Conference Paper

Performance Investigations of IEEE 802.11 a54 Mbps WPA2 Laboratory Links

José A. R. Pacheco de Carvalho, Cláudia F. F. P. Ribeiro Pacheco, Antonio D. Reis, and Hugo Veiga

Universidade da Beira Interior

Abstract

The increasing importance of wireless communications, involving electronic devices, has been widely recognized. Performance is a fundamental issue, resulting in more reliable and efficient communications. Security is also crucially important. Laboratory measurements are presented for several performance aspects of Wi-Fi IEEE 802.11a 54 Mbps WPA2 point-to-point and four node point-to-multipoint links. Our study contributes to performance evaluation of this technology under WPA2 encryption, using available equipment (HP V-M200 access points and Linksys WPC600N adapters). New results are given from TCP and UDP experiments concerning TCP throughput versus TCP packet length, jitter and percentage datagram loss versus UDP datagram size. Comparisons are made to corresponding results for Open links. Conclusions are drawn about the comparative performance of the links.

Keywords: Wi-Fi, WLAN, IEEE 802.11a, Wireless network laboratory performance, Multi-Node WPA2 links

Corresponding Author:
José A. R. Pacheco de Carvalho
pacheco@ubi.pt

Received: 26 November 2019
Accepted: 13 May 2020
Published: 2 June 2020

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the ICEUBI2019 Conference Committee.

1. Introduction

Electromagnetic waves in several frequency ranges, propagating in the air, permitted the development of contactless communication technologies. Wireless fidelity (Wi-Fi) and free space optics (FSO) are typical examples of wireless communications technologies, using microwaves and laser light, respectively. Their importance and utilization have been growing worldwide.

Wi-Fi uses microwave technology, giving versatility, mobility and favourable prices. The importance and utilization of Wi-Fi have been increasing. It is a complement to traditional wired networks. The chief use is infrastructure mode where a wireless access point, AP, provides communications of Wi-Fi electronic devices with a wired based local area network (LAN) through a switch/router. By this means a wireless local area network (WLAN), based on the AP, is set. At the home level personal devices can communicate through a wireless personal area network (WPAN). Essentially, point-to-point (PTP) and point-to-multipoint (PTMP) microwave links are used in the 2.4 and 5 GHz frequency bands, with IEEE 802.11a, 802.11b, 802.11g, 802.11n and 802.11ac standards [1]. The increasing use of the 2.4 GHz band has resulted in strong electromagnetic interference. Therefore, the use of the 5 GHz band is interesting, in spite of larger absorption and shorter ranges. Wi-Fi communications are not very affected by rain or fog, as wavelengths are in the range 5.6-12.5 cm. However, rain or fog significantly degrades FSO communications, as the typical wavelength range for the laser beam is 785-1550 nm.

Nominal transfer rates for Wi-Fi are up to 11 (802.11b), 54 Mbps (802.11 a, g), 600 Mbps (802.11n) and 3.5 Gbps (802.11ac). Carrier sense multiple access with collision avoidance (CSMA/CA) is Wi-Fi medium access control. 802.11a,g. provide a multi-carrier modulation scheme called orthogonal frequency division multiplexing (OFDM), allowing for binary phaseshift keying (BPSK), quadrature phase-shift keying (QPSK) and quadrature amplitude modulation (QAM) of the 16-QAM and 64-QAM density types. One antenna (one spatial stream) and coding rates up to 3/4 are possible and a 20 MHz channel. 802.11a and 802.11g use the 5 and 2.4 GHz bands respectively.

Studies have been published on wireless communications, wave propagation [2, 3], practical accomplishments of WLANs [4], performance analysis of the effective transfer rate for 802.11b PTP links [5], 802.11b performance in crowded indoor environments [6].

Performance gain has been a central issue, giving more reliable and efficient communications. Requirements have been presented [7]. New telematic applications are especially sensitive to performances when compared to traditional applications.

Wi-Fi security is very important for privacy reasons. Several security methods have been developed to provide authentication such as, by increasing order of security, wired equivalent privacy (WEP), Wi-Fi protected access (WPA) and Wi-Fi protected access II (WPA2).

Several performance measurements have been published for 2.4 and 5 GHz Wi-Fi Open [8, 9], WEP [10], WPA[11] and WPA2 [12] links, as well as very high speed FSO [13]. Performance evaluation of IEEE 802.11 based Wireless Mesh Networks has been given [14]. Studies are published on modelling TCP throughput [15]. A formula that bounds average TCP throughput is available [16].

It is significant investigating the effects of TCP packet size, UDP datagram size, network topology, increasing levels of security encryption, on link performance and compare equipment performance for several standards. Performance studies have been published for 5 GHz 802.11n WPA2 links [17]. In the present work new Wi-Fi results are given from measurements on 802.11a WPA2 links at 54 Mbps, namely through OSI level 4 from TCP and UDP experiments. Performance is evaluated and compared in laboratory measurements of WPA2 two-node (PTP) and four-node point-to-multipoint (4N-PTMP) links using available equipment. TCP throughput is measured versus TCP packet length. Jitter and percentage datagram loss are evaluated versus UDP datagram size. Comparisons are also made to corresponding results obtained for Open links. In relation to previous work [18], an extended research on performance is carried out in the present work.

