Comparative Performance Studies of Laboratory WEP IEEE 802.11g PTP Links

José A. R. Pacheco de Carvalho[1],

Cláudia F. F. P. Ribeiro Pacheco[2], Hugo Veiga[3], António D. Reis[4]

Abstract – **The importance of wireless communications, involving electronic devices, has been growing. Performance is a very relevant issue, leading to more reliable and efficient communications. Laboratory measurements are made about several performance aspects of Wi-Fi (IEEE 802.11 g) WEP point-to-point links. A contribution is given to performance evaluation of this technology, using available equipments (DAP-1522 access points from D-Link and WPC600N adapters from Linksys). Detailed results are presented and discussed, namely at OSI layers 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.**

Keywords – **Wi-Fi, WLAN, WEP Point-to-Point Links, 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. 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 favourable prices. The importance and utilization of Wi-Fi has been increasing 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 (such as a personal computer, a wireless sensor, a PDA, a smartphone, a video game console, a digital audio player) with a wired based LAN through a switch/router. In this way a WLAN, based on the AP, is formed. Wi-Fi has penetrated the personal home, where a WPAN allows personal devices to communicate. Point-to-point and point-to-multipoint setups are used both indoors and outdoors, requiring specific directional and omnidirectional antennas. Point-to-point and point-to-multipoint links use 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], 802.11b 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 as microwave radio signals travel through the air and can be easily captured. WEP was initially intended to provide confidentiality comparable to that of a traditional wired network. The CRC32 checksum used in WEP does not provide a great protection. In spite of presenting weaknesses, WEP is still widely used in Wi-Fi networks for security reasons, mainly in point-to-point links. A shared key for data encryption is involved. In WEP, the communicating devices use the same key to encrypt and decrypt radio signals. More advanced and reliable security methods have been developed to provide authentication such as, by increasing order of security, WPA and WPA2.

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]. In the present work new Wi-Fi (IEEE 802.11 g) results arise, using WEP encryption, through OSI levels 4 and 7. Performance is evaluated following laboratory measurements of WEP and Open point-to-point links, using the same type of available equipments. Comparisons are made, leading to conclusions about the comparative performance of the links.

[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, E-mail: 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, E-mail: 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, E-mail: 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, E-mail: adreis@ubi.pt.

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 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 g). This was checked through a portable computer, equipped with a Wi-Fi 802.11 a/b/g/n adapter, running NetStumbler software [15]. For WEP encryption, it was activated in the AP and the PC wireless adapter using 128 bit encryption and a shared key composed of 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 Fig. 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 Fig. 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.

III. RESULTS AND DISCUSSION

The access point and the PC wireless network adapter were manually configured, for IEEE 802.11 g, with typical fixed 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 the WEP and Open links at OSI layers 1 (physical layer), 4 (transport layer) and 7 (application layer) using the setup of Fig. 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 Fig. 2. The main average TCP and UDP results are summarized in Table I, both for WEP and Open links..

In Figs. 3-4 polynomial fits were made to the 802.11 g TCP throughput data for WEP and Open links, respectively, where R^2 is the coefficient of determination. A very good agreement was found for the 802.11 g data, within the experimental error, for WEP and Open links. Average values were found of 14.7+-0.4 Mbps and 14.5+-0.4 Mbps for WEP and Open links, respectively. In Figs. 5-6, the data points representing jitter data for 802.11 g for WEP and Open links, respectively, were joined by smoothed lines. It was found that average jitter is slightly higher for WEP (2.6+-0.2 ms) than for Open links (2.3+-0.1 ms), meaning that increasing security leads to a slight degradation of jitter performance. In Fig. 7, percentage datagram loss data for 802.11 g are shown for WEP links. It was found that average percentage datagram loss is slightly higher for WEP (1.6+-0.4 %) than for Open links (1.2+-0.1 %), meaning that increasing security leads to a slight degradation of performance.

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 g as in [10]. The results show the same trends found for TCP throughput.

Generally, except for TCP throughput, it was found that average jitter and percentage datagram loss results show that increased security in WEP links leads to slight degradations in performances compared to Open links.

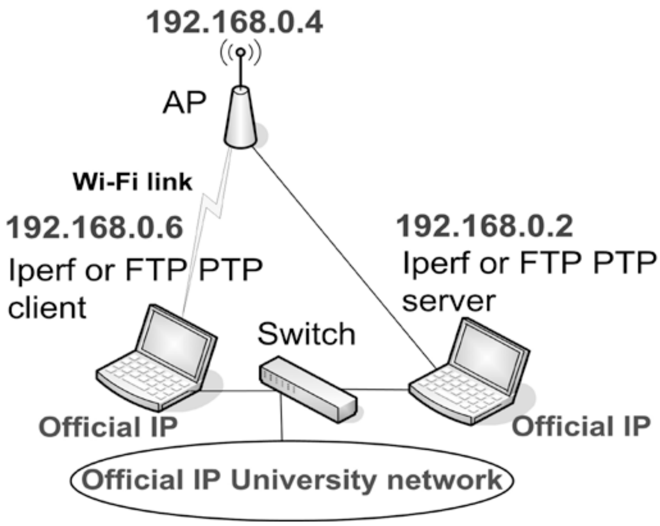

Fig. 1- Laboratory setup scheme.

