Laboratory Performance of Wi-Fi IEEE 802.11 B,G WPA2 Point-to-Point Links: a Case Study

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

Abstract—**Wireless communications using microwaves are increasingly important, e.g. Wi-Fi. Performance is a crucial issue, leading to more reliable and efficient communications. Security is equally very important. Laboratory measurements are made about several performance aspects of Wi-Fi (IEEE 802.11b, g) WPA2 point-to-point links. A contribution is given to performance evaluation of this technology under WPA2 encryption, using available equipments (WRT54GL wireless routers from Linksys). 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 open links. Conclusions are drawn about the comparative performance of the links.**

Index Terms—**Wi-Fi, WLAN, WPA2 Point-to-Point Links, IEEE 802.11b, IEEE 802.11g, Wireless Network Laboratory Performance.**

I. INTRODUCTION

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

Wi-Fi is a microwave based technology providing for versatility, mobility and favourable prices. The importance and utilization of Wi-Fi have been growing for complementing traditional wired networks. It has been used both in ad hoc mode and in infrastructure mode. In this case an access point, AP, permits communications of Wi-Fi devices with a wired based LAN through a switch/router. In this way a WLAN, based on the AP, is formed. Wi-Fi has reached the personal home, forming a WPAN, allowing personal devices to communicate. Point-to-point 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]. As the 2.4 GHz band becomes increasingly used and interferences increase, the 5 GHz band has received considerable attention, although 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. CSMA/CA is the medium access control. Wireless communications, wave propagation [2,3] and practical implementations of WLANs [4] have been studied. Detailed information has been given about the 802.11 architecture, including performance analysis of the effective transfer rate. An optimum factor of 0.42 was presented for 11 Mbps point-to-point links [5]. Wi-Fi (802.11b) performance measurements are available for crowded indoor environments [6].

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

Wi-Fi security is very important. Microwave radio signals travel through the air and can be easily captured by virtually everyone. 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. In WEP, 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. WPA implements the majority of the IEEE 802.11i standard [1]. It includes a MIC, message integrity check, replacing the CRC used in WEP. WPA2 is compliant with the full IEEE 802.11i standard. It includes CCMP, a new AES-based encryption mode with enhanced security. WPA and WPA2 can be used in either personal or enterprise modes. In this latter case an 802.1x 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 [8-10] and WEP links [11], as well as very high speed FSO [12]. In the present work new Wi-Fi (IEEE 802.11 b,g) results arise, using personal mode WPA2,

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

H. Veiga and N. Marques are with the Remote Detection Unit and the Informatics Centre, University of Beira Interior, 6201-001 Covilhã, Portugal (e-mails: hveiga@ubi.pt; nmarques@ubi.pt).

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

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

through OSI levels 4 and 7. Performance is evaluated in laboratory measurements of WPA2 point-to-point links using available equipments. Comparisons are made to corresponding results obtained for open links.

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

II. EXPERIMENTAL DETAILS

The measurements used (Fig.1) Linksys WRT54GL wireless routers [13], with a Broadcom BCM5352 chip rev0, internal diversity antennas, firmware DD-WRT v24-sp1-10011 [14] and a 100-Base-TX/10-Base-T Allied Telesis AT-8000S/16 level 2 switch [15]. The wireless mode was set to bridged access point. In every type of experiment, interference free communication channels were used. This was checked through a portable computer, equipped with a Wi-Fi 802.11 a/b/g adapter, running NetStumbler software [16]. WPA2 personal encryption was activated in the APs, using AES and a shared key composed of 9 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 was planned and implemented for the measurements, as shown in Fig. 2. At OSI level 4, measurements were made for TCP connections and UDP communications using Iperf software [17], permitting network performance results to be recorded. 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. TCP packets and UDP datagrams of 1470 bytes size were used. A window size of 8 kbytes and a buffer size of the same value were used for TCP and UDP, respectively. 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, which indicates the smooth mean of differences between consecutive transit times, was continuously computed by the server, as specified by RTP in RFC 1889 [18]. The scheme of Fig. 2 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 and client PCs were HP nx9030 and nx9010 portable computers, respectively, running Windows XP. They were configured to maximize the resources allocated to the present work. Batch command files were 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 Unit network, via switch.

