obsolete but 80211n is still widely used. IEEE 802.11ac is the latest standards. This standard supports a theoretical throughput of 1.3 Gbps [1]. It is much faster than 802.11n, which provided in practice up to 170 Mbps [8], while it has the theoretical bandwidth in up to 300-500Mbps. The 802.11ac is faster than 802.11n because it uses beamforming technology and bigger channel width [1]. Beamforming detects where devices are and then intensifies the signals in their directions [2]. The 802.11ac channel width increased from a maximum of 40 MHz in 802.11n to 80 MHz or even 160 MHz [2]. As the IEEE 802.11ac is the most recent wireless standard, we will investigate the effect of latest network security protocol (WPA2) using a LAN with this standard.

The WLAN used is in Windows 8-Server 2012 environment. Windows 8.1 has added support for emerging technologies as resolution improvement, 3D printing, Wi-Fi Direct, and Miracast streaming [3]. At the time the research started Windows 8 was the latest windows operating system. IPv6 is the latest version of the internet protocol, which is also known as Next Generation (IPng). This protocol is designed to upgrade and replace the internet version 4 and designed to be forward compatible with the newer devices which come with the most up-to date features. Functions that are generally seen as working in IPv4 were kept in IPv6. Functions that do not work or are infrequently used were removed or made optional. IPv6 supports 128-bit address space and can potentially support 2^{128} unique IP addresses (as opposed to address space of 2^{32} of IPv4). With this large address-space scheme, IPv6 has the capability to provide unique addresses to all devices or node attached to the Internet in foreseeable future [4].

The related works on the impact of wireless LAN security on performance is as follows. In 2004, Baghaei and colleagues [5] conducted a performance evaluation of the effect of implementing security mechanisms on IEEE 802.11b using multiple clients WLANs. This study showed that applying WEP encryption, decreased throughput on average by approximately 86.1% and 54.3% for TCP and UDP when compared to open system network.

In 2006, Ezedin and colleagues [6] investigated the impact of security mechanisms on the performance of IEEE 802.11g WLANs by implementing different WEP encryption keys on TCP and UDP protocols. Results showed that implementing WEP security for key sizes of 64-bit and 128-bit reduced the TCP throughput by 1.9% to 4.5% respectively. For UDP, the throughput reduction was by 0.23% for WEP 64-bit as compared to 6% reduction for WEP 128-bit key.

In 2007, Filho and colleagues [7] conducted a performance evaluation of IEEE 802.11g WLANs by using two security mechanisms with different cryptographic key lengths. Their results showed that WEP-128 reduced TCP throughput by 20% whilst applying WEP-64 decreased the throughput by 8%. Applying WPA encryption had 14% throughput reduction.

In 2009 and 2011, Kolahi and colleagues [8] conducted two studies on the impact of WPA2 security on performance of IPv4 and IPv6 on two client-server wireless 802.11n networks implementing Windows Vista-Windows Server 2008 and Windows XP-Windows Server 2008. Results, indicated for both Windows XP and Vista, enabling WPA2 resulted in less throughput than open systems for both IPv4 and IPv6.

In 2011, Li and colleagues [9] evaluated the performance of IEEE 802.11n Wi-Fi peer-peer network for both IPv4 and IPv6 by applying WPA2 security mechanism. Their results for Windows 7 showed that the TCP throughput with WPA2 security decreased by 6.21% (IPv4) and 3.11% (IPv6). In contrast, the TCP throughput with WPA2 security for Fedora 12 declined by 5.55% (IPv4) and 3.8% (IPv6).

Further work was done by Kolahi and colleagues [10. 11,12] on the impact of security on performance in 802.11n WLANs environment using both client server and peer-peer networks for Windows XP and Windows 7. These studies also showed security degrades performance in terms of bandwidth and delay.

To the author's knowledge, there is no research to date in the literature on studying WPA2 security-bandwidth trade-off on client-server (Windows 8.1-Windows Server 2012) using latest wireless standard 802.11ac. The motivation behind this study is therefore to evaluate 802.11ac for IPv4 and IPv6 with and without WAP2 security. We also determine the actual bandwidth because our previous study in 802.11n [8,9] showed that the theoretical limit cannot be reached.

