12-2005

Physical Layer Simulation Study for the Co-existence of WLAN Standards

Chad Joseph Kiger
University of Tennessee - Knoxville

Recommended Citation

Kiger, Chad Joseph, "Physical Layer Simulation Study for the Co-existence of WLAN Standards. " Master's Thesis, University of Tennessee, 2005.
https://trace.tennessee.edu/utk_gradthes/2121

To the Graduate Council:

I am submitting herewith a thesis written by Chad Joseph Kiger entitled "Physical Layer Simulation Study for the Co-existence of WLAN Standards." I have examined the final electronic copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Electrical Engineering.

Mostofa K. Howlader, Major Professor

We have read this thesis and recommend its acceptance:

Donald W. Bouldin, Daniel B. Koch, Stephen F. Smith

Accepted for the Council:
Carolyn R. Hodges

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

To the Graduate Council:

I am submitting herewith a thesis written by Chad Joseph Kiger entitled “Physical Layer Simulation Study for the Co-existence of WLAN Standards.” I have examined the final electronic copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Electrical Engineering.

Mostofa K. Howlader
Major Professor

We have read this thesis
and recommend its acceptance:

Donald W. Bouldin

Daniel B. Koch

Stephen F. Smith

Accepted for the Council:

Anne Mayhew
Vice Chancellor and
Dean of Graduate Studies

(Original signatures are on file with official student records.)

Physical Layer Simulation Study for the Co-existence of WLAN Standards

A Thesis
Presented for the
Master of Science Degree
The University of Tennessee, Knoxville

Chad Joseph Kiger
December 2005

Dedications

I would like to dedicate this thesis to everyone who has aided in my achievement of obtaining a master's degree from the University of Tennessee. First and foremost, I would like to dedicate this thesis to my parents, without their help I would not have been able to attend UT. My mother, Janice Kiger, for always believing in me and letting me make my own mistakes. My father, Ricky Kiger, for never allowing me to settle for imperfection and always making me find ways to improve. Jeremy Kiger, my older brother, teaching me strength and to never give up through our various brotherly battles, and Roxanne Kiger, my older sister, who paved the path of high expectations in high school for me to achieve. My little brother and sister, Kurt Kiger and Heather Kiger, for understanding why I had to be in Tennessee while they were growing up at home in Michigan. My grandparents who always encouraged me. High school teachers such as Eugene Huber and Brian Girbach who realized my potential and held me to a higher standard. Lastly I dedicate this thesis to my friends and girlfriend here in Knoxville, without their friendship and support I may never have stayed at UT and had my many great experiences.

Acknowledgements

I would like to extend my appreciation to everyone who has helped me along the path of completing my Master of Science degree in Electrical Engineering. First of all, without the help of Dr. Mostofa Howlader, none of this would have been possible. I would like to thank him for both his guidance and the honor of allowing me to be a part of his Wireless Communications Research Group; it was truly a fulfilling experience. I would also not have been able to pursue my degree without the help of Dr. Donald Boudlin. Not only for the lessons learned in his classroom, as well as the support he has shown through serving on my committee, and the help that he, along with Michael Crabtree and Dr. Robert Bodenheimer, have granted me through the aid of the Bodenheimer Fellowship. It was a privilege to be recognized, and I hope I will always live up to their expectations. This accomplishment would also not have been possible without the aid of my other two committee members, Dr. Daniel Koch and Dr. Stephen Smith. Dr. Koch through the skills developed in his classroom and Dr. Smith for his encouragement at ORNL.

This research work has been performed in the Wireless Communications Research Group (WCRG) at University of Tennessee, Knoxville, sponsored by the RF & Microwave System Group (RFMSG) of the Oak Ridge National Laboratory (ORNL) under the contract UT-B 4000025441 and UT research account number R011344113. I am also especially indebted to Paul Ewing, leader of the RFMSG, who has provided me with this great opportunity.

Abstract

Interference is a prime factor that limits the performance of devices within the 2.4 GHz ISM Band. Due to the ISM Band being unlicensed and free to all users, there is an abundance of devices within this frequency range. The three most prominent of such devices used for data communication consist of Bluetooth, Wifi, and Zigbee. In order to understand whether these three protocols can co-exist with each other, a physical layer system model will be developed for each protocol. These systems models will be combined and their interaction with each other examined to determine the effects of the interference under different channel conditions. The channel models will consist of general AWGN and Rayleigh fading channels, along with a site-specific case involving both Ricean and Rayleigh fading.

Preface

In today's world, there is a growing concern regarding the state of the environment and the effects that pollution will have on the future existence of mankind. Words such as global warming and the ozone layer are predominantly finding their way into the news coverage. Some experts believe that the increase of CO_2 in the atmosphere due to the burning of fossil fuels for electricity generation is at the heart of the cause of the depleting ozone layer and the increase in global warming.

Because of the diminishing natural resources and the effects that the burning of fossil fuels has on the atmosphere, there is an expanding desire to reduce the dependency on fossil fuels for electricity and focus more on nuclear power. With this shifting of demand stems a need for more efficient processes from current nuclear facilities and also requires for newer plants to be constructed. This results in a revamping of the way in which power plants will be constructed because since the Three Mile Island incident at the Pennsylvania facility in 1979, no new nuclear facilities have been constructed in the United States. Since then there have been major advancements in technology, which could be used to improve the efficiency of these plants. Therefore, not only do the facilities being constructed need to be updated, but also updates to the legacy systems in use in current plants need to be installed.

One small area in which these updates need to take place in is in the monitoring and sensing aspect of a nuclear power plant. One convenient and cost effective practice that could be employed would be to shift from a dependency on wired communications to wireless. Everything from accessing the Internet to monitoring reactor conditions could be done using wireless devices that are already developed. This is not only convenient from the aspect of the portability and unobtrusiveness of wireless devices, but it is also cost effective in that running wires in a nuclear power plant can cost up to $2,000 per foot for the required specialized wiring.[1]

Two obstacles prevent the widespread use of wireless devices within the confines of a nuclear power plant, and they are security and robustness. Security stems from either information being captured form an outside source, or an outside saboteur introducing his or her own data into different aspects of the facility. Since security deals more with data encryption, it will not be dealt within this report. This report will therefore deal with the robustness or reliability of wireless devices. More specifically, the ability for wireless devices to coexist in an environment where there is the presence of other interfering devices.

The Nuclear Regulatory Commission (NRC), the governing body over the rules and guidelines imposed upon nuclear power plants, is very interested in this topic of interference caused by wireless devices because in order for new procedures and applications to be installed into nuclear facilities, they must first pass the strict policies of the NRC to allow for safety. The NRC will not authorize the use of wireless devices until they are confident the devices will work properly and not harm other aspects of nuclear power production. This is the task that the NRC has placed upon Oak Ridge National Labs and me in particular, to develop a software tool to be used in conjunction with other methods of determining the coexistence of wireless devices within a nuclear power plant.

Contents

List of Tables

List of Figures

List of Abbreviations

ARQ	Automatic Repeat Request
ASK	Amplitude Shift Keying
AWGN	Additive Gaussian White Noise
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
CAD	Computer Aided Design
CB	Citizens Band
CCK	Complementary Code Keying
CDMA	Code Division Multiple Access
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DQPSK	Differential Quadrature Phase Shift Keying
DSSS	Direct Sequence Spread Spectrum
FCC	Federal Communications Commission
FEC	Forward Error Correction
FHSS	Frequency Hopping Spread Spectrum
FSK	Frequency Shift Keying
FWT	Fast Walsh Transform
GFSK	Gaussian Frequency Shift Keying
GHz	Gigahertz
GMSK	Gaussian Minimum Shift Keying
GPS	Global Positioning System
GSM	Global System for Mobile Communication
HVAC	Heating, Ventilation, and Air Conditioning
IEEE	Institute of Electrical and Electronic Engineers
IFFT	Inverse Fast Fourier Transform
IR	Infrared
ISI	Inter-Symbol-Interference
kHz	kilohertz
LAN	Local Area Network
LOS	Line-of-Sight
MAC	Medium Access Control Layer
MAN	Metropolitan Area Network

MBOA	Multi-band OFDM Alliance
MBWA	Mobile Broadband Wireless Access
MHz	Megahertz
MSK	Minimum Shift Keying
NLOS	Non Line-of-Sight
NRC	Nuclear Regulatory Commission
OFDM	Orthogonal Frequency Division Multiplexing
O-QPSK	Offset Quadrature Phase Shift Keying
PAN	Personal Area Network
PBCC	Packet Binary Convolutional Code
PDA	Personal Data Assistant
PHR	PHY Header
PHY	Physical Layer
PLCP	Physical Layer Convergence Protocol
PPDU	PHY Beacon Packet
PSDU	PLCP Service Data Unit
PSK	Phase Shift Keying
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
SFD	Start Frame Delimiter
SHR	Synchronization Header
SIG	Special Interest Group
SIR	Signal-to-Interference Ratio
SNR	Signal-to-Noise Ratio
TDMA	Time Division Multiple Access
UHF	Ultra High Frequency
UNII	Unlicensed National Information Infrastructure
UWB	Ultrawideband
VHF	Very High Frequency
WAN	Wide Area Network
Wifi	Wireless Fidelity
WiMax	World-Wide interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network

Chapter 1

Introduction

1.0 Wireless Communication

What is wireless? Werbach describes wireless communications as “a form of magic. Words and pictures fly over invisible pathways with near instantaneous speed.”[2] Wireless communication allows for the production of music from a device smaller than a matchbox toy car, or the ability to control a surveillance aircraft from the comfort of an office. It also has the capability to permit a conversation between two people on opposite ends of the globe, as if they were standing right next to each other. Before dealing with the different methods that could be implemented to perform such tasks, it is important to learn more about the backbone of wireless communications.

Wireless communications is accomplished through the use of electromagnetic waves. A radio wave can “oscillate at frequencies between about 3 kilohertz (kHz) and 100 gigahertz (GHz).”[2] This spectrum is broken down into multiple sections and either sold to telecommunication companies for private use, reserved for government use, or considered to be unlicensed and free to all users so long as they abide by government regulations. The spectrum allocation is pictured in Figure 1.1. The lower portion of the spectrum, any frequency below 2.4 GHz, is used for a wide variety of devices and purposes, but is primarily concerned with voice communication.

Entertainment uses of this lower spectrum include AM and FM radio, from 535 kHz to 1.7 megahertz (MHz) and 88 MHz to 108 MHz respectively. Television stations are also located in this spectrum, ranging from 54 MHz to 220 MHz (VHF) and 470 to 890 MHz (UHF), subtracting

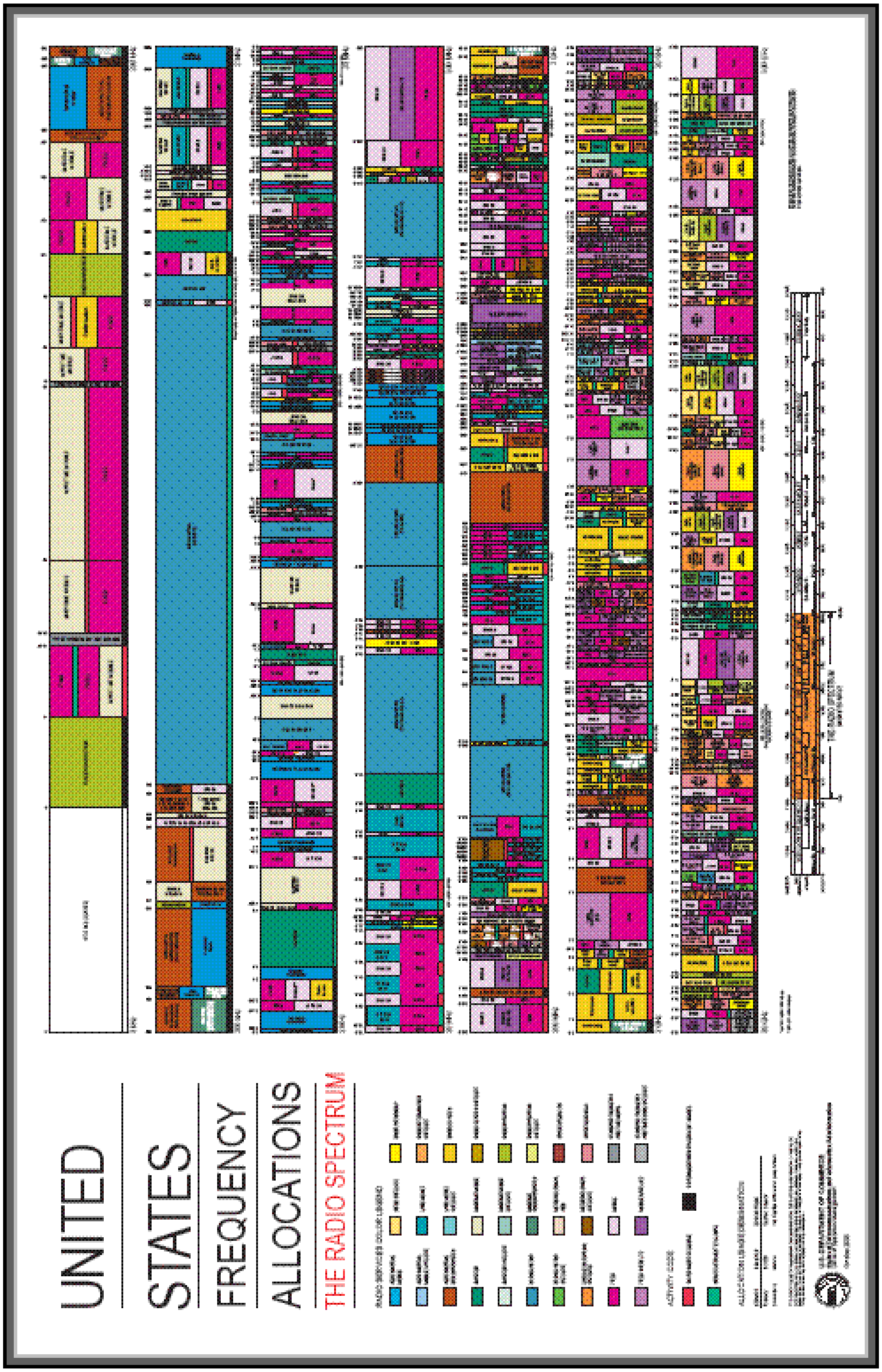


Figure 1.1 - United States Frequency Allocation

the band of FM radio frequencies. Voice communication in this lower spectrum can be implemented in cell phones, which use the frequencies 824 MHz to 849 MHz, or in Citizen Band (CB) radios from 26.96 MHz to 27.41 MHz. Other devices also operate within the frequencies of this spectrum and include remote controlled toys, Global Positioning System (GPS), and even garage door openers.

1.1 Wireless Specifications

In wireless communications there is a growing demand to shift the emphasis from voice to data communication, in order to achieve the higher data rates required for data communication, the upper spectrum needs to be taken advantage of which includes all frequencies between 2.4 GHz and 60 GHz. Many devices currently operate within this range, especially within the unlicensed bands. To promote both homogeneous behavior and interoperability, the IEEE has formed standards for devices to conform to so that some sort of order can be maintained within these frequency bands. Standards, which deal with wireless communication, consist primarily of the family of 802 standards. Several of these standards along with their intended coverage areas and corresponding bit rates can be found in Figure 1.2. This figure shows that there are four main types of coverage areas, PAN, LAN, MAN, and WAN. A Personal Area Network (PAN) is defined as the immediate space surrounding a device, usually confined to a single room, and only has a range on the order of 10m. A Local Area Network (LAN) is an expansion of a PAN and can include multiple rooms; this type of network usually delivers service to a number of devices, whereas a PAN is designed as a point-to-point connection. Expanding upon an LAN, a MAN (Metropolitan Area Network) can deliver point-to-multipoint communication between devices within a business building or an entire block of business buildings, a MAN is typically referred to when dealing with an urban environment. On the other hand, when moving to a rural environment in which there are very few obstructions, a Wide Area Network (WAN) is commonly considered. A WAN can service an entire community.

The six different standards are all aimed toward different goals, with the exception of possibly Bluetooth and ultrawideband (UWB). A representation of how the purpose of each device does not overlap with the other devices can be found in Figure 1.3. Notice how when the coverage area in which the devices are intended to deliver service to increases, the maximum bit rate for each network has a tendency of dropping, going from the 500 Mbits/s of ultrawideband down to

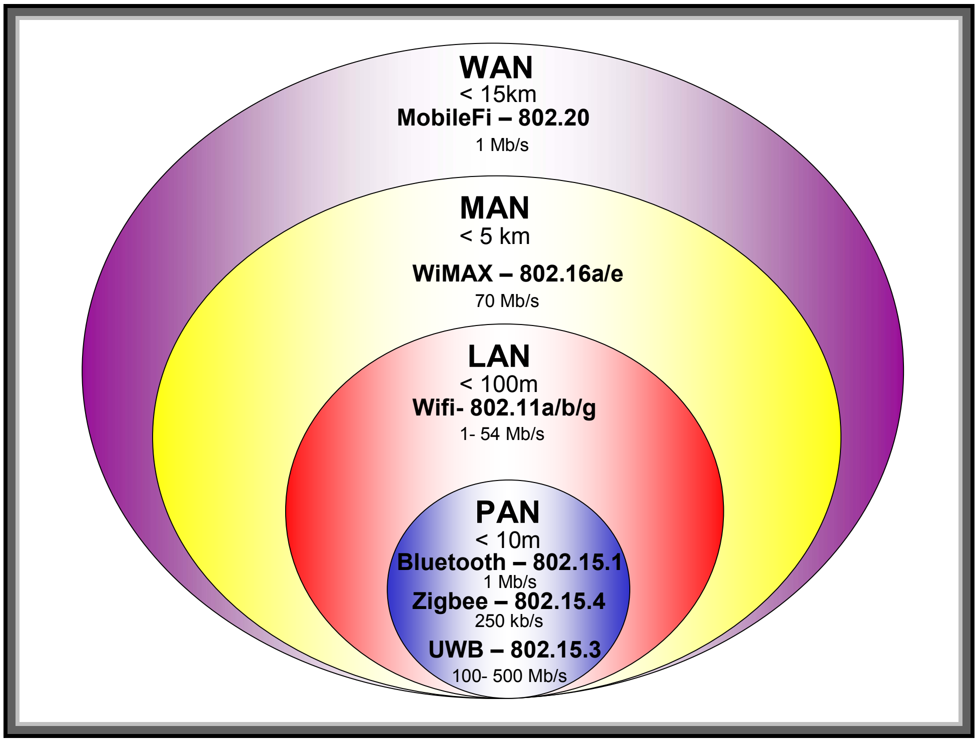


Figure 1.2 - Wireless Protocol Coverage

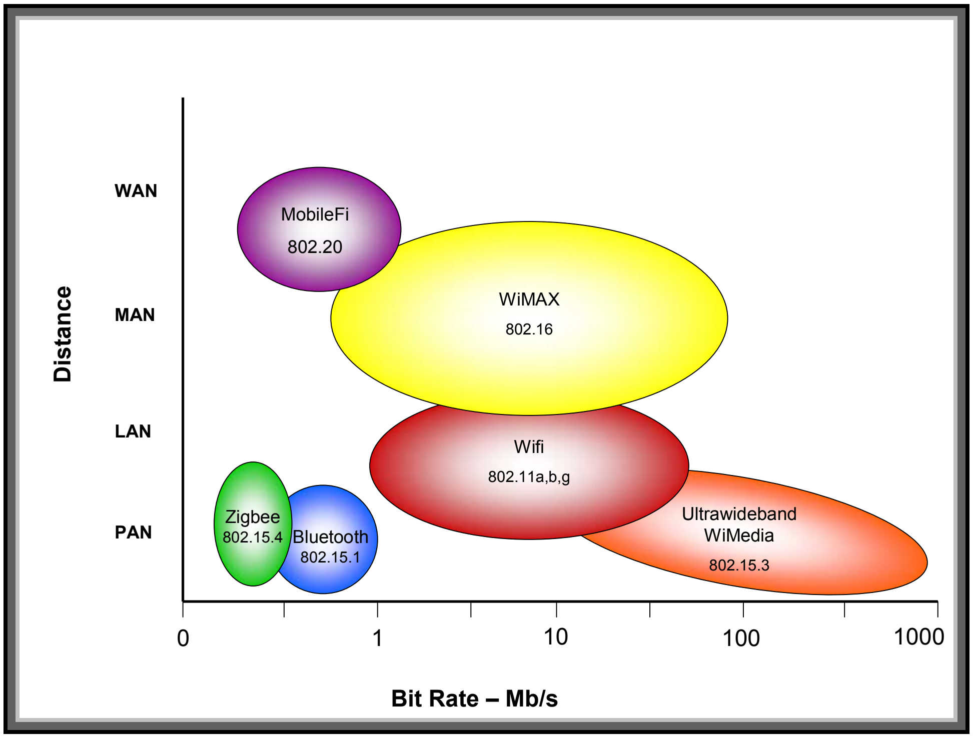


Figure 1.3 - Wireless Protocol Coverage vs. Bit Rate

the 1 Mbits/s rate of MobileFi, this can be attributed to both the concepts of distance limiting the bandwidth and that as the network needs to provide service to more users, the bandwidth available to each user decreases.

1.1.1 Wifi

Wifi is perhaps the most wide-known of the six standards. It is used in routers as a link between a computer and the Internet. Wifi comes in three different forms, 802.11a, 802.11b, and 802.11g. With these three different types of devices, data rates between 1 Mbits/s and 54 Mbits/s are possible. A typical range in the area of 100 m can be expected for all devices. Wifi is one of the foundations of this report and will be explored in further detail in Chapter 2.

1.1.2 Zigbee

Another device which will be given an in depth examination in Chapter 2 is Zigbee. Zigbee has just recently been developed and is geared towards low-power, low-rate communication techniques used in functions such as home automation and sensors. Zigbee only achieves a data rate of 250 kbits/s, but because it only services an area of 10-70 m, it can utilize more power-efficient methods of transmission.

1.1.3 Bluetooth

The third and final protocol under investigation in this report will be Bluetooth. The reasons these three standards were chosen, and not the other devices presented in this chapter, will be explored in Chapter 2. Bluetooth is a cable-replacement device used mainly in conjunction with computers, but also finding applications in cell phones. It was developed to be a low-power, low-cost alternative to Wifi in much a similar way as Zigbee was developed to be an even lower power and lower cost solution than Bluetooth. Bluetooth can provide 1 Mbits/s data rates for coverage from a few meters to a hundred meters, depending on its three different transmitted power levels.

1.1.4 Ultrawideband

Other data communication devices are emerging as reliable alternatives and/or companions to the three previous protocols. To bridge the link between Bluetooth and UWB, both of these types of devices are aimed towards being a cable replacement, although UWB is trying to reach broader markets than Bluetooth. UWB wants to take over not only the market of devices connected to a computer like keyboards and printers, but also the market dealing with audio and video connections, such as DVD to TV connections, which require large amounts of bandwidth to be able to transfer the streamlining video images. The only saving quality for Bluetooth is that Bluetooth has the capability to transmit over an area bigger than the 10 m which is the extent of UWB; however, with the increase in distance, the Bluetooth transmitter will consume more power, making it less power efficient than its UWB counterpart.

Ultrawideband is determined as any signal located within the 7.5 GHz of spectrum between the frequency range of 3.1 GHz to 10.6 GHz and which occupies at least 500 MHz of bandwidth. The original concept of UWB is a variation of what is being marketed for use today. From its inception, UWB was a carrier-less system, which instead of modulating a signal, would merely send sequences of pulses, which were extremely short in duration, lasting in the range of 10 ps to 1000 ps. Because these pulses have such extremely high frequencies, there is no need for them to be modulated. The information, therefore, is buried either within the duration of the individual pulses, the relative amplitudes of the pulses, or else in the spacing or dead time between the pulses, very different from the Phase Shift Keying (PSK) used in a majority of the modulation techniques of other wireless devices which transmits the data within the phase of the signal.

One advantage of using UWB is that due to the extensive bandwidth available, there is a large potential for extremely high data rates, which has been utilized to achieve rates of up to 480 Mbits/s. This would allow UWB to replace such wired applications as USB 2.0 carrying data at 480 Mbits/s or Firewire/IEEE 1394 using speeds in the range of 400 to 800 Mbits/s. Because UWB is on par with such applications, it could be used to replace these high-speed and short-distance cables[3].

A second advantage to using UWB is in reference to the associated power consumption between UWB and all other wireless standards. UWB can achieve the high data rates even though it is over fifty times more energy efficient than the other wireless technologies[3]. This power efficiency can be accredited to the government for placing such strict regulations on the protocol in fear of UWB interfering with other devices. However, UWB transmits at power levels less than spurious emissions of appliances and of switching power supplies in computers[4].

The low power and large bandwidth of UWB allow it to be a good neighbor to other devices while being robust to multipath and noisy environments. The lower power keeps UWB from interfering with other devices in two ways. The first way is via absolute power level; the second is because the low power limits the range of UWB, therefore as long as other devices are located a sufficient distance away from the UWB, on the order of 10 m, the presence of UWB will go unnoticed, especially if there is an obstruction between the two devices. This is because at the higher frequencies used in UWB, the signal cannot propagation through walls.

The robustness of UWB comes from its extremely wide bandwidth. In the presence of interferers, it is unlikely for other devices to have a bandwidth comparable to that of UWB; Wifi has a bandwidth of 22 MHz, and Bluetooth only 1 MHz, therefore the interferer will only affect a small portion of the signal, even in the presence of multiple interferers. At this extremely high data rate, with such short pulses, UWB performs very well against multipath. Since the delay spread, which for indoor environments is on the order of nanoseconds, is much larger than the pulse width, which is measured in picoseconds, the energy can be captured in the receiver[4].

Due to the advantages associated with employing an UWB system, several companies are vying for the lead in developing the technology. Unlike the previous protocols, UWB does not have a standard ratified by the IEEE. The 802.15.3a task group is currently working to finalize the WPAN standard for UWB. However, there are two competing designs being adopted and employed. Intel leads the Multi-band OFDM Alliance (MBOA) and is supporting a system combining a three million hops/s frequency hopping technique with an OFDM modulation technique employed by such devices as portions of Wifi and WiMax. Their competition is the XtremeSpectrum group, headed by Motorola, which is instantiating a CDMA (Code Division Multiple Access) direct-sequence system similar to what is used within cell phones[5].

At present there is no clear winner in the race to have their design incorporated as the standard. Neither group has been able to meet the 75% of votes required to ratify the standard. There was an edge given to the MBOA, however it was not the clear winner, as such both groups have pressed on in development and are working to produce UWB devices. There has been a development from the MBOA camp in which a new group, WiMedia Alliance, has been formed. WiMedia is a more streamlined name used to promote the UWB standard being developed by the MBOA.

1.1.5 WiMAX

Intel is also developing another wireless communication technology along with AT&T, Fujitsu, and Seimens Mobile. In this case, the group is adopting the specifications within the 802.16 standard, associated with point to multipoint WMANs (Wireless Metropolitan Area Networks). These companies have identified their efforts as WiMax (World Wide interoperability for Microwave access).

WiMax is geared towards providing broadband type Internet service throughout the world. The protocol is very similar to the HiperMAN standard being employed in Europe. WiMax is aimed towards replacing the fiber optic and copper wire backbone of the current networks being employed. Although there is less desire to switch within urban environments, where the existing wired infrastructure is already in place, there is a need for this service within developing countries and rural areas where the resources are not available due to a lack of customers or a lack of funding. However, because of the wide range of WiMax, extending 31 miles, by utilizing a minimum number of base stations, coverage would be available to these remote places, for a cost much less than installing a copper or fiber optic infrastructure.

WiMax can achieve such a wide coverage area because of the high transmitter power that it is allowed to sustain, coupled with the use of directional antennas. WiMax has limited a maximum of 500 customers per base station to be provided with service; this allows for a higher bandwidth to be provided to each customer, thus maintaining an overall high data rate. This illustrates how when moving from a rural to an urban environment, the coverage areas will need to be compacted, to allow for an increase in the number of base stations due to the higher congestion of customers.

