Throughput Analysis of IEEE WLAN "802.11 ac" Under WEP, WPA, and WPA2 Security Protocols

Talal Mohammed Alghamdi *tvtc.talal@tvtc.gov.sa*
Al Majmaah College of Technology
Riyadh
Saudi Arabia

Abstract

WLAN (Wireless Local Area Networks) are gaining their grounds, and widely deployed in organizations, college campuses, public places, and residential areas. This growing popularity of WLAN makes these networks more vulnerable towards attacks and data thefts. Attacker attempts unauthorized access to the network for accessing the sensitive data of the users. Thus, it's necessary to address all the security challenges and its countermeasures using various encryption algorithms to prevent the attacks. However, with the use of security protocols the performance of the WLAN network can be varied. Thus this paper addresses the impact of various security protocols on the WLAN network, keeping throughput as the benchmark for network performance.

IEEE 802.11 ac is the latest wireless standard that operates in 5 Ghz frequency band with higher data rate, compare to its previous standards. This research has also chosen IEEE 802.11 ac standard for investigating the impact of security protocols including WEP (Wired Equivalent Privacy), WPA (WiFi Protected Access), and WPA2 (WiFi Protected Access 2) on throughput of WLAN IEEE 802.11 ac in Windows environment using TCP and UDP traffic for both IP versions (IPv4 & IPv6). The research was launched in a real test-bed setup, with a Client/Server network structure. The results from the experiment showed that the performance of data throughput in the open system were higher comparable to secured systems. However, the results demonstrated that the performance of throughput have different behavior to different security protocols under TCP/UDP traffic with IPV4 & IPV6. A detailed comparison of results in all scenarios is explained in the paper.

Keywords: IEEE 802.11ac, Throughput, Security Protocol, IPv4, IPv6.

1. INTRODUCTION

Latest advancements in WLAN technology have increased its deployment in real life environment. Mobility, ease of use, versatility, and connectionless nature of wireless network has made this system as one of the preferred communication medium in organization, universities campuses, and public domain. IEEE 802.11ac is the fifth generation and latest WLAN standard of Wi-Fi 802.11 family, having advanced features compare to its previous standards [1]. IEEE 802.11ac uses 5 Ghz frequency band with backward compatibility to its previous standard, and assures higher data rate compare to previous standards. Some of the enhanced features of the 802.11 ac standards include the following [2-4]:

- Wider channel binding
- Supports higher modulation techniques like 256-QAM (Quadrature Amplitude Modulation)
- MU-MIMO (Multi-User Multiple Input Multiple Output) which allows It allows the transceiver to handle different streams from or to various transceivers simultaneously
- Spatial stream beamforming

The characteristics and nature of wireless network make these networks more vulnerable towards security attacks compare to wired network. Thus, security is an important criterion in WLAN communications networks. To secure a wireless network from personal level to the enterprise level, it is essential to have a secure communication. Confidentiality and integrity of information must be maintained. To ensure the security threats several security protocols are available for WLAN, which are WEP, WPA, and WPA2. Based on these security protocols most WLAN operates either as open system or with available personal & enterprise security protocols.

Based on the literature review conducted, it can be summarized that there is not enough research available that can validate the throughput of 802.11ac in a real environment. Thus, research will focus on throughput analysis of 802.11ac WLAN performance on Windows 10 with enabling and disabling the WLAN security protocols in a real environment. A detailed comparative throughput analysis of 802.11 ac standard is provided under WEP, WPA, & WPA2 security protocols.

The remainder of the paper comprised of five sections, and is organized as follows. Section 2 presents the background study. Section 3 consists of throughput analysis with and without security protocols. Section 4 provides a detailed discussion of the findings. Finally, conclusion & future work is explained in section 5.

2. BACKGROUND STUDY

WLAN is a form of wireless communication that uses a series of IEEE 802.11 standards. IEEE 802.11 family comprises of several standards which are IEEE 802.11a, b, g, n, and ac. In 1997, IEEE released the first protocol that operated on 2.4GHz ISM band, and used for medium access method CSMA/CA. The coverage area was 20 meters for the indoor and approximate 100 meters for the outdoor usage. The data rate was only 1 to 2 Mbps. Two years later, IEEE released 802.11b that provided higher data rate (11Mbps) with higher coverage area. It covered nearly 38 meters for the indoor and about 140 meters outdoor. The channel bandwidth was 20 MHz and the method of modulation was only DSSS. In 2003, IEEE published next standard which is 802.11g. It has higher throughput compare to its previous standard 802.11b. It included Orthogonal Frequency Division Multiplexing (OFDM) as a modulation scheme.

In 2009, the IEEE published officially next standard which is IEEE 802.11n. The 802.11n standard introduced Multiple Input and Multiple Output MIMO with 40 MHz channel bandwidth [5]. It operates on 2.4 GHz and 5 Ghz band, with capability of 600 Mbps data rate theoretically by using the spatial stream. In late 2013, the IEEE released 802.11ac [1]. The 802.11ac introduces several advanced features that led to VHT as a solution for WLANs. 802.11ac includes Multi-User MIMO (MU-MIMO) to handle multiple users at the same time. Furthermore, it operates only on 5GHz channel band and provides wider channel bandwidth 40, 80, and 160 MHz.