II. NETWORK SETUP

To measure the performance of 802.11ac for IPv4 and IPv6 on Windows 8.1 and Windows Server 2012 WLAN, the server machine is connected to the Linksys Business LAPAC1750PRO Access Point (AP) via a Cat 5e crossover cable. The client is connected to the server to the Linksys Access Point (AP) wirelessly. The distance between the access point and the workstations was well within one meter in-order to maintain the optimum signal strength, in order to find the maximum practical throughput of 802.11ac. Previous work had indicated that theoretical values s different from practical values. The channel bandwidth is set to 80 MHz in 802.11ac. The hardware specifications for both the client and server machines consists of an Intel® Core™ i7 Duo 6300 2.87 GHz, a Western Digital Caviar 160 GB hard-drive, 16.00 GB of RAM. The client machines was installed with an AC1750 Wireless Dual Band PCI Express Adapter and a Realtek GbE LAN chip (10/100/1000 Mbps) Gigabit Ethernet NIC installed on the server machine.The operating system installed was Microsoft Windows 8.1 as the client and Windows Server 2012 as the server. The test bed setup remained constant for all experiments conducted. The test bed diagram is shown in Figure 1.

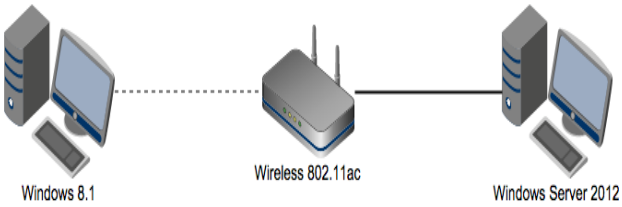

Figure1: Network test bed

III. DATA GENERATION AND TRAFFIC MEASUREMENT TOOL

JPerf 2.0.2 [13, 15] tool with graphical interface was selected for this particular test-bed to analyze the performance of wireless Client-to-Server network on 802.11ac. IPerf, a C++ programming language tool, is a freeware end-to-end active tool used to measure the network performance. It generates and measures the traffic for both the TCP and UDP packets in either IPv4 or IPv6 between two workstations. IPerf allows the user to set various parameters that can be used for evaluating a network, and provide tests for throughout, and delay [14]. IPerf has been found to provide the highest correct bandwidth measurement compared to other popular traffic generators in a laboratory environment [15].

IV. RESULTS

The throughput and RTT (round trip time) and CPU usage of TCP and UDP were evaluated for both IPv4 and IPv6 on an IEEE 802.11ac network. Data packets are gradually increased in size from 128 Bytes to 1408 Bytes. The second phase of the experiment evaluate the impact of WPA2 on the IEEE 802.11ac client-server WLAN network. For each packet size, a total of 20 runs are carried out, and the result are averaged and standard deviation of result are calculated. The standard deviation average was less than 0.03 of the average of results of 20 runs.

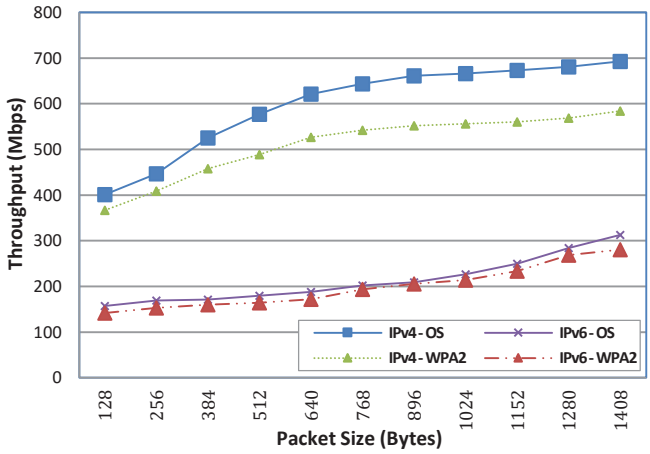

Figure 2: TCP Throughput Comparison for IPv4 and IPv6 in 802.11ac WLAN, Open System vs. WPA2 security.

