

CO-CHANNEL INTERFERENCE BETWEEN
IEEE 802.11 WLAN AND
BLUETOOTH

By

SHADI HANNOUF

Bachelor of Science

University of Balamand

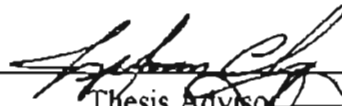
Tripoli, Lebanon

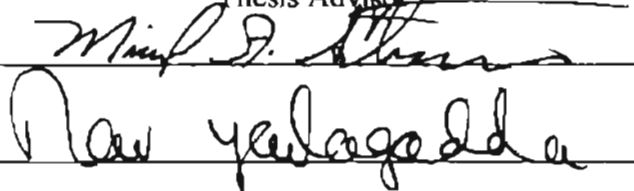
1999


Submitted to the Faculty of the
Graduate College of the
Oklahoma State University
in partial fulfillment of
the requirements for
the Degree of
MASTER OF SCIENCE
August, 2001

CO-CHANNEL INTERFERENCE BETWEEN
IEEE 802.11 WLAN AND
BLUETOOTH

Thesis Approved:



Thesis Advisor


Dean of the Graduate College


Dean of the Graduate College

PREFACE

For clear understanding of this subject, a reader should have knowledge of Direct Sequence and Frequency Hopping Spread Spectrum schemes. This report is based on a lot of research in the above-mentioned areas. The idea has been provoked by a simple accidental interference problem that has occurred during some lab experiments. One can easily implement a co-channel interference experiment at any indoor enterprise by using any software that would measure throughput and shows actual signal graphics.

My thanks for my dear professor, Dr. Jong-Moon Chung, who has given me a great motivation in the time of need. Also, my thanks to my dear colleagues at our research group; not to forget Sriram for his inspiration at many times.

Table of Contents

Chapter		Page
I.	Introduction	1
	1.1 IEEE 802.11	2
	1.2 Bluetooth	2
	1.3 Potential Interference: Bluetooth and IEEE 802.11	3
	1.4 Thesis Outline.....	4
II.	A- IEEE 802.11	5
	2.A.1 General Description of the Architecture	5
	2.A.2 Components of the IEEE 802.11 Architecture.....	6
	2.A.3 Logical Service Interfaces.....	9
	2.A.4 Overview of the Services.....	12
	2.A.5 Relationship Between Services.....	17
	2.A.6 Difference Between ESS and IBSS LANs.....	19
	2.A.7 Message Information Contents That	20
	Support the Services	
	2.A.8 MAC Service Definition.....	24
	2.A.9 Frame Formats.....	25
	2.A.10 Complementary Code Keying.....	30
	B-Bluetooth	33
	2.B.1 Bluetooth Radio System Architecture.....	33
	2.B.2 Interpiconet Communications.....	38
	2.B.3 Physical Link Definition.....	40
	2.B.4 Packet Definition.....	41
	2.B.5 Error Correction.....	47
	2.B.6 Connection Establishment.....	49
	2.B.7 Hop Selection Mechanism.....	50
	2.B.8 Power Management.....	53

Chapter	Page
II.	
2.B.9 Security.....	54
C-Performance of Spread Spectrum Techniques	56
2.C.1 Direct Sequence Spread Spectrum	57
2.C.2 Frequency Hopping Spread Spectrum	61
2.C.3 Comparison between DS and FH.....	63
2.C.4 Multiple Access Interference in a	66
Hybrid System with a FSK Scheme	
2.C.5 Multiple Access Interference in a Hybrid	69
System with QPSK Scheme	
2.C.6 Narrow Band Interference in a	73
Hybrid System with a BPSK Scheme	
III. Broad Study of Interference	76
3.1 Approaching Interference from Other Users.....	76
3.2 Correlator's Process.....	83
3.3 CDMA with Other Digital Modulations and Coding.....	89
IV. Timing Considerations for Co-channel Interference between WLAN and Bluetooth	91
4.1 Previous Work	91
4.2 Recap of Bluetooth Radio Technology	92
4.3 Bluetooth and IEEE 802.11 Coexisting	93
4.4 Power and Probability Analysis	94
4.5 Packet Timing Discussion	97
4.6 WLAN Packet Error	99
4.7 Performance of WLAN Among	100
Bluetooth Piconets	
4.7.1 Voice Discussion.....	100
4.7.2 Traffic Implementations on WLAN.....	104
4.7.3 Data Discussion.....	105
4.7.4 Traffic Implementations on.....	106
Bluetooth	

Chapter	Page
V.	Discussion and Observations
	5.1 IEEE 802.11b..... 108
	5.2 Channel Overlap with Bluetooth..... 118
	5.3 Probability of Bit Error.....119
	5.4 Adaptive Frequency Hopping..... 121
	5.5 The Automatic Interference Rejection 129
	System for Bluetooth and IEEE 802.11b Systems
VI.	Conclusion 138
	References..... 141

LIST OF FIGURES

Figure	Page
2.1	Components of an IEEE 802.11 Architecture..... 7
2.2	ESS Components Including Portals..... 8
2.3	Distribution of Services..... 10
2.4	States and Classes..... 18
2.5	IBSS Network..... 19
2.6	MAC Frame Format..... 26
2.7	Frame Control Field..... 26
2.8	Bluetooth System..... 33
2.9	Time Slots..... 35
2.10	Example of Piconet Structure..... 39
2.11	Packet Format..... 41
2.12	Channel Access Code..... 42
2.13	Header..... 42
2.14	Hop Selection Mechanism..... 52
2.15	Spread Spectrum System..... 57
2.16	DSSS Transmitter..... 59
2.17	DSSS Receiver..... 60
2.18	Hybrid System Model..... 67
3.1	DS/CDMA System Model..... 77
3.2	DS/CDMA Coherent Correlation Receiver..... 78
3.3	Effect of Multi-user Interference on QPSK DSSS..... 80
3.4	Effect of Narrow-Band Jamming on DSSS-BPSK..... 81
3.5	Effect of Wide-Band Jamming on DSSS-BPSK..... 82
3.6	Effect of Pulsed Interference on DSSS..... 83
3.7	Discrete Aperiodic CrossCorrelations..... 85
3.8	Probability of Bit Error via Standard Gaussian Approximation..... 87
3.9	Capacity of DS/CDMA..... 89
4.1	Topology Considered..... 94
4.2	Overlap of WLAN and Bluetooth Packets..... 97
4.3	Packet Error Probability of WLAN for a BT Voice Link..... 102
4.4	WLAN Throughput vs. Packet Size in Bytes..... 103
4.5	Performance of IEEE 802.11 in Data Bluetooth Environment..... 106
5.1	Sketch of an ad hoc Network..... 110
5.2	Sketch of an Infrastructure Network..... 111
5.3	North American Channel Selection – Overlapping..... 115
5.4	Three AP's with Overlapping Coverage..... 117

Figure	Page
5.5	Frequency Overlap between IEEE 802.11b..... 118 Channel 1 and Bluetooth Spectrum
5.6	Frequency Overlap between IEEE 802.11b.....120 Channels 1 and 6 and Bluetooth Spectrum
5.7	Frequency Overlap between IEEE 802.11b.....121 Channels 1, 6, and 11 and Bluetooth Spectrum
5.8	Zander <i>et al</i> AFH Model..... 122
5.9	Gillis et al. Adaptive Frequency Hopping Scheme..... 123 of a Cordless Telephone System
5.10	Short Cycle..... 125
5.11	Longer Cycle.....125
5.12	Structure of AFH..... 128
5.13	Device Identification and Operation Mode for AFH.....129
5.14	The Automatic Interference Rejection System (AIRS).....130 For Bluetooth and IEEE 802.11b
5.15	The BER Performance of Bluetooth with IEEE 802.11b..... 133 Interference and AWGN
5.16	The BER Performance of IEEE 802.11b with Bluetooth..... 135 Interference and AWGN

LIST OF TABLES

Table		Page
4.1	Interfering Bluetooth Users Statistics.....	95
5.1	IEEE 802.11b Various Rate Characteristics.....	109
5.2	DSSS PHY Frequency Channel.....	116

Chapter I

Introduction

Most industry experts agree that the number of products incorporating the recently approved Bluetooth wireless standard will explode during the first couple of years of the new millennium. Bluetooth, which establishes wireless connections between devices such as mobile phones, PDAs, and headsets, operates at relatively low data rates over short distances using very little power. On the other hand, IEEE 802.11 is a wireless LAN standard approved by IEEE a couple of years ago and operates at higher data rates over longer distances using more power. Companies today are strongly benefiting from using 802.11 – compliant wireless LANs to support efficient mobile communications between handheld data collectors and corporate IS databases.

The IEEE 802.11b wireless LAN systems featured in this paper use radios in the 2.4-GHz frequency band – the same band used by microwave ovens. The advantages of this band are that it provides a lot of spectrum space and doesn't require licensing of the radio devices. But the same advantages attract several other types of portable data devices that could interfere with each other. Driven by images of big revenues from wireless data connectivity, the companies backing these products have polarized into camps, have hired attorneys, and making technical arguments before the FCC. The result is likely to be a technical compromise, but arriving at that compromise might delay some very useful products.

1.1 IEEE 802.11

The initial 802.11 PAR (Project Authorization Request) states, "... the scope of the proposed wireless LAN standard is to develop a specification for wireless connectivity for fixed, portable, and moving stations within a local area." The PAR further says, "...the purpose of the standard is to provide wireless connectivity to automatic machinery and equipment or stations that require rapid deployment, which may be portable, handheld, or which may be mounted on moving vehicles with a local area."

The resulting standard, which is officially called "IEEE Standard for Wireless LAN Medium Access (MAC) and Physical Layer (PHY) Specifications," defines over-the-air protocols necessary to support networking in local area. As with other IEEE 802-based standards (e.g. 802.3 and 802.5), the primary service of the 802.11 standard is to deliver MSDUs (MAC Service Data Units) between peer LLCs (Logical Link Controls). Typically, a radio card and access point provides functions of the 802.11 standard.

1.2 Bluetooth

Bluetooth is a plan for inexpensive, very low powered and short-range frequency-hopping radio system that would link your pagers, personal access devices, cell phones, and laptops. This link could, for example, provide your laptop with access to the Internet through your cell phone or let you synchronize data across your cell phone, PDA, and notebook. In a more advanced scenario, Bluetooth devices connect to fast access points in

public facilities such as airports and arenas. Devices like these could and one day likely will verify your identity and guide you to your boarding gate, rental car, or stadium seat.

The Bluetooth pavilion at the Consumer Electronics Show in Las Vegas in January 1999 was a busy place, with demonstrations of ISDN-to-Bluetooth, DSL-to-Bluetooth, USB-to-Bluetooth, and automobile-to-Bluetooth devices, to name a few of the many. Ideally, these devices should become available in the third quarter of 2000. In a recent study, Frost & Sullivan predicted “ gargantuan growth” for Bluetooth-based devices and technology, with sales of \$36.7 million in 2000 and \$699.2 million by 2006.

1.3 - Potential Interference: Bluetooth and IEEE 802.11

Unfortunately, there could be a speed bump. Bluetooth uses very low transmission power, about 0.01W, so more powerful devices may be able to overwhelm its signal. The plan is for Bluetooth to hop around local interference sources, like a microwave oven, using a fast frequency-hopping scheme (about 1600 hops per second spread over 79 channels). But that frequency-sharing scheme might sometimes bump into ratios using the 802.11b WECA direct-sequence scheme if they're nearby. Because of a high demand for both wireless PANs and LANs, it's important that Bluetooth and 802.11 coexist in proximity. Interference happens when Bluetooth and 802.11 devices transmit at the same time near each other. This causes a destruction of data bits, prompting the system to retransmit entire data packets. As a result, the interference lowers throughput of the system and presents sluggish performance to end-users. The likelihood is that Bluetooth products

will likely jam the operation of 802.11, not the other way around. The reason is that Bluetooth hops through frequencies 600 times faster than 802.11. While an 802.11 device is transmitting on a particular frequency, a nearby Bluetooth product will most likely interfere with 802.11 transmission many times before the 802.11 device hops to the next frequency. This barrage of radio signals emanating from Bluetooth products could seriously degrade the operation of an 802.11 network. The potential for interference, particularly to the low-powered Bluetooth, remains an open problem.

1.4 Thesis Outline

All the above provoked the need for this research. Later in this paper, I will present in Chapter II a quick literature review of Bluetooth and IEEE 802.11, and performance of Frequency Hopping (FH) and Direct Sequence (DS) schemes. Appendices A, B, C, and D conveys a lot of very good material attached to Chapter II, which could help much in understanding WLAN technology, Bluetooth, and other interference issues. Chapter III gives a broad study of interference within FH and DS. Chapter IV is the actual approach of conquering interference between Bluetooth and IEEE 802.11. Chapter V gives the observations and results. Chapter VI gives a conclusion of the research and suggestions for future work.

Chapter II

Literature Review

2.A IEEE 802.11

2.A.1 General Description of the Architecture

In IEEE 802.11 wireless networks, the addressable unit is a station (STA). The STA is a message destination, but not (in general) a fixed station. The physical layers, PHY, used in IEEE 802.11 use a medium that has neither absolute nor readily observable boundaries outside of which stations with conformant PHY transceivers are known to be unable to receive network frames. The medium, thus, is not much reliable and depend much on dynamic topologies. An IEEE 802.11 wireless network lack full connectivity because of the dynamic topologies, it has time-varying and asymmetric propagation properties.

One of the requirements of IEEE 802.11 is to handle *mobile* as well as *portable* stations. A portable station is one that moves from location to location, but is only used while at fixed location. Mobile stations actually access the LAN while in motion. An IEEE 802.11 network handles station mobility within the MAC layer.

2.A.2 Components of the IEEE 802.11 architecture

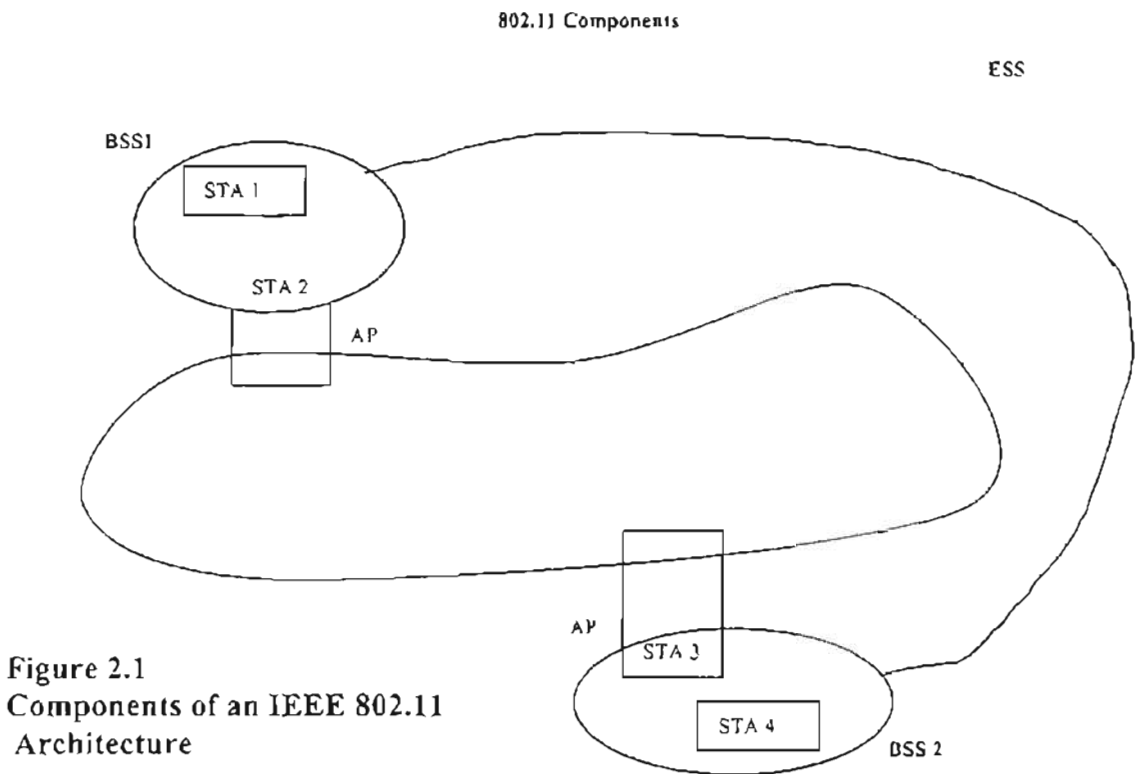
The IEEE 802.11 architecture consists of several components that interact to provide a wireless LAN that supports station mobility transparently to upper layers. The *basic service set*, BSS, is the basic building block of an IEEE 802.11 LAN. The ovals used to depict a BSS designate the coverage area within which the member stations of the BSS may remain in communication. If a station moves out of its BSS, it can no longer directly communicate with other members of the BSS. The independent BSS, IBSS, is the most basic type of IEEE 802.11 LAN. A minimum IEEE 802.11 LAN may consist of only two stations. This type of IEEE 802.11 LAN, often referred to as an ad-hoc network, is often formed without pre-planning, for only as long as the LAN is needed.

STA to BSS association is dynamic. To become a member of an infrastructure BSS, a station shall become “associated”. These associations involve the use of the distribution system service, DSS. PHY limitations determine the direct station-to-station distance that may be supported.

Instead of existing independently, a BSS may also form a component of an extended form of network that is built within multiple BSSs. The architectural component used to interconnect BSSs is the distribution system, DS. IEEE 802.11 logically separates the *wireless medium*, WM, from the *distribution system medium*, DSM. Each logical medium is used for different purposes, by a different component of the architecture. This provides flexibility to the architecture. The DS enables mobile device support by

providing the logical services necessary to handle address to destination mapping and seamless integration of multiple BSSs.

An access point, AP, is an STA that provides access to the DS by providing DS services in addition to acting as a STA. Data moves between a BSS and the DS via an AP (see figure below). Note that all APs are also STAs; thus they are addressable entities. The addresses used by an AP for communication on the WM and on the DSM are not necessarily the same.



The DS and BSSs allow IEEE 802.11 to create a wireless network of arbitrary size and complexity. This is referred to as the *extended service set*, ESS, network. The

key concept is that the ESS network appears the same to an LLC layer as an IBSS network. Stations within an ESS may communicate and mobile stations may move from one BSS to another, within the same ESS, transparently to LLC. The extended service set is shown in above figure. The BSSs may partially overlap, may be physically disjointed, or may be physically collocated. One or more ESS networks may be physically present in the same space as one or more ESS networks.

To integrate the IEEE 802.11 architecture with a traditional wired LAN, a final logical architectural component, a *portal*, is introduced. A portal is the logical point at which MSDUs from an integrated non-IEEE 802.11 LAN enter the IEEE 802.11 DS. All data from non-IEEE 802.11 LANs enter the 802.11 architecture via a portal. It is possible for one device to offer both the functions of an AP and a portal (figure below).

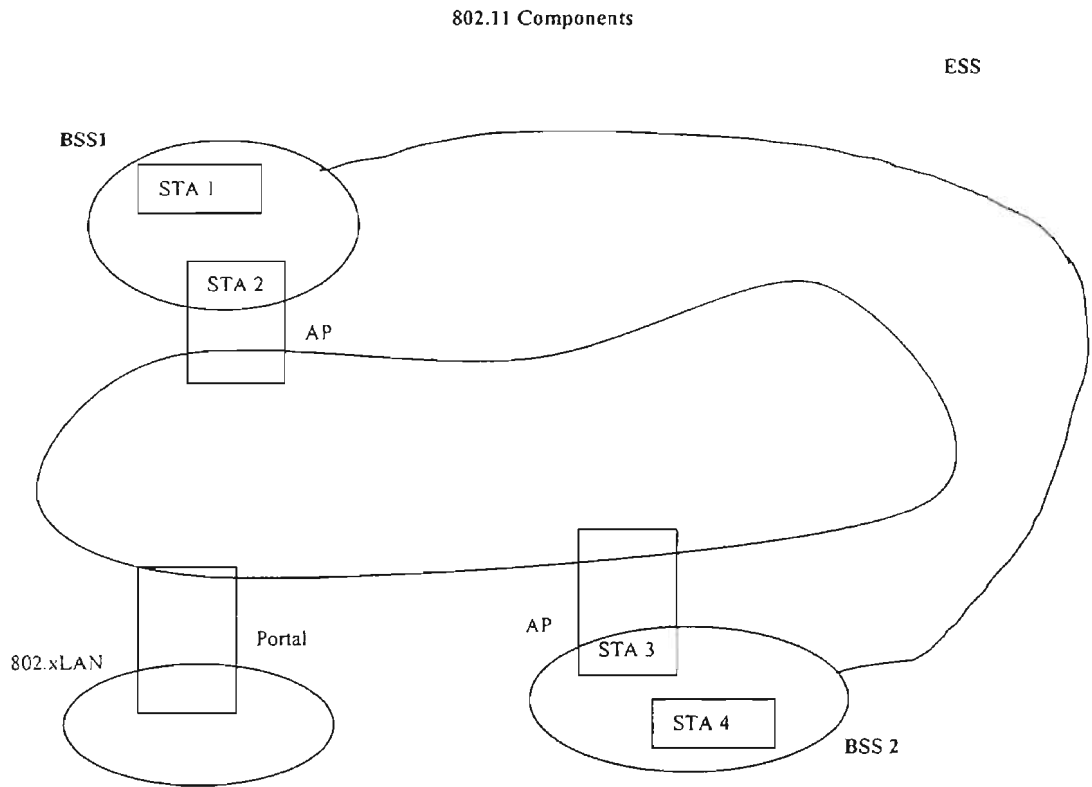


Figure 2.2 ESS Components Including Portals

2.A.3 Logical Service Interfaces

A DS may be created from many different technologies including current 802 wired LANs. IEEE 802.11 does not constrain the DS to be either data link or network layer based, nor does it constrain a DS to be either centralized or distributed in nature. IEEE 802.11 only specifies services associated with different components of the architecture. There are two categories of IEEE 802.11 services: the *station service*, SS, and the *distribution system service*, DSS. The IEEE 802.11 MAC layer uses both categories. The complete set of IEEE 802.11 architectural services are as follows: *Authentication, Association, Deauthentication, Disassociation, Distribution, Integration, Privacy, Reassociation, and MSDU delivery.*

The station service, SS, is present at every station; it's specified by MAC sublayer entities. The SS is as follows: *Authentication, Deauthentication, Privacy, and MSDU delivery.*

The DS provides the distribution system service, DSS. It's also specified for use by MAC sublayer entities. These services are represented by arrows within the APs. The arrows indicate that the services are used to cross media and address space logical boundaries. DSSs are accessed via an STA that also provides DSSs i.e. an AP. The DSSs are as follows: *Association, Disassociation, Distribution, Integration, and Reassociation.*

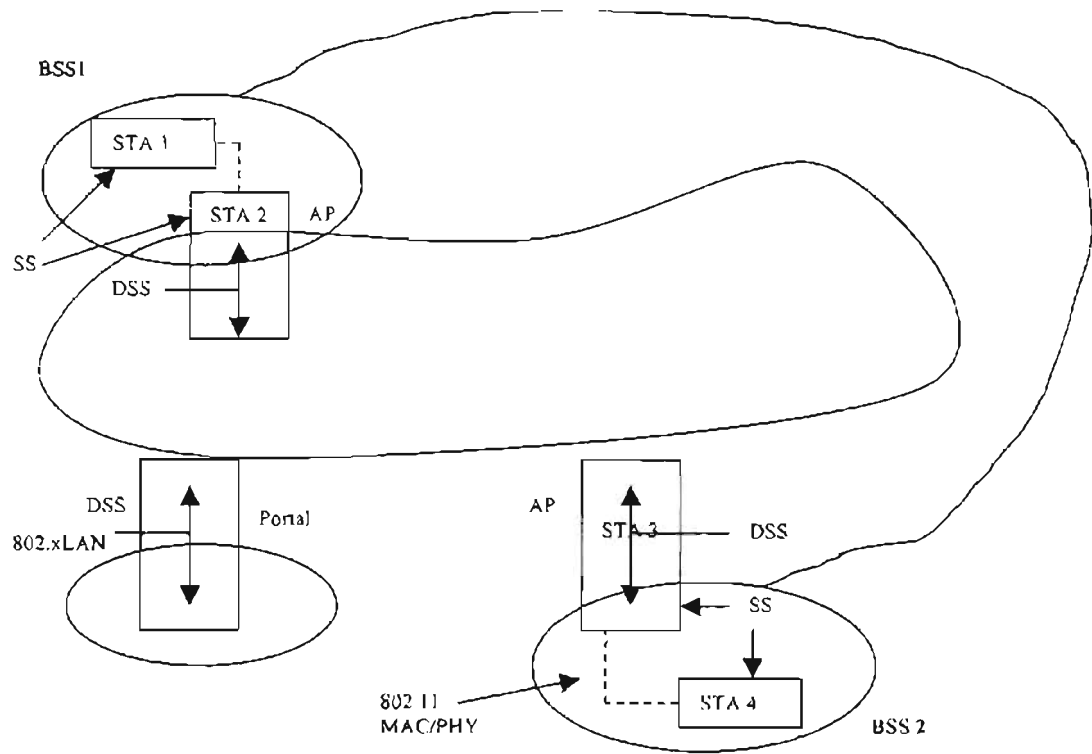


Figure 2.3 Distribution of Services

WM, DSM, and an integrated wired LAN may all be different physical media in the IEEE 802.11 architecture. Also, each of these components may be operating within different address spaces. IEEE 802.11 only uses and specifies the use of the WM address space. Each IEEE 802.11 PHY operates in a single medium, which is the WM. The IEEE 802.11 MAC operates in a single address space. MAC addresses are used on the WM.

IEEE 802.11 has chosen to use the IEEE 802 48-bit address space. Therefore, IEEE 802.11 addresses are compatible with the address space used by the 802 LAN family. This choice of address space implies that the wired LAN MAC address space and the IEEE 802.11 address space may be the same. Still, IEEE 802.11 allows for all three logical address spaces to be distinct. A multiple address space example is one where the DS implementation uses network layer addressing. In this case, the WM address space and the DS address space would be different.

2.A.4 Overview of the services of IEEE 802.11

Each of the services is supported by one or more MAC frame types. Some of the services are supported by MAC *management messages* and some by MAC *data messages*. The IEEE 802.11 MAC sublayer uses three types of messages: *data*, *management*, and *control*. The data messages are handled via the MAC *data service path*. The management messages are handled via the MAC *management service data path*. The control messages are used to support the delivery of IEEE 802.11 data and management messages.

2.A.4.1 Distribution of messages within a DS

2.A.4.1.a Distribution

It's invoked by every data message to or from an IEEE 802.11 STA operating in an ESS. A data message, being sent from STA 1 to STA 4, should be sent from STA 1 to STA 2 (the input AP). The AP gives the message to the distribution service of the DS, which in turn deliver the message within the DS in such a way that it arrives at the appropriate DS destination for the intended recipient. The message is distributed to STA 3 (the output AP) and STA 3 accesses the WM to send the message to STA 4. IEEE 802.11 doesn't specify how the DS delivers the message. The necessary information is provided to the DS by the three association related services (association, reassociation, and disassociation). Note that if the message had been intended for a station that was a

member of the same BSS as the sending station, then the input and output APs for the message would have been the same. In both of the above cases, the distribution service was logically invoked, irrespective of traversing the physical DSM or not.

2.A.4.1.b Integration

Once the distribution service determines that the intended recipient of a message is a member of an integrated LAN, the output point of the DS would be a portal instead of an AP. This kind of messages cause the DS to invoke the Integration function, which is responsible for accomplishing whatever is needed to deliver a message from the DSM to the intended LAN media.

2.A.4.2 Services that support the distribution service

The primary purpose of a MAC sublayer is to transfer MSDUs between MAC sublayer entities. The information required for the distribution service to operate is provided by the association services. Association can only be understood by knowing the mobility types. There are three mobility types: *No-transition (static, local movement)*, *BSS-transition*, and *ESS-transition*.

2.A.4.2.a Association

The concept of association provides to the DS what the distribution service needs to know which AP to access for the given IEEE 802.11 STA. Association is a DSS. An STA should be associated to an AP before it is allowed to send a data message via an AP. The association service provides the STA-to-AP mapping to the DS. An STA may be associated with no more than one AP at any given instant. Association is always associated by the mobile STA, not the AP. An AP may be associated with many STAs at one time.

2.A.4.2.b Reassociation

Association is sufficient for no-transition message delivery between IEEE 802.11 stations. The additional functionality needed to support BSS-transition mobility is provided by the reassociation service. Reassociation is a DSS. Reassociation is invoked to move a current association from one AP to another. Thus, keeping the DS informed of the current mapping between AP and STA as the station moves from BSS to BSS within an ESS. Reassociation also enables changing association attributes of an established association while the STA remains associated with the same AP. Reassociation is always initiated by the mobile STA.