2.1 Related Work

Several studies exist in the literature that carries out the performance analysis of IEEE 802.11 standards. The focus of this research is to perform the throughput analysis of 802.11 ac standard under various security protocols. A dearth research has been done by the researchers to analyze the impact of security protocols on performance of throughput. A variety of research is available that evaluate the performance analysis of wireless network standards (802.11 b/g/n), but limited research is available on the 802.11ac standard.

In [6], author has analyzed the performance of throughput under various encryption techniques including WEP and WPA on 802.11g wireless network standard. The research concludes that the throughput performance degraded when the security protocols are enabled. In [7], authors have studied the performance of security protocols in a client-server environment over IEEE 802.11n network under different security protocols and operating systems. The research concluded that the wireless performance is dependent on operating system with significant impact of security protocols on the network performance. In [8], author has further enhanced their work by analyzing the performance with more Operating Systems including Linux in their previous research. The

results are similar to the previous research with performance degradation in all network parameter including throughput, jitter, and drop rates with different security protocols enable. However research remarks that WPA2 security protocol has different behavior in 802.11n network, compare to other protocols.

In [9], authors have analyzed the bandwidth under WPA2 security protocol for both IP versions with UDP protocol. Research concluded that IPv4 has better performance with open system and higher bandwidth is produced for UDP protocol. In [10], authors have proposed a comparative study with two different operating systems (windows and Fedora), to analyze the best suitable cases for bandwidth over IPv6. Research concluded that Fedora provides the best results for bandwidth and RTT over IPv6. In [11], authors have analyzed the performance of Open VPN rather than WEP to secure 802.11g wireless network. Both IP protocols are analyzed under various scenarios with different data rate and packet sizes. Findings of the study suggest that a performance enhancement of throughput and latency under Open VPN compare to WEP.

A performance analysis of throughput and delay is conducted with varied scenarios including different set of encryption protocols in Multimedia Applications [12]. The research claims that the performance of multimedia application degraded under security protocols. In [13], authors have analyzed the impact of security techniques in IEEE 802.11n wireless network with various operating systems and quantified it. The main theme of the research was to analyze the impact of WPA2 security protocol on throughput for different operating systems. The research concluded that throughput decrease for both IP versions under WPA2 security protocol. However compared to IPv6, IPv4 protocol has achieved lesser throughput performance degradation. In [14], authors have performed a performance analysis of IEEE 802.11n under open system and WPA2 security protocols for two windows operating system (Windows XP, Windows 7). The results concluded that there is a significant decrement on TCP throughput for both operating systems under WPA2 security protocol, compared to open system. However, IPv4 produces higher throughput for both open system and WPA2 security protocols in compare to IPv6.

IEEE 802.11ac is the latest standard with improved speed, improved throughput, and with other salient features. Because of relatively latest WLAN standard, 802.11ac is the latest trend of research. However in compare to other standard fewer studies are available in the literature that evaluates the throughput of 802.11ac under various security protocols. In [15], authors have performed a comparative performance analysis of 802.11 ac & 802.11n in an outdoor environment with interference. The authors have compared average throughput for both wireless standards in line of sight and non-line of sight conditions. In [16], author has performed a performance analysis of 802.11 ac features in indoor WLAN environment. Finding suggests that the IEEE 802.11ac achieves higher throughput compare to its previous standards.

In [17], authors have evaluated the IEEE 802.11ac performance of saturated wireless backhaul networks in terms of PHY and MAC layers features. The proposed wireless mesh backhaul consisted of six mesh nodes one of them was connected to the Internet, which supported 802.11ac/n. The results showed that MU-RTS/CTS outperformed the MU-Basic, especially, when the number of nodes and A-MPDU size were increased. Moreover, authors highlighted that system throughput increased when there was an increase in number of antennas. In [55], researchers presented a new technique based on the handshake of RTS/CTS to the selected stations in order to evaluate the performance of IEEE 802.11ac packet aggregation in non-saturation network. Also, they highlighted the buffer size influence on the maximum throughput can be achieved. Researchers assumed the estimation and reporting of the channel state information CSI for each transmission, as well as the only transmitter is the AP, and the active users as only receivers. Results indicated that packet aggregation notably helped the increase of performance; particularly, when the number of antenna is slightly lower than number of STAs, and the existence of large buffer that can interact with the destination's packet. Under those cases, the proposed technique is ideal for performance, as well as, it has the ability to maximize the number of packets and spatial streams in an A-MPDU frame. Finally, researchers suggested

that increases in number of packets for scheduling in each transmission would result in higher delay.

In [18], authors have performed a measurement-based study conducted in an office building to analyze the performance of IEEE 802.11ac standard. The study pointed out that distance play a major role in the performance improvement. Researchers stated that significant performance improvements are sensitively subjected to channel conditions. The research showed that the achieved data rates swiftly decreased with the distance of transmitter and receiver increased. In [19] authors have, evaluated the wireless video transmission by using algorithms of lossless video compression and 8x8 MIMO-OFDM wireless transceiver over simulated IEEE802.11ac WLAN. The proposed system that they used is to evaluate the transmission, consists of three main parts; image compression, error correction, and wireless transceiver part. Results indicated that wireless video sequences can be transferred over 22db SNR wireless channel with pixel restoration rate of 99.99%. Researchers confirmed that transmitting HD video, in case of SNR 22db or more can be performed without quality loss.

