Performance Effects of WPA2 Encryption and Topology on IEEE 802.11a Laboratory Links

J. A. R. Pacheco de Carvalho, H. Veiga, C. F. Ribeiro Pacheco, A. D. Reis

Abstract—**The increasing importance of wireless communications, involving electronic devices, has been worldly recognized. Performance is a crucial issue, leading to more reliable and efficient communications. Security is also critically important. Laboratory measurements were performed about several performance aspects of Wi-Fi IEEE 802.11a WPA2 point-to-multipoint links. Our study contributes to the performance evaluation of this technology, using available equipments (HP V-M200 access points and Linksys WPC600N adapters). New detailed results are presented and discussed, namely at OSI levels 4 and 7, from TCP, UDP and FTP experiments: TCP throughput, jitter, percentage datagram loss and FTP transfer rate. Comparisons are made to corresponding results obtained for WPA2 point-to-point and Open links. Conclusions are drawn about the comparative performance of the links.**

Index Terms—**Wi-Fi; WLAN; IEEE 802.11a; WPA2; Point-to-Multipoint and Point-to-Point Links; Wireless Network Laboratory Performance.**

I. Introduction

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

Wireless communications are significantly important for their versatility, mobility and favorable prices. It is the case of microwave based technologies, e.g. wireless fidelity (Wi-Fi). Wi-Fi permits complementing traditional wired networks. Its importance and utilization have been growing. Both ad hoc and infrastructure modes have been used. In this case an access point (AP), permits communications of Wi-Fi electronic devices with a wired based local area network (LAN), through a switch/router. Thus, a wireless local area network (WLAN) is formed, based on the AP. Wi-Fi has reached the personal home level, where a wireless personal area network (WPAN) permits communications of personal devices. Point-to-point (PTP) and point-to-multipoint (PTMP) topologies are used both indoors and outdoors, with specific directional and omnidirectional antennas. Wi-Fi uses microwaves in the 2.4 and 5 GHz frequency bands and IEEE 802.11a, b, g, n standards [1,2]. The 2.4 GHz band has been increasingly used, resulting in higher electromagnetic interference. Therefore, considerable efforts have been put on the 5 GHz band where, however, absorption increases and ranges are shorter.

Nominal transfer rates up to 11 (802.11b), 54 Mbps (802.11 a, g) and 600 Mbps (802.11n) are specified. Carrier sense multiple access with collision avoidance (CSMA/CA) is the medium access control. Studies have been published on wireless communications, wave propagation [3,4], practical setups of WLANs [5], performance analysis of the effective transfer rate for 802.11b PTP links [6], 802.11b performance in crowded indoor environments [7].

Performance evaluation has been a fundamentally important criterion to assess communications quality, leading to more reliable and efficient communications and, therefore, improving enterprise information system yield. In comparison to traditional applications, new telematic applications are especially sensitive to performances. Requirements have been given [8].

Wi-Fi security is very important, ranging from the personal level to the enterprise information system level. Confidentiality is essential. However, as microwave radio waves propagate in the air, they can be very easily captured. Wired equivalent privacy (WEP) was initially intended to provide confidentiality like that of a traditional wired network. A shared key for data encryption is involved. The communicating devices use the same key to encrypt and decrypt radio signals. The cyclic redundancy check 32 (CRC32) checksum used in WEP does not provide a great protection. Besides presenting weaknesses, WEP is still reasonably used in Wi-Fi networks for security reasons, mainly in point-to-point links. More advanced and reliable security methods have been developed to provide authentication such as, by increasing order of security, Wi-Fi protected access (WPA) and Wi-Fi protected access II (WPA2). WPA implements the majority of the IEEE 802.11i standard. It includes a message integrity check (MIC), replacing the CRC used in WEP. WPA2 is compliant with the full IEEE 802.11i standard [1]. It includes Counter Mode with Cipher Block Chaining Message Authentication Code

Manuscript received March 17, 2016. 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.

J. A. R. Pacheco de Carvalho is with the Remote Sensing Unit and the Physics Department, University of Beira Interior, 6201-001 Covilha, Portugal (phone: +351 275 319 703; fax: +351 275 319 719; e-mail: pacheco@ ubi.pt).

H. Veiga is with the Remote Sensing Unit and the Informatics Centre, University of Beira Interior, 6201-001 Covilha, Portugal (e-mail: hveiga@ubi.pt).

C. F. Ribeiro Pacheco is with the Remote Sensing Unit, University of Beira Interior, 6201-001 Covilha, Portugal (e-mail: a17597@ubi.pt).

A. D. Reis is with the Remote Sensing Unit and the Physics Department, University of Beira Interior, 6201-001 Covilha, Portugal, and with the Department of Electronics and Telecommunications/ Institute of Telecommunications, University of Aveiro, 3810 Aveiro, Portugal (e-mail: adreis@ubi.pt).

