The Impact of Security Protocols on TCP/UDP Throughput in IEEE 802.11ax Client-Server Network: An Empirical Study

Nurul I. Sarkar *, Nasir Faiz, Jahan Ali

Posted Date: 11 August 2025

doi: 10.20944/preprints202508.0757.v1

Keywords: IEEE 802.11ax; security; Wi-Fi 6; TCP/UDP; WPA3; packet loss; throughput

 doi:10.20944/preprints202508.0757.v1

Article

The Impact of Security Protocols on TCP/UDP Throughput in IEEE 802.11ax Client-Server Network: An Empirical Study

Nurul I. Sarkar [1,*], Nasir Faiz [1] and Jahan Ali [1,2]

[1] Department of Computer and Information Sciences, Auckland University of Technology, Auckland 1010, New Zealand

[2] Department of IT and Electrical Engineering, International College of Auckland, Auckland 1010, New Zealand

* Correspondence: nurul.sarkar@aut.ac.nz; Tel: +64211758390

Abstract

The IEEE 802.11ax (Wi-Fi 6) technologies provide high capacity, low latency, and increased security. While many network researchers examine Wi-Fi security issues but the security implications of 802.11ax have not been fully explored yet. Therefore, in this paper, we investigate how security protocols (WPA2, WPA3) affect TCP/UDP throughput in IEEE 802.11ax client-server networks using a testbed approach. Through an extensive performance study, we analyze the effect of security on transport layer protocol (TCP/UDP), internet protocol layer (IPV4/IPV6), and operating systems (MS Windows and Linux) on system performance. The impact of packet length on system performance is also investigated. Results obtained show that WPA3 offers greater security and its impact on TCP/UDP Throughputs is insignificant, highlighting the robustness of WPA3 encryption in maintaining throughput even in secure environments. With WPA3, UDP offers higher throughputs than TCP and IPv6 consistently outperforms IPv4 in both TCP and UDP throughput. Linux outperforms Windows in all scenarios, especially with larger packet sizes and IPv6 traffic. These results suggest that WPA3 provides optimized throughput performance in both Linux and MS Windows in 802.11ax client-server environments. Our research provides some insights into the security issues in Gigabit Wi-Fi that can help network researchers and engineers to contribute further towards developing greater security for the next generation wireless networks.

Keywords: IEEE 802.11ax; security; Wi-Fi 6; TCP/UDP; WPA3; packet loss; throughput

1. Introduction

The IEEE 802.11ax ("802.11ax") standard (Wi-Fi 6) is one of the most widely used gigabit Wi-Fi technologies (released in 2018) even though a new Wi-Fi 7 (802.11be) technology has recently been released (2024). However, 802.11ax is intended to address the most critical issues facing Wi-Fi today, including performance, device proliferation, and application diversity [1–8]. The 802.11ax addresses capacity and offered four times higher speed of 802.11ac (Wi-Fi 5). The capability to operate both at 5GHz and 2.4 GHz simultaneously is an improvement in 802.11ax compared to 802.11ac which can operate at 5GHz only [9–11]. In addition, 802.11ax technology can help in dealing with performance issues of IoT devices that support only 2.4 GHz connections. Finally, Wi-Fi (802.11ax) offers better system performance as the devices receive data simultaneously and IoT traffic management.

The wireless local area network (WLAN) known as Wi-Fi covers up to a hundred meters depending on the environment and setup, such as offices, homes, public places, and public transport. The wireless metropolitan area network (WMAN) covers about a city, and wireless wide area network (WWAN) covers an area larger than a city up to about 50 km [3]. One of Gigabit Wi-Fi 802.11ac technologies was introduced in [12]. Many organizations and residential houses are still

 doi:10.20944/preprints202508.0757.v1

using 802.11ac wireless communication due to low cost [11]. Next 802.11ax was introduced in 2020 offering multigigabit Wi-Fi (up to 10 Gbps), which is the point of interest in this paper. It is a high-efficiency Wi-Fi technology incorporates significant advancements [13]. The primary focus of 802.11ax is to improve the throughput at media access control (MAC) layer [14].

Compared to its predecessors, there are various modifications in 802.11ax, including a higher throughput-per-area, a new PHY protocol, and more advanced modulation and coding schemes [12]. Furthermore, with the introduction of uplink (UL) multi-user multiple-input multiple-output (MU-MIMO) technology, the reduction of the channel sounding using UL MIMO transceivers, the reduction in the time to transmit the HE long-training fields (HELTF). This technology offers eight spatial streams, more efficient spectrum usage [14]. Additionally, recent advancements in Wi-Fi 6E incorporate several enhancements such as increased data transfer speeds, decreased latency, increased capacity, and better traffic management [1,15].

The number of the MIMO spatial streams and the widening of the channel are the same in both 802.11ax and 802.11ac, but 802.11ax has better PHY protocol and higher modulation and coding schemes. In addition, 802.11ax uses an orthogonal frequency division multiple access (OFDMA) approach which is new in Wi-Fi but extensively used in cellular networks. In comparison to wired networks, wireless networking systems are vulnerable to various security threats due to their inherent nature and characteristics.

There are three security modes in WLANs. These modes include open security, personal, and enterprise security. Secure communication is necessary for securing wireless networking systems from personal to enterprise level [11]. WPA, WPA2, and WPA3 are examples of wireless security protocols. These securities may impact the performance of WLAN. To provide authentication, authorization, and data integrity to the connected nodes, a server and Enterprise Security mode are required. A RADIUS (Remote Authentication Dial-In User Service) [12] server runs on Linux and is used for implementing the enterprise protocols. The research questions/challenges and research contributions are discussed next.

1.1. Research Challenges

In this study, we address the following three research questions/challenges:

Research Question 1: What impact does WPA3 have on throughput performance of 802.11ax client-server networks?

To address Research Question 1, we identify and discuss the key factors influencing security protocols affecting the performance of 802.11ax networks. These factors include encryption overhead, key management, and protocol negotiation times. The proposed solution involves analyzing WPA3 protocols in both personal and enterprise settings using a RADIUS server for enterprise-level authentication. WPA3 introduces small overheads due to its advanced encryption, but it ensures greater security and maintains high throughput in 802.11ax networks due to the efficiency of the protocol in high-density environments.

Research Question 2: What impact do transport layer protocols (TCP and UDP) have on throughput performance of 802.1ax in IPv6 networks?

The selection of transport protocols (TCP or UDP) can significantly influence network performance, particularly when combined with IP protocols (IPv4 vs. IPv6) and varying packet sizes. The connection-oriented nature of TCP contrasts with the connectionless approach of UDP, leading to differences in overhead, which in turn affects throughput and latency.

