

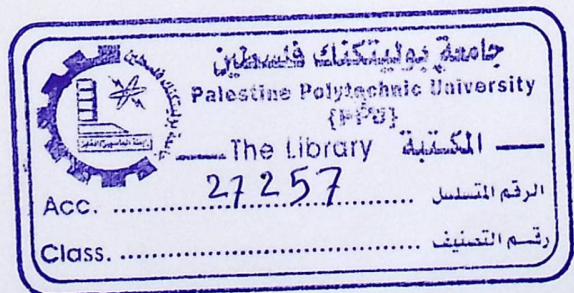


Palestine Polytechnic University
Deanship of Graduate Studies and Scientific Research
Master of Informatics

The Mutual Interference Between Bluetooth And 802.11n MIMO Devices

Submitted By
Mohammad Ayyash

In Partial Fulfillment of the Requirements for the Degree
Master of Informatics
July, 2011



The undersigned hereby certify that they have read and recommend to the Deanship of Graduate Studies and Scientific Research at Palestine Polytechnic University the acceptance of a thesis entitled:

The Mutual Interference Between Bluetooth And 802.11n MIMO Devices

Submitted by **Mohammad I Ayyash**

in partial fulfillment of the requirements for the degree of Master in Informatics

Graduate Advisory Committee:

Committee Chair Name, University:

Dr. Mahmoud Hasan Saheb, Palestine Polytechnic University

Signature: _____

Date: 30/11/2011

Committee Member Name (Supervisor), University:

Dr. Murad Abu Subaih, Palestine Polytechnic University

Signature: _____

Date: 30.11.2011

Committee Member Name, University:

Dr. Radwan Tahboob, Palestine Polytechnic University

Signature: _____

Date: 30/11/2011

External Committee Member Name, University:

Dr. Samer Bali, AL-Quds University

Signature: _____

Date: 30/11/2011

Thesis Approved

Prof. Dr. Karim Tahboub

Dean of Graduate Studies and Scientific Research

Palestine Polytechnic University

Signature: : _____

Date: 4.12.2011

Abstract

The demand for high data rate WLAN becomes very high. Therefore, The IEEE has standardized the 802.11n, which implements multiple input multiple output (MIMO) antennas. The emergence of several radio technologies, such as Bluetooth and IEEE 802.11 WLANs operating on the same 2.4 GHZ unlicensed industrial scientific and medical (ISM) frequency band, may lead to interference and mostly strong degradation in the performance of these technologies, especially when these devices are operating in the same area. Though some studies have addressed the interference between Bluetooth and 802.11 networks, these studies are limited in the sense that they focus on the impact of one technology on the other in specific limited scenarios. Also the studies are limited to the initial versions of 802.11 like the 802.11b/g.

In this thesis we address the mutual impact between the standard 802.11 b/g/n and Bluetooth devices in different scenarios. We quantify the effect of each network on the other. We perform these measurements for all versions of the standard 802.11 for comparison purposes. A special focus is given to the 802.11n standard, which implements multiple antenna system and its physical and medium access control (MAC) layer have been considerably changed. 802.11n promises to provide up to 600Mbps data rate using two 20MHz wide channels (40MHz) rather than a single 20MHz channel as in the case of IEEE 802.11a/b/g. The work is based on measurements from real experimental setup. The results of this work are expected to be very useful for methods that try to enable coexistence of Bluetooth and 802.11n based WLAN, and for the designers who try to make the effect of interference as less as possible, especially the devices which have hardware that supports the standard 802.11n and Bluetooth.

ملخص

لقد تم تصميم البروتوكول الخاص بالشبكات اللاسلكية والعديد من الأجهزة على أن تستخدم نفس الترددات ، حيث أنها تستخدم المدى الرقمي المجاني 2.4 جيجا هيرز ، ومن هذا المنطلق فان جميع الدراسات التي درست ظاهرة تأثير الشبكات اللاسلكية والبلوتوث عندما يعملان في نفس المكان أكدت على أن هناك تأثير واضح لكل نظام على الآخر خاصة عندما يعملان في نفس المنطقه . الا أن جميع هذه الدراسات لم تأخذ بعين الاعتبار النسخ الحديثة من بروتوكول الشبكات اللاسلكية 802.11n بل ركزت على النسخ 802.11b/g .

لذلك ، و بسبب أن بروتوكولات 802.11n تعتمد تعديلات جوهرية في الطبقتين الفيزيائية وربط البيانات ، تركز هذه الدراسة على طبيعة ومستوى تأثير نظامي البلوتوث وشبكات الواي فاي التي تعتمد على 802.11n كل على الآخر. واعتمدت الدراسة على مبدأ البحث التجريبي المتحكم به باستخدام أجهزة حقيقية حديثة . وقد أثبتت نتائج التجارب العلمية وجود تأثير قوي للبلوتوث على شبكة الواي فاي 802.11n ، بينما أثبتت النتائج أن تأثير شبكات الواي فاي على البلوتوث ليس كبيراً.

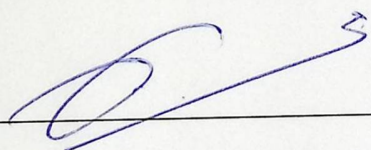
وتعتبر نتائج هذه الدراسة مفيدة للغاية لتصميم آليات وخوارزميات من أجل تقليل التشويش بين نظامي البلوتوث والواي فاي المعتمد على معيار 802.11n وتمكين كلا النظامين من العمل في نفس المكان.

STATEMENT OF PERMISSION TO USE

DECLARATION

I declare that the Master Thesis entitled "*The Mutual Interference between Bluetooth and 802.11n MIMO Devices*" is my own original work, and hereby certify that unless stated, all work contained within this thesis is my own independent research and has not been submitted for the award of any other degree at any institution, except where due acknowledgment is made in the text.

Mohammad Ayyash

Signature: _____ 

Date: 14-12-2011

DEDICATION

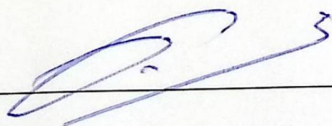
STATEMENT OF PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for the master degree in Informatics at Palestine Polytechnic University, I agree that the library shall make it available to borrowers under rules of the library. Brief quotations from this thesis are allowable without special permission, provided that accurate acknowledgement of the source is made.

Permission for extensive quotation from, reproduction, or publication of this thesis may be granted by my main supervisor, or in his absence, by the Dean of Graduate Studies and Scientific Research when, in the opinion of either, the proposed use of the material is for scholarly purposes. Any copying or use of the material in this thesis for financial gain shall not be allowed without my written permission.

Mohammad Ayyash

Signature: _____



Date: 4-12-2011

ACKNOWLEDGEMENT

DEDICATION

I dedicate this work to my parents and my wife. Without their patience, understanding, there continuous support, and most of all love, the completion of this work would not have been possible during my vital educational years. Also their endless patience and encouragement when it was most required.

I also acknowledge the help of Dr. Muzad Abu Saleh, Dr. Rawan Talib, and Dr. Samir Salim for their support and assistance especially during the revision of my thesis.

The completion of this work would not have been possible without the guidance and the help of several individuals who in one way or another contributed and extended their valuable assistance in the preparation and completion of this study.

ACKNOWLEDGMENT

I wish to thank the members of my committee for their support, patience, and good humor. Their gentle but firm direction has been most appreciated. Dr. Murad Abu Subaih was particularly helpful in guiding me toward a qualitative methodology, whose encouragement, guidance and support from the initial to the final level enabled me to develop an understanding of the subject.

I would like to acknowledge the help of Dr. Murad Abu Subaih, Dr. Radwan Tahboob and Dr. Samer Bali for their support and assistance especially during the evaluation of my thesis.

This dissertation would not have been possible without the guidance and the help of several individuals who in one way or another contributed and extended their valuable assistance in the preparation and completion of this study.

1. ISG	Internet Special Interest Group
2. CRC	Cyclic redundancy check
3. CSMA/CA	Carrier sense multiple access with collision avoidance
4. CTS	Clear to send
5. DCF	Distributed coordination function
6. DIFS	DIFS medium access
7. DSSS	Dual phase shift keying
8. DSP	Digital signal processing
9. FHSS	Fast frequency spread spectrum
10. FCS	Frame check sequence
11. FHSS	Frequency hopping spread spectrum
12. FHSS	Fast frequency hopping spread spectrum

Abbreviations:

	Abbreviation	Full term
1.	ACK	Acknowledgement
2.	ACL	Asynchronous connectionless link
3.	Ad-Hoc	A decentralized of wireless network
4.	Bluetooth	Harald Blatand (King ofe of Denmark.)
5.	BSIG	Bluetooth Special Interest Group
6.	CRC	Cyclic redundancy check
7.	CSMA/CA	Carrier sense multiple access with collision avoidance
8.	CTS	Clear to send
9.	DCF	Distribution coordination function
10.	DIFS	DCF interframe space
11.	DPSK	Dual phase shift keying
12.	DSP	Digital signal processing
13.	DSSS	Direct sequence spread spectrum
14.	FCS	Frame check sequence
15.	FHSS	Frequency hopping spread spectrum
16.	FMSS	fuzzy matrices switching scheme

17.	GFSK	Gaussian Frequency Shift Keying
18.	HEC	Header Error check
19.	IAFH	interference aware frequency hopping
20.	ICMP	Internet control message protocol
21.	IrDA	Infrared data association
22.	ISM	industrial scientific and medical
23.	LAN	Local area network
24.	MAC	Media access layer
25.	MADWIFI	Multiband Atheros Driver for Wi-Fi
26.	Mathlab	Matrix laboratory
27.	MIMO	Multi input multi output
28.	MZ	(Mausezahn) packet generator
29.	NAV	NAV timer
30.	OFDM	Orthogonal frequency division multiplexing
31.	PCF	Point coordination function
32.	PHY	Physical layer
33.	Piconet	A group of Bluetooth devices connected
34.	PIFS	PCF interframe space
35.	PLCP	Physical layer convergence procedure

36.	PLW	PSDU length word
37.	PMD	Physical medium dependent
38.	PSF	PLCP signaling
39.	PSK	Phase shift keying
40.	PS-POLL	Power save Poll
41.	RF	Radio frequency
42.	RSSI	Receive signal strength indicator
43.	RTS	Request to send
44.	SCO	Synchronous connection oriented
45.	SFD	Start of frame
46.	SIFS	Short interframe space
47.	SNIR	signal to noise and interference ratio
48.	SYNC	Synchronization
49.	TCP	Transmission Control Protocol
50.	TDD	Time division duplex
51.	TDM	Time division multiplexing
52.	Tshark	Packet tracker tool
53.	UBUNTU	Operating system depend on Linux
54.	UDP	User datagram protocol

55.	VOIP	Voice over IP
56.	WAN	Wide area network
57.	WEP	wired equivalent privacy
58.	WIFI	Wireless Fidelity
59.	WLAN	Wireless lan
60.	WPAN	Wireless personal area network

Table of Contents

Abstract.....	iii
ملخص.....	iv
DECLARATION.....	v
STATEMENT OF PERMISSION TO USE	vi
DEDICATION	vii
ACKNOWLEDGMENT	viii
Abbreviations:	ix
Table of Contents	xiii
List of Figures:.....	xviii
List of tables	xxi
Chapter 1	1
Overview	1
1.1 Introduction	1
1.2 Related Work	3
1.3 Thesis Objectives.....	4
1.4 Thesis Outline	4
CHAPTER 2	6
Wireless Background	6
2.1 Why wireless?	6
2.2 Wireless versus wired networks.....	7
2.3 Wireless Networks Limitations	7

2.4	Radio Spectrum.....	8
2.5	IEEE 802.11.....	9
2.5.1	802.11 Networks Components	9
2.5.2	WLAN Timing and Modes.....	10
2.5.3	Interframe Spacing	10
2.5.4	Access Methods	11
2.6	Layers of 802.11 Standard	12
2.6.1	Frame Types	12
2.6.2	PHY Frame format :	13
2.6.2.1	Framing in FH (frequency hopping)	13
2.6.2.2	Framing in DS	14
2.6.3	MAC Frame	15
2.6.4	Samples of control frames	18
2.6.4.1	Request to send (RTS).....	18
2.6.4.2	Clear To Send (CTS)	18
2.6.4.3	Acknowledge Frame (ACK)	19
2.6.4.4	Power Save Poll (PS-Poll).....	19
2.7	IEEE 802.11 PHY and MAC Layers:	20
2.7.1	IEEE 802.11 PHY Layer.....	20
2.7.1.1	FH (frequency hopping).....	21
2.7.1.2	DS (direct sequence spread spectrum).....	21
2.7.1.3	Orthogonal Frequency Division Multiplexing (OFDM)	22
2.8	Coding techniques	23

2.9	802.11n Standard.....	23
2.9.1	PHY Enhancements	25
2.9.2	MAC Enhancements	25
2.9.3	Multiple Input Multiple Output (MIMO) concept.....	25
CHAPTER 3		27
Bluetooth (IEEE 802.15.1 standard)		27
3.1	What is Bluetooth?.....	27
3.2	Physical Layer (PHY).....	27
3.2.1	Functions	28
3.2.2	Requirements.....	28
Transmitter characteristics		28
3.2.3	Receiver Characteristics	29
3.3	Medium Access Control (MAC).....	29
3.3.1	Base Band Specifications	29
3.4	Packet Format	30
3.5	Bluetooth Modes	31
3.6	Bluetooth Protocols	32
3.7	Modeling Interference between Bluetooth and WIFI.....	32
Chapter 4.....		35
Devices and Tools		35
4.1	Introduction	35
4.2	Hardware :	35
4.2.1	DWA-643 :	35

4.2.2	DWA-556 :	36
4.2.3	TP-Link-TL-WR941N :	37
4.2.4	Bluetooth device (BT-3620 V2.0):	37
4.3	Software requirements:	38
4.3.1	Linux Operating Systems	38
4.3.2	The Drivers for Wireless Network Interface Cards:	38
4.3.2.1	Multiband Atheros Driver for Wireless Fidelity (MadWifi)	38
4.3.3	Wireless Tools:	39
4.3.4	TShark :	39
4.3.5	MZ (Mausezahn) packet generator :	40
4.3.6	BLUETOOTH MANAGER (Blue Soleil) :	40
CHAPTER 5		41
Results		41
5.1	Experimental Setup	41
5.2	Effect of Bluetooth on 802.11	41
5.2.1	Scenario 1 (802.11b network)	41
5.2.1.1	Throughput of (802.11b)	41
5.2.1.2	Loss of (802.11b)	43
5.2.2	Scenario 2 (802.11g network)	44
5.2.2.1	Throughput (802.11g)	44
5.2.2.2	Loss (802.11g)	45
5.2.3	Scenario 3 (802.11n network)	46
5.2.3.1	Throughput (802.11n)	46

5.2.3.2	Loss (802.11n).....	48
5.2.4	802.11 Standard and Loss of Frames	49
5.2.4.1	802.11 Standards Throughput.....	49
5.2.4.2	802.11 Standard Loss Of Frames.....	50
5.3	Effect Of 802.11 On Bluetooth	51
5.3.1	Bluetooth Throughput With Interference (802.11)	51
5.3.2	Bluetooth Loss With Interference (802.11).....	53
5.4	Summary of Results.....	54
CHAPTER 6	56
CONCLUSION And Future Work	56
References:	57
Appendices	58
Appendix A : Upuntu commands	58
Appendix B : Paper	61

List of Figures:

Figure	page
Figure 1.1: 802.11 and Bluetooth networks.....	1
Figure 2.1: Unlicensed radio spectrum.....	8
Figure 2.2: Wireless components.....	10
Figure 2.3: types of interframe space.....	11
Figure 2.4: Basic access method.....	11
Figure 2.5: RTS/CTS access method.....	12
Figure 2.6: Frame structure.....	13
Figure 2.7: FH PHY.....	14
Figure 2.8: DS PHY frame.....	14
Figure 2.9: MAC frame format.....	15
Figure 2.10: Frame control field	15
Figure 2.11: RTS frame.....	18
Figure 2.12: CTS frame.....	19
Figure 2.13: ACK frame.....	19
Figure 2.14: PS-POLL frame.....	20
Figure 2.15: IEEE 802.11 MAC and PHY.....	20

Figure 2.16:	Frequency hopping concept.....	21
Figure 2.17:	MIMO concept.....	26
Figure 3.1:	Bluetooth devices.....	27
Figure 3.2:	Unlicensed Radio Spectrum.....	28
Figure 3.3:	Bluetooth Channels.....	30
Figure 3.4:	Bluetooth packet format.....	31
Figure 4.1:	802.11 standard devices (clients, access point).....	35
Figure 4.2:	DWA-643 wireless adapter.....	36
Figure 4.3:	DWA-556 wireless adapter.....	36
Figure 4.4:	TP-Link-TL-WR941N.....	37
Figure 4.5:	BT-3620 V2.0 BT device.....	38
Figure 4.6:	Bluetooth manager (Bluesoleil).....	40
Figure 5.1:	802.11b with Bluetooth.....	42
Figure 5.2:	802.11b Throughput.....	43
Figure 5.3:	802.11b Loss of frames.....	44
Figure 5.4:	802.11g with Bluetooth.....	44
Figure 5.5:	802.11g Throughput.....	45
Figure 5.6:	Loss of frames in 802.11g.....	46
Figure 5.7:	802.11n with throughput.....	47
Figure 5.8:	802.11n Throughput.....	47
Figure 5.9:	802.11n Loss of frames.....	48
Figure 5.10:	802.11 standard Throughput.....	50
Figure 5.11:	802.11n Loss of frames	51

Figure 5.12:	Bluetooth scenario with 802.11 interference (802.11).....	52
Figure 5.13:	Bluetooth Throughput with interference.....	53
Figure 5.14:	Bluetooth Loss with interference.....	54

List of tables

Table	page
Table 2.1: Common frequency bands.....	9
Table 2.2: Frame types.....	16
Table 2.3: ISM band channels.....	22
Table 2.4: IEEE 802.11 standard.....	22
Table 3.1: Bluetooth frequencies.....	28
Table 3.2: Bluetooth power classes.....	29
Table 5.1: IEEE802.11b Throughput and Loss of frames.....	42
Table 5.2: IEEE802.11g Throughput and Loss of frames.....	45
Table 5.3: IEEE802.11n Throughput and Loss of frames.....	47
Table 5.4: IEEE802.11 standard throughput.....	49
Table 5.5: IEEE802.11 Loss of frames.....	50
Table 5.6: Bluetooth throughput with interference.....	52
Table 5.7: Bluetooth Loss with interference.....	53

Chapter 1

Overview

1.1 Introduction

The past several years have been exciting for wireless communication. Wireless access becomes one of the life basics. Therefore, we can see different wireless devices almost in all houses and offices. Bluetooth service becomes one of the most important features of mobiles and laptops. It is known that most of personal networks including Bluetooth and 802.11 WLANs operate within the industrial scientific and medical (ISM) band (2.4 GHz). When Bluetooth coexist with IEEE 802.11, interference becomes a crucial issue as shown in Figure 1.1. IEEE 802.11 and Bluetooth devices will mutually interfere. Interference will degrade the performance of these devices. In this thesis, it is aimed at studying the mutual impact between Bluetooth and the new emerging WLAN MIMO devices based on the recently approved 802.11n standard. The motivation of the study comes from the fact that these devices implement significantly different physical and MAC layers. [8,7,2]

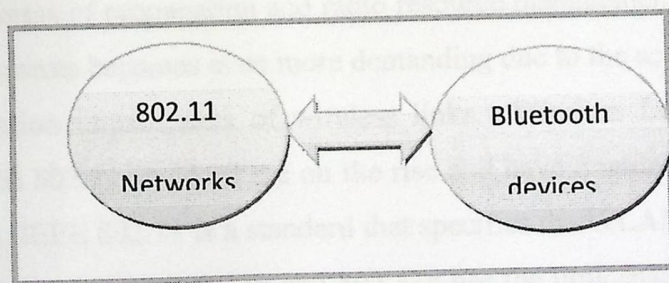


Figure 1.1: 802.11 and Bluetooth networks.

One of the most challenges for the Wireless technologies is the frequency spectrum. Each wireless technology needs a range of frequency to use in order to avoid interference with other wireless networks. Therefore, the spectrum becomes more crowded in these days. At the same time, manufacturers continue to design new technologies which need new frequency reservations. Thus, we see several technologies are working on the same frequency bands.

. In this work, we will focus on Bluetooth and 802.11 networks which operate on the same ISM band.

