Comparative Performance Studies of Laboratory WPA IEEE 802.11b,g Point-to-Point Links

José A. R. Pacheco de Carvalho[1], Cláudia F. F. P. Ribeiro Pacheco[2], Hugo Veiga[3], António D. Reis[4]
[1]José Pacheco de Carvalho is with the Remote Detection Unit and the Physics
Department at the University of Beira Interior
R. Marquês d'Ávila e Bolama, 6201-001 Covilhã, Portugal
{pacheco@ubi.pt}

[2]Cláudia Pacheco is with the Remote Detection Unit at the University of Beira Interior
R. Marquês d'Ávila e Bolama
6201-001 Covilhã, Portugal
{a17597@ubi.pt}

[3]Hugo Veiga is with the Remote Detection Unit and the Informatics Centre at the
University of Beira Interior
R. Marquês d'Ávila e Bolama, 6201-001 Covilhã, Portugal
{hveiga@ubi.pt}

[4]António Reis is with the Remote Detection Unit and the Physics
Department at the University of Beira Interior, and with the
Department of Electronics and Telecommunications, Institute of Telecommunications at the University of Aveiro
3810 Aveiro, Portugal
{adreis@ubi.pt}
.

ABSTRACT: *Wireless communications using microwaves are increasingly important, e.g. Wi-Fi. Performance is a very crucial issue, resulting in more reliable and efficient communications. Security is equally very important. Laboratory measurements are made about several performance aspects of Wi-Fi IEEE 802.11 b, g WPA point-to-point links. A contribution is given to performance evaluation of this technology under WPA encryption, using available equipments (DAP-1522 access points from D-Link and WPC600N adapters from Linksys). Detailed results are presented and discussed, namely at OSI levels 4 and 7, from TCP, UDP and FTP experiments, permitting measurements of TCP throughput, jitter, percentage datagram loss and FTP transfer rate. Comparisons are made to corresponding results obtained for open links. Conclusions are drawn about the comparative performance of the links.*

Keywords: WLAN, Wi-Fi, WPA Point-to-Point Links, IEEE 802.11b, IEEE 802.11g, Wireless Network Laboratory Performance

Received: 8 May 2023, Revised 3 July 2023, Accepted 10 July 2023

DOI: 10.6025/jdp/2023/13/3/65-73

1. Introduction

Contactless communication techniques have been developed using mainly electromagnetic waves in several frequency ranges, propagating in the air. Wi-Fi and FSO, whose importance and utilization have been recognized and growing, are representative examples of wireless communications technologies.

Wi-Fi is a microwave based technology providing for versatility, mobility and favorable prices. The importance and utilization of Wi-Fi has been growing as it complements traditional wired networks. It has been used both in ad hoc mode and in infrastructure mode. In this case a WLAN arises based on an access point, AP, which permits communications of Wi-Fi electronic devices with a wired based LAN through a switch/router. Wi-Fi has penetrated the personal home, where a WPAN allows personal devices to communicate. Point-topoint and point-to-multipoint configurations are used both indoors and outdoors, requiring specific directional and omnidirectional antennas. Wi-Fi uses microwaves in the 2.4 and 5 *GHz* frequency bands and IEEE 802.11a, 802.11b, 802.11g and 802.11n standards [1]. The 2.4 *GHz* band is intensively used and is having increasing interferences. Therefore considerable attention has been focused 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. The medium access control is CSMA/CA. There are studies on wireless communications, wave propagation [2,3], practical implementations of WLANs [4], performance analysis of the effective transfer rate for 802.11b point-to-point links [5], 802.11*b* performance in crowded indoor environments [6].

Performance has been a very important issue, resulting in more reliable and efficient communications. In comparison to traditional applications, new telematic applications are specially sensitive to performances. Requirements have been pointed out [7]. E.g. requirements have been quoted as: for video on demand/moving images, 1-10 *ms* jitter and 1-10 *Mbps* throughput; for Hi Fi stereo audio, jitter less than 1 ms and 0.1-1 *Mbps* throughputs.