To the best of our research survey that we conducted for this research, it can be claimed that a few research is available that evaluates performance evaluation, or throughput analysis of IEEE 802.11ac standard under various security protocols. The same can also be concluded on the basis of survey research done on 802.11ac by the authors [20]. Most of studies that analyze the performance analysis under various security protocols are done with IEEE 802.11 previous standards.

3. THROUGHPUT ANALYSIS OF IEEE WLAN "802.11 AC" UNDER WEP, WPA, & WPA2 SECURITY PROTOCOLS

In this section the two experiments that are carried out in research lab to analyze the impact of security protocols, and open system (without security protocols) on throughput of IEEE 802.11 ac to fulfill the research objective. These experiments comprises of three key phases in order to evaluate the throughput analysis of security protocols over the 802.11 ac WLAN. The first phase is evaluating the 802.11ac WLAN performance without enabling any security protocols. The second phase, evaluates the 802.11ac WLAN while the security protocols are enabled. The second phase has three main stages, and in each stage there will be only one security protocol enabled, namely, WEP, WPA, and WPA2, respectively. The last phase will be a comparison between the first and second phase. There exist three main methods that are used for security protocols evaluation as: simulation, test-bed, and theoretical-based. Theoretical-based and simulation evaluation methods produce less realistic results, whereas test-bed method allows implementing various scenarios in a real environment that lead to results realism. Thus, this research has also adopted test bed method for the evaluation.

2.2 Experimental Test-bed

In order to study the impact of different security protocols on the throughput of WLAN 802.11ac in different network scenarios, an experimental test-bed is developed. The experimental setup will consider network type, hardware, and operating system. A client- server model has been used as network type and connected via an access point, depicted in Fig. 1.

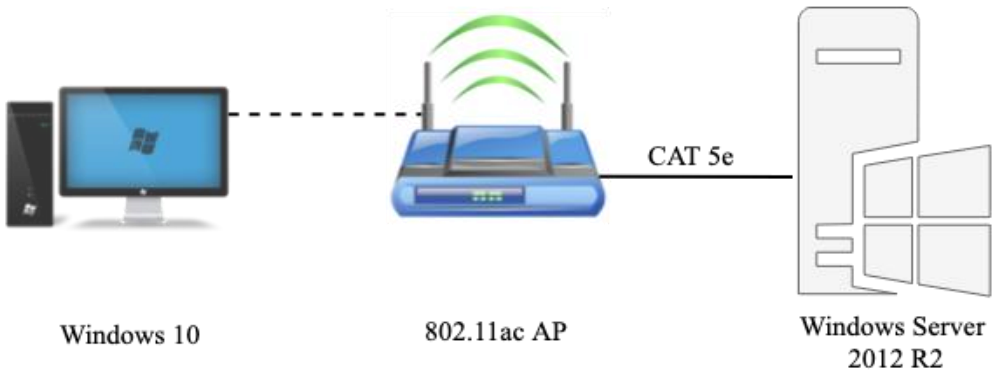

FIGURE 1: A Client/Server based Test-bed.

For the involved hardware, the client PC is equipped with capable 802.11ac wireless network card which is configured properly depending on the network structure. CAT5e cable linked the server PC to wireless 802.11ac AP. The setup will be launched under Windows 10 and Windows Server 2012 R2 operating systems environment. The detailed description of test-bed design is provided in table 1.

System/Software Tool	Function	Specification
Linksys EA 6300 AC 1200 Dual band Smart Wireless router	Wireless router	For ac max 867 Mbps speed, 2.4 Ghz & 5 Ghz, IEEE 802.11 b,a,g,n,ac standards
Client	Client Node	Intel(R) Core™ i7-6700 CPU @ 3.40GHz 3.40 GHz with Windows 10
Server	Server Node	Intel(R) Core™ i7-6700 CPU @ 3.40GHz 3.40 GHz with Windows Server R2
Client Tools	Packet generator, performance monitoring	Netperf, Typeperf
Server Tools	Packet Generator	Netperf

TABLE 1: Technical Specifications.

2.3 Experimental Configuration

In order to test the performance, the test-bed carried out as shown in Fig. 1. The network was designed as client-to-server in Windows environment. Further, various configurations were applied which includes IP version, security protocol, packet type, and packet size. For each individual case these parameters were configured, implemented, tested, and recorded. Once the network setup and parameters were configured, appropriate traffic was generated. The Netperf tool is used as the traffic generator tool that generates packets [21]. Netperf is also capable to collect data that are needed for throughput analysis. The experimental parameters used for the test bed are summarized in table 2.

Parameters	Parameter Values	
Network	Client/Server	
IP Versions	IPv4	IPv6
Security Protocols	Enable	Disable
Network Traffic (Packet type)	TCP	UDP
Packet Size	128, 384, 640, 896, 1152, & 1408 (Bytes)	

TABLE 2: Experimental Parameters.

4. EXPERIMENTAL FINDINGS

The aim of the research is to study the impact of various security protocols in 802.11 ac system throughput. The experimental test bed with various possible configurations is explained in previous section. The finding of the experiment and a detailed discussion is explained in next subsection.