To explore Research Question 2, we examine the specific factors that distinguish the impact of TCP and UDP on network performance in both IPv4 and IPv6 environments. The key factors include protocol overhead, packet loss, and throughput efficiency. In our methodology, both TCP and UDP protocols were implemented and tested across IPv4 and IPv6 networks using different packet sizes. The findings revealed that UDP, being connectionless, delivered lower latency but experienced higher packet loss compared to TCP. Conversely, TCP, due to its connection-oriented design,

 doi:10.20944/preprints202508.0757.v1

achieved higher throughput, particularly with larger packet sizes. Additionally, IPv6 demonstrated slightly improved performance with large packets, attributed to its more efficient header structure.

Research Question 3: What impact multi-user MIMO (MU-MIMO) on the performance of 802.11ax networks in high-density environments, and how can security protocols (WPA3) be optimized to support this?

The 802.11ax introduces uplink and downlink MU-MIMO, allowing multiple devices to communicate simultaneously. However, managing multiple simultaneous connections in high-density environments (e.g., public places or large offices) poses challenges for maintaining high throughput and low latency, especially when security protocols like WPA3 are applied. The complexity of securing these parallel connections without degrading performance needs to be explored.

To address Research Question 3, we assess the various dynamics that influence the performance of MU-MIMO in high-density environments, including channel interference, device synchronization, and security overhead. The proposed solution implements uplink and downlink MU-MIMO in IEEE 802.11ax networks with WPA3 encryption and tests performance in crowded scenarios. Our results show that MU-MIMO significantly improves throughput by allowing multiple devices to communicate simultaneously. However, the additional encryption overhead from WPA3 introduces minimal delays in device synchronization. To mitigate this, we propose optimizing WPA3 key management and encryption algorithms, ensuring that security does not negatively impact MU-MIMO performance.

1.2. Research Scope and Contribution

The main contributions of this paper are outlined as follows:

- We provide an in-depth evaluation of 802.11ax security protocols (WPA2 and WPA3) in client-server networks. To this end, we thoroughly investigated the impact of WPA2 and WPA3 on system performance in both personal and enterprise networking environments.
- We optimize WPA3 performance in high-density environments by reducing the overhead introduced by advanced encryption processes, ensuring both security and efficiency in wireless communication. To this end, we demonstrate the effect of these security protocols on network throughput.
- We provide a comparative analysis of the impact of transport layer protocols (TCP and UDP) on system performance for IPv6 network layer protocol. To this end, we provide a detailed comparison of TCP and UDP protocols, analyzing their performance across both IPv4 and IPv6 802.11ax networks. By varying packet lengths, we examined protocol efficiency, packet loss, and latency. This contribution provides an insight into the optimal transport protocols and packet lengths for achieving higher throughput and reliability in both legacy and modern IP networks Wi-Fi 6 standards.
- We study the performance optimization of Multi-User Multiple Input Multiple Output (MU-MIMO) in high-density 802.11ax networks. To this end, we investigate the impact of uplink and downlink MU-MIMO in 802.11ax in high-density environments, focusing on the synchronization and management of multiple devices. We also explored the methods of security protocols like WPA3 could be optimized to maintain high throughput and low latency in such settings. Our study demonstrates practical methods to improve MU-MIMO performance, enabling efficient multi-user communication in dense networks while ensuring robust security.

1.3. Structure of the Paper

The related work on 802.11ax Wi-Fi security protocols and network performance are presented in Section 2. The research methodology is discussed in Section 3. The system evaluation, test results, and analysis of the impact of security protocols (WPA2, WPA3), transport protocols (TCP, UDP), and IP versions (IPv4, IPv6) on system performance are presented in Section 4. The benefits and practical implications are discussed in Section 5. Finally, the paper is concluded in Section 6.

 doi:10.20944/preprints202508.0757.v1

2. Background and Related Work

IEEE 802.11ax, also known as Wi-Fi 6, represents a significant evolution in wireless networking technology. It addresses growing demands for high-speed, high-capacity wireless communication, especially in dense environments such as offices, stadiums, and urban areas. While Wi-Fi 6 promises substantial improvements over its predecessor (IEEE 802.11ac), particularly in terms of throughput, latency, and capacity, several factors influence its real-world performance, including security protocols, transport layers (TCP/UDP), and network layers (IPv4/IPv6). These factors are crucial when assessing the practical application of Wi-Fi 6 in diverse environments [16–23].

Wi-Fi 6 introduces several key features that distinguish it from previous Wi-Fi standards. Orthogonal Frequency Division Multiple Access (OFDMA) and MU-MIMO significantly enhance the efficiency and capacity of the network by enabling simultaneous data transmission from multiple devices. The enhanced Basic Service Set (BSS) coloring feature reduces interference in high-density environments, further improving throughput [17].

The work by Khorov et al. [20] provides an in-depth analysis of the enhancements brought by 802.11ax, particularly in crowded environments. Their study shows that the standard is well-suited to handle the increasing proliferation of IoT devices, smart appliances, and other connected devices, which require stable and high-capacity wireless networks. However, while Wi-Fi 6 offers numerous advancements, its performance is subject to various external factors, especially in relation to the security protocols that protect data integrity and user privacy [20]. Security protocols are vital for safeguarding wireless networks, particularly in enterprise and public environments. The WPA3 protocol, introduced to replace WPA2, provides enhanced encryption and better protection against brute-force attacks. However, the trade-off is the additional computational overhead introduced by WPA3, which can degrade network performance, especially in bandwidth-intensive applications.

Alghamdi [21] conducted a comparative analysis of WPA2, and WPA3 security protocols on Wi-Fi networks and found that WPA3's advanced encryption mechanisms introduced significant latency and reduced throughput compared to WPA2. However, the existing literature has focused primarily on isolated environments, and there is limited research on the interaction between security protocols and other network layers, such as the transport and internet layers. This research addresses this gap by critically examining the effect of WPA2 and WPA3 on Wi-Fi 6 performance in different transport (TCP/UDP) and network layers (IPv4/IPv6) to provide a more holistic understanding of how security protocols influence network performance in real-world applications. The transition from IPv4 to IPv6 has been a major focus in recent networking literature, driven by the growing demand for IP addresses due to the proliferation of IoT devices and mobile technology. IPv6 offers a larger address space, better routing efficiency, and enhanced support for mobile networks, making it more suitable for modern networking needs. It also eliminates the need for Network Address Translation (NAT), reducing overhead and improving performance [24]. Deng et al. ([25] demonstrated that IPv6 generally outperforms IPv4 in Wi-Fi networks, particularly in terms of latency and throughput. However, these studies focused primarily on earlier Wi-Fi standards such as IEEE 802.11ac, and there is limited research on how IPv6 performs in Wi-Fi 6 environments, particularly in combination with advanced security protocols like WPA3.