At present, WiMax is strictly a stationary service provider, meaning that the receiving antenna must be placed in a fixed location. To achieve wide coverage, these antennas are normally placed on rooftops, although changes are being made to allow for indoor antennas, and later on, use in mobile applications. Because WiMax's aim is to provide a replacement of DSL, cable, and T1 Internet connections, it follows that WiMax can be used in conjunction with Wifi. Signals could be routed to a building using WiMax, once a network is available to a building, Wifi could be implemented to provide the Internet access within the building.

Similar to both WiMedia and portions of Wifi, WiMax also incorporates an OFDM system for modulation. This system can operate within two frequency ranges, either the 10 to 66 GHz range or the 2 to 11 GHz range. The difference is that in the higher frequency range, a line-of-sight (LOS) path is required because the higher frequencies cannot penetrate through walls, whereas in the lower frequency range they can. The addition of the lower frequency range is part of the 802.16a section created for the standard. Because there is a large amount of bandwidth available to WiMax, it is able to achieve a higher data rate than Wifi. In a single channel, these data rates can reach 75 Mbits/s, with a possibility of 350 Mbits/s using multiple channels. The ability to use multiple channels allows for WiMax to be highly scalable, whenever more bandwidth is required, all that is needed is the addition of more channels.

Some drawbacks to the WiMax protocol include the other users of the spectrum, especially in the lower-range. Many other devices are already located within this spectrum, with some frequencies unavailable due to government regulations; therefore, finding available space to limit the interference could be an issue. A second concern dealing with the upper spectrum is the LOS requirement. In order to achieve acceptable performance within this upper range of frequencies, more antennas will need to be placed in strategic locations to maintain coverage, this leads to a higher implementation and maintenance cost. A third drawback is in development of 802.16e, which provides for delivery of service to mobile users. This may also cause competition with standard 802.20, or mobile broadband service being developed by MobileFi. Even though these two systems do not provide the same service, they would likely be supplying the same users.

1.1.6 MobileFi

Although the specifics of the standard have not yet been developed, 802.20 is a standard aimed towards providing broadband service to mobile users. Little progress has been made in the adoption of a standard partly due to a struggle for the Chairman's position of the task group assigned to creating the standard[6]. The 802.20 standard or "Standard Air Interface for Mobile Broadband Wireless Access Systems Supporting Vehicular Mobility – Physical and Media Access Control Layer Specification," looks to deliver Mobile Broadband Wireless Access (MBWA) to customers within a given service area[7]. Standard 802.20 has been given such names as WiMobile and MobileFi. .

An advantage that MobileFi has over the mobile standard for WiMax, 802.16e, is that MobileFi can maintain integrity at a speed up to 155 mph, compared to WiMax only being able to achieve speeds of up to 93 mph[8]. This is because WiMax is aimed to service a user walking with a PDA or traveling with a laptop, whereas MobileFi would be trying to service passengers accessing the Internet through a laptop in a car or for deployment in high-speed trains[6].

MobileFi will take advantage of the licensed bands below 3.5 GHz to allow for a data rate of 1 Mbits/s, comparable to a cable or DSL connection. It will also be geared towards high-speed downlink and uplink capabilities and will be able to allow for voice communication, online gaming, and the ability to perform financial transactions because of the low latency associated with MobileFi.

In the near future, broadband service will be able to be obtained from one of three different sources: WiMax, MobileFi, and 3G networks. Reasons for which MobileFi will have difficulty competing with WiMax include the absence of a high demand for internet service traveling at 155 mph, and also the limitation of only operating in the licensed band below 3.5 GHz, which limits the bandwidth available and the possibility of an increase in interference from other devices. Coupled with the fact that WiMax has a head start in standard development and product deployment, MobileFi could miss out on the initial market and get left behind. MobileFi is also at a disadvantage to 3G services because cellular providers would not likely adopt MobileFi service and thus undercut the time, effort, and money that have been put into solidifying their own Internet service. Therefore, careful consideration needs to go into the 802.20 standard to persuade users that MobileFi really has its own niche.

Chapter 2

Standards

2.0 ISM Band

Before discussion of the three wireless protocols to be studied, it is important to know a few of the underlying similarities common to all three protocols. Some of the basic knowledge needed includes the when, where, why, how, and who. These questions can all be answered with one acronym, ISM, or the Industrial, Scientific, and Medical Band.

The ISM band is a band of frequencies in the 2.4 GHz range, more specifically 2.4 – 2.4835 GHz. This band is a free and unlicensed band that can be used by anyone to transmit information wirelessly. The government created this range so that no one company could hold the rights to use these frequencies of interest. It was created in hopes that any device acting wirelessly would have the opportunity to exist at the frequency along with other wireless devices. Since the creation of the ISM band, the FCC (Federal Communications Commission) has put numerous regulations on the use of the band, and the IEEE (Institute of Electrical and Electronic Engineers) has adopted several standards for devices that can be used in the ISM band. Three of such standards, along with their most common protocols are listed as follows: Standard 802.11b, which part of the protocol of Wifi^{TM} (Wireless Fidelity) falls under; Standard 802.15.4, for which Zigbee is the rising protocol; and Standard 802.15.1, also referred to as Bluetooth. In some cases, these protocols are not the only ones being used under a given standard, but since they are the most common, they will be treated as one and the same.

2.1 Zigbee

Zigbee is the first protocol that will be examined. Zigbee is interesting because it has come about out of convenience more than anything else. A collection of major corporations, the most significant eight being Ember, Freescale, Honeywell, Invensys, Mitsubishi, Motorola, Philips, and Samsung, all committed to standardizing cost-effective, low-power, wirelessly networked, monitoring and control products based on an open global standard[9]. This basically means that these companies are looking for a protocol that does not use a large amount of bandwidth and is not very complex, because both would lead to a higher cost and higher power consumption. A lot of the products today fall under this category, thus opening up a large market for products of this nature, and since its inception, over a hundred more companies have joined the justly named Zigbee Alliance.

2.1.1 Zigbee Applications

One question that arises is just what is the market base for products falling into the previous mentioned category? The market base consists of three main categories: personal, business, and industrial. The personal category deals with people as individuals, and the main focus for Zigbee is in home automation, creating ways to make everyday activities easier through the use of wireless devices. The business market deals with companies that are not producing any type of product on site, but more deals with office applications. The flip side to that is the industrial category, which entails a broad range of services spanning from a nuclear power plant producing electricity in Spring City, TN, to a FedEx warehouse distributing packages in Montana. Since the industrial environment is of the greatest concern, the focus of this report will be concentrated on these types of venues.

2.1.2 Sensory Devices

Wireless sensors are probably the biggest market available to Zigbee products within an industrial environment, simply because they encompass such a vast array of applications. Within a nuclear power plant, the purpose of these sensors can range anywhere from controlling the environment of the power plant itself, including heating and lighting, to protecting the safety of the workers, and even to protecting the plant from espionage.

The environment of the power plant can include both the lighting and the heating, ventilation, and air-conditioning (HVAC), both of which can be controlled through the use of either light or temperature sensors[10] For instance, if windows are located in a particular room of the plant, and if sensors placed on the windows detected enough light was entering the window, then the lights within the room could be dimmed due to the decrease in the need for lighting, causing less drain of electricity, meaning less overhead costs. The HVAC can be controlled in a similar way- if the temperature sensors placed throughout a large control room maintain a temperature below a certain threshold, then the heat will be turned on and vice versa for the air conditioning. The two examples could also be used where the offices are located within a power plant, if motion sensors do not detect someone is occupying an office then both the lights and HVAC can be turned off to the room until either someone re-enters the office, the temperature goes beyond a second threshold, or a certain time of the day is reached, in the morning for instance, then the devices could be turned back on in anticipation of someone entering the room.

2.1.3 Safety

Secondly, the safety of the workers could also be protected through the use of Zigbee sensors. This protection could range from making sure that machinery is operating properly, to monitoring reactor coolant temperature levels, to maintaining healthy conditions within the work environment.

For instance, sensors could be placed on water pumps and generators to ensure that they are performing properly and maintaining their appropriate rpm (revolutions per minute) speeds and that they are not overdrawing large amounts of energy. Sensors could also be used to monitor the wear that various parts within the machines are experiencing due to everyday use, and sound sensors could observe noises that are being produced by the machines. If the sensors recognize abnormal noise or that the parts are close to failure, then an alarm could be triggered.

Certain traits of the Zigbee specification can be exploited by these tasks. For instance, through the use of on-chip intelligence, these devices could analyze the information they are accumulating on their own and then only relay information to a main terminal if a given threshold has been exceeded, thus allowing for slower data rates because of the decrease in the amount of data that needs to be exchanged and also affording a savings in battery consumption.

Due to the decrease in the duty cycle of these devices from only transmitting intermittent data, their battery life expectancy can be in the range of one to three years, an appealing figure when compared with the hours and/or days of Bluetooth and Wifi. This allows for the sensors to be placed and not having to be concerned about the device failing due to battery failure. Otherwise, had these devices not been so power efficient, then the battery in each device would constantly need replacement, thus defeating the convenience of having wireless devices.

Another attribute of Zigbee products that helps them to keep the power consumption to a minimum is that they can enter a sleep mode; in this state they consume almost no power but can be awakened at any time. There is typically a 15 ms delay for a device to change from sleep mode to being awake, and then there is also another 15 ms delay for the active slave to access the channel. This is comparable to the 30 ms it would take for enumeration (a new device to access a given network)[9]. For these types of sensors, having a 15 or 30 ms delay is well within the latency requirements due to the polling nature of their applications, which means that most devices will spend much of the time in sleep mode, only awaking to send data about its current state at a given time.

Another application for the sensors to accommodate would be in the monitoring of various processes throughout a nuclear power plant. Temperature gauges and other sensors could be placed within a coolant chamber to not only report whether the coolant is at an acceptable temperature but also the coolant level itself and whether a leakage of any kind has occurred. These types of monitoring applications can be extended to having radiation and other types of warning sensors placed throughout the plant to warn of contamination in the air or within the cooling water systems.

2.1.4 Security

The final area for which these types of sensors could serve would be in the application of preventing espionage. Zigbee devices could be used to aid in the functionality of various security devices. Whether used with motion sensors on the ceiling or pressure sensors within the floor, they could be used to detect whether a restricted area has been accessed and then alert the central security system, which could then relay information to other security features. The other security features could include the controlling of lights, alarms, door locks, and cameras.

One topic that has not yet been mentioned is the distance that a wireless device would have to be able to transmit across. Most applications of Zigbee will typically fall within the 10-meter range, although in some applications it can exceed 70 meters. For more coverage area, a higher transmitted power is required, thus causing the device to draw more energy from the battery and creating the need to change or recharge the battery more often. This is typically not the aim for a device using Zigbee, so it is often not customary to use Zigbee in this way, although in may be applicable in certain situations.

One way Zigbee uses to get around the distance dilemma is to relay information between several devices until it reaches the desired device. Zigbee can conform to various topologies, two of which are star and peer-to-peer networks. Within a star network there is only one coordinator and the rest of the devices are considered the slaves. Within this configuration, the slaves may only talk to the coordinator but not to each other. In a peer-to-peer network, also considered a cluster, there is still only one coordinator but the slaves may now communicate with each other[10]. To circumvent the previous predicament where the information obtained by a Zigbee device needs to travel a long distance, the total transmission length may be broken up between several devices or clusters, allowing for less transmitted power and thus longer battery life per device.

Although sensors offer a broad range of applications, they are not the only applications in which Zigbee could excel. Zigbee could be utilized in RF tagging, either of employees which would allow them access to buildings and other areas, or in inventory, keeping track of packages and equipment by allowing Zigbee transmitters to give updates of their locations are regular intervals. Therefore Zigbee should be given consideration when trying to design any type of wireless device.

2.1.5 Physical Layer

In order to better understand why Zigbee is so useful for the previously explored applications, a background of the actual specifications of the protocol itself is needed. Zigbee incorporates the use of a DSSS (Direct Sequence Spread Spectrum) system to help make it more robust and less susceptible to interference. In the 2.4 GHz range, Zigbee uses the frequencies 2.405 GHz to 2.480 GHz. This range is subdivided into 16 different channels, each with an equal spacing of 5 MHz. Allocating the available bandwidth in this fashion allows for a signal quality improvement due to less ISI (inter-symbol-interference), because while the channel has an available bandwidth of 5 MHz, the signal only occupies a spectrum of 2 MHz. This also allows for the implementation of more channels if the need ever arose for such an improvement due to the extra 3 MHz of available channel bandwidth[11].

Zigbee has a basic bit rate of 250 kbps for the 2.4 GHz frequency range. In order to spread the signal and make it become DSSS, the signal is mapped into a 32-chip length PN sequence. Unlike most other DSSS systems, Zigbee does not multiply input bits by a PN sequence; it just maps the input bits to a pre-defined PN sequence. Zigbee has a databank of sixteen different 32-chip sequences. These sixteen different chip sequences can represent four information bits; four bits therefore represent a Zigbee symbol. With a 250 kbps bit rate, when divided by the four bits per symbol, results in a 62.5 ksymbols/s symbol rate. Taken one step further, each symbol represents the 32 chips in a PN sequence, so the chip rate becomes 2.0 Mchips/s.

The set of sixteen 32-chip PN sequences are quasi-orthogonal to each other and come from cyclic shifts and/or conjugation. The first eight sets of the sixteen simply cyclically shift the length by four chips each time, so after the first sequence, the four chips at the end are put in the front and the rest of the chips are pushed back by four. For the next sequence, the last four chips of the second sequence are placed in the front and all the bits are again pushed back by four. At the ninth sequence, a new sequence is introduced that takes the first original sequence and inverts the odd indexed chips (starting with the first chip indexed as the zero point). Once the ninth sequence is created, the following sequences are then found by shifting the ninth sequence in the same manner as the first eight were done. This continues until the full set of sixteen different PN sequences are made. The set of sixteen sequences and their corresponding data symbol can be found in Table 2-1[12].

Table 2-1 - Zigbee Symbol-to-Chip Mapping Sequences

Data Symbol (decimal)	Data Symbol (binary) (b_0, b_1, b_2, b_3)	Chip Values $(c_0, c_1, \ldots c_{30}, c_{31})$
0	0 0 0 0	1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0
1	0 0 0 1	1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0
2	0 0 1 0	0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0
3	0 0 1 1	0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1
4	0 1 0 0	0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1
5	0 1 0 1	0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0
6	0 1 1 0	1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1
7	0 1 1 1	1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1
8	1 0 0 0	1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1
9	1 0 0 1	1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1
10	1 0 1 0	0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1
11	1 0 1 1	0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0
12	1 1 0 0	0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0
13	1 1 0 1	0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1
14	1 1 1 0	1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0
15	1 1 1 1	1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0

Once the appropriate PN sequence has been chosen for the input symbol, successive chip sequences are concatenated and the chips are modulated using offset quadrature phase-shift keying (O-QPSK)[12]. Since the 802.15.4 standard specifies that half-sine pulse shaping must be used, the O-QPSK modulation is equivalent to MSK or minimum-shift keying, which can be defined as continuous-phase FSK with a minimum modulation index (h=0.5) that will produce orthogonal signaling[13].

O-QPSK is a form of QPSK (Quadrature Phase Shift Keying), which can send two bits of information per symbol, but O-QPSK employs a technique of delaying the Q-phase of transmission by one bit period. QPSK is formed by separating a signal into its I-phase (In-phase or Direct-phase) and Q-phase (Quadrature-phase), it can be thought of as the real and imaginary parts of a complex number, with the I-phase being the real part and the Q-phase being the imaginary part. By delaying the Q-phase by a bit period, this allows for only one zero crossing to occur at a time, with a zero crossing of the phases representing a change in the data bit. With only one zero crossing occurring at a time, the phase transition for O-QPSK is only 90° instead of the 180° that can occur for QPSK. For half-sine pulse shaping, this results in one phase of the signal being at its peak of the sine wave while the other is at a zero crossing and vice versa for the other phase. This allows for a much more reliable demodulation of the signal.

For Zigbee, in order to separate the signal into its I-phase and Q-phase, the PN sequence is broken down into a two sets of sixteen different chips. From the original sequence, the even-indexed chips are placed in the I-phase and the odd-indexed chips are placed in the Q-phase. For the offset found in O-QPSK, the Q-phase is delayed by half of a chip or double the inverse of the chip rate. It was found earlier that the chip rate was equal to 2 Mchips/s; T_c in Figure 2.1 corresponds to the inverse of that value[12]. The figure also shows that the chips in the individual phases have duration time of twice the chip period, thus the per-phase chip rate is half the overall chip rate and is equal to 1 Mchips/s.

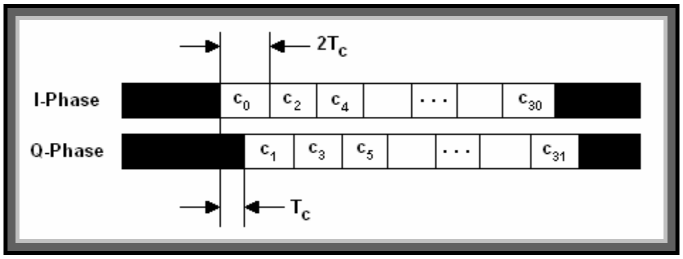


Figure 2.1 – O-QPSK Chip Offsets

2.1.6 MAC Layer

The MAC layer deals with how information is sent at the packet level. As stated earlier, a data symbol consists of 4 information bits. In order to know where these four bits come from, a more abstract look will be taken. But first it is important to note that for 802.15.4, transmission is done in octets or groups of eight bits, as will be shown in the proceeding explanation. All the following information about how the packets are formed is taken from the 802.15.4 standard. A packet, also known as a PPDU (PHY beacon packet) consists of three fundamental elements, which are the SHR, the PHR, and the payload.

The SHR (synchronization header) consists of the synchronization components, namely the preamble and the SFD, and is a total of five octets long, or 40 bits. The preamble requires four of those octets and each octet is composed of all binary zeros, or 32 zeros. It is used to synchronize the receiver with the incoming signal. The fifth and final octet is called the SFD field. The SFD field is used to designate when the incoming data in about to begin. After the 32 zeros go through, the SFD is composed of the bits 11100101, and once the receiver recognizes these bits, it knows that the preamble is over and must prepare itself for the next stage, which is the PHR.

The PHR (PHY header) is only one octet long but is vital to receiving the information that was originally sent. It specifies how long the PSDU (the PSDU, or PLCP Service Data Unit, is formed in the MAC sub layer and is not within the scope of this report, but is essentially the sent information itself) will be in octets. A maximum of 2^7 octets or 128 octets can be sent for one packet, corresponding to 1024 bits of total information. The final bit of the PHR octet is reserved for later use.

The final component of the packet is the PHY payload or PSDU. It can be of varying length as specified by the PHR above. One small detail to note is that when the octets are grouped into data symbols, each data symbol is composed of four bits, while the packet information is grouped into 8 bits. The way this is resolved is to place the first four bits (b_0, b_1, b_2, b_3) into one data symbol, and the second group of four bits (b_4, b_5, b_6, b_7) are placed into a second data symbol[12].

Now that the fundamentals for the Zigbee standard have been set forth, the next standard, Wifi, followed by Bluetooth may be presented so that a comparison between the differing standards can be drawn.

2.2 Wifi

No matter where anyone looks these days, it is hard to find a place where wireless Internet is unavailable. Whether it is a hotel room, a local café, or just a business office, because of the surge in number of laptop computers and PDAs (personal data assistants), people everywhere are prompting the need for wireless Internet access points.

2.2.1 Applications

Within an industrial environment, laptops and PDAs are infusing themselves into the workplace. With machines becoming less dependent on human interface, and processes being converted to become computerized, there is a need to be able to upgrade and test equipment and this need has been dependent on allowing the equipment to be able to be connected to a laptop allowing a diagnostics test to be performed and newer software downloaded. Rather than containing all of the necessary software on the laptop it can be placed onto the main server and simply downloaded as it is needed through the use of a wireless network.

Other ways in which wireless networks could be exploited would be through the service of other devices that are accessible to the Internet via Wifi. PDAs could allow technicians to communicate with troubleshooters while inspecting faulty equipment, through the use of picture and text messaging to obtain instant feedback, rather than being delayed by poor communication. They could also allow for better methods of ordering the needed supplies and equipment to maintain proper working conditions. Rather than having the steps of taking inventory, checking the needed supplies, then entering them into a computer to have them ordered, a more efficient approach would be to order materials directly through a PDA as the inventory is taken. This would increase in the efficiency and decrease in the chances of a mistake occurring.

More and more, laptops are replacing desktop computers due to their portability. The use of wireless Internet would allow for legacy systems to be upgraded without the added cost of running Ethernet cord throughout a building and maintaining hundreds of access ports. Instead, by allowing Wifi routers to be used, a minimal amount of cord would need to be placed within walls, floors, and ceilings to connect the routers, cutting down on the added overhead due to remodeling. As long as the networks are secure and do not allow unwanted users onto them, these networks would work just as well as wired networks, with the added flexibility of not always needing to be located near an access port. This will allow users within a plant to stay connected, but also allow for them to stay in touch with the outside world, thus two nuclear power plants could exchange updated safety procedures and measures that should be taken in a crisis so that if a catastrophe does occur then everyone will be better equipped to handle such situations. Therefore through the use of access points the family of 802.11 IEEE standards is helping to keep the world connected. .

2.2.2 802.11 Standards

Within the 802.11 family of standards, the three that have found prominence today are 802.11a, 802.11b, and 802.11g. It can be considered that 802.11a and 802.11b are distinct protocols within themselves and that 802.11g is a fusion of those two standards molded into one. This is because 802.11g encompasses the more attractive traits of 802.11a, which is the speed, and the broad compatibility of 802.11b. The relevant functional aspects of each of the three standards will be discussed; along with a more in-depth explanation of its operation. One interesting similarity to note is that all three protocols instantiate the same MAC (Medium Access Control) layer defined by the 802.11 standard and it is only how the PHY (Physical) layer is implemented that distinguishes the protocols from one another. Since the MAC layers are the same, and are also beyond the scope of this report, information pertaining to the MAC layer will only be presented as needed.

2.2.3 802.11b

The most prominent of the three protocols for the IEEE standard 802.11 is 802.11b (also referred to as Wifi), which has found its market in business offices, research facilities, and on university campuses. Almost all wireless routers today are Wifi compliant, even though there is a surge of 802.11g-compliant devices becoming available on the market. The universal switch from Wifi to 802.11g has not yet fully occurred, thus Wifi will be the main topic of discussion. Unlike Zigbee, Wifi's aim is not to be implemented in wireless sensors or as a simple cable replacement for computer devices, but was created to connect devices through the use of the Internet. Wifi was made with data speed in mind, not low power consumption or low complexity. Therefore there is no real comparison between Zigbee and Wifi. In most Zigbee applications, Wifi would not only consume too much power, but would also be overkill; none of Zigbee's applications require high-speed data rates. In a likewise manner, Zigbee is not suited to perform Wifi's tasks because in the time it takes Zigbee to perform a given task, Wifi has the potential to be forty-four times faster. Consequently, it would be like comparing dial-up to broadband access. With such a decrease in throughput through the use of Zigbee, the efficiency within the work environment would decrease drastically, therefore Wifi would be the more desirable choice for Internet connection.

2.2.4 802.11b Physical Layer

Wifi can be broken down into four different data rates (1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps), but before exploring them there are some common requirements set forth for all data rates. First and foremost, Wifi operates in the same ISM band as Zigbee, specifically from 2.4 GHz to 2.4835 GHz. In the U.S., out of a total of 14 channels, only the first 11 are allowed to be used and their center frequencies range from 2.412 GHz to 2.462 GHz, with each channel occupying approximately 22 MHz. Thus it can be seen that only three channels do not overlap each other, channels 1, 6, and 11[14]. Secondly, the aggregate chip rate for all four data rates is 11 Mchips/s, which corresponds to occupying a total bandwidth of 22 MHz. Finally, while the 802.11 standard supports three types of physical layers, DSSS, frequency hopping spread spectrum (FHSS), and Infra-Red (IR), it is recognized that all four data rates encompass the DSSS system, but only the two slower data rates are used in FHSS and IR systems.

A brief introduction is needed into the workings of the 1 Mbps and 2 Mbps schemes in order to understand how the 5.5 Mbps and 11 Mbps rates were later achieved, although all the testing done for this project was conducted using the assumption of the 11 Mbps rate. The main reason that it is important to study the slower data rates is because all compliant Wifi devices that operate at any given data rate must also be able to operate at the 1 Mbps rate. The requirement was set into place because in order for a device to send or receive data, it must know specifics about the message itself, so all vital information about a message including its data rate and its payload are sent in the headers (specifically called the PLCP headers, Physical Layer Convergence Protocol) which are transmitted at 1 Mbps modulation. This is one way of ensuring that not only will the receiver know which modulation scheme to use, whether it is for the slower or faster data rates, but also the other transmitters will know how long to refrain from using the channel before attempting to access the channel for themselves. Since the header contains information about the rate and the payload of a signal (which in this context signifies the time duration of the packet transmission) the other transmitters can decipher this information from the header and know to wait at least that long before trying to access the channel.

The 1 Mbps data rate is realized using a combination of a Barker code DSSS spreading function along with a BPSK (Binary Phase-Shift Keying) modulation scheme. The Barker code used is an eleven-bit sequence (10110111000) that is XOR'd with the input data stream[15]. This is done by concatenating the successive 11-chip sequences resulting from the XOR between the 11-bit Barker code and the individual message bits. Thus each message bit is encoded by 11 chips, the 1-bit at a 1 Mbps rate multiplied by the 11 chips that represent that one bit yielding a chip rate of 11 Mchips/s as was previously specified. The resulting chip sequence is then modulated using BPSK modulation, which represents one bit per symbol of transmission.

On the contrary, the 2 Mbps data rate incorporates a QPSK modulation scheme that can represent two bits of information per transmitted symbol. Thus twice the information can be sent using QPSK in the same bandwidth as the 1 Mbps BPSK scheme. Therefore the information is encoded in the same way as before, but now instead of BPSK modulation, DQPSK (Differential QPSK) is used instead. DQPSK modulates sequential symbols by a phase rotation. This increase in the bit rate occurs at the expense of either a need for a higher transmitted power, or a diminished range of effectiveness. Since the FCC has put regulations on the maximum effective transmittable power in the ISM band, which is 1000 mW, the only factor left to control is the effective range. Thus as the distance between the transmitter and receiver increases, the modulation scheme used will adjust to one of the slower rates in order to maintain a tolerable signal level[15].

The 11 Mbps and 5.5 Mbps data rates can be thought of as an extension to the 2 Mbps data rate previously discussed. Both schemes still maintain the 11 Mchips/s chip rate and the both are modulated using DQPSK modulation. The difference is that the two higher data-rate formats incorporate a different and more complex DSSS technique that will change the way bits are grouped and the way in which they are spread.

The technique implemented by the higher data rates is a design first conceived by Marcel J.E. Golay in 1951. Golay had being doing some work with uses of spread-spectrum models pertaining to light emitting through slits. In doing this work he stumbled across complementary sequences that proved to contain valuable mathematic properties. He later published a paper about the binary sequences he had discovered, mainly about what made them so appealing and how they were created. It is an extension of work similar to this that helped bring about the evolution of CCK (Complementary Code Keying) codes, which is a type of polyphase complementary codes. The codes that Golay helped discover are a type of polyphase codes called binary complementary codes. The difference between the two is that binary complementary codes take on binary values (ones or zeros) while polyphase complementary codes can take on a number of different values so long as they maintain complementary properties. For the case in hand, CCK uses codes containing four different phase values that take on complex values, namely the values {1, -1, j, -j}[16].

Due to its superior coding properties over the Barker sequence, CCK was implemented to make the data transmission of Wifi more efficient and robust. The efficiency comes from the increase in data rate within the same signal bandwidth, and the robustness comes from the improved coding ability of incorporating multiple sets of possible transmitted code words, rather than just one Barker sequence implemented by the slower data rates.

To increase the speed of the data being transmitted, CCK transmits eight complex chips for every 8 information bits, yielding an 8:8 or 1:1 ratio, rather than the 11:1 ratio of chips to bits for 1 Mbps transmission accounting for an 11x increase in data throughput. The increase in data is accomplished in a multi-stage process. First and foremost, groups of eight bits must be gathered to create an information symbol. The individual groups of 8 bits are then separated into two unequal partitions, one portion being the first two bits of the symbol, the second portion being the last six bits of the symbol. The first portion will be used later to modulate the signal and will be ignored for now. Since the second portion contains a group of six bits, there is a possibility of 2^6=64 potential combinations. These six bits will determine which one of the 64 possible 8 chip codewords will be outputted. This will be more useful after discussing the two-step method for determining the codeword.