4.1 TCP Throughput

Figure 2 & 3 presents the throughput results grouped together by various security protocols for both IPv4 & IPv6, to understand the overall impact of security protocols on TCP throughput. In fig. 2 & 3, TCP throughput values are presented corresponds to different packet size. Evaluating the wireless network with different variant of security protocols and with open system, it is evident that wireless network with encryption achieves the highest throughput (283 Mbps). It is also noticed that for most of other security protocols the throughput values are less than 300 Mbps, which are lower than standard theoretical values which is 1 Gbps.

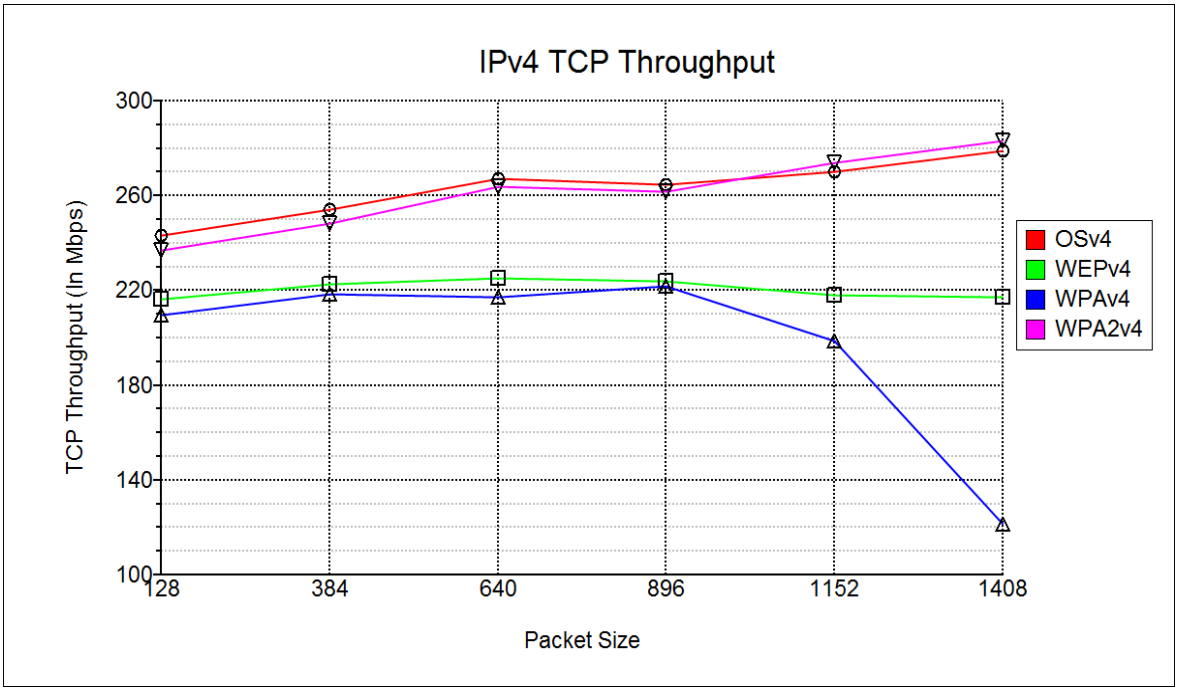

FIGURE 2: IPv4 TCP Throughput in all scenarios for IEEE 802.11ac.

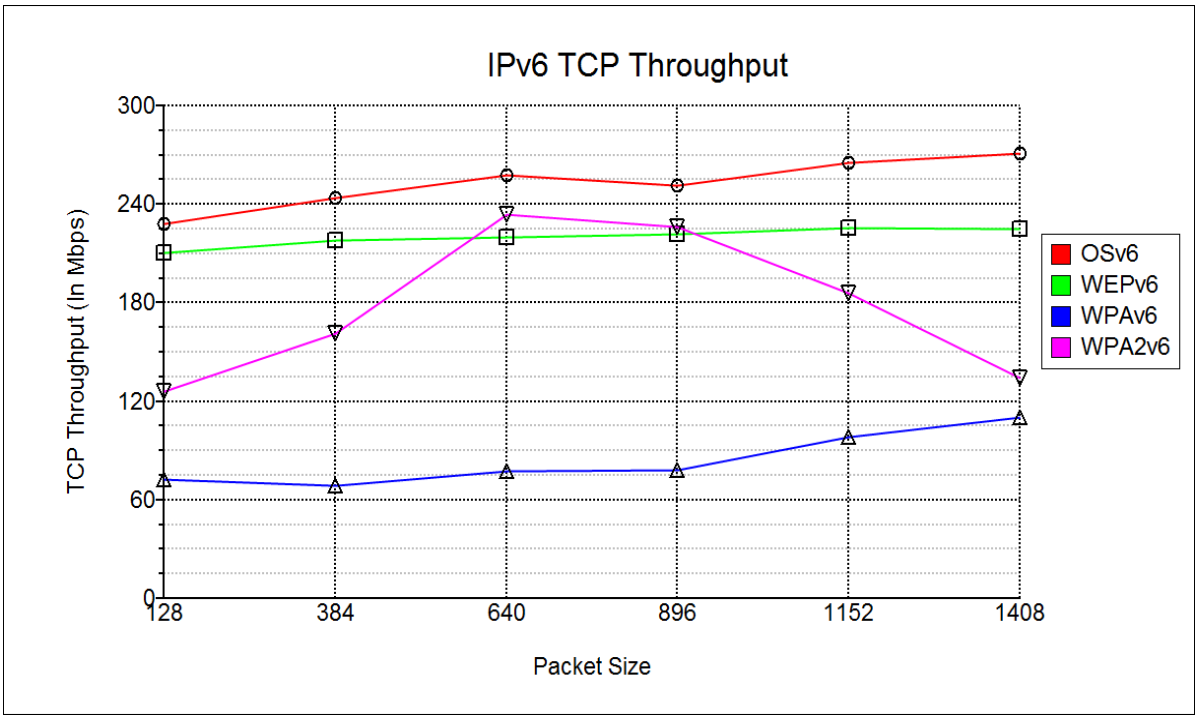

FIGURE 3: IPv6 TCP Throughput in all scenarios for IEEE 802.11ac.