MU-MIMO is one of the most important features of Wi-Fi 6, allowing multiple devices to communicate simultaneously with the access point. This significantly enhances network capacity and reduces latency in high-density environments. However, managing multiple connections poses challenges, particularly when security protocols like WPA3 are in place. Hoefel [17] explored the impact of MU-MIMO on network performance in Wi-Fi 6 networks and found that while MU-MIMO improves throughput, it also increases the complexity of device synchronization, especially when encryption is enabled. Additionally, packet size plays a significant role in determining network performance. Larger packets generally lead to higher throughput but can cause more packet loss in congested networks. Tsetse et al. [19] showed that packet size optimization is crucial for balancing throughput and latency in Wi-Fi networks.

 doi:10.20944/preprints202508.0757.v1

The literature highlights significant advancements in Wi-Fi 6 technology, particularly in terms of throughput, latency, and efficiency. However, the interaction between security protocols, transport layers, and network layers remains underexplored. While WPA3 offers enhanced security, its impact on network performance is substantial, particularly when combined with TCP/UDP protocols and IPv4/IPv6 configurations. By critically analyzing these interactions, this research contributes to the optimization of Wi-Fi 6 networks for both performance and security, addressing the gaps identified in the existing literature. Deng et al. [26] provide a comprehensive evaluation of IEEE 802.11ax WLANs, emphasizing its ability to enhance throughput and spectral efficiency. The study highlights the role of OFDMA in enabling simultaneous transmission to multiple users, thereby reducing contention and improving network efficiency. Similarly, Weller et al. [16] focus on the performance measurement of 1024-QAM and Downlink OFDMA, demonstrating significant improvements in data rates and spectral efficiency. Their findings indicate that these features are particularly effective in environments with high user density, such as stadiums and urban areas. However, the performance gains of Wi-Fi 6 are not without challenges. Qu et al. [27] note that the efficient deployment of Wi-Fi 6 requires careful configuration and management of network resources. For instance, the dynamic allocation of OFDMA subcarriers and the optimization of MU-MIMO transmissions are critical for maximizing throughput. The study also highlights the need for robust interference management techniques to mitigate the impact of co-channel interference in dense deployments.

Alghamdi [21] examines the impact of security protocols on the performance of WLANs, focusing on IEEE 802.11ac. The study highlights the trade-offs between security and performance, noting that encryption and authentication mechanisms can introduce significant overhead, thereby reduce throughput and increase latency. While the study predates Wi-Fi 6, its findings are relevant for understanding the security-performance trade-offs in modern WLANs. Tsetse et al. [28] extend this analysis to IEEE 802.11ac networks, demonstrating that the overhead associated with security protocols can have a pronounced impact on network performance. Their findings suggest that the implementation of advanced security mechanisms in Wi-Fi 6 must be carefully balanced against the need for high throughput and low latency.

The studies provide valuable insights into the performance and security of Wi-Fi 6 networks. However, several gaps remain in literature. First, there is limited research on the interaction between advanced security mechanisms and the performance of Wi-Fi 6 in high-density environments. Second, the impact of Wi-Fi 6E on network security requires further investigation, particularly in the context of emerging threats and vulnerabilities. Finally, more work is needed to address the challenges of deploying Wi-Fi 6 in real-world scenarios, including interference management, resource allocation, and the optimization of security protocols. The summary of related work is presented in Table 1.

Table 1. Summary of related work on impact of security protocols on Wi-Fi client-server network.

Reference	Scope	Transport Layer (TCP/UDP)?	IP Layer (IPv4/v6)?	Gigabit Wi-Fi Security?	Testbed approach?
[29]	802.11ax dynamic sensitivity control	×	×	×	√
[22]	Overview of 802.11	×	×	×	×
[26]	Performance evaluation of 802.11ax	√	×	×	√
[24]	802.11ax performance for Infrastructure	√	√	×	√
[16]	Wi-Fi 6 performance of 1024-QAM and DL OFDMA	√	×	√	√
[18]	Wireless security in Wi-Fi 6e networks	×	×	√	×

 doi:10.20944/preprints202508.0757.v1

[27]	Survey and performance evaluation of 802.11ax	√	√	√	√
[30]	Dynamic sensitivity control in WLANs	×	×	×	√
[31]	Throughput analysis of 802.11ac security	√	×	√	√
[28]	Impact of security on 802.11ac networks	√	×	√	√
[20]	Tutorial on 802.11ax high efficiency WLANs	√	√	×	√
Our work	Exploring Wi-Fi 6 security	√	√	√	√
	Investigated the effect of Wi-Fi 6 Security on TCP/UDP throughput and packet losses in client-server networks using a testbed approach.				

3. Methods

3.1. Research Methodology Adopted

We employ a test-bed measurement approach to study the system performance. Research methodologies are typically categorized into three main types: qualitative analysis, quantitative analysis, and a mixed-method approach that combines both. For this study, a quantitative approach was adopted (testbed) to evaluate the network's performance.

In this study we focus on system throughput performance. We also measure jitter and packet losses empirically. The network performance metrics that we considered are briefly discussed next.

- **Throughput**: Throughput is the quantity of application layer data transferred across the network. It is the rate at which messages are transmitted from source to the destination node. For instance, a network throughput is the average data rate (measured in bits per second) across the network. For maximum performance, all packets must be able to get to the right destination without any errors. If an excessive number of packets are losing their way during transmission, the network's performance is likely to be dropped. Therefore, it is crucial to keep track of network traffic speed. It can help gain the visibility of network performance in real-time and provide better understanding of the rate of delivery of packets. The network's throughput average is generally believed to reflect the network's overall performance accurately. The fact that if network throughput performance is not optimal indicating an issue with packet loss or network congestion on the network.
- **Packet Loss:** Packet losses occur when some or all the data packets moving over a network do not reach their destination. Loss of packets in the TCP connection can also prevent congestion and deliberately reduce the speed of the connections. For example, for UDP Down to 60 Mbps and losses 40% indicating that during the most recent test cycle, the server sent one megabit of data in 10 milliseconds and the client received 0.6 megabits in 10 milliseconds, with 0.4 megabits lost in transit. It is usually the reason for the loss of packets. There are two primary protocols that can be transmitted either TCP or User Datagram Protocol (UDP) transport layer protocol. The TCP needs a reliable connection to send traffic. It returns to the packets lost in times with a very high delay and resends them until they reach their destination. When using UDP traffic, there is no automated transmission for lost packets. However, UDP is utilized in live streaming applications (e.g., VoIP and video traffic), handling specific amounts of loss of packets.
- **Jitter:** Information is transferred to data packets transmitted over the network. Jitter is a measure of delay variance (in milliseconds) experienced by the packets of the same flow. For real-time applications (e.g., voice and video), the packets must be released to the destination in the correct order and at the same rate released at the source. The buffer at the client (called de-jitter buffer) compensates for the jitter introduced by the network if the delay variation is not too much. It is usually caused by congestion on networks, and occasionally, routes change.

 doi:10.20944/preprints202508.0757.v1

3.3. Research Methods

The purpose of empirical study (testbed) was to observe live network performance using real hardware/software. The client-server network testbed is shown on Figure 1. It consists of a Server, an 802.11ax Access point/Router (TP-Link) and a wireless client (802.11ax laptop). The server is connected to TP-Link Router with a category 6 (CAT6) cable (1 Gbps).