Protocol (CCMP), a new Advanced Encryption Standard (AES) based encryption mode with enhanced security. Either personal or enterprise modes can be used. In this latter case an 802.1x server is required. Both Temporal Key Integrity Protocol (TKIP) and AES cipher types are usable and a group key update time interval is specified.

Several performance measurements have been made for 2.4 and 5 GHz Wi-Fi Open [9], WEP [10-11], WPA [12-13] and WPA2 [14] links, as well as very high speed FSO [15]. It is important to investigate the effects of increasing levels of security encryption, network topology, on link performance and compare equipment performance for several standards. In the present work new Wi-Fi (IEEE 802.11 a) results arise, using WPA2 links, namely through OSI levels 4 and 7. Performance is evaluated in laboratory measurements of WPA2 point-to-multipoint (PTMP) links using new available equipments. Comparisons are made to corresponding results obtained for WPA2 PTP and Open links. The present work complements previous work of the authors for Open links [16], by investigating the 5 GHz band, where there was the least electromagnetic interference, and WPA2.

In prior and actual state of the art, several Wi-Fi links have been investigated. Performance evaluation has been considered as a crucially important criterion to assess communications quality. The motivation of this work is to evaluate performance in laboratory measurements of WPA2 PTMP links using new available equipments. Comparisons are made to corresponding results obtained mainly for WPA2 PTP and Open links. This contribution permits to increase the knowledge about performance of Wi-Fi (IEEE 802.11a) links [4-6]. The problem statement is that performance needs to be evaluated under security encryption and several topologies. The solution proposed uses an experimental setup and method, permitting to monitor signal to noise ratios (SNR) and noise levels (N) and measure TCP throughput (from TCP connections) and UDP jitter and percentage datagram loss (from UDP communications).

The rest of the paper is structured as follows: Section II is about the experimental details i.e. the measurement setup and procedure. Results and discussion are given in Section III. Conclusions are drawn in Section IV.

II. Experimental Details

The equipments used in the measurements comprised a HP V-M200 access point [17], having three external dual-band 3x3 MIMO antennas, IEEE 802.11 a/b/g/n, software version 5.4.1.0-01-16481 and a 100-Base-TX/10-Base-T Allied Telesis AT-8000S/16 level 2 switch [18]. Two out of three PCs were used having a PCMCIA IEEE.802.11 a/b/g/n Linksys WPC600N wireless adapter with three internal antennas having gains of 2.7 dBi at 2.4 GHz and 1.2 dBi at 2.4 GHz [19], to enable three-node PTMP (PTMP) links to the access point. In every type of experiment, communication channels were used having no interference (ch 36 for 802.11a). This was mainly checked through a portable computer, equipped with a Wi-Fi 802.11 a/b/g/n adapter, running Acrylic WiFi software [20]. WPA2 encryption with AES was activated in the AP and the wireless adapters of the PCs, with a key composed of twenty six hexadecimal characters. The experiments were made under far-field conditions. No power levels above 30 mW (15 dBm) were used, as the wireless equipments were close.

A versatile laboratory setup has been planned and implemented for the PTMP measurements, as shown in Fig. 1. It can involve up to three wireless links to the AP. At OSI level 4, measurements were made for TCP connections and UDP communications using Iperf software [21]. For a TCP client/server connection (TCP New Reno, RFC 6582, was used), TCP throughput was obtained. For a UDP client/server communication with a given bandwidth parameter, UDP jitter and percentage loss of datagrams were determined. TCP packet size and window size were 8k bytes. UDP datagram size and buffer size were 1470 bytes and 8k bytes, respectively.

One PC, with IP 192.168.0.2 was the Iperf server and the others, with IP 192.168.0.6 and 192.168.0.50, could be the Iperf clients (client1 and client2). Jitter, which gives the smooth mean of differences between consecutive transit times, was continuously computed by the server, as specified by the real time protocol RTP, in RFC 1889 [22]. Another PC, with IP 192.168.0.20, was mainly used to control the settings in the AP. The laboratory setup permitted three types of experiments to be made: PTP, using the client1 and the control PC as server; PTMP, using the client1 and the 192.168.0.2 PC as server; 4N-PTMP, using simultaneous connections/communications between the two clients and the 192.168.0.2 PC as server.

The scheme of Fig. 1 was also used for FTP measurements, where FTP server and client applications were configured in the PCs.

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 was the operating system. They were set to optimize the resources assigned to the present work. Batch command files have been re-written to enable the new TCP, UDP and FTP tests.

The results were obtained in batch mode and written as data files to the client PCs disks. Every PC had a second network adapter, to permit remote control from the official IP University network, via switch.