Figure 2 shows the TCP throughput for IPv4 and IPv6 on WLAN 802.11ac Client-Server (Windows 8.1 -Windows Server 2012) with WPA2 security and open system. In most scenarios, as the packet size increases the throughput of TCP also increase consistently along with them.

On open system network, IPv4 considerably outperforms IPv6 on all packet sizes. The maximum difference in throughput was spotted at packet size 896 Bytes. At this packet size IPv4 on open system outperforms IPv6 by 68.38% (661 Mbps for IPv4 compared to 209 Mbps for IPv6), which offered 452 Mbps higher throughput. On WPA2, IPv4 again significantly higher than IPv6 on all packet sizes. This maximum difference in throughput between WPA2 enabled is spotted at packet size 640 Bytes where IPv4 outperforms IPv6 by 67.36% (527 Mbps for IPv4 compared to 172 Mbps for IPv6) and which offered a maximum of 355 Mbps higher throughput.

Therefore when running IEEE 802.11ac in open system network, the throughput of TCP is higher. The maximum difference in throughput between open system and WPA2 security enabled was spotted at packet size 1152 Bytes for IPv4 and 1408 Bytes for IPv6. At packet size 1152 Bytes IPv4 on open system outperforms IPv4 on secured WPA2 by 16.79% (673 Mbps for IPv4 open system compared to 560 Mbps for

IPv4 WPA2), which offered 113 Mbps higher throughput. At packet size 1408 Bytes, IPv6 on open system outperforms IPv6 on secured WPA2 by 10.22% (313 Mbps for IPv6 open system compared to 281 Mbps for IPv6 WPA2), which offered 32 Mbps higher throughput.

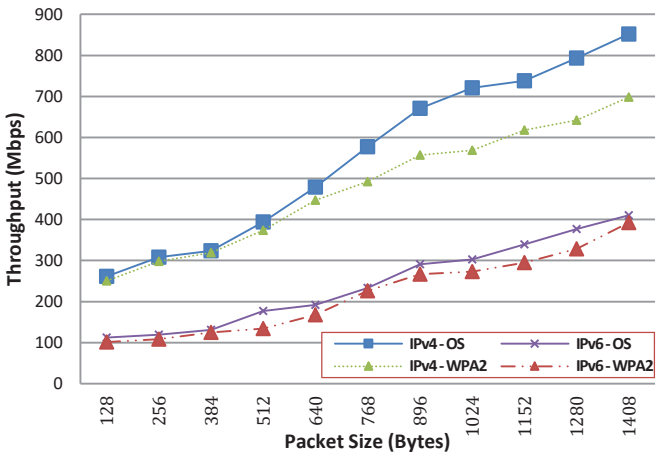

Figure 3: UDP Throughput Comparison for IPv4 and IPv6 on 802.11ac WLAN, Open System vs. WPA2 security

Figure 3 shows the UDP throughput for IPv4 and IPv6 on Windows 8.1 with Windows Server 2012 running on WPA2 and open system network. In all scenarios, as the packet size increases, the throughput of UDP also increases consistently along with them. On open system network, IPv4 outperforms IPv6 on all packet sizes. The maximum difference in throughput was spotted at packet size 1408 Bytes. At this packet size, IPv4 on open system outperforms IPv6 by 51.87% (852 Mbps for IPv4 compared to 410 Mbps for IPv6), which offered 442 Mbps higher throughput. On WPA2, IPv4 outperforms IPv6 on all packet sizes. The maximum difference in throughput is spotted at packet size 1152 Bytes where IPv4 outperforms IPv6 by 52.26% (618 Mbps for IPv4 compared to 295 Mbps for IPv6) and which offered a maximum of 323 Mbps higher throughput.

