Performance Study of the Impact of Security on 802.11ac Networks

3

Anthony Tsetse, Emilien Bonniord, Patrick Appiah-Kubi, and Samuel Tweneboah-Kodua

Abstract

Wireless Local Area Networks (WLAN) are gaining popularity due to the ease of use and ubiquity. Notwithstanding, their inherent characteristics make them more vulnerable to security breaches compared to wired networks. IEEE 802.11ac specification is currently the widely used WLAN standard deployed by most organizations.

We study the impact of security on 802.11AC WLANs using different security modes (No Security, Personal and Enterprise Security) using a test WLAN. The performance analysis is based on throughput, delay, jitter, loss ratio and connection time. Our experiments indicate a performance improvement when no security is implemented relative to other security modes. For throughput performance, improvements ranged between 1.6 and 8.2% depending on the transport (TCP/UDP) and network (IPv4/IPv6) layer protocol. Improvements between 2.8 and 7.9% was observed when no security is implemented for delay. Jitter, Loss Ratio and connection time experienced between 1.3 and 18.6% improvement in performance. Though the performance degradation because of implementing security measures on 802.11ac WLANs appear relatively insignificant per the study, we believe the situation could be different when a heterogeneously complex setup is used. However, other factors (e.g. channel congestion, interference etc.) may equally be responsible for the performance degradation in WLANs that may not be necessarily security related.

Keywords

Security · Wireless Network Performance · 802.11ac · IPv4 · IPv6

3.1 Introduction

In recent times, there has been tremendous advancement in Wireless Local Area Network (WLAN) Technology. The ubiquitous nature of Wireless network architecture has made the system one of the preferred data communication medium in the industry. 802.11ac [1] is one of current wireless communication standards deployed by most organizations and is part of the Wi-Fi (802.11) family of standards developed by IEEE. The specification indicates a default frequency of 5GHz and backward compatibility with earlier [1] standards (e.g. 802.11n) which operate in the 2.4GHz frequency range. The 802.11ac standard extends the capability of its predecessors at the MAC layer. Some of the enhancements in the 802.11ac standard include [2–4];

- extended channel binding
- Multi-user Multiple-input multiple-output (MU-MIMO)
- Spatial streams beam forming.
- Larger channel bandwidths of 80 and 160 MHz
- 256-quadrature amplitude modulation (QAM)
- A theoretical maximum aggregate bit rate of 6.7Gbps at the physical layer is achievable by 802.11ac access points using eight spatial streams.

A. Tsetse (✉)
Department of Computer Science, Northern Kentucky University, Highland Heights, KY, USA
e-mail: tsetse@nku.edu

E. Bonniord
IUT Laninion, University De Rennes, Rennes, France
e-mail: emilien.bonniord@etudiant.univ-rennesl.fr

P. Appiah-Kubi
Information and Technology University of Maryland University College, Largo, MD, USA
e-mail: Patrick.appiahkubi@umuc.edu

S. Tweneboah-Kodua
School of Technology, Ghana Institute of Management and Public Administration, Accra, Ghana
e-mail: stkoduah@gimpa.edu.gh

S. Latifi (ed.), *Information Technology – New Generations*, Advances in Intelligent Systems and Computing 738,
https://doi.org/10.1007/978-3-319-77028-4_3

Wireless Networks by virtue of their characteristics are vulnerable to various security threats compared to wired networks. Most WLANs operate in three security modes; no security, personal and enterprise security. 802.11i [5] standard is the defacto protection standard used in protecting WLANs. Wi-Fi Protected Access version 2 (WPA2) is widely used in the implementation of 802.11i. With Enterprise Security mode, a server is required to provide Authentication, Authorization and Auditing services to the connected nodes. In this study, a Remote Authentication Dial-In User Service (RADIUS) [6] Server running on Linux is used to implement the enterprise security protocols.