III. Results and Discussion

The wireless network adapters of the PCs were manually configured for IEEE 802.11 a with typical nominal transfer rates (6, 9, 12, 18, 24, 36, 48, 54 Mbps). For every fixed transfer rate, data were obtained for comparison of the laboratory performance of WPA2 and Open PTP and PTMP links at OSI levels 1 (physical layer), 4 (transport layer) and 7 (application layer) using the setup of Fig. 1. For every nominal fixed transfer rate, 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, resulting in average jitter and average percentage datagram loss [16].

At OSI level 1, signal to noise ratios (SNR, in dB) and noise levels (N, in dBm) were measured. Signal indicates the strength of the radio signal the AP receives from a client PC, expressed in dBm. Noise indicates how much background noise, due to radio interference, exists in the signal path between the client PC and the AP, expressed in dBm. The lower (more negative) the value is, the weaker the noise. SNR indicates the relative strength of client PC radio signals versus noise in the radio signal path, expressed 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 Fig. 2. The links had good, high, SNR values.

The main average TCP and UDP results are summarized in Table I, for WPA2 and Open, PTP and PTMP links. The statistical analysis, including calculations of confidence intervals, was carried out as in [23].

In Figs. 3-6 polynomial fits were made (shown as y versus x), using the Excel worksheet, to the 802.11a TCP throughput data for WPA2 PTP and PTMP, as well as Open links, where R2 is the coefficient of determination, which gives information about the goodness of fit. If it is 1.0 it means a perfect fit to data. It was found that, on average, TCP throughput is slightly better for Open than WPA2 PTP links (Table I). This is also the case considering Open and WPA2 PTMP links (Table I). This is due to increase in data length due to WPA2 encryption. However, TCP performance gets significantly degraded in passing from PTP to PTMP links, as the AP has now to maintain links with two PCs.

In Figs. 7-10, the data points representing jitter and percentage datagram loss were joined by smoothed lines. It was found that, on average, the best jitter performances are for Open PTP links (Table I). This is also true if we compare Open and WPA2 PTMP links (Table I). But average jitter performance for PTMP gets degraded when compared to PTP links. Figs. 7-8 show decreases in jitter with increasing nominal transfer rate.

Concerning average percentage datagram loss, the best performances were found for Open PTP links (Table I). This also applies when comparing Open and WPA2 PTMP links (Table I). Percentage datagram loss performance for PTMP is worse than for PTP links.

In comparison to Open links, for WPA2 links, TCP throughput, jitter and percentage datagram loss were found to show performance degradations for WPA2 links, where data length is increased due to encryption. For TCP throughput the decreases were 1.3% and 2.5% for PTP and PTMP links, respectively. These values are within the experimental error. TCP throughput gets visibly degraded by about 47% in changing from PTP to PTMP links, where the processing requirements for the AP are higher so as to maintain links between two PCs.

At OSI level 7 we measured FTP transfer rates versus nominal transfer rates configured in the wireless network adapters of the PCs for IEEE 802.11 a, as in [11]. The results show the same trends found for TCP throughput.

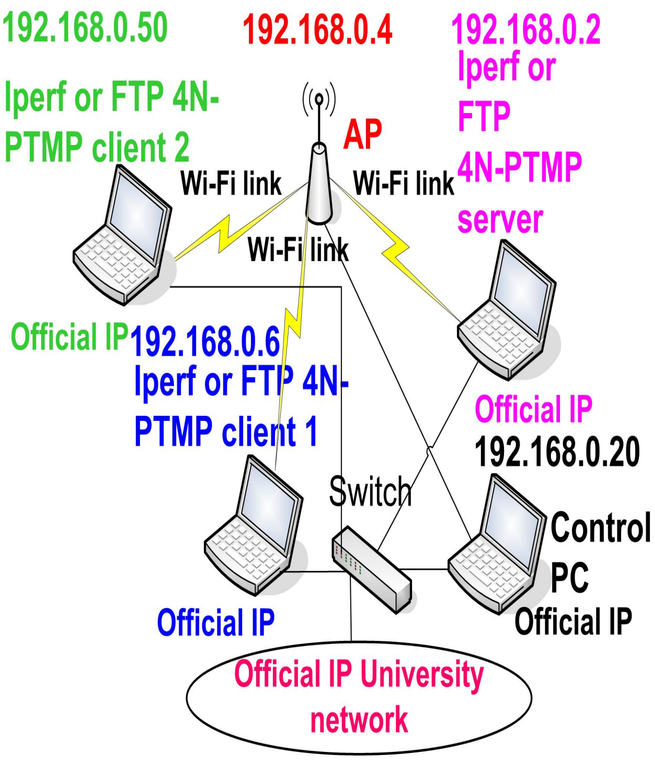

Fig. 1- Laboratory setup scheme.