The IEEE802.11b/g divides the 83.5 MHz into 20 MHz wide channels. Channels are separated by 5 MHz. In this case, the 2.4 GHz band can support up to three non overlapping channels. Channels one, six and eleven are popular in WI-FI legacy network networks. The new version of IEEE802.11n optionally uses two channels 40MHz instead of 20MHz. This is called channel bonding. That will allow the data rates up to 600 Mbps. Theoretically, this increases the probability to have interference with any other technology working in the same frequency band, especially when networks operate in the same area.[1]

The IEEE802.15.1 (Bluetooth) divides the 83.5 MHz into 79 channels 1 MHz wide. It uses the frequency hopping technique to avoid interference as well as for security reasons. Because these channels are shared with the IEEE802.11 channels, Bluetooth and 802.11 networks are likely to interfere.[1,2]

During the last decade, wireless local and personal area networks are widely deployed. The rapid proliferation of wireless networks has posed fundamental challenges to the design of wireless networks. The next generation of wireless networks promise to provide high speed wireless access through more advanced physical and MAC technologies. They are expected to support a variety of high quality applications. At the same time, several challenges are imposed by the wireless environment, in terms of propagation and radio resource management. Furthermore, efficient design of network components becomes even more demanding due to the scarcity of radio spectrum and the inherent transmission impairments of wireless links. Wireless Local Area Networks (WLANs) based on the IEEE 802.11 standard are on the rise and have a wide implementation both in private and public places. IEEE 802.11 is a standard that specifies the WLAN communication in the 2.4, 3.6 and 5 GHz frequency bands. 802.11b and 802.11g use the unlicensed 2.4 GHz Industrial Scientific and Medical (ISM) band. Hence, the devices may be interfered by signals from Bluetooth, microwave ovens, and cordless telephone devices. Spread spectrum techniques are used in both Bluetooth and 802.11 equipments to control their susceptibility to interference. While 802.11b implements Direct Sequence Spread Spectrum (DSSS), 802.11g uses Orthogonal Frequency Division Multiplexing (OFDM). On the other hand, Bluetooth uses a Frequency Hopping Spread Spectrum (FHSS) signaling technique. Though some studies have addressed the interference between Bluetooth and 802.11 networks, these studies are limited in the sense that they focus on the impact of one technology on the other in specific limited scenarios. Also, the studies are limited to the initial versions of 802.11 like the 802.11a/b/g.[1,10,12]

The IEEE802.11b/g divides the 83.5 MHz into 20 MHz wide channels. Channels are separated by 5 MHz. In this case, the 2.4 GHz band can support up to three non overlapping channels. Channels one, six and eleven are popular in WI-FI legacy network networks. The new version of IEEE802.11n optionally uses two channels 40MHz instead of 20MHz. This is called channel bonding. That will allow the data rates up to 600 Mbps. Theoretically, this increases the probability to have interference with any other technology working in the same frequency band, especially when networks operate in the same area.[1]

The IEEE802.15.1 (Bluetooth) divides the 83.5 MHz into 79 channels 1 MHz wide. It uses the frequency hopping technique to avoid interference as well as for security reasons. Because these channels are shared with the IEEE802.11 channels, Bluetooth and 802.11 networks are likely to interfere.[1,2]

During the last decade, wireless local and personal area networks are widely deployed. The rapid proliferation of wireless networks has posed fundamental challenges to the design of wireless networks. The next generation of wireless networks promise to provide high speed wireless access through more advanced physical and MAC technologies. They are expected to support a variety of high quality applications. At the same time, several challenges are imposed by the wireless environment, in terms of propagation and radio resource management. Furthermore, efficient design of network components becomes even more demanding due to the scarcity of radio spectrum and the inherent transmission impairments of wireless links. Wireless Local Area Networks (WLANs) based on the IEEE 802.11 standard are on the rise and have a wide implementation both in private and public places. IEEE 802.11 is a standard that specifies the WLAN communication in the 2.4, 3.6 and 5 GHz frequency bands. 802.11b and 802.11g use the unlicensed 2.4 GHz Industrial Scientific and Medical (ISM) band. Hence, the devices may be interfered by signals from Bluetooth, microwave ovens, and cordless telephone devices. Spread spectrum techniques are used in both Bluetooth and 802.11 equipments to control their susceptibility to interference. While 802.11b implements Direct Sequence Spread Spectrum (DSSS), 802.11g uses Orthogonal Frequency Division Multiplexing (OFDM). On the other hand, Bluetooth uses a Frequency Hopping Spread Spectrum (FHSS) signaling technique. Though some studies have addressed the interference between Bluetooth and 802.11 networks, these studies are limited in the sense that they focus on the impact of one technology on the other in specific limited scenarios. Also, the studies are limited to the initial versions of 802.11 like the 802.11a/b/g.[1,10,12]

The aim of this thesis is to study and analyze the mutual impact of 802.11n and Bluetooth devices through empirical controlled experiments. Though the thesis focuses on 802.11n WLAN devices, other technologies such as 802.11b/g are also considered. The results are expected to be useful for methods that try to enable coexistence of Bluetooth and 802.11n based WLANs.

1.2 Related Work

The mutual impact of Bluetooth and 802.11 WLAN has attracted several research groups during the last decade.

The paper of [8] derived a mathematical model for evaluating the impact of Bluetooth on IEEE802.11. The approach is illustrated by examining coexistence between IEEE802.11 and Bluetooth within typical operational ranges, for both technologies regarding traffic and RF environment. In [7], the authors presented empirical results based on controlled experiments to measure the effects of interference between IEEE 802.11b and Bluetooth considering both co-channel and adjacent channel interference. In [2], the authors used simulation experiments to measure the interference between Bluetooth and IEEE 802.11 WLANs. A comparison between low and high mobility WLAN nodes shows that Bluetooth devices are strongly impacted by high mobile WLAN nodes than slow mobile ones. The paper of [1] evaluates the mutual interference between Wi-Fi and Bluetooth networks. Two different coexistence mechanisms based on traffic scheduling techniques were proposed to reduce interference effects. In [10], the authors studied the mutual effect between the Bluetooth and the 802.11 technologies. They carried out empirical experiment for different payloads. Experimental results demonstrated that a significant degradation in performance when Bluetooth communications co-exist with 802.11 WLANs for a selected set of applications. The authors also did not observe performance degradation on 802.11 wireless transmissions in the presence of interfering Bluetooth traffic. The authors of [12] study the interference between the Bluetooth and IEEE.11b systems through simulations. They concluded that power control may have limited benefits in this environment. They found that using a slower hop rate for Bluetooth may cause less interference to WLAN. Voice transmission using Bluetooth presents the worst type of interference to WLAN. In [13], the authors address WI-FI and Bluetooth coexistence through empirical experiments. They introduced a TDM-based coexistence solution and showed that no

simultaneous operation of Bluetooth and WLAN can be guaranteed when the two technologies are integrated into the same device. The authors of [9] tried to mitigate the interference between IEEE 802.11 WLAN and Bluetooth through diversity techniques. In [6], the authors proposed a new non-collaborative mechanism to prevent WLAN from interfering with Bluetooth with minor modification in the 802.11 and Bluetooth standards. Authors of [3] study the performance of 802.11b networks in the presence of interference-aware Bluetooth devices through simulation. They concluded that with interference aware frequency hopping, the throughput of the 802.11b networks is improved while the probability of collision and the packet error rate are decreased significantly. The paper of [15] evaluates the behavior of IEEE 802.11 networks in the presence of Bluetooth networks. The paper published in [11] evaluates the interference between Bluetooth and IEEE 802.11 networks. The authors concluded that the interference increases as the number of nodes increases. The most recent related work is the work published in [14]. The authors studied the impact of IEEE 802.11n operation on IEEE.15.4 devices. They concluded that the overlap in the IEEE 802.11n control channel causes severe deterioration in both loss rate and the packet latency for IEEE 802.15.4 traffic. In this work, we contribute to the previous work by providing results of empirical experiments that characterizes the mutual interference impact between Bluetooth and the new high throughput 802.11n MIMO devices. The motivation of the work stems from the fact that these devices implements significantly different techniques both at the MAC and PHY layers. In this thesis, we will study the mutual interference effect between 802.11 and Bluetooth networks. A special focus is given to the new emerging devices 802.11n which use MIMO technologies and implement different physical and MAC layers. The motivation for this study comes from the fact that 802.11n technologies promises to provide high data rates and expected to replace existing legacy devices based on 802.11b/g standards.

1.3 Thesis Objectives

In this thesis, we plan to have the following answers.

1. The effect of 802.11 networks on the Bluetooth.
2. The effect of the Bluetooth on 802.11 networks.

1.4 Thesis Outline

The rest of this thesis is organized as follows:

- Chapter 2 talks about the wireless concept. A comparison between the wireless technology and wired technology, the wireless limitations, radio spectrum in general. IEEE 802.11 standard concepts, wireless timing modes, interframe spacing, layers for 802.11 standards. In another word in this chapter a theoretical direction of the wireless networks were explained.
- Chapter 3 presents historical and theoretical information about the Bluetooth devices, physical and MAC layers, transmitter and receiver characteristics, the Bluetooth packet format and the Bluetooth modes.
- Chapter 4 discusses the tools used in the experiments (hardware and software). Brief explanation on these tools is presented.
- Chapter 5 presents and analyzes the experimental results.
- Chapter 6 concludes this thesis and presents ideas for future work.

CHAPTER 2

Wireless Background

2.1 Why wireless?

Over the past five years, the world has become increasingly mobile. As a result, traditional ways of networking the world have proven inadequate to meet the challenges posed by our new collective lifestyle. If users must be connected to a network by physical cables, their movement is dramatically reduced. Wireless connectivity, however, poses no such restriction and allows a great deal more free movement on the part of the network user.

The most obvious advantage of wireless networking is mobility. Wireless network users can connect to existing networks and are then allowed to roam freely. A mobile telephone user can drive miles in the course of a single conversation because the phone connects the user through cell towers. Initially, mobile telephony was expensive. Costs restricted its use to highly mobile professionals such as sales managers and important executive decision makers who might need to be reached at a moment's notice regardless of their location. Mobile telephony has proven to be a useful service. Likewise, wireless data networks free software developers from the tethers of an Ethernet cable at a desk.

Developers can work in the library, in a conference room, in the parking lot, or even in the coffee house across the street. As long as the wireless users remain within the range of the base station, they can take advantage of the network. Commonly available equipment can easily cover a corporate campus, with some work, more exotic equipment, and favorable terrain, we can extend the range of an 802.11 network up to a few miles.

Wireless networks typically have a great deal of flexibility, which can translate into rapid deployment. Wireless networks use a number of base stations to connect users to an existing network. The infrastructure side of a wireless network, however, is qualitatively the same whether you are connecting one user or a million of users, to offer service in a given area, you need base

stations and antennas in place. Once that infrastructure is built, however, adding a user to a wireless network is mostly a matter of authorization. With the infrastructure built, it must be configured to recognize and offer services to the new users, but authorization does not require more infrastructures, adding a user to a wireless network is a matter of configuring the infrastructure, but it does not involve running cables, punching down terminals, and patching in a new jack, like in wired networks as (telephony networks) .

2.2 Wireless versus wired networks

There are many differences between wireless and wired networks regarding the environment. As an example, if a frame needs to be transmitted in an Ethernet network, it is reasonable to assume that the destination will receive it correctly. But, in radio links, especially when the frequencies are unlicensed (ISM band), it is must to assume that interference will exist. Therefore, the designers of 802.11 considered ways to work around the radiation from different sources like microwave ovens and other RF sources.

2.3 Wireless Networks Limitations

Wireless mobile networks do not replace fixed networks. The main advantage of mobility is that the network user is moving. Servers and other data center equipment must access data. But, the physical location of the server is irrelevant. As long as the servers do not move, they may as well be connected to wires that do not move.

The speed of wireless networks is constrained by the available bandwidth. Information theory can be used to deduce the upper limit on the speed of a network. Unless the regulatory authorities are willing to make the unlicensed spectrum bands bigger, there is an upper limit on the speed of wireless networks. Wireless network hardware tends to be slower than wired hardware. Unlike the 10-GB Ethernet standard, wireless-network standards must carefully validate received frames to guard against loss due to the unreliability of the wireless medium.

Radio waves can suffer from a number of propagation problems that may interrupt the radio link, such as multipath interference and shadows. Security on any network is a prime concern, on wireless networks, it is often a critical concern because the network transmissions are available to anyone

stations and antennas in place. Once that infrastructure is built, however, adding a user to a wireless network is mostly a matter of authorization. With the infrastructure built, it must be configured to recognize and offer services to the new users, but authorization does not require more infrastructures, adding a user to a wireless network is a matter of configuring the infrastructure, but it does not involve running cables, punching down terminals, and patching in a new jack, like in wired networks as (telephony networks) .

2.2 Wireless versus wired networks

There are many differences between wireless and wired networks regarding the environment. As an example, if a frame needs to be transmitted in an Ethernet network, it is reasonable to assume that the destination will receive it correctly. But, in radio links, especially when the frequencies are unlicensed (ISM band), it is must to assume that interference will exist. Therefore, the designers of 802.11 considered ways to work around the radiation from different sources like microwave ovens and other RF sources.

2.3 Wireless Networks Limitations

Wireless mobile networks do not replace fixed networks. The main advantage of mobility is that the network user is moving. Servers and other data center equipment must access data. But, the physical location of the server is irrelevant. As long as the servers do not move, they may as well be connected to wires that do not move.

The speed of wireless networks is constrained by the available bandwidth. Information theory can be used to deduce the upper limit on the speed of a network. Unless the regulatory authorities are willing to make the unlicensed spectrum bands bigger, there is an upper limit on the speed of wireless networks. Wireless network hardware tends to be slower than wired hardware. Unlike the 10-GB Ethernet standard, wireless-network standards must carefully validate received frames to guard against loss due to the unreliability of the wireless medium.

Radio waves can suffer from a number of propagation problems that may interrupt the radio link, such as multipath interference and shadows. Security on any network is a prime concern, on wireless networks, it is often a critical concern because the network transmissions are available to anyone

within range of the transmitter with the appropriate antenna. On a wired network, the signals stay in the wires and can be protected by strong physical-access control (locks on the doors of wiring closets, and so on). On a wireless network, sniffing is much easier because the radio transmissions are designed to be processed by any receiver within range.

2.4 Radio Spectrum

Wireless devices are constrained to operate in a certain frequency band. Each band has an associated bandwidth, which is simply the amount of frequency space in the band. Bandwidth has acquired a connotation of being a measure of the data capacity of a link. A great deal of mathematics, information theory, and signal processing can be used to show that higher bandwidth slices can be used to transmit more information. As an example, an analog mobile telephony channel requires a 20-kHz bandwidth, TV signals are vastly more complex and have a correspondingly larger bandwidth of 6 MHz. Figure 2.1 shows this spectrum.

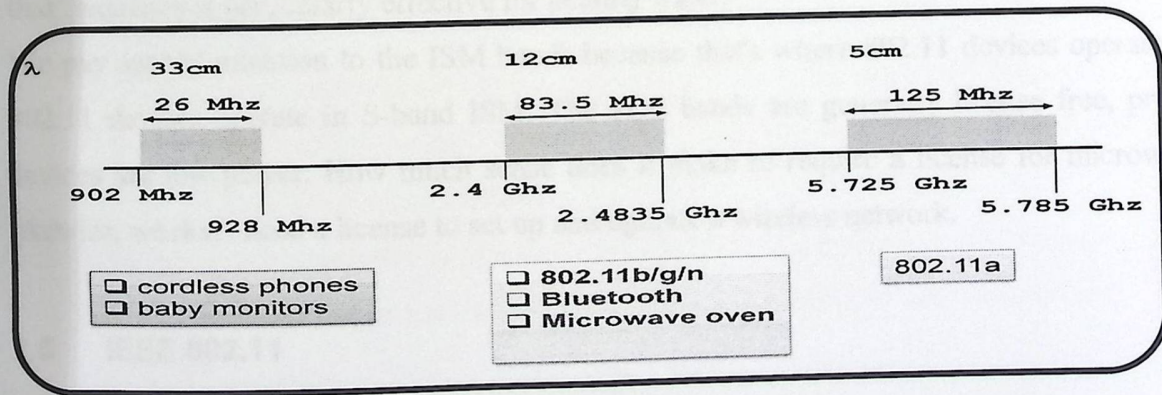


Figure 2.1 : Unlicensed radio spectrum.

The following table lists some common frequency bands used in the world.

Table 2.1 : common frequency bands.

Band	Frequency Range
UHF ISM	902-928 MHz
S-Band	2-4 GHz
S-Band ISM	2.4-2.5 GHz
C-Band 4-8 GHz	4-8 GHz
C-Band satellite downlink	3.7-4.2 GHz
C-Band Radar (weather)	5.25-5.925 GHz
C-Band satellite uplink	5.925-6.425 GHz
X-Band Radar (police/weather)	8.5-10.55 GHz
Ku-Band	12-18 GHz
C-Band ISM	5.725-5.875 GHz

In table 2.1, there are three bands labeled ISM, which is an abbreviation for industrial, scientific, and medical. ISM bands are set aside for equipment that, broadly speaking, is related to industrial or scientific processes or is used by medical equipments. Perhaps the most familiar ISM-band device is the microwave oven, which operates in the 2.4-GHz ISM band because electromagnetic radiation at that frequency is particularly effective for heating water.

We pay special attention to the ISM bands because that's where 802.11 devices operate. Common 802.11 devices operate in S-band ISM. The ISM bands are generally license free, provided that devices are low-power. How much sense does it make to require a license for microwave ovens, likewise, we don't need a license to set up and operate a wireless network.

2.5 IEEE 802.11

2.5.1 802.11 Networks Components

The following items construct the wireless networks as shown in figure 2.2

1. Distribution system: It is the backbone network used to relay frames between access points, it is often called simply the backbone network.

2. Access points: Frames on an 802.11 network must be converted to another type of frame for delivery to the rest of the world. Devices called access points perform the wireless-to-wired bridging function. Also APs are used to provide users wireless connectivity in infrastructure mode.
3. Wireless medium: It is the wireless medium used to move frames from station to station though the RF layers have proven far more popular.
4. Stations: networks are made to transfer data between stations.

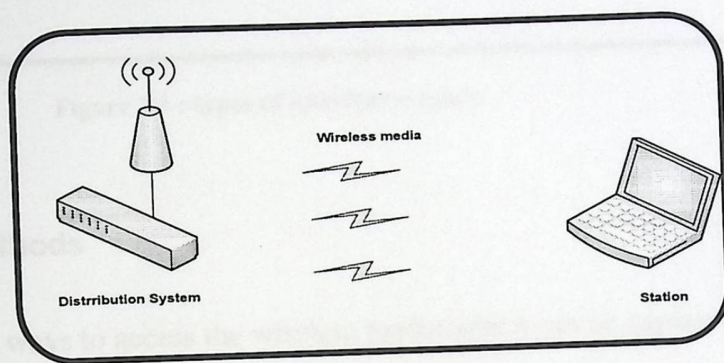


Figure 2.2: Wireless components.

2.5.2 WLAN Timing and Modes

- Distribution coordination function (DCF): it is the basic of CSMA/CA. It first checks the media if it is clear before sending data, to avoid collisions; the DCF may use the CTS/RTS clearing technique.
- Point coordination function (PCF): it is used for special stations called point coordinators to ensure that the medium is provided without contention.

2.5.3 Interframe Spacing

802.11 MAC layer uses three different interframe spaces as shown in Figure 2.3

1. Short interframe space (SIFS): it is used for high priority transmissions such as CTS/RTS frames.
2. PCF interframe space (PIFS): it is also called the priority interframe space, and it is used by the PCF during contention free operations.

3. DCF interframe space (DIFS): it is the minimum medium idle time for contention based services; stations may have immediate access to the medium if it is free for period longer than DIFS.

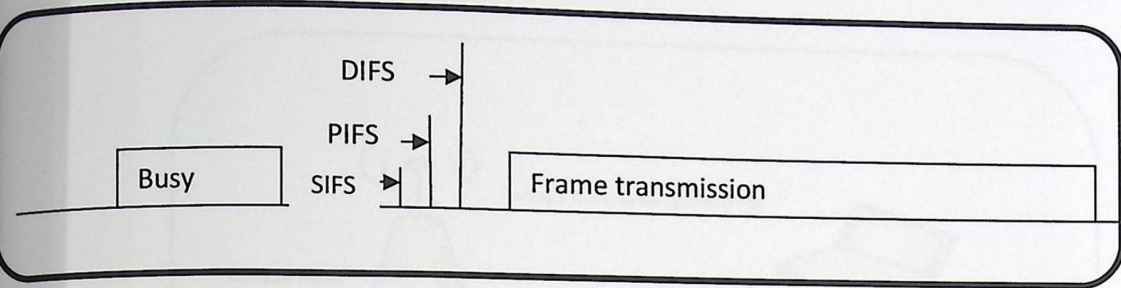


Figure 2.3 : types of interframe space.

2.5.4 Access Methods

There are more than ways to access the wireless media which can be explained as follows

➤ Basic method: This method depends only on data and acknowledgement frames. The scenario starts when a station wants to send data, it senses the medium first, if it is idle it waits for a period of time called DIFS, after this time if the medium still idle the station starts to send data, while the data is sent, if any other station want to send data, it will find the NAV timer not equal to zero. It can compute the approximate time for the medium to be busy from the data frame itself. When the ACK for the sent data is received the medium becomes free and can be used by any other station depending on the same scenario. The following flow chart explains this scenario.

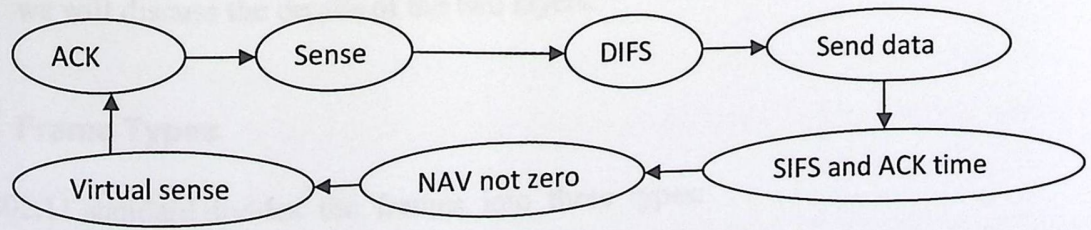


Figure 2.4 : basic access method.

➤ RTS/CTS method: In this method, RTS, CTS, Data, ACK frames are used to get the wireless media the scenario starts when a BS needs to send data on the wireless media, it

sends an (RTS) frame to the destination address. The destination node sends a (CTS) frame after that the station starts to send the data frames and wait for the ACK frames, the following figure explain this method.

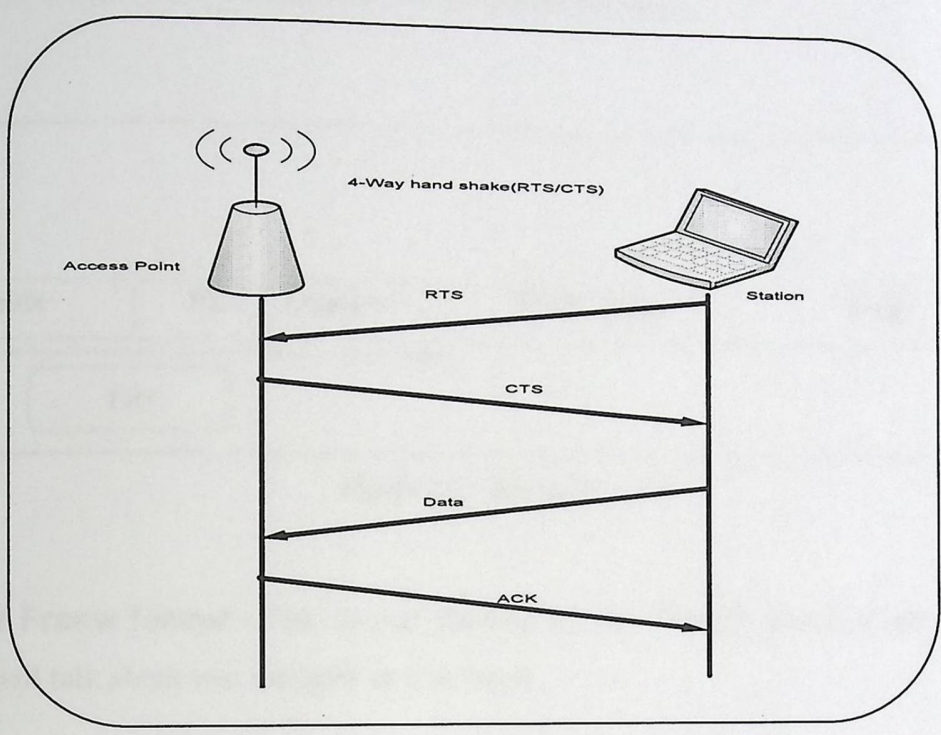


Figure 2.5: RTS/CTS access method.

2.6 Layers of 802.11 Standard

In this thesis, we mainly concentrate on the MAC and PHY layers of the WLAN 802.11. So, we will discuss the details of the two layers:

2.6.1 Frame Types

The 802.11 standard divides the frames into three types:

1. Management frames : These frames are sent on the same media but they will not be forwarded to upper layers.

2. Control frames : These frames are responsible for the medium access layer. Examples are the RTS/CTS.
3. Data frames : Which are the frames that carry data.