2.A.4.2.c Disassociation

This service is invoked whenever an existing association is to be determined. Disassociation is a DSS. In an ESS, this tells the DS to void existing association

information. The disassociation service can be invoked by any party to an association. Either party can't refuse disassociation. APs may need to disassociate STAs to enable the AP to be removed from a network for service or for other reasons. STAs attempt to disassociate whenever leaving a network. However, the MAC management is designed to accommodate loss of an associated STA.

2.A.4.3 Access and confidentiality control services

Two services are required for IEEE 802.11 to provide functionality equivalent to that which is inherent to wired LANs. First, *Authentication* is used instead of the wired media physical connection. *Privacy* is used to provide the confidential aspects of closed wired media.

2.A.4.3.a Authentication

This service is used by all stations to establish their identity to stations with which they will communicate. If a mutually acceptable level of authentication has not been established between two stations, an association shall not be established. Authentication is an SS. IEEE 802.11 doesn't mandate the use of any particular authentication scheme. IEEE 802.11 provides link level authentication between STAs. IEEE 802.11 authentication is used simply to bring the wireless link up to the assumed physical standards of a wired link; it's neither an end-to-end nor a user-to-user authentication.

IEEE 802.11 requires mutually acceptable, successful, authentication. An STA may be authenticated with many other STAs at any given instant.

2.A.4.3.b Preauthentication

Preauthentication is typically done by an STA while is already associated with an AP with which previously authenticated. IEEE 802.11 does not require that STAs preauthenticate with APs. However, authentication is required before an association can be established. If the authentication is left until reassociation time, this may impact the speed with which an STA can reassociate between APs, limiting BSS-transition mobility performance. The use of preauthentication takes the authentication service overhead out of the time-critical reassociation process.

2.A.4.3.c Deauthentication

Deauthentication is invoked whenever an existing authentication is to be terminated. Deauthentication is an SS. As authentication is a prerequisite for association, deauthentication shall cause the station to be disassociated. Also, deauthentication shall not be refused by either party. It may be invoked by either authenticated party.

2.A.4.3.d Privacy

Any IEEE 802.11-compliant STA may hear all like-PHY IEEE 802.11 traffic that is within range. To provide privacy, IEEE 802.11 has the ability to encrypt the contents of messages; this is called the privacy service. Privacy is an SS. IEEE 802.11 specifies an optional privacy algorithm (wired equivalent privacy – WEP) that is designed to satisfy the goal of wired LAN “equivalent” privacy. Privacy may be invoked for *data* frames and some *authentication management* frames. The default privacy state for all IEEE 802.11 STAs is “in the clear”. If this default is not acceptable to one party or the other, data frames shall not be successfully communicated between LLC entities. When unencrypted data frames are received at a station configured for mandatory privacy, or when encrypted data frames using a key not available at the receiving station, they are discarded without an indication to LLC.

2.A.5 Relationships between services

An STA keeps two state variables for each STA with which direct communication via the WM is needed: Authentication state and Association state. These two variables create three local states for each remote STA. The current state existing between the source and destination station determines the IEEE 802.11 frame types that may be exchanged between that pair of STAs. The state of the sending STA is with respect to the intended receiving STA. The allowed frame types are grouped into classes and the classes correspond to the station state. Class 1 frames are allowed in State 1. Class 1 or 2 frames are allowed in State 2. Classes 1,2, &3 frames are allowed in State 3.

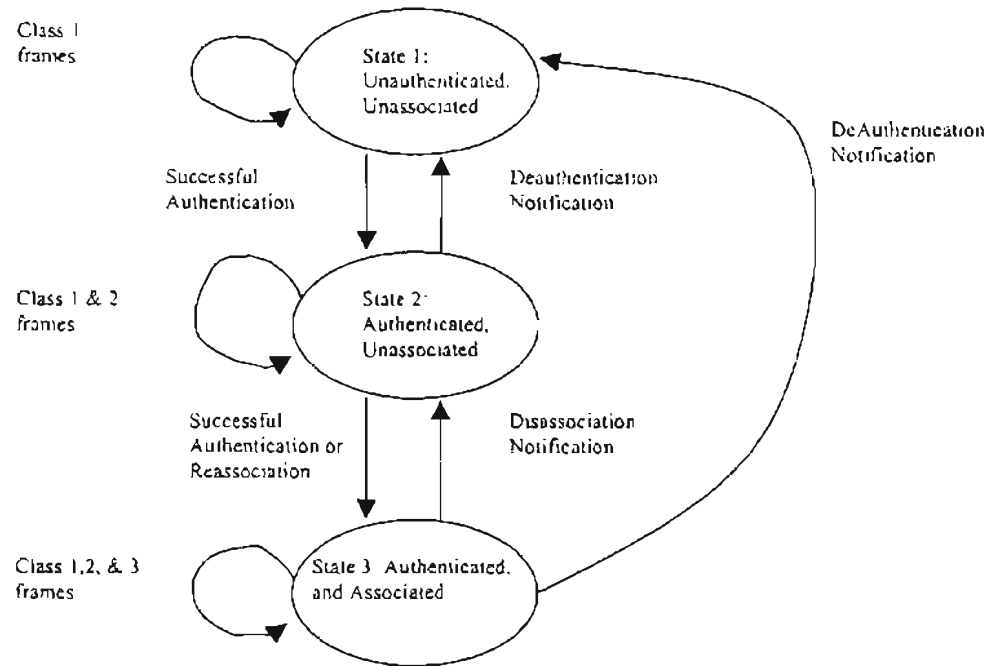


Figure 2.4 States and Classes

The following shows how frame classes are defined.

a) Class 1 frames:

- 1) Control frames: Request to send (RTS), Clear to send (CTS), Acknowledgment (ACK)
- 2) Management frames: Authentication and Deauthentication
- 3) Data frames: data frames with frame control (FC) bits "to DS" and "from DS" both false.

- b) Class 2 frames (if & only if authenticated; allowed from within State 2 and State 3 only):
 - 1) Management frames such as Association request/response, Reassociation request/response, and Disassociation.
- c) Class 3 frames (if & only if associated, allowed only from within State 3):
 - 1) Data frames: either “to DS” or “from DS” frame control (FC) bits may be set to true to utilize DSSs.
 - 2) Management frames: Deauthentication notification when in State 3 implies disassociation as well, changing the STA’s state from 3 to 1.
 - 3) Control frames

2.A.6 Difference between ESS and IBSS LANs

In an IBSS network, an STA communicates directly with one or more STAs. Thus, there is only one BSS. Further, since there is no physical DS, there can't be a portal, an integrated wired LAN, or the DSSs. Thus, the ESS configuration would reduce to the figure below. Only SSs apply to an IBSS, and so only Class 1 and Class 2 frames are allowed since there is no DS in an IBSS.

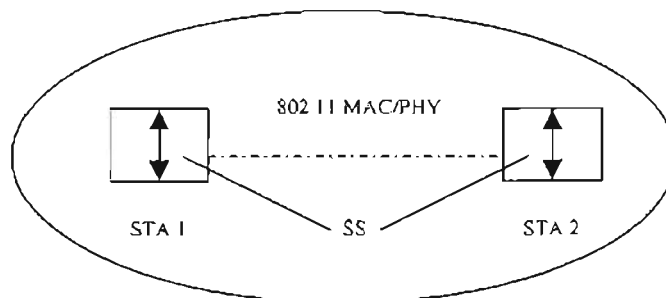


Figure 2.5 IBSS Network

2.A.7 Message information contents that support the services

2.A.7.1 Data

Data Messages

- Message type: data
- Message subtype: data
- Information items: IEEE source address of message, IEEE destination address of message, and BSS ID
- Direction of message: from STA to STA

2.A.7.2 Association

Association Request

- Message type: management
- Message subtype: Association request
- Information items: IEEE address of the STA initiating the association, IEEE address of the AP with which the initiating station will associate, and ESS ID
- Direction of message: from STA to AP

Association Response

- Message type: management
- Message subtype: Association response

- Information items:
 - Result of the requested association, with values “successful” and “unsuccessful”.
 - If the association is successful, the response shall include the association identifier.

- Direction of message: from AP to STA

2.A.7.3 Reassociation

Reassociation request

- Message type: management
- Message subtype: Reassociation request
- Information items: IEEE address of the STA initiating the reassociation, IEEE address of the AP with which the initiating station will reassociate, IEEE address of the AP with which the initiating station is currently associated, and ESS ID.
- Direction of message: from STA to AP

2.A.7.4 Disassociation

- Message type: management
- Message subtype: disassociation

- Information items: IEEE address of the station that is being disassociated.
This shall be the broadcast address in the case of an AP disassociating with all associated stations.
- Direction of message: from STA to AP or otherwise.

2.A.7.5 Privacy

The privacy service causes MPDU encryption and sets the WEP frame header bit appropriately.

2.A.7.6 Authentication

Whenever an STA has to authenticate with another STA, the authentication service causes one or more authentication management frames to be exchanged. The exact sequence of frames and their content is dependent on the authentication scheme invoked.

Authentication (first frame of sequence) – always unencrypted

- Message type: management
- Message subtype: authentication

- Information items: authentication algorithm identification, station identity assertion, authentication transaction sequence number, and authentication algorithm dependent information.
- Direction of message: first frame in the transaction sequence is always from STA 1 to STA 2

Authentication (intermediate sequence frames)

- Message type: Management
- Message subtype: Authentication
- Information items: authentication algorithm identification, authentication transaction sequence number, and authentication algorithm dependent information.
- Direction of message: Even transaction sequence numbers – from STA 2 to STA 1. Odd transaction sequence numbers – from STA 1 to STA 2

Authentication (final frame of sequence)

- Message type: management
- Message subtype: authentication
- Information items: authentication algorithm identification, authentication transaction sequence number, authentication algorithm dependent information, and the result of the requested authentication with values “successful” and “unsuccessful”.
- Direction of message: STA 2 to STA 1

2.A.7.7 Deauthentication

- Message type: management
- Message subtype: deauthentication
- Information items: IEEE address of the STA that is being deauthenticated, IEEE address of the STA with which the STA is currently authenticated, and the broadcast address in the case if a STA deauthenticating all STAs currently authenticated.
- Direction of message: from STA to STA.

2.A.8 MAC Service Definition

The *Asynchronous Data Service* provides peer LLC entities with the ability to exchange MAC service data units, MSDUs. To support this service, the local MAC uses the underlying PHY-level services to transport an MSDU to a peer MAC entity. This transport is connectionless basis.

Security Services in IEEE 802.11 are provided by the wired equivalent privacy (WEP) mechanism, which provides confidentiality, authentication, and access control in conjunction with layer management.

MSDU Ordering provided by the MAC sublayer permit, and may in some cases require, the ordering of MSDUs, as may be necessary to improve the likelihood of successful delivery based on the current operational mode of the designated recipient station(s). The sole effect of such a service is a change in the delivery order of broadcast and multicast MSDUs, relative to directed MSDUs, originating from a single source station address.

The IEEE 802.11 MAC supports three service primitives. First, the *MA-UNITDATA.request* primitive requests a transfer of an MSDU from a local LLC sublayer entity to a single peer LLC sublayer entity, or multiple peer LLC sublayer entities in the case of group addresses. Second, the *MA-UNITDATA.indication* primitive defines the transfer of an MSDU from the MAC sublayer entity to the LLC sublayer entity, or entities in the case of group addresses. Third, the *MA-UNITDATA-STATUS.indication* primitive has local significance and provides the LLC sublayer with status information for the corresponding preceding *MA-UNITDATA.request*.

2.A.9 Frame formats

2.A.9.1 MAC frame formats

Each frame consists of the following basic components:

- a) A *MAC header*, which compromises frame control, duration, address, and sequence control information.

- b) A variable length *frame body*, which contains information specific to the frame type.
- c) A *frame check sequence* (FCS), which contains an IEEE 32-bit cyclic redundancy code (CRC).

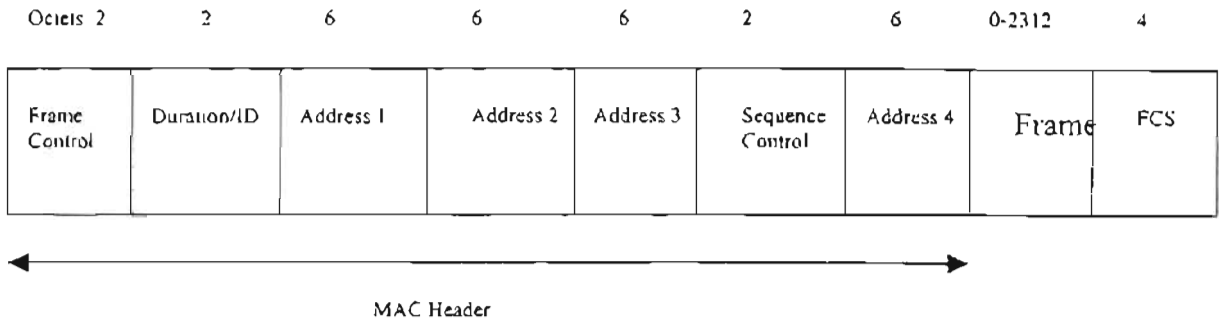


Figure 2.6 MAC Frame Format

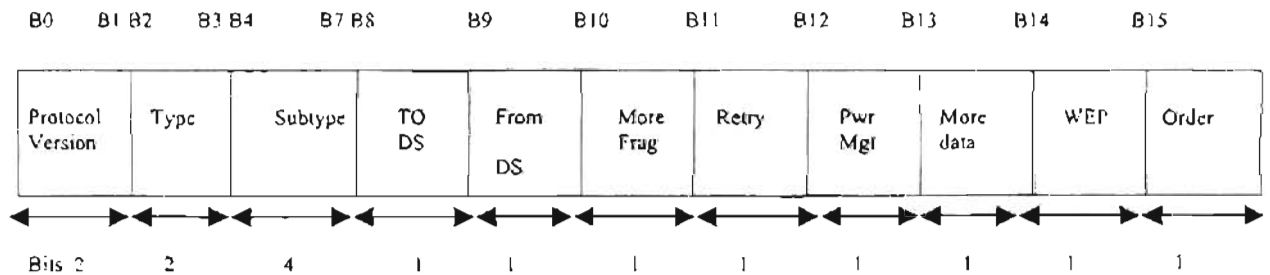


Figure 2.7
Frame Control Field

Figure 2.6 shows a MAC frame format. The figure depicts the fields/subfields as they appear in the MAC frame and in the order in which they are passed to the physical layer convergence protocol (PLCP), from left to right. As shown in figure App A-4, the *Frame Control* field consists of the following subfields: *Protocol Version*, *Type*, *Subtype*,

To DS, From DS, More Fragments, Retry, Power Management, More Data, Wired Equivalent Privacy (WEP), and Order.

- a) The *Protocol Version* field is 2 bits in length and is invariant in size.
- b) The *Type* (2 bits) and *Subtype* (4 bits) fields together identify the function of the frame. There are three frame types: control, data, and management. Each of the frame types has several defined subtypes.
- c) The *To DS* field is 1 bit in length and is set to 1 in data type frames destined for the DS. It is set to 0 in all other frames.
- d) The *From DS* field is 1 bit in length and is set to 1 in data type frames exiting the DS. It is set to 0 in all other frames.
- e) The *More Fragment* field is 1 bit in length and is set to 1 in all data or management type frames that have another fragment of the current MSDU or current MMPDU to follow. It is set to 0 in all other frames.
- f) The *Retry* field is 1 bit in length and is set to 1 in any data or management type frames that are a retransmission of an earlier frame. It is set to 0 in all other frames.
- g) The *Power Management* field is 1 bit in length and is used to indicate the power management mode of a STA. The value of this field remains constant in each frame from a particular STA within a frame exchange sequence. The value indicates the mode in which the station will be after the successful completion of the frame exchange sequence. A value of 1 indicates that the STA will be in power-save mode. A value of 0 indicates that the STA will be in active mode.
- h) The *More Data* field is 1 bit in length and is used to indicate to a STA in power-save mode that more MSDUs, or MAC management PDUs (MMPDUs) are

buffered for that STA at the AP. This field is valid in directed data or management type frames transmitted by an AP to an STA in power-save mode. A value of 1 indicates that at least one additional buffered MSDU, or MMPDU, is present for the same STA.

- i) The *WEP* field is 1 bit in length. It is set to 1 if the *Frame Body* field contains information that has been processed by the WEP algorithm. The WEP field is only set to 1 within frames of type Data and frames of type Management, subtype Authentication. The WEP field is set to 0 in all other frames.
- j) The *Order* field is 1 bit in length and is set to 1 in any type frame that contains an MSDU, or fragment thereof, which is being transferred using the StrictlyOrdered service class. This field is set to 0 in all other frames.

The *Duration/ID* field is 16 bits in length. In control type frames of subtype Power Save (PS)-Poll, the Duration/ID field carries the association identity (AID) of the station that transmitted the frame in the least significant bits, with the 2 most significant bits both set to 1. the value of the AID is in the range 1- 2007. In all other frames, the Duration/ID field contains a duration value as defined for each frame type.

There are four *Address* fields in the MAC frame format. These fields are used to indicate the BSSID, source address (SA), destination address (DA), transmitting station address (TA), and receiving station address (RA). Certain address field usage is specified by the relative position of the Address field (1-4) within the MAC header, independent of the type of address present in that field. For example, receiver address

matching is always performed on the contents of the Address 1 field in received frames, and the received address of CTS and ACK frames is always obtained from the Address 2 field in the corresponding RTS frame, or from the frame being acknowledged.

The *Sequence Control* field is 16 bits in length and consists of two subfields, the *Sequence Number* and the *Fragment Number*. The Sequence Number is a 12-bit field indicating the sequence number of an MSDU, or MMPDU. Sequence numbers are assigned from a single modulo 4096 counter, starting at 0 and incrementing by 1 for each MSDU or MMPDU. The Fragment Number field is a 4-bit indicating the number of each fragment of an MSDU or MMPDU. The fragment number is set to 0 in the first or only fragment of an MSDU or MMPDU and is incremented by 1 for each successive fragment of that MSDU or MMPDU.

The *Frame Body* field is a variable length field and contains information specific to individual frame types and subtypes. The minimum frame body is 0 octets. The maximum length frame body is defined by the sum (MSDU + ICV + IV); where ICV and IV are the WEP fields.

The *FCS* field is a 32-bit field containing a 32-bit CRC. The FCS is calculated over all the fields of the MAC header and the Frame Body field.

2.A.10 Complementary Code Keying

2.A.10.1 Complementary Sequences

The IEEE 802.11 Standard specifies Complementary Code Keying (CCK) as the modulation scheme for 5.5 and 11 Mbps data rates in the 2.4GHz band. Complementary codes, also referred to as binary complementary sequences or series, comprise a pair of equal length sequences having the property that the number of pairs of like elements with any given separation in one series is equal to the number of pairs of unlike elements with the same separation in the other.

Complementary codes are characterized by the property that their periodic autocorrelative vector sum is zero everywhere except at the zero shift. Given a pair of complementary sequences with a_i and b_i elements, where $i = 1, 2, \dots, n$, the respective autocorrelative series are given by $c_j = \sum_{i=1}^{n-j} a_i a_{i+j}$ and $d_j = \sum_{i=1}^{n-j} b_i b_{i+j}$. Ideally, the two sequences $\{a_i\}$ and $\{b_i\}$ are complementary if $c_j + d_j = \begin{cases} 0 & j \neq 0 \\ 2n & j = 0 \end{cases}$. j represents the number of shifts between sequence 1 and 2. The autocorrelation function is the result of the autocorrelation over all bit shifts of the codes. This is analogous to computing the autocorrelation of a digital signal over all the phase shifts of the signal. c_j and d_j terms represent the difference between the number of agreements and disagreements between

the shifted and unshifted codes. For the zero shift c_i and d_j are a maximum. For all other shifts c_i and d_j terms are minimized.

2.A.10.2 Polyphase Codes

The binary complementary code was merely a binary sequence having complementary properties. Likewise a polyphase complementary code is a sequence having complementary properties, the element of which have phase parameters. The code set defined in the IEEE 802.11 high rate standard is a complex complementary code set; it's elements a_i are a member of the set of complex numbers $\{1, -1, j, -j\}$, and the code set is characterized by the autocorrelative property described previously for binary codes.

2.A.10.3 CCK Modulation

The complementary codes are referred to as spreading codes because they are used to spread the occupied bandwidth of the DSSS waveform. The IEEE 802.11 complementary spreading codes have a code length 8 and a chipping rate of 11 Mchips/s. The 8 complex chips comprise a single symbol. By making the symbol rate 1.375 Msymbols/s, the 11 Mbps waveform ends up occupying the same approximate bandwidth as that for the 2 Mbps 802.11 QPSK waveform, thereby allowing for 3 non-overlapping channels in the ISM band.

The 8-bit CCK code words are derived from the following formula:

$$c = \{ e^{j(\varphi_1+\varphi_2+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_4)}, -e^{j(\varphi_1+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_3)}, e^{j(\varphi_1+\varphi_3)}, -e^{j(\varphi_1+\varphi_2)}, e^{j\varphi_1} \}$$

where c is the code word with LSB first to MSB last. This formula is used to generate the code sets for both 11 and 5.5 Mbps data rates. The parameters $\varphi_1, \dots, \varphi_4$ determine the phase values of the complex code set and are defined in the 802.11 high rate standard. For the 11 Mbps data rate each symbol represents 8 bits of information. At 5.5 Mbps 4 bits per symbol are transmitted.

The data bit stream is partitioned into bytes as (d7, d6, d5, ..., d0) where d0 is the LSB and is first in time. The 8 bits are used to encode the phase parameters $\varphi_1, \dots, \varphi_4$ according to scheme shown in the table below.

Bit	Phase Parameter
(d1,d0)	φ_1
(d3,d2)	φ_2
(d5,d4)	φ_3
(d7,d6)	φ_3

Table 2.1 DQPSK Modulation of Phase Parameters

Using the above table, given a data bit stream, we can find out the complex code word. Six bits of the data bit stream are used to select one of 64 complex codes. The other 2 bits are used to QPSK modulate, i.e. rotate, the 8 chip complex code word.

B-Bluetooth

2.B.1 - Bluetooth Radio System Architecture

2.B.1.1 - General Description

Bluetooth is a short-range radio link intended to replace the cable(s) connecting portable and/or fixed electronic devices. The most prominent features are *robustness*, *low complexity*, *low power*, and *low cost*. Bluetooth operates in the unlicensed ISM band at 2.4 GHz.

The Bluetooth system consists of a *radio unit*, a *link control unit*, and a support unit for *link management* and *host terminal interface* functions. This is shown in figure 2.8.

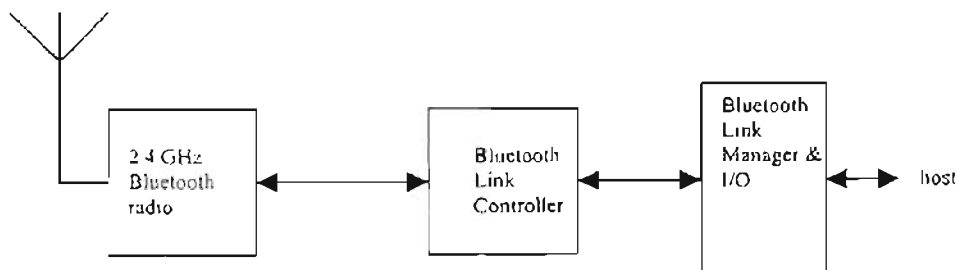


Figure 2.8
Bluetooth System

The Bluetooth system provides a *point-to-point* connection, or a *point-to-multipoint* connection, in which the channel is shared among several units. 2 or more units sharing the same channel form a *piconet*, in which one unit acts as a master of the

piconet, and others act as slaves, and they may amount up to 7 slaves. Multiple piconets with overlapping coverage areas form a *scatternet*.

2.B.1.2 - Radio spectrum

ISM band: 2400 – 2483.5 MHz

2.B.1.3 - Channel Definition

A channel is represented by a pseudo-random hopping sequence through 79 or 23 RF channels. The channel is divided into time slots. Each slot corresponds to a hop. Consecutive hops correspond to different RF hop channels. The corresponding hop rate is 1600 hops/s.

2.B.1.4 - Time Slots

Each time slot is 625usec. Time slots are numbered according to the Bluetooth clock of the piconet master. Slot numbering ranges from 0 till $2^{27} - 1$. This is cyclic with a cycle length of 2^{27} . In the time slaves, master and slave can transmit packets. Packets transmitted may extend over up to 5 time slots. If a packet occupies more than one time slot, the hop frequency shall remain the same for the duration of the packet. Time-Division Duplex (TDD) scheme is used. Master & slave alternatively transmit. The master starts its transmission in even-numbered time slots only. The slave starts its transmission in odd-numbered time slots only. TDD frame length is 1.25 ms.

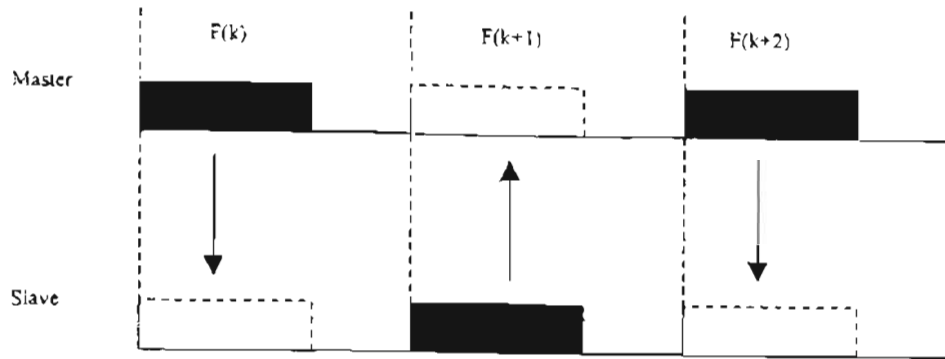


Figure 2.9 Time Slots

2.B.1.5 - Interference Immunity

It can be obtained either by interference suppression or by avoidance. Suppression can be obtained by coding or direct-sequence spreading. Interference avoidance (frequency and/or time) is more attractive since with desired user rates on the order of 1 Mb/s and beyond, coding is inadequate.

2.B.1.6 - Multiple Access Scheme

It is driven by the lack of coordination and the regulations in the ISM band. Frequency-hopping (FH)-CDMA is the best choice for Ad-Hoc radio systems. The signal can be spread over a large frequency range, but instantaneously only a small bandwidth is occupied; thus, avoiding interference in the ISM band. Hop carriers are orthogonal. Interference on adjacent hops can effectively be suppressed by filtering.

Bluetooth is based on FH-CDMA. It uses a set of 79 hop carriers at a 1 MHz spacing. Channel type is a hopping channel. Hopping dwell time is 625 μ sec. Many pseudo-random hopping sequences have been defined. Slaves use the master identity to select the same hopping sequence and to add time offsets to their respective native clocks to synchronize to the frequency hopping. Channel is divided into time slots. The minimum time slot is 625 μ sec. Full-duplex communications is achieved by applying time-division duplex (TDD).

2.B.1.7 - Modulation Scheme

Signal bandwidth of FH systems is limited to 1 MHz. Data rates are limited to about 1 Mbps. Non-coherent detection scheme is most appropriate at the receiver because of frequency hopping and also because of burstiness of data traffic. "Frequency Shift Keying" modulation with modulation index $k=0.3$ is used (Logical 1's are sent as +ve frequency deviations, and Logical 0's are sent as -ve frequency deviations). Demodulation can be accomplished by a "limiting FM discriminator".

2.B.1.8 - Medium Access Control

A large number of uncoordinated communications can take place in the same area. Therefore, this would lead to a large number of participants. A single FH channel supports a gross bit rate of 1 Mbps. This capacity is to be shared by all participants on the channel. A FH Bluetooth channel is associated with a piconet. A piconet channel is identified by the identity (hop sequence) and the system clock (hop phase) of a master

unit. Number of units that can participate on a common channel is a max of 8. It also limits the overhead required for addressing.

A master/slave role is only attributed to a unit for the duration of the piconet. The unit that establishes the piconet becomes the master.

1-The master's control

The master controls the traffic on the piconet and takes care of access control. The 625 μ sec allows only the transmission of a single packet. Communication is only possible between the master, and one or more slaves. Time slots are alternately used for master transmission and slave transmission.

2-Master Transmission

A master includes a slave address of the unit for which info is needed.

3-Master Preventing Collision

A master applies a "polling technique". For each slave-to-master slot, the master decides which slave is allowed to transmit. Only the slave addressed in the master-to-slave slot directly preceding the slave-to-master slot is allowed to transmit in this slave-to-master. If the master has info to send to a specific slave, this slave is polled explicitly and can return info. If the master has no info to send, it has to poll the slave explicitly with a short poll packet. Independent Collocated piconets may interfere when the occasionally use the same hop carrier.