It is somewhat remarkable how the different 8-chip codewords are created. It can be thought of as being done in either one of two ways, which both ways are essentially the same, except one way uses a direct method whereas the second way uses a two step method. Before proceeding to explain the two methods, a common nomenclature to both methods needs to be introduced. The eight bits that make up a message symbol can be broken down into four groups of two bits each. As an example, if the 8-bit message symbol (b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7) sent was to be 01110110, then the four groups or two bits {(b_0, b_1), (b_2, b_3), (b_4, b_5), (b_6, b_7)} would be {(01), (11), (01), (10)}. By examining Table 2-2 out of the 802.11b Standard, the corresponding phase values can be found.

Table 2-2 - Bit Pattern

Bit Pattern $\{d_i, d_{(i+1)}\}$ $\begin{pmatrix} d_i \text{ is first} \\ \text{in time} \end{pmatrix}$	Phase Values φ_1	Phase Values $\varphi_2, \varphi_3, and\ \varphi_4$
0 0	0	0
0 1	$\pi/2$	$\pi/2$
1 0	$3\pi/2\ or \left(-\pi/2\right)$	π
1 1	π	$3\pi/2\ or \left(-\pi/2\right)$

It can be seen that the phase values for the example octet (01, 11, 01, 10) can be determined as:

$$\varphi_1 = 01 = \frac{\pi}{2}; \varphi_2 = 11 = \frac{3\pi}{2}; \varphi_3 = 01 = \frac{\pi}{2}; \varphi_4 = 10 = \pi.$$

These four phase values will be used in both the direct and two-step methods that will be presented.

The direct method simply takes the previous four phase values and plugs them directly into an equation to determine what the sent coded bits will be. Even though this it not the conventional way of creating the codeword it is the intuitive way and merits study. The four phase values are entered into the following equation.

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

By solving the above equation, the sent complex codeword is obtained and can take on the values of {1, -1, j, -j}. From the previous example using the input bits 01110110, the following outputted codeword would be {-j, 1, -1, j, j, -1, -1, j}. As was stated earlier, this is the intuitive way and the way determining the codeword is most often presented, however, this is not the way the codeword is found when modulating the signal in a real world system. To determine this, the two-step method must be presented.

The two-step method still uses the same four phase values as before, but instead of plugging the four phase values directly into the equation as before, a different phase equation is used. As can be seen from the equation above, the first phase value φ_1 can be found in each term. Consequently, the term $e^{j\varphi_1}$ can be factored out of the expression and simply multiplied by later to rotate all of the terms. When factored out of the previous equation, it leaves the equation

$$c = \{e^{j(\varphi_2+\varphi_3+\varphi_4)}, e^{j(\varphi_3+\varphi_4)}, e^{j(\varphi_2+\varphi_4)}, -e^{j(\varphi_4)}, e^{j(\varphi_2+\varphi_3)}, e^{j(\varphi_3)}, -e^{j(\varphi_2)}, 1\}.$$

This equation will still output an 8-chip codeword, but this codeword is not rotated by the φ_1 value. This is the equation that will be used to create the databank of 64 different 8-chip codeword sequences previously mentioned above. When the bits are actually modulated, only the last six bits of the message symbol are sent to the codeword decision block. This means that the second equation must be used since it does not account for the first two bits of the message symbol. The needed codeword value could be determined on the fly using the above equation, but it is more likely to predetermine all 64 different possible codeword values and stored them in an accessible memory bank. This way as the six bits are read in, they will correspond to a certain place in memory, and those 8 codeword chips in memory will be outputted. From the previously used example for the direct method, if using the same phase values for the new equation, the output chips would be {-1, -j, j, 1, 1, j, j, 1}. These chips obviously are not equal to the sent chips found previously in the direct method. This is why the second step of the method is required; if all of the values in the chip sequence above are rotated 90°, or a value of π/2, i.e., multiply each chip by $e^{j(\pi/2)_1}$ or by the value { j }. The resulting chip sequence would be equal to the chip sequence for the direct method which was {-j, 1, -1, j, j, -1, -1, j}.

DQPSK modulation is accomplished by utilizing the first two bits of the symbol, which were previously set aside and are used to differentially modulate the codeword so that each chip maintains the same phase rotation. This phase rotation can be detected in the receiver and add two more bits of coding. The question might arise, why use the DQPSK modulation scheme, why not just use QPSK with the direct method of determining the codeword since they have already been differentially encoded. The two methods are identical in theory, but much different when considering the decoding within the receiver. The main problem occurs in the receiving and decoding of the data. In order to determine what the sent message symbol is, the direct method would require a bank of 256 correlators. Correlators tend to make receiver design more complex and, thus, more expensive. Therefore, by using the two-step method of DQPSK modulation, only

64 correlators would be required along with a phase detector. Although both implementations are theoretically equivalent, the latter is shown to be more cost-efficient.

The previous explanation was a concise overview of the Wifi protocol. A more detailed explanation can be found within the Standard itself, which is an amendment to the original 802.11 standard and will also go into a more in-depth look at the MAC layer. Since the scope of this study does not entail concentrating on the MAC layer, it will be left to the reader to pursue. A brief study of the other possible 802.11 protocols that could have been chosen will be looked at followed by an explanation of why they were not included.

2.2.5 802.11a

Out of the IEEE standard 802.11, several different physical layer specifications have evolved, with the most prominent being 802.11b or Wifi, although 802.11a is in many ways more appealing. For starters, the frequency range for 802.11a does not lie within the 2.4 GHz ISM band. This is attractive because the ISM band has become over crowded with Zigbee, 802.11b and 802.11g, Bluetooth, and even microwave ovens, as just a few examples. With the congestion stems a need for a system less susceptible to interference; in order to maintain this robustness, a system must suffer a degradation in efficiency and will experience a decrease in overall data throughput. To increase its output bit rate, 802.11a takes advantage of the 5-GHz UNII (Unlicensed National Information Infrastructure) band.

2.2.6 802.11a Physical Layer

The 802.11a scheme has an improvement on the order of a 5x increase in output data rates over 802.11b. From the Standard for 802.11a, this PHY layer can support eight different data rates, which are 6, 9, 12, 18, 24, 36, 48, and 54 Mbps, although the mandatory rates are 6, 12, and 24 Mbps[17]. These rates are realized through the use of 52 different subcarriers as required by the OFDM (Orthogonal Frequency Division Multiplexing) system used by 802.11a. A more detailed look into how the 52 subcarriers are used can be found in Linksys White Paper[18]. OFDM is implemented as pipelining. For example, instead of transmitting a 24 Mbps data rate on one carrier, the 20 MHz channel is broken down into 52 different subcarriers, with 48 of those 52 each carrying a data rate of 0.5 Mbps in parallel with each other. The other four subcarriers do not carry data and are “pilot” tones[18]. These 52 subcarriers are modulated using BPSK, QPSK, 16-QAM (Quadrature Amplitude Modulation), or 64-QAM, depending on the desired data rate[17]. Sending data using multiple carriers has several advantages to single carrier modulation that are not within the scope of the report and can be found within the White Paper[18].

Within the 5-GHz UNII band, 802.11a is subdivided into three different channels of 100 MHz each, occupying a total of 300 MHz. This means that 802.11a and 802.11b both have approximately 100 MHz of bandwidth to use. The three different channels for 802.11a and their respective bandwidths are: the U-NII lower band (5.150 to 5.250 GHz), the U-NII middle band (5.250 GHz to 5.350 GHz), and the U-NII upper band (5.725 to 5.825 GHz). The need for the three different bands results from 802.11a offering 12 separate subchannels, each with a bandwidth of 20 MHz. This 20 MHz channel is divided into the 52 separate subcarriers. The use of the three bands allows for no overlap of the subchannels, very different from Wifi, where only three channels do not have overlap. A more important reason for the three main U-NII bands of 802.11a is to distinguish from different transmission output powers. It allows for a maximum of 40 mW in the lower U-NII band, this band is mainly for indoor use and the lower power can be used because it does not have to span long distance. In order to be used outdoors, where distances could greater than they would be indoors, the upper U-NII band allows for a maximum output power of 800 mW. For cases in between such as a large warehouse, or when an application may need to span short distances between an outdoor and indoor transceiver, the middle U-NII band allows for a maximum output power of 200 mW. For 802.11a compliant devices, it is not a requirement for them to be able to transmit and receive in all three bands[18].

The brief overview of 802.11a is given as an example of how when using the same MAC layer, completely different PHY layers can be implemented to achieve different performances while maintaining the same overall goal, which is a very high speed wireless connection to transfer data. 802.11a will not be studied within this project because it operates in the 5-GHZ UNII band that it is unsuitable for the interference studies at the 2.4 GHz band. If the ISM band becomes too overcrowded, these devices may become an outlet for 802.11b users who need to operate in a cleaner environment. To achieve the 802.11a data rates within the ISM band, 802.11g has been developed.

2.2.7 802.11g

The fairly new and rising 802.11g has not been around for very long and is only now starting to show itself with the marketplace. It is capable of maintaining 802.11a type data rates, up to 54

Mbps. It is essentially another version of 802.11a simply placed in the ISM band, with a few slight differences. Therefore a need for an explanation of the similarities and differences between 802.11g and both 802.11a and Wifi arises.

Due to the fact that in the 5-GHz UNII band, 802.11a used 100 MHz of bandwidth, and the fact that in the ISM band, 82 MHz of bandwidth is occupied by Wifi, it appears to be a feasible task of translating one to the other. The protocol 802.11g specifically does this; it incorporates the same OFDM carrier modulation as 802.11a and can obtain the same data rates. 802.11g also uses a PBCC (Packet Binary Convolutional Code) modulation scheme that can be found in the 802.11b standard which is different method of coding other than CCK which can achieve higher data rates, but will not be delved into in this report.

One difference that 802.11g must account for is that it must also be back compatible with the Wifi devices, meaning that it must be able to operate at the same data rates as Wifi using the same modulation schemes. This restriction was put in place so that the existing networks using Wifi, mainly the wireless devices placed in laptops and PDAs, would still operate in the new 802.11g environments. This would help to alleviate the problem of having a full-scale switch from one protocol to the other. This would allow the network routers within a building to be switched to 802.11g while the devices connected through the wireless network could be operated using either of the two protocols. As time progressed, the old Wifi devices could be phased out and replaced with the updated and faster 802.11g devices.

For the reason that 802.11g has not extensively been used in the market place yet and has not proven to be as widely acceptable and reliable in the mainstream business and university worlds as Wifi has, 802.11g will not be a protocol under study for this project. Wifi will be concentrated upon letting future testing for the newer protocol be done at a later time.

2.3 Bluetooth

Much like Wifi, another household name that has emerged as a popular choice for wireless connectivity is Bluetooth. Bluetooth is a technology that was developed by the Swedish company L.M. Ericsson for short-range cable replacement[20] The name comes from a chapter of Scandinavian history during the 10th century when Denmark was ruled by King Harald Blatand, which when translated into English means Harold Bluetooth. Harald Blatand is known for bringing peace to the land now formed by Norway, Sweden, and Denmark[21] In much the similar way that Blatand united the different cultures during that time, Bluetooth is used to support the solidarity of various devices, so that better communication between them can be possible. Blatand's influence is prevalent in the Bluetooth logo, with the letters "H" and "B" from the runic alphabet for which are represented as a symbol resembling an asterisk ᚼ and a ᛒ, respectively.

Bluetooth was started in much the same way as Zigbee, four years after its inception, a consortium of companies with similar needs got together and generated a new and universal mode for which data transfer could be accomplished without the need for wires and without sacrificing the speed of the data transfer. The consortium of companies included Ericsson, IBM, Intel, Nokia, and Toshiba, which formed what is known as the Bluetooth Special Interest Group (SIG). Their similar needs included needing a short-range, low-power wireless protocol, which would be robust enough to meet the needs of their customers. Since the SIG sought after promoting products that could interact with products from differing companies, there stemmed a need for one basic standard that could be a model for all of the corporations to abide by.

2.3.1 Applications

A cornerstone for Bluetooth compliant devices has been the ability to communicate with the modern PC. This ability opens Bluetooth to a vast array of potential applications since computers are essential for any type of research or in controlling processes such as nuclear reactions and other extremely delicate processes that require precise monitoring. To aid in human control of the computers, there has been a demand for more products associated with a computer to become wireless, including: keyboards, mice, and printers, along with products that can be used in conjunction with computers such as PDAs and cell phones.

Certain Bluetooth qualities make it desirable for applications of use such as computer accompaniments. While Bluetooth does not possess the speed of Wifi, 11 Mb/s compared to 1 Mbps for Bluetooth, 1 Mb/s is still well suited to be used in conjunction with a computer whenever it deals with a human interface. Due to the nature of the applications of entering words on a keyboard or scrolling with a mouse, they do not require large amount of bandwidth. Even Zigbee, with a maximum bit rate of 250 kb/s has started to be used for some of these devices.

Another such quality of Bluetooth, although Zigbee may be shown to have a bigger advantage, is in the amount of energy that is consumes. Normally Bluetooth mice have built in rechargeable batteries with the charger located within the receiver. This way whenever the battery runs low, docking the mouse into the receiver unit allows it to charge, a typical charge will last anywhere from one to three days depending on usage. A keyboard on the other hand, typically is powered by off-the-shelf disposable batteries and can be used for anywhere from six months to a year before having to be replaced, much more efficient than would a similar device that incorporated the Wifi standard, which would have to be plugged into a wall outlet due to its power consumption, thus defeating the purpose of being wireless.

Since keyboards and mice typically are used within close proximity to a PC there is no need to consider the range of such devices, this however does become an issue when devices such as printers or scanners are considered. For instance, printers may be located on the opposite side of a room or even in a completely different room all together. This may or may not be a problem depending on the conditions of the channel that the signal must travel through. Typically Bluetooth is operational up to a range of about 10m to 100m, depending on the selected power level. Bluetooth offers transceivers with a range of different power levels. Power-Class 1 transceivers can transmit with a maximum output power of 20 dBm allowing a range up to 100m. Power-Class 2 devices can transmit up to a range of approximately 10m with a maximum output power of 4 dBm. The most common applications use Power-Class 2 chips. The third and final Power-Class 3 transceivers may only transmit a maximum of 0 dBm and are for very short range applications, typically 1m[22]. Therefore if printers were being used in conjunction with Power Class 1 transceivers, then in a wide-open area, a range of 100m could be achieved, but this figure drops drastically within an indoor environment due to walls and objects causing reflections and absorbing power, so the overall range can be considerably less than 100m. This additional power consumption can be tolerated because they occur on printers, desktop computers, or laptops that are typically supplied by wall sources, without the need for battery recharge.

2.3.2 Cable-Replacement

Bluetooth is a cable-replacement protocol. Rather than sending data through a wire, the medium that is used is air, removing the hassle of wires running in inconvenient places. For instance, with PDAs and the capabilities of cell phones becoming increasingly more sophisticated, there is a demand to have synchronization between these devices and a PC. For example, calendars, email, and file handling are all desirable items to be shared between two devices. If the example of using a PDA for either repair work or for ordering materials were re-introduced, and wireless internet was not available, then the information could simply be downloaded from the PDA to a computer through a wireless Bluetooth connection and then ordered, rather than the need to copy everything from one machine to another manually. Also, when taking measurements of various processes throughout a power plant, the results can be recorded using one device and transferred to an off-site computer at another facility, so that testing can be performed on the data. For instance, if a channel sounder were being used by an outside company to characterize the fading parameters within a nuclear facility, and by rule, no outside devices with memory were allowed into the facility, then secure laptops owned by the nuclear plant could be used to take the measurements, the contents analyzed to ensure that no critical information had been compromised, and then transferred off of the laptop at a later time through a Bluetooth connection to the consulting firms device for data analysis.

2.3.3 Physical Layer

To help determine what is within a Bluetooth transceiver chip that allows for wireless connectivity, a look into the standard itself is required. Much like Wifi and Zigbee, Bluetooth can be dismantled into two separate partitions, the MAC and PHY layers. For the purpose of this study the PHY layer will be explained in some depth whereas the MAC layer will just be briefly touched upon. A more extensive look into both layers may be found in the Bluetooth core specification[23].

First and foremost, the Bluetooth approach to combating interference is very different from the way both Zigbee and Wifi try to accomplish this task. Zigbee and Wifi use DSSS techniques where the narrow signal bandwidth is extended into a wider bandwidth thus allowing for the chance of an interferer depleting the entire signal to be minimal. In the time domain this is accomplished by taking a signal bit and multiplying it by a Pseudo-Noise (PN) sequence. If a sixty-three-length PN sequence is used, then for every bit of information, there will be sixty-three corresponding chips that will be sent. So at the receiver, there is a more likely chance that many of the sixty-three chips will be able to be received without error rather than a single bit. Bluetooth on the other hand uses a FHSS technique. Rather than spreading the entire signal over a portion of the allotted frequency band, Bluetooth keeps the same narrowband signal and just changes the carrier frequency of the transmitted signal, thus hopping from one frequency range to another. This hopping fashion minimizes the likelihood that an interferer will be located on several hop sequences in a row.

There are multiple variations of hopping schemes used for FH-SS systems. The main two methods are fast-hop which incorporates multiple hops per bit, and slow-hop which will sends multiple bits per hop. Bluetooth is of the latter type and will transmit one complete packet per frequency hop. A packet can contain anywhere from 126 to 2971 bits[23]. The maximum time duration of any one packet is 625 μs due to the rate of the 1600 hop/s that Bluetooth employs.

In the 2.4 GHz unlicensed ISM frequency band, Bluetooth uses 79 of the 83.5 MHz bandwidth available. This allows for 79 channels, which are 1 MHz wide, corresponding to the data rate of 1 Mb/s, to be used determined by the equation[24].

$$\begin{aligned}&(2402+k)MHz, k=0,1,2,....78.\\&e.g.2402,2403,2404,2405,2406,......2480\end{aligned}$$

Due to regulations set forth by the FCC part 15.247, a device may not transmit for longer than 0.4 seconds on any particular channel within a given 30-scond time frame. This means that at least 75 of the 79 channels must be utilized in the hopping sequence. The hopping sequence is a predetermined sequence that combines the 79 channels in pseudo-random order[25].

Bluetooth incorporates a modulation scheme similar to the cellular standard for Global System for Mobile Communication (GSM). GSM uses a Gaussian Minimum Shift Keying (GMSK) technique, and Bluetooth uses a very similar Gaussian Frequency Shift Keying (GFSK). Both techniques are modeled from Frequency Shift Keying (FSK) modulation schemes. In order to better understand GFSK and GMSK, a conceptual foundation in FSK and MSK (Minimum Shift Keying) must be explored.

FSK is utilized so as to change the frequency of a signal when either a binary one or zero is sent, unlike PSK, which changes the phase of the signal, or Amplitude Shift Keying (ASK), which changes the amplitude of the outgoing signal. For Bluetooth, a positive frequency deviation from the carrier corresponds to a binary one being transmitted, conversely a negative frequency deviation is transmitted when a binary zero is sent. The minimum frequency deviation acceptable according to the standard has been set to 115 kHz. FSK has two distinct advantages over both ASK and PSK modulation techniques. First and foremost, the additive thermal noise in the receiver directly affects the amplitude and phase messages contained within the signal, whereas the noise will not affect the message of the FSK signal in a direct manner. The second advantage is contained within the complexity that must go into the transmitter and receiver design itself. The varying envelope of the ASK and PSK signals make the design of the RF circuitry very complex, thus making the footprint of the design bigger, both of which lead to a higher cost. FSK on the other hand is a constant envelope modulation, creating less complexity, a smaller footprint, and a lower cost, desired by Bluetooth products.

There are two different kinds of FSK modulators; one is a continuous-phase modulation scheme while the other is discontinuous. This comes from the type of transmitter used, if two different oscillators are used, one to send the higher frequency and one to send the lower frequency, then when the signals switch from one oscillator to the other, the phase of the outgoing signal will change instantaneously causing it to be discontinuous. If a frequency modulator is used in which changes to the signal are accomplished with the aid of an integration technique, then the outgoing phase will be continuous. This leads into MSK, which is a form of continuous-phase FSK.

MSK is very similar to the O-QPSK modulation scheme with half-sine pulse shaping used for Zigbee. Couch defines MSK as a continuous-phase FSK signal with a minimum modulation index (h=0.5) that will produce orthogonal signaling. His text provides the proofs of both statements dealing with the similarities between O-QPSK and with MSK[13]. When the sinusoidal pulse shaping of MSK is replaced with Gaussian pulse shaping, the resulting modulation is GMSK. GMSK improves the spectral efficiency of the MSK signal and also helps to stabilize the frequency variations over time[26] When dealing with GMSK, it is useful to know the value of BT, which is defined as the product of the parameters B, the 3 dB baseband bandwidth of the Gaussian filter, and T, the baseband symbol duration[26]

To understand why GFSK and GMSK are similar but not equal, it will be best to look at an example between the parameters of the two wireless standards, Bluetooth and GSM. GSM uses GMSK with a modulation index h=0.5 and a BT product of the Gaussian filter BT = 0.3. Bluetooth on the other hand uses a modulation index h to be between 0.28 and 0.35 with a BT product BT=0.5, thus it can be seen that since the modulation index is less than 0.5, the signaling is not MSK therefore it is considered GFSK. Similarities can be seen between the values of h and BT for Bluetooth and GSM. This is because both systems made tradeoffs between the two variables. As both h and BT increase, the bandwidth also increases. But as h and BT decrease, the eye of the signal becomes wider and also as h decreases the BER increases. This means that in assuming the system is modeled as an MSK rather than an FSK system, the result will be an overestimate of the true performance. The results obtained for Bluetooth will be better than if the system were modeled after an FSK system.

2.3.4 MAC Layer

The standard covers the PHY layer as previous discussed and also the MAC layer which deals with how the data is organized and sent. Each Bluetooth device is given a 48-bit device address, which is used for authenticity when creating a connection between devices. If two or more devices are trying to communicate with each other then a piconet is created. A piconet consists of a master device and its accompanying slave devices. There is nothing about a device that makes it either a master or a slave, all devices are built equally and being a master only depends on who initiates the contact. A piconet can contain up to 255 devices, although at a given time only eight can be active, one master with seven slaves. The reason behind this will be explained later when dealing with the different modes of operation. When several piconets are located within the same area, and some devices belong to several piconets, a scatternet evolves. Within a scatternet, masters and slaves can belong to different piconets. A master in one piconet can be a slave in another, and vice versa, a slave in one piconet can be a master in another, but a master of one piconet cannot be a master of a different piconet, otherwise it would just be considered as one big piconet. This is because the timing and hopping sequence is controlled off of the master's clock.

The timing within a Bluetooth network is critical because the protocol follows a TDMA (Time Division Multiple Access) system in which devices are given certain time increments in which they are allowed to transmit data. The communication is broken down into time slots and each time slot has duration of 625 μs , which comes from the 1600 hops/s. The master transmits on the odd time slots and the slaves are allowed to transmit on the even time slots as determined by the master. Therefore, only one time slot is allotted for each packet, although in some cases a packet may need to transmit more bits than are allowed in a single timeslot, in this case a master may allow for a given device to transmit for more than one time slot, as long as the total number of slots used is odd, e.g. 1, 3, 5, and so on. The practice of allowing a packet to last a duration longer than one time slot is utilized in pure data transmission only[27].

Bluetooth allows for two different types of communication links, SCO and ACL. Synchronous links or SCO links are mainly used for voice transmissions in which an application must have forward and reverse communication at regular intervals on dedicated time slots. SCO packets are rarely transmitted with coding and are never retransmitted because the voice transmission cannot be delayed for retransmission[28].

Asynchronous links, ACL, are pure data links that can allow for retransmission if a packet is received in error. These packets are coded with a cyclic redundancy check (CRC) or forward error correction (FEC) or both. ACL links also allot time slots as they are needed for certain devices. Rather than having dedicated time slots, as is done with SCO links, this allows for a packet to last for more than one time slot. Although, if an SCO link is being used, the ACL link must wait for time slots to become available, due to the real-time nature of the voice SCO link taking priority[28].

Before discussing the details of the FEC and CRC procedures, it may be useful to describe the structure of a general Bluetooth packet. The packet can be broken down into three parts, the access code, the header, and the payload. The access code comes at the beginning of every packet and consists of 72 bits which are used for synchronization, DC offset compensation, and identification[23] The header consists of 54 bits which are used to determine which device is transmitting, the type of packet being sent, the length of the packet being sent, whether the previous data was received successfully, and to check the header integrity[23] Finally the payload can consist of 0-2745 bits which contains the intended data to be transmitted along with any CRC or FEC that was incorporated into the data. A more in depth detailing of the packet can be found with the Bluetooth standard but that is outside of the scope of this report[23].

There are four basic types of error correction that is incorporated into the Bluetooth Standard and they may or may not be implemented depending on the application. Two FEC methods, the 1/3 rate and the 2/3 rate, can be instantiated. The 1/3 rate FEC is a redundancy technique that simply repeats each bit three times, so only a third of the payload of the packet is actually filled with information. The 2/3 rate FEC integrates a (15,10) shortened Hamming code with a generator polynomial equal to 65 in octal representation.[23] This is equal to taking 10 information bits and generating 15 coded bits that can be sent. The third error correction scheme is an automatic repeat request (ARQ) system in which the packet will simply be retransmitted until an acknowledgement is sent saying that the packet was successfully received, this acknowledgement is incorporated into the packet header as a single bit. If no acknowledgement is sent then the repetition will continue until a timeout value is reached, once it is exceeded, the packet will be discarded and the next packet will be transmitted. The fourth and final error correction system is the CRC. The CRC is composed of 16 bits and are generated by the CRC-CCITT polynomial 210041, which is given in octal representation[23].

While in a piconet, a device may be in one of four different modes. The first mode is an active mode in which the device is interacting with the other devices within a piconet, sending and receiving data. The next three modes all deal with power saving modes. The sniff mode uses the most power of the three and occurs when the device listens to the communication traffic within the piconet at a reduced rate but does not transmit data of its own. Another mode, which is a little more power efficient, is the hold mode. In the hold mode the device neither transmits nor receives data, with this down time the device can perform other operations or simply go into a power-save mode. The fourth mode is the park mode. The only difference between the hold and park mode is that in the park mode the device gives up its member address and in the hold mode it maintains its member address. This is where a piconet can contain either 8 or 255 devices, the member address is a 3-bit number, which can maintain up to 8 active members of a piconet. Each device is also given an 8-bit inactive member address in which it can stay synchronized with the master unit but does not actively participate. Therefore if a piconet contains 34 devices, 8 of these devices are in active mode and 26 are in park mode. If the master tells an active device to enter park mode, then the master can signal one of the parked devices to enter into active mode. While in parked mode, the device is in the most power efficient mode.

Chapter 3

Physical Layer System Models

3.0 Simulation

Why is there a need to simulate various ISM band devices and perform an interference study, why not just perform testing on site? When an on-site study is executed, there is no doubt about the results because they have been performed and tested. Subsequently, performance of a measurement campaign will yield a near 100% accuracy for the stimuli tested. Since the overall goal is to determine whether or not the three protocols can coexist with each other in an industrial environment, and since the campaign precisely did this, measured the interference between the different protocols for the assumed parameters, then why is there a need for simulation?

The need for simulation occurs because the amount of time that it would take to physically take measurements in all areas for which a coexistence study has been deemed necessary is a daunting task. With the different possible combinations of transmitters, receivers, and interferers, there becomes an endless amount of measurements to be taken. If a computer program could be created which would be able to take a physical layout of a building and compute the interference for certain combinations of different signals, then an educated guess could be made from these calculations and only a minimal number of measurements would need to be taken on-site in order to verify the functionality of the computer simulator. Therefore modeling the three protocols and simulating their physical layers can save a large amount of both time and money.