In general, the frame of 802.11 standard has the following shape:

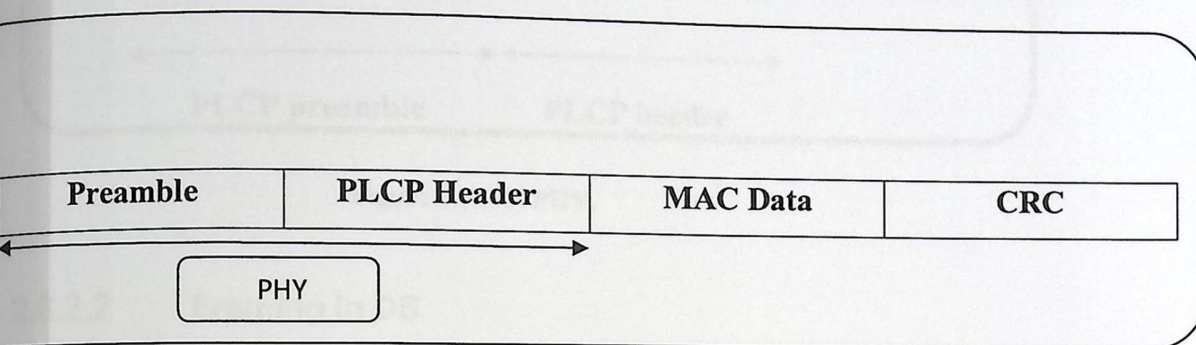


Figure 2.6 : Frame structure.

2.6.2 PHY Frame format : The format depends on the way the physical layer is implemented, we will talk about two methods in this thesis

2.6.2.1 Framing in FH (frequency hopping)

The FH PHY adds a five-field header to the frame received from the MAC, as shown in figure 2.4

- Sync: it is 80 bit alternating ones and zeroes (010101,...). Any station sees this sync pattern starts to receive data.
- SFD: start of frame which is a 16 bit that indicates to the beginning of the frame The FH PHY uses a 16-bit SFD: 0000 1100 1011 1101.
- PLW (PSDU length word): It is a 12 bits field indicates to the length of the MAC frame.
- PSF (PLCP signaling): it is a 4 bits field that indicates to the speed at which the payload MAC frame is transmitted.
- HEC (Header Error check): It is a 16 bits field calculated by the sender and checked by the receiver.

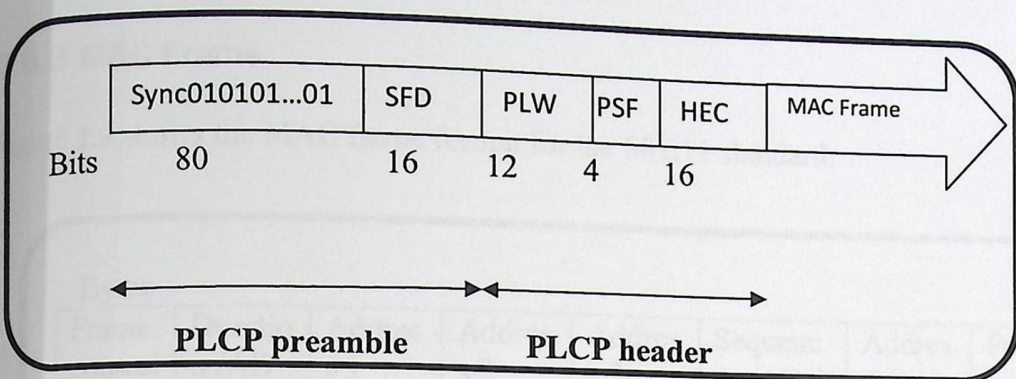


Figure 2.7: FH PHY.

2.6.2.2 Framing in DS

The DS PHY adds six-field header to the frame received from the MAC, as shown in figure 2.5

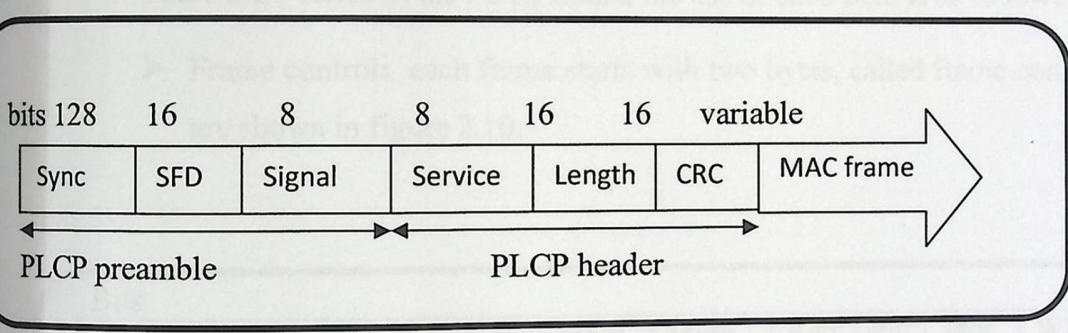


Figure 2.8: DS PHY frame.

- Sync: it is 128 bit field consists of ones.
- SFD: start of frame which is a 16 bits field that indicates to the beginning of the frame: 0000 0101 1100 1111.
- Signal: It is an eight bits field that indicates to the transmission rate of the MAC frame.
- Service: It is an eight bits field that reserved for future.
- Length: It is a 16 bits field that indicates to the number of microseconds required to transmit the frame.
- CRC: It is a 16 bits field calculated by the sender and checked by the receiver.

2.6.3 MAC Frame

Figure 2.9 shows the MAC frame format for the 802.11 standard.

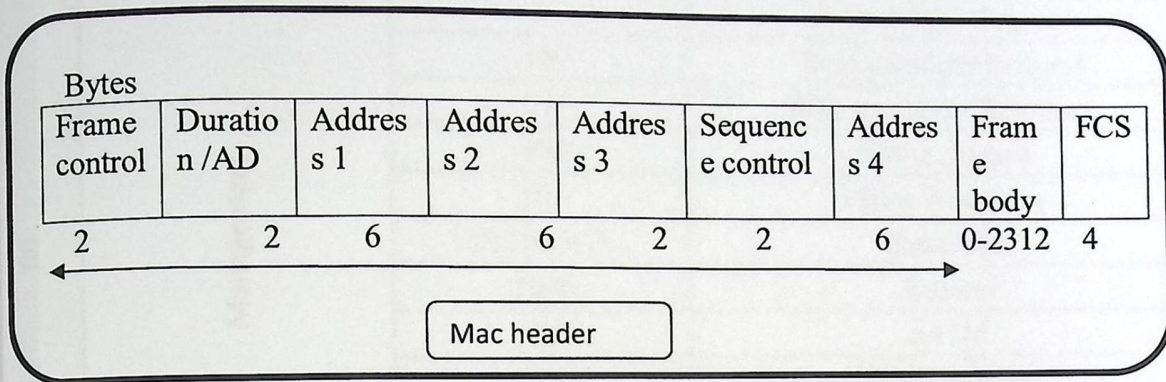


Figure 2.9 : MAC frame format.

There are 9 fields in the MAC frame, the use of each field is as follows

- Frame control: each frame starts with two bytes, called frame control. The sub fields are shown in figure 2.10.

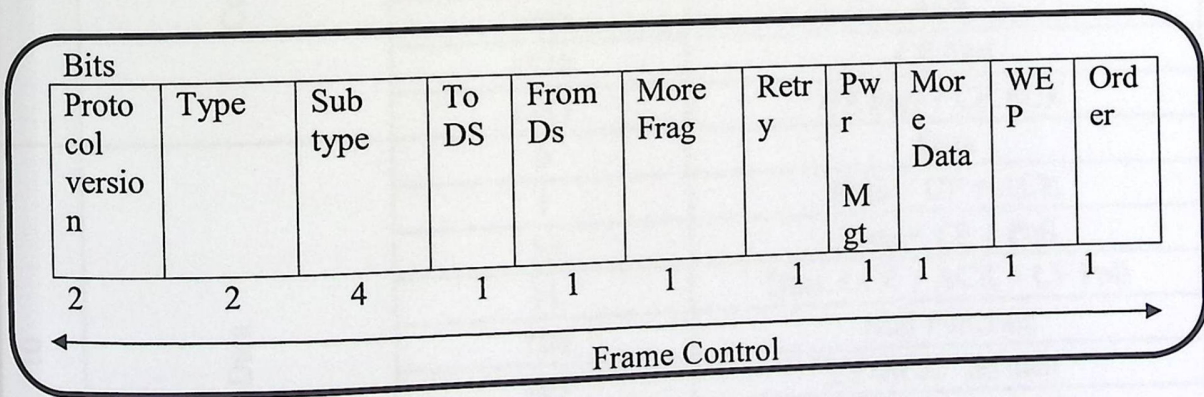


Figure 2.10 : Frame control field.

1. Protocol version: it is a two bits field indicates to the version of the MAC used.
2. Type: It is a two bits field indicates to the frame type which can be (management 00, control 01, data frames 10, 11 is reserved).

3. Sub type: It is a four bits field indicates the type of the frame according to the type field. Table 2.2 shows all values of Type and Sub type values .

Table 2.2 Frame types.

Type	Type Description	Subtype	Subtype Description
00	Management	0	Association request
		1	Association Request
		10	Reassociation Request
		11	Reassociation Response
		100	Probe request
		101	Probe Response
		0110-0111	Reserved
		1000	Beacon
		1001	ATIM
		1010	Disassociation
		1011	Authentication
		1100	Deauthentication
		1101-111	Reserved
		01	Control
1010	PS-Poll		
1011	RTS		
1100	CTS		
1101	ACK		
1110	CF End		
1111	CF End + CF ACK		
10	Data	0	Data
		1	Data + CF + ACK
		10	Data + CF + Poll
		11	Data + CF + ACK + CF Poll
		100	Null Function
		101	CF-ACK" no data"
		110	CF-Poll "not data"
		111	Cf-ACK+CF+Poll
		1000-1111	Reserved
		1111	Reserved
11	Reserved	0000-1111	Reserved

4. To DS and from DS: It is a 1 bit. Each field indicates that the frame is to distribution system or from distribution system.

5. More fragment bit: It is a 1 bit field indicates that there are more fragments or not.
6. Retry bit: It is a 1 bit field indicates that the frame is retransmission.
7. Power management bit: It is a one bit field indicates that the network card is in save mode or not.
8. More data bit: It is a one bit field indicates that there is at least one frame buffered at the access point.
9. Wep bit: It is a 1 bit field indicates that the WEP (wired equivalent privacy) is used. This is used for security issues.
10. Order bit: It is a one bit field indicates that the fragments are in order.

Table 2.2 explains the frame types, and sub types that may be in any frame, and the description of each frame. Depending on these codes the devices either the base stations or the clients can sense the wireless media and know what these codes mean, and decide what action has to be done.

- **Duration / ID field:** It is a two bytes field indicates to the number of microseconds that the medium is expected to remain busy for the transmission currently in progress. So, all stations must monitor the headers of all frames they receive and update the NAV accordingly.
- **Address fields:** 802.11 frames may contain up to four address fields, the general rule of thumb is that Address 1 is used for the receiver, address 2 for the transmitter, with the Address 3 field used for filtering by the receiver. Addressing in 802.11 follows the conventions used for the other IEEE 802 networks, including Ethernet. Addresses are 48 bits long.
- **Sequence Control Field:** It is a two byte field used for defragmentation and discarding duplicate frames.
- **Frame body:** It is the data field. 802.11 can transmit frames with a maximum payload of 2,304 bytes. (Implementations must support frame bodies of 2,312 bytes to accommodate WEP overhead).
- **Frame check sequence (FCS):** 802.11 closes its frame by the FCS which called CRC. The FCS allows stations to check the integrity of received frames. All fields in the MAC header

and the body of the frame are included in the FCS. When frames are sent to the wireless interface, the FCS is calculated before those frames are sent out over the RF link. Receivers can then calculate the FCS from the received frame and compare it to the received FCS. If the two match, then there is a high probability that the frame was not damaged in transit.

2.6.4 Samples of control frames

The control frames serve the data frames in a way to support the availability of wireless medium for the data frame. The common control frames are the RTS, CTS, ACK and power save poll.

2.6.4.1 Request to send (RTS)

These frames are used to gain control for the wireless medium in order to transmit large frames, access to the medium can be reserved only for unicast, broadcast and multicast frames. The RTS frame like other control frames is all header and no data is transmitted in the body of the frame. The duration field is the time required to transmit the next data or management frame, plus one CTS frame, plus one ACK frame plus SIFS interval time, the receive address is the address of the STA on the wireless medium that is intended immediate recipient of the next data on management frame, the transmit field is the address of the STA transmitting the RTS frame, and FCS is directly follow the header. Figure 2.11 shows the RTS frame

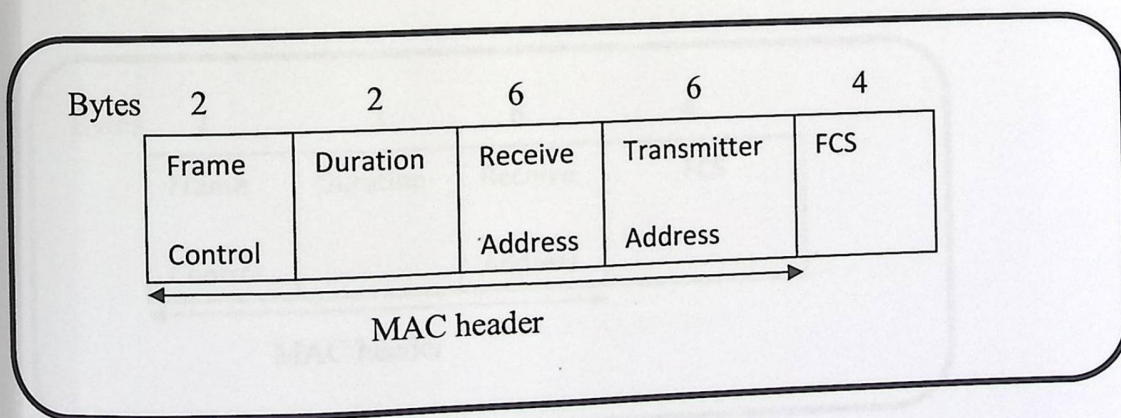


Figure 2.11 : RTS frame.

2.6.4.2 Clear To Send (CTS)

This is the answer for RTS frame. The receive address is copied from the transmitter address field of the previous RTS frame. The duration is the value obtained from the duration field of the

immediately previous RTS frame minus the time required to transmit the CTS frame and its SIFS interval. Figure 2.12 shows the format for RTS frame.

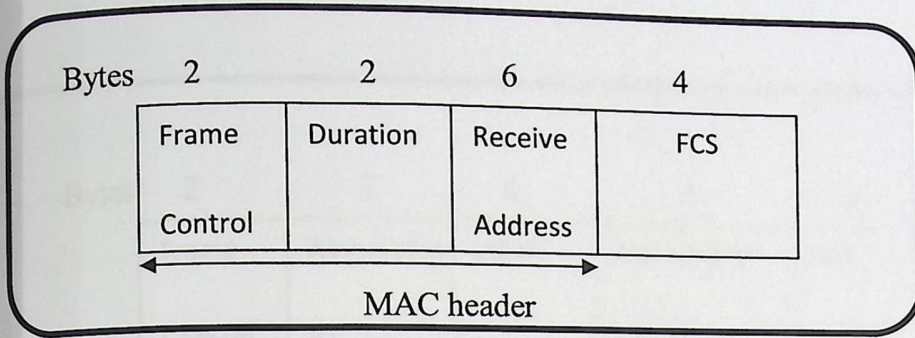


Figure 2.12 : CTS frame.

2.6.4.3 Acknowledge Frame (ACK)

This frame is used with any data transmission, including plain transmission, frames preceding RTS/CTS handshake and fragmented frames. The receive address of ACK frames is copied from the transmit address of the previous frame. The duration is obtained from the duration field of the previous frame minus the time required to transmit the ACK frame and its SIFS. Figure 2.13 shows the format for this frame.

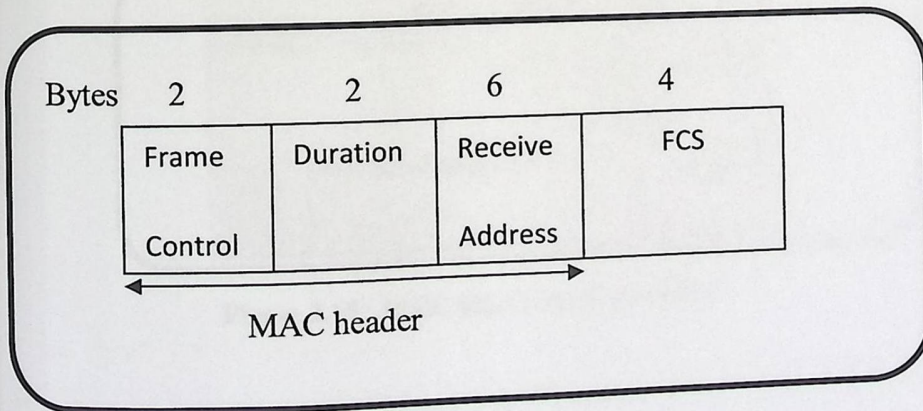


Figure 2.13: ACK frame.

2.6.4.4 Power Save Poll (PS-Poll)

This frame is used when the station wakes from a power saving mode. So, it transmits a PS-POLL frame to the access point to retrieve any buffered frames. Figure 2.12 shows the format of this frame.

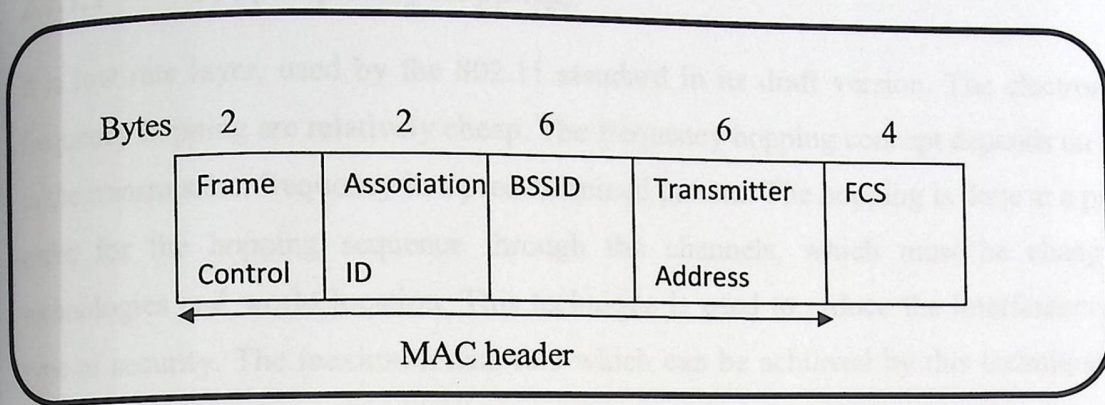


Figure 2.14 : PS-POLL frame.

2.7 IEEE 802.11 PHY and MAC Layers:

IEEE 802.11 standard defines different layers. In this work, we are interested in the medium access control (MAC), and physical layer (PHY) layer which specify the modulation methods used and the signaling characteristics for the transmission.

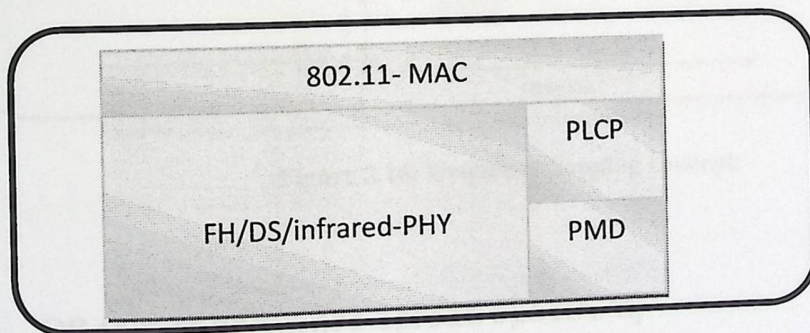


Figure 2.15 : IEEE 802.11 MAC and PHY.

2.7.1 IEEE 802.11 PHY Layer

The physical layer consists of two sub layers, physical layer convergence procedure (PLCP) and the physical medium dependent (PMD). The PLCP frame is the interface between the frames from the MAC and the radio transmissions in the air. The PMD sub layer is responsible for sending any bits

received from the PLCP sub layer using the antenna as shown in figure 2.15. The physical layer of 802.11 supports three types of frequency spectrum techniques:

2.7.1.1 FH (frequency hopping)

It is low rate layer, used by the 802.11 standard in its draft version. The electronics that support frequency hopping are relatively cheap. The frequency hopping concept depends on the rapid change in the transmission frequency in a predetermined pattern. The hopping is done at a previously known order for the hopping sequence through the channels, which must be changed by different technologies and world location. This technique is used to reduce the interference. Also, it adds a type of security. The maximum data rate which can be achieved by this technique is starting from 1Mbps or 2 Mbps depending on the type of modulation used (PSK or DPSK), figure 2.14 shows the concept of frequency hopping.

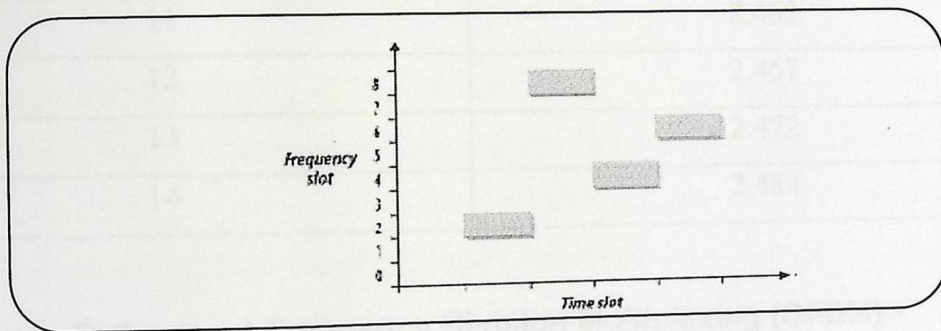


Figure 2.16: frequency hopping concept.

2.7.1.2 DS (direct sequence spread spectrum)

It is the most useful technique used by 802.11 standards. This technique needs more power to achieve the same rate as used in the FH technique. The importance of this technique is that it is more adaptable to be designed for higher data rate than the frequency hopping technique. Direct sequence systems require more sophisticated signal processing, which reflect into more complex hardware and higher electrical power consumption. The 802.11b standard uses the complementary code keying technique to achieve up to 11Mbps. The location of the channels in the DS ISM band is as follows :

Table 2.3 : ISM band channels.