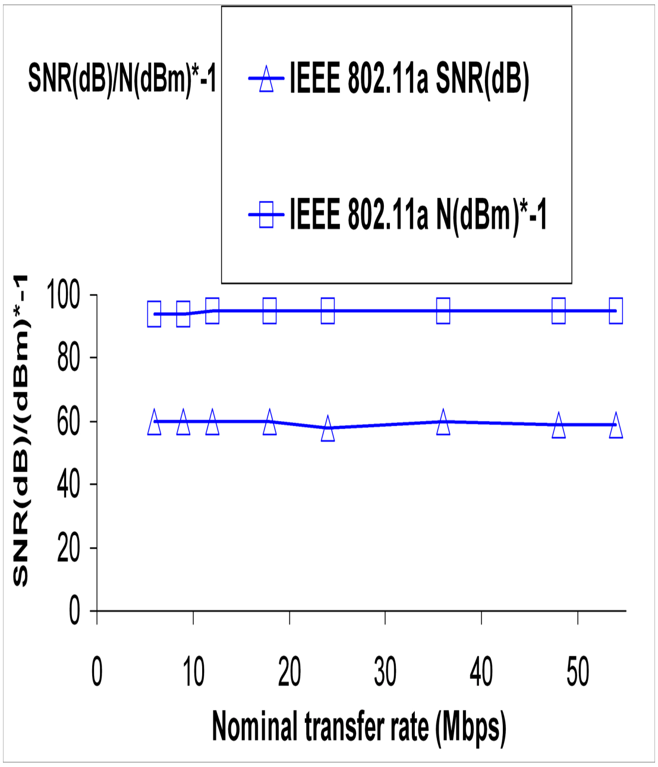

Fig. 2- Typical SNR (dB) and N (dBm). WPA2.

TABLE I
AVERAGE IEEE 802.11 A WPA2 AND OPEN RESULTS: PTP; PTMP

Encryption	WPA2		OPEN	
Parameter/ Link type	PTP	PTMP	PTP	PTMP
TCP throughput (Mbps)	14.8 +-0.5	7.9 +-0.2	15.0 +-0.5	8.1 +-0.2
UDP-jitter (ms)	2.6 +-0.3	3.0 +-0.6	2.2 +-0.1	2.6 +-0.2
UDP-% datagram loss	1.9 +-0.1	2.9 +-0.1	1.4 +-0.1	1.7 +-0.5

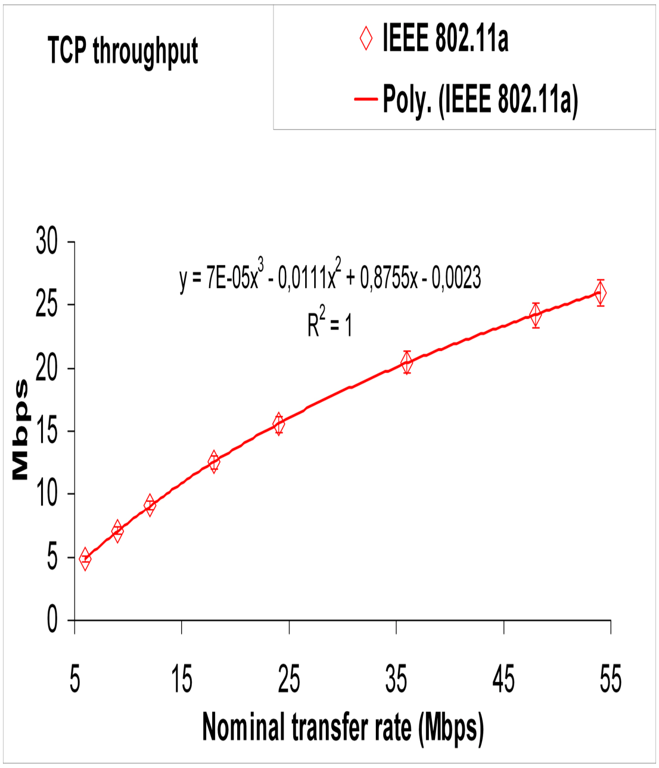

Fig. 4- TCP throughput (y) versus technology and nominal transfer rate (x). Open PTP.