Wi-Fi security is very important. Microwave radio signals can be very easily captured as they travel through the air. Therefore, several security methods have been developed to provide authentication such as, by increasing order of security, WEP, WPA and WPA2. WEP was initially intended to provide confidentiality comparable to 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 CRC32 checksum used in WEP does not provide a great protection. However, in spite of its weaknesses, WEP is still widely used in Wi-Fi communications for security reasons, mainly in point-to-point links. WPA implements the majority of the IEEE 802.11*i* standard [1]. It includes a MIC, message integrity check, replacing the CRC used in WEP. Either personal or enterprise modes can be used. In this latter case an 802.1*x* server is required. Both 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 [8-9] and WEP links [10], as well as very high speed FSO [11]. It is important to find the effects of WPA encryption on link performance. Therefore, in the present work new Wi-Fi (IEEE 802.11 *b,g*) results arise, using personal mode WPA, through OSI levels 4 and 7. Performance is evaluated in laboratory measurements of WPA point-to-point links using new available equipments. Comparisons are made to corresponding results obtained for open links.

The rest of the paper is structured as follows: Chapter 2 presents the experimental details i.e. the measurement setup and procedure. Results and discussion are presented in Chapter 3. Conclusions are drawn in Chapter 4.

2. Experimental Details

The measurements used a D-Link DAP-1522 bridge/access point [12], with internal PIFA *2 antenna, IEEE 802.11 *a*/*b*/*g*/*n*, firmware version 1.31 and a 100-Base-TX/10-Base-T Allied Telesis AT-8000S/16 level 2 switch [13].The wireless mode was set to access point mode. The firmware from the manufacturer did not make possible a point-to-point link with a similar equipment. Therefore, a PC was used having a PCMCIA IEEE.802.11 *a*/*b*/*g*/*n* Linksys WPC600N wireless adapter with three internal antennas [14], to enable a PTP link to the access point. In every type of experiment, interference free communication channels were used (*ch* 8 for 802.11*b,g*). This was checked through a portable computer, equipped with a Wi-Fi 802.11 *a*/*b*/

g/*n* adapter, running NetStumbler software [15]. WPA personal encryption was activated in the AP and the PC wireless adapter using AES and a shared key with 26 ASCII characters. The experiments were made under far-field conditions. No power levels above 30 *mW* (15 *dBm*) were required, as the access points were close.

A laboratory setup has been planned and implemented for the measurements, as shown in Figure 1. At OSI level 4, measurements were made for TCP connections and UDP communications using Iperf software [16]. For a TCP connection, TCP throughput was obtained. For a UDP communication with a given bandwidth parameter, UDP throughput, jitter and percentage loss of datagrams were determined. Parameterizations of TCP packets, UDP datagrams and window size were as in [10]. One PC, with IP 192.168.0.2 was the Iperf server and the other, with IP 192.168.0.6, was the Iperf client. Jitter, representing 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 [17]. The scheme of Figure 1 was also used for FTP measurements, where FTP server and client applications were installed in the PCs with IPs 192.168.0.2 and 192.168.0.6, respectively. The server PC also permitted manual control of the settings in the access point.

The server and client PCs were HP nx9030 and nx9010 portable computers, respectively, running Windows XP. They were configured to optimize the resources allocated to the present work. Batch command files have been written to enable the TCP, UDP and FTP tests.