The compatibility of the latest standard (like WPA2) with wireless network gives the best throughput in the network with security protocol enabled. However, with security protocols enabled, throughput values drop to that comparable to previous wireless standards. It is also noticed that the throughput of IPv6 for most of the security protocols is slightly lower compared to IPv4, with significant fluctuation for most packet sizes. One possible reason of having low throughput values for IPv6 compared to IPv4 is that packets having larger overhead in IPv6.

4.2 UDP Throughput

The throughput results grouped together by various security protocols to understand the overall impact of security protocols on UDP throughput for IPv4 & IPv6 are shown in fig. 4 & 5. The UDP throughput values are presented with various packet sizes. Evaluating the wireless network with different variant of security protocols and with OS, it is evident that wireless network without encryption (open system), achieves the highest throughput. The highest throughput is achieved and equal to 876.9 Mbps.

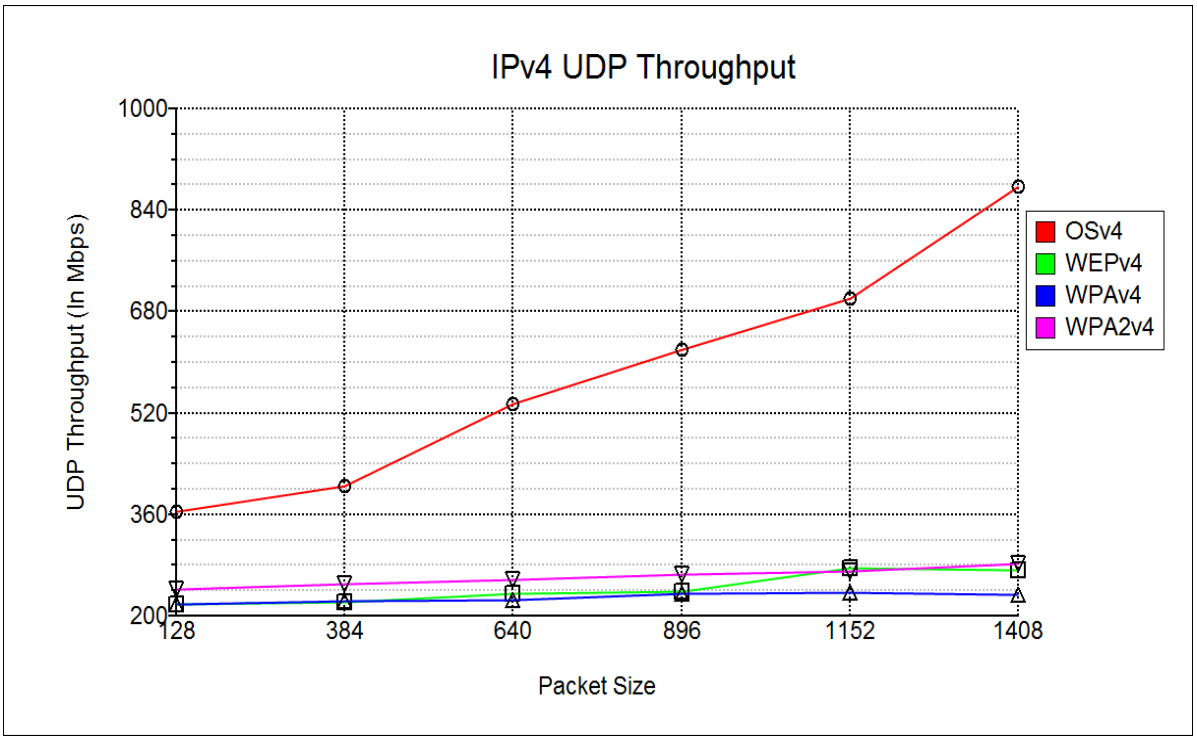

FIGURE 4: IPv4 UDP Throughput in all scenarios for IEEE 802.11ac.