2.B.2 - Interpiconet Communications

Multiple piconets in the same area form a scatternet. Units in Bluetooth can participate in different piconets due to packet-based communications over slotted links. Since a radio can tune to a single hop carrier only, at any instant of time, a unit can communicate in one piconet only. However, a unit can jump from piconet to another by varying the channel parameters, that is the master's identity and clock.

A unit can change roles when jumping from one piconet to another. It can be a slave in different piconets, but a master in only one piconet since the master's parameters specify the piconet FH channel.

The Hop-selection mechanism has been designed to allow for inter-piconet communications. By changing the identity and clock input to the selection mechanism, a new hop for the new piconet is selected. To make jumps between different piconets, a HOLD mode has been introduced.

The Bluetooth network supports both point-to-point and point-to-multi-point connections. Within SCATTERNET, several ad-hoc piconets (subnets) can be established and linked together. Each piconet is established by a different frequency-hopping channel. All users participating on the same piconet are synchronized to this channel. The figure below gives a good example.

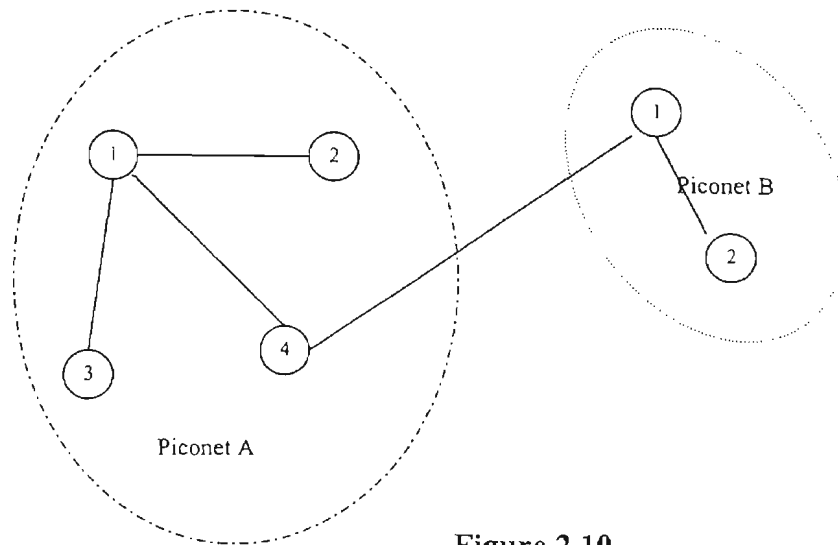


Figure 2.10
Example of Piconet Structure

Bluetooth is mainly a “packet-based” communication technology. All about this will be discussed later in this chapter because of the importance this has helped in the understanding of this technology.

2.B.3 Physical Link Definition

Two different link types can be established between the master and the slave, an SCO link and an ACL link.

2.B.3.1 Synchronous Connection Oriented Link (SCO)

SCO links use circuit switching. They are characterized by symmetric synchronous services. They require reservations of TDD frames at regular intervals. In the reserved frames, the slave doesn't have to be addressed in the master-to-slave in order to transmit in the slave-to-master slot.

2.B.3.2 Asynchronous Connectionless Link (ACL)

ACL links use packet switching. They are characterized by asymmetric asynchronous services. They use a polling access scheme. An ACL packet can be transmitted in any frame except for the frames reserved for the SCO links. In order to avoid collisions on the channel a polling access scheme is used. The slave is only allowed to transmit in the slave TX slot when addressed by the MAC address in the preceding slave RX slot.

2.B.4 Packet Definition

2.B.4.1 Packet format

A packet consists of 3 fields: a 72-bit access code, a 54-bit header, and a (2-342 bytes) payload. Packets may consist of the shortened access code only, of the access code and the header, or of the access code, header, and payload.

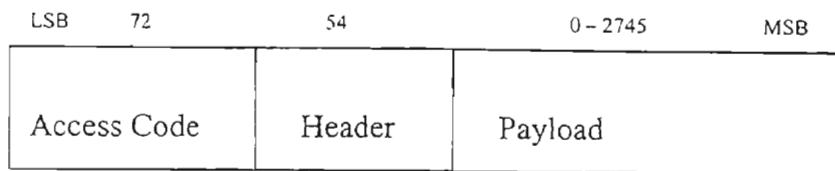


Figure 2.11 Packet Format

2.B.4.2 Channel access code

The packet starts with a 72-bit channel access code. All packets sent in the same piconet are preceded by the same channel access code. The access code identifies all the packets exchanged on the channel of the piconet. It consists of a preamble, a sync word, and a trailer. The preamble is either 1010 or 0101 depending on whether the LSB of the sync word is 1 or 0 respectively. The sync word is a 64-bit code derived from the master. The trailer is either 1010 or 0101 depending on whether the MSB of the sync word is 0 or 1 respectively.

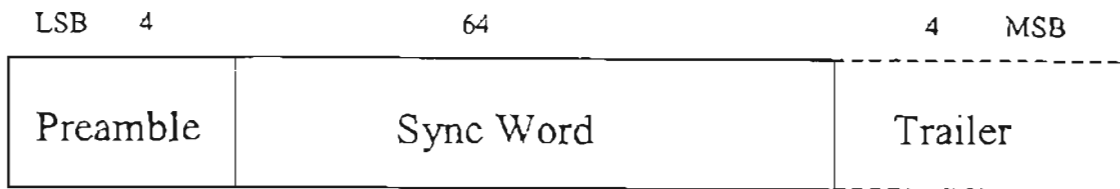


Figure 2.12 Channel Access Code

2.B.4.3 Header

It contains lower-level link control information, and consists of 6 fields: a 3-bit sub address (MAC address), a 4-bit packet type (type), a 1-bit flow control bit flow (flow), a 1-bit acknowledge indication (ARQN), a 1-bit sequence number (SEQN), and an 8-bit header error check (HEC). Total header info is 18 bits. It's protected with a 1/3 forward-error correction coding resulting in a 54-bit header length.

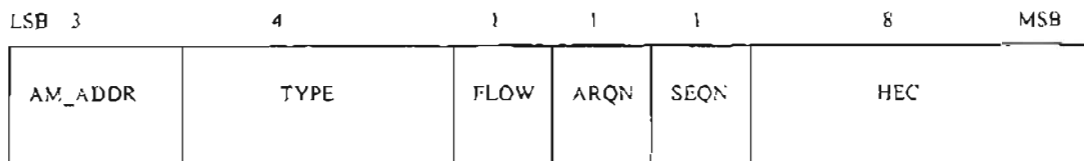


Figure 2.13 Header

2.B.4.4 M-ADDR

Each slave is assigned a temporary MAC address for the duration of the connection. The all-zero address is reserved for broadcasting purposes.

2.B.4.5 TYPE

It specifies which packet type is used. The TYPE code also reveals how many slots the current packet will occupy. This allows the non-addressed receivers to go to sleep for the duration of the occupied slots.

2.B.4.6 FLOW

This bit is used over the ACL link. When the RX buffer for the ACL connection in the recipient is full and is not emptied by the link support unit, a STOP indication (FLOW=0) is returned to stop the transmission of data temporarily. When the receiver buffer is empty, a GO indication (FLOW=1) is returned.

2.B.4.7 ARQN

Informs the sender whether the reception of the packet in the preceding slot was successful (ARQN=1) or unsuccessful (ARQN=0). The ARQN is piggy-backed in the return packet. The success of the reception is checked by means of a cyclic redundancy check (CRC), which is added to the payload.

2.B.4.8 SEQN

A numbering field to distinguish new packets from retransmitted packets. The SEQN bit is toggled for each new packet transmission. A retransmitted packet keeps the

same SEQN bit. IF two consecutive packets are received with the same SEQN bit, the second packet is ignored.

2.B.4.9 HEC

Each header has a header-error-check to check the header integrity. Before generating the HEC, the HEC generator is initialized with the 8-bit upper address part (UAP) of the master identity. Before checking the HEC, the receiver must initialize the HEC check circuitry with the proper 8-bit UAP. If the HEC does not check, the entire packet is disregarded.

2.B.4.10 Payload

It carries the actual user info and control info for the higher levels.

2.B.4.11 Packet types

The 4-bit TYPE code specifies 16 different packet types: 4 control packets, 6 single time-slot packets, 4 three time-slot packets, and 2 five time-slots packets.

2.B.4.12 Link control packets

1. ID packet: consists of the access code without the trailer. It has a fixed length of 68 bits. It's used in response routines like call setup.

2. NULL packet: consists of the access code and packet header only, and so has no payload. Total length is 122 bits. It is used to return link information to the source regarding the ARQN and FLOW. It doesn't have to be acknowledged.
3. POLL packet: also has no payload; requires an acknowledgment from the recipient. The master in a point-to-multipoint configuration so as to poll the slaves uses it. It can be used to check the connection in case no info has been exchanged for a longer period of time.
4. FHS packet: it reveals the unit identity and clock status of the sender. The payload contains 18 information bytes plus a 16-bit CRC. The payload is coded with a 2/3 rate FEC that brings the gross payload length to 240 bits. In case the FHS packet is sent by the master at call setup, the M-ADDR field in the FHS payload contains the MAC address assigned to the slave.
5. DM1 packet: supports control messages in any link type. It can also carry regular user data.

2.B.4.13 ACL packets

1. DM1 (Data Medium Rate): it carries data information only. The payload contains up to 18 info bytes plus a 16-bit CRC. The info plus CRC bits are coded with a 2/3 rate FEC.

2. DH1 packet (high data rate): similar to the DM1 packet except that the payload is not FEC encoded.
3. DM3 packet: similar to DM1 but with an extended payload. It may cover up to 3 time slots. $2/3$ rate FEC is used.
4. DH3 packet: similar to the DM3 packet, except that the info is not FEC encoded.
5. DM5 packet: is a DM1 packet with an extended payload. It may cover up to 5 time slots. $2/3$ rate FEC is used.
6. DH5 packet: similar to the DM5 packet, except that the payload is not FEC encoded.
7. AUX1 packet: is a DH1 packet with no CRC. It occupies a single time slot only.

2.B.4.14 SCO packets

1. HV1 packet (high quality voice): a pure voice packet; it's $1/3$ FEC encoded. It has to be sent every 2 time slots. It has 10 voice bytes.
2. HV2 packet: a pure voice packet. It has 20 voice bytes. A $2/3$ rate FEC is used. It has to be transmitted every 4 time slots.
3. HV3 packet: a pure voice packet. It has 30 voice bytes. It's not protected by any FEC. It has to be transmitted every 6 time slots.
4. DV packet (Data & Voice): it's a combined data-voice packet. The payload is divided into a voice field of 80 bits and data field containing up to 150 bits. The

voice bytes are PCM samples. The voice field is not protected by FEC. The data field contains up to 10 info bytes, to which a 16 bit CRC is added, and together are encoded with a 2/3 rate FEC. The voice and data fields are treated separately. The voice field is routed to the synchronous I/O port and is never retransmitted. The data field is part of an ACL link.

2.B.5 Error Correction

There are 3 error-correction schemes defined for Bluetooth: 1/3 rate FEC, 2/3 rate FEC, and ARQ scheme for the data.

2.B.5.1 FEC code: 1/3 rate

It 's a simple 3-bit repeat code; each bit is repeated 3 times. Decoding is performed by majority decision on the 3 received bits. This repeat code is applied in the header and the HV1 packet. The 1/3-rate FEC is used for packet header and also payload of the synchronous packets on the SCO link. It uses a 3-bit repeat coding, which allows reduction of instantaneous bandwidth; also intersymbol interference introduced by the receiver filtering is decreased.

2.B.5.2 FEC code: 2/3 rate

The 2/3-rate FEC is a shortened Hamming code used on the payload of synchronous packets on the SCO link; also used on the payload of asynchronous packets on the ACL link. For each block of 10 bits, 5 parity bits are added. The 2/3

FEC code is used for the HV2 packet, the data in the DV packet, and the DM and FHS packets.

2.B.5.3 ARQ scheme

An ARQ scheme can be applied on the ACL link. Each payload contains a CRC, Cyclic Redundancy Code, to check for errors. Packet retransmission is carried out if the reception of the packet is not acknowledged. The ARQ scheme can be either stop-and-wait ARQ, go-back-N ARQ, or selective-repeat ARQ. Bluetooth uses fast ARQ. Only failed packets are retransmitted. Thus, it has selective-repeat ARQ efficiency. It has a reduced overhead. Only a 1-bit sequencing number suffices in the fast-ARQ scheme. If a 2/3-rate FEC code is added, type-I hybrid ARQ scheme results. ACK/NACK info is piggybacked in the packet header of the return packet. By creating the ACK/NACK field in the header of the return packet, using Reception/Transmission switching time, the recipient determines the correctness of the received packet.

An unnumbered ARQ scheme is applied, in which data transmitted in one slot, is directly acknowledged by the recipient in the next slot. An ACK (ARQ=1) or a NACK (ARQN=0) is returned in response to the recipient of previously received packet. For a packet transmission to be successful, at least the HEC must check. In addition, the CRC must check if present. When a master sends a POLL packet to verify the connection at the start, this packet initializes the ARQ bit to NAK. Data packets containing CRC and empty slots only affect the ARQ bit.

2.B.6 Connection Establishment

It's composed of 3 elements: scan, page, and inquiry.

2.B.6.1 Scanning

A unit periodically wakes up to listen for its identity (access code). It opens up a sliding correlator, and matches up the access code derived from its identity. The scan window is 10 ms. It scans at a different hop carrier every time it wakes up. The hop sequence is 32 hops in length, is cyclic, is a pseudo-random sequence (derived from the unit's identity), and is unique for each Bluetooth device.

2.B.6.2 Paging

The paging unit knows the identity of the unit to connect to. Thus, it knows the wake-up sequence, and so it can generate the access code (page message which is transmitted repeatedly at different frequencies every 1.25 ms).

In a 10 ms period, 16 different hop carriers are visited. If the idle unit wakes up in any of these 16 frequencies, it will receive the access code, and connection set up procedure follows. The max access delay is (2 × sleep time).

When the idle unit receives the page message, it returns a message containing an access code derived from the idle unit's identity. The paging unit becomes the master using its identity and clock (which defines the FH channel). The idle unit becomes the slave.

If units have met before, the paging unit will have an estimate of the clock in the idle unit. The clock estimate is still useful at least 5 hours after the last connection.

2.B.6.3 Inquiry

In this case, the identity of the receiving unit is not known. The unit desiring to make a connection broadcasts an inquiry message. The inquiry message is an access code derived from a reserved identity. The inquiry message induces recipients to return back their address & clock info.

2.B.7 Hop Selection Mechanism

The mechanism satisfies the following requirements:

1. The sequence is selected by the unit identity. The phase is selected by the unit clock. This supports piconet concept where the master unit defines the hop channel by its identity and clock.

2. The sequence cycle covers about 23 hours. This prevents repetitions in the interference pattern when several piconets are collocated (voice services).
3. 32 consecutive hops span about 64 MHz of spectrum. This provides maximal interference immunity by spreading as much as possible over a short time interval (voice services). Also, it provides the desired features for the wake-up and inquiry sequences, which are 32 hops in length.
4. All frequencies are visited with equal probability.
5. Number of hop sequences is very large i.e. many hops patterns available. That's why many piconets can co-exist in the same area.
6. By changing the clock and/or identity, the selected hop changes instantaneously. This provides flexibility to run forward and backward in the sequence by running the clock forward and backward. Also, it supports jumping between piconets by changing master parameters.

The first block selects a 32-hop sequence with pseudo-random properties. The least significant part of the clock hops through this sequence according to the slot rate (1600 slots/sec). The first block provides an index in a 32-hop segment. Segments are mapped on the 79-hop carrier list. Even numbered hops are listed in the 1st half of the

list while odd numbered hops are listed in the 2nd half of the list. An arbitrary segment of 32 consecutive list elements spans about 64 MHz.

For paging and inquiry procedures, the mapping of the 32-hop segment on the carrier list is fixed. As the clock runs, the same 32-hop sequence and 32-hop carriers will be used. However, different identities will map to different segments and different sequences.

During connection, the more significant part of the clock takes part in sequence selection and segment mapping. After 32 hops (1 segment) the sequence is altered; the segment is shifted in the forward direction by 16 hops.

Figure 2.14 shows the above explained mechanism

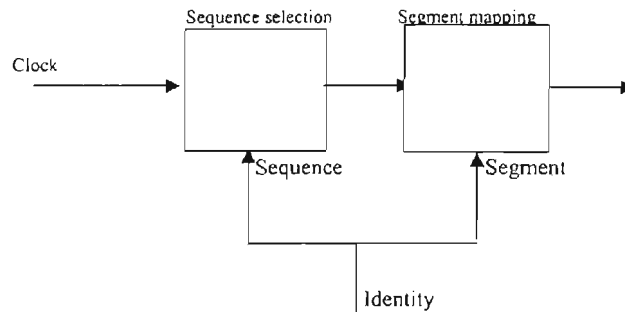


Figure 2.14 Selection Mechanism

2.B.8 Power Management

Idle mode: In idle mode, the unit only scans a little over 10 ms every T sec (1.28sec – 3.84 sec). The duty cycle is less than 1%.

Park mode: in park mode, the duty cycle is less than that of the idle mode's duty cycle. Park mode is applied only after the piconet has been established. The slave listens to the channel. The slave has to listen to the access code and packet header (126 usec)

Sniff mode: in sniff mode, slave doesn't scan at every master-to-slave slot, but has a larger interval between scans.

Connection state: during connection, current consumption is minimized and wasteful interference is prevented, because transmission occurs only when data is available. If only link control info needs to be transferred, a NULL packet is sent, without payload.

During continuous Transmission/Reception operations, a unit starts to scan for the access code at the beginning of the reception slot. If access code is not found, the unit returns to sleep until the next transmission slot (master) or reception slot (slave). If access code is received, the header is decoded, and the type of packet and its duration will be known.

Nominal transmission power for short range connectivity is 0 dBm. In Bluetooth radio specifications, up to 10 dBm is allowed.

2.B.9 Security

2.B.9.1 Authentication Procedure

Authentication process occurs at connection establishment. It verifies the identities of the units involved via a challenge-response routine. In this routine, a “claimant” transmits its claimed 48-bit address to the “verifier”. The “verifier” returns a “challenge”, a 128-bit random number (AU_RANDOM).

The E1 “hash function” accepts 3 items: 48-bit address claimant, a 128-bit AU_RANDOM, and a 128-bit common secret “link key”. It gives out a 32-bit “signed response” SRES. The SRES is sent out to the “verifier”, which compares it with its own SRES, and if matching, the “verifier” continues with connection establishment.

2.B.9.2 Encryption Procedure

The E1 “hash function” produces a 96-bit authenticated cipher offset (ACO). The payload of each packet is encrypted; payload bits are modulo-2 added to a “binary key

stream". The "binary key stream" is generated by a second "hash function" E0. E0 is based on Linear Feedback Shift registers (LFSRs).

After Encryption is enabled, master sends a random number EN_RANDOM to the slave. Before transmission of each packet, the LFSR is initialized by a combination of: EN_RANDOM, master identity, encryption key, and slot number. The encryption key is derived from: a secret link key, EN_RANDOM, and ACO. The slot number is changed for each new packet, and so initialization is new for each new packet.

The 128-bit link key provides an agreement between 2 units (to provide security in N units, $(N \times (N-1)/2)$ link keys are required. The link key is a secret key residing in the Bluetooth hardware and is not accessible by the user. The link key is a central element in the security process. It's generated during an initialization phase, where the user has to enter an identical PIN in both devices to authorize initialization, and after that the link key resides in both devices and can from then on be used for automatic authentication without user interaction.

C – Performance of Spread Spectrum

Techniques

In military radio communication systems, there has during the past 10 years been a fast growing interest in using spread-spectrum (SS) techniques in the high frequency (HF) portion of the spectrum. There is a number of reasons for this interest. Firstly, SS technology has proven to be an efficient method to attain protection against intentional jamming, and secondly, SS is a way to improve the low probability of detection (LPD) properties of the radio system. Additionally, SS modulation yields enhanced reliability of transmission on frequency-selective fading channels, such as the HF band. SS radio systems are traditionally divided into frequency-hopping (FH) and direct-sequence (DS) systems.

Interference, one of the most benevolent enemies for wireless communications is our main issue here. Interference is relative to the parameters being considered: modulation techniques, systems used, channel considered.... etc. interference could be Narrow-band or Multi-Access; both of which are handled mainly by frequency hopping techniques. Thus hybrid systems came to presence using two different modulation schemes: FSK and QPSK. This section of Chapter II will discuss the performance of a DS system in additive white Gaussian noise (AWGN) and in a jamming environment. Also, multi-access interference from other DS signals and self-interference from multipaths will be discussed here. The section to be presented will discuss the Frequency

Hopping (FH) scheme, as well as the Direct Sequence (DS) scheme. Interference would be approached from both schemes' perspectives. To get into co-channel interference among an environment of DS systems coexisting with FH systems, the discussion will be based upon a typical scenario of which Bluetooth and IEEE802.11 WLAN cards exist in the same enterprise. During the discussion, many suggestions will be presented for interference avoidance.

2.C.1 – Direct Sequence Spread Spectrum

Let's have a look at a simple SS digital communication system.

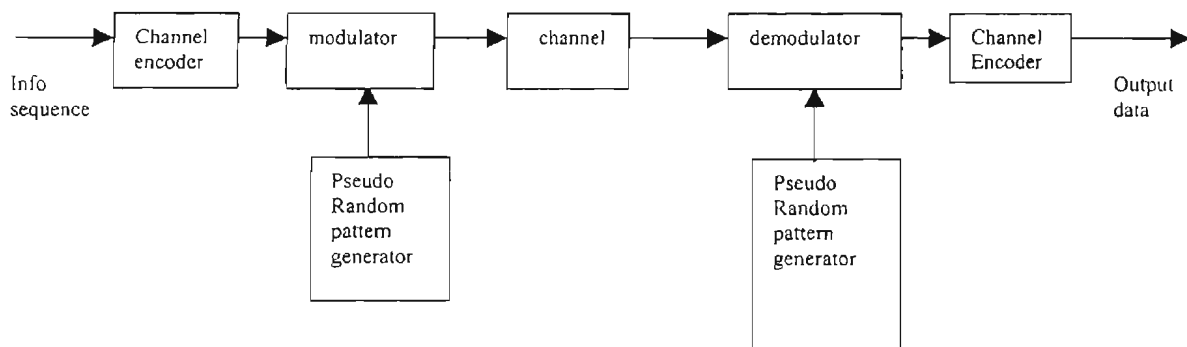


Figure 2.15
Spread Spectrum System

Initially, prior to the transmission of information, synchronization may be achieved by transmitting a fixed pseudo random bit pattern that the receiver will recognize in the presence of interference with a high probability.

Interference could be either “broadband” (some times called wideband) or “narrowband” depending on the type of spread spectrum signal being used. Each could also be “continuous” or “pulsed” accordingly. A jamming signal may consist of one or more sinusoids in the bandwidth used to transmit the information. The frequencies of the sinusoids may remain fixed or they may change with time according to some rule. Note that if interference is broadband, then it may be characterized as AWGN.

What about modulation schemes?

Phase Shift Keying (PSK) is appropriate in applications where phase coherence between the transmitted signal and the received signal can be maintained over a time interval that is relatively long compared to the reciprocal of the transmitted signal bandwidth. Whereas, Frequency Shift Keying (FSK) is appropriate in applications where such phase coherence can't be maintained due to time-variant effects.

How are Direct Sequence (DS) and Frequency Hopping (FH) signals created?

Simply, a PN sequence applied to a PSK modulation yields a DS signal. Similarly, the same PN sequence applied to a FSK modulation yields a FH signal.

This section will discuss the performance of a DSSS-BPSK system in additive white Gaussian noise (AWGN) and in a jamming environment. Also, multi-access

interference from other DS signals and self-interference from multipaths will be discussed here. Difficulty of interception will also be studied.

What are the effects of white noise and jamming?

Looking at the figures below, depicting the transmitter-receiver block diagram, assume that the local PN signal ($c(t)$) and the local carrier ($A \cos(2\pi f_c t)$) are in perfect synchronization with the incoming PN signal and the incoming carrier, respectively. The received signal consists of noise as well as interference components. Not taking

interference into account, the signal-to-noise ratio would be $SNR = \frac{E_b}{N_o} = \frac{A^2 T / 2}{N_o}$, A

being the amplitude of the transmitted signal, T being the data bit duration, $N_o / 2$ being

the two-sided power spectral density (PSD) of the white Gaussian noise in the channel,

and E_b / N_o being the energy-per-bit to noise-spectral-density ratio. It's obvious that the

SNR is independent of the chip rate T_c ; thus, *spreading the spectrum has no advantage with respect to AWGN in the channel.*

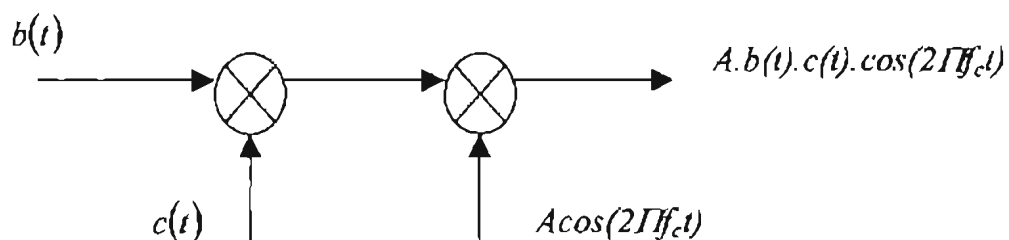


Figure 2.16
DSSS Transmitter

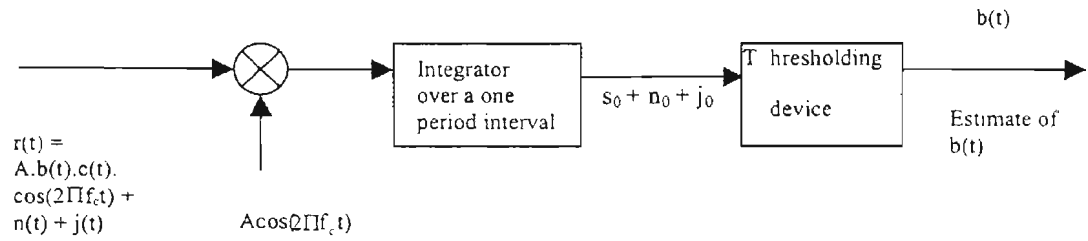


Figure 2.17 DSSS Receiver

Assuming that the jamming (interfering) signal is a *narrowband* signal, that's the jamming signal bandwidth is much less than the DS signal bandwidth, the variance of the

jamming signal is $E(j_o^2) = \frac{P_j T^2}{4N}$. It's known that the chipping rate $N = \frac{T}{T_c}$.

Therefore, the smaller the T_c , the less effect $E(j_o^2)$ has, for some value of P_j . In this case,

$SNR = \frac{A^2 T / 2}{N_o + P_j T_c}$. So, it's obvious that as T_c grows smaller, P_j will have a less

effect in reducing the SNR.

Now, assuming that jamming is *wideband*, that's the bandwidth of the jamming signal is larger than the bandwidth of the DS signal, the power of the output due to the

jamming signal is now $E[j_o^2] = \frac{P_j T}{4B_j}$, B_j being the bandwidth of $j(t)$. This result in an

$SNR = \frac{A^2 T / 2}{N_o + \frac{P_j}{B_j}}$. When N is large, the DS signal bandwidth is also large, which

implies that B_j is large and the jamming effect is small. Therefore, when N is large, the

average jamming power P_j , has to be large in order for the jamming to be effective. That's why SS systems are very attractive after all.

From the above discussion, what can we do to avoid interference? In a narrowband interference case, use a relatively small value of T_c . For wideband interference, use a relatively large value of N . Both cases lead us to *use a large processing gain to avoid interference*. Also, since the average jamming power has to be relatively large in order for it to cause damage to a DS signal, then our worry about damage caused by Bluetooth on IEEE 802.11 is less since Bluetooth use low power.

Interference from other DS users will be treated individually at the Appendix by the end of this report.

2.C.2 – Frequency Hopping Spread Spectrum

Frequency Hopping (FH), on the other hand, is actually transmitting the signal at different frequencies at a very high rate according to some pattern related also to a PN code that has been fed by a frequency synthesizer. The signal's amplitude won't be affected, but security becomes more intense due to frequency hopping; thus, FH systems has high resistance to interference, multi-user access; not adding the relative simplicity of implementation with DSP micro-controllers. For CDMA systems, which use DS methods, the parameter N (spreading gain) could be insufficient to suppress the multi-

user interference without employing power control of the transmitted signal or higher complexity multi-user detector. Therefore, a proper hopping sequence design should be used, which is called FH, or M-ary Frequency Shift Keying FH. The simplicity of this design lies in its receiver, where only the signal frequency needs to be detected. FH reduces the effects of narrow band interference by using a strategy that adapts the set of hop frequencies to avoid interference. On the other hand, DS uses adaptive techniques.