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

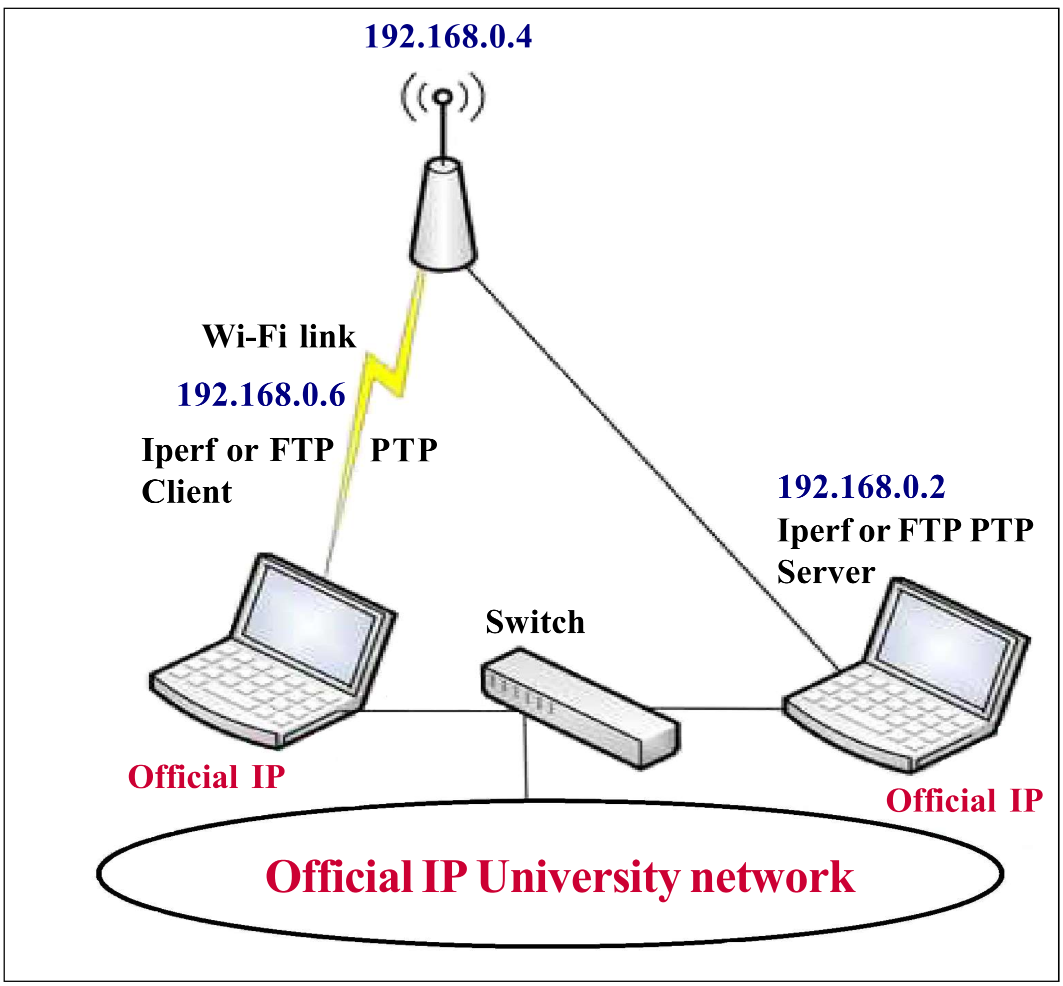

Figure 1. Laboratory setup scheme

3. Results and Discussion

The access point and the PC wireless network adapter were manually configured, for each standard IEEE 802.11 *b*, *g*, with typical fixed transfer rates (1, 2, 5, 11 *Mbps* for 802.11*b*; 6, 9, 12, 18, 24, 36, 48, 54 *Mbps* for 802.11*g*). For every fixed transfer rate, data were obtained for comparison of the laboratory performance of the WPA and Open links at OSI layers 1 (physical layer), 4 (transport layer) and 7 (application layer) using the setup of Figure 1. For each standard and every nominal fixed transfer rate, an average TCP throughput was determined from several experiments. This value was used as the bandwidth parameter for every corresponding UDP test, giving average jitter and average percentage datagram loss.

At OSI level 1, noise levels (N, in dBm) and signal to noise ratios (SNR, in dB) were monitored and typical values are shown in Figure 2 and Figure 3, for open and WPA links, and 802.11*b*, *g*, respectively.

The main average TCP and UDP results are summarized in Table I, both for WPA and open links. In Figure 4 polynomial fits were made to the 802.11*b*, *g* TCP throughput data for WPA links, where R2 is the coefficient of determination. It was found that the best TCP throughputs are for 802.11 *g*, for every link type. The 802.11 *b*, *g* average data are reasonably close for both link types. The best average 802.11*g* TCP throughput is for open links. In Figures 5-7, the data points representing jitter and percentage datagram loss were joined by smoothed lines. Concerning jitter it was found that, on average, the best jitter performances are for 802.11 *g* for both link types. For each standard, jitter performances agree reasonably well within the experimental errors. However average jitter for 802.11 b is slightly higher for WPA (5.5+- 0.2 *ms*) than for Open links (5.3+-0.3 *ms*), meaning that in this case increasing security leads to a minor degradation of jitter performance. Figure 7 shows percentage datagram loss data. Except for 802.11 *g*, where the highest value is for WPA, no significant sensitivities were found for most data (1.4 % on average), within the experimental errors, either to standard or link type.