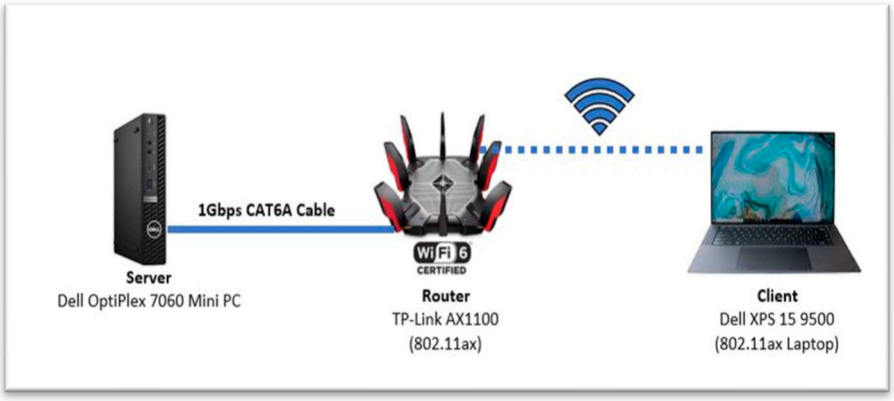


Figure 1. The Gigabit Wi-Fi 6 (802.11ax) client-server network testbed.

We studied the transport layer (TCP/UDP), network layer (IPv4/IPv6), and WPA2 and WPA3 security protocols to explore the impact of security on system performance. We first examine the performance of Wi-Fi 6 security in an open system (no security). We then validate the system performance enabling the WPA2 and WPA3 security protocols. For all the scenarios considered in the investigation, Windows Firewall and Antivirus are disabled. The router is configured to only work as an AP and in 802.11ax mode, with a 5GHz operating frequency (for interference-free communication frequency of wireless channel 48, 5.2 GHz). We first configured access point (AP) to disabled security protocol to create an open system for investigation. We then configured WPA2 and WPA3 for further exploration and investigation. This allows us to investigate the impact of Gigabit Wi-Fi security on system performance.

3.4. Data Generation Tool

IPerf [1] is as an open-source network analysis tool to measure network bandwidth. This tool offers client/server network functionality to measure throughputs between nodes. iPerf generates TCP and UDP traffic loads between two hosts. It determines the maximum network bandwidth (throughput) between a server and a client to perform stress testing on the network's communication channel. It is compatible with Linux and Windows operating systems for various parameters as shown in Table 2, including TCP and UDP with IPv4 and IPv6 protocols.

Table 2. Parameters used in the investigation.

Parameter	Value
Network Configuration	Client/Server
Security Protocol	Disable
Transport layer protocol	TCP/UDP
IP Version	4/6
Packet Size	128Kb
Bandwidth/data rate	1024Mbps
Time	30 seconds

 doi:10.20944/preprints202508.0757.v1

3.5. Windows Testbed Setup (Microsoft Windows, 64-bit)

The objective of the Windows testing method is to assess the performance of the network using iPerf3 as a network testing tool on both the server and client sides. By running iPerf3 on a Windows Server and connecting it with a Windows Client, the experiment measures the network's bandwidth and performance under specific parameters such as packet size, bandwidth, and duration. The test evaluates the effectiveness of IPv4 communication, with a focus on throughput and data transfer efficiency over a 30-second window. The results provide insights into the network's capacity to handle varying packet sizes and bandwidth settings under controlled conditions. The following commands parameters of windows have been set for the testing purposes as shown in Table 3.

Table 3. Technical specifications for setting up a testbed.

Hardware/software	Function	Technical specifications
TP-Link AX11000 Tri-Band Router	Wireless router	AX11000 delivers Wi-Fi Speeds over 10 Gbps
Dell XPS 15 9500	Client	Intel Core i7-10750H@ 2.60GHz 16GB DDR4 Ram Intel Wi-Fi 6 AX1650s Wireless Network Adapter 160MHz
Dell OptiPlex 7060	Server	Intel i5-8500T 2.1-GHz 8 GB DDR4 RAM Intel 7 I219-LM Gigabit Ethernet Adapter
IPerf 3	Traffic generator/collector	
CommView for Wi-Fi	Wireless monitoring tool	802.11 a/b/g/n/ac/ax networks
MS Windows OS	Server and Client	Windows 10 (64-bit)

4. Results

The client-server network (Windows-based) testbed was set up and configured to study the system performance. The investigation centered on four primary performance metrics including MS Windows TCP and UDP throughputs, jitters, and packet losses (IPv4 vs. IPv6). These results and comparative analysis provide a deeper understanding of the impact of security protocols on system performance in varying packet lengths. After the initial observation, we obtain TCP/UDP throughputs for open security, WPA2, and WPA3 utilizing both IPv4 and IPv6 traffic. It is important to note that jitter and packet losses are also measured and analyses. The UDP traffic analysis is particularly relevant to connectionless communication protocols where packet timing and loss significantly impact the system performance. This structured approach enabled a thorough evaluation of the interplay between security protocols, transport layers, and IP versions in the Windows environment. The system performance measurement and analysis are structured through six studies presented next.

(i) Study 1: Throughput performance

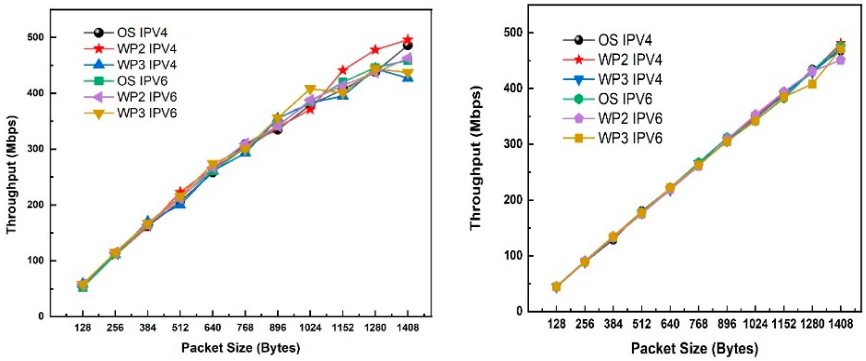
In Figure 2 (a), we plot packet length versus TCP throughput for WPA2 and WPA3 security protocols for both IPv4 and IPv6 client-server (MS Windows 10) network. The results for open security (device security turn off) are also presented for comparison purposes. Likewise, the impact of Wi-Fi 6 security on UDP throughput is shown in Figure 2 (b).

Generally, TCP throughput increases as packet length increases. In an open network, IPv4 considerably outperforms IPv6 for all packet sizes. The noticeable difference was observed at packet length of 1024-byte IPv6 outperforms IPv4 by 23% at this packet size (520 Mbps for IPv6 compared to 400 Mbps for IPv4), which offers a 120 Mbps increase in throughput.