III. RESULTS AND DISCUSSION

The access points were configured for each standard IEEE 802.11 b, g with typical nominal transfer rates (1, 2, 5.5 and 11 Mbps for IEEE 802.11 b; 6, 9, 12, 18, 24, 36, 48, 54 Mbps for IEEE 802.11 g). For each standard, measurements were

made for every fixed transfer rate. In this way, data were obtained for comparison of the laboratory performance of the links, measured namely at OSI levels 1 (physical layer), 4 (transport layer) and 7 (application layer) using the setup of Fig. 2. In each experiment type, 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 Fig. 3 and Fig. 4 for WPA2 and open links, respectively.

The main average TCP and UDP results are summarized in Table I, both for WPA2 and open links. In Fig. 5 polynomial fits were made to the 802.11b, g TCP throughput data for WPA2 links, where R^2 is the coefficient of determination. It was found that the best TCP throughputs are for 802.11 g. A fairly good agreement was found for the 802.11 b, g data both for WPA2 and open links. In Figs. 6-7, 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 802.11 g both for WPA2 (2.4 +- 0.1 ms) and open links (1.2 +- 0.1 ms). On average, both for 802.11 b and 802.11g, the best jitter performances were found for open links. Concerning percentage datagram loss data (1.4 % on average) no significant sensitivities were found, 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 points for the IEEE 802.11b, g standards. Every measurement was the average for a single FTP transfer, using a binary file size of 100 Mbytes. The average results thus obtained are summarized in Table 1, both for WPA2 and open links. In Fig. 8 polynomial fits are shown to 802.11 b, g data for WPA2 links. It was found that, for each link type, the best FTP performances were for 802.11g. A fairly good agreement was found for the 802.11 b, g data both for WPA2 and open links. These results show the same trends found for TCP throughput.

Generally, except for jitter, the results measured for WPA2 links were found to agree, within the experimental errors, with corresponding data obtained for open links.

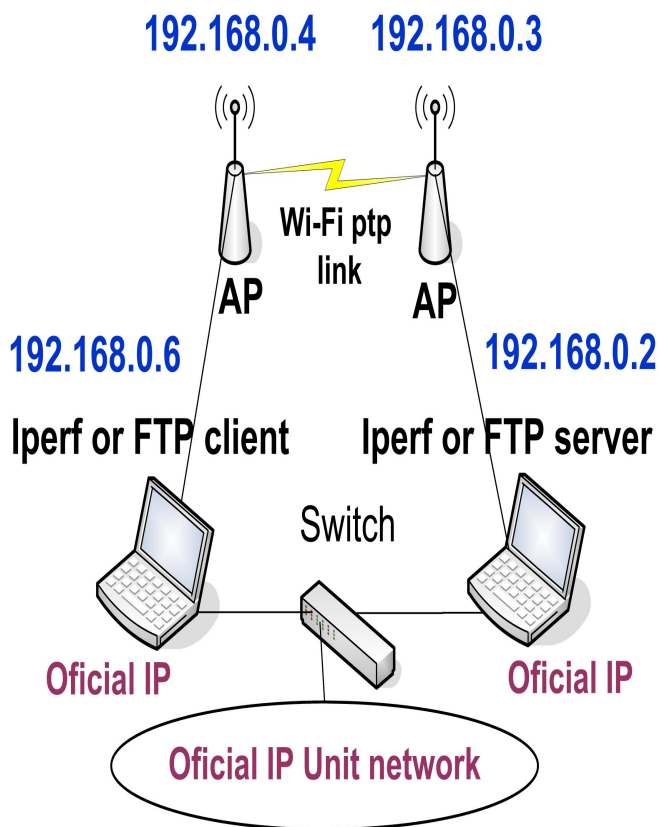Fig. 1- Wireless router (A) [13] and switch (B) [15].
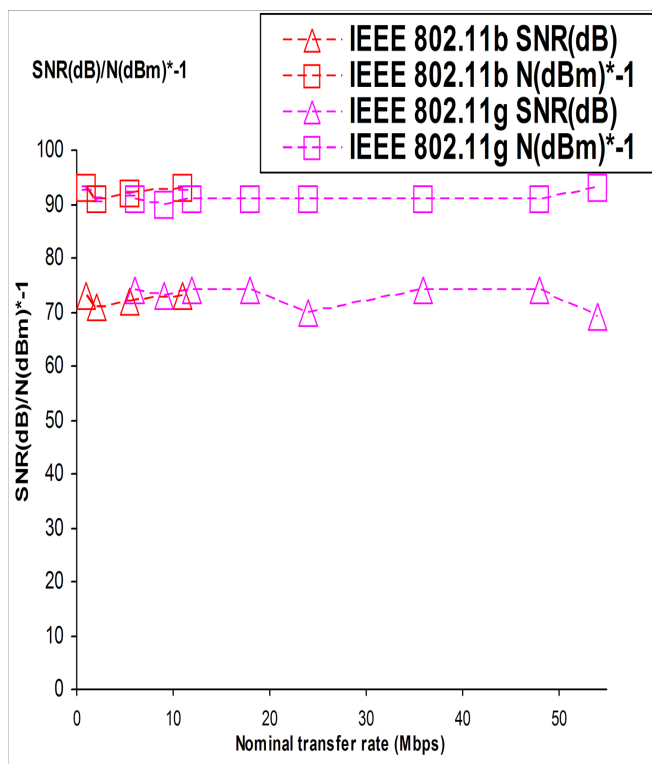
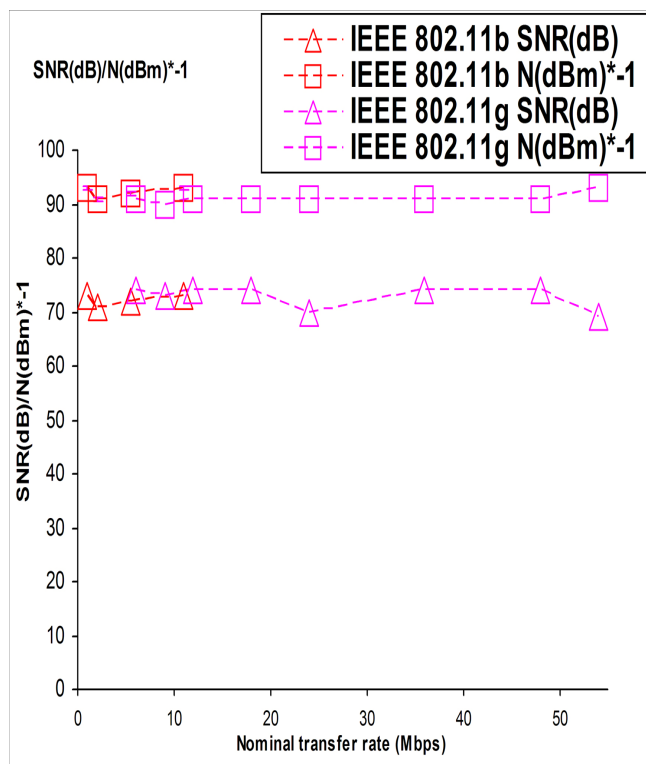Fig. 2- Laboratory setup scheme.