At OSI level 7 we measured FTP transfer rates versus nominal transfer rates configured in the access point and the PC wireless network adapter for IEEE 802.11 *b*, *g* as in [10]. The results show the same trends found for TCP throughput.

Generally, except for 802.11*g* TCP throughput, 802.11 *b* jitter and 802.11*g* percentage datagram loss, the results measured for WPA links were found to agree, within the experimental errors, with corresponding data obtained for Open links.

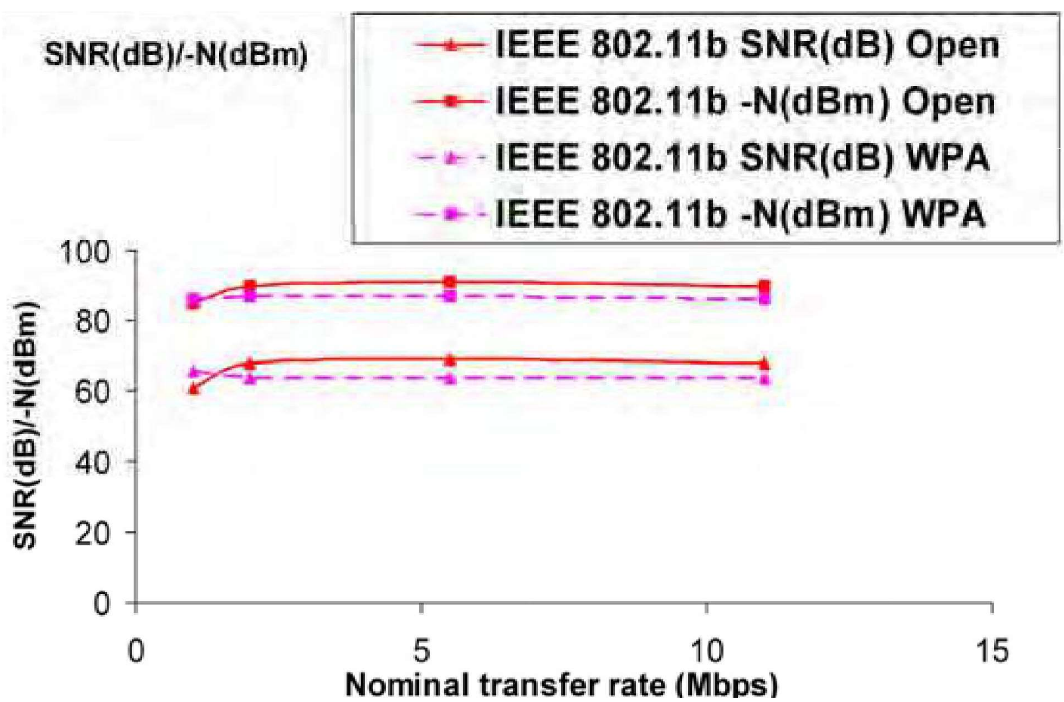