For WPA2, IPv6 outperforms IPv4 for all packet sizes. IPv6 outperforms IPv4 by 21% (480 Mbps for IPv6 and 380 Mbps for IPv4) and offers a maximum throughput increase of 100 Mbps. For WPA3, the maximum difference in throughput is spotted at packet length of 1024 bytes. IPv6 offers higher

 doi:10.20944/preprints202508.0757.v1

throughput than IPv4 by 20% (490 Mbps for IPv6 and 390 Mbps for IPv4). Therefore, when running IEEE 802.11ax in an open system network, TCP maintains consistent throughput regardless of packet sizes. The most significant difference in throughput between an open system and one with WPA2 security is observed at packet length of 1408 bytes.



2(a) TCP Throughput **2(b) UDP Throughput**

Figure 2. Effect of Wi-Fi 6 Security (Open system, WPA2 and WPA 3) on throughput performance in IPV4 and IPV6 network (a) TCP Throughput; and (b) UDP Throughput.

By looking at Figure 2(b), it is evident that UDP throughput increases with packet size increases. For an open security (no security), IPv6 offers higher throughput than IPv4 across all packet sizes. For instance, IPv6 achieves 16.5% (575 Mbps for IPv6 and 480 Mbps for IPv4) higher UDP throughput than IPv4 at the packet size of 1408 bytes. For WPA2 security, the greatest disparity between IPv6 and IPv4 occurs at packet size of 1280 bytes, with IPv6 surpassing IPv4 by 18.2% (520 Mbps for IPv6 compared to 425 Mbps for IPv4). Similarly, for WPA3 security, the maximum throughput difference is observed at packet size of 1408 bytes, where IPv6 outperforms IPv4 by 17.4% (570 Mbps for IPv6 versus 470 Mbps for IPv4).

When comparing IPv4 performance across the studied security modes (open security, WPA2, and WPA3), the TCP throughput remains approximately consistent, indicating minimal variation. In contrast, IPv6 exhibits slight differences in throughput depending on the security mode. The most notable difference occurs at packet size of 1408 bytes, where WPA2 drops throughput by 7.7% (520 Mbps for open system and 480 Mbps for WPA2). This suggests that while IPv6 generally delivers superior performance, the choice of security mode can influence throughput, particularly at larger packet sizes. These findings highlight the importance of considering IP versions and security configuration when optimizing throughput performance. We observe that WPA3 drops TCP and UDP throughputs by 3.8% and 0.9% for IPv6. Overlay, IPv6 outperforms IPv4 in both open and protected systems such as WPA2 and WPA3.

(ii) Study 2: Jitter performance

Figure 3 shows the Jitter (ms) for IPv4 and IPv6 on WLAN 802.11ax Client-Server (Windows 10) with WPA2 and WPA3 security and open system. One can observe that this test exhibits no jitter for both IPv4 and IPv6, which correspond to all OS, WPA2, and WPA3 security protocols.

 doi:10.20944/preprints202508.0757.v1

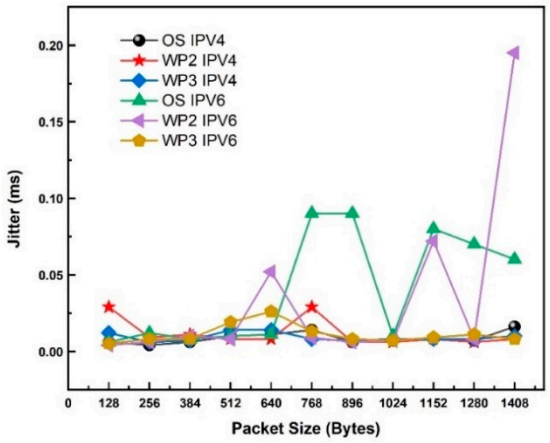


Figure 3. Jitter performance. Comparison of 802.11ax performance for Open System vs. WPA2 and WPA3 security in IPV4 and IPV6 network.

(iii) Study 3: Packet losses

Figure 4 shows the lost datagram for IPv4 and IPv6 in an 802.11ax client-server network for security protocols (WPA2 and WPA3). Operating systems supporting IPv4 and IPv6 were identified by measuring their packet sizes between 128 and 1408 bytes. The results for lost datagrams show that both MS Windows and Linux IPv4 portray the same throughputs. For IPv6, the lost datagram (in %) steeply increases as the packet size increases. However, Windows outperforms (about 5%) Linux for most larger packet sizes. The maximum performance difference between Linux and Windows IPv6 is at packet size of 512 bytes. However, Linux outperforms Windows IPv6 by 100%.

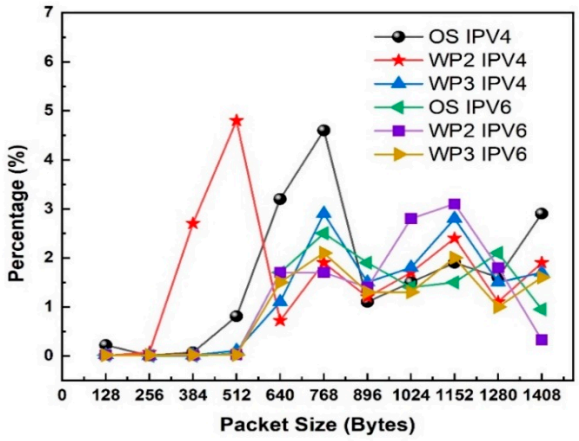


Figure 4. Packet losses. Comparison of WPA2, WPA3 and open security for IPV4 and IPV6 network.

4.2. Comparative Analysis

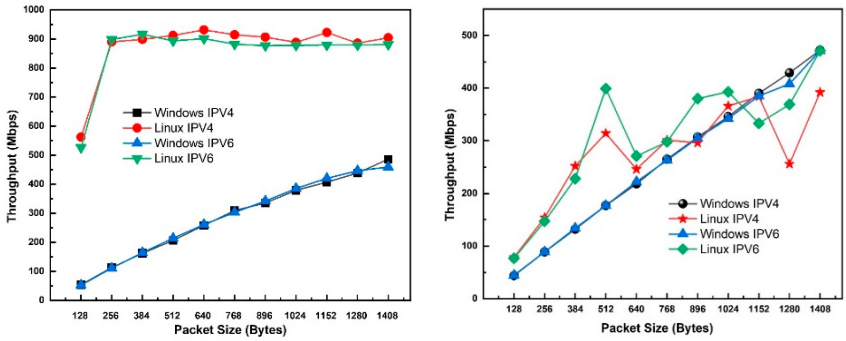
In this section we study the impact of Windows and Linux on system throughput for various security protocols, including WPA2 and WPA3. We focus on analyzing system performance using both Linux and Windows testbeds for various scenarios, including the effect of WPA3, WPA2, and open security on TCP/UDP throughput (Windows vs. Linux).