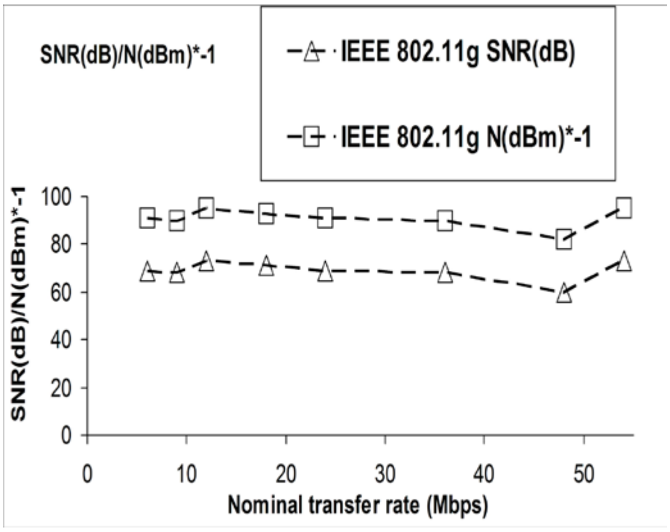

Fig. 2- Typical SNR (dB) and N (dBm).

TABLE I
AVERAGE WI-FI (IEEE 802.11G) RESULTS;
WEP AND OPEN LINKS.

Link Types	**WEP**	**OPEN**
Parameter/ IEEE standard	**802.11g**	**802.11g**
TCP throughput (Mbps)	14.7+-0.4	14.5+-0.4
UDP-jitter (ms)	2.6+-0.2	2.3+-0.1
UDP-% datagram loss	1.6+-0.4	1.2+-0.1

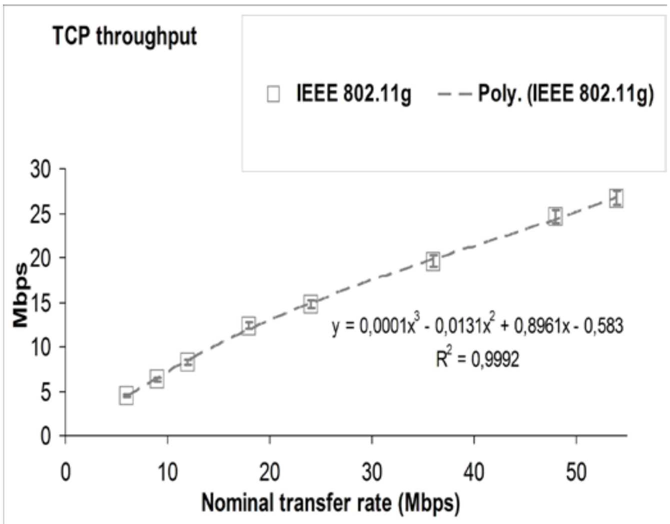

Fig. 3- TCP throughput versus technology and nominal transfer rate; WEP links.

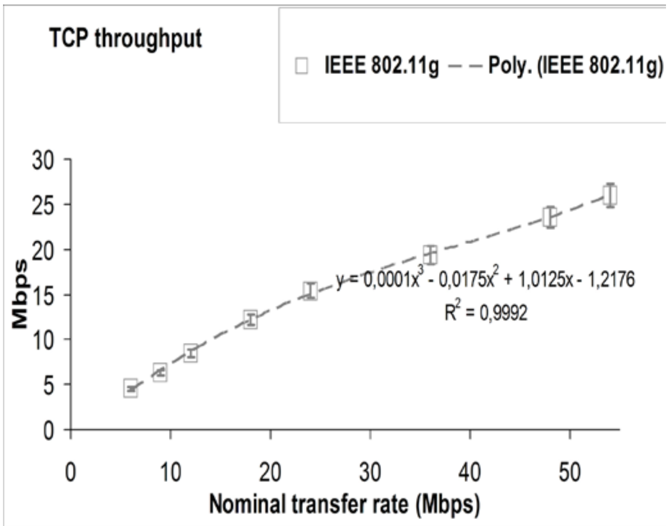

Fig. 4- TCP throughput versus technology and nominal transfer rate; Open links.

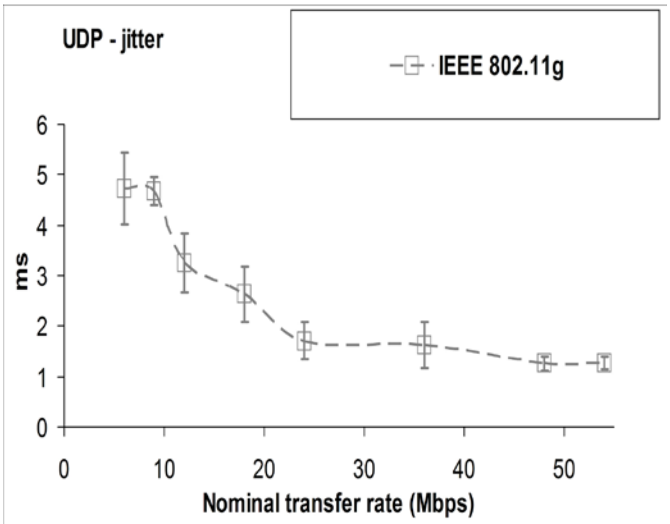

Fig. 5- UDP - jitter results versus technology and nominal transfer rate; WEP links.