Figure 2. Typical SNR (*dB*) and N (*dBm*); 802.11b;WPA and open links

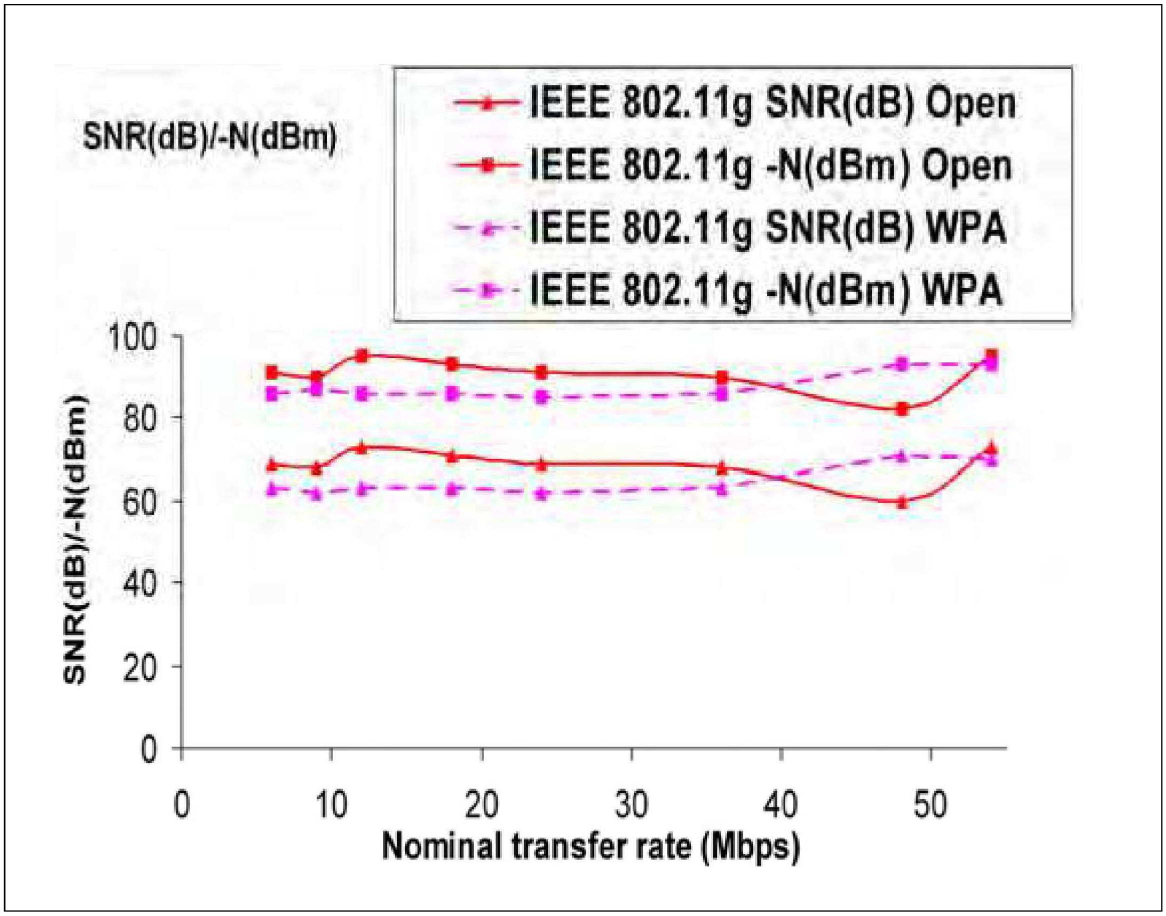

Figure 3. Typical SNR (dB) and N (dBm); 802.11g; WPA and open links

Link type	**WPA**		**Open**	
Parameter/ IEEE standard	**802.11*b***	**802.11*g***	**802.11*b***	**802.11*g***
TCP throughput (*Mbps*)	2.9 +-0.1	13.4 +-0.4	3.0 +-0.1	14.5 +-0.4
UDP-jitter (*ms*)	5.5 +-0.2	2.3 +-0.1	5.3 +-0.3	2.3 +-0.1
UDP-% datagram loss	1.2 +-0.2	1.8 +-0.2	1.2 +-0.2	1.2 +-0.1
FTP transfer rate (*kbyte/s*)	280.2 +-11.2	1450.6 +-58.0	289.9 +-11.6	1526.9 +-61.1