3.1 Monte Carlo Simulation

The next question to arise might be what sort of testing should be conducted, how are the models to be built? As an initial starting point, the first step most often is to conduct Monte Carlo simulations. Monte Carlo simulations are based on the probability of a random event occurring. As pertaining to a simulation of a communication device, Monte Carlo simulations contain no sort of pulse shaping of the signal at the transmitter (rectangular pulses are used), the channel is assumed to be AWGN (Additive White Gaussian Noise), the data symbols created to be sent through the simulation cannot be dependent upon each other and must be equally probable, and finally there can be any filtering in the system[19]. Incorporating all of these assumptions into an experiment may seem to oversimplify the simulation, but as a first step it is an excellent starting point. Not only does it get to the basis of the simulations and help to fully understand the operability of a given protocol but it is also a fast and efficient simulation due to the no filtering assumption. This allows the user to ascertain results to be compared with known results and ascertain whether or not the models are being properly created.

3.2 Zigbee Simulation

For Zigbee, the Monte Carlo simulation was set up using the following procedure. This procedure can be broken down into three different parts, which include the transmitter, channel, and receiver. The transmitter will generate the sent message bits and then encode them so that they may be transmitted. The channel adds both the fading and the AWG noise to the transmitted signal. The receiver then decodes the sent signal and determines what the sent signal was.

3.2.1 Zigbee Transmitter

The transmitter for the simulation can be broken down into two separate parts. These two parts include the message generation and the message encryption or spreading. A block diagram of the transmitter can be found in Figure 3.1. First is the message generation and since the basic building block of a Zigbee information packet is a data symbol composed of four message bits, this infers that a random variable between 0 and 15 needs to be created. This comes from the fact that four message bits can have 16 different possible values. This symbol that has a value of 0 to 15 is then fed into the spreading function of the transmitter.

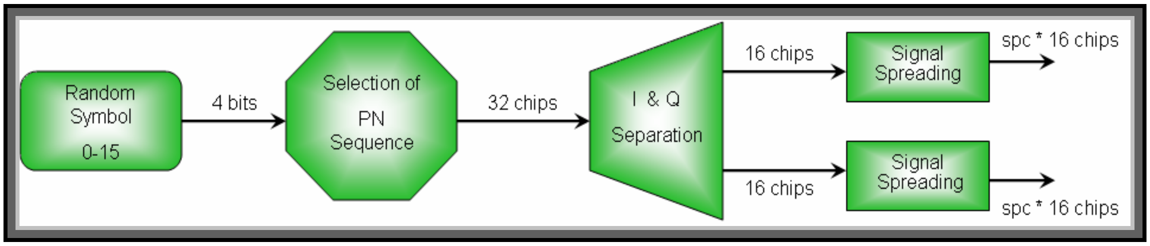


Figure 3.1 - Zigbee Transmitter

As was shown earlier, Zigbee has its own set of 16 quasi-orthogonal PN sequences, with each sequence corresponding to a symbol between 0 and 15 as determined by its binary equivalence. So once the symbol is passed to the spreading function, the spreader will output the corresponding PN sequence. For instance if a symbol of value 9 (1001) was sent to the input of the spreader, the 32 chip PN sequence corresponding to the 9 would be outputted (the sequence can be found in Table 1).

Once the proper chip sequence has been selected, it will pass through a few more steps before being ready to be entered into the channel. The next two steps are basically signal conditioning steps and involve simply a change of value and a change of indexing. The first step is to change the chip values from 1s and 0s as shown in Table 1, to values of 1s and -1s. Values of 1 stay and 1 and values of 0 change to values of -1. This is done for convention and to refrain from multiplying by a zero since the zero becomes a -1. This would also be used so that if pulse shaping was later added, the signal of 1s and -1s could be multiplied by the half sine pulse shaping and the correct output would be realized. As opposed to a 1 and 0 representation where when the half sine pulse shaping was multiplied by the message, the portion corresponding to a sent binary 1 would look like the positive portion of a sine wave, but the portion corresponding to a sent binary zero would look like a flat line at zero rather than a negative portion of a sine wave. Since for this example no pulse shaping is used, either convention would work, but using a 1 and -1 representation is intuitively more appealing.

The next step of the signal conditioning was referred to as a change of indexing step. Another way of putting it is that the signal would be separated into a direct (I) phase and a quadrature (Q) phase so that it may be QPSK modulated. If the 32-chip sequence was thought to contain place values from 0 to 31, meaning the first value of the chip sequence was thought to hold the zero place, while the last value of the chip sequence was thought to hold the 31st place. The when the chip sequence was separated into its I and Q phase equivalence, the even indexed chips would be placed in the I phase and the odd indexed chips would be placed in the Q phase. This can more easily be seen by an example from the 802.15.4 standard. Figure 3.2 shows how the chips would be grouped had the input sequence been 32 chips long beginning with the chips 11011001… and so forth. If separated as specified, the I phase includes the values {1 0 1 0} and the Q phase includes the values {1 1 0 1}. This figure also shows house half sine pulse shaping would be implemented. Once the chip sequence is separated into its I and Q phase, the signal is almost ready to be introduced to the channel.

3.2.3 Zigbee Receiver

Upon reception of the transmitted signal that has been either faded or just having noise added to it, the signal must be down sampled, or more specifically, integrated over the chip interval. This means that when the chip is upsampled, if the spc is equal to two, the two values would be summed together for the downsampling. This will be done for every set of chips values, resulting in a signal half as long as the transmitted signal and equal to the length of the original signal before the upsampling. The resulting values can span the entire range of positive and negative values. Now that the signal has been downsampled, the signal is ready to be entered into the receiver design.

For the Zigbee receiver, which can be found in Figure 3.3,, after the summation over the chip interval, the result is a soft decision which can take on any range of values and not just a solid 1 or -1. This allows for a more reliable result to be obtained from the correlation. This allows for a value near a strong 1 to have more of an influence on the value being a one rather than a value more near 0 which could have resulted from a -1 having noise added to it.

Once the soft decision has been made, the received signal is separated into blocks of 16 chips. Remembering that there are still separate phases, an I and a Q phase. Therefore the grouping of 16 chips in each phase will result in being equivalent to the 32 chips in one PN sequence. Therefore, each of the possible PN sequences are grouped into their respective I and Q phase representations, as set forth earlier, where the even chips are placed in the I phase and odd chips are placed in the Q phase. Rather than the PN sequence containing 1s and 0s, they will be transformed to contain values of 1 and -1. Once separated, the I and Q phases of both the received signal and of the transmitted PN sequence are correlated with each other. This results in the need for 32 correlators, 16 for the I phase and 16 for the Q phase. The correlators consist of multiplying each of the 16 possible transmitted sequences with the received sequence for both

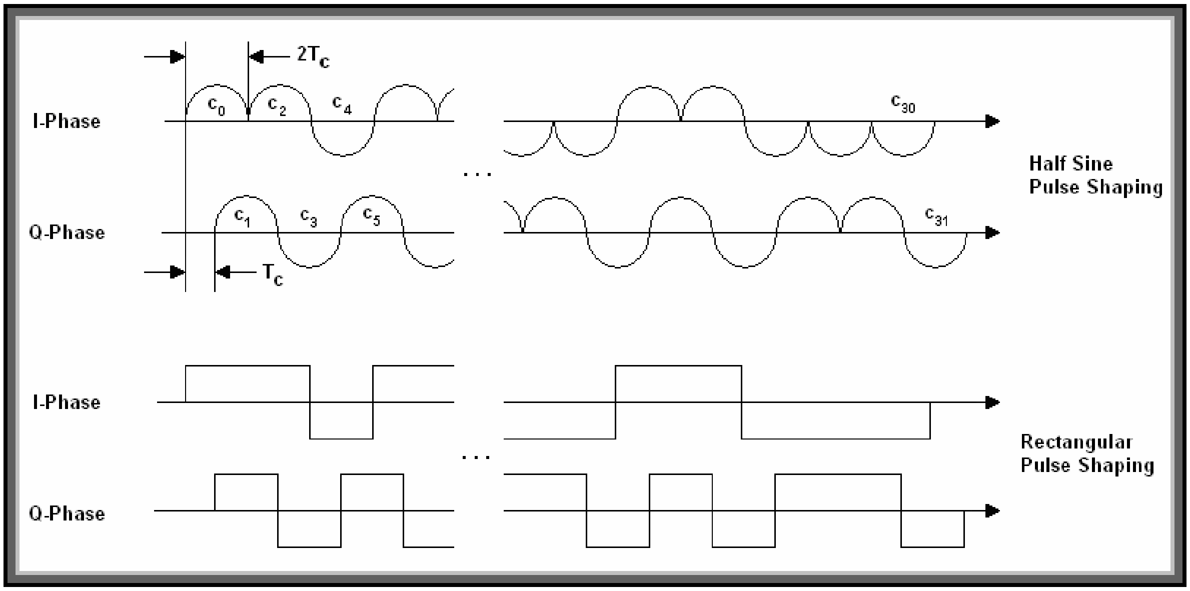


Figure 3.2 – Chip Sequence Separation with Half-Sine Pulse Shaping

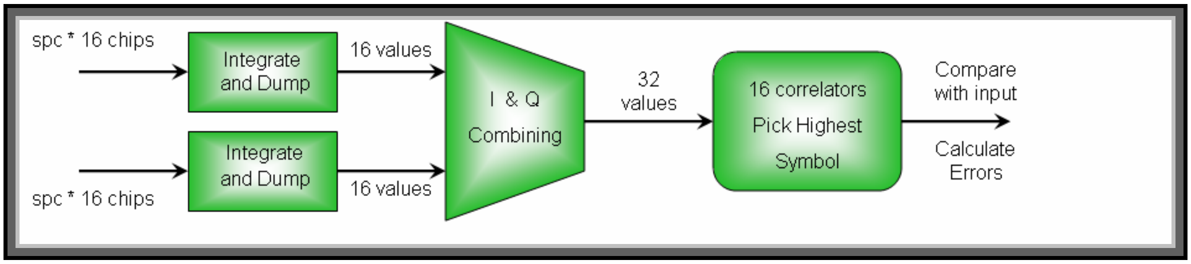


Figure 3.3 - Zigbee Receiver

the I phase sequences and the Q phase sequences. The result will be that if two chips have the same sign, they will add to the correlation and if the two chips have different signs then the value will decrease the correlation. Once all sixteen values are summed together, the highest value will be chosen corresponding to the PN sequence assumed to have been sent. If the PN sequences for the I and Q phases agree with each other, then that sequence will be chosen as being transmitted and the corresponding symbol obtained. However if the two phases do not agree on the same sequence then the two sequences will have their correlation values added together from each phase and the largest value chosen.. Once the data symbol is found, it is converted to a binary number and compared with the transmitted binary message. For instance if a symbol 4 {0 1 0 0} was sent but the received symbol was a 12 {1 1 0 0} then the result is a total of 1 error, since only one bit is different between the two symbols.

3.3 Wifi Simulation

For Wifi, the Monte Carlo simulation is set up using the following procedure. Very similar to how the simulation for Zigbee was broken down, the procedure for Wifi can be broken down into the same three parts, the transmitter, channel, and receiver. The transmitter generates the sent message bits and then encodes them so that they may be transmitted. The channel adds both the fading and the noise to the transmitted signal. The receiver then decodes the received signal and compares it with the sent signal to obtain the number of errors.

3.3.1 Wifi Transmitter

The transmission technique for Wifi varies from the transmission of Zigbee, as can be seen in Figure 3.4,, even though both claim to use a DSSS system. Both still contain the signal generation and the system encoding, but there is a slight difference in the former and a big difference in the latter. This is evident in the fact that Zigbee has a chip rate 8 times greater than the bit rate, and for Wifi, the chip rate is equal to the bit rate.

The first step for the Wifi transmitter is the generation of a random signal. Since Wifi uses a base symbol size of 8 bits, it is convenient to create 8 random variables that have given values of 1 or 0 and place them into one symbol. The next task for the transmitter is to encode the data bits. This process takes three steps to complete and consists of breaking the 8 data bits into the four

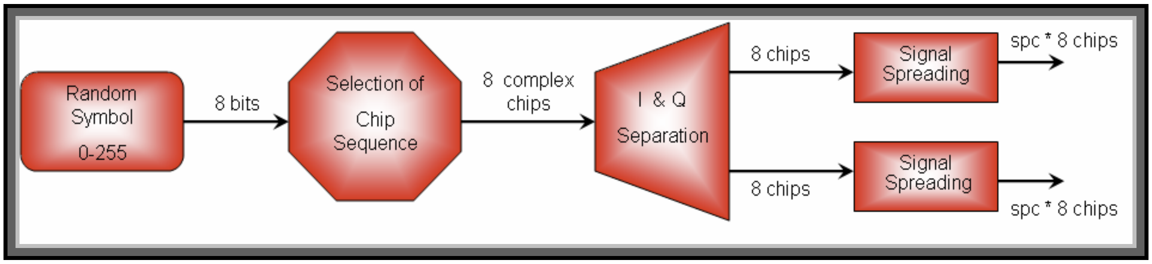


Figure 3.4 - Wifi Transmitter

phase values, determining the codeword, and then doing some signal conditioning to make the signal easier to transmit. The first step is fairly straightforward and is determined in the background information; it takes the 8 data bits, and groups them into four sets of two. Each group of two bits represents a phase value found in Table 2.

The following step to encoding the data involves the use of Eq (1). Normally when using Wifi, Eq (2) is used, but since correlators have not yet been introduced into the system, and since the computation can be minimized by not taking the extra step of creating the codeword, and then rotating the codeword, it can all be done at once using Eq (1) without suffering any of the integrity of the simulation. The effect is to create 8 coded chips from the 8 data bits.

The 8 coded chips can have the values {1, -1, j, -j}. In order to represent these values in an I and Q representation, three symbols are needed {1, -1, 0}. It is desired to only require two symbols {1, -1}. In order to make this transformation, the coded chips values must first be rotated and then scaled. This is accomplished by adding a rotation of $\pi/4$ to the coded chip values. This results in values of the form $\{\pm 0.707 \pm j0.707\}$, which would work when trying to transmit either a 0.707 or a –0.707 because they are two distinct values, but the convention is to use a 1 or –1 so the values are simply swapped, 1 for 0.707 and –1 for –0.707. This is a valid switch because the increase in signal power is accounted for when calculating the noise variance.

In order to allow for a greater efficiency, the simulation execution runtime needs to be sped up; therefore the above transmitter process is only performed in one single instance at the very beginning of the simulation. Every possible 8-bit input is fed into the process and the resulting 8-chip outputs are stored in a lookup table. This allows for a possibility of 256 different combinations. Therefore, all that is needed during the execution of the simulation is for a random variable to be chosen from the values of 0 to 255, and using that value to scan through the lookup table and output the corresponding 8-chip sequence. This saves time by not having to group the bits, encode them and then rotate them.

The only step left before transmission is to upsample the chips in order to have one or more copies of each chip, which is not necessary for a Monte Carlo simulation, and it would have a bigger impact had pulse shaping been used, as such it is incorporated so that the simulation can be built upon at a later time.

3.3.3 Wifi Receiver

Phase detection is the method used within the decoder found in Figure 3.5. But before going into phase detection, the receiver must downsample the received signal by accounting for the upsampling of the chips. This is done by adding the adjacent chips that were copies of each other and making the decision that if the sum is positive a 1 was sent and if the sum is negative then a zero was sent.

Next the two phases, I and Q, are added back together by making the I phase the real part and the Q phase the imaginary part of the received codeword. This results in a codeword that has values of $\{\pm 1 \pm j1\}$, which are not equal to the desired values that are {1, -1, j, -j}. Therefore, the values must be rotated back by a value of $\pi/4$. In this simulation it is done by assignment, it checks to see if the real part is a 1, if it is then it checks for the value of the imaginary part, if the imaginary part is 1, then the chip value is a 1, otherwise the chip value is a –j. On the other hand if the real part were a –1, then the routine would check to see if the imaginary part were a 1, if it was then the chip value would be a j, otherwise the chip value would be set to be –1. Once completed for all the chips, the simulation must obtain the phases. This is done by inversing the equation for the chip value of the eighth chip in the codeword. As can be seen, this chip value only contains the value of phase 1. From this value, similar inversing can be done to the 4th, 6th, and 7th chips in the codeword to determine their phases.

Now that the phases are known, which can have values of $\{0, \pi/2, \pi, 3\pi/2\}$; the corresponding binary values can be found from Table 2. The binary values can then be concatenated and the resulting 8 bit received data bits are now known. The data bits can be compared to the original sent data bits and a count can be kept for the number of errors that occur. Much like Zigbee, the Wifi simulation is conducted for different values of signal-to-noise (SNR) and the corresponding number of errors is tabulated. Once completed the number of bits in error is divided by the total number of bits sent and that is plotted versus SNR.

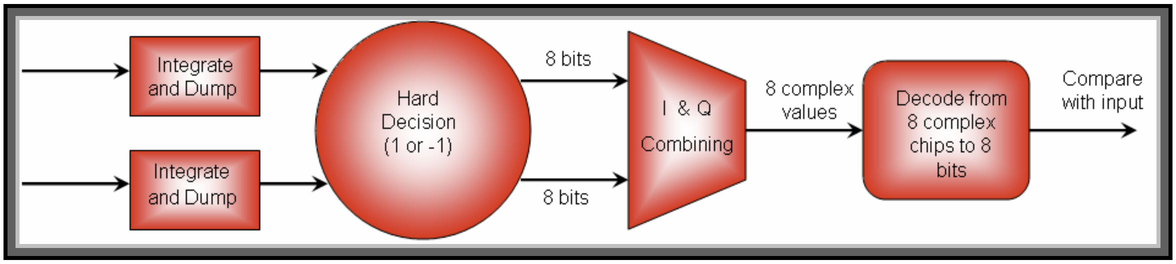


Figure 3.5 - Wifi Receiver

3.4 Bluetooth Simulation

In the final simulation model for Bluetooth, the Monte Carlo simulation was created in a very similar manner as were the previous two models. Although for Bluetooth there are some assumptions that need to be made before a model can be created that will allow it to be joined with the previous two models so that an interference study to be conducted. There are two main groups of assumptions that must be made, one deals with the fact that Bluetooth is based on an FSK modulation scheme which must be dealt with in the transmitter, and the second group of assumptions stems from the FH-SS nature of Bluetooth and will be dealt with within the interference study when the models must be joined together.

3.4.1 Bluetooth Transmitter

The first assumption that can be made is that the GFSK system of Bluetooth will be modeled as a regular FSK system because of the fact that in a Monte Carlo simulation, pulse shaping is not considered. This means that the Gaussian pulse shapes can be disregarded and not considered. This assumption goes along with the other two models' assumptions in the fact that their pulse shaping techniques were not included such as the half sine pulse shaping of Zigbee. The main reason for not considering the Gaussian filter to shape the outgoing signal is to decrease the run-time of the model. In order to include pulse shaping, each bit must be spread in order to resolve a Gaussian pulse out of it, this in turn increases the amount of time needed for the simulation to run by a factor of however many samples are taken, upwards of 50 -100 times.

The second major consideration that must be taken into account is that in the other two simulations, they are broken down into their I and Q phase components. So to ease the combining of all of these models, it would be helpful for them all to be based off of that fact.

Therefore it becomes logical to create an FSK model that will use I and Q components rather than frequency components. One such way to do this is to model an FSK system using an MSK system. It was shown in the background portion of the report that GMSK and GFSK are very similar modulation techniques. If the assumption is made that by letting h, the modulation index for Bluetooth, be equal to 0.5, then it becomes a GMSK system, whereby after pulse shaping has been discarded, it then becomes an MSK system. An MSK signal can be represented using I and Q components. Therefore the assumption will be made that Bluetooth's modulation can be approximated using MSK techniques.

To create a transmitter for Bluetooth modeled after an MSK system, it involves having a data source to create a data stream consisting of 1s and -1s. For MSK, the I and Q components are created in much the same way as for Zigbee. The even indexed bits are placed in the I phase and the odd indexed chips are placed in the Q phase, with the first bit indexed as the 0^{th} bit. Since Bluetooth uses FH-SS instead of DS-SS, the created data bits are the sent bits, they are not spread using and type of PN sequence. Now that the data is in the I and Q phase, they can be sampled so that there may be more than one sample per chip. This will become more prevalent when combining the models for the interference study. The Bluetooth transmitter can be found in Figure 3.6, notice there is no type of PN sequence involved because of the FHSS system.

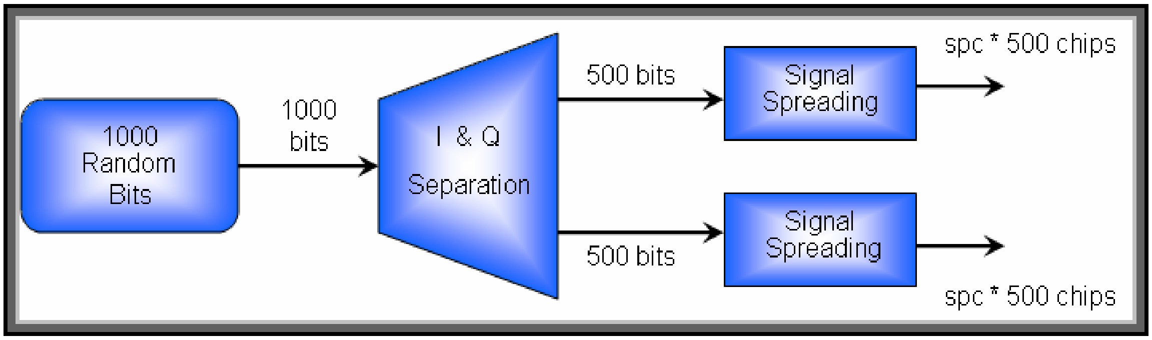


Figure 3.6 - Bluetooth Transmitter

3.4.3 Bluetooth Receiver

The receiver for the Bluetooth model will be modeled to perform much like an integrate and dump receiver design shown in the block diagram of Figure 3.7. The incoming data is summed over the length of a bit period, whether it consists of a single chip or a number of chips, depending on the value of spc. After being summed, if the value is greater than zero, a value of one will be assumed to have been sent, if the value is less than zero, then a binary zero will be assumed to have been sent. This will be done in both the I and Q branches of the receiver, once completed they will be intermixed in the same way that they were separated and will become one long data stream. This data stream will be compared with the sent data and the number of errors determined. Exactly like the previous two models, the Bluetooth simulation is conducted for different values of SNR and the corresponding number of errors is tabulated.

3.5 Channel

Now that the transmitted signal has been created, it is ready to be passed through the wireless channel model. The model will consist of two separate parts, the fading model and the AWGN model. The fading model is only used when fading is considered and is not used for the ideal channel case in which only AWGN is considered. Both cases will be considered within the results portion of the report.

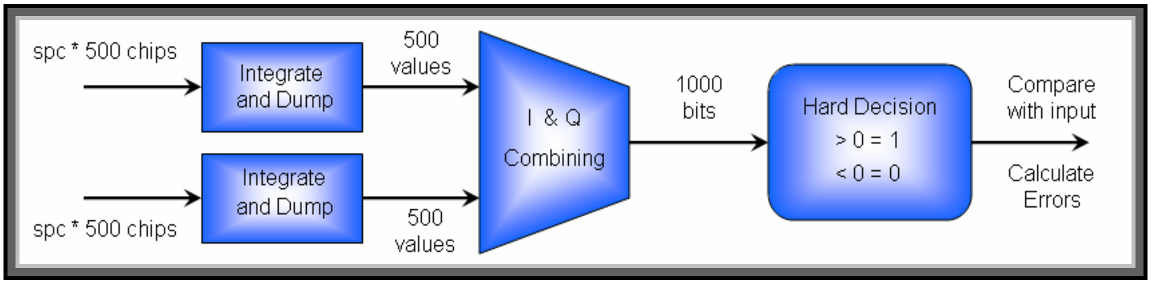


Figure 3.7 - Bluetooth Receiver

3.5.1 AWGN

The AWGN model is perhaps the trickiest portion of the whole simulation in terms of subtlety. It is something that does not draw a lot of attention to itself, but can be difficult to implement, mainly because of the scaling factor. The noise is created from two separate noise generation sources. One source for the I phase and once source for the Q phase. The two phases must have independent sources, otherwise, the AWGN assumption may not hold true anymore because the two phases could become cross-coupled. Therefore, for each phase, the following procedure must be followed. The noise consists of generating a random variable with a zero mean and a standard deviation and variance both equal to one. The random variable is then scaled by the noise variance.

The noise variance is dependent upon the amplitude of the signal, which for the Monte Carlo simulation for Zigbee is $\sqrt{2}$, the number of chips per bit, which is equal to 8 (due to 4 bits being represented by 32 chips), the number of samples per chip (spc), which is arbitrarily set to 2 (more important for pulse shaping, does not change the simulation since as there are more spc, the noise variance also increases), and the SNR. The main variable is the SNR, as the SNR increases the noise variance decreases making the noise level lower.

Once the noise variance is multiplied by the random variable the result is then added to a single chip. For example if the random variable was 0.25 and the noise variance was 0.4 then the noise value would be equal to {0.1}. If for instance the transmitted chip were a 1 then the noise added to the signal would yield a value of 1.1. As seen later, this will result in the chip not being in error. If for example the next chip was sent and this time the new random variable was had a value of -2.8 (since a new random variable needs to be created for each chip) and the noise variance was still 0.4 (the noise variance only changes for a new SNR) then the resulting noise value would be equal to {-1.12}. If that next chip was also a 1, then when the noise was added to the chip, the result would be a chip with the value of {-0.12} that will be detected as a 0 and an error will have occurred.

3.5.2 Fading

To improve the accuracy of the system model for the on-site floor plan design, fading must be incorporated into the channel. There are two assumed channel types widely used to model indoor wireless channels. The first case is when there is a LOS path between the transmitter and the receiver, in this situation a Ricean fading envelope is assumed. The second case is when there is an object obstructing the LOS path between the transmitter and receiver, such as a wall, desk, pipes, or a person walking. In each case there becomes no direct path between the transmitter and receiver creating a non line-of-sight (NLOS) scenario, which is often modeled as a Rayleigh fading distribution over the wireless channel. These distributions will be explored further and their similarities and differences will become apparent.

There are two different varieties of fading, large and small scale. Large scale fading occurs due to signal attenuation caused by path loss, it fluctuates as the transmitter is moved away from the receiver at distances much greater than a few wavelengths of the signal, and is the average power of the signal over a local distance. Small scale fading, on the other hand, is not caused by path loss since small scale fading is the instantaneous fluctuations in the power of the signal. Since over short distances, on the order of wavelengths, the path loss will remain approximately constant, there must be some other phenomenon affecting the signal.

The phenomenon can be explained in two parts. The first part of the explanation deals with the phase of the signal. When two signals intersect each other in space, the overall effect of the resulting signal can range from the summation of the two signals to the subtraction of the two signals, this is because two signals which are out of phase with each other will add destructively, and conversely two signals which are in phase with each other will add constructively. The second part can be explained by imagining any number of signals combining at a single point, the overall effect will result in one single value, which is what happens within a receiver, and this value will change as the environment in which the signal is propagating changes. However, since our environment is assumed to be static to an extent, this value will not vary a great deal, therefore the receiver is thought to be receiving signals in a ray form. The ray form is composed a numerous signals added together to give the overall effect of one signal. Because this ray is formed from a wide variety of signals, its value will fluctuate as if it were the receiver point. The simulation assumes there are ten such of these rays being received. Each of the ten rays will be Rayleigh faded unless there is a LOS ray and in that case the LOS ray will not fluctuate and will maintain a constant value.

3.5.3 Ricean

The first fading channel to be studied is the Ricean distribution, in which a LOS path is present and unfaded. In this situation, the individual paths are not Ricean faded. Ricean fading is a collection of the entire ten paths and signifies the distribution that the overall effect can best be modeled after. Ricean fading is a collection of a number of Rayleigh faded paths which can be superimposed upon a signal with a constant value. This constant value can be used to determine the Ricean K-factor which signifies the energy contained within the dominant path with respect to the spectral energy of the secondary paths, however, for the present simulation, the K-factor is not used to produce the fading because the theoretical energy of each signal has already been determined through the use of Wireless Insite. For this simulation, the nine Rayleigh faded rays are added to one ray which is given a normalized energy value. The K-factor can be used to explain the connection between Ricean and Rayleigh fading.

3.5.4 Rayleigh

Rayleigh fading is a special case of Ricean fading, which is a way of saying that when the Ricean K-factor is equal to 0, Ricean fading degenerates to Rayleigh fading. This is another way of saying that the stationary DC value corresponding to the LOS path is no longer present. For the simulation, this means that the ten rays are all Rayleigh faded and none are composed of a normalized energy value.