Therefore when running IEEE 802.11ac in open system network, the throughput of UDP is higher. The maximum difference in throughput between open system and WPA2 security enabled was spotted at packet size 1408 Bytes for IPv4 and 1280 Bytes for IPv6. At packet size 1408 Bytes IPv4 on open system outperforms IPv4 on secured WPA2 by 18.07% (852 Mbps for IPv4 open system compared to 698 Mbps for IPv4 WPA2), which offered 154 Mbps higher throughput. At packet size 1280 Bytes, IPv6 on open system outperforms IPv6 on secured WP2 by 12.99%, (377 Mbps for Ipv6 open system compared to 328 Mbps for IPv6 WPA2) which offered 49 Mbps higher throughput.

The result for IEEE 802.11n [8] with WPA2 enabled on IPv4 for XP OS showed the decrease of TCP throughput in an average of approximately 7.07% (6.83 Mbps) less than open systems, this is almost less than half of what we measured with IEEE802.11ac, which offered 16.79% (113 Mbps) lower throughput. For IPv6, TCP throughput drop of at least 5.42% (4.71 Mbps) in 11n WLANs, when 11ac networks decrease the data rate by 10.22% (32 Mbps). Overall, compared to 802.11n, 802.11ac has the higher percentage TCP throughput degradation values for both IPv4 and IPv6 by implementing WPA2 security.

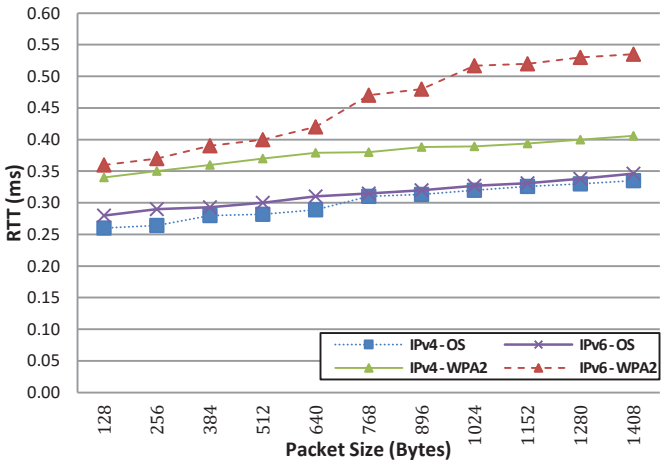

Figure 4: TCP RTT Comparison for IPv4 and IPv6 on 802.11ac WLAN, Open System vs. WPA2 security

Figure 4 shows the TCP RTT for IPv4 and IPv6 on Windows 8.1 with Windows Server 2012 running on WPA2 and open system network with no security. On open system, IPv4 outperforms IPv6 on all packet sizes. The maximum difference between IPv4 and IPv6 in RTT for TCP was spotted at packet size 256 Bytes. At this packet size, IPv4 on open system on average offered 8.96% (0.264 ms for IPv4 compared to 0.29 ms for IPv6), lower latency rate of 0.026 ms than IPv6 on open system. On WPA2, IPv4 outperforms IPv6 on all packet sizes. IPv4 had provide lower latency than IPv6 on secured WPA2. The maximum difference in RTT is spotted at packet size 1280 Bytes where IPv4 outperforms IPv6 by 24.52% (0.40 ms for IPv4 compared to 0.53 ms for IPv6), IPv4 was faster by 0.013 ms.

The maximum difference in RTT between open system and WPA security enabled system was spotted at packet size 640 Bytes for IPv4 and 1280 Bytes for IPv6. At packet sizes 640 Bytes, IPv4 on open system on average outperforms IPv4 on secured WPA2 by 23.74% (0.289 ms for IPv4 open system compared to 0.379 ms for IPv4 WPA2), which offered 0.09 ms lower latency. At packet size 1280 Bytes, IPv6 on open system on average outperforms IPv6 on secured WPA2 by 36.22% (0.338 ms for IPv6 open system compared to 0.53 ms for IPv6 WPA2), which offered 0.192 ms lower latency. The result showed that when WPA2 is not present, the latency is much lower for both IPv4 and IPv6.