In prior and actual state of the art, several Wi-Fi links and technologies have been investigated. Performance evaluation has been stated as a crucially important criterion to assess communications quality. The motivation of this work is to evaluate performance in laboratory measurements of WPA2 PTP and 4N-PTMP 802.11a links at 54 Mbps using accessible equipment and compare the results to those obtained for Open links. Thus enlarging the knowledge about performance of Wi-Fi (IEEE 802.11 a) links. The problem basis is that performance needs to be evaluated under several TCP and UDP parameterizations, link topologies and security encryption. The constructed solution uses an experimental setup and method, to monitor signal to noise ratios (SNR) and noise levels (N), and measure TCP throughput (from TCP connections) versus TCP packet size, and UDP jitter and percentage datagram loss (from UDP communications) versus UDP datagram size. Following, the paper is structured as follows: Section 2 gives the experimental conditions i.e. the measurement setup and procedure. Results and discussion are presented in Section 3. Conclusions are drawn in Section 4.

2. Experimental details

The experiments were made during the first semester 2019. We have used a HP V-M200 access point [19], with three external dual-band 3x3 MIMO antennas, IEEE 802.11 a/b/g/n, software version 5.4.1.0-01-16481, a 1000-Base-T/100-Base-TX/10-Base-T layer 2 3Com Gigabit switch 16 and a 100-Base-TX/10-Base-T layer 2 Allied Telesis AT-8000S/16 switch [20]. Three PCs were used having a PCMCIA IEEE.802.11 a/b/g/n Linksys WPC600N wireless adapter with three internal antennas [21], to enable four-node PTMP (4N-PTMP) links to the access point. An interference free communication channel was used (ch 36). This was ensured through a portable monitoring computer, equipped with a Wi-Fi 802.11 a/b/g/n/ac adapter, running Acrylic WiFi software [22]. WPA2 encryption with AES-CCMP was activated in the AP and the wireless adapters of the PCs, with a pass phrase resulting in an encryption key of 256 bits. The experiments were conducted under far-field conditions. No power levels above 30 mW (15 dBm) were used, as the wireless equipment were nearby. In fact, the distances involved were large in comparison to the wavelength used (5.8 cm).

A versatile laboratory setup has been planned and realized for the experiments, as shown in Figure 1. Up to three wireless links to the AP are possible. At OSI level 4, measurements were made for TCP connections and UDP communications using Iperf software [23]. For a TCP client/server connection (TCP New Reno, RFC 6582, was used), TCP throughput was obtained for a given TCP packet size, varying from 0.25k to 64k bytes. For a UDP client/server communication with a given bandwidth parameter, UDP jitter and percentage loss of datagrams were determined for a given UDP datagram size, varying from 0.25k to 64k bytes.

The Wi-Fi network was as follows. One PC, with IP 192.168.0.2 was the Iperf server and the others, with IPs 192.168.0.6 and 192.168.0.50, were the Iperf clients (client1 and client2, respectively). Jitter, which is the root mean square of differences between consecutive transit times, was continuously computed by the server, according to the real time protocol RTP, in RFC 1889 [24]. A control PC, with IP 192.168.0.20, was mainly used to control the settings of the AP. The net mask was 255.255.255.0. Three types of experiments are possible: PTP (two nodes), using the client1 and the control PC as server; PTMP (three nodes), using the client1 and the 192.168.0.2 server PC; 4N-PTMP (four nodes), using simultaneous connections/communications between the two clients and the 192.168.0.2 server PC.

The server and client PCs were HP nx9030 and nx9010 portable computers, respectively. The control PC was an HP nx6110 portable computer. Windows XP Professional SP3 was the operating system. The PCs were arranged to provide maximum resources to the present work. Batch command files have been re-written for the new TCP and UDP experiments.

The results were obtained in batch mode and recorded as data files to the client PCs disks. Every PC had a second Ethernet network adapter, to permit remote control from the IP APTEL (Applied Physics and Telecommunications) Research Group network, via switch.

3. Results and Discussion

The wireless network adapters of the PCs were manually configured for a nominal rate of 54 Mbps. WPA2 encryption was activated in the AP and the wireless network adapters of the PCs. Transmit and receive rates were monitored in the AP during the experiments. They were typically 54 Mbps. For every TCP packet size in the range 0.25k-64k bytes, and for every corresponding UDP datagram size in the same range, data were acquired for WPA2 PTP and 4N-PTMP links at OSI levels 1 (physical layer) and 4 (transport layer) using the setup of Figure 1. For every TCP packet size an average TCP throughput was calculated from a set of experiments. This value was fed in as the bandwidth parameter for every corresponding UDP test, giving average jitter and average percentage datagram loss.

At OSI level 1, signal to noise ratios (SNR, in dB) and noise levels (N, in dBm) were obtained in the AP. Signal gives the strength of the radio signal the AP receives from a client PC, in dBm. Noise means how much background noise, due to radio interference, exists in the signal path between the client PC and the AP, in dBm. The lower the value is, the weaker the noise. SNR indicates the relative strength of client PC radio signals versus noise in the radio signal path, in dB. SNR is a good indicator for the quality of the radio link between the client PC and the AP. The measured data were similar for all types of experiments. Typical values are shown in Figure 2. The links have shown good, high, SNR values.