FH technique is very attractive for wireless communication systems due to its resistance to interference, multi-user access, and simplicity of implementation with DSP micro-controllers. Since the wireless communication channels are continuous-time, the discrete-time sequence is transformed into a continuous signal using a signaling pulse defined as $P_T(t) = 1$ for $0 < t \leq T$. The information pulse corresponding to bit m is $s_m(t) = A \cos[2\pi(f_b + f_m)t]P_{T_b}(t - mT_b)$, where f_b conveys the encoded information, and f_m is chosen from a set of N spreading frequencies. For binary FSK, there are $2N$ frequencies ($f_m + f_{b0}$, $f_m + f_{b1}$).

Implementing such a transmitter is easy using a DSP processor such as ADSP2181 from Analog Devices. K users, representing K frequencies, such that each user has a frequency f_m , where $m = 0, 1, \dots, K-1$. This assures multiple accesses. The

transmitter output signal would be $s(t) = \sum_{n=0}^{K-1} s_n(t) = A \sum_{n=0}^{K-1} \cos[2\pi(f_n + f_b)t]P_{T_b}(t - mT_b)$.

Thus, there are K sinusoidal signals with a finite duration (T_b). The receiver on the other hand must separate K sinusoidal signals from the received signal.

2.C.3 - Comparison between DS and FH

Let's investigate interference characteristics between wireless LAN systems that use DS and FH. Experimental results showed that varying the modulation parameters changed the interference characteristics of the throughputs of wireless LAN systems. We know that the IEEE 802.11 WLAN coverage radius is 50m. When the source of disturbance is a FH system, the signal-to-noise ratio (after despreading) of a DS system

would be $\frac{S}{N} = \frac{D.R}{\sigma^2 + \frac{U}{G_p}}$ where D is the desired signal power, R is the cumulative

distribution of the desired signal, U is the undesired signal power, G_p is the processing gain, and σ^2 is the noise power. Now, when the source of disturbance is a DS system,

the signal-to-noise ratio (after despreading) of an FH system would be $\frac{S}{N} = \frac{D}{\frac{\sigma^2}{K} + \frac{U}{G_p.W}}$

where K is the number of information digits, and W is the ratio of the operating frequency bandwidth to that of the main lobe in the interference signal. WLANs such as IEEE 802.11 employ an error correction function called Go-Back N. In this error control, throughput S (bit/sec) is expressed by the average effective transmission time T_e and the

length N (bit) of the transmission frame, such that $S = \frac{N}{T_e}$. The FH system takes more

time to transmit the correct frames when the errors were caused in the multiple frames transmitted based on the transmission control protocol (TCP) congestion avoidance, which is the algorithm in which the number of frames being transmitted at any one time

is increased until time frame error results. Considering all the above, if the $\frac{D}{U}$ ratio is examined, while maintaining a bit-error rate $\frac{E_b}{N_o} = 20dB$ (E_b being the energy per bit, N_o being the noise power spectral density), $\frac{D}{U}$ required for the FH system is less than $\frac{D}{U}$ required for the DS system. However, when the $\frac{D}{U} > 8$ dB, throughput of a DS system is greater than throughput of an FH system. This gives us a reason to believe that FH systems perform better in interference environments.

An advantage of FH systems, compared to DS systems, is that the clock rate in the PN sequence generator needs to be as high to obtain the same bandwidth.

DS systems reduce the interference power by spreading it over a wide frequency spectrum, while in FH systems, at any given time different users transmit different frequencies, thus interference avoidance is better in FH. DS systems can be designed with coherent or noncoherent demodulations, whereas FH systems usually require noncoherent demodulations. Coherent DS systems enjoy a performance advantage of about 3 dB over FH systems. With the same PN generator clock rate, FH signals can hop in frequency over a much wider band than that occupied by a DS signal. FH systems can exclude systems can exclude frequency channels that have frequent or strong interference. DS systems are most susceptible to the near-far problem, i.e. the phenomenon that a nearby interferer can seriously impair or even wipe out the intended communication, due to the higher average power of a nearby interferer. FH systems are more susceptible to

interception than their DS counterparts because the time required for PN code acquisition is shorter in FH systems, while it takes longer in DS systems. FH systems are tolerant of multipath signals and interferences, while DS receivers require special circuitry to operate satisfactorily in this kind of environment.

In DS systems, each user is assigned a unique PN code with low crosscorrelation property, thus enabling a large number of users to share the same (wide) frequency band. The signals from other users become noise-like interferences. The number of users that the system can accommodate is determined by the required SNR. In FH systems, the signal from each user has a transmitted frequency that hops over the allocated frequency band, in such a way that no two users use the same frequency at the same time.

Many technologies has evolved, emanating from the need of conquering interference, and one of the most popular in the market is actually using "Hybrid" systems. This chapter will not go into deep of "hybrid" systems, but an Appendix by the end of this report is actually dedicated for this sake, since it has been included by the literature review contributing towards this study.

2.C.4 Multiple Access Interference in a hybrid system with a FSK scheme

The Multiple Access interference plays an important role in determining the total interference in a Spread Spectrum system, particularly in a non-cellular environment, where power control is barely possible. Thus, assume a spatial distribution of users, which results in a non-equal power reception for different users. A DS/FFH has all the advantages of DS (jamming rejection, fading rejection, and security) plus beating the Near-Far effect. Each data bit is divided over a number (N_{FH}) of frequency-hop channels (carrier frequencies). In each frequency-hop channel, a complete PN-sequence of length N is combined with the data signal. Applying Fast Frequency Hopping (FFH) requires a wider bandwidth than Slow Frequency Hopping (SFH). Every Receiver is identified by a combination of an FH-sequence and N_{FH} PN-codes. FSK modulation scheme is chosen (in a while, QPSK modulation scheme is discussed). The following figure depicts a Hybrid System with a BPSK modulator; any modulation scheme can be applied however.

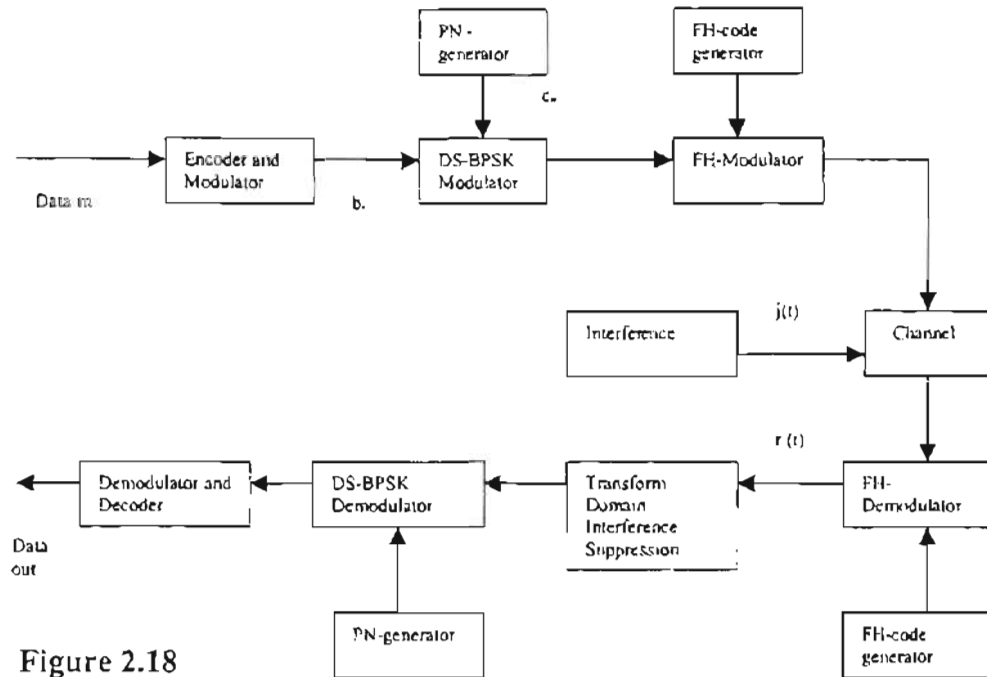


Figure 2.18
Hybrid System Model

Multiple Access interference occurs when a reference user and a non-reference user use the same FH-channel for a fraction of a frequency-hop. In DS, all codes are transmitted in the same frequency slot; therefore, codes will correlate completely. In DS/FFH, two subsequent codes are transmitted in different frequency slots, which makes codes correlate partially. If K users exist, user i being the reference user, then there are $K-1$ multiple access interferers. The transmitted signal of the k^{th} user for a DS/FFH system using an FSK modulation scheme is

$$s_k(t) = \sqrt{2P} a_k(t) \cos\left\{ \left(\omega_c + d_k(t) \Delta_{FH} + \frac{1}{2} b_k(t) \Delta_{FSK} \right) t + \theta_k \right\}$$

where Δ_{FH} is the frequency hopping spacing, P is the common transmitter power, ω_c is the center frequency, θ_k is the phase of the k^{th} carrier, $b_k(t)$ is the bit stream (FSK modulated), Δ_{FSK} is the FSK spacing, $a_k(t)$ is the PN-code waveform, and $d_k(t)$ is the sequence

$\left\{ \frac{-N_{FH}}{2} + \frac{1}{2}, \frac{-N_{FH}}{2} + 1\frac{1}{2}, \dots, \frac{N_{FH}}{2} - \frac{1}{2} \right\}$ with a duration T_h . The receiver on the other

hand will collect all the received signals

$$r(t) = \sum_{k=1}^K \sqrt{2P} a_k(t) \cos\left\{(\omega_c + d_k(t)\Delta_{FH} + \frac{1}{2}b_k(t)\Delta_{FSK})t\right\} + n(t)$$

where $n(t)$ is channel

noise. At the receiver, a correlation receiver, synchronized with user i responds to

$r(t)$ with an output

$$Z_i = \sqrt{2P} \left\{ T_h + \sum_{k=1, k \neq i}^K R_{k,i}(\tau_k) \cdot \cos \phi_k \right\} + \int_0^{T_h} n(t) a_i(t) \cdot \cos\left\{(\omega_c + d_k(t)\Delta_{FH} + \frac{1}{2}b_k(t)\Delta_{FSK})t + \theta_k\right\}$$

where $R_{k,i}(\tau_k)$ is a continuous time partial cross correlation function defined between two instants of time, τ_{k1} and τ_{k2} . The interval (τ_{k1}, τ_{k2}) is the time that two users share i and k share the same frequency-hop channel.

Of course, the result to be anticipated is the signal-to-interference ratio $\left(\frac{S}{I}\right)$.

$$\frac{S}{I} = \frac{2^{E_{b,i}} / N_o}{1 + \frac{1}{6N} \cdot \frac{2}{N_o} \cdot \sum_{k=0, k \neq i}^K E_{b,k}}$$

where $E_{b,i}$ and $E_{b,k}$ are the received energy per bit for the

i^{th} user and k^{th} transmitter respectively, N_o is the single-sided spectral density, and K is the number of users sharing with the reference user the same frequency hop channel.

Diversity is inherent for FFH; therefore, as only one bit is transmitted in N_{FH} frequency slots, it is possible to detect all frequency hops separately and then make a majority rule,

which of course leads to an enhanced performance, and so the signal-to-interference ratio

becomes
$$\frac{S}{I} = \frac{2^{E_{h,i}}/N_o}{1 + \frac{1}{6N} \cdot \frac{2}{N_o} \cdot \sum_{k=0, k \neq i}^K E_{b,k}}$$
 where $E_{h,i}$ is energy per frequency hop.

In FFH, the probability of hit, i.e. the chance that two transmitters share the same frequency slot simultaneously, is $P_{hit} = \frac{1}{q}$ where q is the number of frequency hop

channels. Whereas, in SFH, $P_{hit} = \frac{1 - N_b^{-1}}{q} + \frac{2}{N_b \cdot q}$ where N_b is the number of bits per

hop. The channel is a Rayleigh fading channel. The BER (Bit-error-rate) is

$$BER = \frac{1}{2 + \frac{S}{I}}$$

for an FSK scheme. When comparing DS/FFH and DS/SFH without

applying the diversity inherent to FFH, both systems will perform about the same. There is only an advantage of using FFH over SFH if N_b is limited.

2.C.5 Multiple Access Interference in a hybrid system with QPSK scheme

In this part of the hybrid system discussion, the modulation considered is a quadrature phase shift keying (QPSK) modulation. A mobile radio channel is investigated in the presence of interference and noise. Both deterministic and random signature sequences and memoryless random frequency-hopping patterns are considered. Low rate orthogonal codes such as Hadamard codes, which maximize the performance of the SS

multiple access communication channels, are used as deterministic signature sequences. Let's discuss the two different systems for hybrid DS/FH.

In System 1, data bits are first QPSK modulated and shaped with $\psi(t)$. Then the inphase and quadrature components of the signal are spread with different signature code words, $C_{2k}(t)$ and $C_{2k-1}(t)$. This signal is then frequency hopped according to the k^{th} user's hopping pattern (different users having different patterns). The output of the k^{th} user's

transmitter would be

$$s(t) = \sqrt{2P}b_{2k-1}(t)\Psi(t)C_{2k-1} \cdot \sin\{2\pi[f_c + f_k(t)] + \theta_k + \alpha_k(t)\} + \sqrt{2P}b_{2k}(t)\Psi(t)C_{2k} \cdot \cos\{2\pi[f_c + f_k(t)] + \theta_k + \alpha_k(t)\}$$

where P is the power of the k^{th} user's transmitter signal, $b_{2k-1}(t)$ and $b_{2k}(t)$ are the data sequences which produce a sequence of rectangular pulses of duration T , $C_{2k-1}(t)$ and $C_{2k}(t)$ are code waveforms for the quadrature and inphase components, f_c is the center frequency, θ_k is the phase angle introduced by the k^{th} modulator spreader, α_k is the phase waveform introduced by the local oscillator that generates $f_k(t)$, and $\psi(t)$ is the shaping waveform.

In System 2, M users who use orthogonal spreading codes share the same frequency hopping patterns. There are two cases: Synchronous case, where all M users begin transmission simultaneously, and the Asynchronous case, where delays occur. The transmitted signal in the synchronous case would be

$$s(t) = \left[\sum_{m=1}^M \sqrt{2P}b_{2m-1}(t)\Psi(t)C_{2m-1}(t) \right] \cdot \sin\{2\pi[f_c + f_k(t)] + \theta_k + \alpha_k(t)\} + \left[\sum_{m=1}^M \sqrt{2P}b_{2m}(t)\Psi(t)C_{2m}(t) \right] \cdot \cos\{2\pi[f_c + f_k(t)] + \theta_k + \alpha_k(t)\}$$

where $b_{2m-1}(t)$ and $b_{2m}(t)$ are data sequences for the m^{th} user, and $C_{2m-1}(t)$ and $C_{2m}(t)$ are orthogonal spreading waveforms of the m^{th} user. For the asynchronous case, the delay introduced change the transmitted signal to

$$s(t) = \left[\sum_{m=1}^M \sqrt{2P} b_{2m-1}(t - \tau_{2m-1}) \Psi(t) C_{2m-1}(t - \tau_{2m-1}) \right] \cdot \sin\{2\pi[f_c + f_i(t)] + \theta_i + \alpha_i(t)\} + \left[\sum_{m=1}^M \sqrt{2P} b_{2m}(t - \tau_{2m}) \Psi(t) C_{2m}(t - \tau_{2m}) \right] \cdot \cos\{2\pi[f_c + f_i(t)] + \theta_i + \alpha_i(t)\}$$

where τ_{2m} and τ_{2m-1} are uniformly distributed in the interval $[0, T]$.

At the receiver, the received signal is passed into a bandpass filter, then into a frequency-dehopper, which has the k^{th} user's frequency hopping pattern. The dehopper acquires the hopping synchronization. The dehopper is followed by a bandpass filter, which is centered at frequency f_c and has a bandwidth B . The received signal would be

$$r(t) = n(t) + \sum_{k=1}^N \sqrt{1/2P} \delta[f_k(t - \tau_k), f_i(t)] \cdot \{b_{2k}(t) C_{2k}(t) \cdot \cos[2\pi f_c t + \Phi_k(t)] + b_{2k-1}(t) C_{2k-1}(t) \cdot \sin[2\pi f_c t + \Phi_k(t)]\}$$

The inphase component of the demodulator output during the time interval $[\lambda T, (\lambda+1)T]$

$$\text{for user } i \text{ is } Z_{2i} = \int_{\lambda T}^{(\lambda+1)T} r(t) \Psi(t) C_{2i}(t) \cdot \cos(2\pi f_c t) dt$$

The quadrature component of the demodulator output during the time interval $[\lambda T,$

$$(\lambda+1)T]$$
 for user i is $Z_{2i-1} = \int_{\lambda T}^{(\lambda+1)T} r(t) \Psi(t) C_{2i-1}(t) \cdot \cos(2\pi f_c t) dt$

where $\lambda = j_i N_o + n_i$ for the j_i^{th} hop and the n_i^{th} data bit.

The channel is a Rayleigh Fading channel whose impulse response is $h_k(t) = \beta_k \cdot \delta(t - \tau_k) \cdot \exp(j\Phi_k)$ where β_k is the path gain, τ_k is the time delay, and Φ_k is

the phase shift, of the n^{th} hopping channel for the k^{th} user. Thus the received signal becomes $r(t) = \sum_{k=i}^K s(t) \otimes h_k(t) + n(t)$, K being the number of interfering users.

To analyze the performance of such a system, the probability of frequency hits should be discussed. Signals from other users hop into the desired user's frequency slots during the interval $[nT, (n+1)T]$. This would either lead into full hits (entire symbol duration) or partial hits (part of symbol duration) for the asynchronous case, and only full hits for the synchronous case.

For the asynchronous case, a full hit from k^{th} user occur during the n^{th} data symbol if $f_k(t - \tau_k) = f_i(t)$ for every t in $[nT, (n+1)T]$; in this case the probability of full hit is $P_f = [1 - N_b^{-1}(1 - q^{-1})]q^{-1}$. A partial hit from the k^{th} user is satisfied if $f_k(t - \tau_k) = f_i(t)$ for some values of $t \in [nT, (n+1)T]$; in this case the probability of partial hit is $P_p = 2N_b^{-1}(1 - q^{-1})q^{-1}$. Therefore, the total probability for the asynchronous case of hit is $P = P_f + P_p$.

For the synchronous case, the probability of hit is a probability of full hit always, so $P = P_f = q^{-1}$.

Remember that for both systems, FH patterns are memoryless random patterns with $q = 162$ frequencies. Length of the signature codes (DS codes) is $N=8$. The number of symbols transmitted during each dwell time is $N_b=1$. Deterministic signature

sequences treated are Hadamard (orthogonal) codes of length $N=8$. Inphase and quadrature portions of the QPSK signal use different signature codes. Only 4 users could be accommodated with orthogonal codes of length 8. In System 1, orthogonal codes provide superior performance to that with random signature codes, that's orthogonal codes minimize BER. In System 2, $M=4$, that's four users (orthogonal signature codes for each) share the same frequency hopping pattern. For the synchronous system, as long as the signature codes are orthogonal, more users can be accommodated with the same frequency-hopping pattern. As for the asynchronous system, the system is assumed to be actually quasi-synchronous (delays are within 1 chip duration of the spread signal); thus, orthogonality of the signature codes is no longer valid, and there would be performance degradation.

2.C.6 Narrow-Band Interference in a Hybrid System with a BPSK scheme

Here, the performance of a narrow-band interference rejection scheme using the transform domain signal processing is studied in a hybrid DS/FH system. The signal of interest is a BPSK modulated direct-sequence SS signal within one frequency-hopping period. The interference is a narrow-band signal with high power level and with a bandwidth relatively much narrower than the bandwidth of a wide-band signal. The interference can be located within the DS-bandwidth that is centered according to the hopping frequency in question. One of the most often used methods for the narrow-band interference rejection is "interference excisers" in the frequency domain, applied in SS receivers prior to the despreading operation.

In a DS/FH SS system both direct-sequence and frequency hop spreading are employed simultaneously throughout the transmission. The modulated data sequence is first spread by multiplication with the DS spreading waveform generated by PN code generator. After the direct-sequence spreading modulation, the signal is up converted by FH-modulator, which changes the frequency of the carrier periodically. The carrier frequency is chosen from a set of frequencies, which are controlled by a code sequence generated by the FH-code generator. In the receiver, the received signal is first down-converted by the FH demodulator and then the DS-despreading is applied by multiplying the received signal with a local replica of the PN code sequence. To make the despreading occur properly both DS- and FH- code sequences generated in the receiver must be synchronized with the sequences generated in the transmitter. The system described above is shown in this following figure.

The influence of the narrow-band interference in the described system can be reduced by transform domain filtering. The "Interference Excision" is that type of filtering takes place in the frequency domain after which the signal is transformed back to the time domain where the rest of the signal is transformed back to the time domain where the rest of the signal processing takes place. To avoid the dissemination of the interferer's energy over a wide frequency range, a "Windowing Function" can be used prior to the transformation processes. After the windowing, the input signal is Fourier transformed. The transform is then multiplied by the transfer function of some appropriate filter, after which the inverse Fourier transform takes place. The block

7

diagram of the transform filter is shown below. Note that the function $w(t)$ represents the windowing function.

To understand this procedure in a better way, assume that the input signal $r(t)$ consists of a DS spread-spectrum signal, high level but narrow-band interference and white Gaussian noise.

Of course, the question that would arise at this stage is how can the system determine the center frequency and bandwidth of interference. Actually, the statistics of the interference can't be known apriori, and hence the structure described before is difficult to implement. Instead, an "adaptive version" (shown below) if the transform domain filter can be implemented to suppress narrow-band interference that is unknown to the receiver.

The interference is either a single tone or partial band interference with respect to the DS-signal. In the figure below there is a set of curves showing the BER results for tone jamming and partial band jamming when signal-to-jammer ratio (SJR) is -15 dB. It's easy to realize that the tone interference causes more performance degradation than the partial band interference; whereas, there is no big difference in performance whether the suppression is used or not for partial band interference when SJR is -15 dB.

Chapter III

Broad Study of Interference

3.1 Approaching Interference from Other Users

The received signal, if considering one interferer, can be designated as such:

$$r(t) = Ab(t)c(t)\cos(2\pi f_c t) + A'b'(t-\tau')c'(t-\tau')\cos(2\pi f_c t + \theta') + n(t)$$

The first part of the received signal is the desired signal, the second is the interfering DS signal, and the third is the noise. After the integrator, the interfering signal becomes

$$\begin{aligned} & A' \int_0^T b'(t-\tau')c'(t-\tau')c(t)\cos(2\pi f_c t + \theta')\cos(2\pi f_c t)dt = \\ & \frac{A'}{2} \cos(\theta') \int_0^T b'(t-\tau')c'(t-\tau')c(t)dt = \\ & \frac{A'T}{2} \cos(\theta') \left[\pm \frac{1}{T} \int_0^T c(t)c'(t-\tau')dt \pm \frac{1}{T} \int_{\tau'}^T c(t)c'(t-\tau')dt \right] \end{aligned}$$

The \pm signs coming from the fact that $b'(t-\tau') = \pm 1$ for the interfering signal. The integrations following the \pm are normalized partial cross correlations of $c(t)$ and $c'(t)$. To minimize the effect of the interfering signals, we have to realize that smaller cross-correlations yield small interference. *Thus, the solution is to design PN signals such that cross-correlations are small.*

Let's take a closer look into an actual DS-CDMA transmission and a corresponding coherent correlation receiver. The DS system block diagram looks as such:

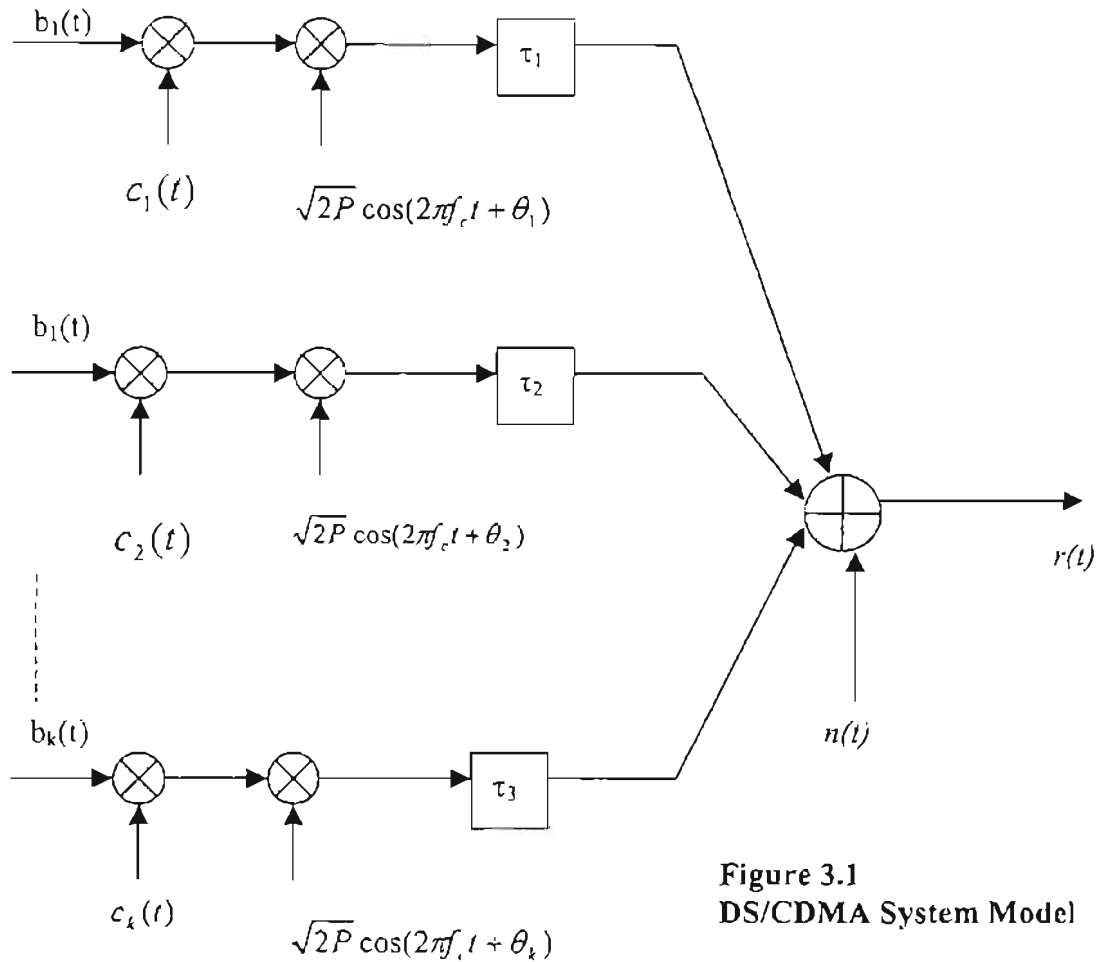


Figure 3.1
DS/CDMA System Model

In the above figure, there are K simultaneous transmissions arriving at the receiver. Each transmission is assigned a subscript k , where $k = 1, 2, \dots, K$. The binary \pm data waveform is a rectangular function with amplitude $+1$ or -1 and may change sign every T seconds. The \pm spreading waveform, $c_k(t)$, is also rectangular, but it is periodic and oscillates at a much higher rate than the data bit rate. The Coherent Cross Correlation receiver on the other hand looks as such:

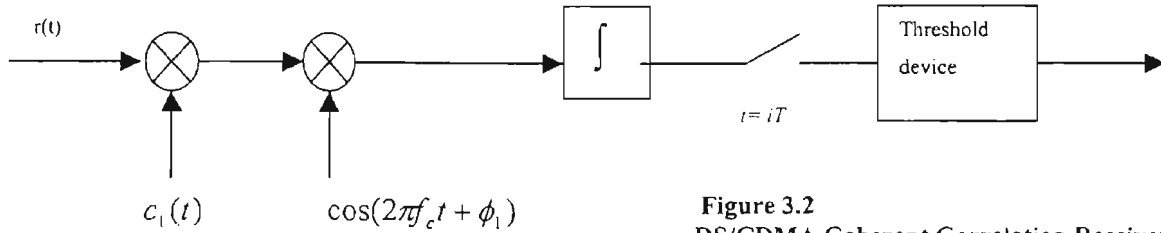


Figure 3.2
DS/CDMA Coherent Correlation Receiver

For user k the resulting DS wave is $s(t) = b_k(t)c_k(t)\sqrt{2P} \cos(2\pi f_c t + \theta_k)$. $s(t)$ is a BPSK signal that can change phase 180 degrees every T_c seconds, and whose average power is P , carrier phase is θ_k , and τ_k is the delay in transmission. The transmission bandwidth of the DS signal is $B = \frac{2}{T_c} = N \cdot \frac{2}{T}$; that is N times the radio frequency bandwidth before transmission. The noise $n(t)$ is Additive White Gaussian Noise (AWGN), has a zero mean, and its samples are mutually uncorrelated and independent. At the receiver, let's say that we are interested in the first user ($k = 1$). Thus, synchronizing to the timing of transmission of user 1 should be the first step. Then, the received signal is despread by multiplying once again by the corresponding user's spreading waveform. After that, the carrier is removed coherently. To recover the data symbol energy and suppress accidental noise, integration for T seconds is applied; after which the correlator output samples that are passed into a threshold device for decision-making. The parameter ϕ_1 is equal to $\theta_1 - 2\pi f_c \tau_1$, which is estimated, for instance via a phase lock loop (PLL) synchronization circuit.