(iv) Study 4: Effect of WPA3 on Throughput (Windows vs. Linux)

Figure 5 (a) shows WPA3 TCP throughputs for IPv4 and IPv6 on 802.11ax Client-Server Windows 10 operating system (OS). The result for Linux is also shown for comparison purposes. In most scenarios, as packet sizes increase, so does TCP throughput for MS Windows. For Linux, throughput rises with an increase in packet sizes to 900 Mbps, after which the curve flattens. On a

 doi:10.20944/preprints202508.0757.v1

WPA3 network, Linux IPv6 and IPv4 significantly outperform Windows 10 by about 40% for all packet sizes, with a maximum difference of 87.6% at packet size of 256 bytes. Linux OS exceeds Windows system by 87.6% (900Mbps for Linux system and 111 Mbps for windows). For WPA3, in the windows operating system, the TCP throughput increases equally for IPv4 and IPv6 with packet sizes.



(a) TCP Throughput **(b) UDP Throughput**

Figure 5. Effect of WPA3 Security on Throughput (Windows vs. Linux) in IPV4 and IPV6 network. (a) TCP Throughput; and (b) UDP Throughput.

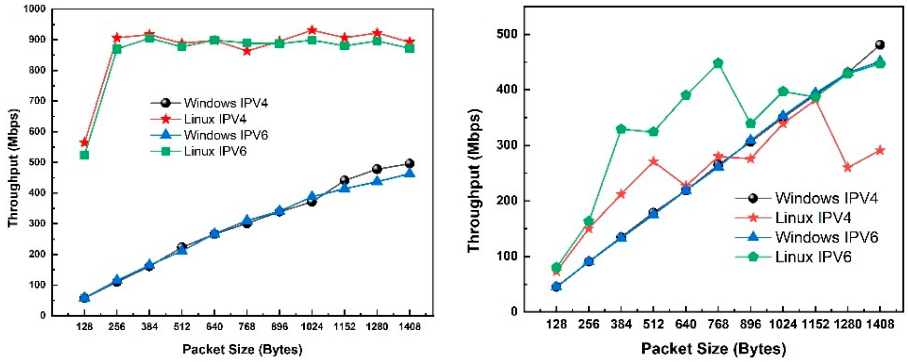
Figure 5(b) shows the UDP throughput for IPv4 and IPv6 on 802.11ax Client-Server (Windows vs Linux) with WPA3 security. As the packet size changes, UDP's throughput also increases consistently along with them. UDP throughput for Linux with IPv6 outperforms Windows IPv6 for all packet sizes up to 1152 bytes, after which the throughput drops consistently with increasing packet size to 1280 bytes and rises again to 1480 bytes, though at a lower rate than MS Windows. Linux throughput on IPv4 outperforms IPv4 Windows for all packet sizes with an average improvement of 30.6%. For WPA3 in Linux vs Windows with IPv4, the maximum difference between Linux IPv4 and Windows IPv4 is at packet size of 512 bytes, where IPv6 outperforms IPv4 by 51.7% (369 Mbps for Linux IPv4 vs 178 Mbps for Windows IPv4), representing a 191 Mbps increase. IPV6's WPA3 security shows that between two OS systems are spotted at 512 bytes where IPV6 Linux shows 372 Mbps over IPV6 Windows at 178 Mbps which is 52.15% difference. On MS Windows, IPv4 and IPv6 had approximately equal throughput for all packet sizes. Across the board, Linux outperforms MS Windows in WPA3-secured networks.

(v) Study 5: Impact of WPA2 Security on Throughput (Windows vs. Linux)

Figure 6 (a) shows the TCP throughput for IPv4 and IPv6 on 802.11ax Client-Server (Windows 10 vs Linux) with WPA2 security. In most scenarios, as the packet size increases, the throughput of TCP also increases consistently for Windows. For Linux, the throughput increases with an increase in packet size to 900 Mbps, after which the curve flattens. On the WPA2 network, Linux IPv6 and IPv4 significantly outperform Windows 10 on all packet sizes by about 40%, with the most significant difference at a packet size of 256 bytes. On WPA2 network, Linux IPv6 and IPv4 significantly outperform Windows for all packet sizes by about 40%. The TCP throughput increases equally for IPv4 and IPv6 throughout the packet lengths for Windows. The Linux system with WPA2 outperforms Windows on IPv6 and IPv4, where the maximum difference is spotted at 256 bytes. Overall, Linux outperforms Windows in WPA2 secured system.

Figure 6(b) shows the UDP throughput for IPv4 and IPv6 on Linux and Windows operating systems running on WPA2 secured network. In all scenarios, as the size of the packet increases, the performance of UDP also increases proportionally. The Linux Operating system with IPv6 and IPv4 outperforms Windows IPv4 and IPv6 with an average increase of 50.4% on all packet sizes.

 doi:10.20944/preprints202508.0757.v1

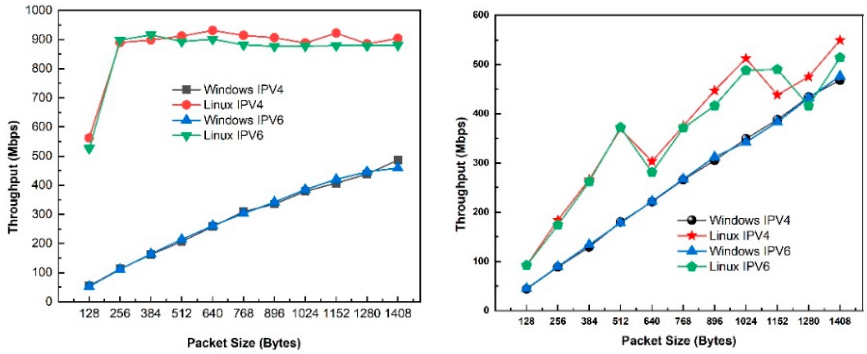


(a) TCP Throughput **(b) UDP Throughput**

Figure 6. Effect of WPA2 Security on Throughput (Windows vs. Linux) over IPV4 and IPV6 network. (a) TCP Throughput; and (b) UDP Throughput.

(vi) Study 6: Impact of Open Security on Throughput (Windows vs. Linux)

Figure 7(a) shows IPv4 and IPv6 TCP throughput on Windows and Linux server for Open security. For Windows, increasing the packet size from 128 to 256 bytes improves throughput by 58.7 Mbps. As we increase the packet size, IPv4 performs equally as IPv6 throughout the packet's length, with a slight difference at packet size of 1408 bytes. For Linux, UDP throughput increases with increased packet size consistently, to 898Mbps, after which the curve flattens. IPv4 performs better than IPv6, with the highest throughput difference of 16 Mbps at 1152 bytes for all packet sizes. As packet size increases, performance remains nearly constant up to 1408 bytes. Linux operating systems with IPv4 and IPv6 have the same throughput for small packet sizes (256 bytes). Still, the throughput increases steeply as the packet size increases. However, for most of the large packet sizes, throughput is slightly constant. Also, IPv4 gives a higher throughput than IPv6 for packet sizes larger than 384 bytes. We observe that Linux outperforms Windows throughout the packet sizes by 60%. The maximum difference is at packet size of 256 bytes, where the Linux server outperforms Windows by 86.6% (898 Mbps for Linux and 111 Mbps for Windows).