We have attempted to study the extent to which the security modes mentioned above impact 802.11ac WLAN performance by running several experiments using a test WLAN. The remainder of this paper is organized as follows. In Sect. 3.2, we briefly discuss related work. In Sect. 3.3, we describe our testbed network, and in Sect. 3.4, a discussion of our finding is presented. The conclusion and future work is given in Sect. 3.5.

3.2 Related Research

IEEE 802.11ac is a new wireless technology standard aimed at improving the speed of transmission, improve throughput, lower latency and improve power usage in wireless devices [7]. As a relatively new standard, research on 802.11ac is very elementary and attracting research interest. A study in [8] investigated the signal strength performance of IEEE 802.11ac in Wi-Fi communication and concluded that the technology can provide good signal quality over distance of up to 1 km as compared to IEEE 802.11n. An empirical study of performance and fairness of 802.11ac feature for an indoor WLAN was conducted in [9]. The study evaluated performance characteristics of the achievable data values of throughput, jitter and fairness in WLAN. Findings of the study showed 802.11ac achieved higher throughput and was fairer with wider channels compared to 802.11a/n. Enhancement for very high throughput in WLAN through IEEE 802.11ac was discussed in [10]. The paper introduced key features as well as MAC enhancements in 802.11ac that affect the performance. The paper further demonstrated that the aggregate MAC service data unit (A-MSDU), aggregate MAC protocol data unit (A-MPDU) and a hybrid of both units outperformed similar configurations in 802.11n. In [11], performance analysis of IEEE 802.11ac Distributed coordination function (DCF) with hidden nodes was conducted and the authors demonstrated that the traditional RTS/CTS handshake had shortcomings that had to be modified to support 802.11ac [21]. The power-throughput tradeoffs of 802.11n/ac in smartphone was discussed in [10]. Theory and practical Wi-Fi capacity analysis for 802.11ac/n was conducted in [12].

To the best of our knowledge, few known security studies have been performed on 802.11ac. Most security studies conducted on wireless standards were conducted on 802.11b/g/n [13–18]. These papers studied the effect of security on performance in WLANs and the robustness of the security standards implemented in these wireless standards.

3.3 Experimental Setup

A test WLAN was configured to run the experiments. Figure 3.1 depicts the topology of the testbed. In Fig. 3.1, Nodes 1 and 2 communicate with each other through the Wireless router and the Server. The experiments involved transmitting data between Nodes 1 and 2 and between Nodes and the webserver. Depending on the experiment run, the Server (Fig. 3.1) functions as a RADIUS Server or Webserver (Apache).

For experiments with no security, the wireless access point was configured such that no security credentials were required from connecting devices. Thus, the no security configuration was an open access network. The personal security mode involved setting up the wireless access point to require connecting devices to enter a paraphrase for authentication and traffic encrypted using AES. In Enterprise mode, clients have to enter a user name and password in other to gain access. The access point verifies these credentials through the RADIUS server prior to granting clients access. The RADIUS server uses Challenge Handshake Authentication Protocol (CHAP) for authentication.

Throughput, Delay, Jitter, Loss Ratio and connection time were used as the performance metrics. On the webserver, a webpage was hosted, allowing Nodes to request resources. The connection time for a Node to successfully establish a TCP connection with the webserver was measured using Wireshark [19]. IPerf3 [20] an open-source traffic analyzer was used as the packet generator to transmit data