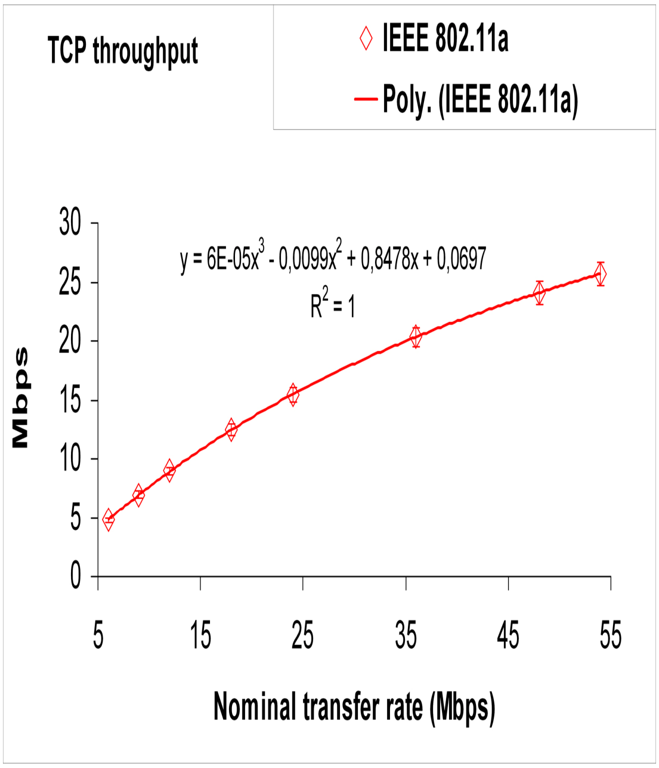

Fig.3- TCP throughput (y) versus technology and nominal transfer rate (x). WPA2 PTP.

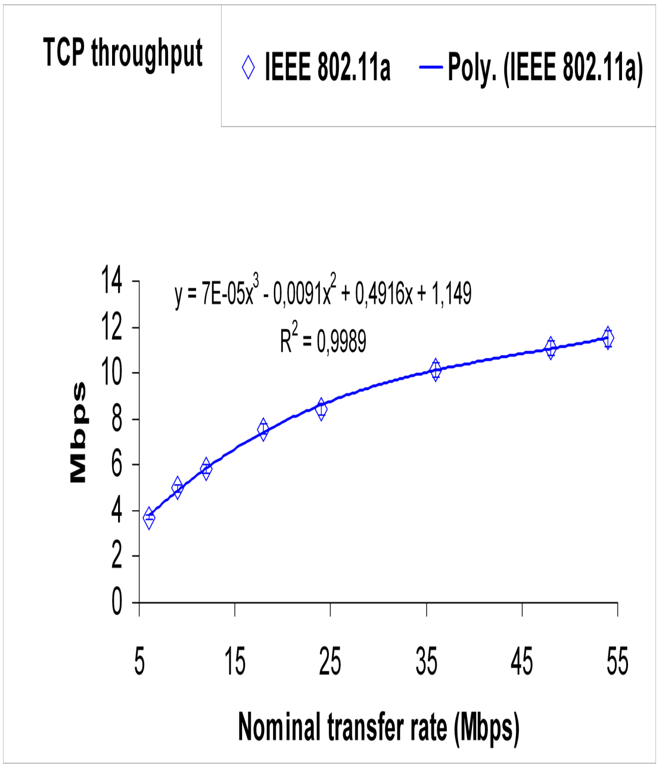

Fig. 5- TCP throughput (y) versus technology and nominal transfer rate (x). WPA2 PTMP.

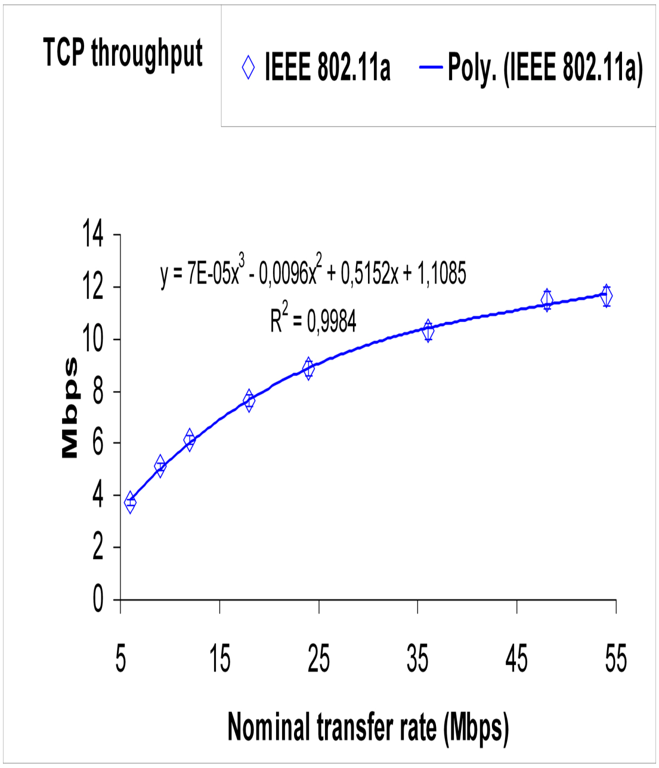

Fig. 6- TCP throughput (y) versus technology and nominal transfer rate (x). Open PTMP.