The main average TCP and UDP results are summarized in Table 1, both for WPA2 and Open 4N-PTMP and PTP links. The statistical analysis, including calculations of confidence intervals, was made as in [25]. In Figs. 3 and 4 polynomial fits were made (shown as y versus x), using the Excel worksheet, to the TCP throughput data both for WPA2 and Open 4N-PTMP and PTP links, respectively, where R^2 is the coefficient of determination. It indicates the goodness of fit. If it is 1.0 it means a perfect fit to data. It was found that, on average, the best TCP throughputs are for PTP both for WPA2 and Open links (Table 1). In passing from PTP to 4N-PTMP throughput reduces to 23%. Similar trends are visible for Open links. This is due to increase of processing requirements for the AP, so as to maintain links between PCs. Throughput results are similar for WPA2 and Open links, within the experimental error. Figs. 3 and 4 show fair increases in TCP throughput with packet size. For small packets there is a large overhead, as there are small amounts of data that are sent in comparison to the protocol components. The role of the frame is very heavy in Wi-Fi. For larger packets, overhead decreases; the amount of sent data overcomes the protocol components.

In Figs. 5-8, the data points representing jitter and percentage datagram loss were joined by smoothed lines. It was found that jitter performances are slightly better for WPA2 than for Open links. This was unanticipated. Also, the average values for 4N-PTMP are lower than for PTP (Table 1), both for Open and WPA2 links. However, we would expect a decrease of jitter performance in passing from PTP to 4N-PTMP due to increase of processing requirements for the AP to maintain links between PCs. For small sized datagrams, jitter is small. There are small delays in sending datagrams. Latency is also small. Jitter increases for larger datagram sizes.

Concerning average percentage datagram loss, performances were found better for PTP than for 4N-PTMP, for both WPA2 and Open links (Table 1). This is due to increase of processing requirements for the AP, for maintaining links between PCs. Figs. 7 and 8 show larger percentage datagram losses for small sized datagrams, chiefly for 4N-PTMP, when the amounts of data to send are small in comparison to the protocol components. There is considerable processing of frame headers and buffer management. For larger datagrams, percentage datagram loss is lower. However, large UDP segments originate fragmentation at the IP datagram level, leading to higher losses, as is particularly clear for 4N-PTMP. Also, average percentage datagram loss performances degrade in passing from Open to WPA2 links, both for PTP and 4N-PTMP links. This suggests the effect of WPA2, where data length increases due to encryption. TCP throughput and percentage datagram loss were generally found to show performance degradations due to link topology, in passing from PTP to 4N-PTMP, where processing requirements for the AP are higher so as to maintain links between PCs. As CSMA/CA is the medium access control, the available bandwidth and the air time are divided by the nodes using the medium. WPA2, where there is increase of data length due to encryption, was found to degrade datagram loss performances.

In comparison to previous research for 5 GHz 802.11n WPA2 links [17], the present results show that 5 GHz 802.11n has essentially given better TCP performances than 802.11a.

Table 1: Average Wi-Fi (IEEE 802.11 a) WPA2 and OPEN results: PTP; 4N-PTMP

Link type	WPA2 PTP	WPA2 4N-PTMP
TCP throughput (Mbps)	22.9+-0.7	5.3+-0.2
UDP-jitter (ms)	3.2+-0.1	2.6+-0.3
UDP-% datagram loss	2.5+-0.2	5.9+-0.9
Link type	Open PTP	Open 4N-PTMP
TCP throughput (Mbps)	23.1+-0.7	5.4+-0.2
UDP-jitter (ms)	3.5+-0.2	2.6+-0.6
UDP-% datagram loss	1.9+-0.2	4.7+-0.2

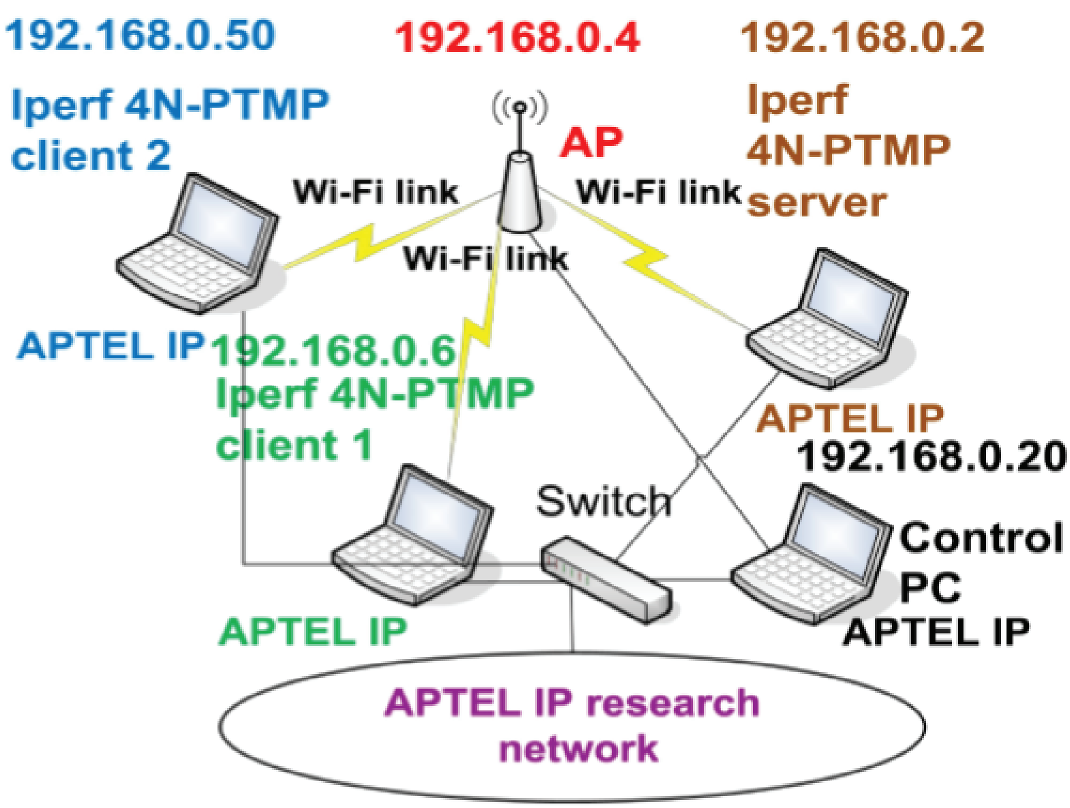

Figure 1: Laboratory setup scheme.