Channel Number	Frequency
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462
12	2.467
13	2.472
14	2.484

2.7.1.3 Orthogonal Frequency Division Multiplexing (OFDM)

This technique depends on dividing the channel into several sub channels, and sending the data through these sub channels. On the receiver side, the main signal will be coded another time from all sub channels, which will increase the data rates. This technique is used in 802.11a which supports up to 54Mbps data rate. The following table shows the IEEE standard versions and some other information:

Table 2.4 : IEEE 802.11 standard.

IEEE standard	Speed	Frequency Band	Access Method	Spread Spectrum
802.11	1 to 2 Mbps	2.4 GHz	Csma/CA	DSSS
802.11	1 to 2 Mbps	2.4GHz	Csma/CA	FHSS
802.11a	Up to 54Mbps	5 GHz	Csma/CA	OFDM
802.11b	Up to 11 Mbps	2.4 GHz	Csma/CA	DSSS

802.11g	up to 54 Mbps	2.4 GHz	Csma/CA	DSSS & OFDM
802.11n	Up to 600Mbps	2.4 GHz	Csma/CA	OFDM & SDM
IrDA	Up to 16 Mbps	Light	N/A	N/A

2.8 Coding techniques

There are different coding techniques used in 802.11 standard

- Phase Shift Keying (PSK): In this technique we change the phase of the sinusoidal carrier to indicate information. The draft version of this technique is called (BPSK). It uses one symbol per digit. The max data rate achieved by it is 1 Mbps. QPSK uses two bits per symbol which double the speed to 2 Mbps. Complementary code keying (CCK) is based on sophisticated mathematical transforms that allow the use of a few 8-bit sequences to encode 4 or even 8 bits per code word, for a data throughput of 5.5 Mbps or 11 Mbps.
- Frequency Shift Keying (FSK): In this technique, the frequency is changed in response to information. One particular frequency for bit One and another for bit zero.
- Amplitude Shift Keying (ASK): In this technique, the amplitude of the carrier is changed according to information and everything else remains fixed, such that bit 1 is sent to a known amplitude and bit 0 to other different known amplitude. There is a special case of the ASK called on off keying (OOK), where one of the amplitudes are zero.
- Quad Amplitude Keying (QAM) : It is a mixed technique between ASK and PSK, it changes both the phase and amplitude to indicate to the data. 16-QAM encodes 4 bits using 16 symbols, and 64-QAM encodes 6 bits using 6 symbols.

2.9 802.11n Standard

This is the new version of the standard 802.11. It comes because of the need for high data rates. In this thesis we focus on this version with all its technical characteristics. There are new enhancements adopted in this version in the Physical and MAC layers. The original 802.11 PHY layer specification focuses on wireless transmission. It assesses the wireless medium state and reports it back to the MAC sub-layer. The main amendments are: IEEE 802.11a, 802.11b, and 802.11g. Both 802.11b and

802.11g	up to 54 Mbps	2.4 GHz	Csma/CA	DSSS & OFDM
802.11n	Up to 600Mbps	2.4 GHz	Csma/CA	OFDM & SDM
IrDA	Up to 16 Mbps	Light	N/A	N/A

2.8 Coding techniques

There are different coding techniques used in 802.11 standard

- Phase Shift Keying (PSK): In this technique we change the phase of the sinusoidal carrier to indicate information. The draft version of this technique is called (BPSK). It uses one symbol per digit. The max data rate achieved by it is 1 Mbps. QPSK uses two bits per symbol which double the speed to 2 Mbps. Complementary code keying (CCK) is based on sophisticated mathematical transforms that allow the use of a few 8-bit sequences to encode 4 or even 8 bits per code word, for a data throughput of 5.5 Mbps or 11 Mbps.
- Frequency Shift Keying (FSK): In this technique, the frequency is changed in response to information. One particular frequency for bit One and another for bit zero.
- Amplitude Shift Keying (ASK): In this technique, the amplitude of the carrier is changed according to information and everything else remains fixed, such that bit 1 is sent to a known amplitude and bit 0 to other different known amplitude. There is a special case of the ASK called on off keying (OOK), where one of the amplitudes are zero.
- Quad Amplitude Keying (QAM) : It is a mixed technique between ASK and PSK, it changes both the phase and amplitude to indicate to the data. 16-QAM encodes 4 bits using 16 symbols, and 64-QAM encodes 6 bits using 6 symbols.

2.9 802.11n Standard

This is the new version of the standard 802.11. It comes because of the need for high data rates. In this thesis we focus on this version with all its technical characteristics. There are new enhancements adopted in this version in the Physical and MAC layers. The original 802.11 PHY layer specification focuses on wireless transmission. It assesses the wireless medium state and reports it back to the MAC sub-layer. The main amendments are: IEEE 802.11a, 802.11b, and 802.11g. Both 802.11b and

802.11a support raw data rates up to 11 Mb/s and 54 Mb/s, respectively. A third PHY specification for 802.11g was introduced, with maximum raw data rate of 54Mbps within the 2.4GHz band.

The MAC architecture of 802.11 is based on logical coordination functions that control medium access. In the legacy IEEE 802.11 standard, there are two types of access schemes: the mandatory distributed coordination function (DCF) and the optional point coordination function (PCF). The DCF is based on Carrier Sensing Multiple Access with Collision Avoidance (CSMA/CA) mechanism. The PCF is based on a poll-and-response mechanism.

These MAC schemes are found to be inadequate to provide acceptable quality of service (QoS) levels for voice over IP (VoIP) applications as well as audio/video conferencing. Therefore, a new extension was developed in 2005, the 802.11e. The 802.11e proposes additional service for differentiating and prioritizing traffic. In addition, IEEE 802.11e offers, the transmission opportunity (TXOP), which is an interval of time in which multiple data frames, can be sent from one node to another. Further, the idea of block ACK was established. With this idea, receivers can acknowledge multiple received data frames using a single extended ACK frame.

The 802.11n PHY layer operates multiple antennas for both transmitter and receiver. MIMO provides antenna diversity and spatial multiplexing. With single input single output (SISO) systems, multipath is typically perceived as interference degrading the ability of the receiver to recover useful information. However, a MIMO system has the ability to simultaneously resolve information from multiple signal paths using spatially separated receiving antennas. Also, the 802.11n PHY layer can optionally use 40MHz channel bandwidth to improve the theoretical capacity limits. Finally, new coding schemes have been proposed for 802.11n.

MAC enhancements have also been proposed for 802.11n. The main enhancement is the frame aggregation. It maximizes throughput and efficiency. Two aggregation types have been defined: aggregate MAC protocol service unit (A-MSDU) and aggregate MAC protocol data unit (A-MPDU).

In A-MSDU, several MSDUs destined to the same receiver are aggregated in a single MPDU. The operation is performed at the top of the MAC layer where the coming MSDUs are buffered and then aggregated in order to form A-MSDU frame. On the other hand, A-MPDU concatenates multiple MPDUs frames in a single PHY protocol data unit (PPDU) frame. It is possible to combine frames

with different traffic identifiers given that sub-frames are addressed to the same receiver. Additionally, there is no waiting time during the formation of the A-MPDU. Only the corrupted MPDUs within an A-MPDU need to be retransmitted. Multiple MPDUs are acknowledged with a single block ACK in response to a block acknowledgment request (BAR).

Another key enhancement specified for 802.11n is the bidirectional data transfer method during a single TXOP. This permits the transportation of data frames in both directions in one TXOP.

Another MAC enhancement in 802.11n is the long network allocation vector (long-NAV). It improves scheduling, given that a node that holds a TXOP may set a longer NAV value intended to protect multiple PPDU's. Another feature is the reduced IFS (RIFS). It is proposed to allow a short time interval of between multiple PPDU's, compared to SIFS defined in the legacy standards.

2.9.1 PHY Enhancements

- It is applicable on both 2.4 and 5 GHz.
- The new PHY supports OFDM modulation with additional coding methods, multiple streams and beam forming
- Multiple input multiple output (MIMO) radio technology.
- High throughput PHY, 40 MHz channels or two adjacent 20 MHz channels are combined to create a single 40 MHz channel.

2.9.2 MAC Enhancements

Block acknowledgement technique was used in 802.11n standard. A performance optimization in which an IEEE 802.11 ACK frame need not follow every unicast frame and combined acknowledgements may be sent at a later point in time, which will increase the data rate for the new standard 802.11n at a noticeable rate.

2.9.3 Multiple Input Multiple Output (MIMO) concept

Transmit and receive with multiple radios simultaneously in same spectrum. This doubles the rate in the case of single radio, as shown in figure 2.17. If we can compare MIMO to traditional single input single output radio (SISO) (with optional receive diversity), we can see multiple independent data streams are sent between the transmitter and receiver antennas to deliver more bits in the specified

bandwidth. Also cross paths between antennas are automatically decoded by the receiver. The following figure shows the concept of MIMO used in 802.11n networks.

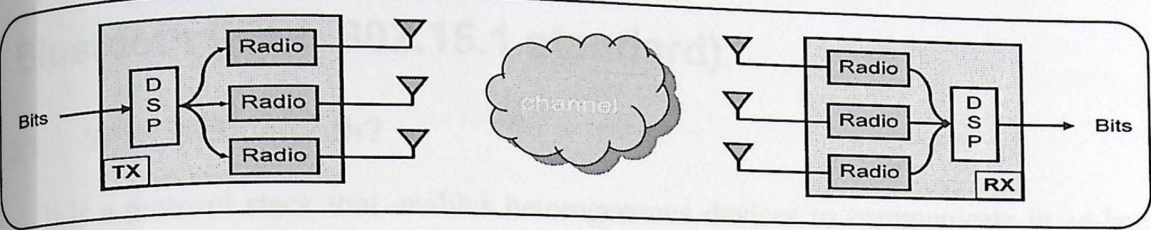


Figure 2.17: MIMO concept.

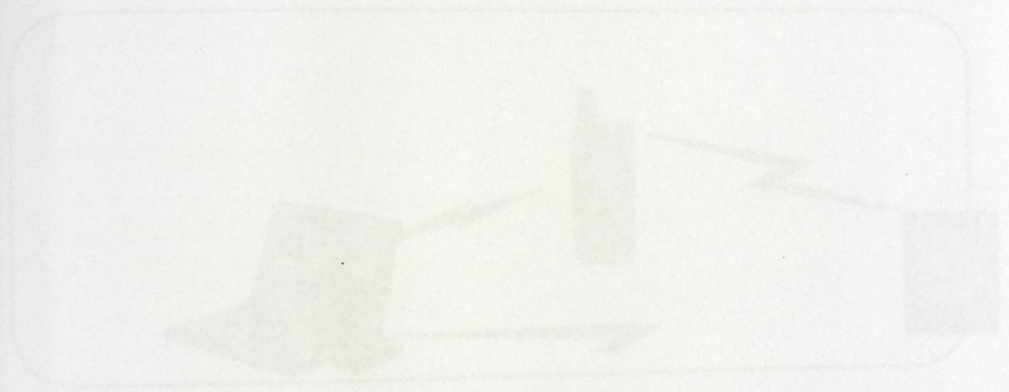


Figure 2.18: Bluetooth devices.

Bluetooth has many applications used in these days like

- Car phone
- Car free computer
- Instant phone/Text transmission
- Wireless phone

Physical Layer (PHY)

CHAPTER 3

Bluetooth (IEEE 802.15.1 standard)

3.1 What is Bluetooth?

It is a protocol stack that enables heterogeneous devices to communicate in ad-hoc manner to exchange information. Also it is cable replacement technology. It connects devices such as phone handsets, headsets, computer peripherals, etc. Also, it is an industry standard that allows wireless communication between devices. It is lower power and cost than the wireless LAN. The following figure shows sample of Bluetooth devices.

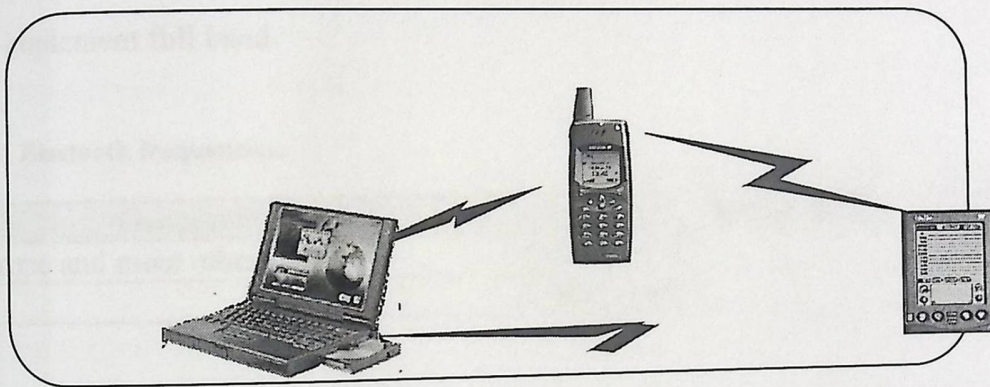


Figure 3.1: Bluetooth devices.

The Bluetooth has many applications used in these days like:

- Conference table.
- Cordless computer.
- Instant photos/files transmission.
- Cordless phone

3.2 Physical Layer (PHY)

3.2.1 Functions

The function of the PHY layer of the Bluetooth can be summarized in the following points

- Responsible for transferring bits between adjacent systems over the air interface.
- Receives a bit stream from the MAC sub layer and transmits the bit stream via radio waves to the associated station or vice versa.

3.2.2 Requirements

- The Bluetooth transceivers operate in 2.4 GHz ISM band as shown in Figure 3.2 and table 3.1.
- Products implementing the reduced frequency band will not work with the products that implement full band.

Table 3.1 Bluetooth frequencies.

Geography	Range (GHz)
Us, Europe and most other countries	2.400 -2.4835
France	2.4465-2.4835

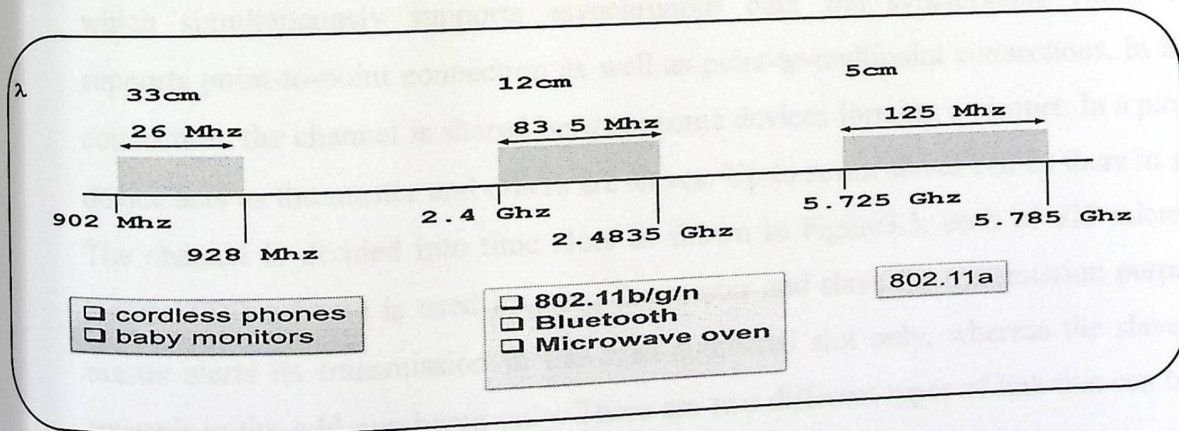


Figure 3.2 Unlicensed Radio Spectrum.

- The equipment can be divided into three power class categories as shown in Table 3.2.
- Gaussian Frequency Shift Keying (GFSK) is used.

Table 3.2 : Bluetooth power classes.

Power Class	Maximum output power	Nominal output power	Minimum output power
1	100 mw	N/A	1 mw
2	2.5 mw	1 mw	0.25 mw
3	1 mw	N/A	N/A

3.2.3 Receiver Characteristics

- The Bluetooth receiver sensitivity level is approximately -70 dBm or better.
- The receiver should have the capability to measure its signal strength and determine whether the transmitter should increase or decrease the power. This is the Receive signal strength indicator (RSSI) measurement.

3.3 Medium Access Control (MAC)

3.3.1 Base Band Specifications

The Symbol rate is 1M Symbols/s, using frequency hopping with a rate of 1600 hops per second. Time division duplex (TDD) is used. Information is exchanged along the channel in terms of packets which can take single time slot, or it can cover up to 5 time slots. Bluetooth can support up to three simultaneous synchronous voice channels, or it can support a channel which simultaneously supports asynchronous data and synchronous voice. Bluetooth supports point-to-point connection as well as point-to-multipoint connections. In multipoint connection, the channel is shared between some devices forming a piconet. In a piconet, one device acts as the master and others are slaves. Up to seven slaves can be there in a piconet. The channel is divided into time slots as shown in Figure3.3, each of 625 micro-seconds length. TDD scheme is used between the master and slave for transmission purposes. The master starts its transmission in the even-numbered slot only, whereas the slaves start to transmit in the odd-numbered only. There are two different types of link that can be defined between the master and the slave:

- Synchronous Connection Oriented (SCO) link: it is a symmetric, point-to-point link between the master and the slave, used to carry real-time traffic (voice). The master can

support up to 3 SCO links to the same slave or different slaves. The master sends SCO packets in the regular interval known as T_{SCO} (SCO interval in slots) in master to slave slots.

- Asynchronous Connection Less (ACL) link: it is a point-to-multipoint link between the master and all the slaves participating in the piconet. The master can establish an ACL link on per-slot basis with any slave. ACL links provide a packet-switched connection. The following figure shows the Bluetooth radio link channels.

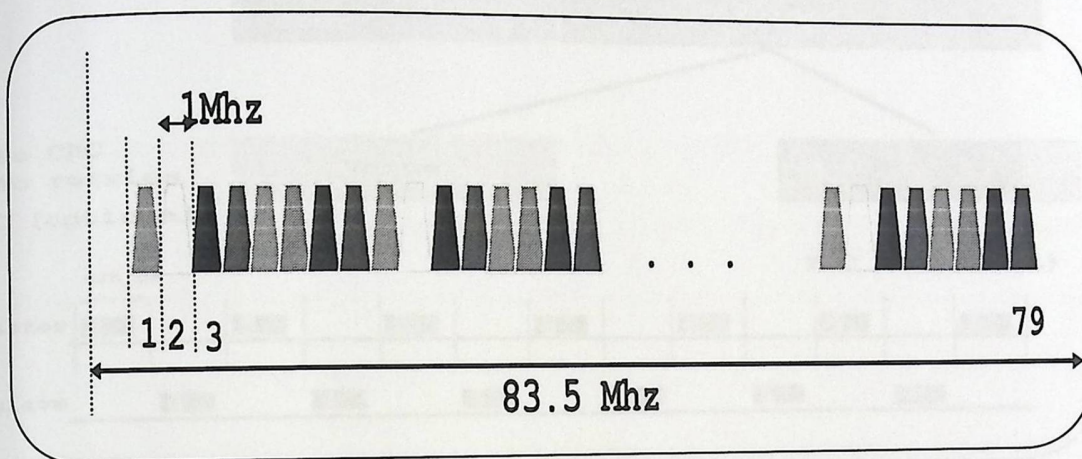


Figure 3.3 Bluetooth Channels.

3.4 Packet Format

The packet format is divided into three fields as shown in Figure 3.4 :

1. Packet access code: it is a 72 bits length, which is the address of piconet master.
2. Packet header :It is a 54 bits divided as :
 - 3 bits for addressing (max 7 active slaves).
 - 4 bits for packet type (16 packet types).
 - 1 bit for flow control.
 - 1 bit for knowledge indicator.
 - 1 bit for sequence number.

- 8 bit for header error check.

The total header, including the HEC, consists of 18 bits, and is encoded with a rate 1/3 FEC resulting in a 54-bit header.

3. Payload: This field is dedicated for data. It takes a range from 0 bits to 2744 bits depending on data type, (voice or data). The following figure shows the packet frame for Bluetooth.

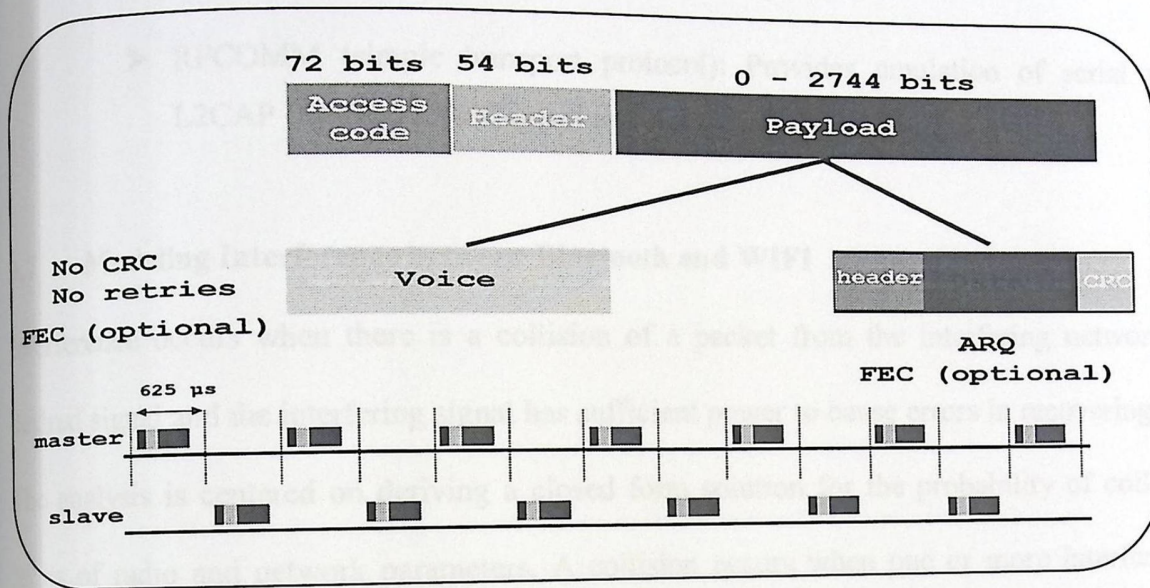


Figure 3.4 Bluetooth packet format.

3.5 Bluetooth Modes

During the connection, Bluetooth device can be in one of the following modes:

- **Active mode:** Bluetooth unit listens for each master transmission. Slaves which are not addressed can sleep through a transmission.
- **Sniff mode:** Unit does not listen to every master transmission. Master polls such slaves in specified sniff slots.
- **Hold mode:** Master and slave agree on a time duration for which the slave is not polled, typically used for scanning, paging, inquiry or by bridge slaves to attend to other piconets.
- **Park mode:** The unit will have very little activity consuming very low power.

3.6 Bluetooth Protocols

There are different protocols working with Bluetooth. The following protocol is the most common:

- Service Discovery Protocol (SDP): Provides attribute based searching of services, browsing through available services, means of discovering new services and Provides removal of unavailable services.
- RFCOMM (simple transport protocol): Provides emulation of serial ports over L2CAP (Logical Link Control and Adaptation Protocol).