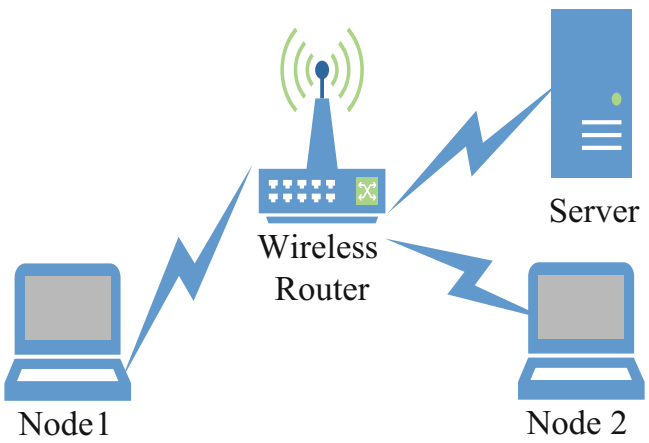

Fig. 3.1 Experimental testbed

Table 3.1 Technical specifications

Equipment/software	Function	Technical specification
Dell Latitude Laptop	Wireless nodes	4GBRAM Intel Core i5- 2410M CPU @ 2.3 GH × 4,64 bit Ubuntu 16.04,802.1ac NIC
Dell OptiPlex 790	Radius server/Apache server	8 GB RAM Intel Core i5- 2400M CPU @ 3.1 GH × 4 64 bit Ubuntu
Talon AD7200 Multi-Band Wi-Fi Router	Wireless router	10/100/1000 Mbps LAN Ports, 60 GHz, 2.4 GHz and 5 GHz bands, IEEE 802.11a/b/g/n/ac/ad
Iperf3	Traffic generator	
Wireshark	Packet capture/analyzer	

between Nodes and measured the metrics of interest. For each measured performance metric, we run 30 experiments for a duration of 30 s and the average value noted. Prior to running connection time related experiments, we cleared the browser cache of traces of any prior TCP connections with the webserver to avoid inaccurate results. The wireless router was configured to use 5GHz frequency range. Table 3.1 provides the technical specifications of equipment used.

3.4 Discussion of Results

Per the objectives of the study, three security modes were used: No security—representing the baseline scenario, Personal Security—using WPA2/AES and Enterprise Security using a WPA2/AES and RADIUS server. For each of these scenarios, IPv4 and IPv6 traffic was used with TCP and UDP as transport layer protocols. Loss Ratio and Jitter were measured only for UDP traffic.

3.4.1 Throughput

Figures 3.2, 3.3, 3.4, 3.5 and 3.6 indicate test results obtained for throughput using different payload sizes and varying the type of security mode and the network layer protocol (IPv4 or IPv6) used. In Figs. 3.2 and 3.3, it can be observed that throughput increases with increasing payload size for TCP and UDP traffic irrespective of the security mechanism deployed.

Figures 3.4 and 3.5 depict IPv6 TCP and UDP throughput respectively. From the diagrams, IPv6 traffic exhibits similar characteristic as IPv4. In Fig. 3.6, we compare throughput for various security modes and different network layer protocols. This figure serves as a summary of our findings for throughput. It is observed that regardless of the type of protocols deployed, throughput is generally higher when no security is