4. Conclusions

In the present work a versatile laboratory setup arrangement was devised and realized, that permitted systematic performance measurements of available wireless equipments (V-M200 access points from HP and WPC600N adapters from Linksys) for Wi-Fi (IEEE 802.11 a) in WPA2 PTP and 4N-PTMP links.

For OSI layer 4, TCP and UDP performances were measured versus TCP packet size and UDP datagram size, respectively. TCP throughput, jitter and percentage datagram loss were measured and compared for WPA2 and Open PTP and 4N-PTMP links. TCP throughput was found to increase with packet size. No significant sensitivity to WPA2 was found, within the experimental error. For small sized datagrams, jitter is small. There are small delays in sending datagrams. Latency is also small. Jitter increases for larger datagram sizes, as mainly visible for PTP. Concerning percentage datagram loss, it was found high for small sized datagrams, chiefly for 4N-PTMP. For larger datagrams it diminishes. However, large UDP segments originate fragmentation at the IP datagram level, leading to higher losses, as is especially clear for 4N-PTMP. In comparison to PTP, both for Open and WPA2 links, TCP throughput and percentage datagram loss were found to show significant performance degradations for 4N-PTMP

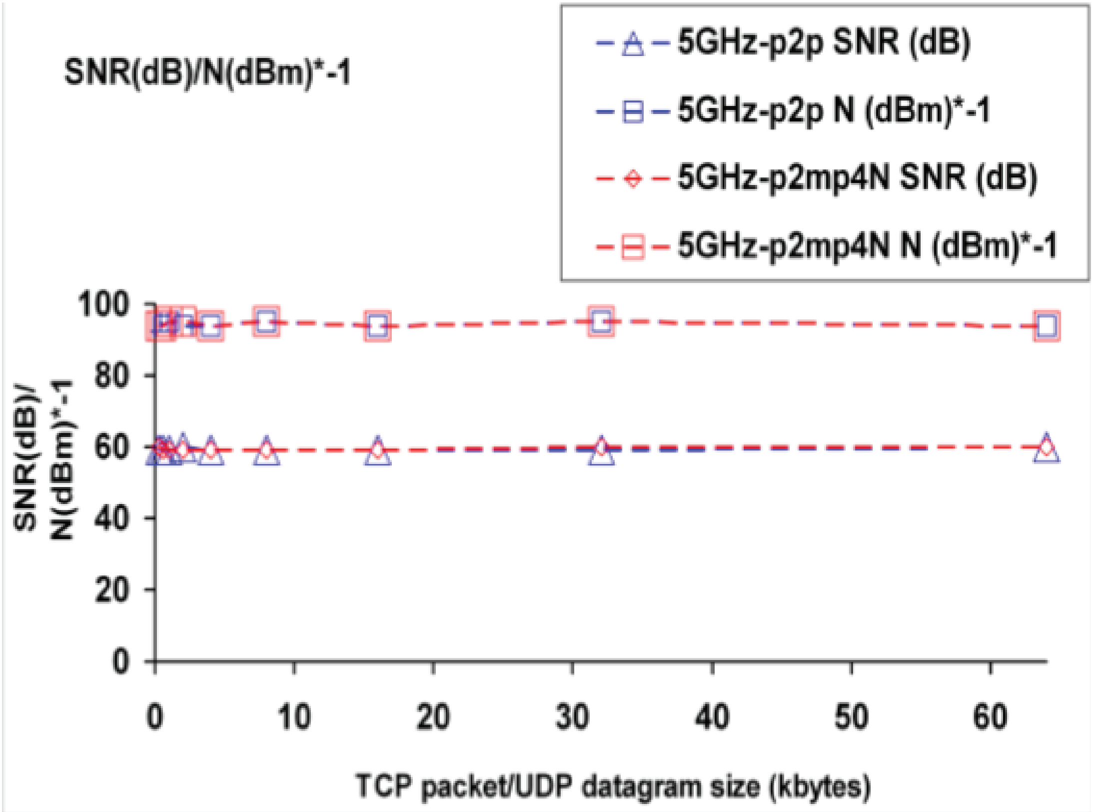

Figure 2: Typical SNR (dB) and N (dBm). WPA2 links

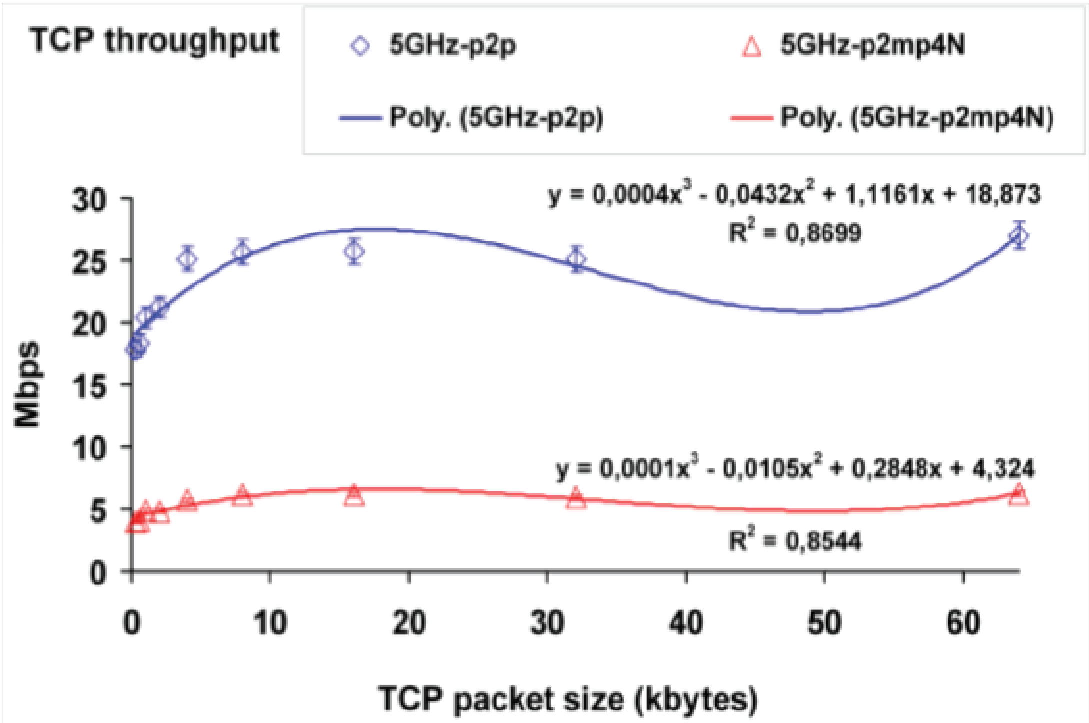

Figure 3: TCP throughput (y) versus TCP packet size (x). WPA2 links.

links, with increasing number of nodes, where the AP experiments higher processing

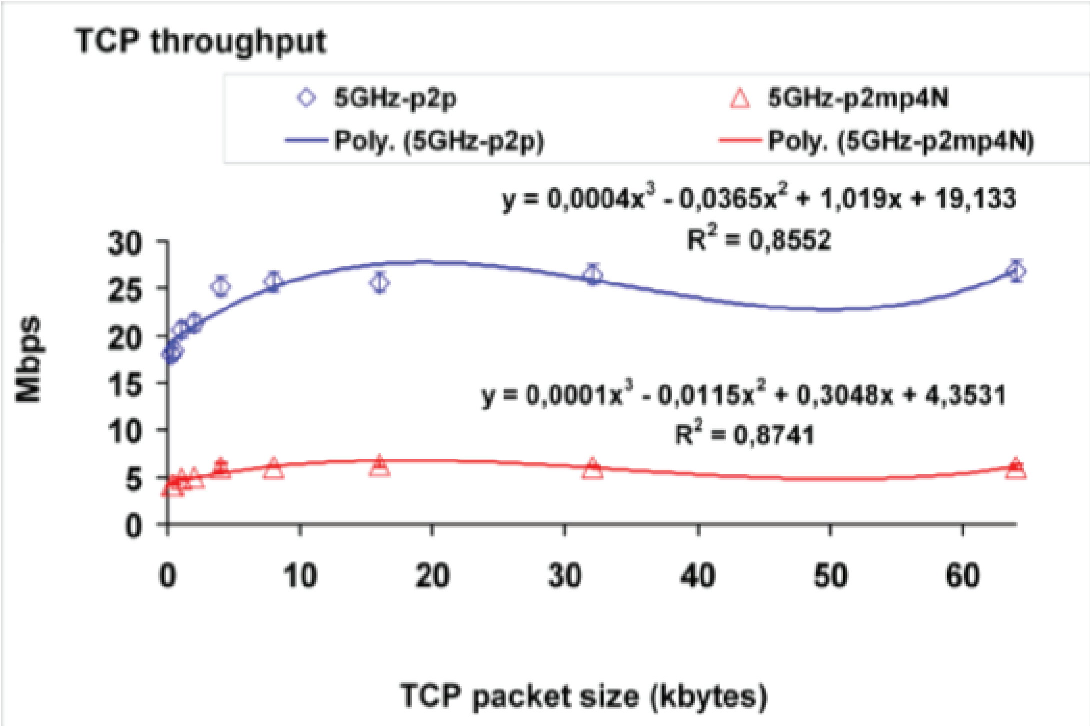

Figure 4: TCP throughput (y) versus TCP packet size (x). Open links.