Fig. 4- Typical SNR (dB) and N (dBm); open links.

Fig. 3- Typical SNR (dB) and N (dBm).

TABLE I
AVERAGE WI-FI (IEEE 802.11 B, G) RESULTS; WPA2 AND OPEN LINKS

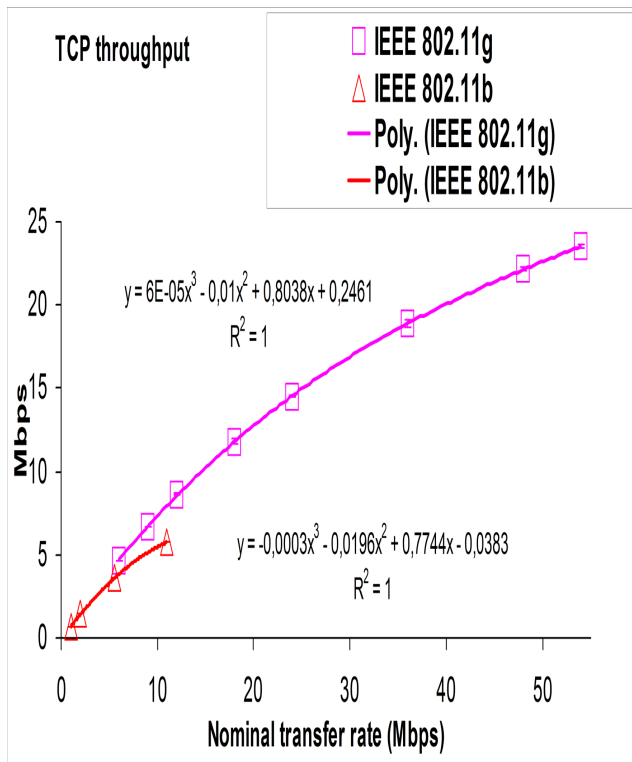| Link type	WPA2		Open	
Parameter/ IEEE standard	802.11b	802.11g	802.11b	802.11g
TCP throughput (Mbps)	2.9 +-0.1	13.9 +-0.4	2.9 +-0.1	13.9 +-0.4
UDP-jitter (ms)	3,6 +-0.2	2.4 +-0.1	2.1 +-0.2	1.2+-0.1
UDP-% datagram loss	1.2 +-0.2	1.3 +-0.1	1.3 +-0.2	1.6 +-0.1
FTP transfer rate (kbyte/s)	349.7 +-10.5	1504.1 +-45.1	342.3 +-10.3	1508.3 +-45.2