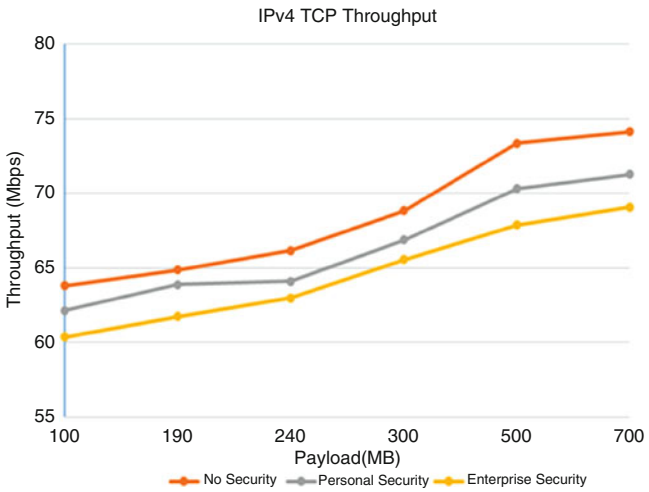

Fig. 3.2 IPv4 TCP throughput

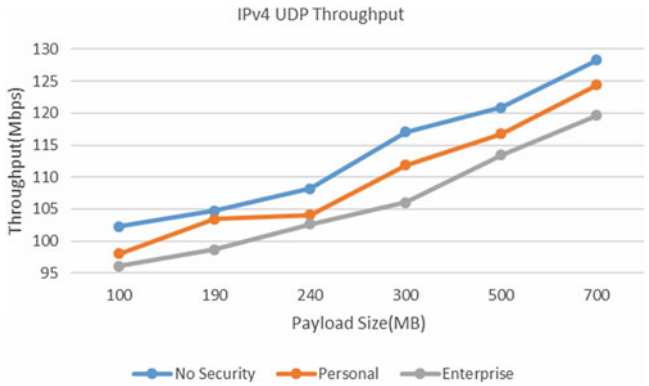

Fig. 3.3 IPv4 UDP throughput

deployed in the network. Thus, when no security is implemented, the WLAN experiences throughput improvements ranging from 1.1 to 6.7% over personal security. The performance improvement experience when Enterprise security is used ranges from 2.2 to 8.2%.The percentage improvement

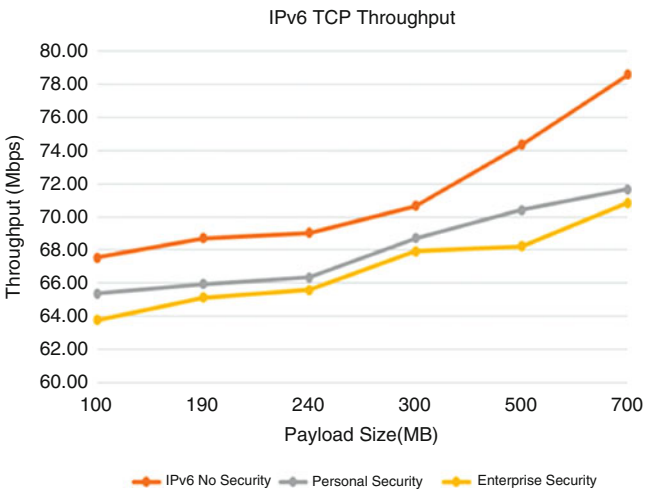

Fig. 3.4 IPv6 TCP throughput

Fig. 3.5 IPv6 UDP throughput

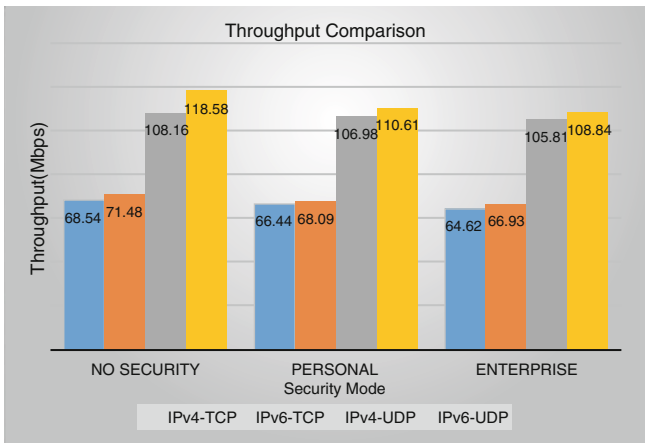

Fig. 3.6 Throughput comparison using different security modes

of IPv6 traffic over IPv4 traffic with regards to throughput ranges between 3 and 5% depending on the transport layer protocol used. The relatively better performance of IPv6 over IPv4 traffic can be attributed to the simple nature of the IPv6 header which reduces the amount of overhead processing.