The Rayleigh fading simulator is shown in Figure 3.8. The diagram is a frequency domain implementation for creating a Rayleigh envelope. The Rayleigh envelope consists of creating two independent random Gaussian sequences. The sequences are then filtered through a Jakes Doppler Spectrum. The spectrum follows a bath-tub curve and is represented as the square-root of the following equation.[26]

$$S_{E_Z}(f) = \frac{1.5}{\pi f_m \sqrt{1 - \left(\frac{f - f_c}{f_m} \right)^2}}$$

Where f_c is the carrier frequency, set as 2.4 GHz, and f_m is the Doppler frequency. In this case the Doppler frequency is approximately 14 Hz. The Doppler frequency is proportional to the

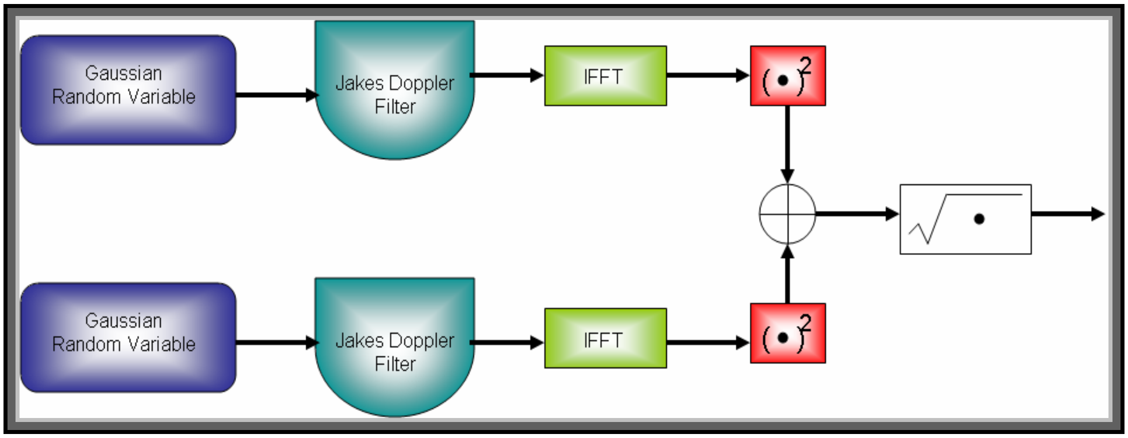


Figure 3.8 - Rayleigh Simulator

velocity of objects in the path of propagation, for the indoor environment, the maximum speeds that need to be considered are those of people walking, which are less than 4 mph, or 6 ft/s.

After the random variables have been filtered, an Inverse Fast Fourier Transform (IFFT) is performed on the two separate sequences. By taking adding the squares of each of the two signals, and then taking the square root of the result, a real signal will be generated. This signal can be multiplied with the transmitted signal to create a Rayleigh faded signal. Due to the two phases of the transmitted signal, the direct and quadrature phase, a separate Rayleigh envelope must be generated for each phase.

3.5.5 Simulation Design - Power

The first step in determining the values of the 10 path gains to be used in the simulation is to take the ten values of received power from Wireless Insite and normalize the path gains to the greatest value of path gain, normally the first arriving path. In doing this, the first arriving path obtains a value equal to 0dB and the subsequent values of the nine other paths will all be less than 0dB. This vector of ten path gain values is then used to scale the value of the Rayleigh channel. For instance, the first path gain of 0 dB means a value of 1 in linear units. Therefore, when multiplying the simulated Rayleigh faded signal by the path gain of the first path, it will result in the just a multiplication by a value of 1, so there is no change. All of the subsequent path however, will have path gains, which are less than one, so the value of the resulting Rayleigh faded paths will be less than the simulated Rayleigh signal.

3.5.6 Simulation Design - Phase

Nearly as important as the power in each path, maybe even more important when considering the fact that the power is normalized, is the value of the phase of the signal. The phase signifies the phase of the sine wave that the signal is being transmitted with, referring to the phase of the message signal, not that of the carrier. The phase is important because two signals with different phases can potentially cancel each other out if they are 180 degrees out of phase with equal power.

The phase is dealt with in a similar way as the power was handled. Since the first arriving path has its power normalized to 0dB or a value of 1, the phase of that signal is also normalized to 0 degrees, since that is where the phase detector will lock on and compare the other signals to the phase of the first arriving path. Therefore since the first path will have the phase of its signal subtracted from it to have a phase equal to 0, all subsequent paths will also have the phase value of the first path subtracted from them.

In order to translate the phase from degrees to a viable number, the cosine of the phase must be taken. The resulting values, when multiplied by the normalized power values, yield the effect of the multi-path. For instance, since the power of the first path is normalized to 1 and the phase has a value of 0, which yields a value of cos(0) = 1, meaning that the power multiplied by the phase is 1(1) = 1, so the first path will always have a value equal to 1. Subsequent paths will have values that fall in the range of 1 down to -1, meaning that some of the paths could take away information from the message. One example would be if the second path had a power value of -3dB, which refers to a value of 0.5, and if the phase was 135 degrees, which yields cos(135) = -.707, then the resulting effect of the second path is (0.5)(-0.707) = -0.35, which means it diminishes the normalized signal by a value of 1/3.

3.5.7 Simulation Design - Delay

A third consideration for improving the accuracy of the simulation is also provided through the output of Wireless Insite, this is the time delay of each signal relative to the time of the signal being transmitted. The delay of the signals are important because if the relative delay of two signals are significant when compared to the chip interval, then the two signals could add with chips being intermixed, a chip from one signal will not be superimposed with itself in the second signal, it will combine with the chip that was received in that time frame. In this situation being presented, ISI is not the merging of pulses within a single path, it is the combining of pulses from different paths. Depending on the delay, the distortion of the symbol caused by ISI will change, it the delay is on the order of half chip periods, then the distortion will be very noticeable, whereas if the distortion is a multiple of a chip period, then the distortion may not be noticeable but information could be lost due to the canceling of signals.

For this simulation, since the relative delays were not considerable when considering the chip periods, they were not implemented into the simulation. In order to accurately model the signals with their delays, instead of the chip period being broken into 2 sections or samples per chip, the number of slices would need to be on the order of nanoseconds. For the protocols being simulated, this corresponds to taking anywhere from 100 samples per chip for Wifi, up to 1000 samples per chip for Bluetooth. Because the runtime of the simulation is directly proportional to the number of samples per chip, this would result in the runtime of each simulation being increased by a magnitude of 10^2 or 10^3, corresponding to additional days of computer processing. Since the delays calculated for the three separate protocols are not significant compared to the chip period, the distortion caused by the addition of the ISI would not affect the overall signal in a substantial way. This means that the increase in accuracy of the simulation would only slightly change while the complexity of the system coupled with the computer processing required for the simulations would increase exponentially. Because the trade-offs do not offset each other, the delay does not warrant being included and thus will be left out of the simulations, but the simulations can be modified at a later point in time.

To illustrate the assertion that incorporating the delay into the simulation would have a diminishing return when considering the amount of accuracy gained through increased complexity versus the escalated runtime caused by the number of samples needed per chip, transmitter files were chosen for each protocol under different propagating characteristics. The propagation parameters will include a LOS case when the propagation is only in the range of a meter, a NLOS in which the wave must travel on the order of five meters, and finally a case where the NLOS travel is stretched farther and must propagate a distance exceeding fifteen meters.

3.5.8 Bluetooth Delay

Since Bluetooth has the longest chip period, $1\mu s$, corresponding to the chip rate of 1 Mchips/s, it will be the first scenario to be considered. For Bluetooth, the LOS situation will be observed to determine how the reflections affect the direct path and whether the shifting of the information bits due to the delay is considerable enough that it should be modeled within the system. From Table 3-1, it can be calculated that the first path, the LOS path, contains 90% of the total power found within all ten paths. Therefore a significant amount of the energy contained within the signal is received at the instant the first path is detected, which does not warrant a need to delay each given path. Also upon inspection of the delays of each path found in Table3-1, all signals are received within 38.1 ns of the first arriving signal, this corresponds to all signals be received within the first 4% of the chip period. Figure 3.9 demonstrates that characteristics of the propagation path due to the delay approximates a rectangle which is the assumed shape used within the simulations.

3.5.9 Zigbee Delay

With a chip rate of 2 Mchips/s, double that of Bluetooth, Zigbee has an equivalent chip period of 500ns. The Zigbee transmitter and receiver combination is chosen such that there is an NLOS scenario, in which the signal will have to propagate through a wall, with a minimum path distance of a 5 m between the transmitter and receiver. As can be seen in Figure 3.10, the results are very similar to those of Bluetooth, the shape approximates a rectangle, with minor imperfections cause by both the power and delay of the secondary paths, two through ten. By looking at Table 3-2, showing the delay corresponding to Zigbee, it can be observed that 93% of the total energy is contained within the first 5 paths, and that these 5 paths occur within the first 1.12% of the chip period, or the first 5.6ns. The total delay spread is only 27.7ns, which relates to only 5.6% of the chip period, making the Zigbee delay not worth being included into the simulation.

3.5.10 Wifi Delay

Unlike the previous two examples, Wifi has a much shorter chip duration, only lasting for 90 ns, a factor of over 5 times faster than Zigbee. This is caused by the 11 Mchips/s assumed from the 802.11b Standard. This means that the delay associated with each path will have a greater effect on the overall signal. Coupling that with the fact that for Wifi, the propagation path implemented was for the signal to undergo several transmissions and/or reflections through or off of walls during its travel, which is in excess of 15 m, thus increasing the delay spread of the signal. As

Table 3-1 - Bluetooth Delay

Path #	Power (dBm)	Delay (ns)	Normalized power	Normalized Delay	% Path Power of Total Power	% Delay of Total Chip Period
1	-37.35	5.22	1	0.00	89.85	0
2	-51.47	8.85	0.039	3.60	3.50	0.36
3	-53.56	12.24	0.024	7.00	2.16	0.7
4	-54.22	14.32	0.021	9.10	1.89	0.91
5	-57.06	16.62	0.011	11.40	0.99	1.14
6	-59.19	21.92	0.007	16.70	0.63	1.67
7	-62.43	23.05	0.004	17.80	0.36	1.78
8	-61.62	29.05	0.003	23.80	0.27	2.38
9	-63.9	29.92	0.002	24.70	0.18	2.47
10	-65.1	43.31	0.002	38.10	0.18	3.81

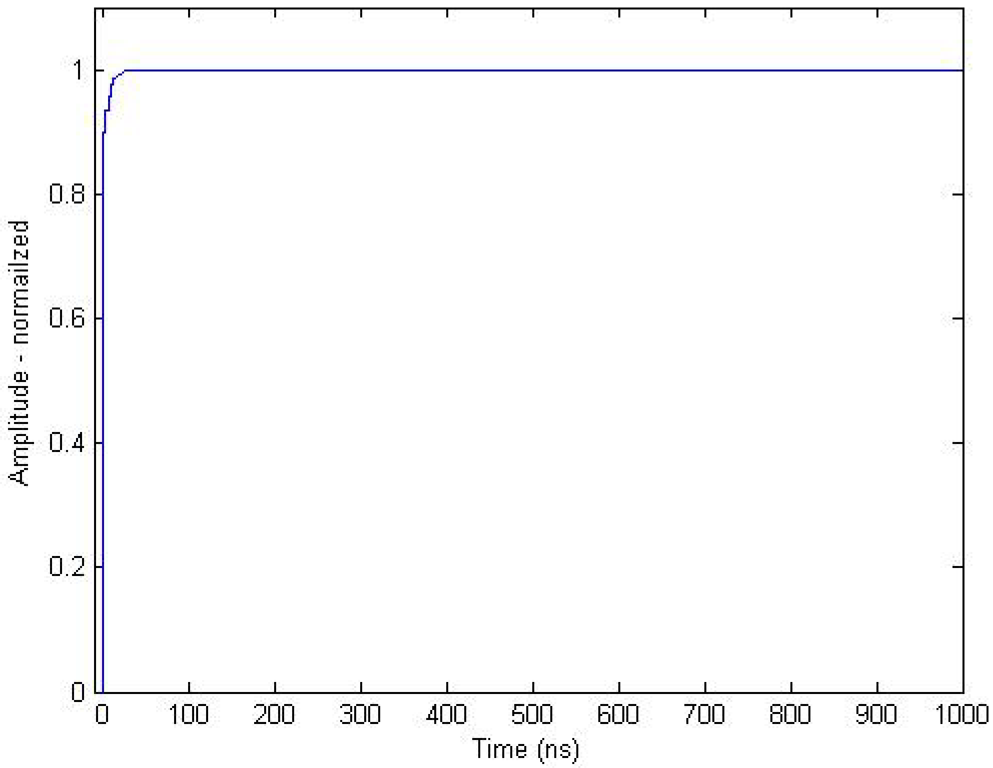


Figure 3.9 - Bluetooth Delay Amplitude

Table 3-2 – Zigbee Delay

Path #	Power (dBm)	Delay (ns)	Normalized power	Normalized Delay	% Path Power of Total Power	% Delay of Total Chip Period
1	-47.84	12.94	1	0.00	73.58	0
2	-57.79	16.06	0.101	3.10	7.43	0.62
3	-62.16	17.03	0.037	4.10	2.72	0.82
4	-58.36	17.55	0.089	4.60	6.55	0.92
5	-61.59	18.58	0.042	5.60	3.09	1.12
6	-62.49	23.27	0.034	10.30	2.50	2.06
7	-67.03	24.12	0.012	11.20	0.88	2.24
8	-67.34	25.15	0.011	12.20	0.81	2.44
9	-64.37	29.14	0.022	16.20	1.62	3.24
10	-67.32	40.66	0.011	27.70	0.81	5.54

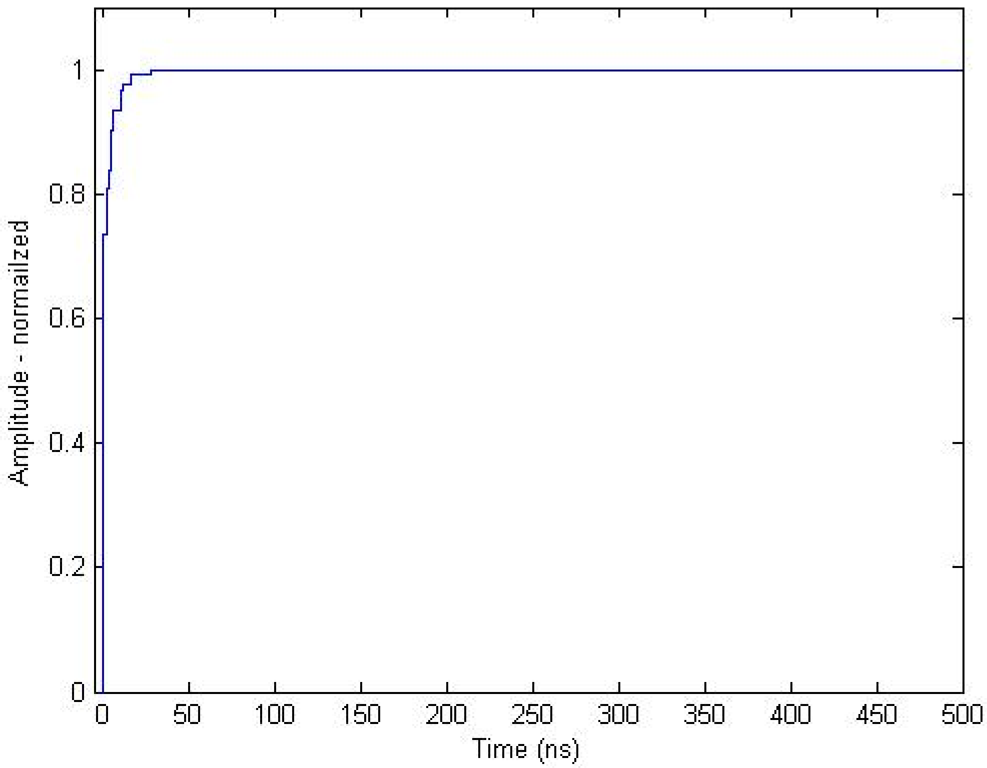


Figure 3.10 - Zigbee Delay Amplitude

can be seen from both the figure representing the waveform caused by the delay in Figure 3.11, and the numerical form in Table3-3, the overall signal is affected much more by the delay than of the previous two examples. The questions that remains is, is the deformation of the signal significant enough to merit being replicated within the simulation? From the table it can be seen that the last signal arrives at 26.8ns, which is a third of the total chip period, but this path only contributes less than half of one percent to the overall signal energy. When considering only the first five arriving paths, they account for over 92% of the total energy of the signal and occur within the first 5% of the chip period, or 4.4ns, since the paths approximate a rectangle, the delay can be disregarded.

3.6 Interference

The way to model the interference between the three different protocols is to conduct it in a block fashion. The first step is to take the transmitter portion of the three different models and place them into one big transmitter file. Then by adding the three separate receivers to the one big transmitter file, three different models were created- one for when Zigbee was the intended signal while Wifi and Bluetooth were the interferes, another for when Wifi was the intended signal with the other two as interferers and the final model for Bluetooth with the two interferers. Once these three models had been developed, another interfering transmitter model was added to them, each one duplicating the model of the intended signal for the specific model (for example in the Zigbee model, another Zigbee transmitter was added that would act as a Zigbee interferer, the same held true for both the Wifi with a Wifi interferer and a Bluetooth model with a Bluetooth interferer). Now that the foundation for an interference model was constructed, the model could be massaged so that it would simulate a real world environment of how the interference would take place.

3.6.1 Site-Specific Channel Model

For the site-specific model, the channel is formulated from Figure 3.12. This figure shows the direct phase branch of the transmitted signal. An identical method is also used to construct the fading channel for the quadrature phase of the transmitted signal. The flow of the diagram is that each individual path is faded and scaled and then the total signal is scaled. For the NLOS

Table 3-3 - Wifi Delay

Path #	Power (dBm)	Delay (ns)	Normalized power	Normalized Delay	% Path Power of Total Power	% Delay of Total Chip Period
1	-34.69	18.08	1	0.00	69.11	0.00
2	-41.64	20.81	0.202	2.70	13.96	3.00
3	-51.33	21.2	0.022	3.10	1.52	3.44
4	-49.36	22.47	0.034	4.40	2.35	4.88
5	-45.98	22.86	0.074	4.80	5.11	5.33
6	-51.33	25.08	0.022	7.00	1.52	7.77
7	-48	29.06	0.047	11.00	3.25	12.21
8	-52	30.83	0.019	12.80	1.31	14.21
9	-51.58	42.61	0.021	24.50	1.45	27.19
10	-56.76	44.86	0.006	26.80	0.41	29.74

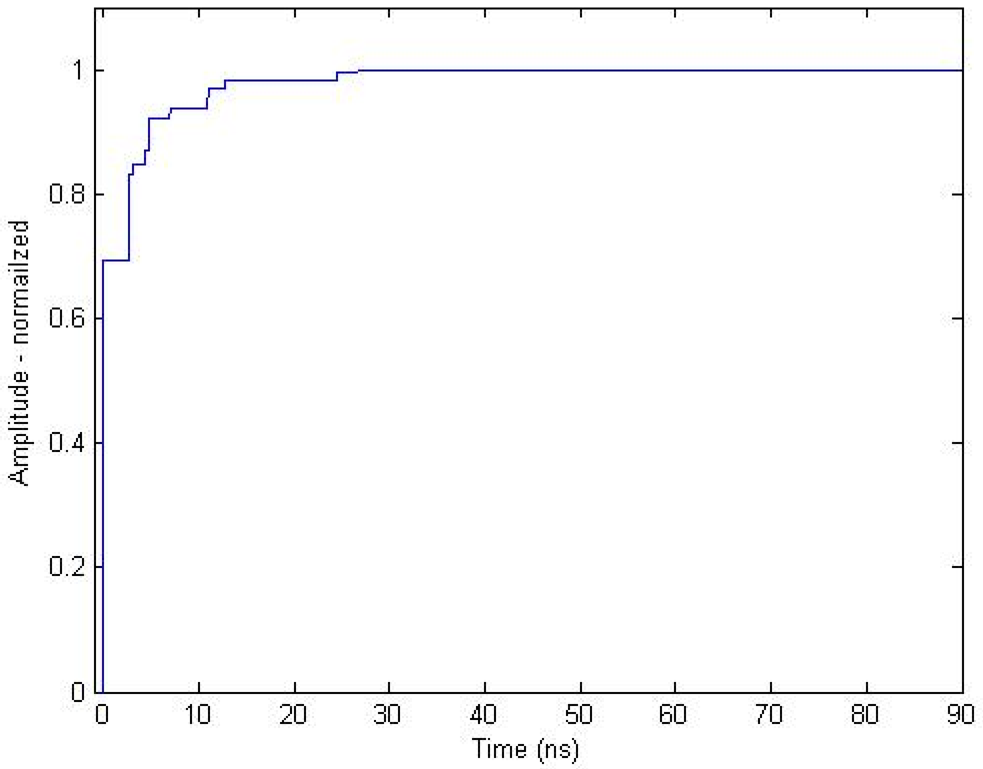


Figure 3.11 - Wifi Delay Amplitude

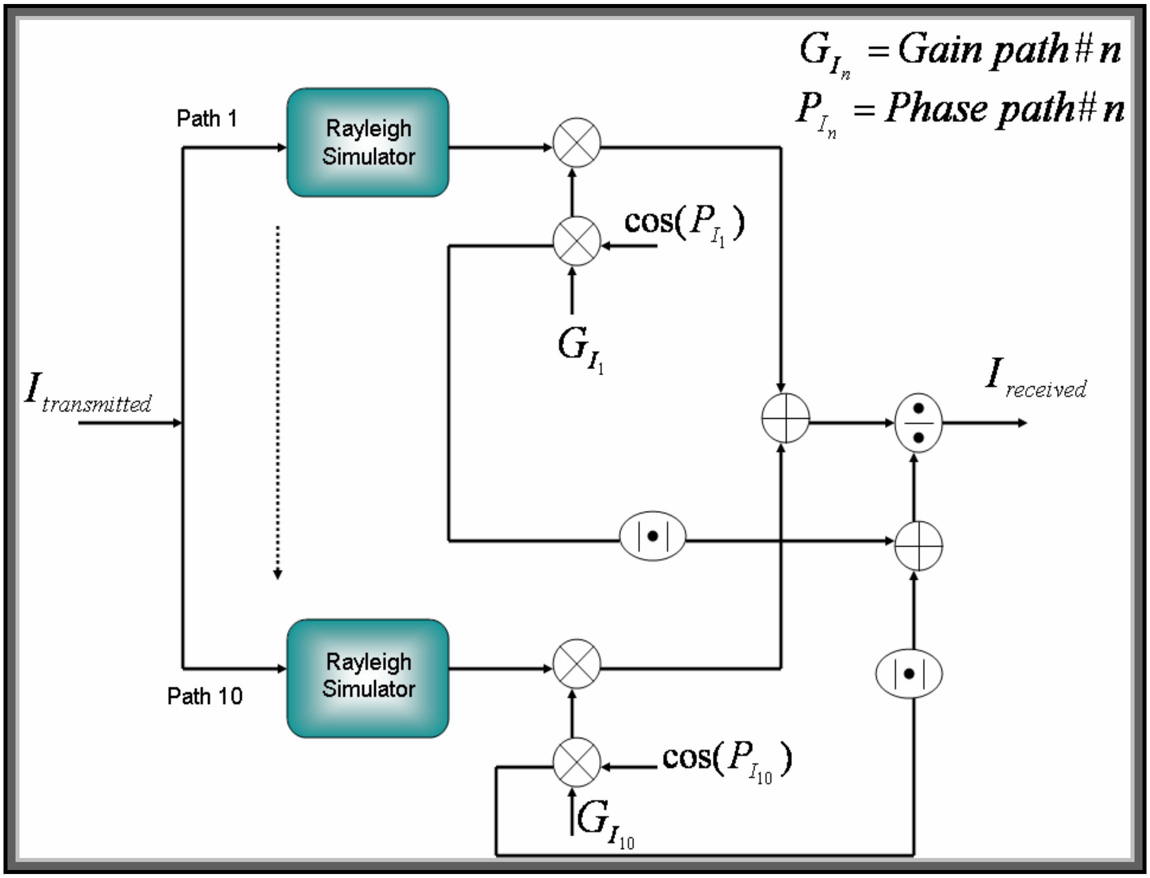


Figure 3.12 - Channel Path Simulator

situation, all ten faded path are created in a similar way. The first step is to pass the transmitted signal through the Rayleigh simulator depicted in Figure 3.8. This results in a path consisting of values greater than zero, showing that the path is only increased or decreased in amplitude and has not been negated in anyway. The Rayleigh faded signal is then scaled by a factor of both the path-gain and the path-phase. The path-gain will have a value between zero and one, therefore the signal is not losing any information and only the amplitude is decreased. The path-phase on the other hand can have a value between one and negative one, lending the possibility for information to be taken away from the overall signal. After each path is scaled to the properties calculated from Wireless Insite, the ten paths are summed together and divided by the total energy contained within the signal. The total energy comes from the multiplication of the path-gain and path-phase. Since some of the values could be negative, the absolute value of multiplication is needed because energy can only have a positive value, even though the effect of a negative signal is that it takes information away from the signal, the energy contained within the signal must be added to the overall signal.

For the LOS case within the site-specific channel model, the only variance from the NLOS model shown in Figure 3.12 is that instead of the first path being Rayleigh faded, the block is passed over. The Rayleigh simulator is not present because the LOS path is not faded because of the absence of scatterers in its path. This phenomenon is the cause of the difference between Ricean and Rayleigh fading for the LOS and NLOS cases.

3.6.3 Chip Rate

In order to make the interference as realistic as possible, the chip rate had to be considered when combining the three different protocols. This is because Zigbee has a chip rate of 2 Mchips/s, Wifi a chip rate of 11 Mchips/s, and Bluetooth has a chip rate of 1 Mchips/s. The relative chip rates of the three protocols are modeled in Figure 3.13 and their respective overlaps. This means that if Zigbee is considered to be the intended signal, then during one second, two million Zigbee chips will be sent, eleven million Wifi chips and only one million Bluetooth chips. This corresponds to during one Zigbee chip, five and a half Wifi chips will be sent while only half of a Bluetooth chip will have been transmitted. To combat this, the following courses of action are taken. It is fairly straightforward to account for the Bluetooth interferer, since only half of a chip is causing interference, this means that the other half of the chip would be occurring during the next chip, meaning that if the Bluetooth signal is stretched by a factor of two, then the two signal would match up perfectly. All that is needed is to spread the Bluetooth signal by copying each chip. The Wifi interferer is a little more troublesome, instead of trying to combine only five and a half chips together, as long as Zigbee is sampled at an even rate, meaning the number of samples per chip is an even number then eleven Wifi chips could be combined and averaged allowing that number to be added to two of the Zigbee chips. This means that for two Zigbee chips being sent, eleven Wifi chips would also be sent. The interference caused by the Wifi signal is therefore the average value of the Wifi signal over those eleven chips. This average value is added to the intended Zigbee signal that is sent. The effect of the interfering signal will depend on its power level and the resistance of Zigbee to the interference through its spread spectrum system.