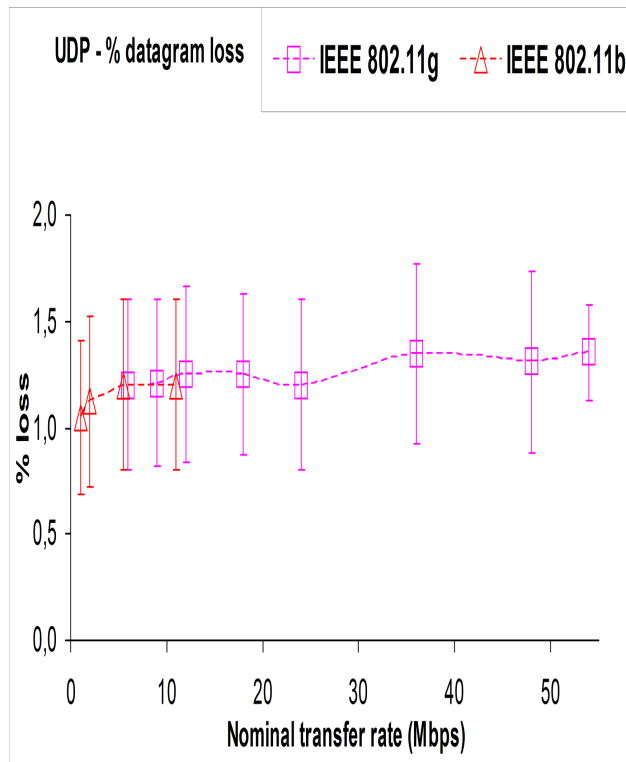Fig. 5- TCP throughput versus technology and nominal transfer rate.

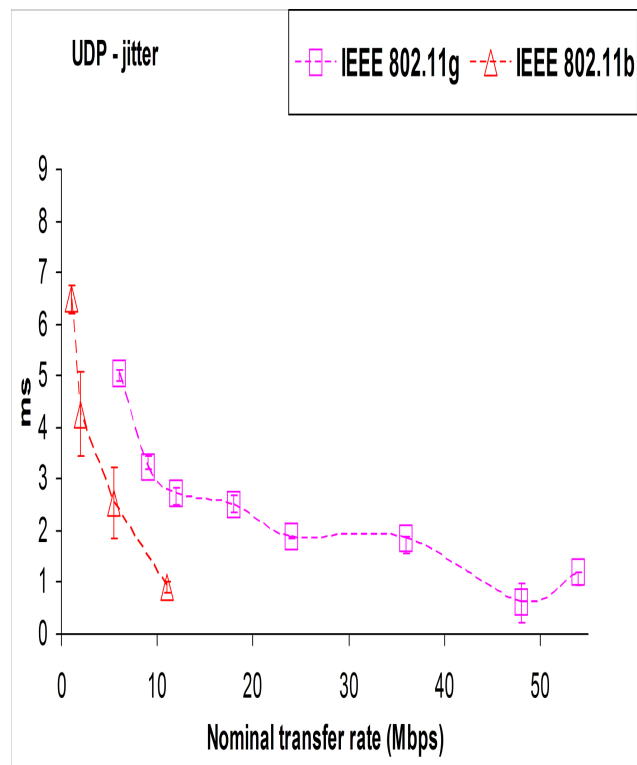Fig. 7- UDP – percentage datagram loss results versus technology and nominal transfer rate.