The other $K-1$ transmissions can be considered as background noise because of spreading. These transmissions are considered as wideband interference signals and are

modeled as (AWGN). Their combined power, thus, can be expressed as $[(K-1)P]$, and their combined bandwidth is still $B = \frac{2}{T_c} = N \cdot \frac{2}{T}$. Therefore, the total noise power becomes $(\frac{N_o}{2} \cdot 2B) + (K-1)P = N_o B + (K-1)P$. This sum is a new Gaussian two-sided noise power spectral density and can be recognized as $\frac{N_o}{2} + \frac{(K-1)P}{2B}$. The term $\frac{I_o}{2} = \frac{(K-1)P}{2B}$ becomes the two-sided power spectral density for the lumped multi-user interference.

The bit-error probability is $P_b = Q(\sqrt{2 \cdot SNR})$ for BPSK (also QPSK). In case of no interference, $SNR = \frac{E_b}{N_o}$. In case of multi-user interference,

$$SNR = \frac{E_b}{N_o + I_o} = \frac{E_b}{N_o + \frac{(K-1)P}{B}}$$

We notice that $P_{b,BPSK}$ increase as K increases, and

$P_{b,BPSK}$ decreases as N increases. In the following figure, I have studied the effect of multi-user interference on QPSK DSSS in terms of probability of bit error versus the number of users. It's important to note that the variation of interferer signal power P won't leave any effect on p.b.e.

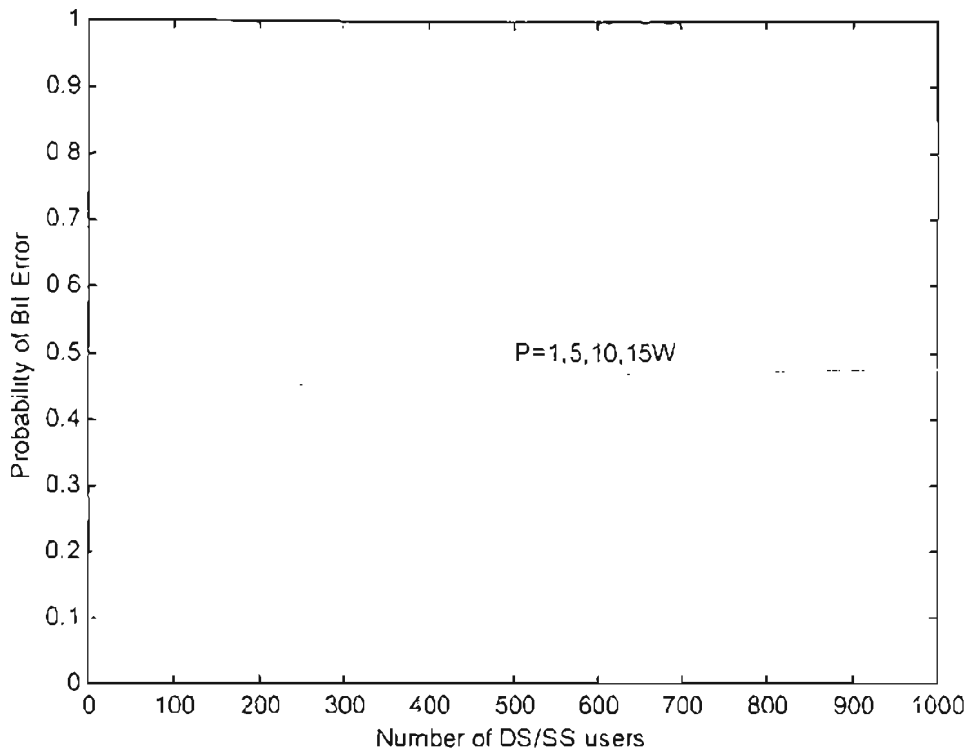


Figure 3.3 Effect of Multi-user Interference on QPSK DSSS

Still in the discussion about jamming, since this thesis will discuss co-channel interference, it's wise to study narrow-band interference. For the equation $SNR = \frac{E_b}{N_o + I_o}$, if the narrow-band interference power is assumed to be 0.5W, then the SNR value for different values of DSSS power (1W, 5W, 10W, 15W) will show something like this figure. Results show that spreading the jamming signal helps overcoming the jamming effect by increasing the SNR performance. Also, increasing the DS signal level (A in the figure) won't provide much SNR improvement at sum level, but it does help to increase SNR to some extent.

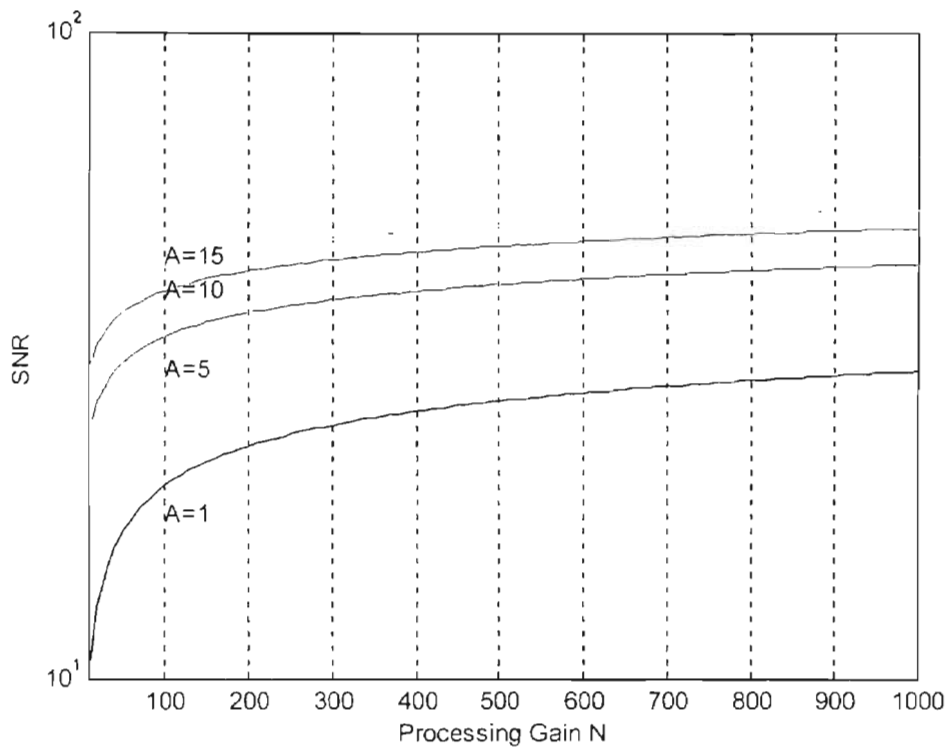


Figure 3.4 Effect of Narrow-Band Jamming on DSSS-BPSK

In case the jamming signal is wide enough to vary from 79MHz to 1GHz, then we are talking about wideband jamming. The results below are very close to the effect of narrow-band jamming.

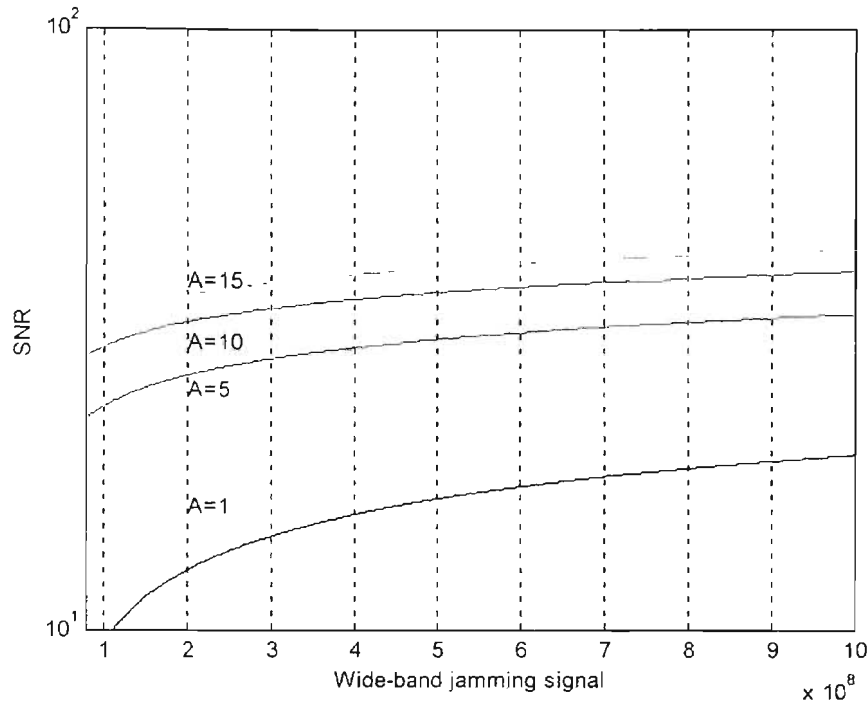


Figure 3.5 Effect of Wide-Band Jamming on DSSS-BPSK

Thus far, we have run over the effect of continuous interference or jamming on a DS spread spectrum signal. We have observed that the processing gain provide a means for overcoming the destructive effects of interference. It's essential to know that there is another jamming threat that has a dramatic effect on the performance of a DSSS system. The jamming signal in this case consists of pulses of spectrally flat noise that covers the entire signal bandwidth. This is called pulsed interference or partial-time jamming. Instead of transmitting continuously, the jammer transmits pulses at a power that is less than the average power, for a percent of time α . When the jammer is idle, the transmitted bits are assumed to be received error-free; otherwise, the probability of error for an uncoded DSSS system is $Q(\sqrt{2\alpha \epsilon_b / J_o})$. The jammer can select the duty cycle α to maximize the error probability. The figure below shows that as α is increased, the

p.b.e. increases, and as the energy-per-bit over jamming power is increased the p.b.e. is decreased.

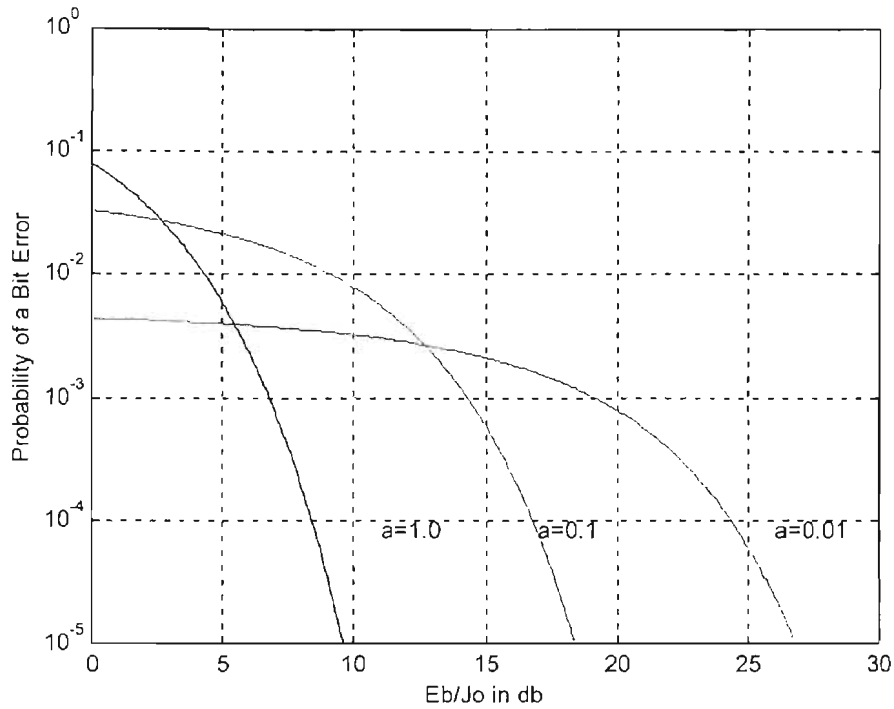


Figure 3.6 Effect of Pulsed Interference on DSSS

3.2 Correlator 's Process

At every point in time, T , the correlator gives an output, Z . Let's say that the first user sent a bit "+1". Assume that synchronization is perfect, that is, $\tau_1 = 0$ and $\theta_1 = 0$, such that all other time delays, τ_k 's, becomes relative delays and can be considered as independent identically distributed random variables uniformly distributed over $[0, 2\pi]$. All interferers' data bits are independent identically distributed random variables with a

phase of $\phi_k = \theta_k - 2\pi f_c \tau_k$. Each decision sample, Z , is equal to $\sqrt{P/2}T + \eta + I$, the first term designates the signal, the second designates noise, and the third designates multi-user interference all lumped together such that $I = \sum_{k=2}^K I_k$. For simplicity of explanation consider one interferer; the correlator output becomes

$$\begin{aligned} I_k &= \int_0^{\tau} b_k(t - \tau_k) c_k(t - \tau_k) \sqrt{2P} \cdot \cos(2\pi f_c t + \phi_k) \cdot c_1(t) \cos(2\pi f_c t) dt \\ &= \sqrt{P/2} \cos \phi_k \left[b_{-1}^{(k)} \int_0^{\tau_k} c_k(t - \tau_k) c_1(t) dt + b_0^{(k)} \int_{\tau_k}^{\tau} c_k(t - \tau_k) c_1(t) dt \right] \end{aligned}$$

Notice that the value of I_k depends on two consecutive interfering bits ($b_{-1}^{(k)}, b_0^{(k)}$) with equal probabilities. Let the corresponding PN sequences of user k and user 1 be respectively $\underline{c}^{(k)} = (a_0^{(k)}, a_1^{(k)}, \dots, a_{N-1}^{(k)})$ and $\underline{c}^{(1)} = (a_0^{(1)}, a_1^{(1)}, \dots, a_{N-1}^{(1)})$. The two partial cross-correlations shown above can be formulated in terms of a discrete aperiodic crosscorrelation $C_{k,1}(i)$ of the corresponding PN sequences such that

$$C_{k,1}(i) = \begin{cases} \sum_{j=0}^{N-1-i} a_j^{(k)} a_{j+i}^{(1)} & 0 \leq i \leq N-1 \\ \sum_{j=0}^{N-1+i} a_{j-1}^{(k)} a_j^{(1)} & -(N-1) \leq i \leq 0 \\ 0 & \text{otherwise} \end{cases}$$

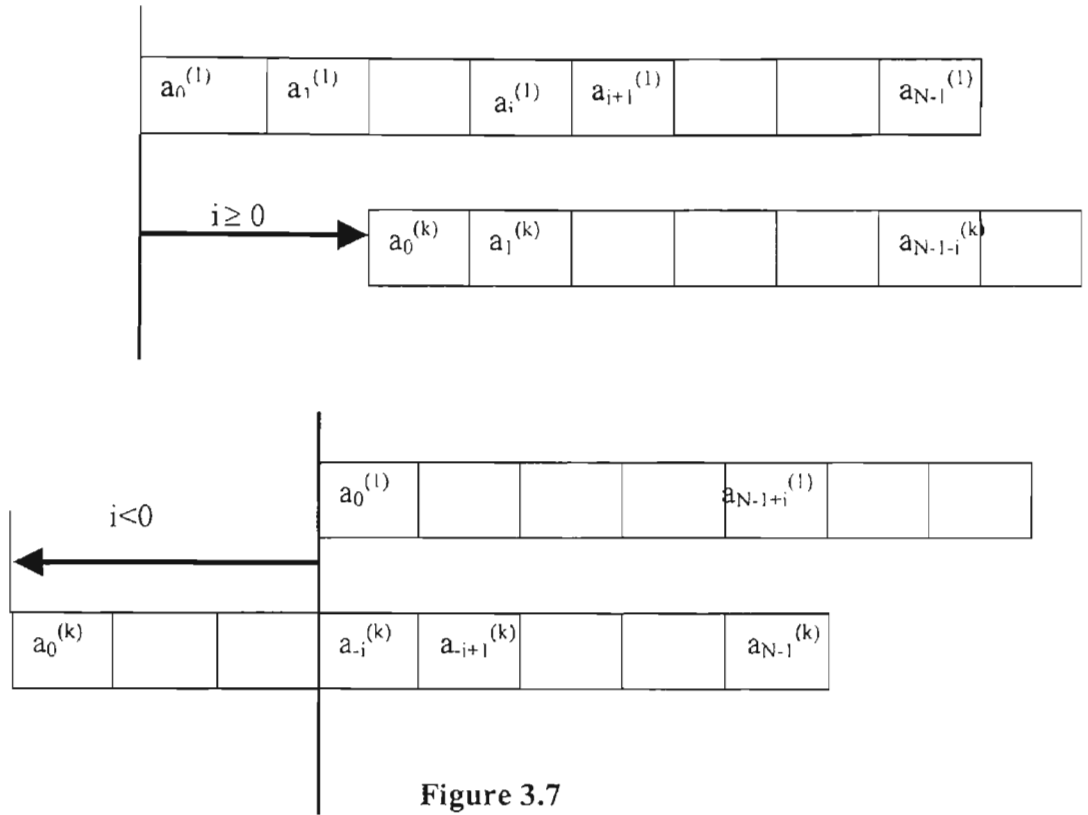


Figure 3.7
Discrete Aperiodic CrossCorrelations

As the above figure shows, if i is positive, the interference sequence is shifted to the right by i chips, and the correlation is performed on $(N-i)$ chip intervals. If i is negative, then the interference sequence is shifted to the left by i chips. The vertical line shown is considered as a reference timing, $t=0$. The relative delay is $\tau_k = iT_c + \gamma_k T_c$ $0 \leq i \leq N-1$, where γ_k is a uniform random variable on $[0,1]$, which makes τ_k not an exact integral multiple of T_c . The resulting partial integrations become

$$\int_0^{\tau_k} c_k(t - \tau_k) c_1(t) dt = T_c [C_{k,1}(-(N-i-1))\gamma_k + C_{k,1}(-(N-i))(1-\gamma_k)]$$

$$= T_c [C_{k,1}(i - N) + (C_{k,1}(1 + i - N) - C_{k,1}(i - N))\gamma_k]$$

and

$$\int_{\tau_k}^T c_k(t - \tau_k) c_i(t) dt = T_c [C_{k,1}(i)(1 - \gamma_k) + C_{k,1}(1 + i)\gamma_k]$$

$$= T_c [C_{k,1}(i) + (C_{k,1}(1 + i) - C_{k,1}(i))\gamma_k]$$

One can compute all the discrete aperiodic crosscorrelations $C_{k,1}(i)$ for all i since the sequences $\{a_j^{(k)}, k = 1, 2, 3, \dots, K\}$ are all deterministic, and hence, I_k could be calculated. The multi-user interference I has a pdf which is a $(K-1)$ fold convolution. To obtain the average bit-error probability, we first fix $I = x$, then compute the error probability via $P(Z < 0 | I = x) = Q\left(\frac{x}{\sqrt{N_o T / 4}} + \sqrt{2E_b / N_o}\right)$, taking into account that “+1” has been sent.

In order to come up with a closed form p.b.e. expression, we may assume that K is large, and model the multi-user interference contribution as an independent Gaussian random variable. The mean of $I = \sum_{k=2}^K I_k$ becomes zero, and the variance of I becomes the sum of variances of I_k , that's $V = \text{var}(I) = \sum_{k=2}^K \text{var}(I_k)$. Using this Gaussian approximation one can obtain, assuming a bit “+1” was sent in $[0, T]$, we can derive that

$$P_b = P(Z < 0 | "+1") = Q\left(\sqrt{P / 2T} \left[(NT_o / 4) + \sum_{k=2}^K \text{var}(I_k) \right]^{-1/2}\right) =$$

$Q\left(\left[\frac{N_o}{2E_b} + \frac{1}{6N^3} \sum_{k=2}^K r_{k,1}\right]^{-1/2}\right)$, where $r_{k,1}$ is an interference parameter. This suggests a

performance measure $\frac{1}{6N^3} \sum_{k=2}^K r_{k,1}$, which should be optimized for the set of K sequences.

The smaller this measure, the better is the set of sequences and the smaller the average p.b.e. Simulating p.b.e via the Standard Gaussian Approximation gives the following figure.

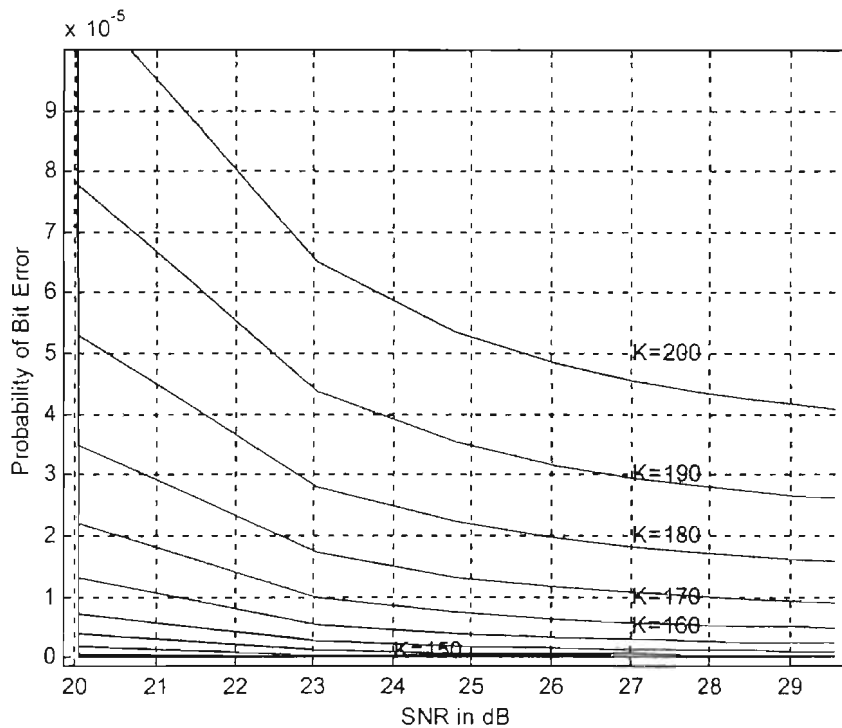


Figure 3.8 Probability of Bit Error via Standard Gaussian Approximation

For long PN sequences, one may model the K sequences as random sequences where each sequence chip is an independent discrete random variable equal to +1 or -1 with equal probability. When K is small, it's not clear that the above Gaussian

approximation will yield an accurate result. However, it can be shown that for large N , the multi-user contribution is accurately approximated by a Gaussian random variable if all τ_k 's and ϕ_k 's are fixed, and if the autocorrelation function value $C_{1,1}(1)$ is also fixed.

Then $V = \text{var}(I) = \sum_{k=2}^K \text{var}(I_k)$ becomes a random variable, but it's probability density

function $f_\nu(\nu)$ can be evaluated by a $(K-1)$ -fold convolution. Then, by fixing $V=\nu$, the

conditional p.b.e. is accurately $P_b = E\left(Q\left(\sqrt{\frac{P}{2}}T[(N_o T / 4) + V]^{-1/2}\right) \right) =$

$\int_0^\infty Q\left(\sqrt{\frac{P}{2}}T[(N_o T / 4) + \nu]^{-1/2}\right) f_\nu(\nu) d\nu$. At this point, employing a Taylor series expansion

to find the above function helps. Finally, we can write an improved approximation

formula based on Gaussian approximation as

$$P_b = \frac{2}{3} Q\left(\left[\frac{K-1}{3N} + \frac{N_o}{2E_b}\right]^{-0.5}\right) + \frac{1}{6} Q\left(\left[\frac{K-1}{3N} + \frac{\sqrt{3}c}{N^2} + \frac{N_o}{2E_b}\right]^{-0.5}\right) + \frac{1}{6} Q\left(\left[\frac{K-1}{3N} - \frac{\sqrt{3}c}{N^2} + \frac{N_o}{2E_b}\right]^{-0.5}\right)$$

The above formula is quite straightforward to compute and accurate enough for most

engineering studies. In the following plot, I show the number of allowable users (K)

versus the average bit-energy SNR (E_b/N_o) for various spreading-factor (N) using the

above formula. If we use only the first term in the above series expansion, the *standard*

Gaussian approximation designated by $P_b \approx Q\left(\left[\frac{K-1}{3N} + \frac{N_o}{2E_b}\right]^{-0.5}\right)$ is derived. The

probability of bit error (p.b.e), if fixed to a maximum of 0.001, then the maximum

number of users K_{max} can be calculated in terms of signal-to-noise ratio (SNR), as the

following figure shows.

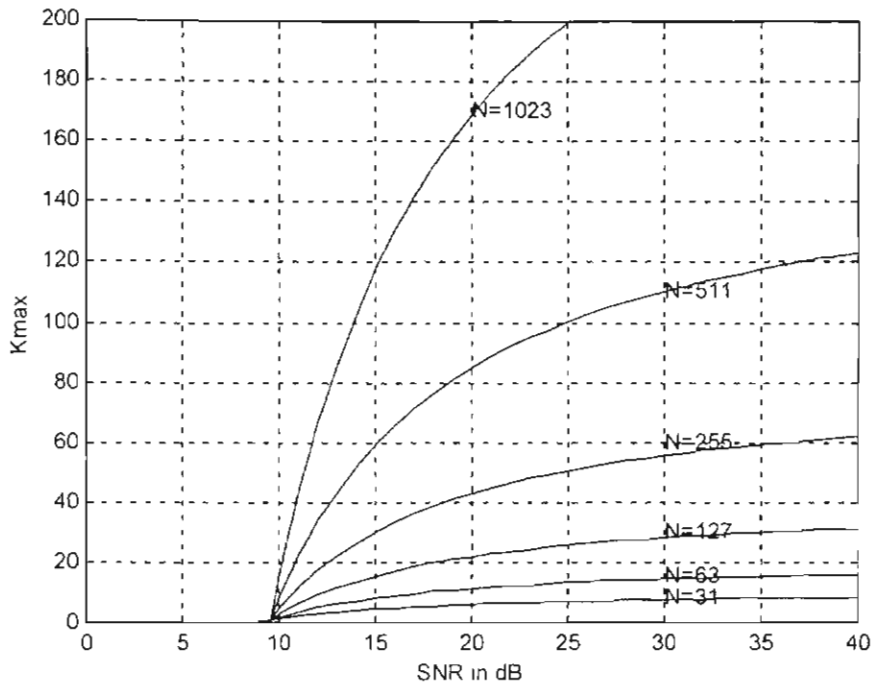


Figure 3.9 Capacity of DS/CDMA

3.3 CDMA with Other Digital Modulations and Coding

When choosing a modulation scheme, we should consider *bandwidth*, *power*, and *performance*. The required transmission bandwidth for a digitally modulated signal is determined by its PSD. The PSD for a BPSK signal is

$$\varphi_r(f) = \frac{A^2 T}{4} [\text{sinc}^2(f - f_c)T + \text{sinc}^2(f + f_c)T].$$

The power, designated by the PSD, is

concentrated around the carrier frequency for BPSK. Note that the PSD can be shaped by

altering the pulse shape and/or introducing correlation in the data sequence. For BPSK, p.b.e. is $P_{b, BPSK} = Q(\sqrt{2.SNR})$.

A more bandwidth efficient scheme than BPSK is the *quadrature phase-shift keying* (QPSK), in which the signaling pulse width is doubled from T to $2T$ seconds. The bit errors in the in-phase channel and the quadrature channel due to the channel AWGN are independent; therefore, BPSK and QPSK have identical p.b.e. performances. QPSK is thus superior to BPSK.

Offset QPSK has the same bandwidth and p.b.e. characteristic as QPSK and is implemented with the quadrature data waveforms offset by T seconds. If we change the rectangular pulse function in OQPSK to sinusoidal half-pulse function, then *minimum-shift keying* (MSK) waveform is obtained. MSK has a continuous phase and the same p.b.e. as QPSK, but its PSD characteristic is better. The spectral characteristic of MSK can be further improved by using Gaussian pulses (thus called GMSK), which might introduce intersymbol interference.