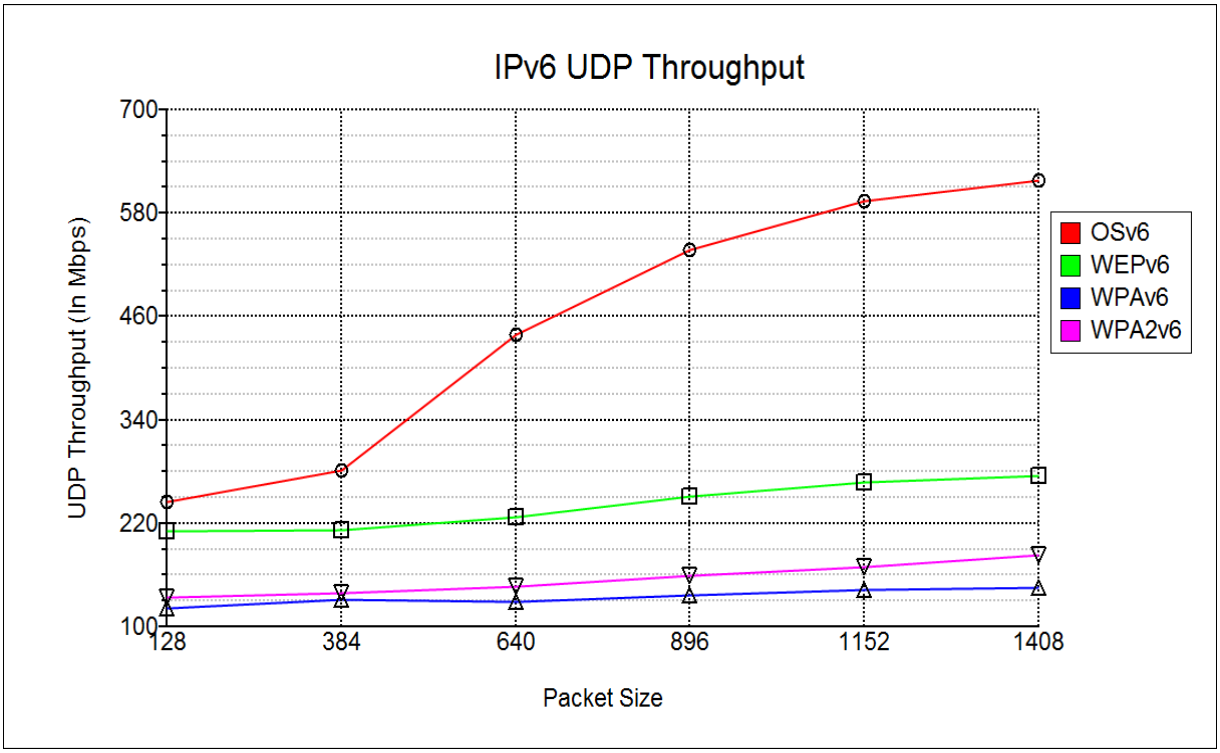

FIGURE 5: IPv6 UDP Throughput in all scenarios for IEEE 802.11ac.

It is also noticed that for most of other security protocols, the UDP throughput values are higher than the values achieved for TCP throughput values. One possible explanation for this is the connectionless nature of UDP protocol when compared to TCP. In these UDP throughput graphs correspond to different packet sizes, the WPA2 security protocol has highest throughput values for IPv4 under all security protocols; whereas WEP security protocol with IPv6 has highest throughput under all security protocol. However, compared to TCP throughput, the UDP throughput outperforms TCP throughput for most packet sizes.

4.3 Impact of Security Protocols on Throughput

Throughput is one of the most significant metric to analyze the network performance. Throughput is defined as the number of Bytes transferred over a network path during a fixed amount of time. There are several factors, which can affect the throughput of TCP connection such as underlying protocol, TCP connections, buffer size, congestion window size, and round trip time. The throughput is computed with four different cases: open system (no security), WEP, WPA, and WPA2 for both IP protocols (with IPv4 and IPv6) in IEEE 802.11ac. The experiment was done with the various test-bed and results were discussed in previous section. The throughput results are summarized in Table 3 for better evaluation of its performance under various security protocols.

Attribute Description		OS	WEP	WPA	WPA2
Average Throughput (Mbps) for TCP protocol	**IPv4**	263.04	220.5	197.82	261.35
	IPv6	253.06	220.05	84.15	177.97
Average Throughput (Mbps) for UDP protocol	**IPv4**	583.64	243.81	228.546	259.63
	IPv6	452.27	240.57	134.73	155
Dropped TCP%	**IPv4**	0%	16.17%	24.79%	0.64%
	IPv6	0%	13.04%	66.75%	29.67%
Dropped UDP%	**IPv4**	0%	58.22%	60.84%	55.23%
	IPv6	0%	46.82%	70.22%	65.73%

TABLE 3: Average Throughput for TCP/UDP Traffic.

Table 3 shows the average throughput values for TCP and UDP for IPv4 and IPv6 under all four cases. From table 3, it can be inferred that highest average throughput is achieved for open system under UDP protocol for IPv4. This outcome seems to be similar to theoretical hypothesis that for UDP traffic the throughput values are on higher side compare to TCP traffic. However, it can be argued that the theoretical upper bound for TCP throughput is slightly lower and equal to 263 Mbps. One important conclusion from Table 3 is that with security protocol enabled, the throughput values decrease, thus performance also degrades. Although WEP and WPA have less complex encryption compared to WPA2, but the throughput for WPA2 is higher. Under security protocol enabled, WPA2 has the best performance for TCP protocol with IPv4. For both TCP and UDP protocols, IPv4 outperforms IPv6 considerably for all four cases with security protocol enabled and disabled. Throughput measurement reached approximately to the expectation and theoretical hypothesis. The throughput performance under four different cases

has similar performance variation as for some other versions of Wireless LAN suggested by the researchers [7-10, 13, 14].