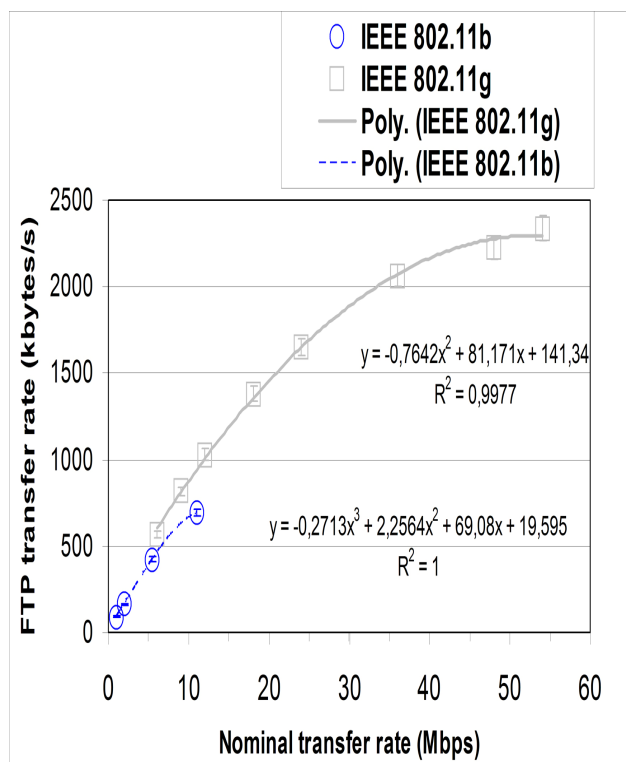Fig. 6- UDP – jitter results versus technology and nominal transfer rate.

Fig. 8- FTP transfer rate versus technology and nominal transfer rate.

IV. CONCLUSION

In the present work a laboratory setup arrangement was planned and implemented, that permitted systematic performance measurements of available wireless equipments (WRT54GL wireless routers from Linksys) for Wi-Fi (IEEE 802.11 b, g) in WPA2 point-to-point links.

Through OSI layer 4, TCP throughput, jitter and percentage datagram loss were measured and compared for each standard. The best TCP throughputs were found for 802.11g. A fairly good agreement was found for the 802.11 b, g data both for WPA2 and open links. Concerning jitter, it was found that on average the best performance was for 802.11 g both for WPA2 and open links. On average, both for 802.11 b and 802.11g, the best jitter performances were found for open links. For percentage datagram loss, no significant sensitivities were found, within the experimental errors, either to standard or link type.

At OSI layer 7, it was found that, for each link type, the best FTP performances are for 802.11g. A fairly good agreement was found for the 802.11 b, g data both for WPA2 and open links. These results show the same trends found for TCP throughput.

Generally, except for jitter, the results measured for WPA2 links were found to agree, within the experimental errors, with corresponding data obtained for open links.

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

REFERENCES

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

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

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

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

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

[6] 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.

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

[8] J. A. R. Pacheco de Carvalho, P. A. J. Gomes, H. Veiga, A. D. Reis, "Development of a University Networking Project", in *Encyclopedia of Networked and Virtual Organizations*, Goran D. Putnik, Maria Manuela Cunha, Eds. Hershey, PA (Pennsylvania): IGI Global, pp. 409-422, 2008.

[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] J. A. R. Pacheco de Carvalho, H. Veiga, N. Marques, C. F. Ribeiro Pacheco, A. D. Reis,"Laboratory Performance of Wi-Fi WEP Point-to-Point Links: a Case Study", *Proc. WCE 2010 - World Congress on Engineering 2010*, pp. 764-767, Imperial College London, London, England, 30 June-2 July 2010.

[11] J. A. R. Pacheco de Carvalho, H. Veiga, N. Marques, C. F. Ribeiro Pacheco, A. D. Reis, "A Contribution to Laboratory Performance Measurements of IEEE 802.11 b,g WEP Point-to-Point Links", *Proc. WINSYS 2010- International Conference on Wireless Information Networks and Systems*, pp. 165-168, Athens, Greece, 26-28 July , 2010.

[12] J. A. R. Pacheco de Carvalho, N. Marques, H. Veiga, C. F. Ribeiro Pacheco, A. D. Reis,"Experimental Performance Evaluation of a Gbps FSO Link: a Case Study", *Proc. WINSYS 2010- International Conference on Wireless Information Networks and Systems*, pp. 123-128, Athens, Greece, 26-28 July , 2010.

[13] Web site http://www.linksys.com; WRT54GL wireless router technical data.

[14] Web site http://www.dd-wrt.com; DD-WRT firmware.

[15] Web site http://www.alliedtelesis.com; AT-8000S/16 level 2 switch technical data.

[16] Web site http://www.netstumbler.com; NetStumbler software.

[17] Web site http://dast.nlanr.net; Iperf software.

[18] Network Working Group, "RFC 1889-RTP: A Transport Protocol for Real Time Applications", http://www.rfc-archive.org