Chapter IV

Timing Considerations for Co-channel Interference Between WLAN and Bluetooth

4.1 Previous Work

In subsequent paragraphs in this chapter we'll run over the development of the probability of an IEEE 802.11 WLAN packet error in the presence of a Bluetooth(s) piconet(s). We will be interested in the effect of Bluetooth (BT) on IEEE 802.11. This theoretical derivation is also a part of the MAC layer discussion to be followed. The parameters hereby are based on the Physical (PHY) Layer model.

A few authors have looked at this issue prior to this thesis, and all focused on the 11 Mbps WLAN. Summarizing previous work, in September 1998 Greg Ennis presented a paper at an IEEE 802.11 meeting under the title "*Impact of Bluetooth on 802.11 Direct Sequence*". Then, he looked at the problem of calculating the probability of an overlap, in both time and frequency, of a continuous sequence of BT packets and an IEEE 802.11b 11Mbps packet. That paper assumed that BT would transmit over the whole 625 μ sec BT slot duration, and it didn't consider much that the time offset between the beginning of the WLAN packet and the first BT packet is a random variable. In November 1998, Jim Zyren responded to Ennis's paper in a subsequent IEEE 802.11 paper with another paper holding the title "*Extension of Bluetooth and 802.11 Direct Sequence Interference*".

Model". Zyren reduced the probability of BT hopping into the WLAN channel from 1/3 to 1/4 based on a 20 MHz wide channel, all based on the effect of the IF filter and the symbol correlator in the WLAN receiver. Zyren also made some changes with respect to the long preamble and header (192 μ sec); he used a short preamble and header (92 μ sec) instead. Zyren also increased the interframe spacing of fragments, which results in a longer time between retransmissions. Later in June 1999, Zyren presented a more complete paper at the Bluetooth'99 conference under the name "*Reliability of IEEE 802.11 Hi Rate DSSS WLANs in a High Density Bluetooth Environment*". He included more detailed Physical layer (PHY) assumptions. He gave a formula for the RF propagation signal levels and also describes the signal-to-interference ratio (SIR) at which Bluetooth causes symbol errors in the WLAN packet.

4.2 Recap of Bluetooth Radio Technology

Bluetooth (BT) is specifically designed to provide low-cost, robust, high-capacity ad-hoc voice and data networking in the 2.4 GHz ISM band. Because of FCC requirements, BT has to adhere to too many requirements: channel bandwidth is limited to 1 MHz; multiple channels, or networks, may not be coordinated; spectrum spreading must be employed; uncoordinated systems may cause severe interference. The BT solution to a robust and low-cost, yet efficient, radio is based on the following characteristics: 1 Mbps symbol rate exploits maximum available channel bandwidth; fast frequency hopping avoids interference; short data packets maximize capacity during interference; fast acknowledgement allows low coding overhead for good links; CSVD voice coding enables operation at high bit-error rates. With these design features, BT

provides extremely flexible and high data rate links in the presence of severe interference. BT does this without sacrificing performance when signal conditions are good. If the surrounding interference is increased, the degradation is very graceful. Throughout the design of BT, completely integrated implementation has always been at a premium.

4.3 Bluetooth and IEEE802.11 Coexisting

It's highly probable that both an IEEE 802.11 card and a Bluetooth (BT) card exist at the same enterprise or a large office site. Both radio types would be required for different applications depending on the need. Both types share a common frequency spectrum within the 2.45 GHz ISM band. Also, both of them are of much requirement for the business users. The IEEE 802.11 WLAN card has a relatively good data rate of 11 Mbps, plus using a Direct Sequence Spread Spectrum (DSSS); all this can provide much mobility to wired networks in large places of usage. As to Bluetooth, it provides services for many applications, including downloading email, accessing local devices like printers or faxes, allowing phone calls, and paging. This will make both of them, Bluetooth and IEEE 802.11, come into very close positions to one another, which may cause eventually destructive interference. Though no one could draw exactly a precise network topology, still some assumptions could be made to analyze interference. An environment with high density can be assumed, where large numbers of both types of devices are present within the topology analyzed. Also, different traffic loads for the Bluetooth piconet can be assumed.

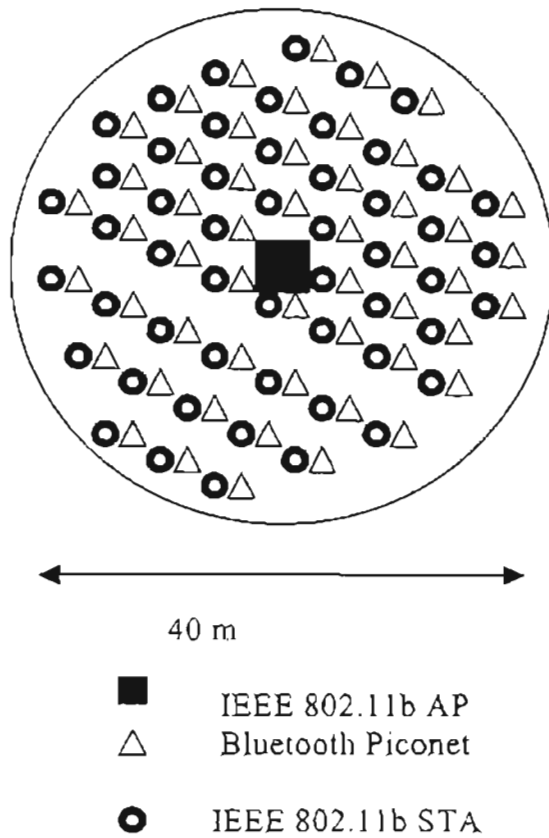


Figure 4.1
Topology Considered
Jim Zvren – June 1999

4.4 Power and Probability Analysis

Consider the topology shown; it is assumed that there is one BT piconet (consisting of two or more BT devices) co-located with each IEEE802.11 station (STA). The STAs may be located up to 20 m from the access point (AP). The average density with the IEEE802.11 basic service set (BSS) is one STA every 25 m². The transmitter power for both STAs and the AP is +20dBm. The degree to which an IEEE802.11 radio

experiences interference is dependent upon its distance from the AP according the following formula:

$$\begin{aligned} \text{Path loss: } L_{path} &= 20 \log(4\pi r / \lambda) , r \leq 8m \\ &= 58.3 + 33 \log(r/8) , r > 8m \end{aligned}$$

Note that the number of potential interfering BT piconets increases as the distance between the STA and the AP increases. Consider the following statistics:

Range	20 m	10 m	4 m
# of Potential Bluetooth Users	13	2	1

Table 4.1 Interfering Bluetooth Users Statistics

Bluetooth interference is considered narrowband. For 11 Mbps, IEEE 802.11 has a reliable service if the signal to interference ratio (SIR) is greater than or equal to 10 dB; that is, if the BT power is less than 10 dB. The received power at each STA from an AP can be seen as such: $P_{rx} = P_{tx} - L_{path}$.

The analysis is based solely on the use of single time slot packets by the BT piconet. It is assumed that this is the worst-case scenario, since the use of multiple time slot packets effectively reduces the BT hop rate and increases throughput. This reduces transmission time and results in longer gaps in BT interference, thereby increasing the chances of successful reception of DSSS packets.

Both technologies use Time Division Duplex (TDD). Let's first get into the effect of BT on IEEE 802.11, which uses 1500-byte size packets for duration of 1210 μsec . A BT packet is sent according to the master's hopping sequence, and the master orients communication within each piconet. Each time slot is 625 μsec , and it can handle different size packets depending on the kind of traffic (paging, data, voice...etc). Interference between both transmissions occurs if an overlap in *time* and *frequency* occurs. According to what has been displayed, a WLAN packet could overlap either two or three BT time packets at most. The total probability of collision, corresponding to one BT piconet, is calculated as such:

Probability that BT will hop into the WLAN pass-band (P_{hop}) = 25%

Probability of two BT packets overlap ($P_{2\text{-slot}}$) = 51.5%

Probability of three BT packets overlap ($P_{3\text{-slot}}$) = 48.5%

Piconet load factor (L_{pico}) = 33% (voice), 100% (data)

→ Probability of collision with n slot overlap ($P_{\text{coll}(n)}$) = $1 - (1 - (P_{\text{hop}} * L_{\text{pico}}))^n$

→ Probability of overall collision (P_{tot}) = ($P_{2\text{-slot}} * P_{\text{coll}(2)}$) + ($P_{3\text{-slot}} * P_{\text{coll}(1)}$) = 19.2%

Then, the total probability of collision, corresponding to multiple (m) BT piconets becomes $P_{\text{mult}(m)} = 1 - (1 - P_{\text{tot}})^m$.

A suggestion at this stage can be to limit the power of the STAs to 10 dBm instead of 20 dBm. This way the number of APs will have to be increased in order to cover the same area, which has been covered by APs with 20 dBm. However, this is possible to be implemented since an AP is nothing but a STA connected to the Ethernet

wired network. By accomplishing this, the power reaching the STAs at the very edge of the WLAN BSS, will be enough to maintain the SIR threshold of 10 dB needed for reliable service because the number of BT interferers will be much less by implementing this topology. Thus, the number of STAs related to each AP would decrease; however, the interfering power would be less from surrounding BT piconets. Note that the radius relative to an AP would be 20 m.

4.5 Packet Timing Discussion

Still in the line of discussing the effect of Bluetooth on WLAN, in the following figure, the WLAN packet is assumed to be sent asynchronously with respect to the BT packets. The WLAN packet duration is T_w seconds. The BT packets occur on a periodic basis with period T_{BT} seconds.

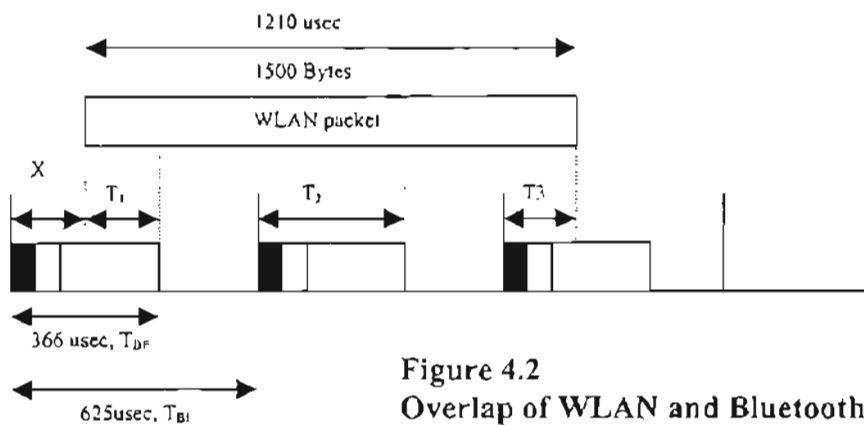


Figure 4.2
Overlap of WLAN and Bluetooth Packets

The number of dwelling periods overlapped, as shown above, is a function of the WLAN packet length and the start-of-transmission time. The start-of-transmission time, x , is a random variable ranging between 0 and $625 \mu\text{sec}$. Let $T_{BI} = 625 \mu\text{sec}$ (single-time slot) be the slot duration for BT, and $T_{BP} = 366 \mu\text{sec}$ (HV3 voice packets or DH1 data packets) be the BT packet duration. If we are using three-slot packets then $T_{BI} = 1.875\text{msec}$ and if five-slot packets then $T_{BI} = 3.125\text{msec}$. Assume x is the offset between the start of the WLAN packet and the first overlapped BT packet. The number of BT packet intervals that overlap the WLAN packet depends on x , T_W , and T_{BI} , and can be derived as

$$N(x) = \begin{cases} \left\lceil \frac{T_W}{T_{BI}} \right\rceil & \text{if } x \leq T_{BI} \cdot \left\lceil \frac{T_W}{T_{BI}} \right\rceil - T_W \\ \left\lceil \frac{T_W}{T_{BI}} \right\rceil + 1 & \text{else} \end{cases}$$

In order to find out the probability of a WLAN packet error we have to realize the packet overlap times, T_i , that shows in the figure. We have already taken one step towards that since we have derived the actual number of overlapping packets, N . Notice that it is possible that if $T_{BP} < T_{BI}$ that the first packet might not overlap with the WLAN packet, even if the interval of that packet overlaps with the WLAN packet. Writing the formula for the overlap time of the first packet, one can see that the overlap time is packet duration, T_{BP} minus x , with a restriction that the overlap time can't be negative. Thus,

$$T_i = \max(T_{BP} - x, 0)$$

As for the next packets, it's obvious that until we get to packet number $(N-1)$ the BT packet entirely overlap with the WLAN packet. So we get,

$$T_i = T_{BP} \quad i = 2, 3, \dots, N-2$$

As for the next to the last packet, the limitation is that it doesn't exceed T_{BP} ; therefore,

$$T_{(N-1)} = \min(x + T_w - (N-2)T_{Bl}, T_{BP})$$

Finally, the last packet; the overlap has two constraints: can't be negative, and not larger than T_{BP} , which leads to

$$T_N = \min(\max(x + T_w - (N-1)T_{Bl}, 0), T_{BP})$$

4.6 WLAN Packet Error

In an IEEE 802.11 WLAN if any of the bits are in error the Cyclic Redundancy Check (CRC) will detect the error and flag the packets as being bad, and this is referred to as *packet error*. This results in the receiver asking for the particular packet to be retransmitted causing a decrease in the WLAN throughput and an increase in network latency. Define *PE* as the WLAN *packet error* event; that's the WLAN packet has at least one bit error, and *GP* as the *good WLAN packet* event; that's the WLAN packet has no bit errors. Since *GP* is the complement of *PE*, $P(PE) = 1 - P(GP)$. Denote S_i the segment, consisting of a sequence of contiguous symbols, of the WLAN packet overlapping with the i^{th} BT packet. Let's call GS_i the event that segment S_i is good. We will condition our discussion on the offset x , which is a random variable whose probability mass function is

a discrete uniform random, $p_x(k) = \frac{1}{K} \quad k = 1, 2, \dots, K$ where $K = \left\lceil \frac{T_{Bl}}{T_s} \right\rceil$. T_s is the

duration of the WLAN symbol. Notice that we have quantized x such that $x = \left\lceil \frac{x}{T_s} \right\rceil$

because it is easier to visualize the packet as sum of symbols. Given $p_x(k)$ one can write $P(GP)$ in terms of conditional probabilities; i.e. $P(GP) = \sum P(GP | x = k)p_x(k)$. The next ordeal is to find $P(GP | x = k)$. We shall assume that without BT there would be no WLAN bit errors. Assuming this, we can write $P(GP | x = k) = P(GS_1, GS_2, \dots, GS_N | x = k)$, where GS_i is the event of a *good segment*. As these segments don't overlap, the events are independent, which gives $P(GP | x = k) = \prod_{i=1}^N P(GS_i | x = k)$. Each individual segment overlaps with a BT packet that can be any of 79 frequencies; where what frequency it is has a major impact on the probability that a WLAN segment being either good or bad. Actually, the BT transmission frequency is a discrete uniform random variable, with a probability mass function $p_{f_i}(j) = \frac{1}{79} \quad j = 1, 2, \dots, 79$. This yields $P(GS_i | x = k) = \frac{1}{79} \sum_{j=1}^{79} P(GS_i | x = k, f_i = j)$. That comes down to knowing the symbol error rate for each segment and the number of symbols in each segment.

4.7 Performance of WLAN Among Bluetooth Piconets

At this point, after stepping into an advanced stage of discussions of the WLAN-BT co-channel interference the discussion can be branched into two different approaches: *BT voice packets* and *BT data packets*.

4.7.1 Voice Discussion

The value of x has to be fixed for simplicity of analysis. First assume an impulse function that is defined as $\delta_v(j) = \begin{cases} 1 \\ 0 \end{cases}$, 1 if a BT voice packet is transmitted in slot j , and 0 else. Therefore, the mean number of bits per WLAN packet 'hit' by BT voice packets becomes

$$S_{ix} = 0.25 \left[\frac{T_1}{T_b} \delta_v(1) + \frac{T_{BP}}{T_b} \sum_{j=2}^{N(x)-1} \delta_v(j) + \frac{T_N}{T_b} \delta_v(N(x)) \right];$$

the probability to correctly receive a WLAN packet becomes

$$P\{\text{correct WLAN packet} | x\} = (1 - P_e)^{S_{ix}};$$

the resulting packet error probability is $\varepsilon = 1 - P\{\text{correct WLAN packet}\} =$

$$= 1 - \int_0^{T_{2f}} (1 - P_e)^{S_{ix}} \cdot \frac{1}{T_{BI}} dx$$

As a standard, the P_e value will be set to 0.001

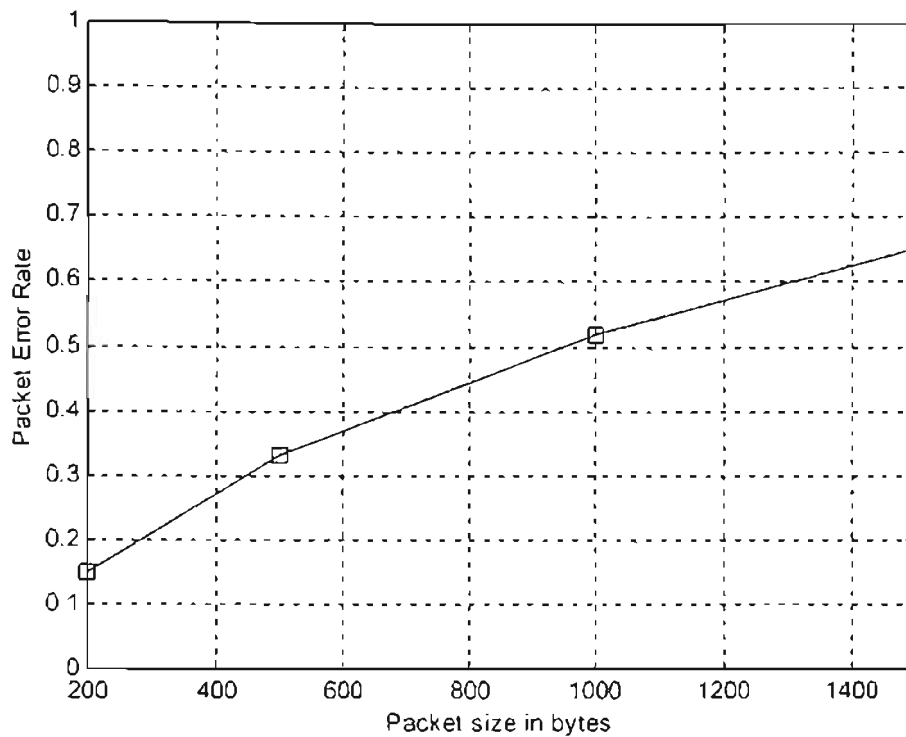


Figure 4.3
Packet Error Probability of WLAN for a BT Voice Link
Carla F. Chiasserni & Ramesh R. Rao

Simulating the results of ϵ with respect to the WLAN packet size reveals a high probability of packet error rate for a packet size of 1500 bytes. At this point, the notion of using 750 bytes instead has showed up. It's obvious in the figure below that using 750 bytes instead of 1500 bytes would decrease the throughput significantly if compared to 11 Mbps. However, if considering the best scenario performance of WLAN in the presence of BT that is when the BT piconet is "idle", then the greatest value for the WLAN throughput would go to 7 Mbps. Looking at the figure lying below, the difference of throughputs between the 1500-byte and the 750-byte packet size is insignificant

whereas the packet error rate ε is well improved as will be shown by the simulation. The figure below is applied for an AP power of 10 dBm as has been recommended earlier.

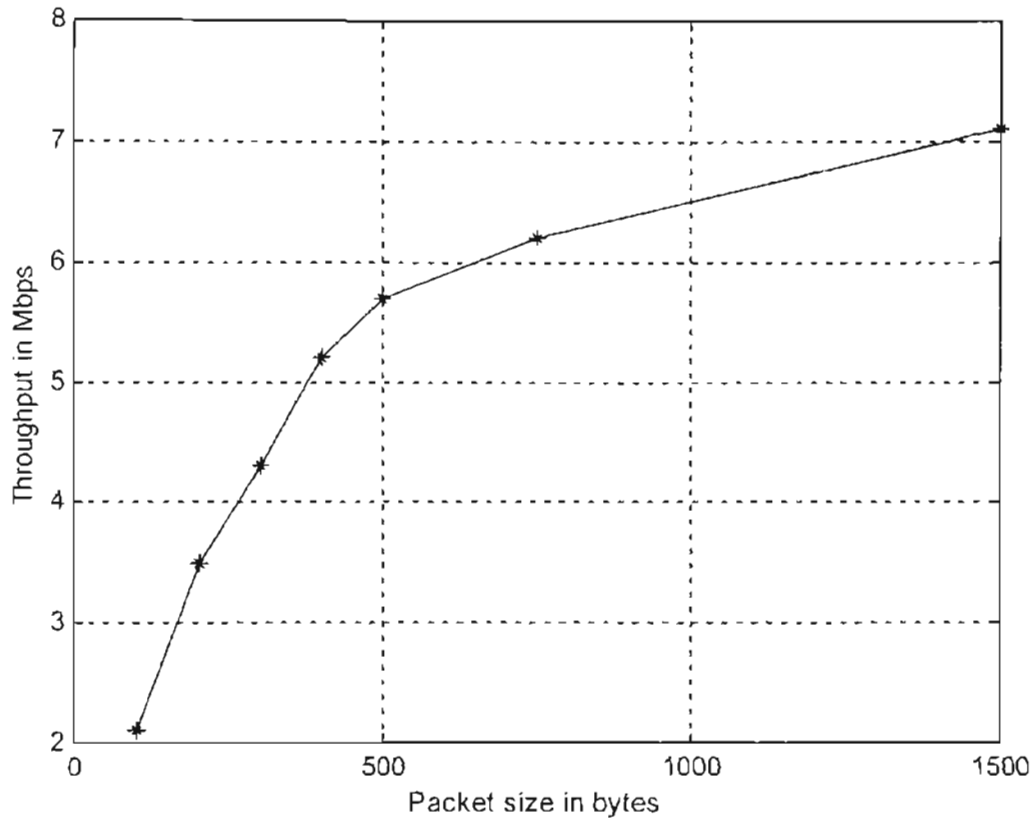


Figure 4.4
WLAN Throughput vs. Packet Size in Bytes
Jim Zyren – June 1999

The interference problem is much less severe as range to the AP decreases. The desired DSSS signal is much stronger at shorter distances from the AP and can overcome the effects of BT interference with much higher probability. This maximum throughput of almost 7 Mbps can be maintained 95.6% of the time at 10m according to Jim Zyren's analysis. The figure shown above by Carla F. Chiasserni & Ramesh R. Rao shows that actually a 750-byte size packet might be an optimum solution for packet error rate.

Consider the value of 500 bytes and then 1000 bytes and followed by 1500 bytes. In the simulation showed, packets be entered discretely, or assuming a stream of packets going in continuously ranging between 200 and 1500 bytes. Thus, this can justify the proposal to use 750-byte packets.

4.7.2 Traffic Implementations on WLAN

It's assumed that each WLAN packet is followed by an acknowledgement and information is streamed in a continuous manner and the data exchange is asymmetric. The value of P_c at the WLAN receiver is set equal to 10^{-3} for any interfering BT piconet. The transmission of a WLAN packet is considered as a failure whenever the packet or the corresponding acknowledgment is corrupted. As it has been noticed, the WLAN packet error probability is quite high and increases as a larger payload is considered. A significant improvement in performance can be achieved if a *traffic control algorithm* is introduced in the WLAN system, however, such as *Carrier Sense Collision Detection* utilization. More in depth, the transmission of a WLAN packet is delayed by a time period whenever the previous packet transmission fails. Also *Collision Avoidance* can be implemented such that when WLAN carrier is notified of an activity in the channel by some intruding BT channel, which has hopped accidentally into the WLAN channel, then the WLAN transmitter would be urged to delay the transmission for a predetermined period of time. One recommendation for that sake is to use a period equal to T_{BT} (slot interval), and keep on testing the channel after each period.

4.7.3 Data Discussion

In what has been revealed earlier, this proposal has presented that under the condition of using a maximum distance of 10 m between a STA and an AP; there would be 2 interfering BT piconets. In order to provide proof for this claim, B interfering piconets shall be assumed. Traffic for each BT piconet is Poisson distributed where each piconet has a data rate λ_i ($i = 1, \dots, B$). The total aggregated traffic would amount to the

sum $\lambda_a = \sum_{i=1}^B \lambda_i$. The probability that K BT packets are transmitted over a time period

equal to N BT packet intervals is $P_K = (\lambda_a N)^K \frac{e^{-\lambda_a N}}{K!}$. The average bit-error probability

at the WLAN reception is $\overline{P_e} = \left(\sum_{i=1}^B P_e^{(i)} \lambda_i \right) / \sum_{i=1}^B \lambda_i$. Consequently, the mean number of bits

per WLAN packet 'hit' by BT, conditioned on the value of x over the $N(x)$ intervals is

$S_{|x} = \sum_{K=0}^{N(x)} S_{|x,K} \frac{(\lambda_a N(x))^K e^{-\lambda_a N(x)}}{K!}$. Thus, the WLAN packet error probability is

$\varepsilon = 1 - \int_0^{T_{Bt}} (1 - \overline{P_e})^S \cdot \frac{1}{T_{Bt}} dx$.[8] The performance of WLAN in a data BT environment is

shown below for different aggregated traffic values. The figure below shows that as λ_a becomes smaller, the packet error probability is smaller. To minimize λ_a , the number of interfering BT piconets, B , shall have to be minimized. In order to do so, the distance

between the AP and STA will be minimized. Thus, the usage of 10 m distance is justified.

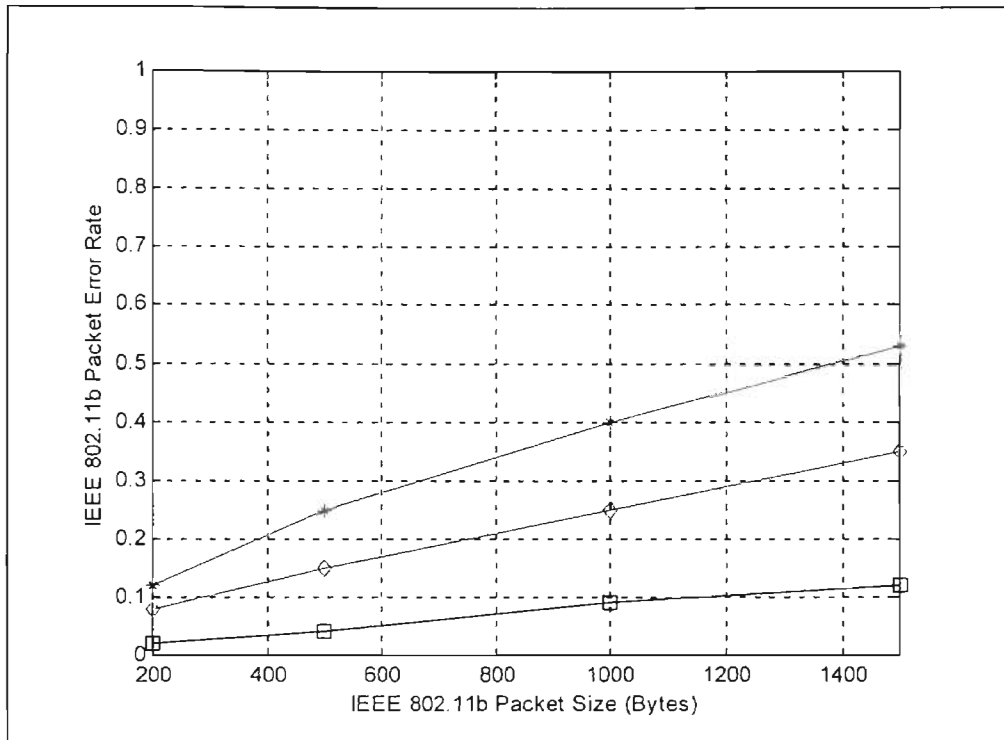


Figure 4.5 Performance of IEEE 802.11 in Data Bluetooth Environment
Carla F. Chiasserni & Ramesh R. Rao

4.7.4 Traffic Implementations on Bluetooth

In order to get a better performance, a *traffic shaping mechanism* can be implemented, such that a BT transmitter cannot send single packets over the channel but must always transmit bursts of M packets. Obviously, BT packets will have to experience some time delay, which can be calculated by considering the delay from the time instant at which a BT packet is generated to the time instant at which it is transmitted and by

averaging over the number of BT packets that are transmitted during a WLAN data stream of 1000 packets. Increasing the burst size would considerably decrease packet error rate and increase the average BT packet delay simultaneously.