(a) TCP IPv4/IPv6 Throughput **(b) UDP Throughput**

Figure 7. Effect of Open security on throughput (Windows vs Linux) over IPv4/IPv6 network (a) TCP Throughput; and (b) UDP Throughput.

Figure 7(b) compares UDP throughput of IPv4 and IPv6 using Windows and Linux security. We observe that the highest throughput is achieved using Linux client-server network than MS Windows 10 Server. For example, for IPv4 using Linux Server, the throughput is 549 Mbps (13.3% increase from Windows 10, which has a throughput of 476) at a packet size of 1408 bytes. On the other hand, the highest throughput for IPv6 using Linux Server is 514 Mbps (7.4% increase from Windows 10 Server, which is at 476 Mbps) at packet size of 1408 bytes. For open system (no security), the maximum difference of IPv4 and IPv6 between Windows and Linux was observed at packet size of 512 bytes where IPv6 and IPv4 on Linux outperform MS Windows by 52.15%.

 doi:10.20944/preprints202508.0757.v1

4.3. Summarization of Results

The summary of key research findings is presented in Table 4. The TCP and UDP throughputs (Mbps) for open system (no security), WPA2, and WPA3 for both IPV6 and IPv4 are shown in Row 2 and Row 3, respectively. Column 5 shows average throughput drops because of Wi-Fi 6 WPA3 security protocol. For instance, WPA3 TCP throughput drops by 3.8% $[\frac{520-500}{520} \times 100\%]$ for IPv6. This throughput degradation is due to encryption overheads.

Table 4. Effect of WPA3 security on TCP/UDP throughput dropping.

	Open system	**WPA2**	**WPA2 Throughput drops (%)**	**WPA3**	**WPA3 Throughput drops (%)**
TCP Throughput (Mbps)	520 IPv6	480 IPv6	7.7	500 IPv6	3.8
	400 IPv4	380 IPv4	5.0	390 IPv4	2.5
UDP Throughput (Mbps)	575 IPv6	520 IPv6	9.6	570 IPv6	0.9
	480 IPv4	425 IPv4	11.5	470 IPv4	2.1
Note	(1) WPA3 UDP offers 12.3% higher throughput than TCP for IPv6. (2) For WPA3, IPv6 outperforms IPv4 by 23% and 16.5% for TCP and UDP throughputs, respectively.				

5. Benefits and Practical Implications

The results from both Windows and Linux testbeds reveal important insights into the impact of Wi-Fi 6 security protocols (Open security, WPA2, and WPA3) on system performance, especially TCP/UDP throughputs for IPv4 and IPv6. While both operating systems showed consistent patterns, MS Windows demonstrated slightly lower throughput than Linux, especially for IPv6 traffic. The higher efficiency of Linux, particularly in handling IPv6 traffic, can be attributed to its more optimized network stack and reduced overheads. For TCP throughput, the Linux-based testbed consistently outperformed MS Windows, with a significant performance gap observed at larger packet sizes demonstrating a 49% increase in throughput for IPv4 at packet size of 1408 bytes. Similarly, UDP throughput on Linux was notably higher, especially for IPv6, where Linux achieved an 87.7% increase than Windows at a packet size of 256 bytes.

We observe that WPA3 introduced small overheads, as expected, due to its more advanced encryption techniques. However, both Linux and Windows testbeds showed that the performance degradation caused by WPA3 was minimal, particularly for IPv6 traffic, where the simplified and more efficient header structure mitigated the impact. This result highlights the robustness of WPA3 in maintaining high throughput and low latency, even in more secure environments. Jitter and packet losses remained minimal in both operating systems, with slight differences in UDP packet delays. Linux's efficient socket layer and faster kernel switches provide better performance for all security protocols with respect to packet transmission and reception.

Overall, our findings suggest that while both Windows and Linux can handle the demands of 802.11ax networks (Wi-Fi 6), Linux outperforms Windows in most scenarios, particularly when dealing with IPv6 traffic and larger packet sizes. This performance gap is likely due to the inherent differences in the network stack and system architecture between the two operating systems investigated. However, the relatively small differences in throughput, jitter, and packet losses contributing to dropping system performance for all security protocols indicate that 802.11ax wireless network is designed to maintain consistent performance, regardless of the security features enabled. These results highlight the scalability and reliability of 802.11ax, making it suitable for complex, high-demand wireless network environments.

 doi:10.20944/preprints202508.0757.v1

6. Conclusions

This study comprehensively analyzed the security features of 802.11ax (Wi-Fi 6) network across both MS Windows and Linux operating systems. We have measured throughput, packet loss, and packet jitter using iPerf3 tool and provided a detailed assessment of network behavior. The research findings revealed that IPv6 consistently outperformed IPv4, attributed to its streamlined header structure, absence of packet fragmentation, and efficient checksum processing. The testbed was set up to study the system performance and to simulate real-world scenarios, facilitated precise data collection across a range of packet sizes, enabling a robust evaluation of system performance in both Linux and MS Windows server environments. Results obtained have shown that the impact of WPA3 security on TCP/UDP Throughputs is not very significant. For instance, WPA3 drops TCP throughput and UDP throughput by 3.8% and 0.9%, respectively for IPv6. This decrease in throughput is due to overheads introduced by advanced encryption technology. IPv6 consistently outperforms IPv4 in both TCP and UDP throughput. UDP offers higher throughput than TCP in IPv6 environments. Linux outperforms MS Windows in all scenarios, especially with larger packet sizes and IPv6 traffic. However, as networks continue to grow in complexity, further research is recommended to explore potential challenges and optimizations. Future studies could investigate energy efficiency and scalability aspects of 802.11ax networks across both MS Windows and Linux operating systems, particularly in more diverse and demanding network conditions. Such investigations would provide valuable insights into enhancing the deployment and performance of next-generation wireless networks.