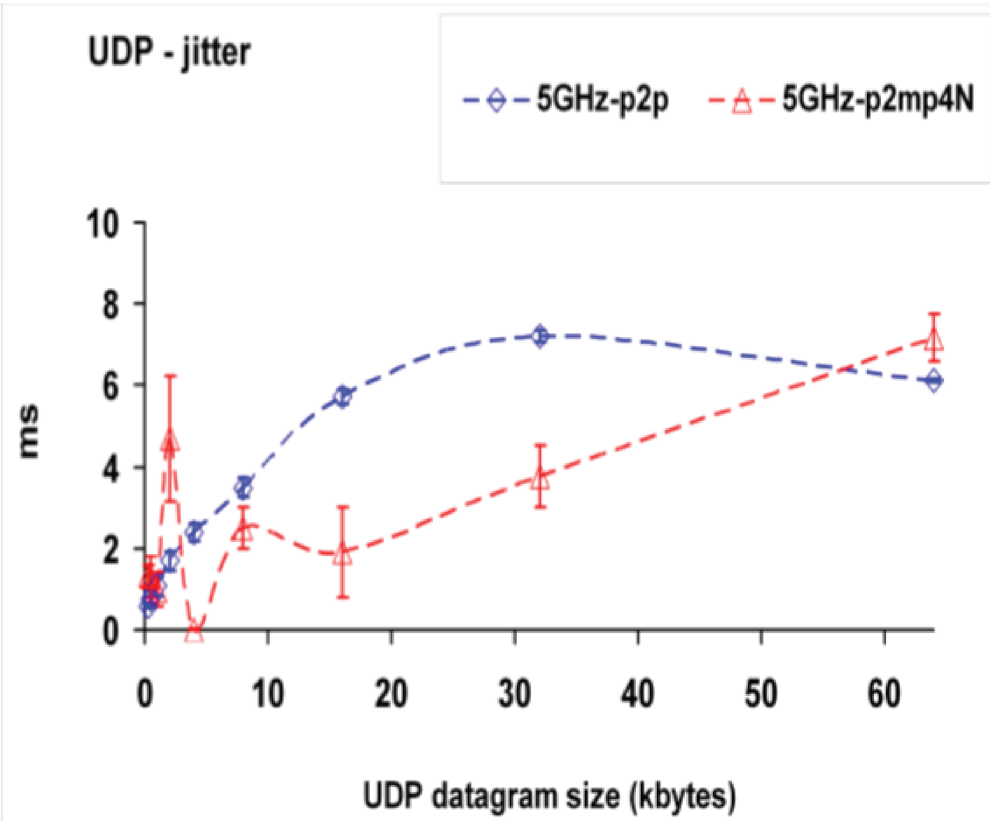

Figure 5: UDP jitter versus UDP datagram size. WPA2 links.

requirements for maintaining links between PCs. As CSMA/CA is the medium access

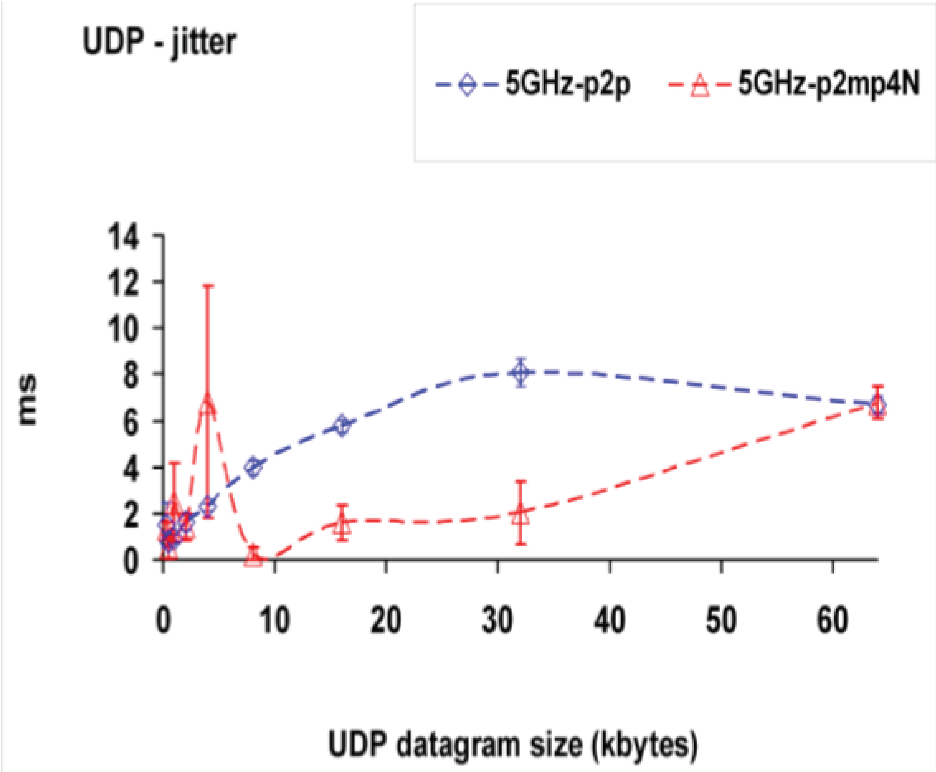

Figure 6: UDP jitter versus UDP datagram size. Open links.