Table 1. Average Wi-Fi (IEEE 802.11 b,g) results; WPA and Open links

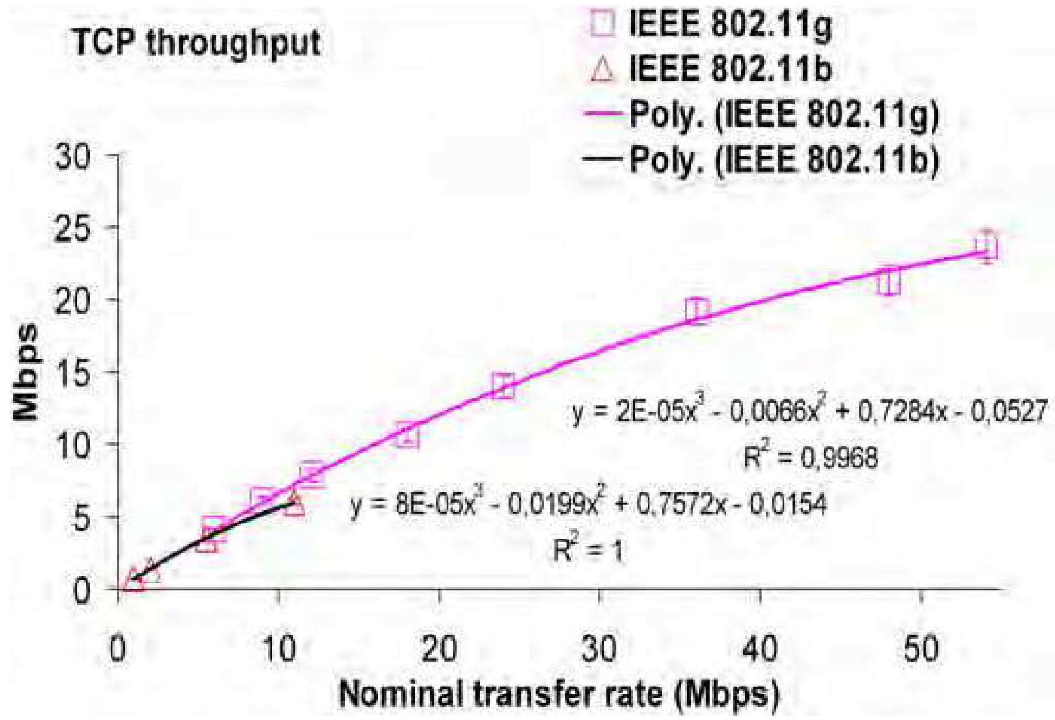

Figure 4. TCP throughput versus technology and nominal transfer rate; WPA links

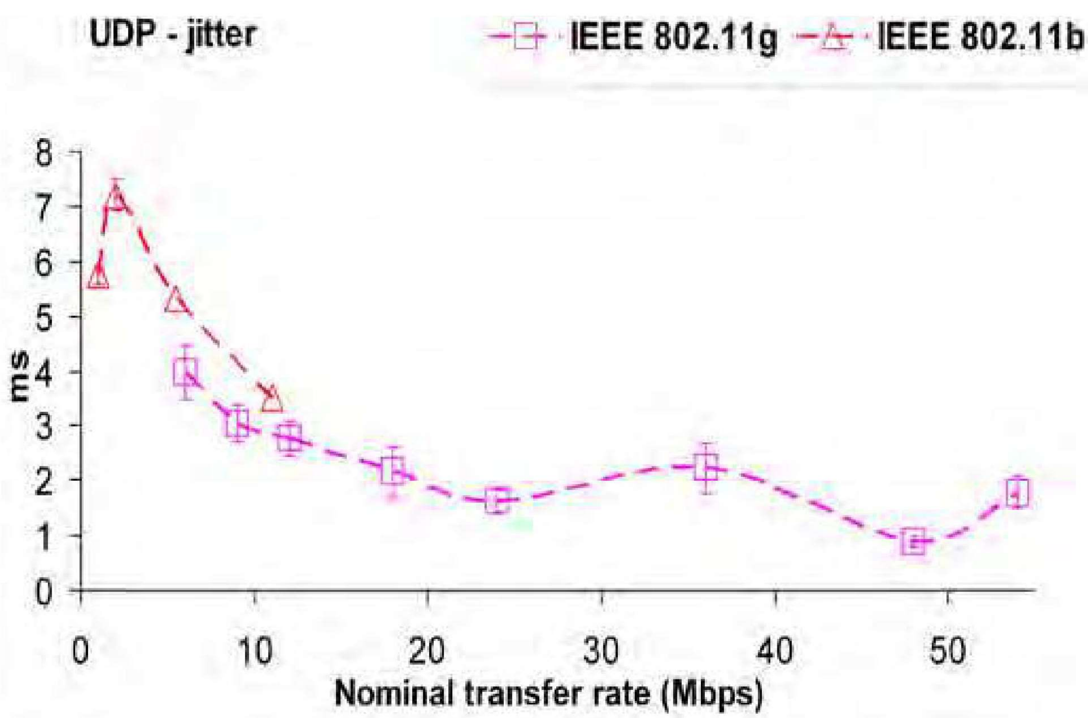

Figure 5. UDP - jitter results versus technology and nominal transfer rate; WPA links