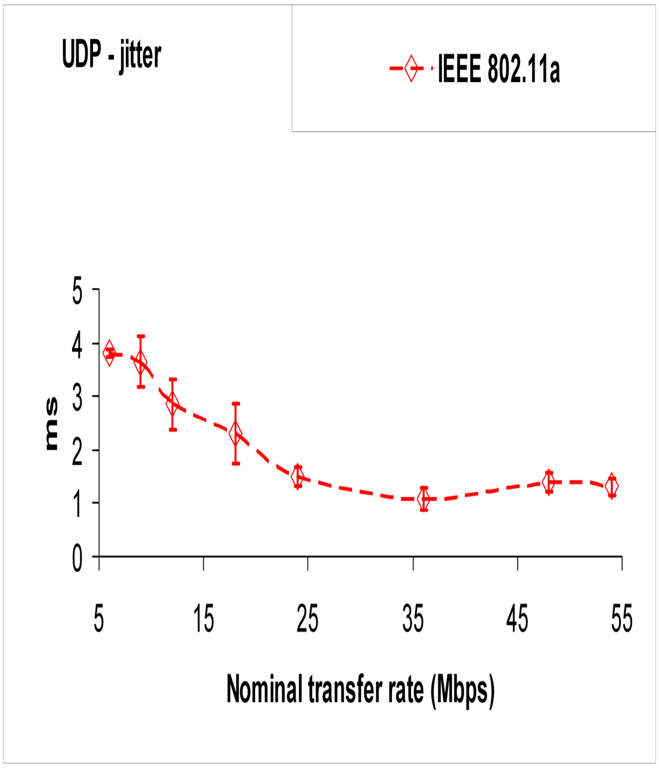

Fig. 8- UDP – jitter results versus technology and nominal transfer rate. Open PTP.

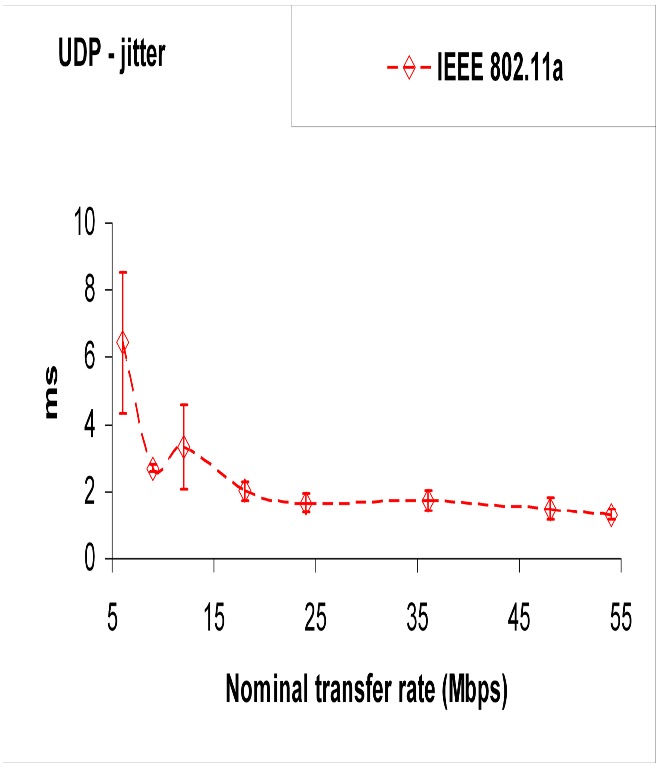

Fig. 7- UDP – jitter results versus technology and nominal transfer rate. WPA2 PTP.