3.7 Modeling Interference between Bluetooth and WIFI

Interference occurs when there is a collision of a packet from the interfering network with the desired signal and the interfering signal has sufficient power to cause errors in recovering the signal.

The analysis is centered on deriving a closed form solution for the probability of collision P_c in terms of radio and network parameters. A collision occurs when one or more interfering signals overlap in both time and frequency with the desired signal. This will lead to a retransmission of the desired signal or a packet. Based on the probability of collision, the packet error rate can be calculated. The Bluetooth devices use a small period of time to keep sensing the channel for a good slot. This time is called the Bluetooth sense time and this process continues till a certain amount of time. Therefore even in this case, there will be an overlap in the time domain, which will result in a small collision. The value depends on how large the Bluetooth sensing window time is.[10]

Bluetooth packets have to use some of the bad channels, thus the probability of collision due to Bluetooth on 802.11 at MAC layer is given by the collision in both time and frequency .

$$P_c = P_c (\text{time overlap}). (\text{frequency overlap}) \quad (1)$$

The packet withdrawal probability is the probability of the sense window overlap with the packet transmission from 802.11 device. In other words it is the probability of collision of the Bluetooth

sense window with the 802.11 packet. Therefore, the packet withdrawal probability can be written as:

$$P_w = \frac{802.11 \text{ frame transmission time} + \text{Bluetooth sense time}}{\text{Total Bluetooth time in interval}} \cdot \frac{N_b}{N_{b_min}} \quad (2)$$

Similarly the probability of collision can be written as :

$$P_c = \frac{802.11 \text{ frame transmission time} + \text{Bluetooth occupied time}}{\text{Total Bluetooth interval}} \cdot \frac{N_b}{N_{b_min}} \quad (3)$$

Where N_b is the number of bad channels.

The probability of packet error determines if the packet must be retransmitted, as the receiver may not be able to decode. When the packets are withdrawn the probability of withdrawal P_w is derived as :

$$PER = 1 - [(1 - pe\{no BT\})^{bits \text{ in } 625 \mu s} \cdot (1 - P_w) + (1 - Pe\{BT\})^{bits \text{ in } 366 \mu s} \cdot (1 - Pe\{no Bt\})^{bits \text{ in } 259 \mu s} \cdot P_w]^k \quad (4)$$

Similarly, the expression for the packet error rate can be derived, when the packets are collided while implementing AFH. Instead of P_w , P_c is substituted in all the above equations. The packet error will then be

$$PER = 1 - [(1 - pe\{no BT\})^{bits \text{ in } 625 \mu s} \cdot (1 - P_c) + (1 - Pe\{BT\})^{bits \text{ in } 366 \mu s} \cdot (1 - Pe\{no Bt\})^{bits \text{ in } 259 \mu s} \cdot P_c]^k \quad (5)$$

Where, $k = \frac{T_{w,t}}{T_{BT,slot}} = \frac{T_{w,t}}{625\mu s}$ and $T_{w,t}$ is the 802.11 packet transmission time.

Throughput is the ratio of the number of bits successfully received to the time taken in transmitting the bits over the medium. The throughput of the 802.11 system in the presence of Bluetooth interference can be written as:

$$T = \frac{\text{Data (WLAN)}}{T_{wt}} \cdot (1 - \text{PER})^{N(\gamma)} \quad (6)$$

Where Data(wlan) is the data rate at which the 802.11 is transmitted, and $N(\gamma)$ is the expected number of interferences as in [10].

Chapter 4

Devices and Tools

4.1 Introduction

In this chapter, description of the devices and tools used in this work were explained. The experiments were performed depending on IEEE802.11 and Bluetooth hardware. We divide this chapter into two parts. Both parts combined to accomplish the experiments in the most proper way. Part one is about the required hardware that been used in the experiments. This hardware is used in different modes (monitor and managed modes) as shown in Figure 4.1. Part two is about the software required like drivers, tools and programs used in the experiments.

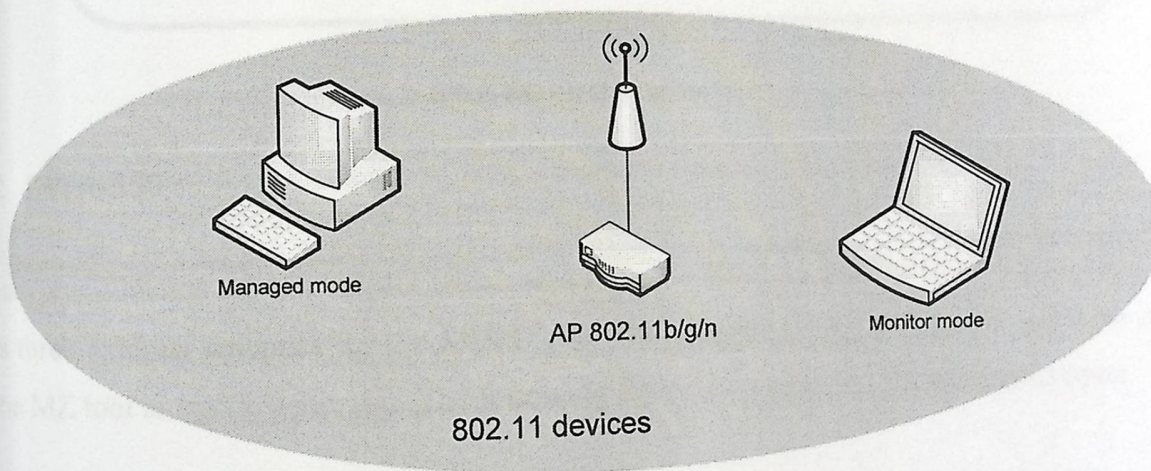


Figure 4.1: 802.11 standard devices (clients, access point).

4.2 **Hardware** : The following part explains the hardware used in our experiment

4.2.1 **DWA-643** : A wireless adaptor which was produced by D-Link. It supports (802.11 a/b/g/n). Its chipset is Atheros ar5418. DWA-643 works in our experiments as a monitor device on

ath9k driver without any problems. We used the iw-tool to configure this device in monitor mode. The iw tool will be explained in the software part. The following figure shows DWA-643 wireless adapter.

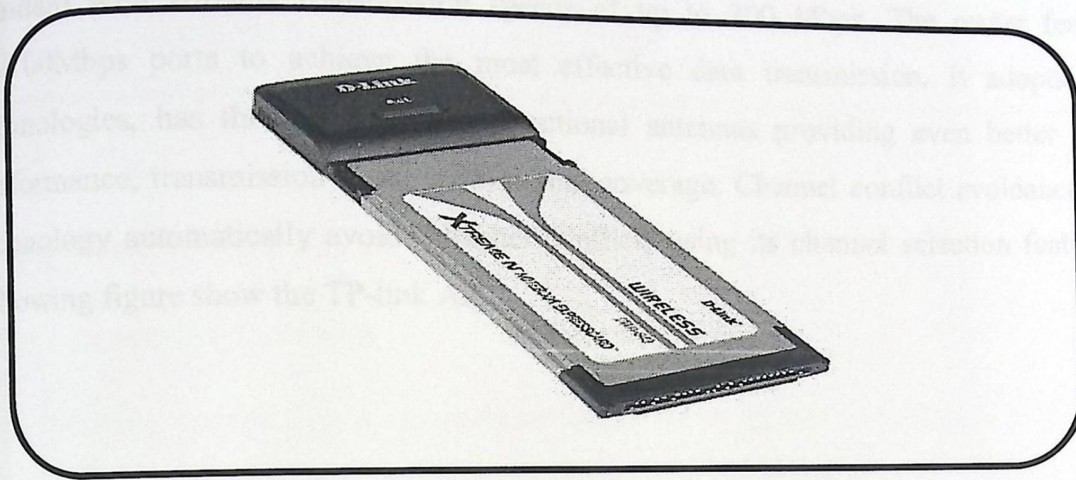


Figure 4.2: DWA-643 wireless adapter.

4.2.2 DWA-556 :

This adaptor contains ar5416 chipset which also supports 802.11n in addition to legacy 802.11a/b/g. It has three external antennas for the MIMO use. This adapter is set to managed mode, in order to use the MZ tool as traffic generator. The following figure shows DWA-556 wireless adapter.

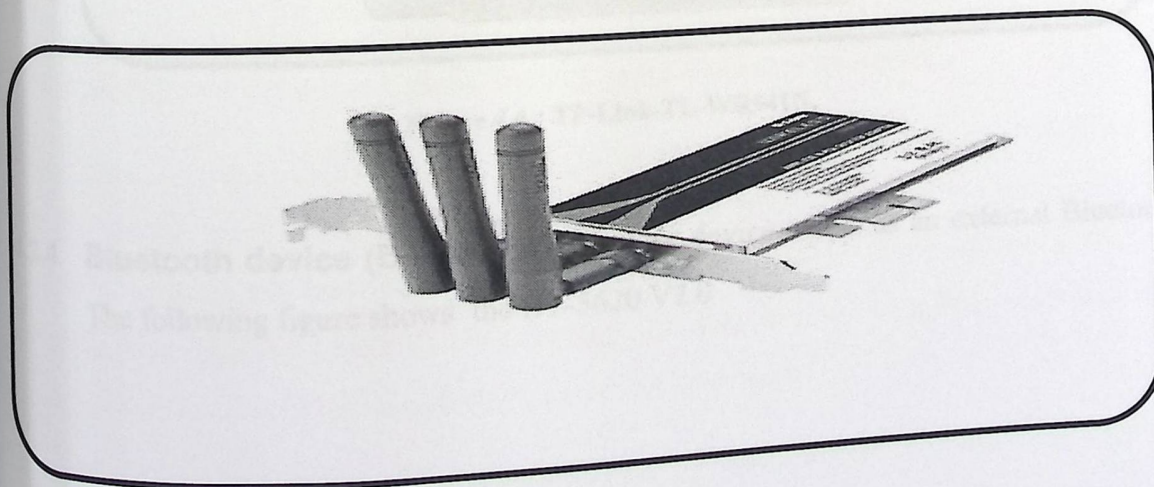


Figure 4.3 : DWA-556 wireless adapter.

4.2.3 **TP-Link-TL-WR941N** : The TL-WR941N Wireless N Router is a combined wired/wireless network connection device designed specifically for small business, office, and home office networking requirements. It complies with the IEEE 802.11n (Draft 2.0) standard with wireless transmission speeds of up to 200 Mbps. The router features 4 10/100Mbps ports to achieve the most effective data transmission. It adopts MIMO technologies, has three fixed Omni directional antennas providing even better wireless performance, transmission rates, stability and coverage. Channel conflict avoidance (CCA) technology automatically avoids channel conflicts using its channel selection feature. The following figure show the TP-link AP.

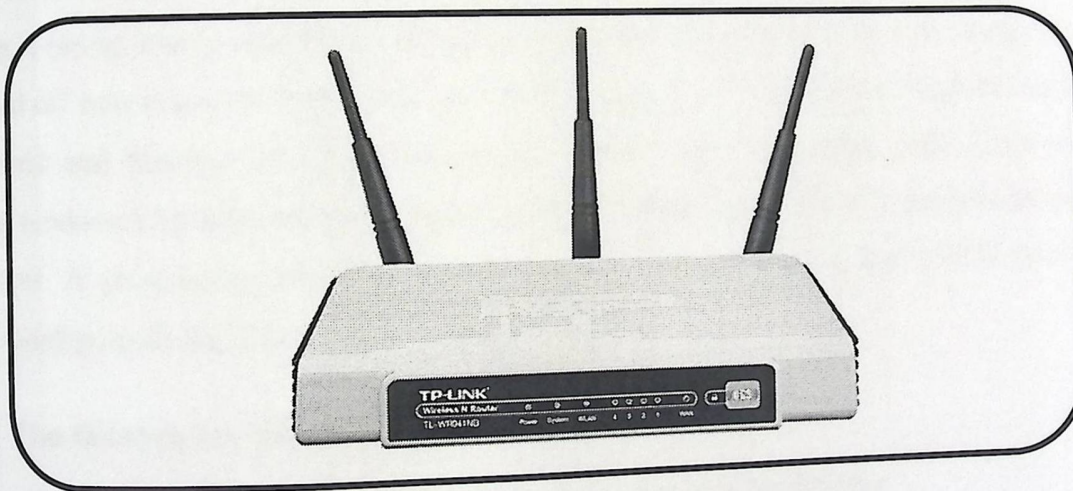


Figure 4.4 : TP-Link-TL-WR941N.

4.2.4 **Bluetooth device (BT-3620 V2.0)**: This device works as an external Bluetooth adapter. The following figure shows the BT-3620 V2.0

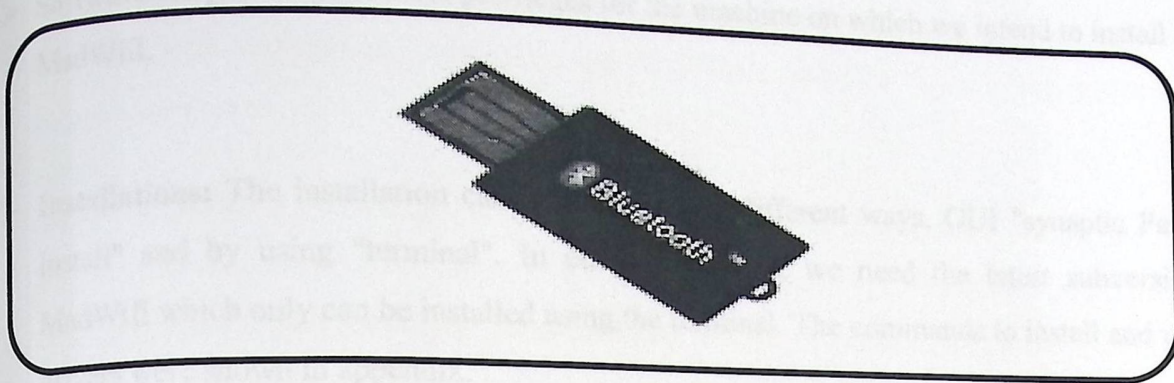


Figure 4.5 : BT-3620 V2.0 BT device.

4.3 Software requirements:

4.3.1 Linux Operating Systems

Linux is an operating system. The accurate name of this operating system is GNU/Linux. Linux is not produced by one company, but a number of companies and a group of developers contribute to develop it (open source operating system). In fact, the GNU/Linux is a core component which is branched off into many different products. These are called Distributions. Distributions change the appearance and function of Linux completely. They range from large, fully supported complete systems (endorsed by companies) to lightweight ones that fit on a USB memory stick or run on old computers. A prominent, complete and friendly distribution to step into GNU/Linux is Ubuntu, used to configure all the system in our experiments.[4]

4.3.2 The Drivers for Wireless Network Interface Cards:

4.3.2.1 Multiband Atheros Driver for Wireless Fidelity (MadWifi)

It is a Linux kernel device driver for Atheros-based Wireless LAN devices. The driver works such that the WLAN card will appear as a normal network interface in the system. In this section, the MadWifi requirements and installation will be described. Also, there will be a brief explanation about the tools used by MadWifi "wlanconfig". In order to make MadWifi work properly, it needs some hardware and software requirements as explained below :

- **Hardware Requirements:** A PCI/miniPCI or Card bus card with an Atheros chipset. USB devices are not yet supported.

- **Software Requirements:** Root privileges for the machine on which we intend to install MadWifi.
- **Installations:** The installation can be done in two different ways. GUI "synaptic Package Install" and by using "terminal". In our experiments, we need the latest subversion of MadWifi which only can be installed using the terminal. The commands to install and update drivers were shown in appendix.
- **Multiband Atheros 9000 series Driver for Wireless Fidelity (Ath9k):** Ath9k is a linux driver for 802.11a/b/g/n universal NIC cards (Card bus, PCI-E, or miniPCI-E - using Atheros 9000 series chip sets). This driver is the latest driver for Atheros Chipsets wireless network cards. The Ath9k driver is used to configure the DWA 643 WNIC into monitor mode using one of its commands which will be explained briefly below.
- **iw "Atheros Tool":** "iw" is a new 802.11 based CLI configuration utility for wireless devices. It supports almost all new drivers that have been added to the kernel recently.
- **Adding interfaces with iw:** There are several modes supported. The modes supported are monitor, managed [also station] and adhoc, samples of the commands to add interface in several mode are shown in appendix.

4.3.3 Wireless Tools:

- **Iwconfig :** This command is used to set parameters which are common across most drivers. The format for the iwconfig command is shown in appendix.

4.3.4 **TShark :** It is a network protocol analyzer. It gives us the opportunity to capture data packets from a live network, or read packets from a previously saved capture file, either printing a decoded form of those packets to the standard output or writing the packets to a file. Without any options set, TShark will work much like tcpdump. It will use the pcap library to capture traffic from the first available network interface and displays a summary line on stdout for each received packet. TShark is able to detect, read and write the same capture files that are supported by Wireshark. The input file doesn't need a specific filename

extension. The file format and an optional gzip compression will be automatically detected. Therefore, the compressed files require the zlib library, samples of the tshark commands are shown in appendix.

4.3.5 **MZ (Mausezahn) packet generator** : It is a free fast traffic generator written in C which allows us to send data packets. Mausezahn can also be used as didactical tool in network labs or for security audits, including penetration and denial of service (DoS) testing. As traffic generator, Mausezahn is used to test IP multicast or VoIP networks. Samples from MZ generator command are shown in appendix :

4.3.6 **BLUETOOTH MANAGER (Blue Soleil)** : It is a Bluetooth manager that make the connection between laptop which have the Bluetooth device and other devices (laptops or mobiles). Also, it gives us the speed of the connection. Figure 4.6 shows the Bluetooth manger.

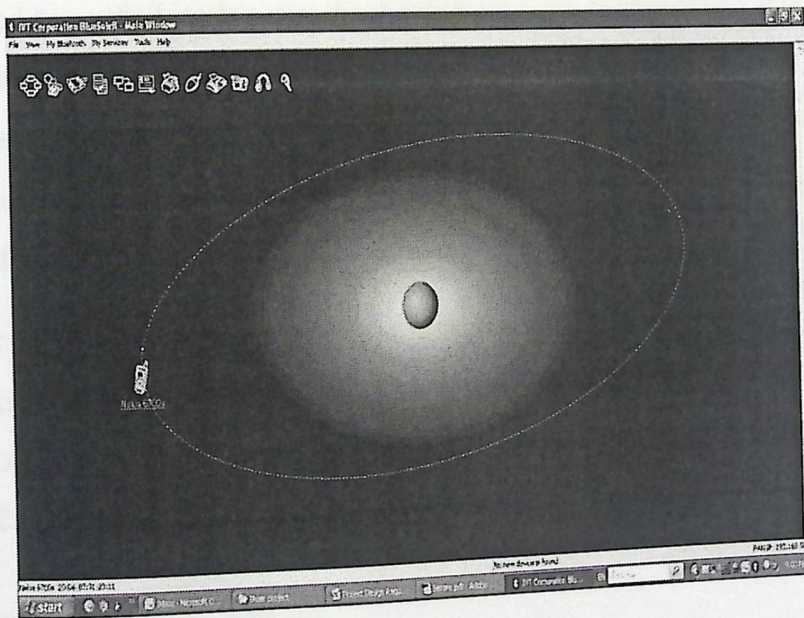


Figure 4.6 : Bluetooth manager (Bluesoleil).

CHAPTER 5

Results

5.1 Experimental Setup

The goal of the empirical experiments is to obtain an estimate of the mutual interference between Bluetooth and 802.11 WLAN devices. Though our focus is on 802.11n, we also consider the other widely used modes 802.11b/g. The experimental network has been placed in typical operation environment. It is comprised of an 802.11 WLAN system (Client and AP) and a simple Bluetooth piconet. The AP is TLWR941N wireless N router. It is connected to a PC server used to receive the 802.11 traffic. Client is equipped with DWA-556 adapter and configured in the managed mode. Another node is used to sniff data frames. It is equipped with DWA-643 adapter based on Atheros chipset and configured in the monitor mode. The Bluetooth system is based on BT-3620 [5]. The MZ traffic generator [15] is used to generate 802.11 traffic. File transfer is used for the Bluetooth network. We measure the throughput of both networks, using the T-Shark and BlueSoleil measurement tools for 802.11 and Bluetooth, respectively.

In this chapter we will discuss the results of experiments executed in wireless and Bluetooth networks. Two cases are considered. The first case focuses on the measurements of 802.11 networks with the existence of Bluetooth. The second case will be for the measurements of the Bluetooth with the existence of 802.11 networks.

5.2 Effect of Bluetooth on 802.11

In this part, we will start our experiments on the elementary versions of 802.11 standard.

5.2.1 Scenario 1 (802.11b network)

5.2.1.1 Throughput of (802.11b)

As shown in Figure 5.1, in this experiment the throughput of 802.11b network with Bluetooth interference in the range were measured. Distance between the Bluetooth transmitter and the 802.11b receiver is varied.

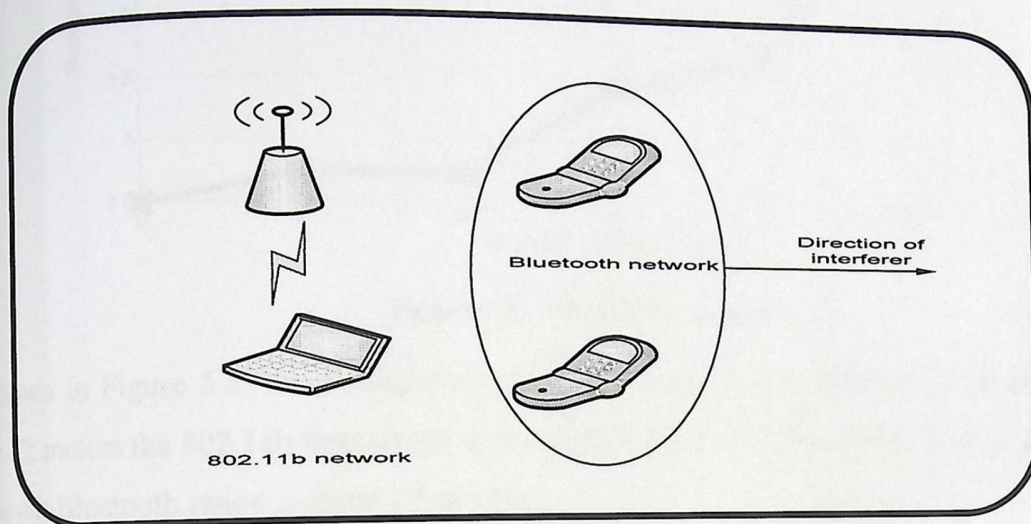


Figure 5.1 802.11b with Bluetooth.

Table 5.1 : 802.11b Throughput and Loss of frames .

802.11b Throughput and Loss of frames							
distance of interferer (meter)	0	2	4	6	8	10	12
Throughput (Mbps)	7.5	7.7	7.7	8.4	8.7	10.9	11
Loss of frames (%)	0.2	0.2	0.15	0.1	0.03	0.05	0.02

Results are shown in Table 5.1 and plotted in Figure 5.2.