References

1. Afaqui, M.S.; Garcia-Villegas, E.; Lopez-Aguilera, E.; Smith, G.; Camps, D. Evaluation of Dynamic Sensitivity Control Algorithm for IEEE 802.11ax. *2015 IEEE Wireless Communications and Networking Conference, WCNC 2015* **2015**, 1060–1065, doi:10.1109/WCNC.2015.7127616.
2. Cranley, N.; Davis, M. Study of the Behaviour of Video Streaming over IEEE 802.11b WLAN Networks. In Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications 2006, WiMob 2006; 2006; pp. 349–355.
3. Banerji, S.; Chowdhury, R.S. On IEEE 802.11: Wireless Lan Technology. *International Journal of Mobile Network Communications & Telematics* **2013**, *3*, 45–64, doi:10.5121/ijmnct.2013.3405.
4. Deng, D.-J.(1); Chen, K.-C.(2); Cheng, R.-S.(3) IEEE 802.11ax: Next Generation Wireless Local Area Networks. In Proceedings of the Proceedings of the 2014 10th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, QSHINE 2014; Institute of Electrical and Electronics Engineers Inc.: (1)Department of Computer Science and Information Engineering, National Changhua University of Education, October 2014; pp. 77–82.
5. Afaqui, M.S.; Garcia-Villegas, E.; Lopez-Aguilera, E. IEEE 802.11ax: Challenges and Requirements for Future High Efficiency WiFi. *IEEE Wirel Commun* **2016**, *24*, 130–137, doi:10.1109/MWC.2016.1600089WC.
6. Deng, D.J.; Lin, Y.P.; Yang, X.; Zhu, J.; Li, Y.B.; Luo, J.; Chen, K.C. IEEE 802.11ax: Highly Efficient WLANs for Intelligent Information Infrastructure. *IEEE Communications Magazine* **2017**, *55*, 52–59, doi:10.1109/MCOM.2017.1700285.
7. Weller, D.; Mensenkamp, R.D.; Vegt, A.V.D.; Bloem, J.-W.V.; Laat, C.D. Wi-Fi 6 Performance Measurements of 1024-QAM and DL OFDMA. *ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Communications (ICC), ICC 2020 - 2020 IEEE International Conference on* 2020, 1–7.
8. Coleman, D. Wireless Security in a 6 GHz Wi-Fi 6E World. *Extreme Networks Blog* 2021.
9. Qu, Q.(1); Li, B.(1); Yang, M.(1); Yan, Z.(1); Yang, A.(1); Deng, D.J.D.-J.(2); Chen, K.C.K.-C.(3) Survey and Performance Evaluation of the Upcoming Next Generation WLANs Standard - IEEE 802.11ax. *Mobile Networks and Applications* **2019**, *24*, 1461–1474, doi:10.1007/s11036-019-01277-9.
10. Aijaz, A.(1); Kulkarni, P.(2) On Performance Evaluation of Dynamic Sensitivity Control Techniques in Next-Generation WLANs. *IEEE Syst J* **2019**, *13*, 1324–1327, doi:10.1109/JSYST.2018.2828318.

11. Alghamdi, T.M. Throughput Analysis of IEEE WLAN "802.11 Ac" Under WEP, WPA, and WPA2 Security Protocols. *Talal Mohammed Alghamdi International Journal of Computer Networks (IJCN)* **2019**, 2019–2020.
12. Tsetse, A.; Bonniord, E.; Appiah-Kubi, P.; Tweneboah-Kodua, S. Performance Study of the Impact of Security on 802.11ac Networks. *Advances in Intelligent Systems and Computing* **2018**, *738*, 11–17, doi:10.1007/978-3-319-77028-4_3.
13. Khorov, E.; Kiryanov, A.; Lyakhov, A.; Bianchi, G. A Tutorial on IEEE 802.11ax High Efficiency WLANs. *IEEE Communications Surveys and Tutorials* **2019**, *21*, 197–216, doi:10.1109/COMST.2018.2871099.
14. Hoefel, R.P.F. IEEE 802.11ax (Wi-Fi 6): DL and UL MU-MIMO Channel Sounding Compression Schemes Impaired with IQ Imbalance and CFO. *IEEE Vehicular Technology Conference* 2020, *2020-May*, 1–6.
15. Kriara, L.; Molero, E.C.; Gross, T.R. Evaluating 802.11ac Features in Indoor WLAN: An Empirical Study of Performance and Fairness. *Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM* **2016**, *03-07-Octo*, 17–24, doi:10.1145/2980159.2980167.
16. Weller, D.; Vegt, A.V.D. Wi-Fi 6 Performance Measurements of 1024-QAM and DL OFDMA. In Proceedings of the Proceedings of the IEEE International Conference on Communications; 2020; pp. 1–7.
17. Hoefel, R.P.F. IEEE 802.11ax (Wi-Fi 6): DL and UL MU-MIMO Channel Sounding Compression Schemes. In Proceedings of the IEEE Vehicular Technology Conference; 2020; pp. 1–6.
18. Coleman, D. Wireless Security in a 6 GHz Wi-Fi 6E World. *Extreme Networks Blog* **2021**.
19. Tsetse, A.; Bonniord, E.; Appiah-Kubi, P. Performance Study of the Impact of Security on 802.11ac Networks. In Proceedings of the Advances in Intelligent Systems and Computing; 2018; Vol. 738, pp. 11–17.
20. Khorov, E.; Kiryanov, A.; Lyakhov, A.; Bianchi, G. A Tutorial on IEEE 802.11ax High Efficiency WLANs. *IEEE Communications Surveys & Tutorials* **2019**, *21*, 197–216, doi:10.1109/COMST.2018.2871099.
21. Alghamdi, T.M. Throughput Analysis of IEEE WLAN "802.11ac" Under WEP, WPA, and WPA2 Security Protocols. *International Journal of Computer Networks* **2019**, *11*, 35–50, doi:10.1109/IJCN.2019.123456.
22. Banerji, S.; Chowdhury, R.S. On IEEE 802.11: Wireless LAN Technology. *International Journal of Mobile Networking & Communication Technology* **2013**, *3*, 45–64, doi:10.5121/ijmnct.2013.3405.
23. Tsetse, A.; Bonniord, E.; Appiah-Kubi, P. Performance Study of the Impact of Security on 802.11ac Networks. In Proceedings of the Advances in Intelligent Systems and Computing; 2018; Vol. 738, pp. 11–17.
24. Deng, D.-J.; Lin, Y.P.; Yang, X.; Zhu, J.; Li, Y.B.; Luo, J.; Chen, K.C. IEEE 802.11ax: Highly Efficient WLANs for Intelligent Information Infrastructure. *IEEE Communications Magazine* **2017**, *55*, 52–59, doi:10.1109/MCOM.2017.1700285.
25. Deng, D.-J.; Chen, K.-C.; Cheng, R.-G. Performance Evaluation of IEEE 802.11ax WLANs. *IEEE Communications Magazine* **2020**.
26. Deng, D.-J.; Chen, K.-C.; Cheng, R.-G. IEEE 802.11ax Performance for Intelligent Infrastructure. *IEEE Netw* **2020**.
27. Qu, Q.; Li, B.; Yang, M.; Yan, Z. Survey and Performance Evaluation of IEEE 802.11ax. *IEEE Communications Surveys & Tutorials* **2020**.
28. Tsetse, A.K.; others Impact of Security on 802.11ac Networks. *Journal of Network and Systems Management* **2018**.
29. Afaqui, M.S.; Garcia-Villegas, E.; Lopez-Aguilera, E. Evaluation of Dynamic Sensitivity Control Algorithm for IEEE 802.11ax. *IEEE Communications Letters* **2017**.
30. Aijaz, A.; Kulkarni, P. Dynamic Sensitivity Control in Next-Generation WLANs. *IEEE Communications Letters* **2017**.
31. Alghamdi, S.A. Throughput Analysis of IEEE WLAN 802.11ac under Security Protocols. *International Journal of Computer Networks & Communications (IJCNC)* **2018**.