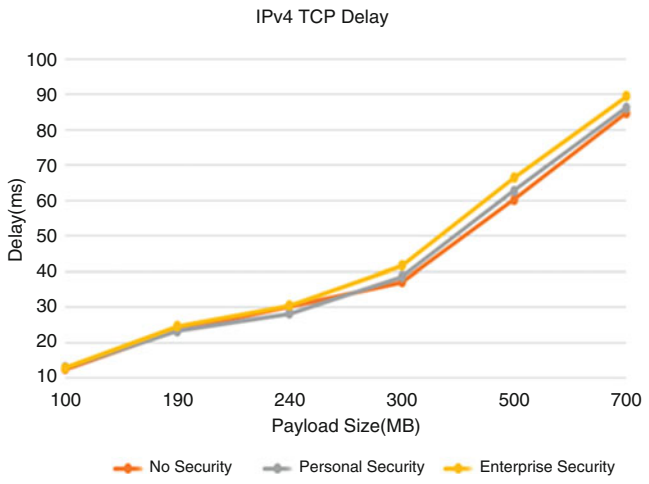

Fig. 3.7 IPv4 TCP delay

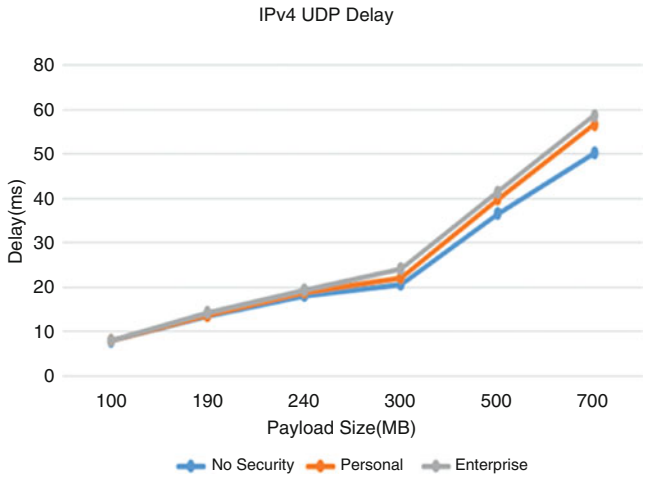

Fig. 3.8 IPv4 UDP delay

3.4.2 Delay

Delay as used here is defined as the time it takes to transfer data between two Nodes. This includes the time taken to establish a connection between nodes in the case of TCP traffic streams. Figures 3.7, 3.8, 3.9, 3.10 and 3.11 provide delay related data for our test network. For both UDP and TCP traffic as indicated in Figs. 3.7, 3.8, 3.9, 3.10 and 3.11, delay increases with increasing payload size. The same trend is true for IPv4 and IPv6 data. It can also be deduced that, consistently, when no security is implemented, the network tends to perform better in terms of delay.

In Fig. 3.11, we compare the delay under various security settings to determine the extent to which the various metrics and protocols impact delay. Based on the results in Fig. 3.11, a 5% performance improvement in delay is experienced for IPv6 relative to IPv4 when TCP is used as the transport layer protocol. Similarly, for UDP traffic, the performance improvement of IPv6 over IPv4 is 3%. In terms of security,