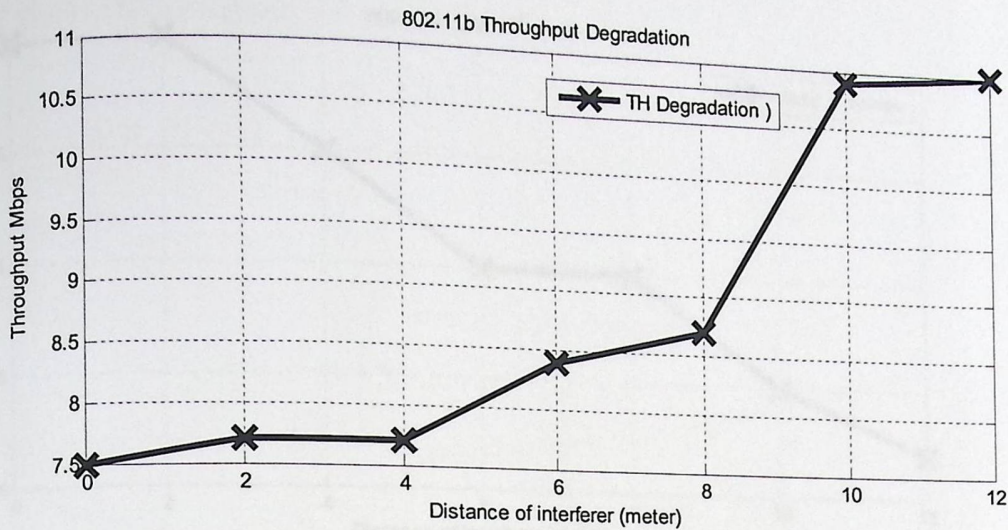


Figure 5.2 : 802.11b Throughput.

As shown in Figure 5.2, the throughput of 802.11b improves as Bluetooth interferer gets farther. After 12 meters the 802.11b throughput gets stable at about 11Mbps. This result is expected because as known Bluetooth range is about 10 meters.

5.2.1.2 Loss of (802.11b)

The same scenario in figure 5.1 was used to measure the loss of frames with existence of Bluetooth. The technique used to measure the loss is as follows:

- Each frame has a field called retry bit
- A number of frames were sent, and the retry bit was checked
- At the end of the experiment, we can know how many frames are retried from the whole frames sent, which gives us the loss rate.

Table 5.1 and Figure 5.3 show the loss rate for the 802.11b network.

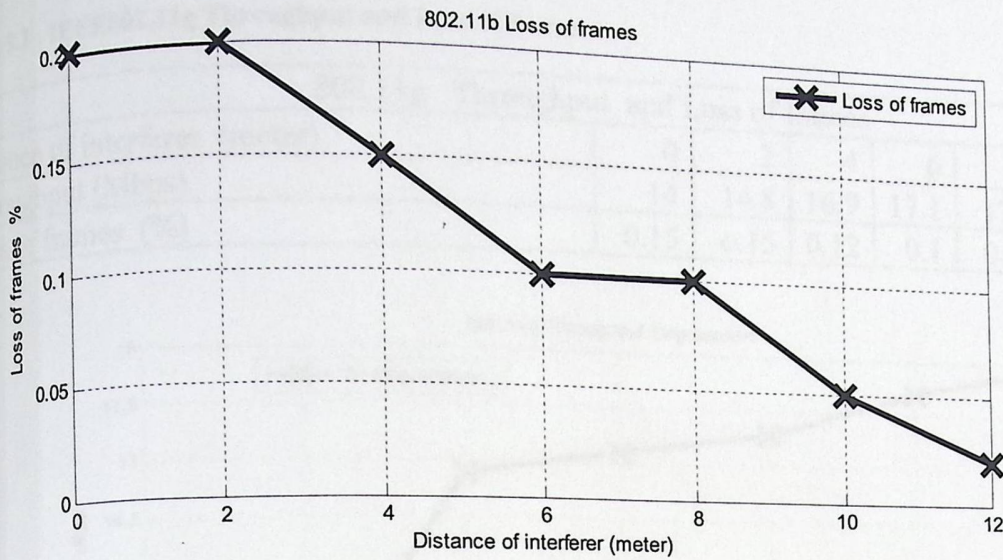


Figure 5.3 802.11b Loss of frames.

From the figure above, we can easily notice the effect of the Bluetooth on the 802.11b network, which depends on the distance of the interferer, such that the loss becomes negligible when the interferer distance becomes more than 12 meter.

5.2.2 Scenario 2 (802.11g network)

5.2.2.1 Throughput (802.11g)

As in scenario 1, we repeat the same experiment for the 802.11 in mode g. Results are summarized in table 5.2 and plotted in figure 5.3. The experiment results show that 802.11g is also affected by Bluetooth interference. The amount of reduction in the throughput of the 802.11g network does also depend on the interferer distance.

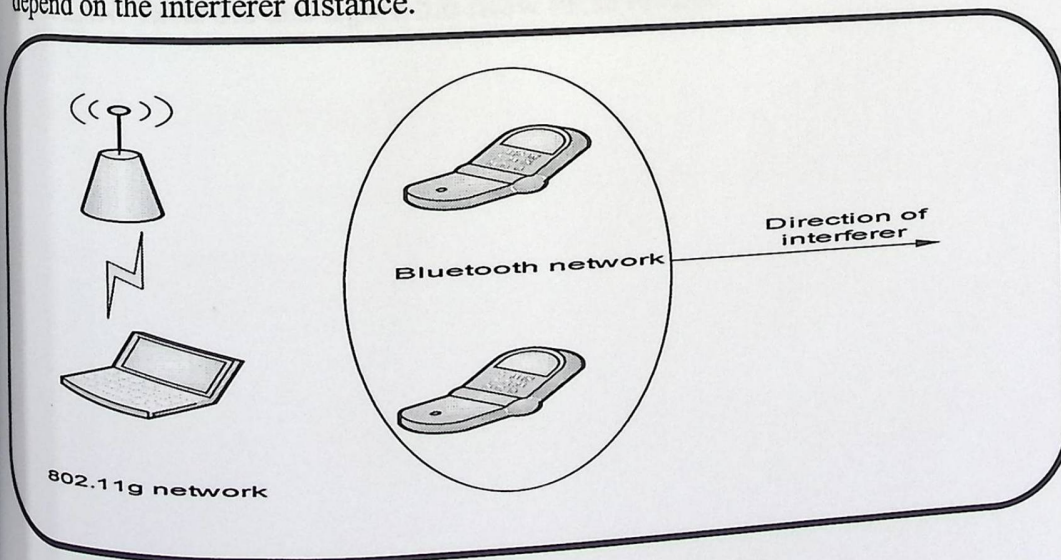


Figure 5.4 : 802.11g with Bluetooth.

Table 5.2 : IEEE802.11g Throughput and Loss of frames.

802.11g Throughput and Loss of frames							
distance of interferer (meter)	0	2	4	6	8	10	12
Throughput (Mbps)	14	14.8	16.9	17.1	17.3	17.7	18
Loss of frames (%)	0.15	0.15	0.12	0.1	0.05	0.05	0.01

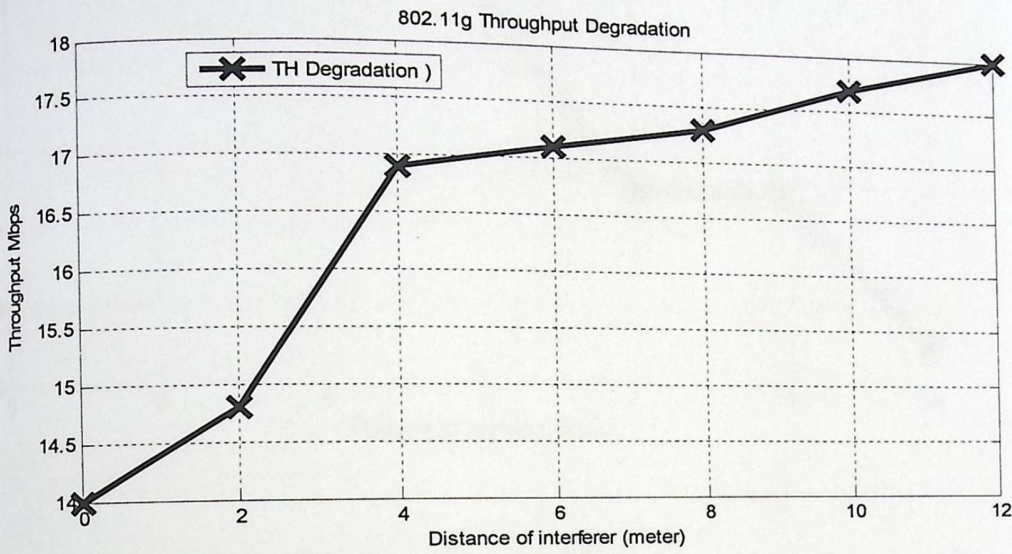


Figure 5.5 : 802.11g Throughput.

5.2.2.2 Loss (802.11g)

With the same technique, we measure the loss of frames in the network 802.11g network with the existence of the Bluetooth interference for different distances between the receiver and transmitter of the WLAN. Table 5.2 and figure 5.6 show these results.

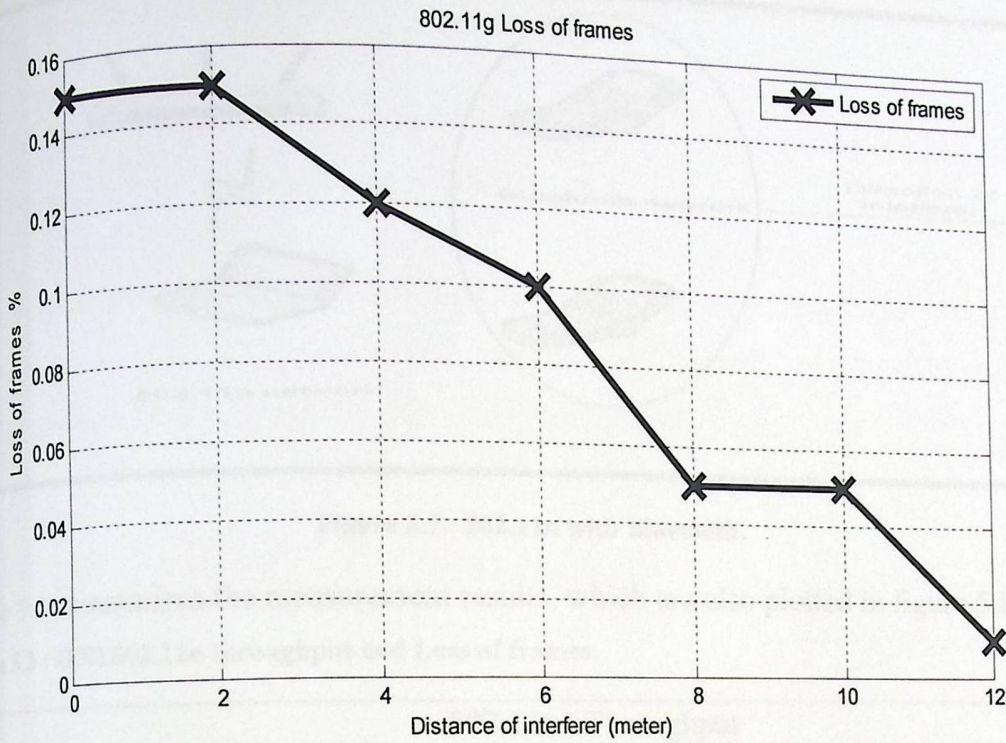


Figure 5.6: Loss of frames in 802.11g.

From figure 5.6, we can see that there is a clear effect on 802.11g networks caused by the Bluetooth network. This variation in the loss is due to distance changing of the interferer. As known, a closer interferer leads to a higher decrease in (signal to noise and interference ratio) SNIR.

5.2.3 Scenario 3 (802.11n network)

5.2.3.1 Throughput (802.11n)

In this scenario, we will measure the throughput of the 802.11n with Bluetooth interference. Figure 5.7 shows this scenario.

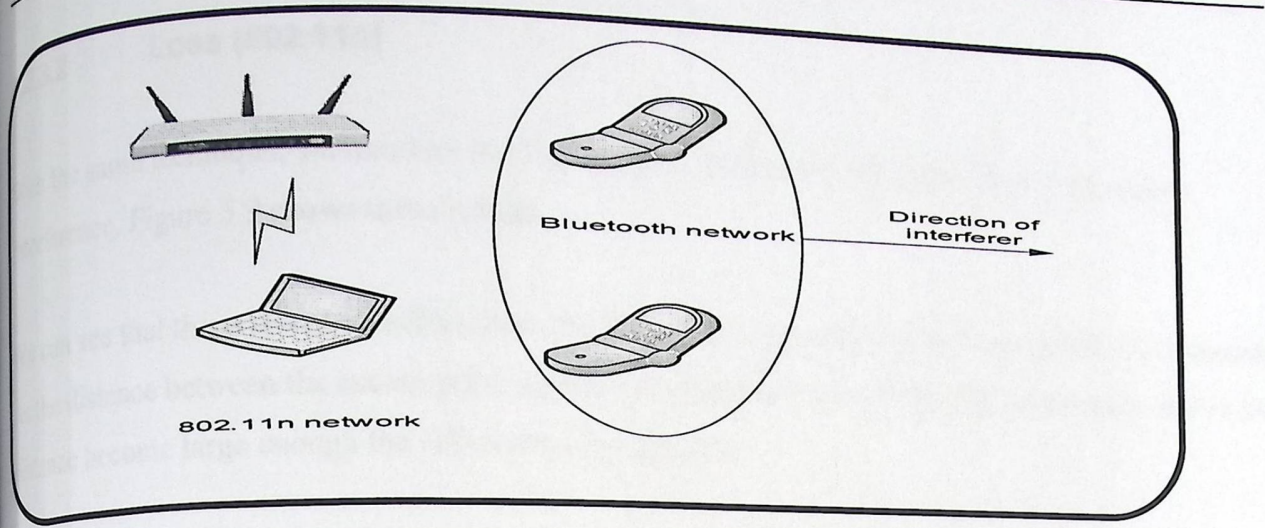


Figure 5.7 : 802.11n with Bluetooth.

Table 5.3 summarizes the measurement results, which are also plotted in figure 5.8.

Table 5.3 : IEEE802.11n throughput and Loss of frames.

802.11n Throughput							
distance of interferer (meter)	0	2	4	6	8	10	12
Throughput (Mbps)	75	80	98	140	163	165	168
Loss of frames (%)	0.45	0.35	0.2	0.1	0.05	0.05	0.03

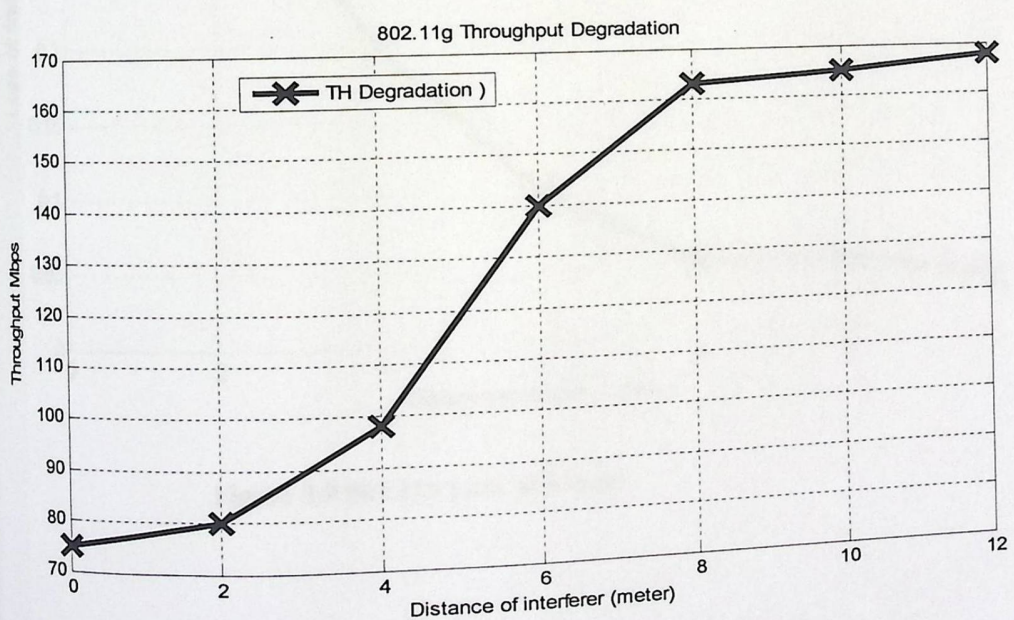


Figure 5.8 : 802.11n Throughput

As we can see from figure 5.8, it is very clear that the effect of the Bluetooth network is larger and more effectible in the case of 802.11n. The max throughput achieved is 168 Mbps and minimum throughput is 75 Mbps with the existence of Bluetooth networks in the range.

Loss (802.11n)

5.2.3.2 With the same technique, we measure the loss in 802.11n network with and without Bluetooth interference. Figure 5.9 shows these results.

We can see that there is a clear effect from the Bluetooth networks on the Loss of 801.11n network. As the distance between the access point and the interferer increased, the effect decreases, and as the distance become large enough the effect can be negligible.

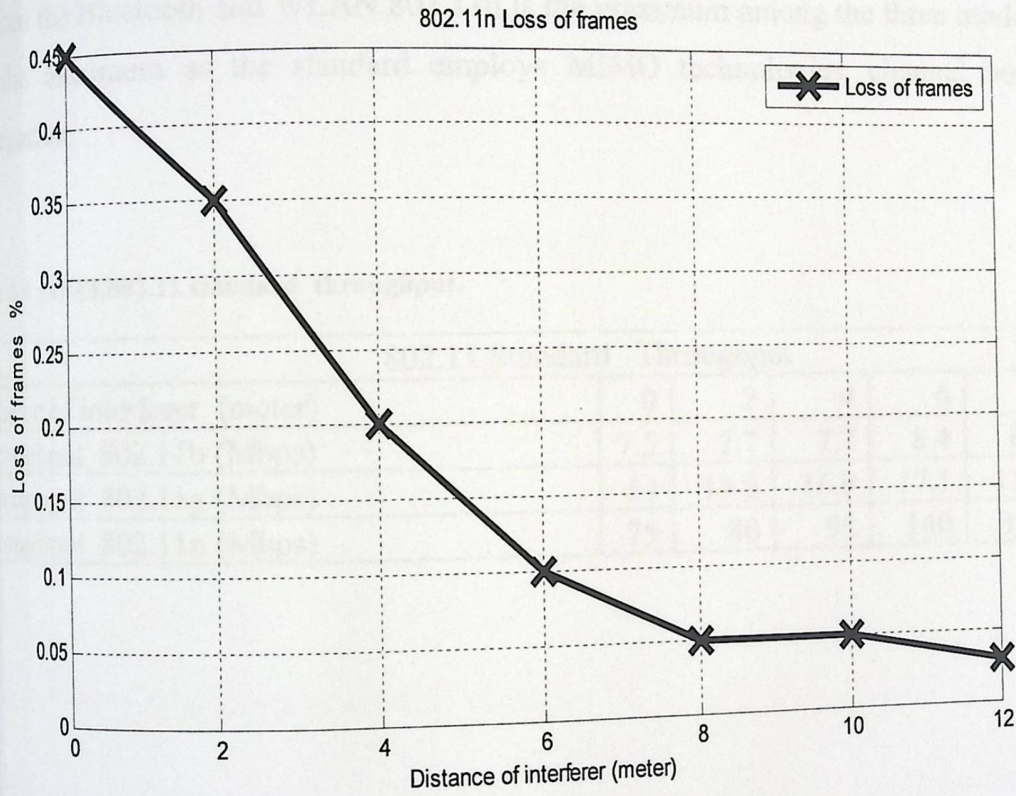


Figure 5.9 802.11n Loss of frames

5.2.4.802.11 Standard and Loss of Frames

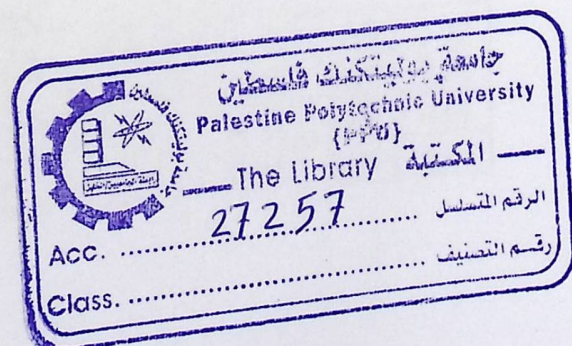
In this section, we will compare the results for the three versions of standard 802.11 together (802.11b/g/n) for both throughput and frame loss rate. Figure 5.10 shows the throughput. Figure 5.11 shows the loss of frames.

5.2.4.1 802.11 Standards Throughput

In this scenario, we plot the throughput of the three standards 802.11b/g/n, on the same plot. This is done in order to compare the results for the three modes. From figure 5.10, we can see that standard 802.11n achieves the maximum throughput among the three modes. Although the mutual effect between the Bluetooth and WLAN 802.11n is the maximum among the three modes, the throughput still the maximum as the standard employs MIMO technologies, channel bonding and frame aggregation.

Table 5.4 : IEEE802.11 standard throughput.