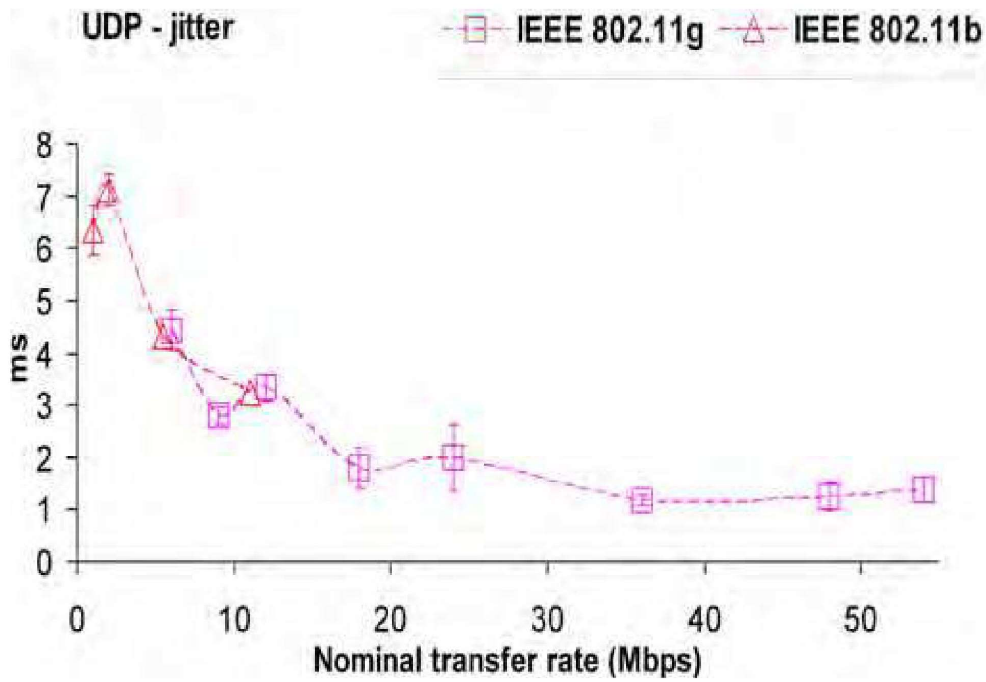

Figure 6. UDP - jitter results versus technology and nominal transfer rate; open links

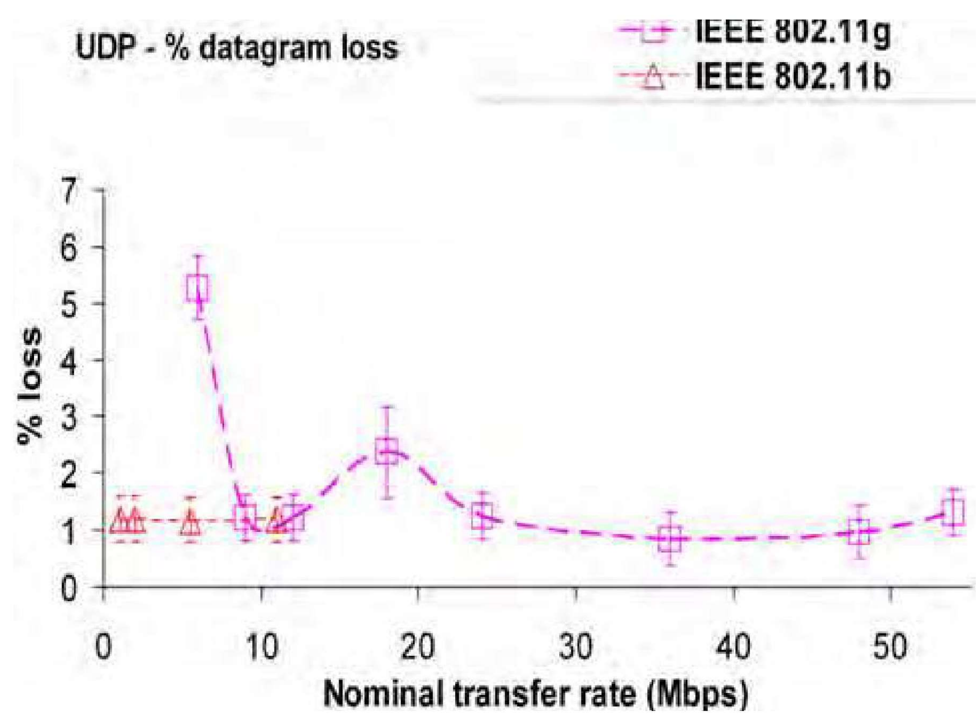

Figure 7. UDP – percentage datagram loss versus technology and nominal transfer rate; WPA links