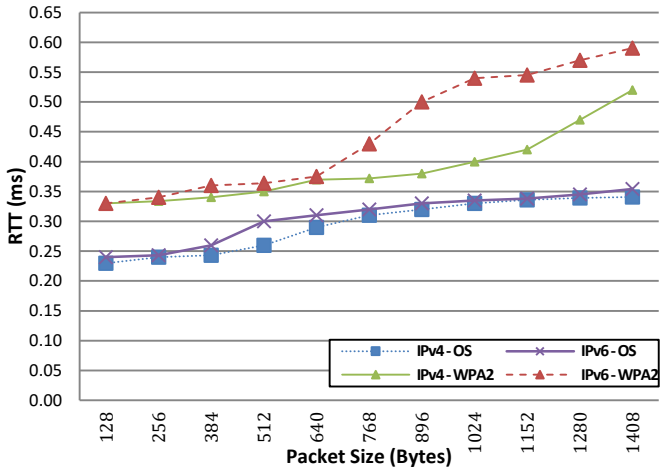

Figure 5: UDP RTT Comparison for IPv4 and IPv6 on 802.11ac WLAN, Open System vs. WPA2 security

Figure 5 shows the UDP RTT for IPv4 and IPv6 with WPA2 security and open system network. IPv4 outperforms IPv6 on all packet sizes. The maximum difference between IPv4 and IPv6 in RTT for UDP was spotted at packet size 512 Bytes. At this packet size IPv4 open system on average offered 13.33 % (0.26 ms for IPv4 compared to 0.30 ms for IPv6) lower latency rate of 0.04 ms than IPv6 on open system. On WPA2, IPv4 outperforms IPv6 on all packet sizes. The maximum difference in latency rate between open system and WPA security enabled system was spotted at packet size 1024 Bytes where IPv4 outperforms IPv6 by 25.92% (0.40 ms for IPv4 compared to 0.54 ms for IPv6) and which was 0.14 ms faster.

The maximum difference in latency rate between open system and WPA2 security enabled system was spotted at packet size 1408 Bytes for IPv4 and IPv6. At packet sizes 1408 Bytes, IPv4 on open system on average outperforms IPv4 on secured WPA2 by 34.42% (0.341 ms for IPv4 open system compared to 0.52 ms for IPv4 WPA2) and which was 0.179 ms faster. At packet size 1408 Bytes, IPv6 on open system outperforms IPv6 on secured WPA2 by 40% (0.354 ms for IPv6 open system compared to 0.59 ms for IPv6 WPA2) and which was 0.236 ms faster.

In both scenarios, as the packet size increase from 128 to 1408 Bytes the RTT escalates consistently. The implementation of WPA2 security had a negative impact on network round trip time (latency). Both TCP and UDP perform better on open system than WPA2 security for both IPv4 and IPv6.

Figure 6 shows the TCP CPU Utilisation for IPv4 and IPv6 on Windows 8.1 with Windows Server 2012 running on WPA2 and open system network with no security. On open system, IPv4 outperforms IPv6 on all packet sizes. The maximum difference between IPv4 and IPv6 in CPU Utilisation for TCP was spotted at packet size 1152 Bytes. At this packet size, IPv4 on open system on average offered 0.22% lower CPU Utilization than IPv6 on open system (5.84% for IPv4 compared to 6.06% for IPv6), On WPA2, IPv4 outperforms IPv6 on all packet sizes. IPv4 provided lower CPU Utilisation than IPv6 on secured WPA2. The maximum difference in CPU usage rate is spotted at packet size 128 Bytes where IPv4 outperforms IPv6 by 0.84% lower CPU Utilisation. (8.16% for IPv4 compared to 9.00% for IPv6).

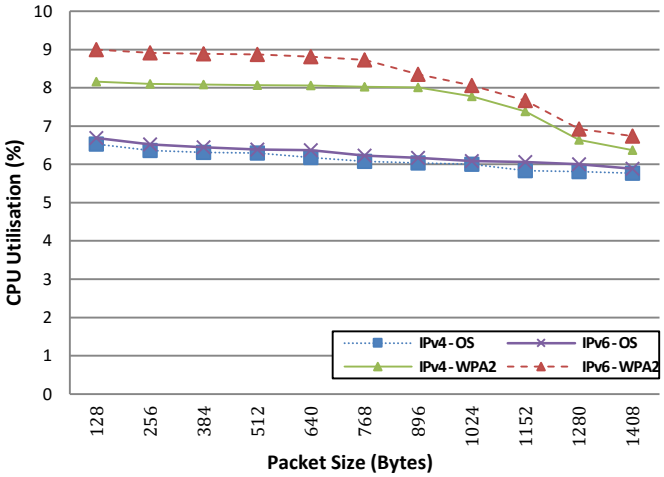

Figure 6: TCP CPU Utilisation Comparison for IPv4 and IPv6 on 802.11ac WLAN, Open System vs. WPA2 security