802.11 Standard Throughput							
distance of interferer (meter)	0	2	4	6	8	10	12
Throughput 802.11b (Mbps)	7.5	7.7	7.7	8.4	8.7	10.9	11
Throughput 802.11g (Mbps)	14	14.8	16.9	17.1	17.3	17.7	18
Throughput 802.11n (Mbps)	75	80	98	140	163	165	168



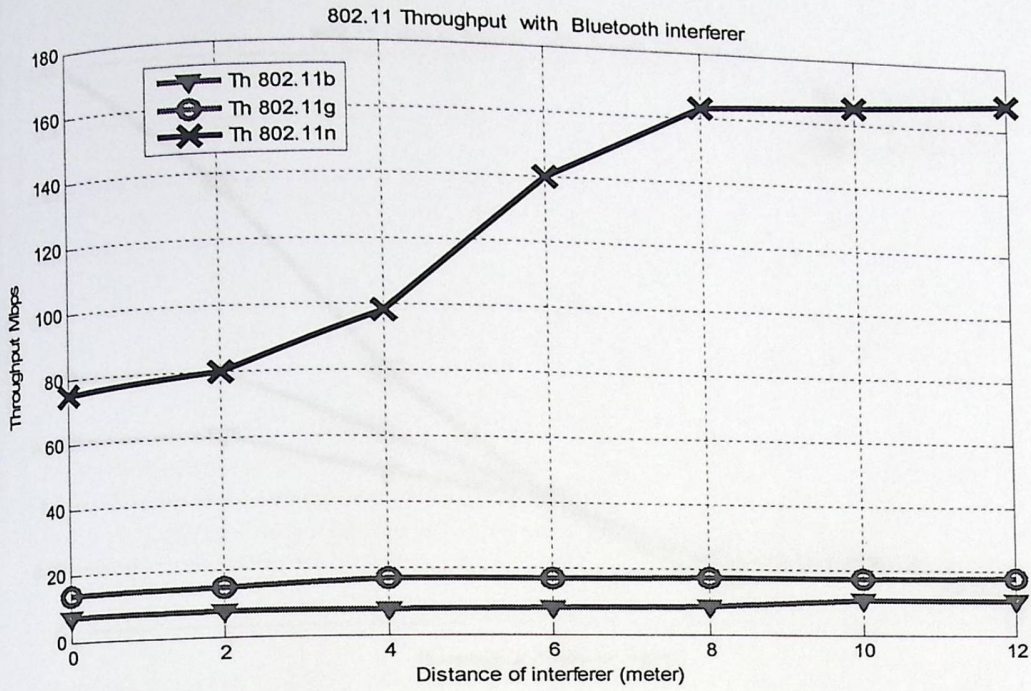


Figure 5.10 802.11 standard throughput

Figure 5.10 shows the effect of Bluetooth on 802.11 WLAN. The results show that the new high throughput MIMO-based 802.11n is mostly affected by Bluetooth interference. The throughput of the 802.11n client is degraded by about 55% when the Bluetooth operate very close. Although the figure scale does not clearly show the degradation for 802.11b/g modes due to Bluetooth interference, it is about 32% for 802.11b and 22% for 802.11g, when the Bluetooth operate very close.

5.2.4.2 802.11 Standard Loss Of Frames

As in the previous scenario, we will measure the frame loss in 802.11b/g/n modes with the existence of Bluetooth devices within the range. Table 5.5 and figure 5.11 show these results.

Table 5.5 : IEEE802.11 Loss of frames.

distance of interferer (meter)	802.11 Standard Loss of frame						
	0	2	4	6	8	10	12
Loss of frames 802.11b %	0.2	0.2	0.15	0.1	0.03	0.05	0.02
Loss of frames 802.11g %	0.15	0.15	0.12	0.1	0.05	0.05	0.01
Loss of frames 802.11n %	0.45	0.35	0.2	0.1	0.05	0.05	0.03

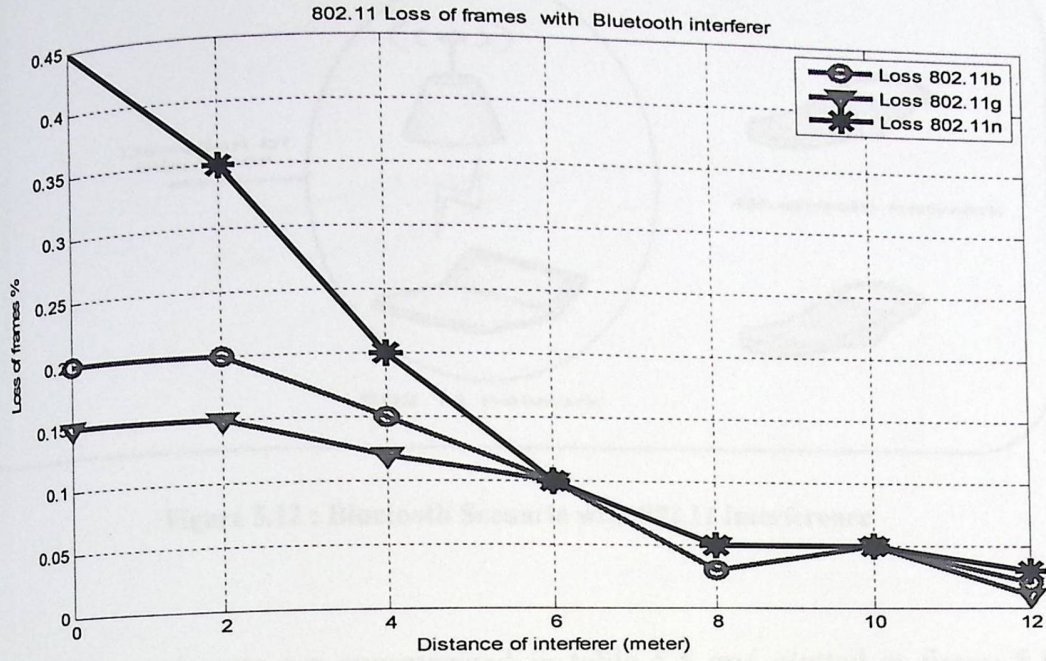


Figure 5.11 802.11 Loss of frames.

We make the following comments on this figure:

- The effect of Bluetooth networks is clear for all modes of 802.11 with different percentage.
- The amount of decrease in the 802.11n Loss is considered the most due to MIMO technology used, channel bonding and frame aggregation. But, in spite of interference, 802.11n achieves the maximum throughput.

5.3 Effect Of 802.11 On Bluetooth

5.3.1 Bluetooth Throughput With Interference (802.11)

In this experiment, it is aimed at characterizing the effect of 802.11b/g/n on a Bluetooth piconet.

We installed the piconet as shown in figure 5.12. The distance between the 802.11 transmitter and the Bluetooth receiver is varied. We measure the Bluetooth throughput for each distance.

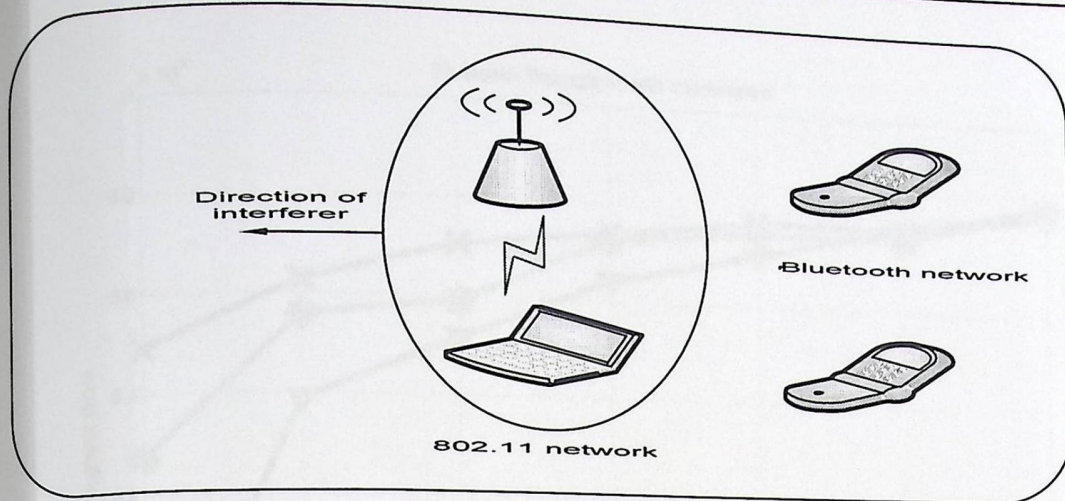


Figure 5.12 : Bluetooth Scenario with 802.11 interference

Results of these experiments are summarized in table 5.6 and plotted in figure 5.13. The results show that the Bluetooth is also influenced by 802.11b/g/n devices operating in the same area. The amount of effect does also depend on the interference distance.

Table 5.6 : Bluetooth throughput with interference.

Bluetooth throughput with interferer							
Distance (m)	0	2	4	6	8	10	12
802.11b Th (bps)	848836	862751	870535	873820	877130	877130	882478
802.11g Th (bps)	827009	855737	858911	872503	875141	875141	882479
802.11n Th (bps)	771875	838994	851332	864039	870535	877130	880465

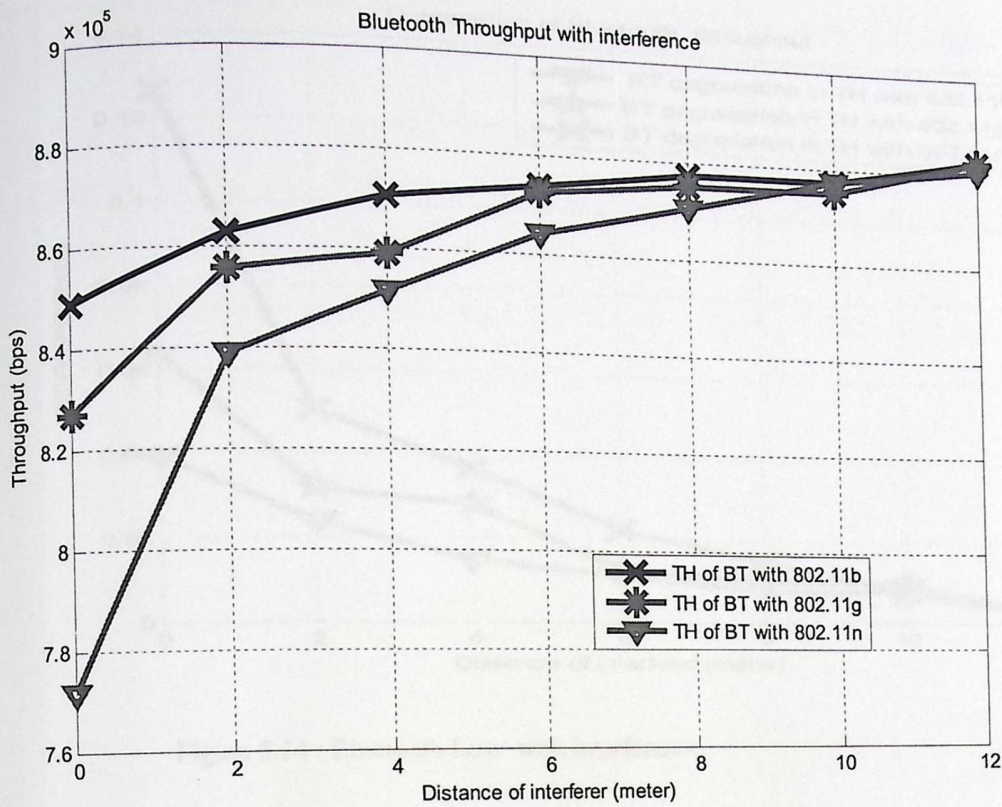


Figure 5.13 : Bluetooth Throughput with interference.

5.3.2 Bluetooth Loss With Interference (802.11)

In order to get a better idea about the effect of 802.11 on Bluetooth piconet table 5.7 and figure 5.14 show the percentage of degradation of Bluetooth network due to 802.11 interference for different distances and 802.11 modes. The results show that the maximum interference comes from the 802.11n mode, which is known to optionally use of 40 MHz band, frame aggregation and MIMO technology. The degradation for 802.11n is about 13%, the degradation is 4% and 6.3 % for 802.11b and 802.11g, respectively.

Table 5.7 : Bluetooth Loss with Interference.

Distance	Bluetooth Loss with WLAN interference						
	0	2	4	6	8	10	12
802.11b loss	0.0396	0.0239	0.015	0.0113	0.0078	0.0076	0.0015
802.11g loss	0.0643	0.0318	0.0282	0.0128	0.0098	0.0098	0.0015
802.11n loss	0.1267	0.0507	0.0368	0.0224	0.0151	0.0076	0.0038

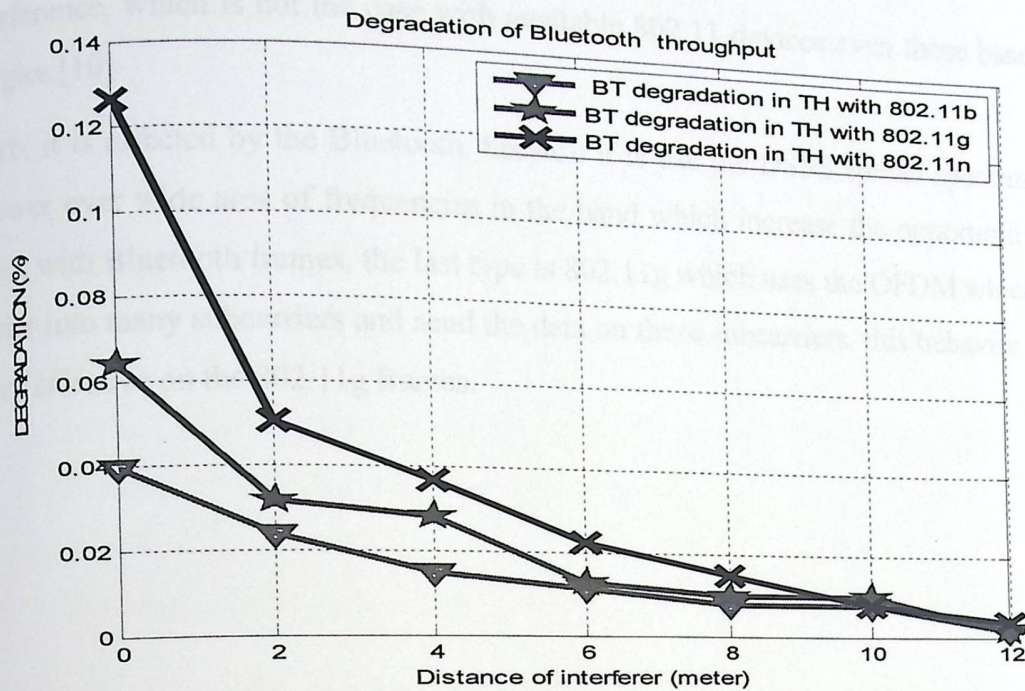


Figure 5.14 : Bluetooth Loss with interference

5.4 Summary of Results

The experimental results show that the new high throughput MIMO-based 802.11n is mostly affected by Bluetooth interference. The throughput of the 802.11n client is degraded by about 55% when the Bluetooth operate very close. Results have shown a degradation of 32% for 802.11b and 22% for 802.11g, when the Bluetooth operates very close. Finally, results have shown the effect of 802.11 WLAN on Bluetooth throughput. The Bluetooth throughput is mostly influenced by 802.11n devices. The amount of degradation is about 12.3% when the 802.11n network is operate in very close proximity. It was found to be about 4% and 6.4% for 802.11b and 802.11g, respectively. These results reveal that the effect of Wi-Fi on Bluetooth is less than the effect of Bluetooth on Wi-Fi.

We attribute these results to the following facts: **First**, the 802.11n uses 40 MHz channels instead of 20 MHz channels (channel bonding), frame aggregation and MIMO technology used which send more than one stream of data. This leads to higher probability for the Bluetooth to hop over the 802.11n channels. **Second**, 802.11n employs OFDM and SDM (spatial division multiplexing) technologies while Bluetooth uses FHSS which possibly making it more resistant to interference. **Third**, it has been noted that some Bluetooth devices utilize special internal mechanisms for

reducing interference, which is not the case with available 802.11 devices even those based on the new technologies.[10]

About 802.11b, it is affected by the Bluetooth, because it is use the DSSS spread spectrum, which spread the power over wide area of frequencies in the band which increase the opportunity to have more collisions with Bluetooth frames, the last type is 802.11g which uses the OFDM which divides the main carrier into many subcarriers and send the data on these subcarriers, this behavior make the Bluetooth very effective on the 802.11g frames.

CHAPTER 6

CONCLUSION And Future Work

This thesis studies the mutual interference between 802.11 and Bluetooth, through empirical experiments. A special focus is given to the new 802.11n devices. The results show that these devices are highly impacted by Bluetooth devices, especially when the two networks operate in close proximity to each other. The results are expected to be useful for methods that try to enable coexistence of Bluetooth and 802.11n based WLANs.

This work is expected to be useful for developing methods to overcome the effect of these systems on each other, especially when designed to be on the same device, like laptops. This is a direction for future work that can be particularly focused on mechanisms for enabling coexistence between 802.11n and Bluetooth.

From the results of this thesis we can make some suggestions for Bluetooth and 802.11n devices which can be summarized as follows:

1. To operate Bluetooth and 802.11n devices with full efficiency, it is needed to have enough distance between these devices. In this way, power received at the receiver of one technology from the other will be small and consequently will not influence the ability of receivers to decode packets correctly.
2. If Bluetooth and 802.11n have to be near each other due to any reason, mechanism for coexistence are necessary in order to enable the technologies to operate acceptably.
3. In the case of using the same hardware like designing the Bluetooth and 802.11n on the same card, the designers have to design mechanisms to enable these two technologies to operate without performance degradation.
4. Lastly, make sure to select a Wi-Fi solution today that provides an upgrade path to 802.11n.

References:

- [1] Chiasserini.C and Rao.R, (2002),” *Coexistence Mechanisms for interference mitigation between IEEE802.11 Wlan and Bluetooth*”, IEEE INFOCOM.
- [2] Cordeiro.C and Agrawal.D, (2002),” *Employing segmentation for effective collocated coexistence between Bluetooth and IEEE 802.11 WLANs*”, IEEE GLOBECOM.
- [3] Gopalet.D and Song.M, (2007), “*Performance analysis of 802.11b networks in the presence of interference-aware Bluetooth devices*”, In proceedings of QSHINE.
- [4] <http://manpages.ubuntu.com/manpages/lucid/man1/mz.1.html>
- [5] http://www.filebuzz.com/findsoftware/Bt_3620_Bluetooth_Driver/1.html
- [6] Huang.T and Ciang.S, (2006), “*Coexistence Mechanisms for Bluetooth SCO link and IEEE 802.11 WLAN*”, In proceedings of ICHIT.
- [7] I. Howitt .Ivan, Mitter.V and Gutierrez.J, (2001),” *Empirical study for IEEE 802.11 and Bluetooth inter operability*”, IEEE VTC01.
- [8] I. Howitt,Ivan , (2001),” *IEEE802.11 and Bluetooth coexistence analysis methodology*”, IEEE VTC01.
- [9] K. Premkumar, S.H. Srinivasan,(2005), “*Diversity techniques for interference mitigation between IEEE802.11 WLANs and Bluetooth*”, IEEE PIMRC.
- [10] Kumar.S, (2003),” *On the coexistence of Bluetooth and IEEE802.11 technologies in real networking environments*”, In proceedings of the 4th International conference on 3G mobile communication.
- [11] Mathew. Chandrababu.A, Elleithy.K and Rizvi.S, (2009), “*IEEE 802.11 & Bluetooth interference: simulation and coexistence*”, In proceedings of the 7th annual Communication Networks and Services Research Conference, CNSR.
- [12] N. Golmie, R.E. Van Dyck, A. Solanian, A. Tonnerre and O. Rebala, May, (2003), “*Interference Evaluation of Bluetooth and IEEE.802.11b systems*”, Journal of Wireless Networks,v.9, issue 3.
- [13] Ophir.LBitran.Y and Sherman.I, (2004), “*WIFI (IEEE802.11) and Bluetooth coexistence: issues and solutions*”, IEEE PIMRC.
- [14] Plepalli.B, Xie.W, Thangaraja.D, Hosseini.H and Bashir.Y, (2009),” *Impact of IEEE 802.11n operation on IEEE 802.15.4 operation*”, In proceedings of the International Conference on Advanced Information Networking and Applications Workshops, WAINA.
- [15] Zielinski.B, (2007), “*IEEE 802.11 network behavior in the presence of Bluetooth network*”, In proceedings of ICNC.

Appendices

Appendix A : Upuntu commands

1. Commands for installing and update wireless drivers in upunto.

```
> su
> sudo nano /etc/apt/sources.list
> sudo apt-get update && sudo apt-get upgrade
> sudo apt-get install build-essential libssl-dev
> sudo apt-get install linux-headers-`uname -r`
> sudo apt-get install subversion
> sudo svn checkout http://svn.madwifi-
project.org/madwifi/trunk/
madwifi-ng
> cd madwifi-ng
> echo "" >> /etc/modprobe.d/blacklist
> echo "#Remove To Install MadWIFI Drivers" >>
/etc/modprobe.d/blacklist
> echo "blacklist ath9k" >> /etc/modprobe.d/blacklist
> echo "blacklist ath5k" >> /etc/modprobe.d/blacklist
> make && make install
> echo ath_pci >> /etc/modules
```

2. To add a monitor interface we use the following command

```
>>iw dev wlan1 interface add ath1 type monitor
>> ifconfig ath1 up
```

3. To create a new managed mode interface we would use:

```
>> iw dev wlan1 interface add ath1 type managed
>> ifconfig ath1 up
```

Appendices

Appendix A : Upuntu commands

1. Commands for installing and update wireless drivers in upunto.

```
> su
> sudo nano /etc/apt/sources.list
> sudo apt-get update && sudo apt-get upgrade
> sudo apt-get install build-essential libssl-dev
> sudo apt-get install linux-headers-`uname -r`
> sudo apt-get install subversion
> sudo svn checkout http://svn.madwifi-
project.org/madwifi/trunk/
madwifi-ng
> cd madwifi-ng
> echo "" >> /etc/modprobe.d/blacklist
> echo "#Remove To Install MadWIFI Drivers" >>
/etc/modprobe.d/blacklist
> echo "blacklist ath9k" >> /etc/modprobe.d/blacklist
> echo "blacklist ath5k" >> /etc/modprobe.d/blacklist
> make && make install
> echo ath_pci >> /etc/modules
```

2. To add a monitor interface we use the following command

```
>> iw dev wlan1 interface add ath1 type monitor
>> ifconfig ath1 up
```

3. To create a new managed mode interface we would use:

```
>> iw dev wlan1 interface add ath1 type managed
>> ifconfig ath1 up
```

4. To delete interfaces we can use

```
>>iw dev ath1 del
```

Where ath1 is the virtual interface created in the command before.

5. Iwconfig command :

```
iwconfig - (help, version)
```

```
iwconfig [interface]
```

```
iwconfig interface [essid X] [freq F] [channel C] [sens S] [ap A] [rate R]  
[rts RT] [frag FT] [txpower T] [enc E] [key K] [retry R]
```

The first format of the iwconfig command gives a brief help message. The second format of the iwconfig command returns the current version of iwconfig along with the version of the wireless extensions with which it was built. In the third format of the iwconfig command, the current wireless status of the interface is returned. If no interface is specified, the current wireless status of every network interface is returned. Non-wireless devices will not return any wireless status. The last form of the iwconfig command allows the user to change any of the optional parameters. Only the parameters which we wish to change need to be specified. Unspecified parameters will not be modified.

6. Samples of Tshark commands :

```
>> tshark -I ath1 -t a // monitors the interface ath1 and show real time .
```

```
>> tshark -i mon0 -a -Tfields -e wlan.fc.type -e wlan.fc.retry>file name
```

Appendices

The first command monitor the interface ath1 and show the real time for the frames, the second command monitors the interface mon0 and puts the results in a file, the type of the frame and the retry bits (0 not retried 1 retried) are appeared in this file.

7. Samples of MZ generator commands :

```
>> MZ WLAN0 -d -A (source IP) -B (dest IP) -t (packet type) -p ( number of packets ) -c 20
```

This command send number of frames defined by character -c, the type of the packet defined by character -t, the source and destination address are defined by characters -A and -B simultaneously.