4. Conclusion

A new laboratory setup arrangement has been planned and implemented, that permitted systematic performance measurements of new available wireless equipments (DAP- 1522 access points from D-Link and WPC600N adapters from Linksys) for Wi-Fi (IEEE 802.11 *b,g*) in WPA point-to-point links.

Through OSI layer 4, TCP throughput, jitter and percentage datagram loss were measured and compared for WPA and open links. Generally, except for 802.11g TCP throughput, 802.11 *b* jitter and 802.11*g* percentage datagram loss, where increasing security encryption was found to degrade performances, the results measured for WPA links were found to agree, within the experimental errors, with corresponding data obtained for Open links.

At OSI layer 7, FTP performance results have shown the same trends found for TCP throughput.

Additional performance measurements either started or are planned using several equipments, security settings and experimental conditions, not only in laboratory but also in outdoor environments involving, mainly, medium range links.

Acknowledgement

Supports from Universidade da Beira Interior and FCT (Fundação para a Ciência e a Tecnologia)/PEst- OE/FIS/UI0524/2011 (Projecto Estratégico-UI524-2011- 2012) are acknowledged.

References

[1] IEEE Standards Association. (Year). IEEE 802.11a, 802.11b, 802.11g, 802.11n, 802.11i standards. Retrieved from http://standards.ieee.org

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

[3] Rappaport, T. S. (2002). *Wireless Communications Principles and Practice* (2nd ed.). Prentice-Hall, Inc.

[4] Bruce III, W. R., Gilster, R. (2002). *Wireless LANs End to End*. Hungry Minds, Inc.

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

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

[7] Monteiro, E., Boavida, F. (2002). *Engineering of Informatics Networks* (4th ed.). FCA-Editor of Informatics Ld.

[8] Pacheco de Carvalho, J. A. R., Gomes, P. A. J., Veiga, H., Reis, A. D. (2008). Development of a University Networking Project. In G. D. Putnik & M. M. Cunha (Eds.), *Encyclopedia of Networked and Virtual Organizations* (pp. 409-422). IGI Global.

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

[10] Pacheco de Carvalho, J. A. R., Veiga, H., Marques, N., Ribeiro Pacheco, C. F., Reis, A. D. (2011). Wi-Fi WEP Point-to-Point Links- Performance Studies of IEEE 802.11 a,b,g Laboratory Links." In S. I. Ao & L. Gelman (Eds.), *Electronic Engineering and Computing Technology*, Series: *Lecture Notes in Electrical Engineering* (Vol. 90, pp. 105-114). Springer.

[11] Pacheco de Carvalho, J. A. R., Marques, N., Veiga, H., Ribeiro Pacheco, C. F., Reis, A. D. (2010). Experimental Performance Evaluation of a Gbps FSO Link: a Case Study. In *Proceedings of the International Conference on Wireless Information Networks and Systems (WINSYS 2010)* (pp. 123-128). Athens, Greece.

[12] D-Link Corporation. DAP-1522 wireless bridge/access point technical manual. Retrieved from http://www.dlink.com

[13] Allied Telesis. AT-8000S/16 level 2 switch technical data. Retrieved from http://www.alliedtelesis.com

[14] Linksys, a division of Cisco Systems, Inc. WPC600N notebook adapter user guide. Retrieved from http://www.linksys.com

[15] NetStumbler. NetStumbler software. Retrieved from http://www.netstumbler.com

[16] National Laboratory for Applied Network Research. Iperf software. Retrieved from http://dast.nlanr.net

[17] Network Working Group. RFC 1889-RTP: A Transport Protocol for Real Time Applications. Retrieved from http://www.rfcarchive.org