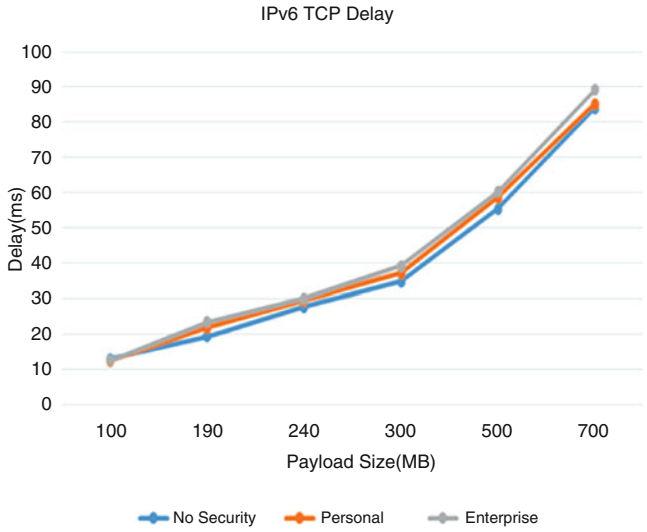

Fig. 3.9 IPv6 TCP delay

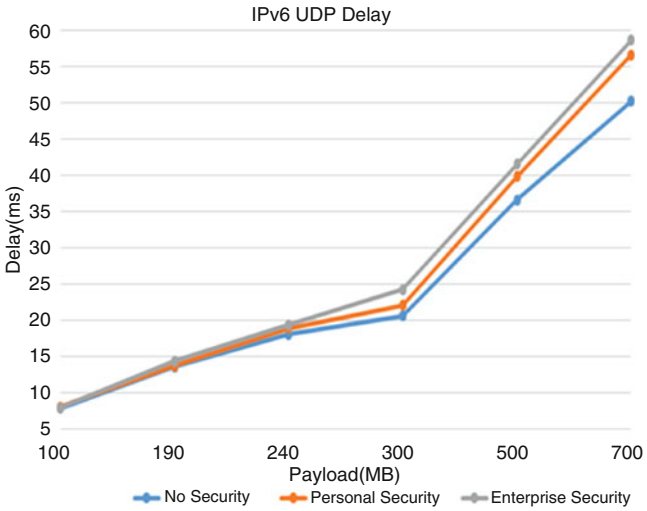

Fig. 3.10 IPv6 UDP delay

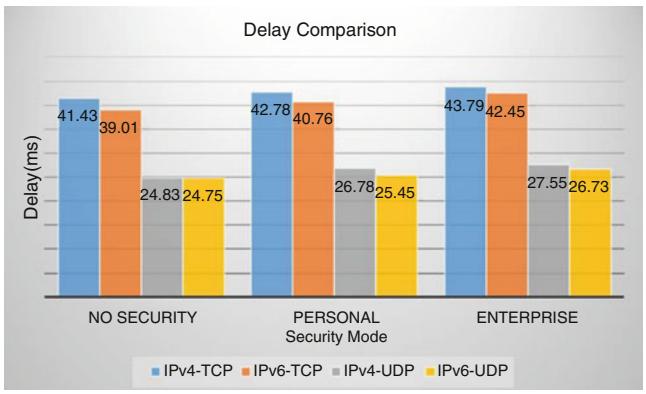

Fig. 3.11 Delay comparison with different security modes

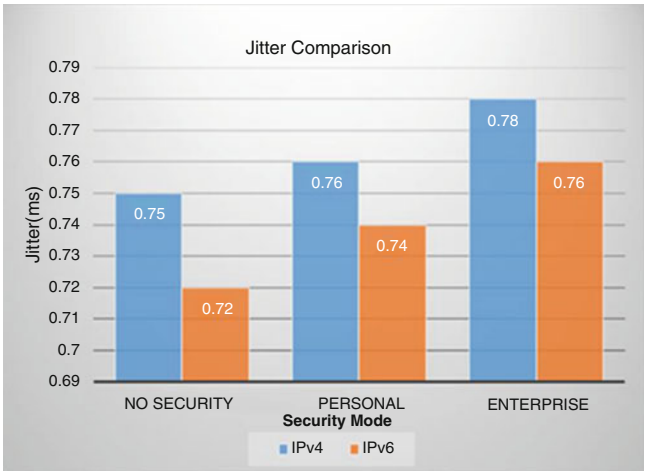

Fig. 3.12 Jitter comparison with different security modes

for TCP traffic when no security is implemented, there is a performance improvement of 3.3–4.5% over personal security and 5.7–8.8% over enterprise security. For UDP traffic, with no security, a 2.8–7.9% improvement is realized over personal security whiles an 8.0–11% enhancement of enterprise security is observed.

3.4.3 Jitter

The relatively simple nature of the testbed with no background traffic or congestion accounts for the low values obtained for jitter. It is likely these results may vary significantly when the network is scaled up. Furthermore (as shown in Fig. 3.12), for jitter, it is realized, a performance degradation of 3% using IPv4 traffic relative to IPv6.A 1.3–2.8% performance improvement is recorded when no security is used relative to personal security and 4–5.6% relative to enterprise security.