Mutual Interference between Bluetooth and 802.11n MIMO Devices

Murad Abusubaih and Mohammad Ayyash
Department of Electrical and
Computer Engineering
Palestine Polytechnic University
Hebron, Palestine
Email: murads@ieee.org

Abstract—802.11 Wireless Local Area Networks (WLANs) and Bluetooth are likely to be used within the same area. The two technologies operate in the 2.4 GHz band. This will result in mutual interference. The new emerging 802.11n Multi Input Multi Output (MIMO) devices implement different Physical and Medium Access Control (MAC) layers compared to legacy 802.11b/g devices. Through empirical experiments, this paper studies and presents results on the mutual impact of 802.11n and Bluetooth devices. The results show that coexistence mechanisms are crucial for the 802.11n to achieve the intended objective throughput.

I. INTRODUCTION

During the last decade, wireless local and personal area networks are widely deployed. The rapid proliferation of wireless networks has posed fundamental challenges to the design of wireless networks. The next generation of wireless networks promise to provide high speed wireless access through more advanced physical and MAC technologies. They are expected to support a variety of high quality applications. At the same time, several challenges are imposed by the wireless environment, in terms of propagation and radio resource management. Furthermore, efficient design of network components becomes even more demanding due to the scarcity of radio spectrum and the inherent transmission impairments of wireless links.

Wireless Local Area Networks (WLANs) based on the IEEE 802.11 standard are on the rise and have a wide implementation both in private and public places. IEEE 802.11 is a standard that specifies the WLAN communication in the 2.4, 3.6 and 5 GHz frequency bands. 802.11b and 802.11g use the unlicensed 2.4 GHz Industrial Scientific and Medical (ISM) band. Hence, the devices may be interfered by signals from Bluetooth, microwave ovens, and cordless telephone devices. Spread spectrum techniques are used in both Bluetooth and 802.11 equipments to control their susceptibility to interference. While 802.11b implements Direct Sequence Spread Spectrum (DSSS), 802.11g uses Orthogonal Frequency Division Multiplexing (OFDM). On the other hand, Bluetooth uses a Frequency Hopping Spread Spectrum (FHSS) signaling technique.

Though some studies have addressed the interference

between Bluetooth and 802.11 networks, these studies are limited in the sense that they focus on the impact of one technology on the other in specific limited scenarios. Also, the studies are limited to the initial versions of 802.11 like the 802.11a/b/g.

The aim of this paper is to study and analyze the mutual impact of new emerging 802.11n and Bluetooth devices through empirical controlled experiments. Though the paper focuses on 802.11n WLAN devices, other technologies such as 802.11b/g are also considered. The results are expected to be useful for methods that try to enable coexistence of Bluetooth and 802.11n based WLANs.

The rest of the paper is organized as follows: In section II, we discuss the related work. Section III provides an overview on 802.11n and Bluetooth technologies. Section IV discusses the interference between Bluetooth and 802.11n devices. In section V, we describe the setup used in the real experiments. Experimental results are provided in section VI before we conclude the paper in section VII.

II. RELATED WORK

The mutual impact of Bluetooth and 802.11 WLAN has attracted several research groups during the last decade.

The paper of [1] derived a mathematical model for evaluating the impact of Bluetooth on IEEE802.11. The approach is illustrated by examining coexistence between IEEE802.11 and Bluetooth within typical operational ranges, for both technologies regarding traffic and RF environment. In [2], the authors presented empirical results based on controlled experiments to measure the effects of interference between IEEE 802.11b and Bluetooth considering both co-channel and adjacent channel interference. In [3], the authors used simulation experiments to measure the interference between Bluetooth and IEEE 802.11 WLANs. A comparison between low and high mobility WLAN nodes shows that Bluetooth devices are strongly impacted by high mobile WLAN nodes than slow mobile ones. The paper of [4] evaluates the mutual interference between Wi-Fi and Bluetooth networks. Two different coexistence mechanisms based on traffic scheduling

techniques were proposed to reduce interference effects. In [5], the authors studied the mutual effect between Bluetooth and the 802.11 technologies. They carried out empirical experiment for different payloads. Experimental results demonstrated that a significant degradation in performance when Bluetooth communications co-exist with 802.11 WLANs for a selected set of applications. The authors also did not observe performance degradation on 802.11 wireless transmissions in the presence of interfering Bluetooth traffic. The authors of [6] study the interference between the Bluetooth and IEEE.11b systems through simulations. They concluded that power control may have limited benefits in this environment. They found that using a slower hop rate for Bluetooth may cause less interference to WLAN. Voice transmission using Bluetooth presents the worst type of interference to WLAN. In [7], the authors address WI-FI and Bluetooth coexistence through empirical experiments. They introduced a TDM-based coexistence solution and showed that no simultaneous operation of Bluetooth and WLAN can be guaranteed when the two technologies are integrated into the same device. The authors of [8] tried to mitigate the interference between IEEE 802.11 WLAN and Bluetooth through diversity techniques. In [9], the authors proposed a new non-collaborative mechanism to prevent WLAN from interfering with Bluetooth with minor modification in the 802.11 and Bluetooth standards. Reference [10] studies the performance of 802.11b networks in the presence of interference-aware Bluetooth devices through simulation. They concluded that with interference aware frequency hopping, the throughput of the 802.11b networks is improved while the probability of collision and the packet error rate are decreased significantly. The paper of [11] evaluates the behavior of IEEE 802.11 networks in the presence of Bluetooth networks. The paper published in [12] evaluates the interference between Bluetooth and IEEE 802.11 networks. The authors concluded that the interference increases as the number of nodes increases.

The most recent related work is the work published in [13]. The authors studied the impact of IEEE 802.11n operation on IEEE.15.4 devices. They concluded that the overlap in the IEEE 802.11n control channel causes severe deterioration in both loss rate and the packet latency for IEEE 802.15.4 traffic.

In this work, we contribute to the previous work by providing results of empirical experiments that characterizes the mutual interference impact between Bluetooth and the new high throughput 802.11n MIMO devices. The motivation of the work stems from the fact that these devices implements significantly different techniques both at the MAC and PHY layers.

III. OVERVIEW OF 802.11N AND BLUETOOTH

A. The 802.11n

Different from IEEE 802.11b/a/g technologies, IEEE 802.11n aims to achieve higher throughput through

enhancements at both PHY and MAC layers. The original 802.11 PHY layer specification focuses on wireless transmission. It assesses the wireless medium state and reports it back to the MAC sub-layer. The main amendments are: IEEE 802.11a, 802.11b, and 802.11g. Both 802.11a and 802.11b support raw data rates up to 11 Mb/s and 54 Mb/s, respectively. A third PHY specification for 802.11g was introduced, with maximum raw data rate of 54Mbps within the 2.4GHz band.

The MAC architecture of 802.11 is based on logical coordination functions that control medium access. In the legacy IEEE 802.11 standard, there are two types of access schemes: the mandatory distributed coordination function (DCF) and the optional point coordination function (PCF). The DCF is based on Carrier Sensing Multiple Access with Collision Avoidance (CSMA/CA) mechanism. The PCF is based on a poll-and-response mechanism.

These MAC schemes are found to be inadequate to provide acceptable quality of service (QoS) levels for voice over IP (VoIP) applications as well as audio/video conferencing. Therefore, a new extension was developed in 2005; the 802.11e. The 802.11e proposes additional service for differentiating and prioritizing traffic. In addition, IEEE 802.11e offers, the transmission opportunity (TXOP), which is an interval of time in which multiple data frames can be sent from one node to another. Further, the idea of block ACK was established. With this idea, receivers can acknowledge multiple received data frames using a single extended ACK frame.

The 802.11n PHY layer operates multiple antennas for both transmitter and receiver. MIMO provides antenna diversity and spatial multiplexing. With single input single-output (SISO) systems, multipath is typically perceived as interference degrading the ability of the receiver to recover useful information. However, a MIMO system has the ability to simultaneously resolve information from multiple signal paths using spatially separated receive antennas. Also, the 802.11n PHY layer can optionally uses 40MHz channel bandwidth to improve the theoretical capacity limits. Finally, new coding schemes have been proposed for 802.11n.

MAC enhancements have also been proposed for 802.11n. The main is the frame aggregation. It maximizes throughput and efficiency. Two aggregation types have been defined: aggregate MAC protocol service unit (A-MSDU) and aggregate MAC protocol data unit (A-MPDU).

In A-MSDU, several MSDUs destined to the same receiver are aggregated in a single MPDU. The operation is performed at the top of the MAC layer where the coming MSDUs are buffered and then aggregated in order to form A-MSDU frame. On the other hand, A-MPDU concatenates multiple MPDUs frames in a single PHY protocol data unit (PPDU)

frame. It is possible to combine frames with different traffic identifiers given that sub-frames are addressed to the same receiver. Additionally, there is no waiting time during the formation of the A-MPDU. Only the corrupted MPDUs within an A-MPDU need to be retransmitted. Multiple MPDUs are acknowledged with a single block ACK in response to a block acknowledgment request (BAR).

Another key enhancement specified for 802.11n is the bidirectional data transfer method during a single TXOP. This permits the transportation of data frames in both directions in one TXOP.

Another MAC enhancement in 802.11n is the long network allocation vector (long-NAV). It improves scheduling, given that a node that holds a TXOP may set a longer NAV value intended to protect multiple PPDU's. Another feature is the reduced IFS (RIFS). It is proposed to allow a short time interval of between multiple PPDU's, compared to SIFS defined in the legacy standards.

B. Bluetooth

Bluetooth is a radio link standard supporting short range portable device communication in an ad-hoc fashion. The system employs FHSS to combat interference and selective fading. A group of devices, which share a common channel, is called Piconet (Pico-network). One of the devices is master unit, which selects a frequency hopping sequence for the piconet and controls access to the channel by means of a polling scheme. Other devices, members of the piconet, are known as slave units.

The master chooses a different hopping sequence so that piconets can operate in the same area without interfering with each other. The slave units are synchronized to the hopping sequence of the piconet master. The system (standardized in IEEE802.15.1) operates in 2.4 GHz ISM band. It divides the 80 MHz into 79 channels. Gaussian Frequency Shift Keying (GFSK) is used for modulation. A device can send both voice and data packet with a data rate of 1Mbps. The operating range is normally 10-50 meters using a transmission power of 1mw. The technology divides the channel into slices of 625 s slots. A new hop frequency is used for each slot.

IV. MUTUAL INTERFERENCE BETWEEN 802.11N AND BLUETOOTH

The emergence of several radio technologies operating on the same 2.4 GHz unlicensed ISM frequency band, may lead to interference and mostly strong degradation in the performance of these technologies, especially when these devices are operating in the same area.

A Bluetooth or a WLAN transmitter interferes with a receiving node (WLAN or Bluetooth) because the interfering power causes a decrease in the carrier to interference ratio

at the receiver side. The interference level depend on the following main points:

- Distance between a WLAN client and the associated access point.
- Interference range of the wireless nodes.
- Network density in the area.
- Transmission power used in both the systems.
- Signal attenuation factor due to propagation

A frame collision occurs when a desired frame overlaps in time and frequency the interfering packets. Assuming continuously established links and the collocated systems are sufficiently close to each other such that the desired frame will be corrupted completely by the interference frame(s) even if they overlap by a single bit. For a long observation interval, a given transmitter uses the 79 hopping channels equally. In IEEE 802.11 DSSS system, a transmitter converts the data stream into another stream which spread over a wideband channel of 22 MHz. The collision probability of Bluetooth to IEEE 802.11 DSSS system is (22/79). However, if 802.11n is used with a 40MHz channel, the collision probability of Bluetooth to IEEE802.11n becomes (40/79).

On the other hand, the likelihood of Bluetooth devices using the interfered channel is low. WLAN applies DSSS to avoid interference and reduce noise effects. It is our objective to examine these arguments.

V. EXPERIMENTS SETUP

The goal of the empirical experiments is to obtain an estimate of the mutual interference between Bluetooth and 802.11 WLAN devices. Though our focus is on 802.11n, we also consider the other widely used modes 802.11b/g. The experimental network has been placed in typical operation environment. It is comprised of an 802.11 WLAN system (Client and AP) and a simple Bluetooth Piconet. The AP is TL-WR941N wireless N router. It is connected to a PC server used to receive the 802.11 traffic. Client is equipped with DWA-556 adapter and configured in the managed mode. Another node is used to sniff data frames. It is equipped with DWA-643 adapter based on Atheros chipset and configured in the monitor mode. The Bluetooth system is based on BT-3620. The MZ traffic generator is used to generate 802.11 traffic. File transfer is used for the Bluetooth network. We measure the throughput of both networks, using the T-Shark and BlueSoleil measurement tools for 802.11 and Bluetooth, respectively.

A. Effect of Bluetooth on 802.11

The scenario used in the experiments is shown in figure 1. We set up a connection between the client and the wireless AP. The client sends traffic to the APs. We also deployed a Bluetooth sender and receiver in the same area. Distance between each sender (Either Bluetooth or 802.11) and the corresponding receiver is fixed to 5m. Then we repeated the experiments changing the distance between the Bluetooth sender and the 802.11 AP (Receiver) in order to examine the

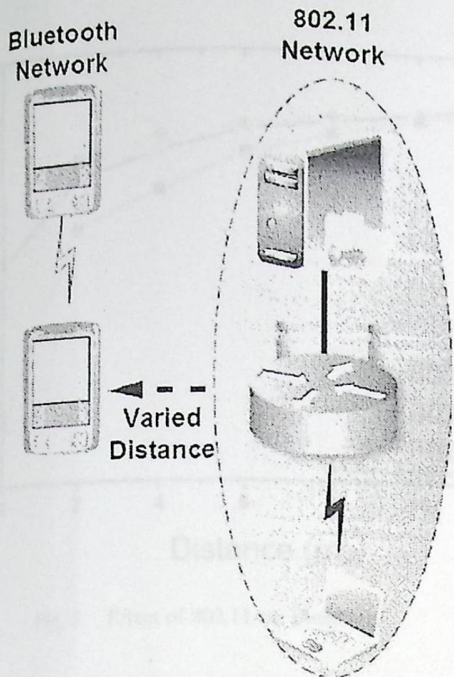


Fig. 1. Effect of Bluetooth on 802.11 - Experiment Setup

distance beyond which the Bluetooth starts not affecting the 802.11.

B. Effect of 802.11 on Bluetooth

Similar to the previous setup. We setup a connection between a Bluetooth sender and receiver as shown in figure 2. We also deployed the 802.11 system in the same area. In this

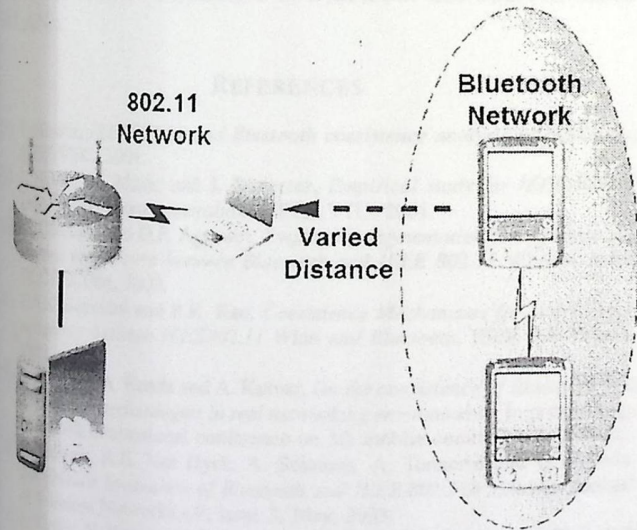


Fig. 2. Effect of 802.11 on Bluetooth - Experiment Setup

experiment, we vary the distance between the 802.11 sender (interferer) and the Bluetooth receiver.

VI. RESULTS

Figure 3 shows the effect of Bluetooth on 802.11 WLAN. The results show that the new high throughput MIMO-based

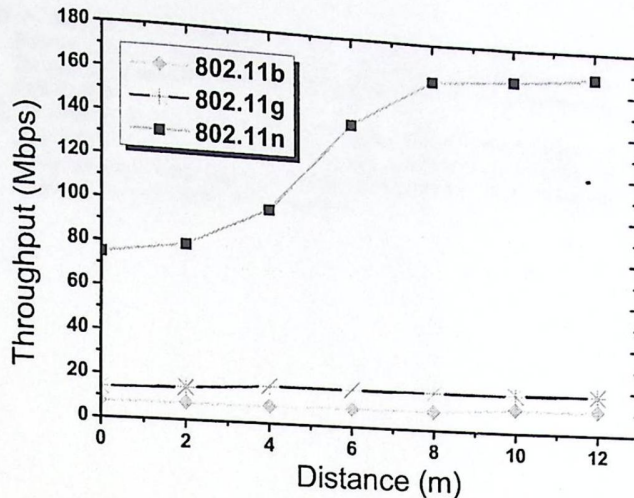


Fig. 3. Effect of Bluetooth on 802.11

802.11n is mostly affected by Bluetooth interference. The throughput of the 802.11n client is degraded by about 55% when the Bluetooth operate very close. Although the figure scale does not clearly show the degradation for 802.11b/g modes due to Bluetooth interference, it is about 32% for 802.11b and 22% for 802.11g, when the Bluetooth operate very close. Figure 4 plots the percentage of frame loss due to Bluetooth interference for the three modes. It has been

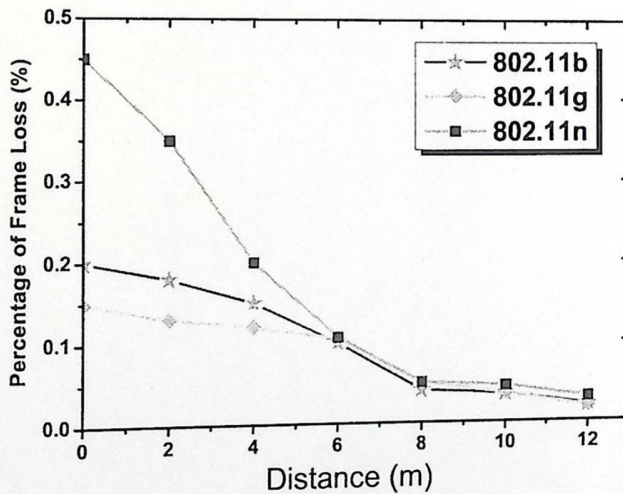


Fig. 4. Effect of Bluetooth on 802.11

computed by analyzing frames content (the retry field) at the receivers' side. Finally, figure 5 shows the effect of 802.11 WLAN on Bluetooth throughput. The results show that the Bluetooth throughput is mostly influenced by 802.11n devices. The amount of degradation is about 12.3% when the 802.11n network is operate in very close proximity. It was found to be about 4% and 6.3% for 802.11b and 802.11g, respectively. These results reveal that the effect of Wi-Fi on Bluetooth is

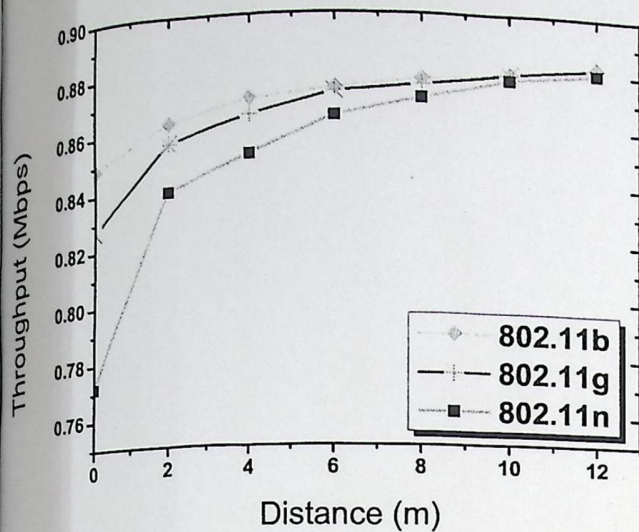


Fig. 5. Effect of 802.11 on Bluetooth

- [12] A. Mathew, N. Chandrababu, K. Elleithy and S. Rizvi, *IEEE 802.11 & Bluetooth interference: simulation and coexistence*, In proceedings of the 7th annual Communication Networks and Services Research Conference, CNSR, 2009.
- [13] B. Plepalli, W. Xie, D. Thangaraja, H. Hosseini and Y. Bashir, *Impact of IEEE 802.11n operation on IEEE 802.15.4 operation*, In proceedings of the International Conference on Advanced Information Networking and Applications Workshops, WAINA, 2009.

less than the effect of Bluetooth on Wi-Fi.

VII. CONCLUSION

This paper studies the mutual interference between 802.11 and Bluetooth, through empirical experiments. A special focus is given to the new 802.11n devices. The results show that these devices are highly impacted by Bluetooth devices, especially when the two networks operate in close proximity to each other. The results are expected to be useful for methods that try to enable coexistence of Bluetooth and 802.11n based WLANs.

REFERENCES

- [1] I. Howitt, *IEEE802.11 and Bluetooth coexistence analysis methodology*, IEEE VTC, 2001.
- [2] I. Howitt, V. Mitter and J. Gutierrez, *Empirical study for IEEE 802.11 and Bluetooth inter operability*, IEEE VTC, 2001.
- [3] C. Cordeiro and D.P. Agrawal, *Employing segmentation for effective co-located coexistence between Bluetooth and IEEE 802.11 WLANs*, IEEE GLOBECOM, 2002.
- [4] C.F. Chiasserini and R.R. Rao, *Coexistence Mechanisms for interference mitigation between IEEE802.11 Wlan and Bluetooth*, IEEE INFOCOM, 2002.
- [5] S. Zeadally, A. Banda and A. Kumar, *On the coexistence of Bluetooth and IEEE802.11 technologies in real networking environments*, In proceedings of the 4th International conference on 3G mobile communication, 2003.
- [6] N. Golmie, R.E. Van Dyck, A. Solanian, A. Tonnerre and O. Rebala, *Interference Evaluation of Bluetooth and IEEE.802.11b systems*, Journal of Wireless Networks, v.9, issue 3, May, 2003.
- [7] L. Ophir, Y. Bitran and I. Sherman, *WiFi (IEEE802.11) and Bluetooth coexistence: issues and solutions*, IEEE PIMRC, 2004.
- [8] K. Premkumar, S.H. Srinivasan, *Diversity techniques for interference mitigation between IEEE802.11 WLANs and Bluetooth*, IEEE PIMRC, 2005.
- [9] T. Huang and S. Ciang, *Coexistence Mechanisms for Bluetooth SCO link and IEEE 802.11 WLAN*, In proceedings of ICHIT, 2006.
- [10] D. Gopalet and M. Song, *Performance analysis of 802.11b networks in the presence of interference-aware Bluetooth devices*, In proceedings of QSHINE, 2007.
- [11] B. Zielinski, *IEEE 802.11 network behavior in the presence of Bluetooth network*, In proceedings of ICNC, 2007.