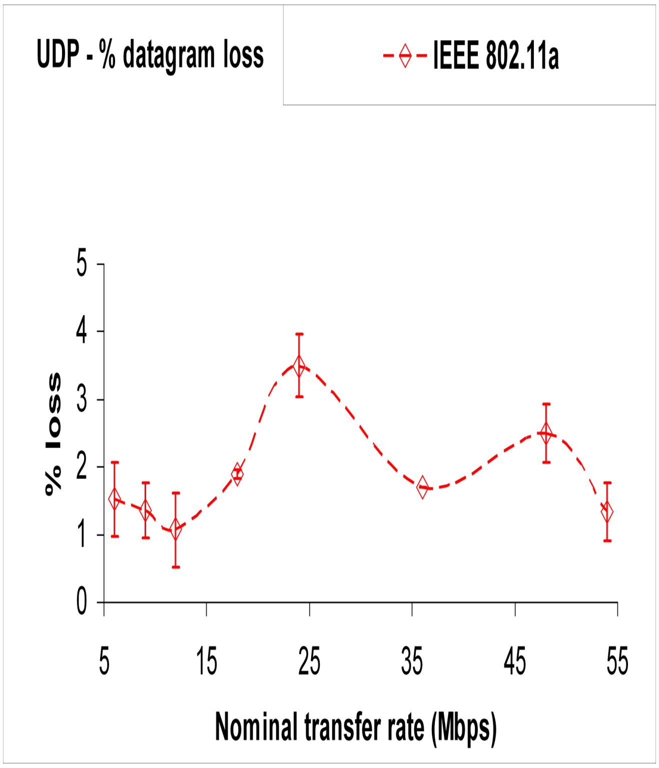

Fig. 9- UDP – percentage datagram loss results versus technology and nominal transfer rate. WPA2 PTP.

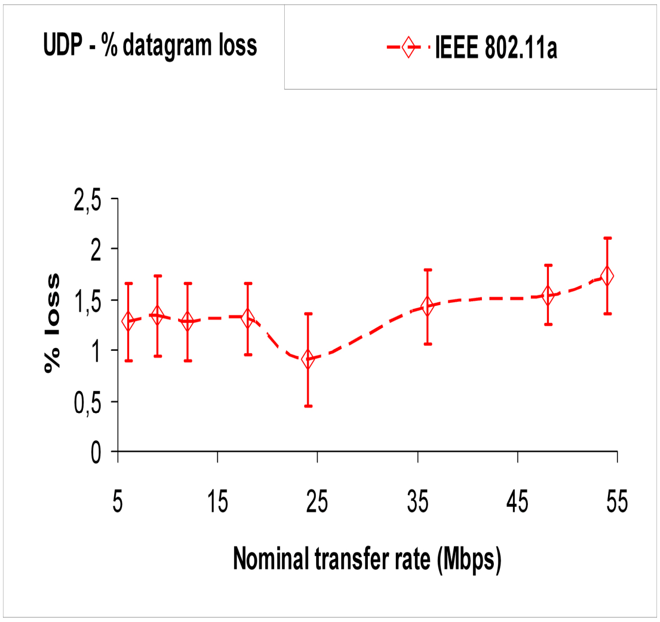

Fig. 10- UDP – percentage datagram loss results versus technology and nominal transfer rate. Open PTP.

IV. Conclusion

In the present work a versatile laboratory setup arrangement was planned and implemented, that permitted systematic performance measurements using new 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 PTMP links.

Through OSI layer 4, TCP throughput, jitter and percentage datagram loss were measured and compared to corresponding results obtained for Open PTP and PTMP links.

In comparison to Open links, TCP throughput, jitter and percentage datagram loss were found to show performance degradations for WPA2 links, where data length is increased due to encryption. However performance decreases in TCP throughput were found to be within the experimental error.

In passing from PTP to PTMP links, more significant performance degradations were found for TCP throughput, jitter and percentage datagram loss, where the processing requirements for the AP are higher so as to maintain links between two PCs. Topology effects on performance were found far more significant than WPA2 encryption effects.

At OSI layer 7, FTP performance results have shown similar trends as those found for TCP throughput.

Further performance studies are planned using several equipments, topologies, security settings and noise conditions, not only in laboratory but also in outdoor environments involving, mainly, medium range links.

References

[1] IEEE Std 802.11-2007, 2007. “IEEE Standard for Local and metropolitan area networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications”, Web site http://standards.ieee.org/getieee802.

[2] . IEEE Std 802.11-2009, 2009. “IEEE Standard for Local and metropolitan area networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications; amendment 5: Enhancements for Higher Throughput”, Web site http://standards.ieee.org/getieee802.

[3] J. W. Mark, W. Zhuang, *Wireless Communications and Networking*, Prentice-Hall, Inc., Upper Saddle River, NJ, 2003.

[4] T. S. Rappaport, *Wireless Communications Principles and Practice*, 2nd ed., Prentice-Hall, Inc., Upper Saddle River, NJ, 2002.

[5] W. R. Bruce III, R. Gilster, *Wireless LANs End to End*, Hungry Minds, Inc., NY, 2002.

[6] M. Schwartz, *Mobile Wireless Communications*, Cambridge University Press, 2005.

[7] N. Sarkar, K. Sowerby, “High Performance Measurements in the Crowded Office Environment: a Case Study”, In *Proc. ICCT’06-International Conference on Communication Technology*, pp. 1-4, Guilin, China, 27-30 November 2006.

[8] F. Boavida, E. Monteiro, *Engenharia de Redes Informáticas*, 10th ed., FCA-Editora de Informática Lda, Lisbon, 2011.