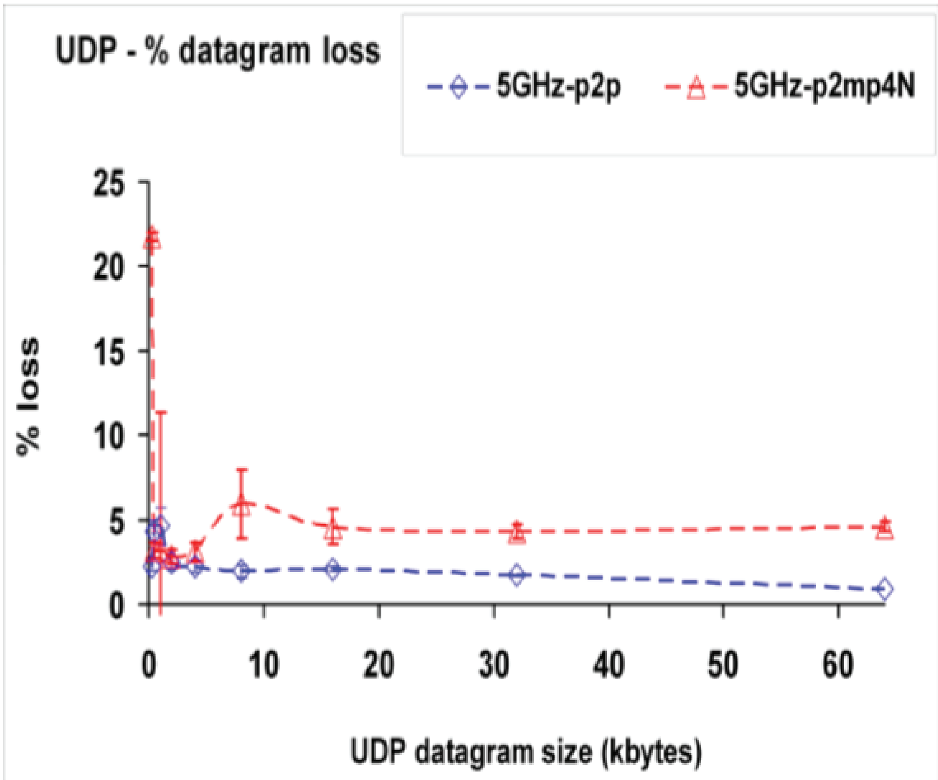

Figure 7: UDP percentage datagram loss versus UDP datagram size. WPA2 links.

control, the available bandwidth and the air time are divided by the nodes using the

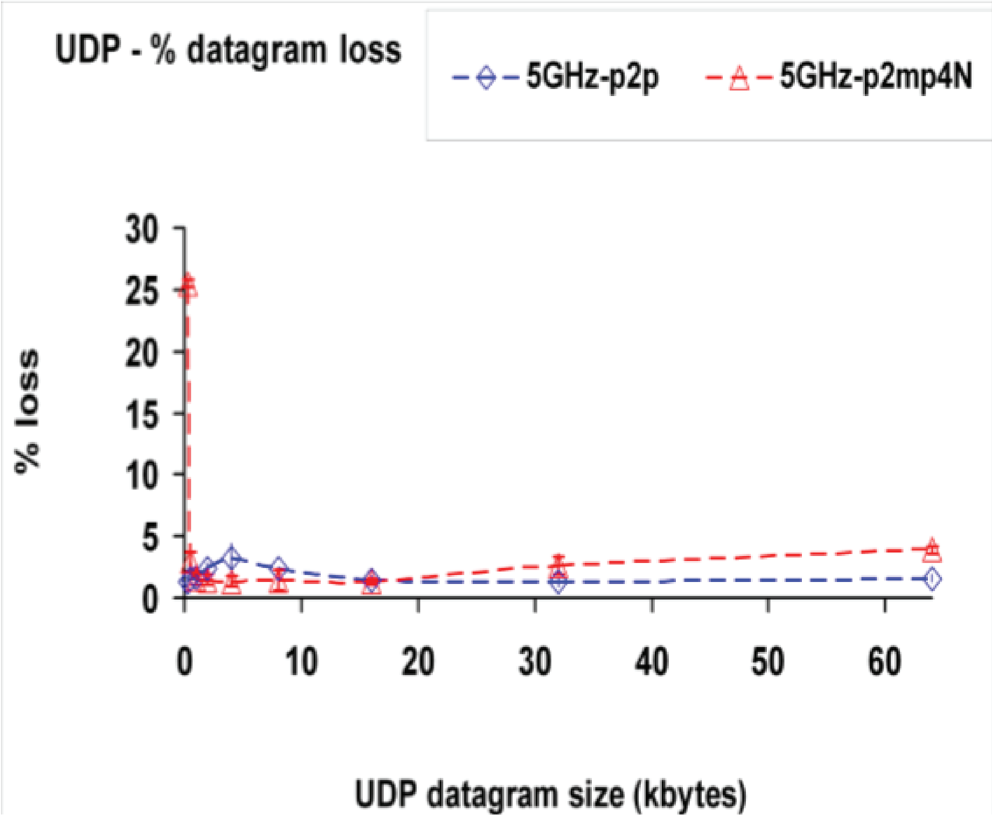

Figure 8: UDP percentage datagram loss versus UDP datagram size. Open links.

medium. WPA2, where there is increase in data length due to encryption, also played its role, specifically for datagram loss performances. The present results show that 5 GHz 802.11n has essentially given better TCP performances than 802.11a.

Further performance investigations are outlined using several standards, equipment, topologies, security settings and noise conditions, not only in laboratory but also in outdoor environments involving, mainly, medium range links.

Acknowledgments

Supports from University of Beira Interior and FCT (Fundação para a Ciência e a Tecnologia)/ PEst-OE/FIS/UI0524/2014(ProjectoEstratégico-UI524-2014) are acknowledged.

References

[1] Web site http://standards.ieee.org; IEEE 802.11a, 802.11b, 802.11g, 802.11n, 802.11i, 802.11ac standards.

[2] Mark, J. W. and Zhuang, W. (2003). *Wireless Communications and Networking*. (New Jersey: Prentice-Hall).