The maximum difference in CPU Usage rate between open system and WPA security enabled system was spotted at packet size 896 Bytes for IPv4 and 768 Bytes for IPv6. At this packet size, IPv4 on open system on average outperforms IPv4 on WPA2 by 1.97% lower CPU Utilisation (6.04% for IPv4 open system compared to 8.01% for IPv4 WPA2). At packet size 768 Bytes, IPv6 on open system on average outperforms IPv6 on secured WPA2 by 2.5% lower CPU Usage (6.23% for Ipv6 open system compared to 8.73% for IPv6 WPA2). The result showed that when WPA2 is not present, the Utilisation is lower for both IPv4 and IPv6.

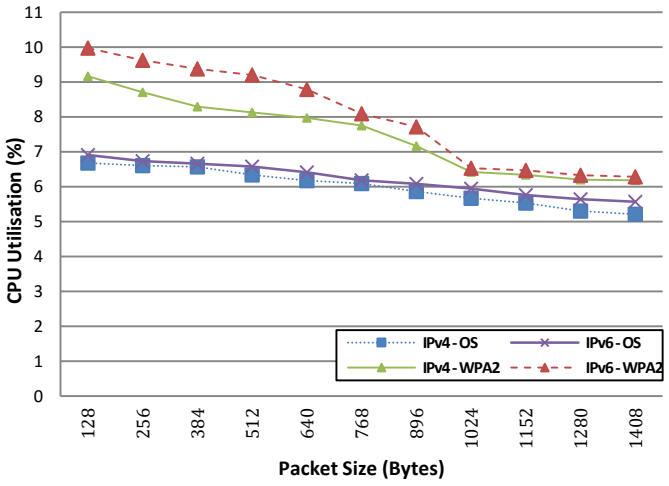

Figure 7: UDP CPU Utilisation Comparison for IPv4 and IPv6 on Windows 8.1 with Windows Server 2012 on Open System vs. WPA2 security

Figure 7 shows the UDP CPU Utilisation for IPv4 and IPv6 on Windows 8.1 with Windows Server 2012 running on WPA2 and open system network. IPv4 outperforms IPv6 on all packet sizes. The maximum difference between IPv4 and IPv6 in CPU Utilisation for UDP was spotted at packet size 1408 Bytes. At this packet size IPv4 open system on average offered lower CPU usage by 0.36% than IPv6 on open system

(5.21% for IPv4 compared to 5.57% for IPv6). On WPA2, IPv4 outperforms IPv6 on all packet sizes. The maximum difference in CPU Usage between open system and WPA security enabled system was spotted at packet size 384 Bytes where IPv6 outperforms IPv6 by 1.08% lower CPU Utilisation (8.29% for IPv4 compared to 9.37% for IPv6).

The maximum difference in CPU usage percentage between open system and WPA security enabled system was spotted at packet size 128 Bytes for IPv4 and IPv6. At this packet sizes, IPv4 on open system on average outperforms IPv4 on secured WPA2 by 2.48% lower CPU Utilisation (6.68% for IPv4 open system compared to 9.16% for IPv4 WPA2).

At packet size 128 Bytes, IPv6 on open system outperforms IPv6 on secured WPA2 by 3.06% lower CPU Utilisation (6.91% for IPv6 open system compared to 9.97% for IPv6 WPA2).

In both scenarios, as the packet size increase from 128 to 1408 Bytes the CPU Utilisation generally decreases. The implementation of WPA2 security had a negative impact on network CPU usage. Both TCP and UDP perform better on open system than WPA2 security for both IPv4 and IPv6.