To conduct the Wifi interference as it pertains to the signals chip rates, the signals are manipulated in much the same way as for Zigbee. This time Bluetooth is spread to cover a value of eleven chips, so that instead of one chip being sampled once, it was sampled a total of eleven times, with this being proportional to the number of samples per chip specified in the Wifi

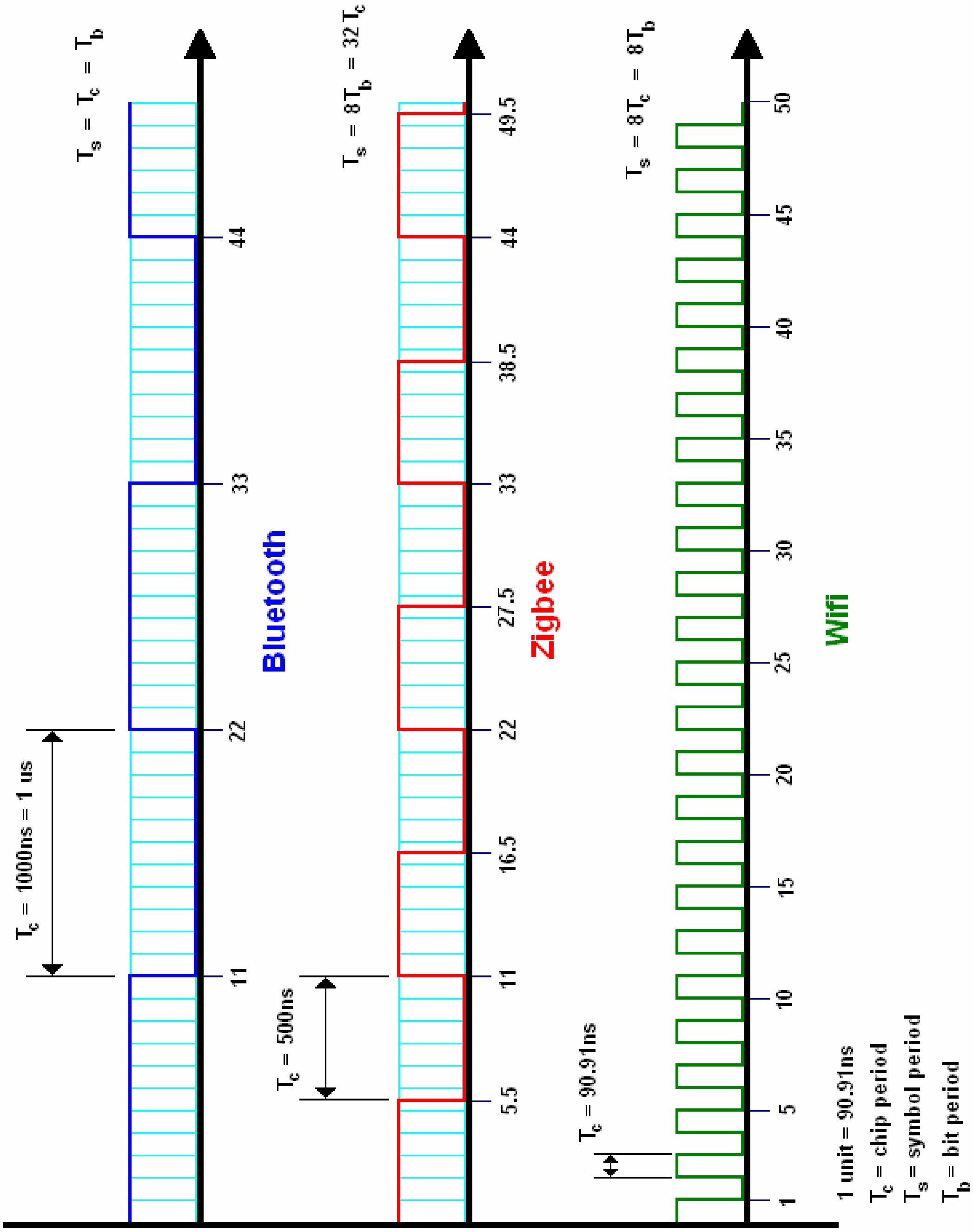


Figure 3.13 - Chip Cycles

program, typically 2 samples per chip. Meaning one Bluetooth chip will be sampled 22 times. Zigbee creates a problem because two is not a factor of eleven. Therefore each sample of a Zigbee chip is spread to cover 11 chips, but again this means that Wifi will have to have an even number of samples per chip so that when combined, 11 Zigbee chips will affect the 2 Wifi chips, which is the correct proportion.

Perhaps the only straightforward interference model can be found in Bluetooth, in which Zigbee will be summed over two chips and Wifi summed over eleven chips then averaged and added to the Bluetooth signal. The only other interferer to account for in these simulations were the transmitters for when the interferer was of the same type as the intended signal, therefore no chip rate modifications were needed to be applied to the signal since they were assumed to be at the same chip rate, the signals were already matched.

3.6.2 Bandwidth

The second means in which the models must be manipulated in order to better model actual interference deals with bandwidth and just how much of a signal can be considered to interfere within the same amount of space as the intended signal. In the ISM band there is a total of 83.5 MHz of bandwidth; of that space, Zigbee occupies sixteen 5 MHz channels, Wifi occupies three non-overlapping 22 MHz wide channels, and Bluetooth uses 79 channels each with a bandwidth of 1 MHz. The total 83.5 MHz along with the channel assignments for Zigbee, Bluetooth, and Wifi can be found in Figure 3.14.

Starting again with the Zigbee model, assuming that each signal occupies only 2 MHz in the 5 MHz channel, then if a Bluetooth signal was introduced which occupied only 1 MHz, then within the 80 MHz range there would be a 2/80 or 1/40 chance that the Bluetooth signal would fall into the same given bandwidth as Zigbee. So on average the Bluetooth would interfere a total of one in forty hops, allowing the equivalent Bluetooth signal to be scaled down by a factor of forty. The same goes for the Wifi signal, on average the Wifi signal will occupy approximately a fourth of the allotted bandwidth, and would interfere with the Zigbee signal on average a fourth of the time. This means that on average the Wifi signal could be scaled back by a factor of four before being added to the Zigbee signal. Finally, the Zigbee interferer must also be modified. Since Zigbee has 16 channels, there is a one in sixteen chance that the interferer will be located on the same channel as the intended Zigbee signal; therefore Zigbee can be scaled by a factor of sixteen.

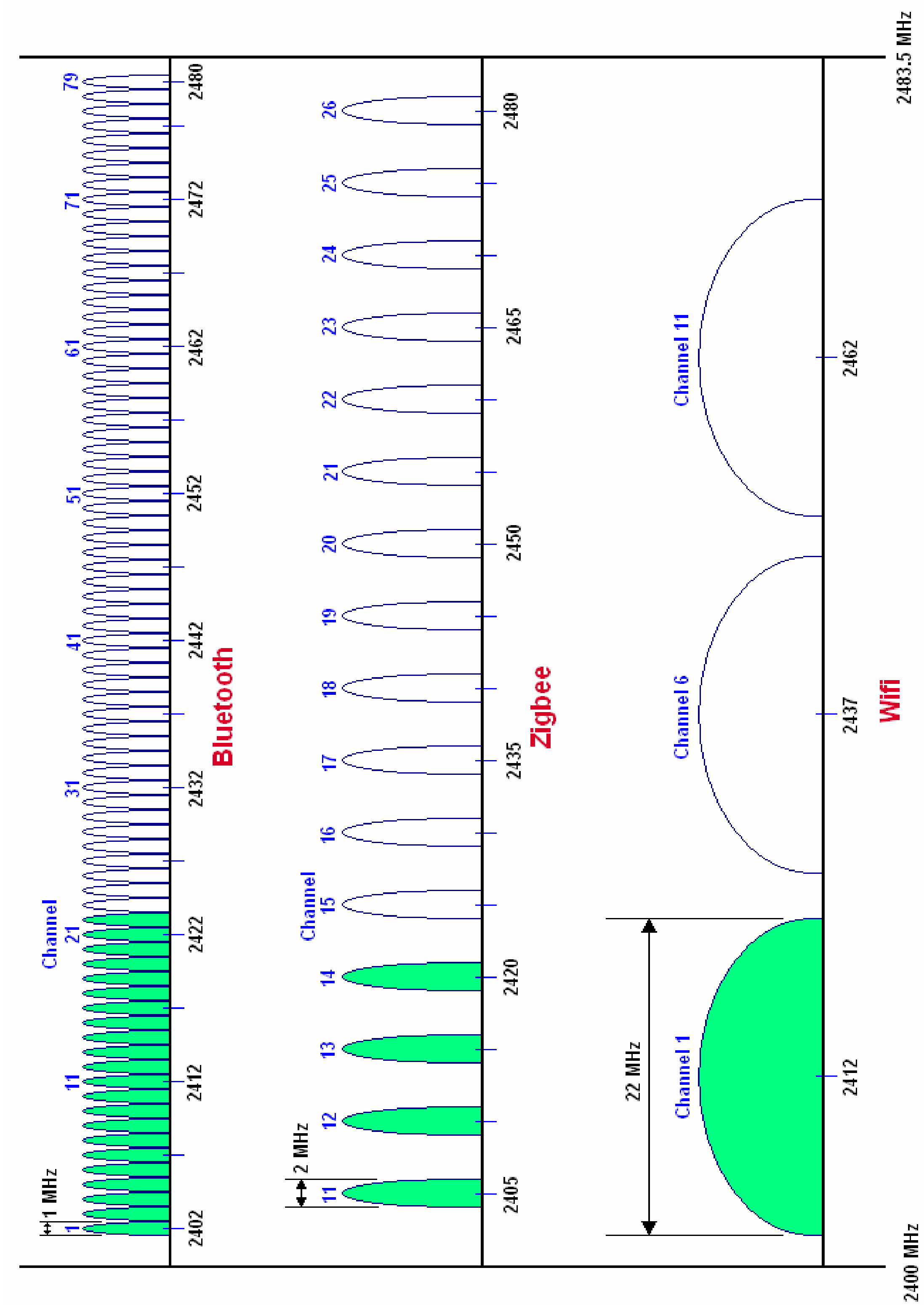


Figure 3.14 - Channel Assignments

The same manipulations to the interferers for the other two models can be applied as was done for the Zigbee model. For instance the Wifi signal would receive interference a fourth of the time from the Zigbee signal and a third of the time from the other Wifi interfering signal. Since Wifi covers 22 MHz, Bluetooth would interfere approximately twenty-two times within its 79 hop sequence, allowing for on average roughly a scale factor of 22/80 to be multiplied by the Bluetooth interferer. The case for the Bluetooth model can be derived in a similar way, the Wifi would need to be scaled down by a factor of 22/80, the Zigbee interferer by a factor of 1/40, and the Bluetooth interfering signal, assuming they are not on the same hopping sequence, would interfere approximately one in eighty times. Now that the two main modifications have been made, accounting for both the chip rate and bandwidths of the signals, the interference models are complete.

The results obtained within Chapters 4 and 5 are only valid for the above assumptions and may contradict with results from previous coexistence studies. This is because the assumptions intend to take the performance of the system as a whole rather than on a case-by-case basis. The case-by-case basis would involve simulating the performance when two devices are located within the same channel bandwidth. Even when trying to simulate this case, both devices will not always be transmitting at the same time, consequently, these results would only be valid under a different set of assumptions, unless a more complex system was developed.

The system being modeled considers on-average interference. Bluetooth is inherently a burst error interferer, meaning that Bluetooth will cause a block of errors when the interferer is located on the same channel as the system and as Bluetooth hops to another channel, the system will not detect any errors. Over a short time window, the errors are dependent upon whether the interferer is co-channel located, but as the reference window is expanded, there will still be burst errors, but over time a statistical average can be taken. This average is modeled as causing errors over the entire range of frequencies, rather than only during certain channels. The same averaging is done to the DSSS systems for both Zigbee and Wifi. The devices will only interferer with each other when they are located within the same channel space; this is because the bandpass filter on the front-end of the receiver will reject the out-of-band frequencies not within the receiving channel. When considering a device with an interferer which may or may not be located within the same channel bandwidth, the effects of the interference is averaged over a substantial time period, thus the effects can be modeled as a statistical average affecting the interferers signal amplitude.

Chapter 4

General Channel Models

4.0 Results

Simulations were performed for the three interference models, one for each protocol, using different parameters and under separate conditions. The first case is to carry out the simulations with a general AWGN channel. This entails varying both the signal's SNR and its SIR (signal-to-interference ratio). Each protocol will produce three separate Bit Error Rate (BER) plots, one for each interferer. This case will aid in determining what the signal's average power range would need to be in order for the receiver to be able to detect a usable signal. Before presenting the AWGN channels results, the coding gain found within both Zigbee and Wifi will be shown to illustrate why the theoretical curves for both QPSK and DQPSK modulation are different than the curves for Zigbee and Wifi respectively.

The second section of the results will take the AWGN system models and incorporate the Rayleigh fading model. The same resulting BER plots will be determined as before for the pure AWGN case. The fading plots will be constructed through a single pulse Rayleigh fading simulator which then creates flat slow fading signals for both the desired signal and for the power of the interferer, unlike the results in Chapter 5 which are obtained by using 10 faded paths.

4.1 Coding Gain

Zigbee and Wifi both incorporate spreading techniques with intrinsic coding gains. This is separate from the processing gains found within DSSS systems. The coding gain helps to combat the effects of a noisy environment, whereas processing gain is used to minimize the effects of interference. Therefore, in the AWGN channel, the coding gain can be found from the performance of the system against the theoretical probability of error for a given modulation technique. The processing gain however, does not change the performance in an AWGN channel because the noise is proportional to the number of chips per bit, as the code is spread by higher factors; the noise variance is also increased. Figure 4.1 shows the performance of Zigbee versus QPSK modulation and Wifi versus DQPSK modulation; the performance of the two protocols results in a decrease in BER from the theoretical calculation. This exhibits the effects that coding gain has on the overall system. The improvement for Zigbee is calculated as 2.5dB at a BER of 10^{-5}, illustrating that the performance of Zigbee at 10^{-5} is approximately 2.5dB better than a QPSK system. At the same 10^{-5} threshold, Wifi has an SNR that is 1dB less than that of DQPSK for the same BER; therefore, CCK incorporates 1dB of coding gain into Wifi.

Since the establishment of Zigbee, the FCC has suspended the 10dB requirement of processing gain for devices operating within the 2.4 GHz ISM band. Processing gain is defined as the chip rate divided by the data or bit rate. The Zigbee signal is spread by a factor of 8, going from four information bits to 32 chips, resulting in a processing gain of 9dB. The CCK characteristics of Wifi inflict an 11dB total processing gain.[29][30] Bluetooth on the other hand does not contain any spreading of the signal, it is a completely narrowband signal. So from an instantaneous standpoint, Bluetooth has 0dB processing gain, but if taken statistically over an entire set of hopping sequences, the effects of one particular channel will not be considered for any of the other 78 channels. This results in a processing gain, which can be thought of as a hopping gain, of 19dB.

4.2 Interference over an AWGN Channel

The results for the AWGN channel will be presented with the Zigbee protocol being the first to be subjected to the interferers. The interferers will be introduced individually, starting with the Bluetooth interferer, then a Wifi interferer, and ending with a Zigbee device being interfered with by another Zigbee device. The resulting BER curves for the other two protocols, Wifi followed by Bluetooth will be introduced to interferers in the same order as was done for Zigbee.

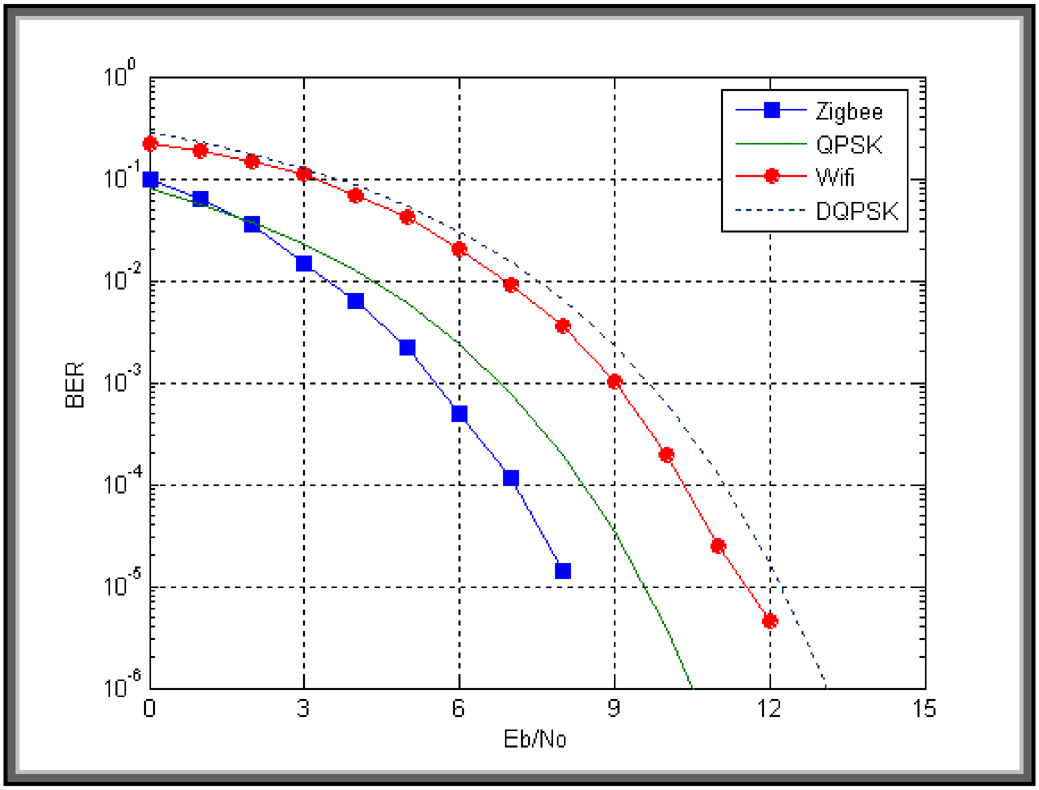


Figure 4.1 - Coding Gain for Zigbee and Wifi

4.2.1 Zigbee

The first model simulated is the Zigbee model, and the first interferer to be considered as a Bluetooth interferer. The results of this simulation can be found in Figure 4.2. It can be seen that for values greater than -16.75dB, meaning that the Zigbee signal is 16.75dB below the Bluetooth signal, the system appears to be interference limited. This causes the BER curve to flatten out and the probability of an error will never decrease. For values of SIR greater than -16.5dB, the system turns into a noise limited system, meaning that as the SNR increases the systems probability of error will decrease and approach zero. This means that the noise is what is hurting the system, the interfering signal level is low enough that it does not affect the system as much when the SIR increases. To maintain a BER of at least 10^{-3}, the SNR must be above 20dB and the interfering signal cannot have a value greater than 16.75dB above the Zigbee signal power. To maintain results typical of a system with no interferers, such as the AWGN case, Zigbee's SIR power cannot be lower than 10dB.

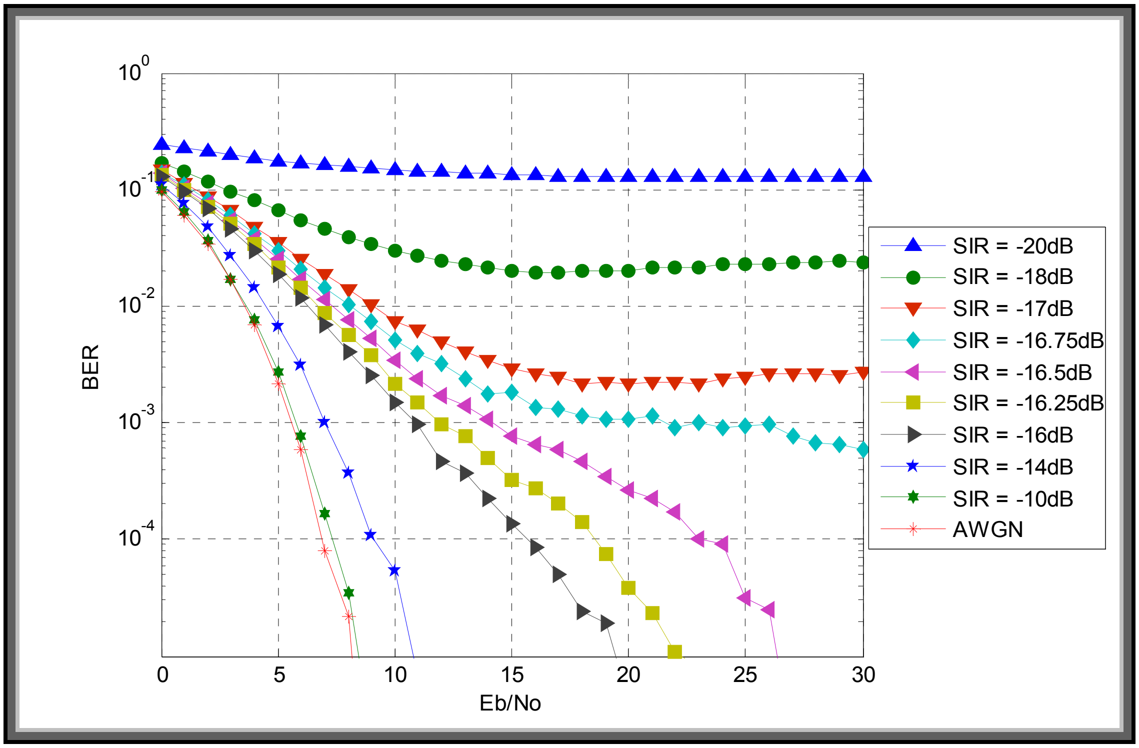


Figure 4.2 – Zigbee Signal with a Bluetooth Interferer – AWGN Channel

The next case considered is when a Wifi interferer replaces the Bluetooth interferer. These results can be found in Figure 4.3. This case with a Wifi interferer appears to be more interference limited than was the previous case, since there is a distinct interference limited level at least down to a probability of error of 10^{-5}. The SIR at this point is -10.5dB, if the Wifi power level is any greater than 10.5dB above the Zigbee signal power, the BER will flatten out at a probability of error greater than 10^{-5}. In order to achieve a noise limited system with a BER less than this, the SIR must be greater than -10.5dB. The model does not achieve AWGN type results until the SIR is at least -5dB, which is when the interference does not affect the signal when compared to the noise.

The third and final scenario for the Zigbee signal is when a second Zigbee signal interferes with the first. If the two devices are located on the same network, then the Zigbee MAC layer would thwart the interference through a listen-before-talk system known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), but assuming the two devices were not part of the same network and had CSMA/CA turned off, then the results of Figure 4.4 would be obtained when sent through an AWGN channel. Unlike the previous two examples, when a Zigbee

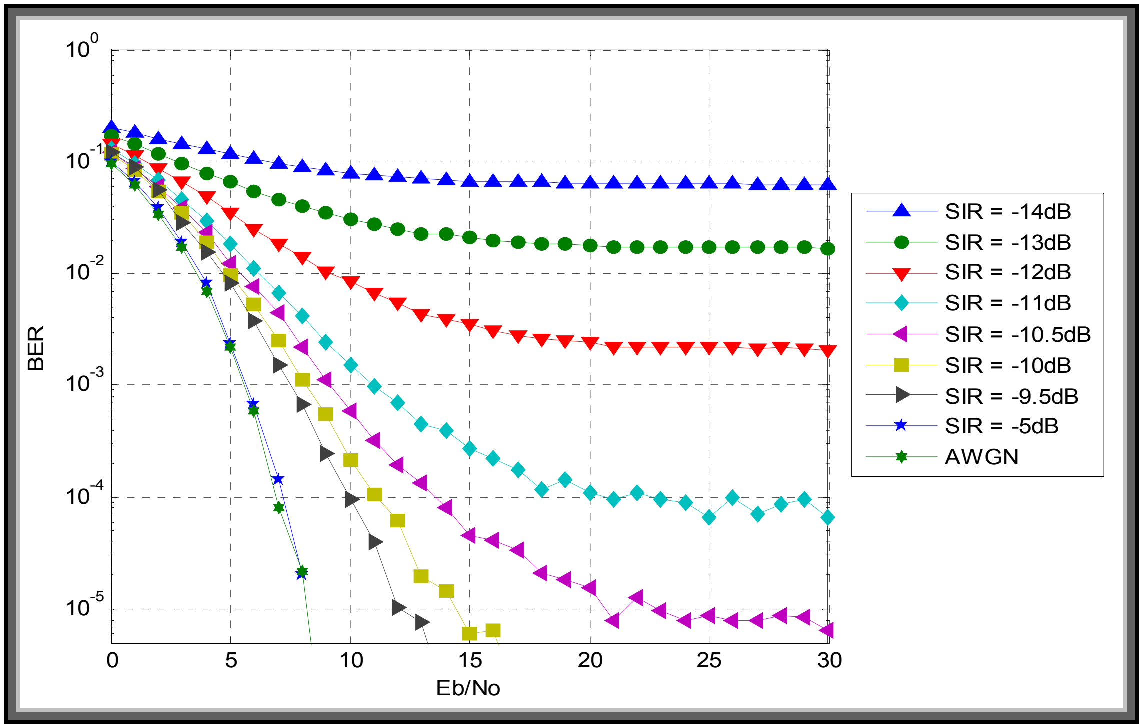


Figure 4.3 – Zigbee Signal with a Wifi Interferer – AWGN Channel

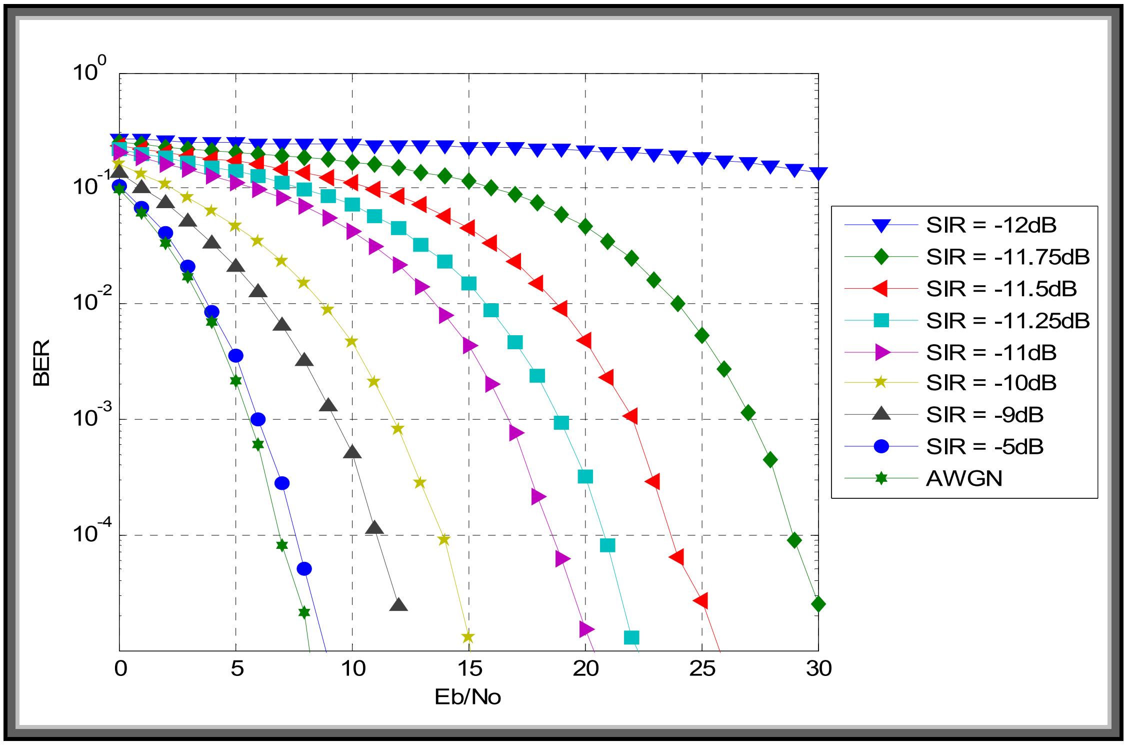


Figure 4.4 – Zigbee Signal with a Zigbee Interferer – AWGN Channel

interferer is introduced to the Zigbee signal the result is no longer an interference limited system, it becomes a noise limited system until the interference completely overwhelms the intended signal. The system doesn't level off at a given probability like the previous two cases, either the system's BER will approach zero errors as the SNR increases or else it hovers near 10^{-1}, which occurs when the SIR falls below -12dB. The BER curve then moves decreases approaching the AWGN situation, which occurs when the SIR is above -5dB.

4.2.2 Wifi

The next simulation is the Wifi model through an AWGN channel to help determine what types of SIR values can be tolerated within this system for the three different types of interferers. Starting with Bluetooth as the initial interferer, the results will be examined in Figure 4.5. Much like when the Zigbee signal was interfered with by another Zigbee signal, it appears that Figure 4.5 is also only noise limited up to the point that an interfering signal completely cancels out the intended Wifi signal. The signal is completely destroyed with an SIR of -6dB, the BER rapidly improves and approaches the AWGN case as the SIR becomes 0dB, this improvement slows after it reaches 0dB and does not fully reach the AWGN case until the power of the interferer is more than 5dB below that of the intended Wifi signal.