Chapter V

Discussion, Observations, And Results

As a chapter overview, chapter V will present the suggested solution for the co-channel interference hazard. First (5.1), a quick view of the IEEE 802.11b network architectures, modulation parameters, functionalities, and channel distribution is given in order to help the reader visualize a real WLAN network. Consequently, in the next section, 5.2, channel overlap will be visualized in terms of frequency spectrums. The resulting error probability because of interference is discussed in a simple manner in section 5.3. Section 5.4 presents a mechanism called *Adaptive Frequency Hopping*, which has been adopted by manufacturers for various applications to solve the same problem. Section 5.5 would suggest this thesis's proposed system. Sections 5.6 and 5.7 studies the performance of each, Bluetooth and IEEE 802.11b systems, in presence of the other plus Gaussian noise, as a function of distance and the desired bit-error-rate.

5.1 IEEE 802.11b

5.1.1 Physical Layer (PHY)

Wireless LAN is being developed to help providing a relatively high bandwidth in a small geographical area, not bigger in size than an enterprise building or a business tower most of the time. Typical service rates for WLANs can be expected to range from 1

Mbps to 20 Mbps. The IEEE has developed an international WLAN standard, whose scope is the physical layer (PHY) and the medium access control (MAC) sublayer implementation. The IEEE 802.11b standard supports a mandatory data rate of 1 Mbps, as well as it supports 2 Mbps, 5.5 Mbps, and 11 Mbps. The table below shows each rate characteristic.

Data rate	Code Length	Modulation	Symbol Rate	Bits/Symbol
1 Mbps	11-Barker code	DBPSK	1 MSps	1
2 Mbps	11-Barker Code	DQPSK	1 MSps	2
5.5 Mbps	8 – CCK	QPSK	1.375 MSps	4
11 Mbps	8 - CCK	QPSK	1.375 MSps	8

Table 5.1 IEEE 802.11b Various Rate Characteristics

As has already been displayed in chapter II, the Basic Service Set (BSS) is the fundamental building block of the IEEE 802.11 architecture. It is analogous to a cell in a cellular communications network. All stations in a BSS should be able to communicate directly with all other stations in a BSS. A BSS can be used to form an *ad hoc* network, which is a deliberate grouping of stations into a single BSS without the aid of an *infrastructure* network. Any two stations can form an ad hoc network, and any station can establish a direct communications session with any other station in the BSS, without having to connect through an Access Point (AP).

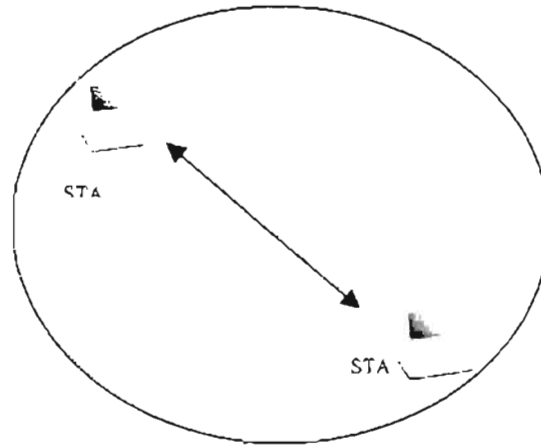


Figure 5.1 Sketch of an ad hoc network

As to *infrastructure* networks, they are established to provide wireless users with specific services and relatively a good range of communication. Such kind of structures is established using APs. The AP is like the base station in a cellular network. APs provide network connectivity between multiple BSSs, thus forming an Extended Service Set (ESS), which consists of multiple BSSs that are communicating together using a common Distribution System (DS). An ESS is also a gateway between wireless users and the wired network. The DS is like the backbone network that deals with MAC level transport of MAC service data units (MSDU).

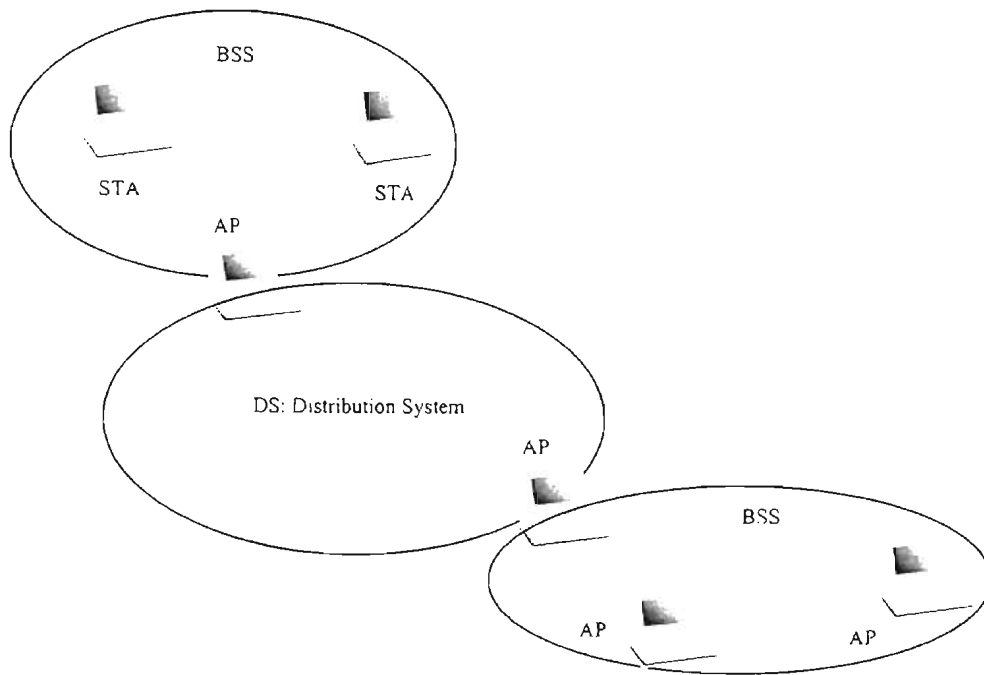


Figure 5.2 Sketch of an infrastructure network

WLAN use *dynamic rate shifting* in order to support very noisy environments as well for extended ranges; that's data rates are automatically adjusted to compensate for the changing nature of the radio channel. Users connect at 11 Mbps rate; however, as devices move beyond the optimal range for 11 Mbps operation, or if annoying interference occurs, 802.11b devices will choose to transmit at lower speeds, i.e. 5.5, 2, and 1 Mbps. This mechanism is a PHY property that is transparent to the user and upper layers of the protocol stack.

5.1.2 MAC Sublayer

This sublayer is responsible for the channel allocation procedures, frame formatting, protocol data unit (PDU) addressing, fragmentation, reassembly, and error

checking. All stations have to provision for channel availability before each packet transmission. Basically, the wireless medium has two modes: contention mode or contention period (CP), and a contention free period (CFP). For the latter one, the AP controls the medium usage, thus there is no need for stations to contend for channel access. For channel control, an AP can use three different types of frames: *management*, *control*, and *data*. All of these frames have been already discussed in chapter II. To recap, the management frames are used to *associate* and *disassociate* a station with the AP, and for timing and synchronization, and *authentication* and *deauthentication*. Control frames are used for hand-shaking and positive acknowledgments during the CP, and to end the CFP. Data frames are used for the transmission of data during the CP and CFP, and can be combined with polling and acknowledgments during the CFP.

5.1.3 Distributed Coordination Function

Distributed Coordination Function (DCF) is an access method used to support asynchronous data transfer. All stations must support the DCF. DCF supports contention services, which means that each station with an MSDU queued for transmission must check for channel availability, and once the MSDU is transmitted, the station must re-contend for the channel for all subsequent frames. DCF is based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol, mentioned in the previous chapter. Carrier sensing is performed by *physical carrier sensing* at the air interface, and at the MAC sublayer by *virtual carrier sensing*. The first detects the presence of other IEEE 802.11 WLAN users by analyzing all detected packets and also

analyzes activity in the channel via relative signal strength from other sources. As for virtual carrier sensing, it is used by a source station to inform all other stations in the BSS of how long the channel will be utilized for the successful transmission of a MAC protocol data unit (MPDU), which is a complete data unit being passed from the MAC sublayer to the physical layer. The MAC header includes a duration field that indicates the amount of time after the end of the present frame that the channel will be utilized to complete the transmission of that frame.

The wireless medium is controlled through the use of Inter-Frame Space (IFS) time intervals between the transmission of frames. IEEE 802.11b standard specifies three IFS intervals: Short-IFS (SIFS), Point Coordination-IFS (DIFS), and Distributed Coordination-IFS (DIFS). SIFS gives a station the highest priority to access the channel over those stations required to wait PIFS or DIFS before transmitting.

Upon collision, the source continues transmitting the complete MPDU. Channel bandwidth is wasted due to corrupted MPDU if the MPDU is large. Request to Send (RTS) and Clear to Send (CTS) control frames can be used by a station to reserve channel bandwidth before the transmission of an MPDU in order to minimize the bandwidth wasted due to collisions. STAs can choose to use RTS/CTS only when the MSDU exceeds the value of RTS_Threshold. It's recommended that RTS/CTS frames not be used for a lightly loaded medium because of the additional delay imposed by these frames in such a case.

Collision avoidance is performed through a random backoff procedure. When an STA has a frame to transmit, it initially senses the channel to be busy or not. If the channel is busy, the STA waits until the channel becomes idle for a DIFS period and then computes a random backoff time. The random backoff time is an integer value that corresponds to a number of time slots. When the medium becomes idle, following a DIFS period, STAs decrement their backoff timer. In the mean time, the medium might become busy again (the station freezes its timer at such case), or the timer reaches zero, then STA transmits its frame.

Using the above explained methodology, fairness is maintained because each STA must check the channel after every transmission of an MSDU. This way, all STAs have equal probability of gaining access to the channel.

5.1.4 Point Coordination Function

Point Coordination Function (PCF) is an optional functionality. It is connection-oriented. It provides contention-free services enabling STAs to transmit without contending for the channel. Within each BSS, Point Coordination (PC) is performed by the AP. PCF occurs according to a CFP repetition interval, which is initiated a Beacon frame. The Beacon frame is transmitted by the AP to provide synchronization and timing. Time must be allocated for at least one MPDU to be transmitted during the CP. The AP determines how long to operate the CFP during any given repetition interval. Time must be allocated for at least one MPDU to be transmitted during the CP. In case of light

traffic, the AP may decide to shorten the CFP and gives the remainder of the repetition interval for the DCF.

5.1.5 PHY Channelisation

IEEE 802.11b is planned to operate in the unlicensed 2.4 GHz frequency band occupying a bandwidth of approximately 83.5 MHz between 2.4 and 2.4835 GHz. Different frequencies are approved according to the considered country. The USA governmental Federal Communication Commission (FCC) allows IEEE 802.11b to operate within 11 channels. The channels are overlapping as the figure below shows.

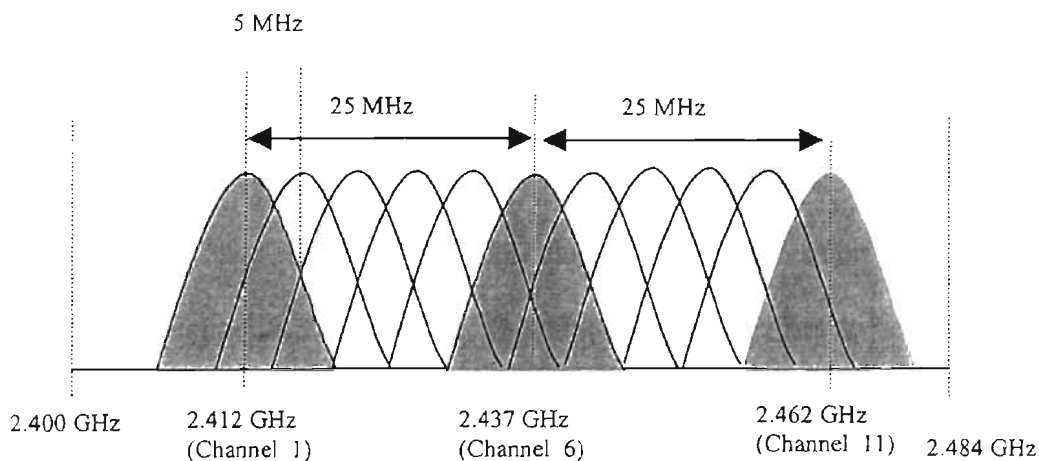


Figure 5.3 North American Channel Selection - Overlapping

The channels are listed numbered 1 to 11 starting from a center frequency of 2412 MHz. The center frequencies are located in 5 MHz intervals, and according to the *adjacent channel rejection* requirement, there has to be five channels between non-overlapping channels in order to avoid interference caused by neighboring APs. As IEEE 802.11b standard has suggested, the receiver adjacent channel rejection is defined between two channels with a separation which is greater than 25 MHz. The rejection shall be equal to or better than 35 dB, with a frame error rate (FER) of 0.08, using 11 Mbps CCK modulation and a PSDU length of 1024 octets.

Channel ID	FCC Channel Frequencies
1	2412 MHz
2	2417 MHz
3	2422 MHz
4	2427 MHz
5	2432 MHz
6	2437 MHz
7	2442 MHz
8	2447 MHz
9	2452 MHz
10	2457 MHz
11	2462 MHz

Table 5.2 DSSS PHY Frequency Channel

The above channel rejection scheme helps constructing a frequency reuse plan, which suggests that neighboring APs can alternate the same frequency sequence (Channel 1, Channel 6, Channel 11). This frequency design has to be taken into concern when choosing operating frequency to the DSSS equipment.

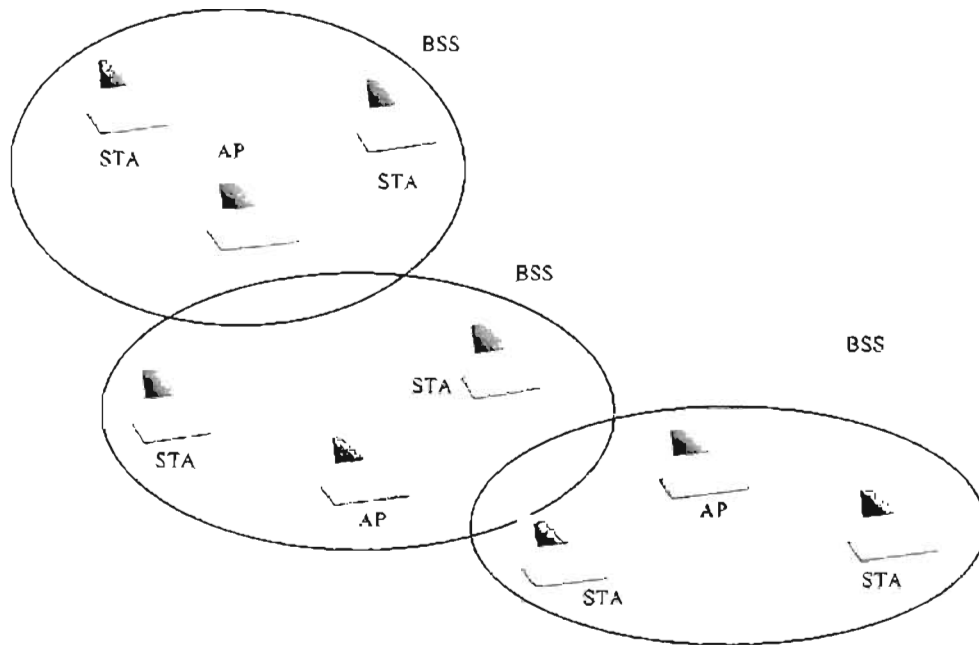


Figure 5.4 Three APs with Overlapping Coverage

Thus it shows above that the 83.5 MHz of available spectrum accommodates up to three equivalent-width, non-overlapping channels. This gives the user the liberty to program up to three APs with one of the three non-interfering channels to be located with overlapping coverage areas.

If one actually overlaps the three above areas perfectly, the aggregate bandwidth in such a localized coverage area can be scaled from 11 to 33 Mbps to provide a denser environment of wireless clients, or to increase bandwidth available to each client. The three APs can be installed just next to each other, and by adjacent channel rejection no interference due to power proximity would occur.

5.2 Channel Overlap with Bluetooth

Already discussed in Chapter III, it's known that interference between Bluetooth and IEEE 802.11 WLAN occurs as both of these technologies use the same unlicensed ISM band, and any overlap in frequency usage at a certain simultaneous usage would lead into destructive interference. Our assumption here is that when collision occurs a Bluetooth (BT) packet is lost, while IEEE 802.11b will see this as a jamming signal effect. As collision occurs, a part of WLAN packet has been corrupted, thus the whole MSDU will have to be retransmitted which hinders the system's throughput. The WLAN channel could be any of those channels given above in the table; for example channel 1 will extend from 2401 MHz to 2423 MHz, thus occupying 22 MHz of the probable BT spectrum territory, as the figure below shows.

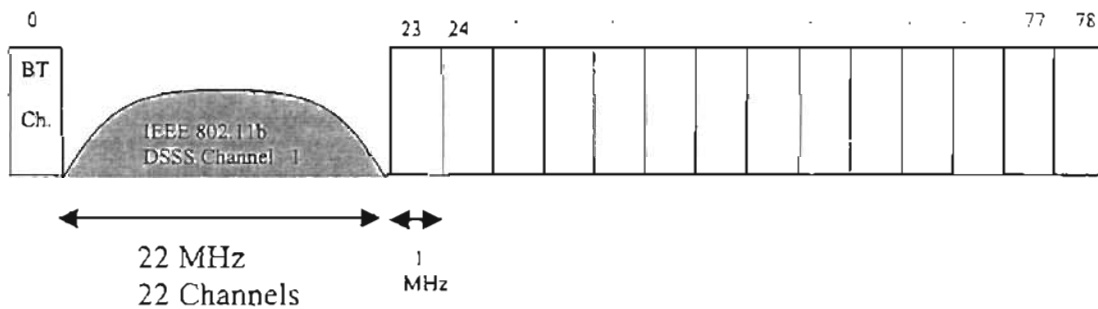


Figure 5.5 Frequency Overlap between IEEE 802.11 Channel 1 and Bluetooth Spectrum

5.3 Probability of Bit Error

The above figure may not show the spectrum overlap up to scale; however, it is assumed that the BT hops (1,2...78,79) are independent, and a hop can occur at any one of these 79 frequencies. Therefore, the probability that BT will hop into the pass-band of IEEE 802.11b WLAN would be $\frac{22}{79}$, thus the probability that BT spectrum won't hop into WLAN frequency range becomes $\frac{(79-22)}{79}$. The probability of bit error of WLAN would differ in value according to the case of jamming and non-jamming as the derivation in chapter II has already presented. In case of jamming (collision), the signal-

power to noise-power ratio (SNR_o) is $\frac{(AT)^2/4}{\left(\frac{N_o T}{4}\right) + \left(\frac{P_j T^2}{4N}\right)}$; A being the WLAN signal

amplitude, T the WLAN bit duration, N_o the noise spectral density, P_j the jammer's power, and N the processing gain implemented. $P_{be(c)}$ will designate the probability of bit

error in case of collision. In case of no collision, $SNR_o = \frac{(AT)^2/4}{N_o T/4}$, and $P_{be(nc)}$ will

designate the probability of bit error. It follows that

$$P_{be(c)} = Q\left(SNR_{o(c)}\right) \left(\frac{22}{79}\right) \text{ and,}$$

$$P_{be(nc)} = Q\left(SNR_{o(nc)}\right) \left(\frac{79-22}{79}\right).$$

This yields to a total probability of bit error

$$P_{be} = P_{be(c)} + P_{be(nc)}$$

The above derivation is taking into account the overlap of the Bluetooth spectrum with only one channel of an IEEE 802.11b network. However, if channel 6 and channel 11, which are non-overlapping, are also within range, then there will be a high probability of overlap.

When studying the effect of jamming on the SNR_o , according to different distances from a BT transmitter, the signal power in dB of the IEEE 802.11b STA seems to maintain a good status as shows in the figure below. The jammer power will vary according to the path loss equation introduced in chapter IV,

$$\begin{aligned} \text{Path loss: } L_{path} &= 20 \log(4\pi r / \lambda), \quad r \leq 8m \\ &= 58.3 + 33 \log(r/8), \quad r > 8m \end{aligned}$$

As for a Bluetooth transmitter, it is quite affected more by the WLAN interference than the latter is being affected by Bluetooth. The probability of channel overlap (collision) increases as channels 6 and 11 are used also. The figures (not to scale) below illustrate this fact.



Figure 5.6 Frequency Overlap between IEEE 802.11 Channel 1 and 6 and Bluetooth Spectrum

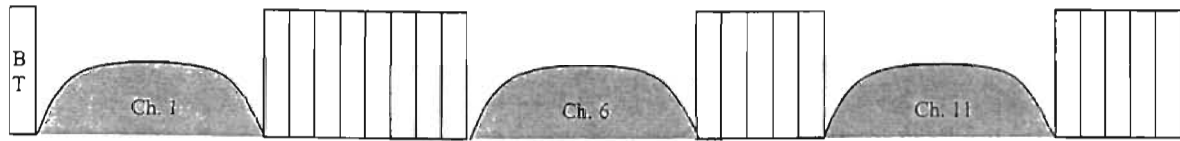


Figure 5.7 Frequency Overlap between IEEE 802.11 Channel 1, 6, and 11 and Bluetooth Spectrum

5.4 Adaptive Frequency Hopping

It's obvious from the above figures that the only means to minimize the number of collisions between Bluetooth and WLAN is actually to make BT hop in an area that isn't being used by any IEEE 802.11b channel. A BT device (master) communicating with another (slave) can manage to hop over frequencies, which are not "contaminated" by any other party's spectrum. This is what is referred to as *Adaptive Frequency Hopping* (AFH). While conventional frequency hopping is blind, AFH use a mechanism that classifies channels (Good or Bad) and adaptively chooses from the pool of 'Good' channels. This mechanism avoids narrow-band interference and frequency-selective fading. It also provides a better Bit-Error-Rate (BER) performance.

5.4.1 Previous Work

In this part, some overview of pervious work in this domain will be studied. Zander *et al.* developed one of the first studies for *Radio Communication Systems Laboratory, Royal Institute of Technology, Sweden*. His system looked as such:

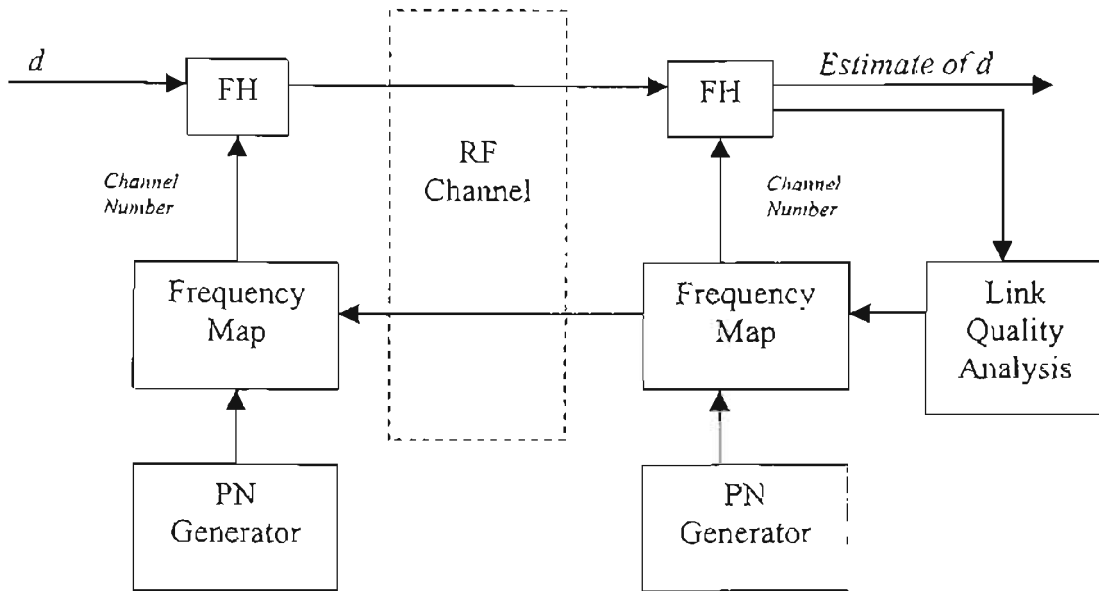


Figure 5.8 Zander *et al* AFH Model

Knuth *et al.* produced another system model for an environment adaptive mechanism in cordless telephones under U.S. patent 5418839 for a home telephone consisting of a handset and a base station. Their adaptive hopping scheme suggested pre-scanning the channels during idle time where a score is applied to each channel. A *Preferred Channel Subset* is selected based on score. Channels within the preferred channel subset, which experience no or little interference over an extended time, are then assigned to the *Clear Channel Subset*. Communication is then carried out in the *Clear Channel Subset*. Channel scanning is done periodically.

Gillis *et al.* designed another apparatus and method for modifying a frequency hopping sequence of a cordless telephone system under U.S. patent 5323447. This adaptive hopping scheme suggested that either the base or handset determines the quality

of each channel of the so-called *First Group* of predetermined channels, by measuring the interference level. The scheme includes selecting one or more channels from a *Second Group* of predetermined channels, which is substituted for channels in the First Group upon which the interference is detected. The figure below reveals the channel change transmission format for Gillis *et al.*

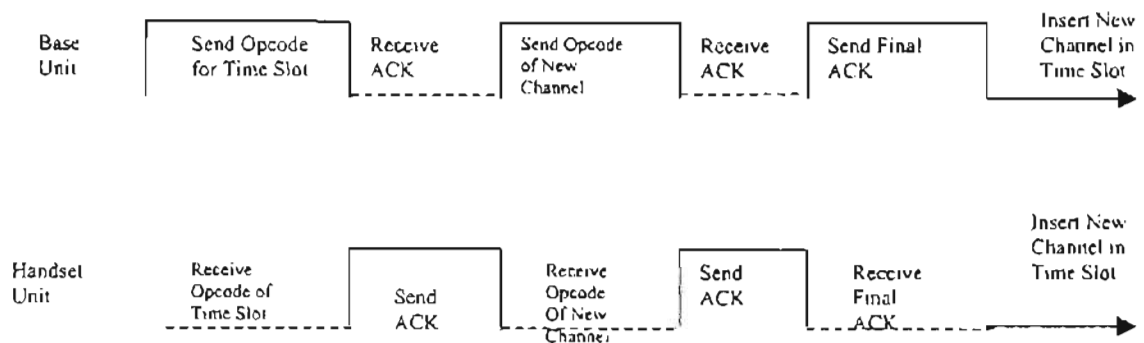


Figure 5.9 Gillis *et al.* Adaptive Frequency Hopping Scheme of a Cordless Telephone System

5.4.2 Channel Classification

Channel classification can be done according to:

- Correlation or error checking of channel access code
- Error checking of head error control (HEC)
- Error checking of cyclic redundancy check (CRC)
- RSSI (Receiver Signal Strength Indicator)
- Packet Loss Ratio (PLR) vs. Channel

5.4.3 Optimal Hopping Sequence

How can the optimal number of frequencies be found?

First, if too many frequencies were used, a greater portion of the available band would suffer interference, which makes placing other users of the band in clear portions not an easy task. The BT system in this case is also more likely to suffer interference from other users of the band. Second, if not enough frequencies were used; interference caused at a specific channel might be too significant in terms of instantaneous packet-error-rate. Also, the chances of a large portion of the channels being simultaneously interfered with are higher.

What are the optimal frequencies to be used?

The optimal hopping channels should suffer the least amount of interference, and also cause the least amount of interference to neighboring systems. Interference

could be local, that's suffered by one end only, and the application may be asymmetric in its sensitivity to interference. Therefore, frequency use doesn't have to be asymmetric and a different hopping sequence may be used in each direction.

What is the optimal order for frequencies?

To provide orthogonality between two different sequences, intended to minimize mutual interference, does not necessarily require pseudo-randomness. However, it is desirable that consecutive transmissions to a specific device preferably be at distant frequencies, in order to allow for frequency diversity and reduce the chances of two

consecutive packet failures. If the two ends of the communications system use a specified frequency, this frequency might as well be used in consecutive time slots.

What is the optimal hopping sequence period?

A shorter period ensures faster acquisition and allows faster adaptation in the presence of another frequency hopping system having the same slot timing. If fast and simple acquisition is desired, and all hopping channels are to be used evenly, the length of the hopping sequence needs to be an integer multiple M of the number of hopping frequencies used. The shortest period possible is equal to the number of hopping channel used ($M=1$).

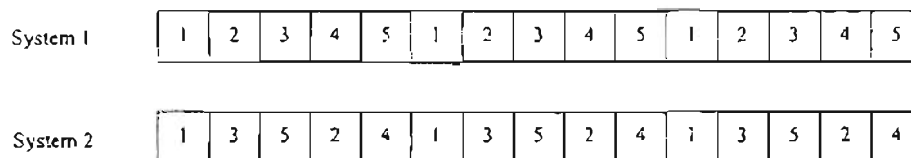


Figure 5.10 Short Cycle



Figure 5.11 Longer Cycle

The two figures above show that repetitive collisions at frequencies shared between the two hoppers lead to quicker replacement of them. For the longer cycle, a “bad” frequency does not always appear as “bad” and will not be replaced as quickly. The situation of lower rate of collisions observed in this case is only temporary (2/15).