[3] Rappaport, T. S. (2002). *Wireless Communications Principles and Practice*. (New Jersey: Prentice-Hall).

[4] Bruce W. R. and Gilster, R. (202). *Wireless LANs End to End*. (New York: Hungry Minds).

[5] Schwartz, M. (2005). *Mobile Wireless Communications*. (Cambridge: Cambridge University Press).

[6] Sarkar, N. and Sowerby, K. (2006). High Performance Measurements in the Crowded Office Environment: a Case Study. *ICCT '06-International Conference on Communication Technology*. (Guilin, China), pp. 1-4.

[7] Boavida, F. and Monteiro, E. (2011). *Engenharia de Redes Informáticas*, (Lisbon: FCA-Editora de Informática Lda).

[8] Pacheco de Carvalho, J. A. R., Veiga, H., Gomes, P. A. J., *et al* (2010). Wi-Fi Point-to-Point Links- Performance Aspects of IEEE 802.11 a,b,g Laboratory Links. *Electronic Engineering and Computing Technology, Series: Lecture Notes in Electrical Engineering*, (Netherlands: Springer), vol. 60, pp. 507-514.

[9] Pacheco de Carvalho, J. A. R., Veiga, H., Ribeiro Pacheco, C. F., and Reis, A. D. (2016). Extended Performance Research on Wi-Fi IEEE 802.11 a, b, g Laboratory Open Point-to-Multipoint and Point-to-Point Links. *Transactions on Engineering Technologies*. (Singapore: Springer), pp. 475-484.

[10] Pacheco de Carvalho, J. A. R., Veiga, H., Marques, N., *et al* (2011). Wi-Fi WEP Point-to-Point Links- Performance Studies of IEEE 802.11 a,b,g Laboratory Links. *Electronic Engineering and Computing Technology, Series: Lecture Notes in Electrical Engineering*. (Netherlands: Springer), vol. 90, pp. 105-114.

[11] Pacheco de Carvalho, J. A. R., Veiga, H., Ribeiro Pacheco, C. F., and Reis, A. D. (2014). Extended Performance Studies of Wi-Fi IEEE 802.11a, b, g Laboratory WPA Point-to-Multipoint and Point-to-Point Links. *Transactions on Engineering Technologies: Special Volume of the World Congress on Engineering 2013*, (Gordrecht: Springer), pp. 455-465.

[12] Pacheco de Carvalho, J. A. R., Veiga, H., Ribeiro Pacheco, C. F., and Reis, A. D. (2014). Performance Evaluation of IEEE 802.11 a, g Laboratory WPA2 Point-to-Multipoint Links. *Lecture Notes in Engineering and Computer Science: Proceedings of the World Congress of Engineering 2014*, (London: WCE 2014), pp. 699-704.

[13] Pacheco de Carvalho, J. A. R., Veiga, H., Marques, N., *et al* (2010). Performance Measurements of a 1550 nm Gbps FSO Link at Covilhã City, Portugal. *Proc. Applied*

Electronics 2010 - 15th International Conference (University of West Bohemia, Czech Republic), pp. 235-239.

[14] Bansal, D., Sofat, S., Chawla, P., and Kumar, P. (2011). Deployment and Evaluation of IEEE 802.11 based Wireless Mesh Networks in Campus Environments. *Lecture Notes in Engineering and Computer Science: Proceedings of the World Congress on Engineering 2011*, (London: WCE 2011), pp. 1722-1727.

[15] Padhye J., Firoiu, V., Towsley, D., and Kurose, J. (1998). Modeling TCP Throughput: A Simple Model and its Empirical Validation. S*IGCOMM Symposium Communications, Architecture and Protocols*, pp. 304-314.

[16] Mathis, M., Semke, J. and Mahdavi, J. (1997). The Macroscopic Behavior of the TCP Congestion Avoidance Algorithm. *ACM SIGCOMM Computer Communication Review*, vol. 27, issue 3, pp. 67-82.

[17] Pacheco de Carvalho, J. A. R., Veiga, H., Ribeiro Pacheco, C. F., and Reis, A. D. (2019). Extended Performance Research on 5 GHz IEEE 802.11n WPA2 Laboratory Links. *Transactions on Engineering Technologies* (Singapore: Springer), pp. 313-323.

[18] Pacheco de Carvalho, J. A. R., Veiga, H., Ribeiro Pacheco, C. F., and Reis, A. D. (2018). Performance Evaluation of IEEE 802.11a 54 Mbps WEP Laboratory Links. *Lecture Notes in Engineering and Computer Science: Proceedings of the World Congress of Engineering 2018*. (London: WCE 2018), pp. 374-379.

[19] HP V-M200 802.11n access point management and configuration guide (2010) http://www.hp.com accessed 3 Jan 2019.

[20] AT-8000S/16 level 2 switch technical data (2009). http://www.alliedtelesis.com accessed 10 Dec 2018.

[21] WPC600N notebook adapter user guide(2008). http://www.linksys.com accessed 10 Jan 2012.

[22] Acrylic WiFi software (2016). http://www.acrylicwifi.com accessed 8 Jan 2019.

[23] Iperf software (2019). http://iperf.fr accessed 16 Feb 2019.

[24] Network Working Group. RFC 1889-RTP: A Transport Protocol for Real Time Applications. http://www.rfc-archive.org accessed 3 Jan 2019.

[25] Bevington, P. R. (1969). Data Reduction and Error Analysis for the Physical Sciences (New ork: McGraw-Hill).