IPv4 had lower RTT, higher throughput and lower CPU utilization, due its lower overhead in its packet compared to IPv6. Implementing WPA2, adds more overhead to the network that results in lower throughput, higher RTT, and higher CPU utilization. UDP hag higher throughput of upto 850 Mbps in 802.11ac as compared to TCP higher throughput of 700 Mbps. TCP is connection oriented that requires connection set up, and has to wait for acknowledgments before it can send more packets. UDP does not have these features, and has lower overheads, and these makes it faster.

V. CONCLUSION

In this paper, due to the large overhead of IPv6 and the impact of WPA2 security, IPv6 with WPA2 gave the least throughput, highest RTT, and highest CPU usage. IPv4 with no security provided the best results.

The highest throughput achieved for 802.11ac Windows 8.1-Server 2012 WLAN (open system, IPv4), was approximately 850 Mbps for UDP and 700 Mbps for TCP. This is lower than 1 Gbps theoretical bandwidth. Implementing. This bandwidth will even be lower if WPA2 security or IPv6 is used, as discussed in this paper. Implanting WAP2 security can reduce bandwidth by 6.78% (113 Mbps) for TCP and by 18.07% (154 Mbps) for UDP.

.

VI. FUTURE WORKS

The future work includes testing more operating systems such as Linux with IPv4 and IPv6 using both open systems and WPA2.

ACKNOWLEDGMENT

The authors would like to thank UNITEC Institute of Technology for funding the research team and providing the inventory needed.

REFERENCES

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

[2] 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.

[3] B. Chacos, “25 hidden features in windows 8.1. PC World," 20 Sep 2015. [Online].Available: http://search.proquest.com/docview/1537318521?accountid=142908.

[4] J. Govil, "On the investigation of transactional and interoperability issues between IPv4 and IPv6," IEEE International Conference on Electro/Information Technology'07 Chicago, IL, 17-20 May 2007, pp. 604 – 609.

[5] N. Baghaei, and R. Hunt, “IEEE 802.11 wireless LAN security performance using multiple clients," 12th IEEE International Conference on Networks (ICON'04) Singapore, 16-19 Nov 2004, pp. 299 - 303 vol.1.

[6] 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," Conference on Innovations in Information Technology Dubai, AUE, Nov 2006, pp. 1 – 5.

[7] 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," IFIP International Conference on Wireless and Optical Communications Networks (WOCN'07) Singapore, 2-4 July 2007, pp. 1 – 5.

[8] 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," 3rd International Conference on New Technologies, Mobility and Security (NTMS'09) Cairo, Egypt, 20-23 Dec 2009, pp. 1 – 4.

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

[10] 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," Baltic Congress on Future Internet Communications (BCFIC'11) Riga, Latvia, 16-18 Feb 2011, pp. 50 – 53.

[11] S.S. Kolahi, S. S., P. Li, M. Argawe, M., and M. Safdari, “WPA2 security-bandwidth trade-off in 802.11n peer-peer WLAN for IPv4 and IPv6 using Windows XP and Windows 7 operating systems.” 2012 IEEE Symposium on Computers and Communications (ISCC), 1-4 July 2012.

[12] S.S. Kolahi, Y.R. Cao, and H. Chen, “Bandwidth-IPSec Security Tradeoff in IPv4 and IPv6 in Windows 7 Environment”, Second International Conference on Future Generation Communication Technologies (FGCT 2013), December 12-14, 2013, London, UK, pp. 148-152.

[13] Code.google.com, “Graphical frontend for IPERF written in Java," [Online].Available: https://code.google.com/p/xjperf/.

[14] R. Blum, Network Performance Open Source Toolkit Using Netperf, tcptrace, NISTnet, and SSFNet, New York, NY, USA: John Wiley & Sons, 2003.

[15] S.S Kolahi, S.Narayan, D.D.T. Nguyen, and Y. Sunarto, “Performance Monitoring of Various Network Traffic Generators," UkSim 13th International Conference on Computer Modelling and Simulation (UKSim'11) Cambridge, UK, March 30 2011-April 1 2011, pp. 501 - 506.