5.4.4 THE AFH Algorithm

Packet failure is detected in every device (master and slaves), and the Packet Error Rate (PER) for each frequency received by it is monitored separately. It's preferred not to use payload BER measurements since they are more difficult to handle and are not always available or statistically reliable and offer little benefit in interference avoidance. Frequency replacement is a programmable entity and therefore it's flexible and can be set differently for different applications of different needs. The master and slave can both initiate a frequency replacement in their reception sequence that is the hopping sequence used by the other party's transmitter. Devices using AFH should be able to accommodate asymmetric use of frequencies, which is helpful when the interference suffered at one end is not identical to that suffered at the other end.

What are the system parameters?

The *channel failure counter* for each frequency is incremented till it reaches a *threshold* value, then the corresponding channel is marked as a "bad" frequency and put into a *need-to-replace* queue. The threshold value is the minimal count to be reached in the channel failure counter before a frequency replacement request is stimulated for the corresponding channel. The threshold value would most probably correspond to some wanted Quality-of-Service. The number added to the channel failure counter is called *increment*, and in case of a packet successfully received at that channel, a number called *decrement* is subtracted from the channel failure counter. In order to accelerate the

replacement of those channels, additional increment called *penalty* could be added to the channel failure counter when a predetermined collision occurs.

How does channel replacement occur?

When a channel is found in the need-to-replace queue, channel replacement could be carried out by initiating a *Change_Freq(Bad_Freq, New_Freq)* message. *Bad_Freq* would be the Bad Frequency Number (5 bit) to be replaced. *New_Freq* would be the New Frequency Number (5 bit) to be used instead. Whichever is the initiator of this message may replace the frequency immediately after sending the message; whereas the recipient of the message will replace the frequency immediately after receiving the message, and have to send an acknowledgment message, *Accepted*. After a successful reception of the *Accepted* message, the frequency change procedure will end, and at this time the next frequency replacement request is allowed to be sent. The two devices will still be communicating through at least 78 frequencies during the replacement procedure, and at the end of the process all 79 frequencies will be aligned. Only one change is done at a time, and communications can't be lost as a result of possible failure in the replacement process. The frequency replacement procedure in a device will affect the frequencies in the reception direction only since AFH can be asymmetric.

5.4.5 Structure of AFH

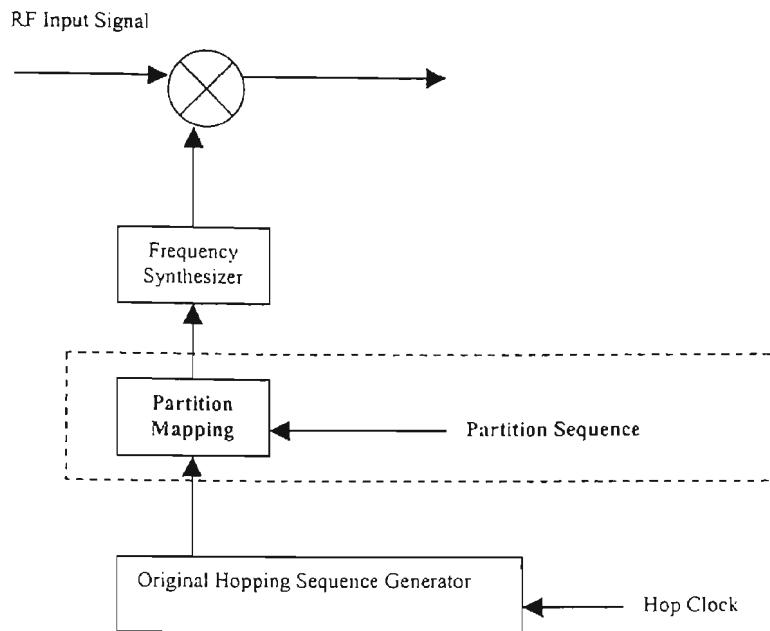


Figure 5.12 Structure of AFH

5.4.6 Device Identification and Operation Mode

A Bluetooth device could identify if another device uses the AFH operational mode by using LMP (Link Manager Protocol) messages for verification. LMP messages have higher priority over user data, referring to the Bluetooth Specifications. The figure below shows how the master-slave communication takes place. This information is exchanged once a new slave has joined a piconet whose master has the option of using AFH mode. A master inquiry if the slave uses AFH might be replied by either “yes” or “no”. *LMP_not_accepted* means that a slave doesn’t use AFH; *LMP_accepted* means otherwise. Low power devices may not support AFH. The master should make the final decision on channel classification of course. A slave could notify the master of a bad channel and ask for channel replacement or a master could sense that a slave is having

error reception and initiate channel replacement. The LMP request should carry extra parameters of the partition sequence. The slave would use the new sequence if the LMP command has succeeded. The master controls all the sequences to use for every slave. AFH might be terminated in case of loss of synchronization or if the master asks for its termination.

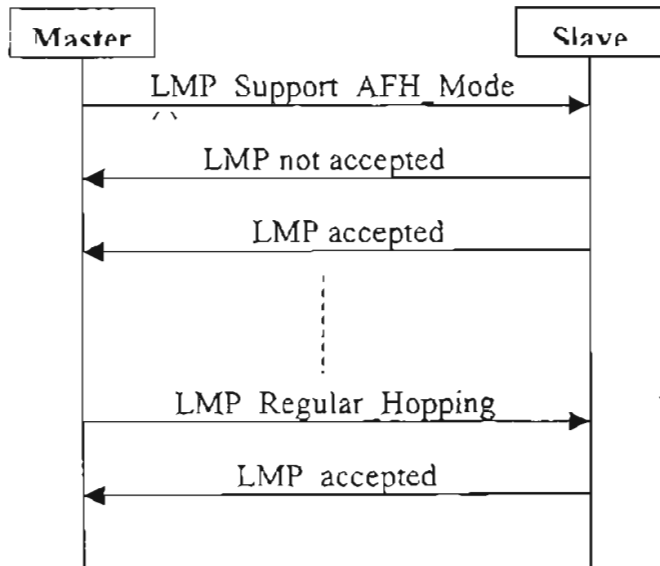


Figure 5.13 Device Identification and Operation Mode for AFH

5.5 The Automatic Interference Rejection System (AIRS)

For Bluetooth and IEEE802.11b Systems

Now that we know how to make a signal adapt to interfering hazards, we can visualize a system to avoid or reject interference automatically. How can we build such a system? Such a system has to be able to determine a few parameters. The system has to be able to determine the existence of the IEEE 802.11b channel in the BT spectrum territory. Second, the system has to predict the level of interference caused by such channel presence. Then, the system must have knowledge of its desired BER performance being sought (application dependent). Fourth, it has to produce a PN code that allows the partition of the frequency-hopping spectrum. Finally, the resulting PN code should be fed to the BT modulator.

In this section the architecture of an Automatic Interference Rejection System (AIRS) is introduced. The AIRS system is an enhancement to the Bluetooth system such that the interference between the IEEE802.11b system and the Bluetooth system is minimized. The research developed in this thesis does not provide the PN code sequence that must be utilized. Instead, this thesis provides a general algorithm that the Bluetooth PN code needs to follow to obtain the desired bit error rate (BER).

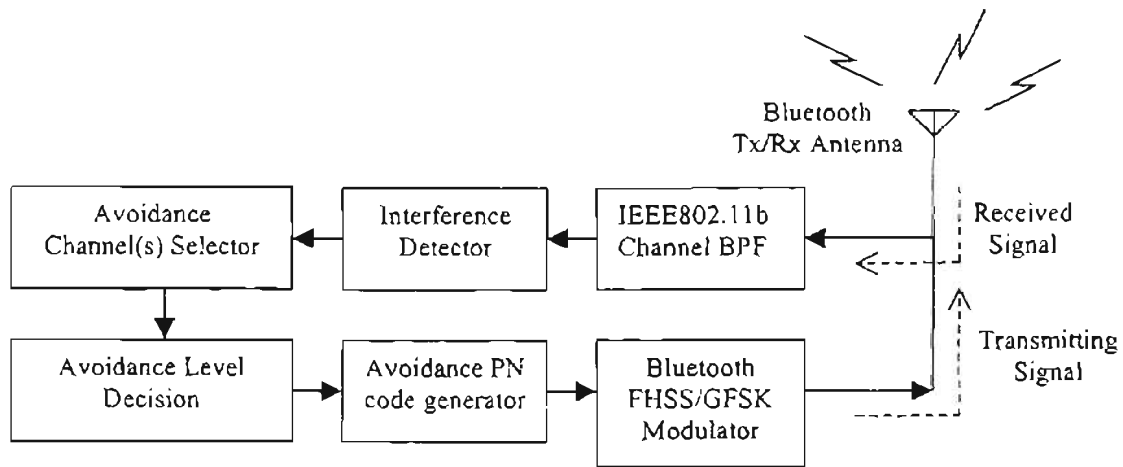


Fig. 5.14 The Automatic Interference Rejection System (AIRS) For Bluetooth and IEEE 802.11b

The proposed system checks for the DSSS channel existence first by using a band-pass filter. A detector is used to measure the interference caused by the overlapping frequency range, and as a result an avoidance scheme can be implemented corresponding to the range of overlap. Then, at that stage the station can determine, according to the desired bit-error-rate, the avoidance level which triggers the needed PN code that makes the FHSS/GFSK signal hop around the uncontaminated area. Figure 5.14 shows the AIRS block diagram model.

In general it is difficult to develop an avoidance system with DSSS since the spreading of the spectrum cannot be controlled simply. On the other hand, Bluetooth systems can have simple avoidance mechanisms added to their PN code-switching algorithm, which can be equally designed to reduce the BER performance of both systems at the same time.

5.6 Performance of Bluetooth in AWGN and IEEE 802.11b Interference

The average probability of bit error (P_e) for Bluetooth frequency hopping spread spectrum (FHSS) systems with IEEE802.11b interference is derived as follows.

First, the average probability of bit error ($P_{e(AWGN)}$) for Bluetooth slow frequency hopping spread spectrum (FHSS) systems under the influence of AWGN can be derived from the M-ary FSK signal AWGN performance. Based on the Bluetooth system model we assume a receiver model of noncoherent detection, matched filtering for maximum SNR gain, and envelop detection for baseband demodulation. The average probability of bit error due to AWGN becomes

$$P_{e(AWGN)} = \sum_{k=1}^{M-1} \left(\frac{(-1)^{k+1}}{k+1} \right) \binom{M-1}{k} \exp\left(\frac{-kE_s}{(k+1)N_0} \right),$$

where $E_s = (\log_2 M)E_b$. To describe the Bluetooth system we apply binary FSK slow-hopping FHSS, which results in

$$P_{e(AWGN)} = \frac{1}{2} \exp\left(\frac{-E_b}{2N_0} \right).$$

Second, the effect of the IEEE802.11b system signal interference on the P_e performance of the Bluetooth signal can be represented as

$$P_{e(IEEE802.11b)} = \frac{\alpha}{2} \exp\left(-\frac{\alpha E_b}{2I_0} \right),$$

where α is the fraction of the Bluetooth bandwidth (i.e., 79 MHz in the U.S.A.) in which the IEEE802.11b signal is interfering. We define α to exist in the range of $0 < \alpha \leq 1$. In

the equation of $P_{e(IEEE802.11b)}$: the IEEE802.11b transmission power is represented as I_0 [W] and for simplicity we assume the IEEE802.11b DSSS transmission signal to be modeled as a zero mean Gaussian random process with a flat power spectral density. This assumption well fits the transmission signal model of DSSS signals, such as the IEEE802.11b signal. The attenuation factor of the interference signal is also function of the carrier frequency and the distance (r) between the Bluetooth system and the IEEE802.11b interfering signal source. Therefore the interference signal can be modeled as

$$J(r) = \frac{I_0 \alpha \lambda}{16\pi^2 r^2} \quad \text{for } 0 < \alpha \leq 1.$$

Combining the effect of AWGN and IEEE802.11b interference signal component we obtain the average probability of bit error of the Bluetooth system under the influence of AWGN and IEEE802.11b as

$$P_e = \{P_{e(AWGN+IEEE802.11b)}\} = \frac{1}{2} \left\{ e^{-\frac{E_b}{2N_s}} + \alpha e^{-\frac{\alpha E_b}{2J(r)}} - \frac{\alpha}{2} e^{-\frac{E_b}{2} \left(\frac{\alpha N_s + J(r)}{N_s J(r)} \right)} \right\}.$$

There are several additional components that need to be considered to make the derivation more comprehensive to include the effects of multipath fading, lognormal shadowing, and other 2.4 GHz ISM band interfering signals. However, due to the fact that this thesis is focused on minimizing the interference between IEEE802.11b WLAN systems and Bluetooth systems, the derivation will only consider the effect of AWGN and co-channel interference.

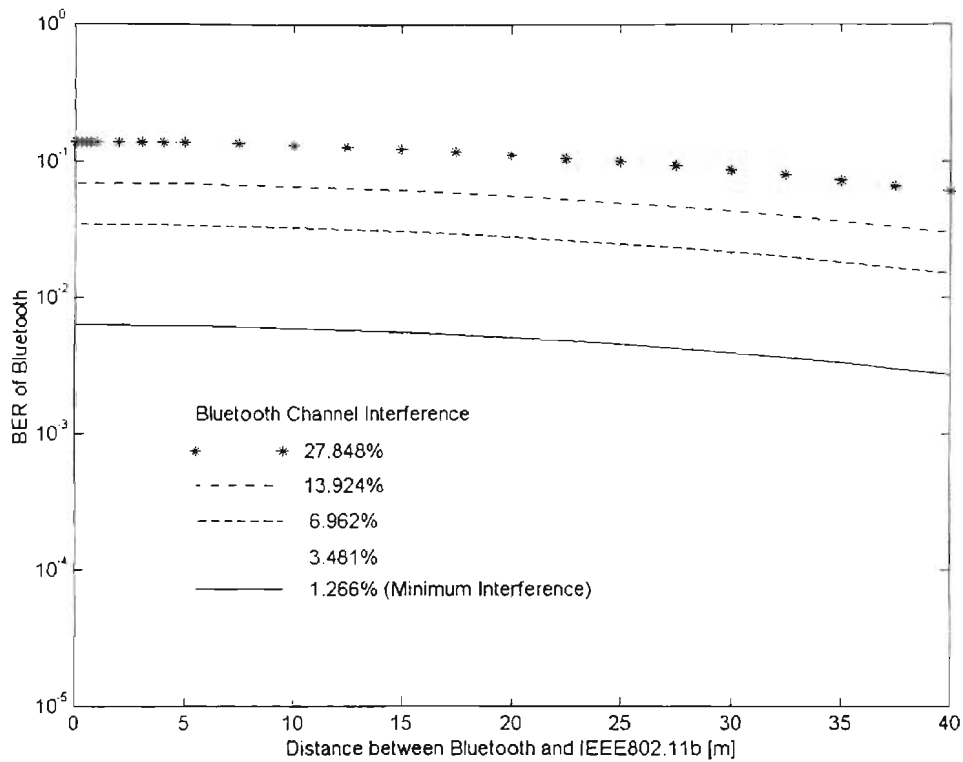


Figure 5.15 The BER performance of Bluetooth with IEEE802.11b interference and AWGN.

Normally, both IEEE 802.11b and BT would actually overlap up to 22MHz out of 79 MHz at the worst case. This amount of overlap makes it very inconvenient for some applications. The very top star-dotted line is actually the worst-case scenario to be assumed. Whereas, the very low line is actually what can be recognized as the bound line that the FCC regulation states. Therefore, our BT system's operation area is anyone of the curves in between these two lines.

5.7 Performance of IEEE 802.11b in AWGN and Bluetooth Presence

In this section, the average probability of bit error (P_e) for the IEEE802.11b system with Bluetooth interference is derived. The Bluetooth interference signal is a FHSS/GFSK signal where the transmission power is noted as P_j . Similar to the method applied to the Bluetooth BER derivations; the attenuation factor of the Bluetooth interference signal is also function of the carrier frequency and the distance (r) between the Bluetooth system and the IEEE802.11b interfering signal source. Thus the interference signal can be modeled as

$$T(r) = \frac{P_j \lambda^2}{16\pi^2 r^2}$$

The IEEE802.11b DSSS/QPSK BER performance can be derived from combining the effect of AWGN and the Bluetooth interference signal components. The IEEE802.11b probability of bit error is

$$P_e = P_{e(AWGN+Bluetooth)} = \beta Q\left(\sqrt{\frac{A^2 T}{N_0}}\right) + (1 - \beta) Q\left(\sqrt{\frac{A^2 T}{N_0 + T(r) T_c}}\right).$$

where β is the fraction of the transmission bandwidth that experiences interference from Bluetooth signals. Per channel of the IEEE802.11b, β will be in the range of $0.012658 \leq \beta \leq 0.27848$ based on the AIRS PN code applied.

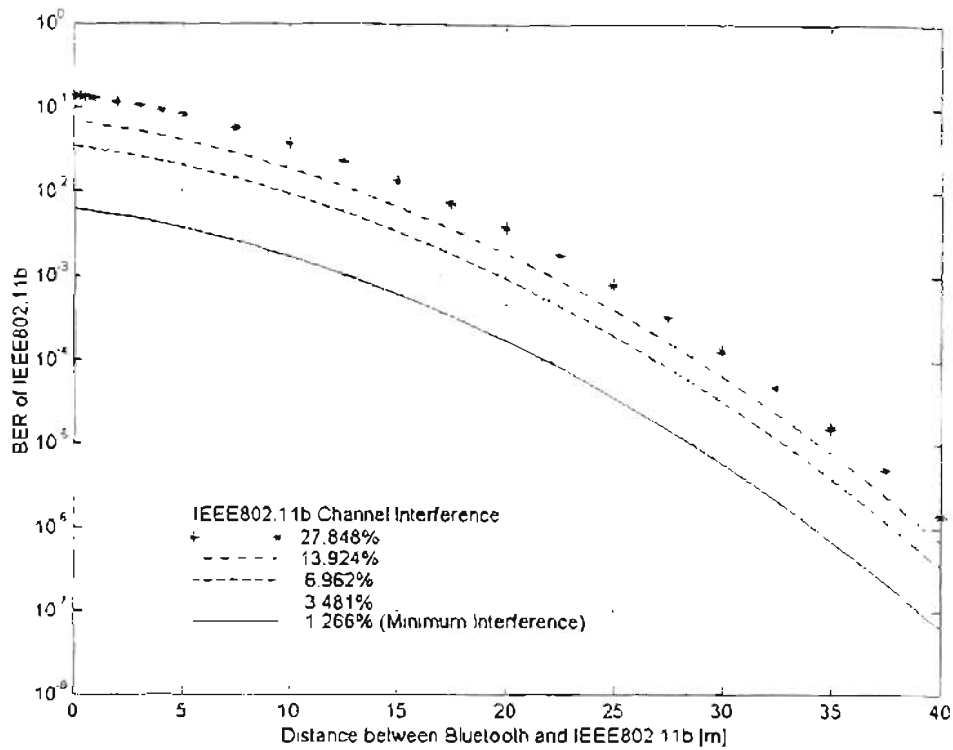


Figure 5.16 The BER performance of IEEE802.11b with Bluetooth interference and AWGN

The bit-error-rate (BER) of IEEE802.11b for an overlap of $\frac{22}{79}$ which is equal to 27.848% shows to be a little bit more than 10^{-1} . At a distance of 10m the BER value is almost 0.06 for the considered overlap of 27.848% (showed by the star-line at the very top); however, it falls to at least one tenth of its value if both systems were forced to have an overlap of 1.266%. Normally, both systems would overlap, as explained before, according to the ratio $\frac{22}{79}$. However, using the suggested Automatic Interference Rejection Scheme, a system can avoid interference to 50% of its original 27.848% value, that is 13.924% (showed by the dashed-dotted line just below the star-line), for which the

system would give a better BER performance. If a system reduces its overlap value by 50% each time, it would reach an overlap ratio of 1.266%. Reducing the overlap range more and more, the Bluetooth system's frequency hopping space would become more and more smaller, and has to take into account the FCC regulation stating that a frequency hopping system should hop at least 75 out of 79 hopping frequencies for at least 0.4 seconds out of 30 seconds. Using this mechanism, a system can adjust itself according to the desired BER and distance of usage. Let's say a BER = 10^{-3} or less is desired at a distance of 20m, then the system performance graph would be any one of the lowest three lines (dashed, dotted, and full lines). As the distance is increased, the BER performance gets better. At a certain distance, a system is able to choose any of the five performance lines to identify its performance depending on the desired BER. This same observation can be made for the BER performance of Bluetooth as well.

Chapter VI

Conclusion

This thesis has investigated the co-existence problem between two of the most used technologies in nowadays enterprises, IEEE 802.11 WLAN cards and Bluetooth cards. Observers say that both technologies will overwhelm the market in the next few years; Bluetooth chips will be almost in all communication equipment very soon, starting with computers and ending in cell phones.

In Chapter II, some of the literature review about the specifications of IEEE 802.11 WLAN and Bluetooth has been reviewed. Also, some focusing on the performance of spread spectrum systems was given at that chapter because of the importance of having knowledge of the different techniques which has been invoked for interference avoidance between Direct Sequence and Frequency Hopping schemes.

In Chapter III, an actual study of different types of interference has been reviewed. This chapter has been meant to give a good look at effects of interference on a system's performance.

Chapter IV is an actual approach to study WLAN/Bluetooth co-channel interference based on a lot of readings of the previous work done so far by other authors. Chapter IV also carries many personal suggestions about finding a solution for that issue.

Chapter V is actually based on the material and suggestions given in the previous chapter, and presents a solution, which can be among of many others presented earlier in this domain.

The automatic interference rejection system (AIRS) has been developed as an enhancement to the Bluetooth system such that the interference between the IEEE802.11b system and the Bluetooth system is minimized. The research developed in this thesis does not provide the PN code sequence that must be utilized, but provides direct guidelines that allow the interference to be reduced. Numerous PN codes that satisfy the AIRS algorithm exist, and therefore, is left for the system implementer to decide. Some of the key observations are summarized below.

Due to the fact that the Bluetooth system utilizes low transmission power and a TDD multiple access mechanism, and also considering the fact that the transmission data rates are relatively low compared to the IEEE802.11b system, the BER performance of the Bluetooth system with IEEE802.11b interference shows a relatively poor BER performance when no AIRS protection is provided. The IEEE802.11b signals act as wideband interference signals and therefore have a significant effect on to the BER performance of Bluetooth systems. In addition, for the IEEE802.11b system, the Bluetooth signals act as narrow band jamming signals to the IEEE802.11b signals and show significant performance degradation.

Significant improvements are shown in both the IEEE802.11b system and the Bluetooth system when the AIRS is in operation and the interference level is reduced. For both the IEEE802.11b system and the Bluetooth system, the BER is lowered down to less than 10% of the original BER performance when the AIRS applies its minimum interference scheme (1.2658% interference), which is the lowest possible interference ratio that the FCC permits.

References

1. Specification of the Bluetooth System, Version 1.0 Draft Foundation, July 5th 1999.
2. IEEE Std 802.11, Wireless LAN Medium Access Control and Physical Layer Specifications, IEEE, Inc., 1997.
3. Lam, A. W.; Tantarana S., Theory and Applications of Spread-Spectrum Systems, May 1994.
4. Takaya, K.; Maeda, Y.; Kuwabera, N., "Interference Characteristics between 2.4-GHz-band Middle-Speed Wireless LANs Using Direct Sequence and Frequency Hopping". *Electromagnetic Compatibility, 1999, International Symposium on, 1999*, Page(s): 690 – 693.
5. Glas, J.P.F, "On Multiple Access Interference in a DS/SS Spread Spectrum Communication System", *Spread Spectrum Techniques and Applications, 1994. IEEE ISSSTA '94., IEEE Third International Symposium on, 1994*, Page(s): 223-227 vol.1.
6. Kumpumaki, T.J.; Isohookana, M.A.; Juntti, J.K., "Narrow-band Interference Rejection Using Transform Domain Signal Processing in a Hybrid DS/FH Spread-Spectrum System", *MILCOM 97 Proceedings, Volume: 1, 1997*, Page(s): 89 – 93 vol.1.
7. Asmer, H.; Sheikh, A.; Gulliver, T., "A Hybrid DS/FH Spread Spectrum System for Mobile Radio Channel: Performance and Capacity Analysis", *Vehicular Technology Conference, 1993., 43rd IEEE, 1993*, Page(s): 305 – 308.
8. Proakis, John G., Digital Communications, 4th Edition.
9. Chiasserini, C. F.; Rao, R. R., "Performance of IEEE 802.11 WLANs in a Bluetooth Environment", *Wireless Communications and Networking Conference, 2000. 2000 IEEE, Volume:1, 2000*. Page(s):94-99.
10. Ennis, G., "Impact of Bluetooth on 802.11 Direct Sequence", *IEEE 802.11-98/319, September 1998*.
11. Zyren, J., "Extension of Bluetooth and 802.11 Direct Sequence Model", *IEEE 802.11-93/378, November 1998*.
12. Zyren, J., "Reliability of IEEE 802.11 Hi Rate DSSS WLANs in a High Density

Bluetooth Environment”, Bluetooth’99, June 8 1999.

13. Zyren, J., “Reliability of IEEE 802.11 WLANs in Presence of Bluetooth Radios”, IEEE 802.15-99/073r0, September 1999.
14. Kamerman, A., “Coexistence between Bluetooth and IEEE 802.11 CCK Solutions to Avoid Mutual Interference”. Lucent Technologies, January 5 1999.
15. Crow, B.; Widjaja, I; Kim, J; Sakai, P, “Investigation of the IEEE 802.11 Medium Access Control (MAC) Sublayer Functions”. INFOCOM '97. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Driving the Information Revolution., Proceedings IEEE . Volume: 1 , 1997 Page(s): 126 -133 vol.1
16. <http://alpha.fdu.edu/~anandt/802.11b.html>
17. Pearson, B, “Complementary Code Keying Made Simple”. Intersil Corporation, May 2000, AN9850.1
18. Halford, K.; Halford, S.; Webster, M; Andern, C, “Complementary Code Keying for Rake-Based Indoor Wireless Communication”. 1999 IEEE.
19. doc.: IEEE 802.15-01/252r0. Bandspeed Inc, Integrated Programmable Communications, Inc., Texas Instruments. May 2001.
20. doc.: IEEE 802.11-01/169r0. Eliezer, O.; Michael, D., Texas Instruments. March 2001.
21. doc.: IEEE 802.15-00/367r0. Gan, H.; Treister, B.; Bandspeed Pty Ltd. November, 2000
22. doc.: IEEE 802.15-091r0. Rios, C. 3Com. September 1999.
23. doc.: IEEE 802.15-01/057r2. Integrated Programmable Communications, Inc. March 10, 2001.
24. doc.: IEEE 802.15. Sizer, T. Lucent Technologies / Bell. November 2000.
25. doc.: IEEE 802.15-00/229r0. Lansford, J, Modilian. July 2000.
26. doc.: IEEE 802.15-00/293r0. Shellhamer, S., Symbol Technologies. September 2000.
27. doc.: IEEE 802.15-00/220r0. Voltz, P. J., Polytechnic University. July 2000.
28. doc.: Chhaya, H. S.; Gupta, S., “Throughput and Fairness Properties of Asynchronous Data Transfer Methods in the IEEE 802.11 MAC Protocol”. 1995 IEEE.

29. <http://www.intersil.com/design/prism/papers/perform.asp>
30. <http://www.euro.dell.com>
31. http://www.tml.hut.fi/Opinnot/Tik-110.551/2000/papers/IEEE_802/wlan.html
32. <http://www.alloy.com.au>
33. http://www.datalinkready.com/cisco/350/a350c_ds.htm
34. http://www.xircom.xoni/cda/page/1,1298,0-0-1_1-1631-1644.00.html
35. doc.: IEEE 802.15-00/133r0. Shellhammer S., Symbol Technologies. May 2000.

VITA

Shadi Hannouf

Candidate for the Degree of

Master of Science

Thesis: Co-Channel Interference between IEEE 802.11 WLAN and Bluetooth

Major Field: Electrical Engineering

Biographical:

Personal Data: Born in Tripoli, Lebanon, on January 1, 1979.

Education: Received a Bachelor of Science in Electrical Engineering from University of Balamand, Tripoli, Lebanon in August 1999. Completed the requirements for the Master of Science degree with a major in Electrical Engineering at Oklahoma State University in August, 2001.

Experience: Employed by Oklahoma State University, School of Electrical and Computer Engineering as a research assistant, 2000 to 2001.