3.4.4 Connection Time

We define the connection time as the time it takes for a TCP connection to be established by measuring delay between the SYN and the ACK from the client. In Fig. 3.13, we observe no significant difference in connection time for cases where no security is implemented and personal security. However, there is an increase of about 14.2–18.6% when enterprise security is used. The extra time required by the RADIUS server to authenticate the client explains the increase in connection time.

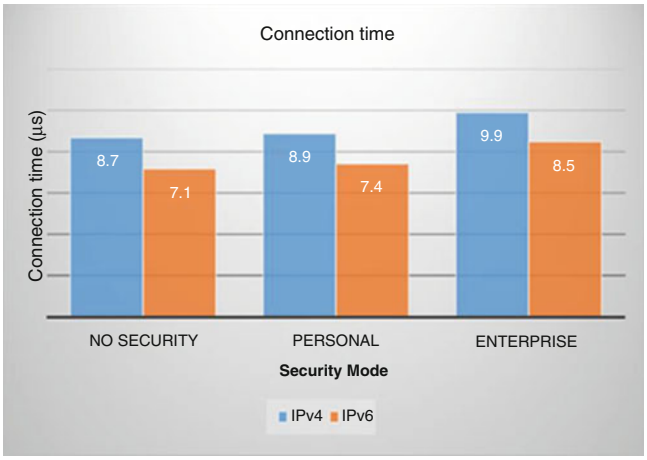

Fig. 3.13 Connection time

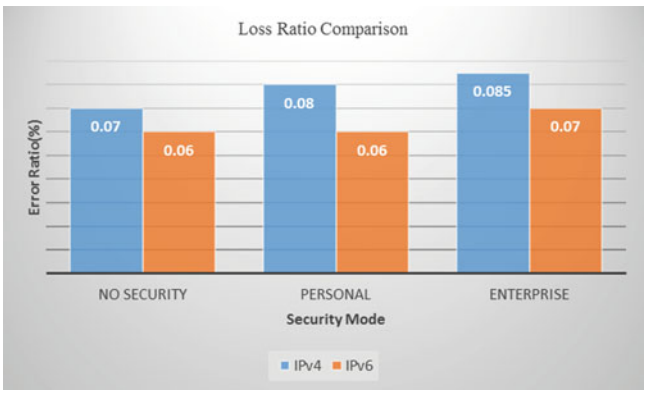

Fig. 3.14 Loss ratio comparison with different security modes

3.4.5 Loss Ratio

The Loss Ratio shows a similar trend as the other metrics used as shown in Fig. 3.14. Unlike the other metrics though, the performance improvements reported are quite significant in some cases. In particular, a 16.7–21.4% improvement is realized for no security over enterprise security. It is worth noting from Fig. 3.13 that, for IPv6 traffic there was no change in loss ratio when personal security is deployed relative to no security. Further experiments would be necessary, perhaps, to ascertain the validity or otherwise of this specific result.

3.5 Conclusion and Future Work

In this paper, we studied the extent to which various security modes impact the performance of 802.11ac WLANs by measuring throughput, delay, jitter, Loss Ratio and connection time. The results indicate a slight performance degradation when various security mechanisms are implemented on 802.11ac WLANs. For throughput performance degraded by between 1.6 and 8.2% depending on the type of security implemented and the transport and network work layer protocol used. Similarly, a performance improvement of between 2.8 and 7.9% was observed when no security is implemented for delay. Jitter, Loss Ratio and connection time experienced between 1.3 and 18.6% improvement in performance. It is worth mentioning that, much as these results may be quite insignificant, organization are likely to experience significant performance issues with an increase in the complexity of their WLANs.

We run the experiments under relatively controlled conditions. As part of future work, we intend extending the topology of the test network to include multiple Basic Service Sets (BSS) with heterogeneous devices including, but not limited to mobile handheld devices with some background traffic introduced in the network.