[9] J. A. R. Pacheco de Carvalho, H. Veiga, P. A. J. Gomes, C. F. Ribeiro Pacheco, N. Marques, A. D. Reis, “Wi-Fi Point-to-Point Links- Performance Aspects of IEEE 802.11 a,b,g Laboratory Links”, in *Electronic Engineering and Computing Technology, Series: Lecture Notes in Electrical Engineering*, Sio-Iong Ao, Len Gelman, Eds. Netherlands: Springer, 2010, Vol. 60, pp. 507-514.

[10] José A. R. Pacheco de Carvalho, H. Veiga, Nuno Marques, Cláudia F. F. P. Ribeiro Pacheco, A. D. Reis, “TCP, UDP and FTP Performances of Laboratory Wi-Fi IEEE 802.11g WEP Point-to-Point Links”, in Communications in Computer and Information Science, M.M. Cruz-Cunha et al., Eds. Berlin Heidelberg: Springer, 2011, Vol. 220, Part II, pp. 188–195.

[11] J. A. R. Pacheco de Carvalho, H. Veiga, N. Marques, C. F. Ribeiro Pacheco, A. D. Reis, “Wi-Fi WEP Point-to-Point Links- Performance Studies of IEEE 802.11 a,b,g Laboratory Links”, in *Electronic Engineering and Computing Technology, Series: Lecture Notes in Electrical Engineering,* Sio-Iong Ao, Len Gelman, Eds. Netherlands: Springer, 2011, Vol. 90, pp. 105-114.

[12] J. A. R. Pacheco de Carvalho, H. Veiga, C. F. Ribeiro Pacheco, A. D. Reis, “Performance Evaluation of Laboratory Wi-Fi IEEE 802.11g WPA Point-to-Point Links Using TCP, UDP and FTP”, Proc. Conference on ENTERprise Information Systems CENTERIS 2012 / HCIST 2012, Vilamoura (Algarve), Portugal, 3-5 October, SciVerseScienceDirect, Procedia Technology, 2012, 5, pp. 302–309.

[13] J. A. R. Pacheco de Carvalho, H. Veiga, C. F. Ribeiro Pacheco, A. D. Reis, “Performance Evaluation of Laboratory Wi-fi Ieee 802.11a Wpa Point-to-multipoint Links”, Proc. Conference on ENTERprise Information Systems CENTERIS 2013 / HCIST 2013, Lisboa-Portugal 23-25 October 2013, SciVerseScienceDirect, Procedia Technology, 2013, 9, pp. 146 – 151.

[14] J. A. R. Pacheco de Carvalho, H. Veiga, C. F. Ribeiro Pacheco, A. D. Reis,” Performance Evaluation of IEEE 802.11 a, g Laboratory WPA2 Point-to-Multipoint Links”, *Proc. WCE 2014 - World Congress on Engineering 2014*, Imperial College London, London, England, 2-4 July, 2014, pp. 699-704.

[15] J. A. R. Pacheco de Carvalho, N. Marques, H. Veiga, C. F. F. Ribeiro Pacheco, A. D. Reis, “Performance Measurements of a 1550 nm Gbps FSO Link at Covilhã City, Portugal”, *Proc. Applied Electronics 2010 - 15th International Conference*, 8-9 September 2010, University of West Bohemia, Pilsen, Czech Republic, pp. 235-239.

[16] J. A. R. Pacheco de Carvalho, C. F. Ribeiro Pacheco, A. D. Reis, H. Veiga, ”Laboratory Performance Measurements of IEEE 802.11 b, g Open Four-node PTMP Links”, Lecture Notes in Engineering and Computer Science: Proceedings of the World Congress on Engineering 2015, WCE 2015, 1-3 July, 2015, London, U.K., pp. 622-626.

[17] HP V-M200 802.11n access point management and configuration guide; 2010; http://www.hp.com; accessed 3 Jan 2016.

[18] AT-8000S/16 level 2 switch technical data; 2009; http://www.alliedtelesis.com; accessed 10 Dec 2015.

[19] WPC600N notebook adapter user guide; 2008; http://www.linksys.com.; accessed 10 Jan 2012.

[20] Acrylic WiFi software; 2016; http://www.acrylicwifi.com; accesse 8 Jan 2016.

[21] Iperf software; 2016; http://iperf.fr; accessed 16 Feb 2016.

[22] Network Working Group. “RFC 1889-RTP: A Transport Protocol for Real Time Applications”, http://www.rfc-archive.org; accessed 3 Jan 2014.

[23] P. R. Bevington, Data Reduction and Error Analysis for the Physical Sciences, Mc Graw-Hill Book Company, 1969.