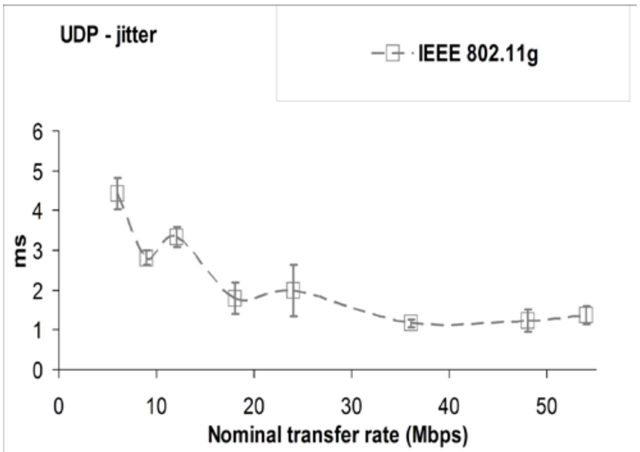

Fig. 6- UDP - jitter results versus technology and nominal transfer rate; Open links.

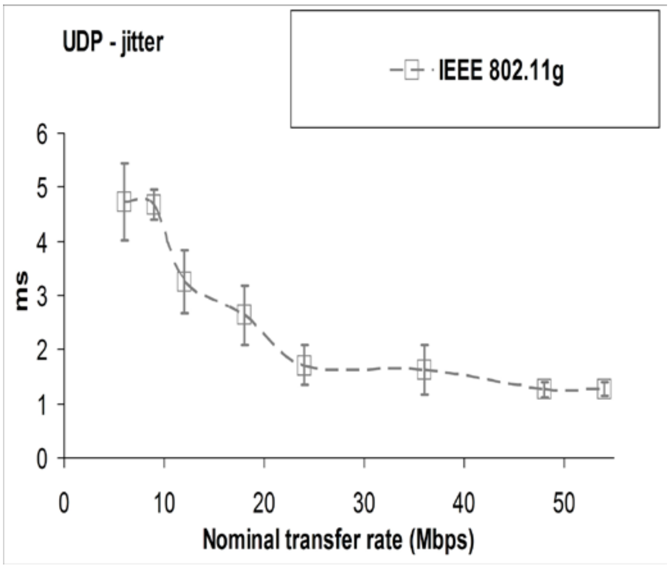

Fig. 7- UDP – percentage datagram loss versus technology and nominal transfer rate; WEP links.

IV. CONCLUSION

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

Through OSI layer 4, TCP throughput, jitter and percentage datagram loss were measured and compared in WEP and Open links. The average TCP throughput 802.11 g data were found to agree fairly well, within the experimental error, for both link types. It was found that average jitter is slightly higher for WEP than for Open links, meaning that increasing security leads to a slight degradation of jitter performance. Concerning average percentage datagram loss is was found to be slightly higher for WEP than for Open links, meaning that increasing security leads to a slight degradation of performance.

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

Generally, except for TCP throughput, it was found that average jitter and percentage datagram loss results show that increased security in WEP links leads to slight degradations in performances compared to Open links.

Additional performance measurements either started or are planned using several equipments, security settings, and topologies, 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/UI0524/2014 (Projecto Estratégico-UI524-2014) are acknowledged.

REFERENCES

[1] Web site http://standards.ieee.org Web site; IEEE 802.11a, 802.11b, 802.11g, 802.11n, 802.11i standards.; accessed 10 Jan 2014.

[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*, 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.

[11] J. A. R. Pacheco de Carvalho, Nuno Marques, H. Veiga, Cláudia F. F. P. Ribeiro Pacheco, A. D. Reis, "Contributions to Experimental Performance Studies of Wi-Fi and FSO Links", Proc. CISTI 2010-5th Iberian Conference on Information Systems and Technologies**,** pp. 221-226, Santiago de Compostela, Spain, 16-19 Junho, 2010

[12] Web site http://www.dlink.com; DAP-1522 wireless bridge/access point technical manual; 2010; accessed 15 Jan 2012.

[13] Web site http://www.alliedtelesis.com; AT-8000S/16 level 2 switch technical data; 2009; accessed 10 Dec 2012.

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

[15] Web site http://www.netstumbler.com; NetStumbler software; 2005; accessed 21 Mar 2011.

[16] Web site http://dast.nlanr.net; Iperf software; 2003; accessed 10 Jan 2008.

[17] Network Working Group. "RFC 1889-RTP: A Transport Protocol for Real Time Applications", http://www.rfc-archive.org; 1996; accessed 10 Feb 2008.