References

1. IEEE Standards Association, Wireless LAN medium access control wireless LAN (MAC) and physical layer (PHY) specifications. (2016), http://standards.ieee.org/getieee802/download/802.11-2016.pdf. Accessed 2 Aug 2017
2. R.V. Nee, Breaking the gigabit-per-second barrier with 802.11ac. IEEE Wirel. Commun. Mag. **18**(2), 4 (2011)
3. S.N. Kelkar, A survey and performance analysis of IEEE 802.11ac Wi-Fi networking. Int. J. Comput. Sci. Inf. Technol. **3**(2), 808–814 (2015)
4. M.-D. Dianu, J. Riihijarvi, M. Petrova, Measurement- based study of the performance of IEEE 802.11ac in an indoor environment, in *IEEE International Conference on Communications*, Sydney, 2014
5. IEEE Standards Association, Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. (2007), [Online]. http://standards.ieee.org/getieee802/download/802.11-2007.pdf. Accessed 2 Aug 2017
6. FreeRADIUS, FreeRADIUS, [Online]. http://freeradius.org/. Accessed 1 Aug 2017
7. Nescout, Netscout White Paper, The impact of 802.11ac wireless networks on network technicians, Nescout, [Online]. http://enterprise.netscout.com/edocs/white-paper-impact-80211ac-wireless-networks-network-technicians. Accessed 1 Aug 2017
8. P. Li, S.S. Kolahi, M. Safdari, M. Argawe, Effect of WPA2 security on IEEE 802.11n bandwidth and round trip time in peer-peer wireless local area networks. Workshops of International Conference on Advanced Information Networking and Applications, in *International Conference on Advanced Information Networking and Applications*, 2011
9. L. Kriaia, E.C. Molero, T. R. Gross, Evaluating 802.11ac features in indoor WLAN: an empirical study of performance and fairness. in *ACM International Workshop on Wireless Network Testbeds, Experimental evaluation & CHaracterization*, New York City, 2016
10. H. Ong, J. Kneckt, O. Alanen, Z. Chang, T.T. Huovinen, T. Nihtila, EEE 802.11ac: Enhancements for very high throughput WLANs, in *IEEE Personal Indoor Mobile Radio Communitcations*, 2011
11. Z. Chang, O. Alanen, T. Huovinen, T. Nihtila, H. Ong, J. Kneckt, T. Ristaniemi, Performance analysis of IEEE 802.11ac DCF with hidden nodes, in *EEE 75th Vehicular Technology Conference (VTC Spring)*, 2012

12. T. Vanhatupa, *Wi-Fi Capacity Analysis for 802.11ac and 802.11n: Theory and Practice* (Ekahau Inc, 2015)
13. R. Mardeni, K. Anuar, A. Salamat, M.G.I. Yusop, Investigation of IEEE 802.11ac signal strength performance in Wi-Fi communication systems, in *Research World International Conference*, Osaka, 2016
14. P.D and B.D, The impact of security overheads on 802.11 WLAN throughput
15. H. Ce, *Effects of Security Features on the Performance of Voice over WLAN* (Stanford University Press, Stanford, 2004)
16. P. Likhar, R.S. Yadav, K.M. Rao, Securing IEEE 802.11g WLAN using OpenVPN and its impact analysis. IJNSA **3**(6), 97–113 (2011)
17. W. Agosto-Padilla, A. Loukili, A. Tsetse, A. Wijesinha, R. Karne, 802.11n wireless LAN performance for mobile devices, in *IEEE/ACS International Conference of Computer Systems and Applications (AICCSA)*, 2016
18. P. Jindal, B. Singh, Quantitative analysis of the security performance in WLANs. J. King Saud. Univ. **29**(3), 246–268 (2014)
19. Wireshark, Wireshark protocol analyzer, [Online]. https://www.wireshark.org/. Accessed 1 Aug 2017
20. IPerf, [Online]. https://iperf.fr/iperf-download.php. Accessed 2 Aug 2017
21. S. Saha, P. Deshpande, P. Inamdar, R. Sheshadri, D. Koutsonikolas, Power-throughput tradeoffs of 802.11ac in smartphones, in *IEEE Conference on Computer Communications (INFOCOM)*, 2015