To introduce the interferers in the same order as for the scenario when Zigbee was the intended signal, the results of the case where a Wifi signal is interfering with another Wifi signal can be found in Figure 4.6. Just like Zigbee, this can only happen when both devices are located on separate networks and even then, Wifi uses a CSMA/CA system to avoid causing interference between Wifi devices. The figure is almost a mirror image of the case when a Bluetooth interferer was considered. It appears to be noise limited up to the point where the interference completely floods the intended signal. For this case, the signal is completely overtaken when the SIR is less than -5dB, and the BER improves rapidly until it reaches 0dB, and then continues to improve slowly until 5dB where it is approximately equal to the AWGN case where no interference is included.

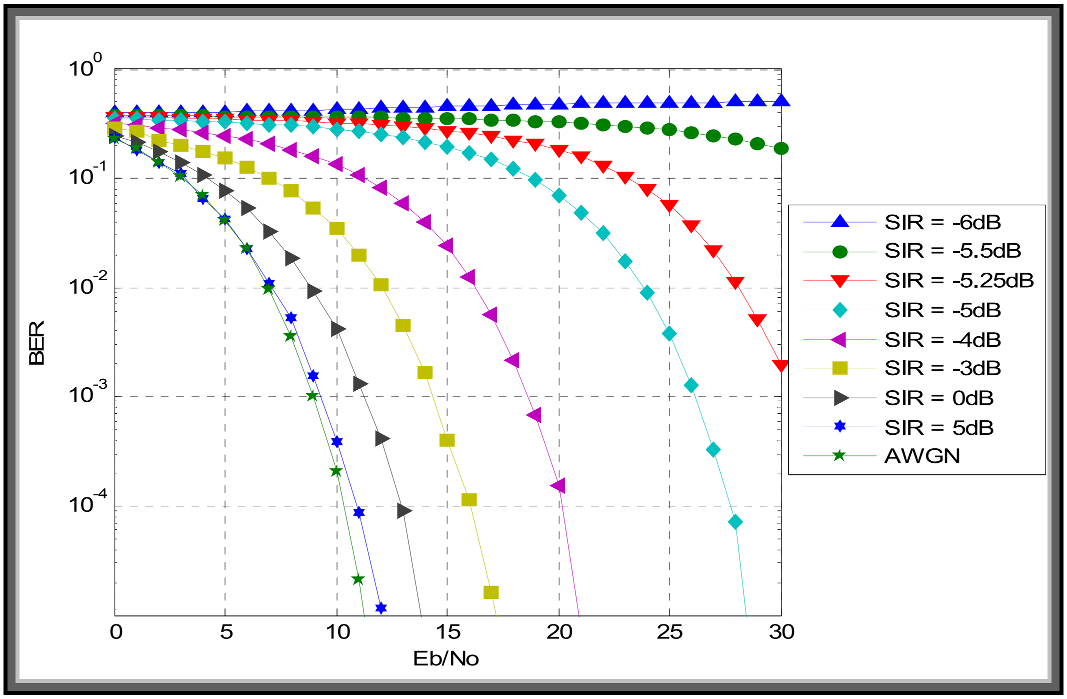


Figure 4.5 – Wifi Signal with a Bluetooth Interferer – AWGN Channel

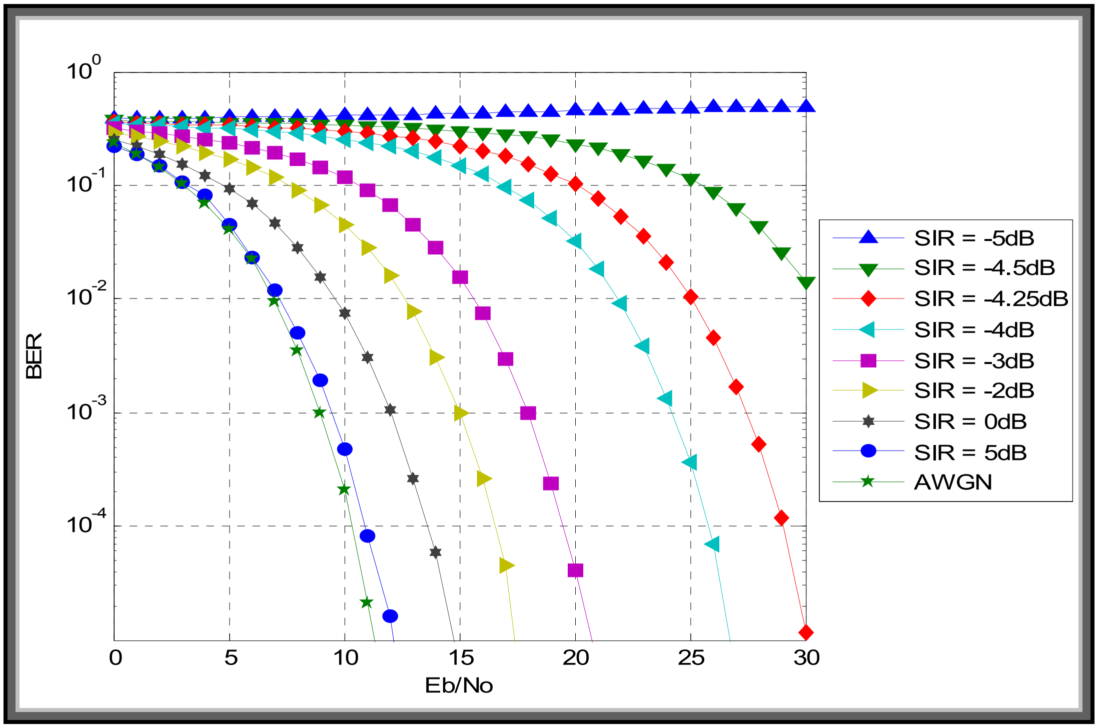


Figure 4.6 - Wifi Signal with a Wifi Interferer - AWGN Channel

The last interferer to be implemented with a Wifi signal is the Zigbee Interferer. In Figure 4.7 it can be seen that the figure is very close to being a replica of the previous figure, incorporating even the same values of SIR. The threshold for not being able to boost the SNR so that a signal can be detected is when the SIR is less than -5dB, for all values of SIR above that, the system is noise limited. Much like the previous example, the BER improves rapidly from an SIR of -5dB to 0dB and then the improvement slows until 5dB where it reaches the AWGN curve. Wifi appears to be able to resist the effects of interference better than Zigbee, meaning that the system never really becomes interference limited, but Wifi cannot tolerate a value of SIR as high as Zigbee, due to the coding gain of Zigbee.

4.2.3 Bluetooth

The last simulated protocol is the Bluetooth model which will help to see the effects that an interfering signal has on an FH-SS system. From Figure 4.8, it can be seen that the effects are very similar to the previous two systems, with the exception that it has more resilience to interference than does Wifi. Figure 4.8 shows the effects of a Bluetooth signal with a Bluetooth interferer. For this scenario, the system is noise limited for values of SIR above -19dB. The effects of the interferer are diminished once the value of the interferer is less than 8dB greater than the signal's power. There is an extreme improvement in the BER over this 11dB range, where it sharply falls off until it reaches -15dB, and then the improvement starts to slow down.

When a Wifi interferer is placed with the Bluetooth signal, the results more resemble the interference limited systems that are found with Zigbee. The BER values level off for different values of a given SIR values as can be seen in Figure 4.9. When the Bluetooth signal is more than 10dB below the interfering Wifi's signal power, the Bluetooth signal is unrecoverable. To obtain a probability of error of at least 10^{-3}, for SNR values greater than 20dB, then an SIR value greater than -6.5dB must be used. In order for the BER to be less than 10^{-5} with an SNR of at least 20dB, the signal can be no more than 5.5dB below the interfering Wifi's signal power. Once the SIR reaches the 0dB threshold, the interference no longer affects the signal and only the noise is a factor in causing errors within the system, due to the fact that the system changes from interference limited to noise limited near an SIR of -5dB.

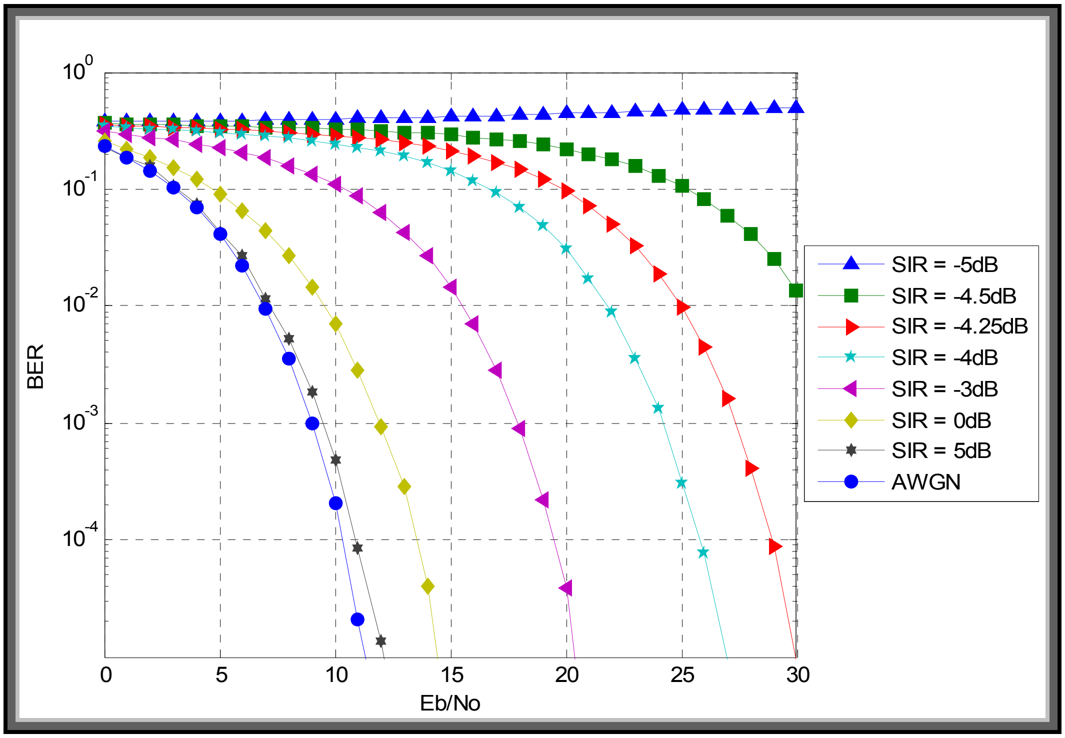


Figure 4.7 – Wifi Signal with a Zigbee Interferer – AWGN Channel

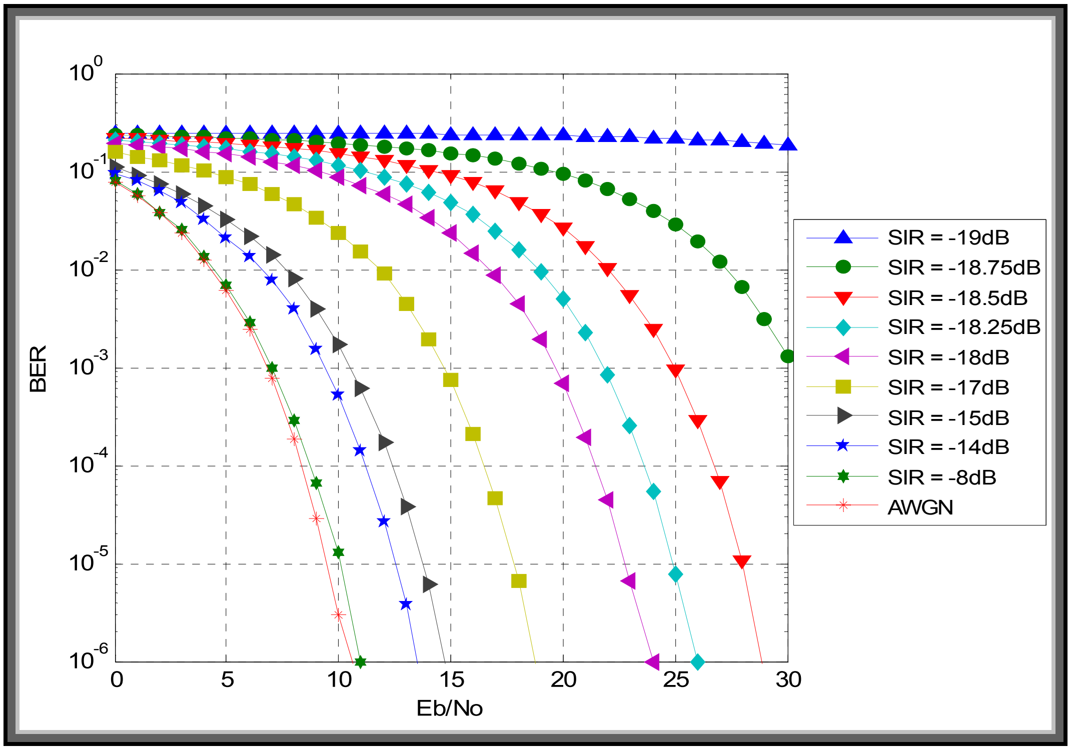


Figure 4.8 – Bluetooth Signal with a Bluetooth Interferer – AWGN Channel

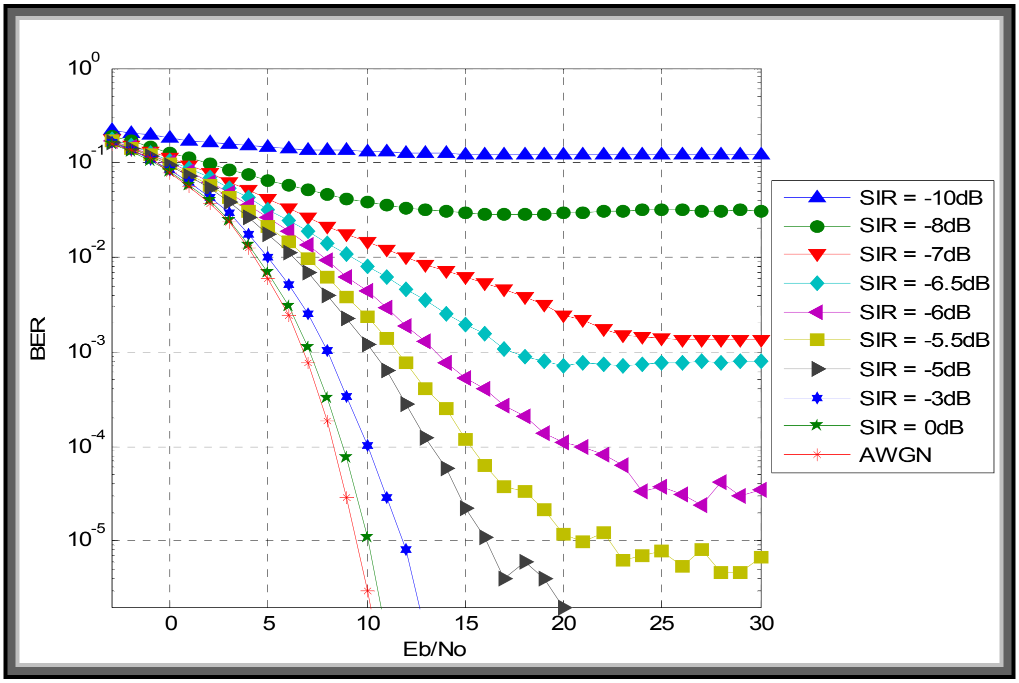


Figure 4.9 – Bluetooth Signal with a Wifi Interferer – AWGN Channel

The final AWGN channel scenario to be simulated is the Bluetooth signal with a Zigbee interferer. Much like the Bluetooth signal with a Bluetooth interferer, this scenario also appears to be noise limited. In Figure 4.10 it can be seen that if the SIR is less than -16dB, the interference drowns out the signal, while if the SIR is greater than -16dB then the system will approach zero errors as the SNR is increased. The performance rapidly changes from having an unrecognizable signal at -16dB to having a BER less than 10^{-3} at an SNR value of 25dB for an SIR value of -15.5dB. The performance continues to rapidly increase towards the AWGN case and the interfering signal no longer affects the signal for values of SIR greater than -5dB.

4.2.4 AWGN Conclusion

Even though the obtained results are only theoretical, especially when assuming a channel comprised solely of noise and no fading, the results are a good indicator of the type of performance than can be expected. From the results, Zigbee and Bluetooth appear to be protocols, which can survive in an environment in which they are not the dominant device, this is

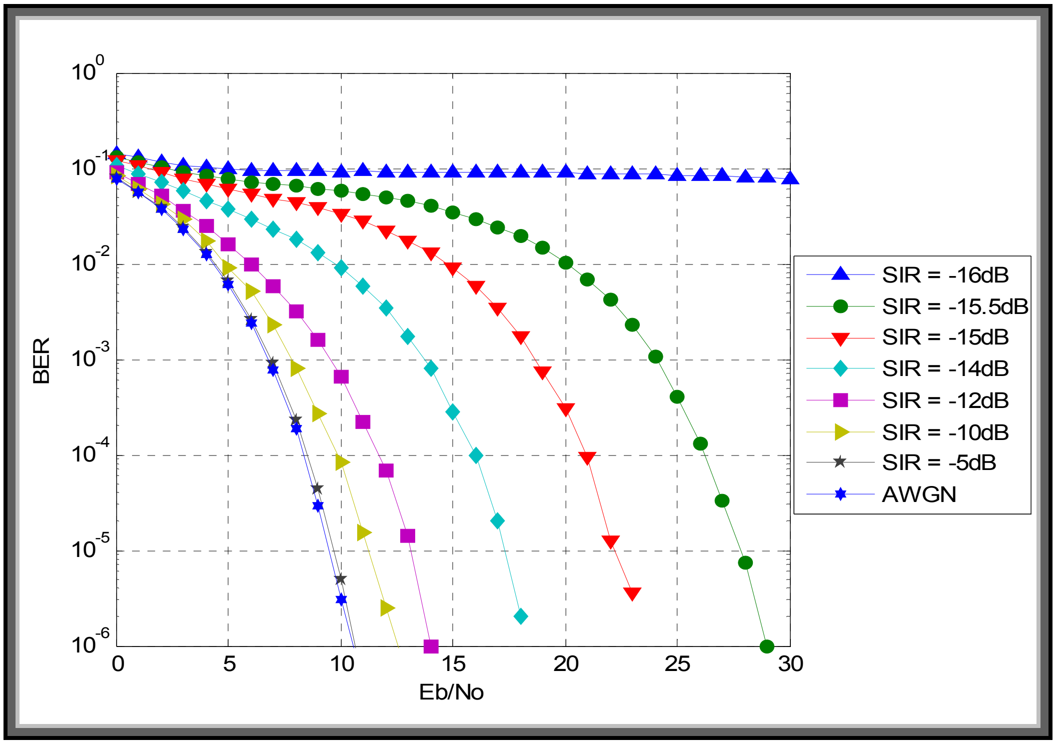


Figure 4.10 – Bluetooth Signal with a Zigbee Interferer – AWGN Channel

due to the fact that they are able to completely disregard interferers with a power level, which is at least 5dB above their own power level, with the exception of Bluetooth with a Wifi interferer where the power levels must be equal. These devices can still tolerate an interferer when the SIR is less than -10dB, however, the Bluetooth with a Wifi interferer can only tolerate an SIR of -6.5dB. Here a signal being able to tolerate an interferer means that in the presence of the interferer, the signal can still reach a BER of at least 10^{-3} at an SNR of 20dB.

The effects of interference on Wifi differ from those obtained for Bluetooth and Wifi, the main difference is that Wifi cannot function at full capacity when an interferer is present with a power level higher than that of Wifi. In order for Wifi to completely ignore the effects of the interferers, Wifi must have an SIR of 5dB. On the other hand, Wifi can tolerate interferers, which have higher power levels, up to 3dB higher than the Wifi signal. This is why Wifi needs to transmitted at such a higher power level than both Bluetooth and Zigbee. A second difference between Wifi and the other protocols is that Wifi is affected in the same way no matter which interfering protocol is present. The performance of Zigbee and Bluetooth fluctuates from interferer to interferer.

4.3 Interference over a Rayleigh Flat Faded Channel

In order to better understand whether or not the three different protocols can coexist with each other and with what power levels of interference they can tolerate, more has to be considered then just a simple AWGN channel. Within a real world environment the signal will experience some sort of fading. The fading is typically modeled as having a Rayleigh distribution. To simulate this situation, a general Rayleigh fading path will be considered for both the signal and the interferer. Since these will only consist of a single path, the incurred fading will be flat fading where the signal amplitude is only affected and the signal itself is not distorted. The results will be presented exactly as they were for the AWGN scenarios, beginning with Zigbee and ending with Bluetooth, and all of the results appear to represent interference limited systems and the probabilities of error will be flat for a certain range of SIR values.

4.3.1 Zigbee

The first case considered for Zigbee is when there was a Bluetooth interferer. Figure 4.11 provides the BER results for the varying SIR values. There has been a 5dB to 10dB decrease in performance from the AWGN channel, which can be attributed to the Rayleigh flat fading. The system does not perform like a system without a Bluetooth interferer until the SIR ratio is 0dB. To maintain a probability of errors below 10^{-3} for an SNR value 20, the SIR ratio must now be above -10dB. The signal becomes unusable for values of SIR below -15dB.

The second fading example for the case of a Zigbee signal involves the use of a Wifi interferer. Similar to the previous plot, Figure 4.12 also depicts an interference limited system since the BER flattens out to a certain probability rather than approaching zero. This time the degradation in performance from the AWGN case only drops by a value of 2dB. The signal now becomes clouded with interference for values less than -12dB whereas before this took place at -14dB. The system also performs as if no interferers were present at -3dB, an increase from -5dB. For this system, values of SIR need to be -7dB and -3dB to maintain BERs of less than 10^{-3} and 10^{-4} respectively, for values of SNR above 25dB. Since the line for when no interferers are present has approximately a constant slope, this shows that the system is flat fading. If it had been frequency selective fading then the plot would suffer in BER and have a downward curve to it.

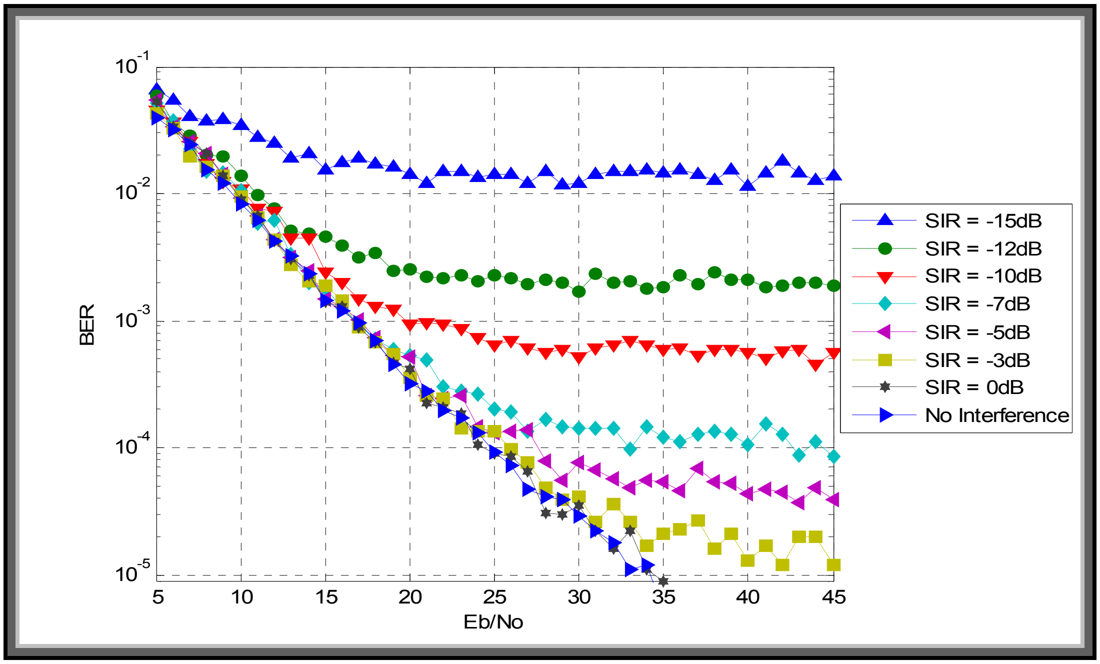


Figure 4.11 – Zigbee Signal with a Bluetooth Interferer – Rayleigh Flat Fading

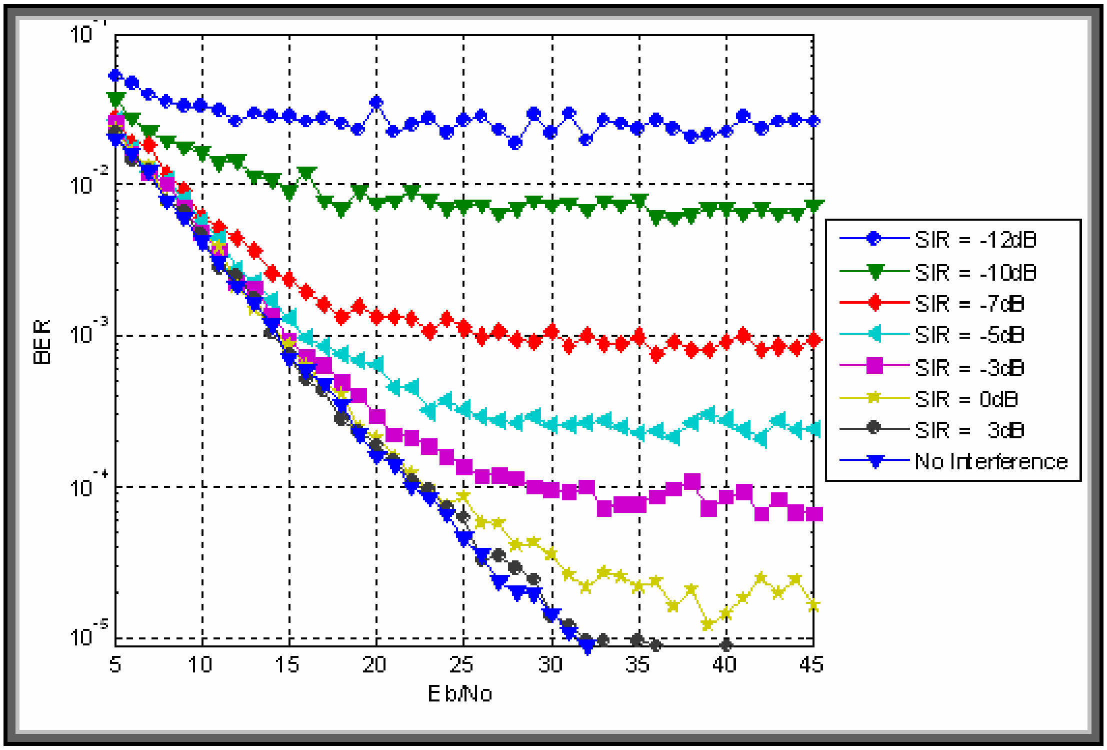


Figure 4.12 – Zigbee Signal with a Wifi Interferer – Rayleigh Flat Fading

Much like the previous two cases, when a Zigbee interferer is introduced to a Zigbee signal, the flat fading causes an increase in BER from the AWGN case. The results of Figure 4.13 demonstrate the effects of the Zigbee interferer. This time the increase in SIR is again between 5dB and 10dB. The system completely gives in to the interference at -7dB, unlike for the AWGN case where this takes place at -12dB. To maintain a BER below 10^{-3} for an SNR above 20 dB, an SIR of approximately -4dB must be used. The system does not completely block out the other Zigbee signal's interference until the intended signal has a signal power at least 5dB greater than the interferer, a change of 10dB from the previous case where it could be 5dB below the interfering signal's power.

4.3.2 Wifi

The simulations will now move to the Wifi system model and how well it performs when subjected to both a fading and AWGN environment along with interferers. The first interferer will again be Bluetooth and the results can be found in Figure 4.14. A significant difference can now be seen from the other cases in the fact that the SIR now must be a positive number meaning the signal power must now be greater than the interferer's power. A decrease of 6dB to 15dB in performance from the previous Wifi example with a Bluetooth interferer can be seen. When the signal and the interferer have equal signal power, the interferer dominates the signal, as the signal power increases to an SIR of 10dB, the probability of error hovers under 10^{-3} for SNR values above 35dB. It takes another 10dB increase in SIR before the signal can completely overcome the interfering signal and perform as if no interferers are present at 20dB.