The research suggests that for the open system the throughput values are higher for IPv4 compared to IPv6 for both TCP and UDP protocols, which is similar to the research conducted by researchers for other wireless standards [9]. This infers that like other wireless standards, the wireless network 802.11ac also have similar characteristics on the performance for IP versions for open system with TCP and UDP protocol. For the open system, the best case is found under the UDP protocol for IPv4. The research also concluded that under security protocols WEP, WPA, and WPA2 there is a significant decrement in the throughput performance, similar to other wireless standard [8-10]. The throughput values for both open system and under security protocols have not reached to the expected theoretical upper bound values. The possible reason for these differences is due to uncontrollable factors such as hardware status, noise, and coexistence of other 802.11 wireless standards that influence the network performance. However, for the WPA2, throughput shows different behavior compared to other security protocols, similar to the research outcomes suggested by the previous researches [8, 22]. In comparison to the highest TCP and UDP throughput values in the OS, WPA has a significant effect on TCP and UDP throughput degradation with 24.79% and 70.22%, while for WEP TCP and UDP throughput decreases 13.04% and 58.22%. The WPA2 security protocol encryption has the lowest level of influence with 0.64% and 65.73% for TCP and UDP throughput. The best scenario under security protocol enabled is WPA2 protocol under IPv4 for TCP traffic. These research outcomes have similar behavior compared to other reference researches.

4.4 Comparative Evaluation of the Results

Compared to the previous researches on wireless standards, a dearth research has been done by the researchers to analyze the impact of security protocols on performance of throughput. A lot of research has been done on the performance analysis of wireless network standards (802.11 b/g/n), but less research is found on the 802.11ac standard.

In [23], authors has analyzed the impact of security on 802.11ac WLAN with three different security modes as no security, personal security, and enterprise security. The result shows throughput performance degradation ranging between 1.6% to 8.2% based on transport (TCP/UDP) and network (IPV4/IPv6) protocols. However the study has been performed using only WPA2/AES security protocol and RADIUS server. The results show similar behavior to this research. In [16], authors have conducted an empirical analysis to investigate the performance and fairness of 802.11ac network in indoor WLAN. Throughput, jitter, and fairness in WLAN is evaluated as a parameter for WLAN network 802.11ac. Findings suggest that 802.11ac achieves higher throughput compare and fairer with wider channels to 802.11a/n. However the impact of security protocols over throughput is not evaluated.

In [24], authors have investigated the impact of security protocol (WPA2) on IEEE 802.11ac client-to-server WLAN. Result shows a performance degradation ranging between10.22% to 18.07% based on transport (TCP/UDP) and network (IPV4/IPv6) protocols. The result shows similar behavior of throughput performance degradation while using security protocols. However research has not included other security protocols such as WEP and WPA in their study. In [25], authors have examined the impact of security protocol on network performance. WPA2-PSK was used as the security protocol in focus while selecting throughput as the performance metric. The experiment was carried out in wireless IEEE 802.11n environment. Result showed that the throughput in non-secured environment is higher compare to secure environment. However, study is performed with older wireless standard 802.11n.

In [26], author has investigate the performance analysis of IEEE 802.11ac using throughput parameter. An aggregate throughput of the system is computed based on a simulation setup. Results shows an enhancement in throughput compare to other wireless standard because of enhanced features of 802.11ac. However impact analysis of security protocols on throughput of 802.11ac network is not evaluated in the research. In [27], author has analyzed the impact of

wireless security protocols (WEP,WPA, & WPA2) in data throughput of IEEE 802.11b/g WLAN. Result has shown performance degradation while security protocol enabled in both 802.11b/g WLAN. However, in comparison 802.11g WLAN has better performance in throughput under most of the security protocols enable.

Compared to the literature available, the outcome of this research has also similar tradeoffs [7-10, 13, 14]. It suggests throughput degradation under various security protocols for both IP versions in 802.11ac wireless network. The best scenario for throughput, for the security enabled phase is achieved in IPv4/TCP while the WPA2 security protocol is enabled.

5. CONCLUSION & FUTURE WORK

The overarching aim of this research paper is to study the impact of various security protocols in 802.11 ac system throughput. In case of open system or network with no security protocols, the best scenario is IPv4/UDP to achieve the best throughput performance. Whereas, the best scenarios with security protocol enabled is achieved in IPv4/TCP for WPA2 security protocol enabled to achieve best throughput. Experimental results prove that enabling security protocols have impact on the network performance. Results suggest that the performance of throughput degrade while security protocols are enabled. However, WPA2, among all the security protocols, achieved the best results compared to others. Another aspect is that throughput values are unable to achieve the expected theoretical upper bound for both open system and under security protocol enabled scenarios.

The experimental test bed used for this research is relatively a more controlled environment. As in near future research will try to extend its research to evaluate the performance of 802.11ac standard in a topology based network, and P2P based network with more heterogeneous devices connected to the network.

6. REFERENCES

[1] V. Kelly, "New ieee 802.11 ac™ specification driven by evolving market need for higher, multi-user throughput in wireless lans," IEEE Standards Association, 2014.

[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] R. Van Nee, "Breaking the gigabit-per-second barrier with 802.11 ac," IEEE Wireless Communications, vol. 18, no. 2, pp. 4-4, 2011.

[4] E. H. Ong, J. Kneckt, O. Alanen, Z. Chang, T. Huovinen, and T. Nihtilä, "IEEE 802.11 ac: Enhancements for very high throughput WLANs," in 2011 IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications, 2011, pp. 849-853: IEEE.

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

[6] E. Barka and M. Boulmalf, "On the Impact of Security on the Performance of WLANs," JCM, vol. 2, no. 4, pp. 10-17, 2007.

[7] S. Narayan, T. Feng, X. Xu, and S. Ardham, "Network performance evaluation of wireless IEEE802. 11n encryption methods on Windows Vista and Windows Server 2008 operating systems," in 2009 IFIP International Conference on Wireless and Optical Communications Networks, 2009, pp. 1-5: IEEE.

[8] S. Narayan, T. Feng, X. Xu, and S. Ardham, "Impact of wireless IEEE802. 11n encryption methods on network performance of operating systems," in 2009 Second International Conference on Emerging Trends in Engineering & Technology, 2009, pp. 1178-1183: IEEE.

[9] 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 802.11 n WLAN in Windows 7-Windows 2008 environment," in 2011 Baltic Congress on Future Internet and Communications, 2011, pp. 50-53: IEEE.

[10] S. S. Kolahi and P. Li, "Evaluating IPv6 in peer-to-peer 802.11 n wireless LANs," IEEE Internet Computing, vol. 15, no. 4, pp. 70-74, 2011.

[11] P. Likhar and R. S. Yadav, "Securing IEEE 802.11 g WLAN using OpenVPN and its impact analysis," arXiv preprint arXiv:1201.0428, 2012.

[12] T. Hayajneh, S. Khasawneh, B. Jamil, and A. Itradat, "Analyzing the impact of security protocols on wireless LAN with multimedia applications," in Proc. of The Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE), 2012.

[13] S. S. Kolahi, Z. Qu, B. K. Soorty, and N. Chand, "The impact of security on the performance of IPv4 and IPv6 using 802.11 n wireless LAN," in 2009 3rd International Conference on New Technologies, Mobility and Security, 2009, pp. 1-4: IEEE.

[14] S. S. Kolahi, P. Li, M. Argawe, and M. Safdari, "WPA2 security-bandwith trade-off in 802.11 n peer-peer WLAN for IPv4 and IPv6 using Windows XP and Windows 7 operating systems," in 2012 IEEE Symposium on Computers and Communications (ISCC), 2012, pp. 000575-000579: IEEE.

[15] Z. Shah, S. Rau, and A. Baig, "Throughput comparison of IEEE 802.11 ac and IEEE 802.11 n in an indoor environment with interference," in 2015 International Telecommunication Networks and Applications Conference (ITNAC), 2015, pp. 196-201: IEEE.

[16] L. Kriara, E. C. Molero, and T. R. Gross, "Evaluating 802.11 ac features in indoor WLAN: an empirical study of performance and fairness," in Proceedings of the Tenth ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation, and Characterization, 2016, pp. 17-24: ACM.

[17] R. Liao, B. Bellalta, J. Barcelo, V. Valls, and M. Oliver, "Performance analysis of IEEE 802.11 ac wireless backhaul networks in saturated conditions," EURASIP Journal on Wireless Communications and Networking, vol. 2013, no. 1, p. 226, 2013.

[18] M.-D. Dianu, J. Riihijärvi, and M. Petrova, "Measurement-based study of the performance of IEEE 802.11 ac in an indoor environment," in 2014 IEEE International Conference on Communications (ICC), 2014, pp. 5771-5776: IEEE.

[19] K. Morinaga, H. Tsutsui, and Y. Miyanaga, "An evaluation of wireless video transmission using lossless video compression and 8× 8 MIMO-OFDM wireless transceiver," in 2013 13th International Symposium on Communications and Information Technologies (ISCIT), 2013, pp. 685-690: IEEE.

[20] R. Karmakar, S. Chattopadhyay, and S. Chakraborty, "Impact of IEEE 802.11 n/ac PHY/MAC High Throughput Enhancements on Transport and Application Protocols—A Survey," IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2050-2091, 2017.

[21] T. N. Homepage. (20/02/2018). http://www.netperf.org/netperf

[22] S. Narayan, C. Jayawardena, J. Wang, and W. Ma, "Performance test of IEEE 802.11 ac wireless devices," in 2015 International Conference on Computer Communication and Informatics (ICCCI), 2015, pp. 1-6: IEEE.

[23] A. Tsetse, E. Bonniord, P. Appiah-Kubi, and S. Tweneboah-Kodua, "Performance Study of the Impact of Security on 802.11 ac Networks," in Information Technology-New Generations: Springer, 2018, pp. 11-17.

[24] S. S. Kolahi and A. Almatrook, "Impact of Security on Bandwidth and Latency in IEEE 802.11 ac Client-to-Server WLAN," in 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), 2017, pp. 893-897: IEEE.

[25] P. A. Ochang and P. Irving, "Performance analysis of wireless network throughput and security protocol integration," Int J Future Generation Commun Netw, vol. 9, no. 1, pp. 71-78, 2016.

[26] T. A. Ashraf Bourawy, "Performance Analysis of IEEE 80.11ac Wireless Local Area Networks," International Journal of Advanced Research in Computer and Communication Engineering, vol. 6, no. 4, pp. 608-613, April 2017 2017.

[27] O. E. Ademola, "Impact of Wireless Security Protocols on Data Throughput," Computing, Information Systems, Development Informatics & Allied Research Journal, vol. 8, no. 1, pp. 1-12, 2018.