The second interferer applied to the Wifi system is when a second Wifi signal is entered. From examination of Figure 4.15, it can be seen that the SIR falls between the same values as that of Figure 4.14, ranging from 0dB to 20dB. With 0dB referring to when the signal is completely distorted by the interferer, and 20dB correlating to when the interferer is completely dominated by the signal. Again, an SIR of at least 10dB must be achieved in order for a probability of error of 10^{-3} to be achieved with an SNR at least 35dB. From the scenario when only noise is considered and not fading, there is approximately 10dB of degradation in performance.

The final interferer to subject the Wifi model to is a Zigbee interfering signal. For the first AWGN case the SIR ranges from values of -5dB to 5dB for signals that are swamped by interferers, to signals that completely block the interfering Zigbee signal. By inspection of Figure 4.16, when

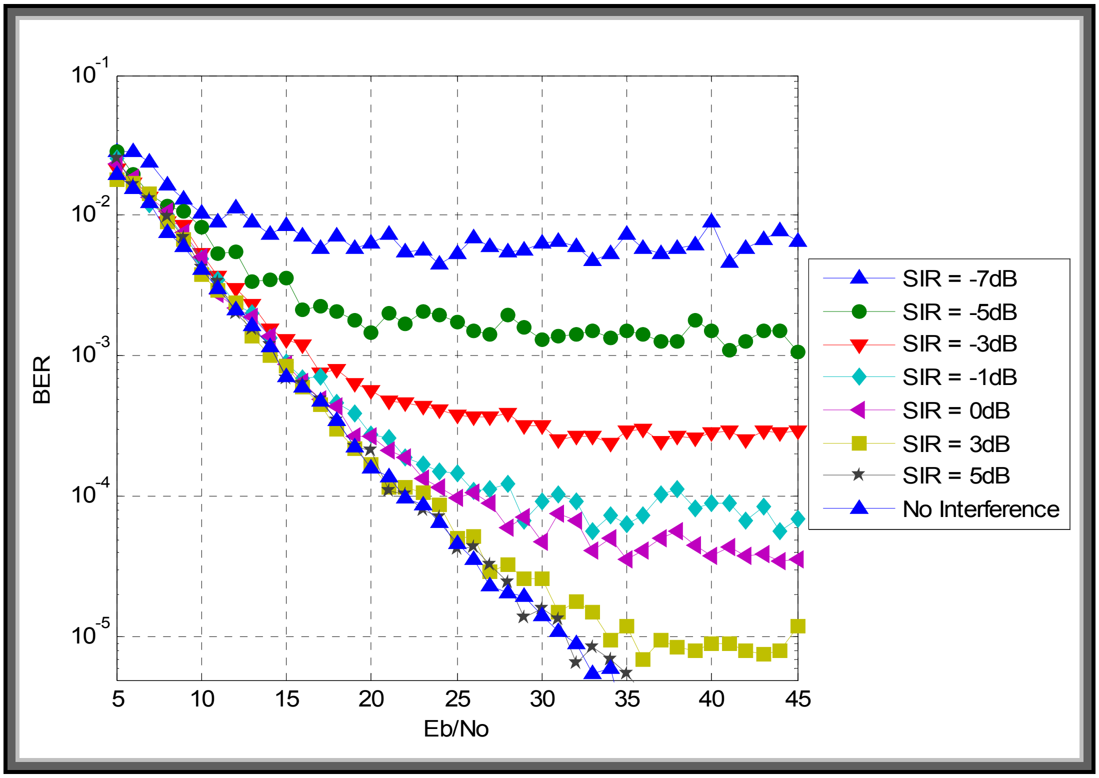


Figure 4.13 – Zigbee Signal with a Zigbee Interferer – Rayleigh Flat Fading

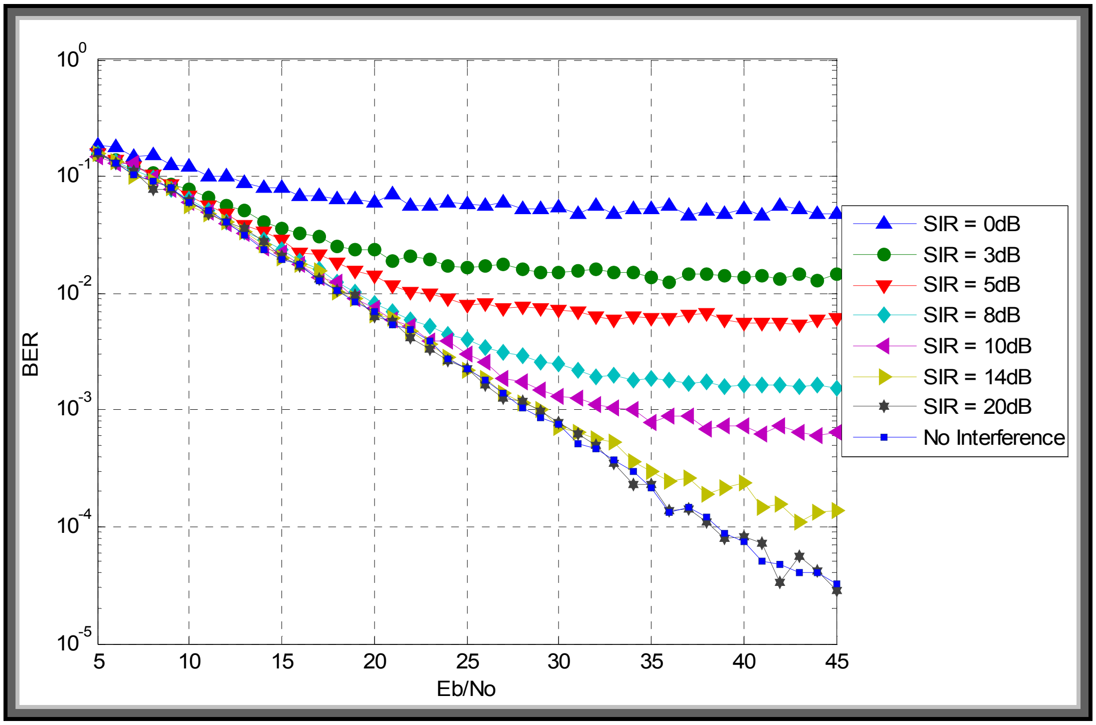


Figure 4.14 – Wifi Signal with a Bluetooth Interferer – Rayleigh Flat Fading

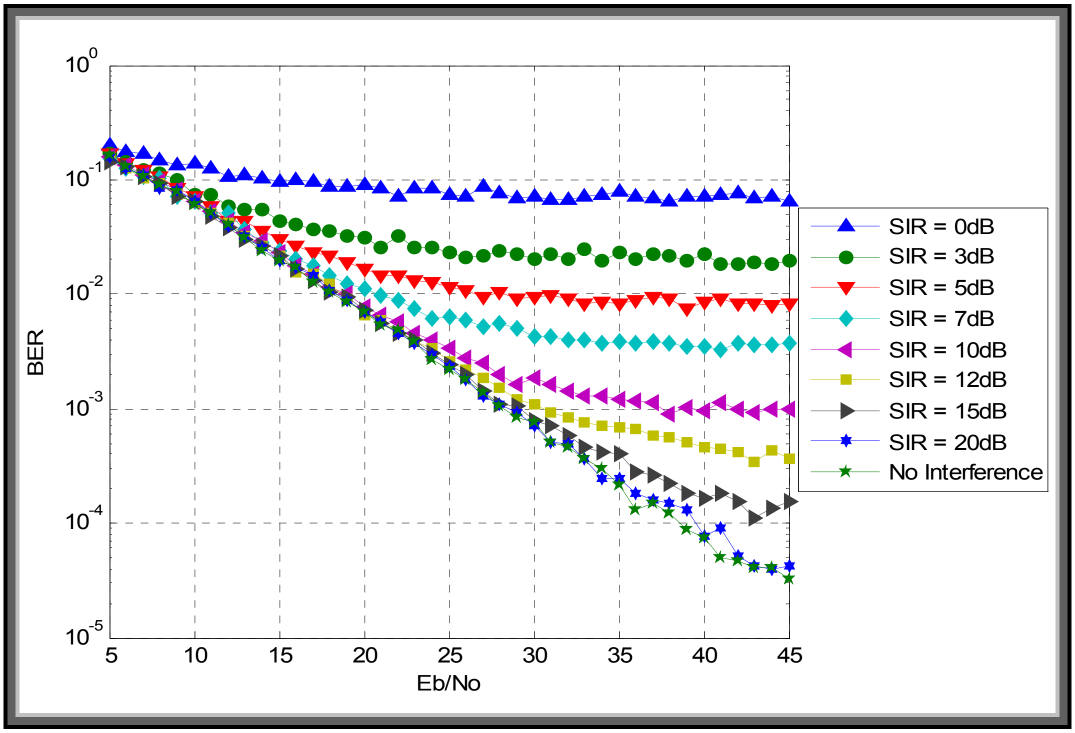


Figure 4.15 – Wifi Signal with a Wifi Interferer – Rayleigh Flat Fading

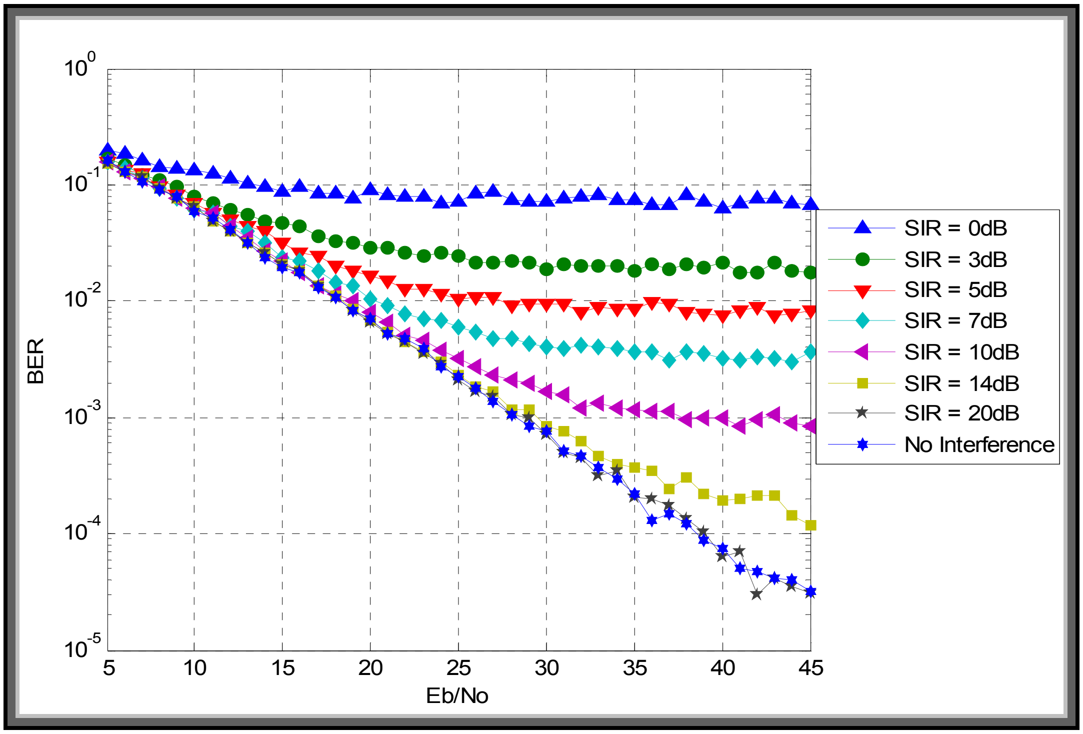


Figure 4.16 – Wifi Signal with a Zigbee Interferer – Rayleigh Flat Fading

including the effects of fading, the SIR must be increased to 20dB before it can thwart off the effects of the interferer. Similar to the two previous examples, the interfering signal overtakes the signal when the two signals have equal powers, and for the system to achieve a BER of 10^{-3} for values of SNR above 35dB, the SIR must be equal to or greater than 10dB. From the previous three figures, it appears that no matter what type of interfering signal is subjected to Wifi, the performance roughly stays the same.

4.3.3 Bluetooth

The final model in which fading needs to be considered for is Bluetooth. The three different cases all still experiencing flat fading and the performance of all three have been hindered by the addition of the fading to the AWGN channel. The Bluetooth interferer creates a range of values for SIR of 20dB from -15dB to 5dB in which the performance will change from no data being able to be extracted from the received signal to the signal performing as if no interference is involved at all. These results can be seen in Figure 4.17. From the graph it can be seen that for an SIR of -5dB the BER stays below 10^{-3} for values of SNR greater than 30dB.

When Bluetooth is combined with a Wifi interferer, the performance is considerably worse than when a Bluetooth interferer is considered. The value of SIR must be roughly 10dB higher to achieve the same performance. Also, the system suffers about a 5dB loss in signal power from the case where only an AWGN case is considered. By inspection of Figure 4.18 it can be seen that a Wifi signal completely saturates the Bluetooth signal for values of SIR less than -5dB while for SNR values greater than 25dB the system can sustain a BER of 10^{-3} as long as the Bluetooth signal is 3dB greater than the interfering Wifi signal. Bluetooth cannot block out the Wifi interferer until the SIR is at least 15dB.

The final fading case for the Bluetooth signal is when a Zigbee interferer is combined with it. For the AWGN only case, Bluetooth is fairly resilient of the Zigbee signal and is able to maintain a signal power 5dB below Zigbee's power level. The Bluetooth power level must increase to at least 5dB above the interfering signal of Zigbee, as demonstrated in Figure 4.19 on the following page. For Bluetooth to maintain the 10^{-3} BER for SNR values above 30dB, the SIR value must be in the neighborhood of -4dB. The Bluetooth signal does not become saturated with the Zigbee interfering signal until the signal falls to more than 12dB below the Zigbee signal.

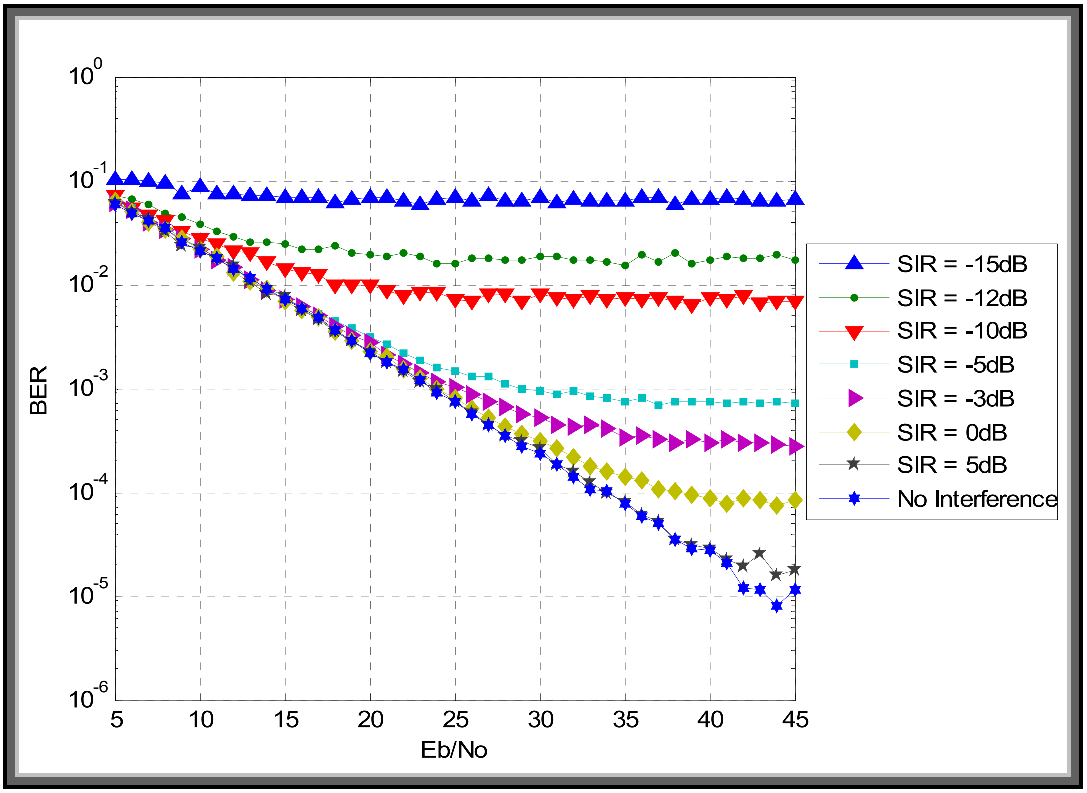


Figure 4.17 – Bluetooth Signal with a Bluetooth Interferer – Rayleigh Flat Fading

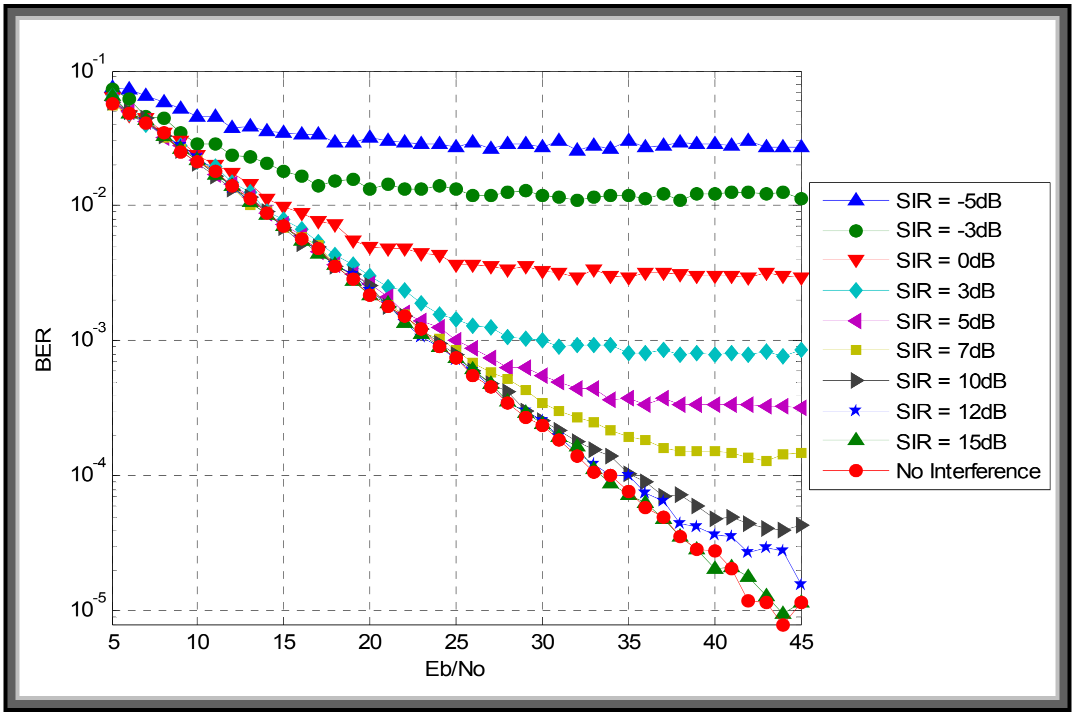


Figure 4.18 – Bluetooth Signal with a Wifi Interferer – Rayleigh Flat Fading

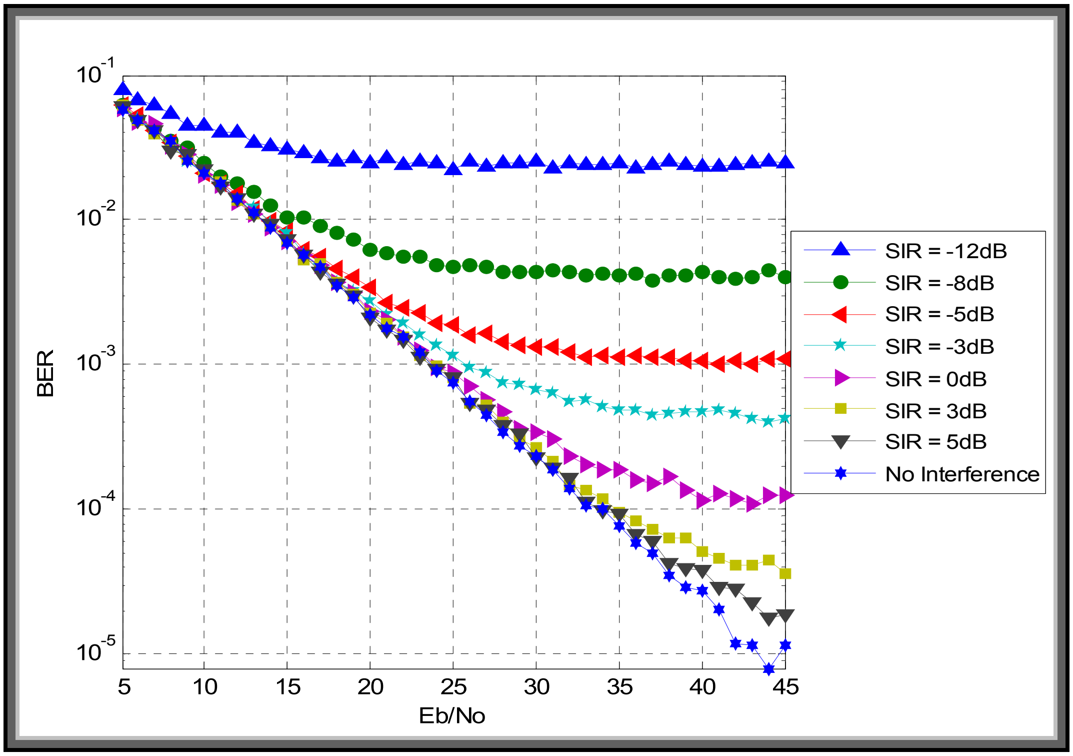


Figure 4.19 – Bluetooth Signal with a Zigbee Interferer – Rayleigh Flat Fading

4.3.4 Rayleigh Fading Conclusions

As expected the performance from the simulations incorporating Rayleigh fading are substantially lower than those incorporating only an AWGN channel. On average the effects of fading causes a 10dB to 15dB drop off in performance. Due to the 10dB to 15dB decrease, the level at which a signal can tolerate a signal has been extended out to now needed to be at least 10^{-3} at an SNR of 30dB. Wifi operates along this 15dB drop off from the AWGN case, all interferers still affect the signal in the same way, however, rather than an SIR of 5dB needed to completely block out the interferers, the value now must be equal to 20dB. Also the signal can now only tolerate interferers with an energy at least 12dB below their own energy, whereas before they could still be received when the interferer had an energy greater than that of the Wifi signal.

Zigbee is not as affected by the fading as Wifi, Zigbee follows a 10dB drop off in performance. However, for Zigbee to operate as if no interferers are present, the SIR must be at least 5dB in the presence of another Zigbee signal, but can extend up to 0dB when a Bluetooth signal is incorporated. When Zigbee only has to be able to tolerate the signals and can withstand only needing a BER of at least 10^{-3}, the Zigbee interferer can now have a higher power level than the

Zigbee signal and approach an SIR of -3db, this value can be decreased to -10dB in the presence of a Bluetooth interferer, with the performance due to the Wifi interferer in between.

Bluetooth is affected much more than Zigbee and encompasses the 15dB decrease in performance. In order for Bluetooth to achieve operation equal to that of having no interferers, Bluetooth must have an energy level at least 5dB to 15dB greater than the interferers, with a Wifi interferer causing an SIR of 15dB to be required . Bluetooth can tolerate signals with values between 3dB and -3dB of its transmitted power, approximately 10dB less than of the previous AWGN situation. The tolerance of Bluetooth to interferers is not as affected by fading as the ability to block them.

Chapter 5

Site Specific Channel Model

5.0 Wireless Insite Environment Simulation

To take the simulation one step further, rather than only incorporating one faded path into the simulation, multiple paths should be considered accounting for the various paths a signal can travel between the transmitter and receiver. In reality, having just one propagation path present is likely to occur only when communicating with a satellite in space, or with a ship on the ocean, due to the absence of reflectors and/or scatterers. For the purpose of this study, which is aiming to predict the performance of wireless devices within a nuclear power plant, numerous scatterers and reflectors that need to be accounted for will be present, especially when a direct path between the transmitter and receiver does not exist. Therefore, not only does a tool need to be used to calculate the different paths between a transmitter and receiver and their respective propagation properties, but the tool must also have the ability to include detailed drawings of objects such as desks, shelves, pipes, air ducts, equipment, and other types of items which can be expected to be found within an industrial environment.

5.1 Wireless Insite

One such software tool with the capability of performing both tasks required is Wireless Insite, developed by Remcom. Wireless Insite is a software tool which predicts the propagation path characteristics of electromagnetic waves. It was originally designed for outdoor urban environments, and it was later extended to include irregular terrain, foliage, indoor, and indoor/outdoor environments. This project takes advantage of using the indoor propagation prediction techniques. The indoor modeling software includes a full 3D vector ray-tracing model that can include having various features set for either an imported floorplan layout or one created through the floorplan editor provided. These different features can include placement of objects within a room that can be made of different materials, and it can take into account the material and thickness of walls, whether they are concrete or drywall. It also allows for the inclusion of doors and windows. Available materials include concrete, wood, metal, and glass along with others and the opportunity to create new materials and save them for future use.

The materials are used to determine various coefficient values such as reflection, transmission, and diffraction, which will all help to result in a more dependable simulation. To compliment selecting various materials, Wireless Insite also permits for the selection of several other parameters and features. The location of transmitters and receivers is allowed through the floorplan editor along with selecting the type of antenna that they are using, such as isotropic or dipole. The software also reserves the right for the selection of several different signal characteristics such as waveform, bandwidth, and carrier frequency. The specific values incorporated into this simulation will be revealed later.

5.1.1 Site Specific Room Model

Due to the fact that a detailed drawing of a nuclear power plant is unavailable, both in the sense that drawing one from scratch would shift the focus away from the goal of the project and that, because of security reasons, a detailed CAD(Computer Aided Drawing) drawing of a power plant cannot be distributed, the test environment used for the simulations will consist of a partial representation of an actual building which would be available if a future measurement campaign were to be conducted to validate the output obtained from Wireless Insite. This results in an office/laboratory type environment which has been developed by a colleague, and made available for modifications. The needed changes consist of modifying both the placement and properties of the transmitters and receivers.

5.1.2 Transmitter/Receiver Placement

For the simulation, as an initial starting point, only one receiver is considered to be present, allowing for a minimization of variables contained within the simulation. Figure 5.1 shows that the receiver is chosen to be placed near the perimeter of the room above a metal workspace. The receiver height, along with all the transmitter heights, were selected to be 2m, which is just above eye level, allowing for the objects placed within the room to have a minimal effect on the results. Since all objects are less than 2m tall, transmitters placed within the main room will be LOS transmitters and ones placed outside the main room will be NLOS transmitters. Once the simulation has been validated, more complex placement of the receiver can be allowed.

From Figure 5.1, it can be seen that the transmitters are placed in such a way that the coverage can be maximized. The main room itself is split into six sections, with a transmitter placed within each partition. This allows for a study of the effects of the performance of the primary LOS path due to the presence of the secondary propagation paths. Transmitters seven through eleven were placed outside of the main room in a way such that some transmitters would only need to transverse through one wall to reach the receiver while others would need multiple reflections and/or transmissions to arrive at the receiver. Conducting this trial will not determine the range of the protocols, since all powers are normalized at the receiver, but it will demonstrate how the path on which the signal propagates, affects the performance.

5.1.3 Signal Properties

Next the properties of the signals in which the transmitters and receivers are using will be explored. From Figure 5.1, it should be noted that at each transmitter and receiver location, there are actually three different transmitters or receivers, one for each protocol. This is because the different signals will not have the same propagation characteristics; therefore the need arises for separate transmitters and receivers. The properties specific to the waveform for each transmitter and receiver can be found in Figure 5.2, showing a window taken from the Wireless Insite program. This figure shows that the Bluetooth signal uses a Gaussian type signal with a bandwidth of 1MHz, located at a carrier frequency of 2405MHz or 2.405GHz, this value corresponds to channel #4 within the Bluetooth spectrum. The second waveform is a sinusoidal waveform representing Zigbee, with a bandwidth of 2MHz and also located at 2.4 GHz, which is channel #1 for Zigbee. Wifi is assumed to contain a raised cosine pulse shaping and is centered at 2.412GHz, relating to channel #1, and occupies a bandwidth of 22MHz.

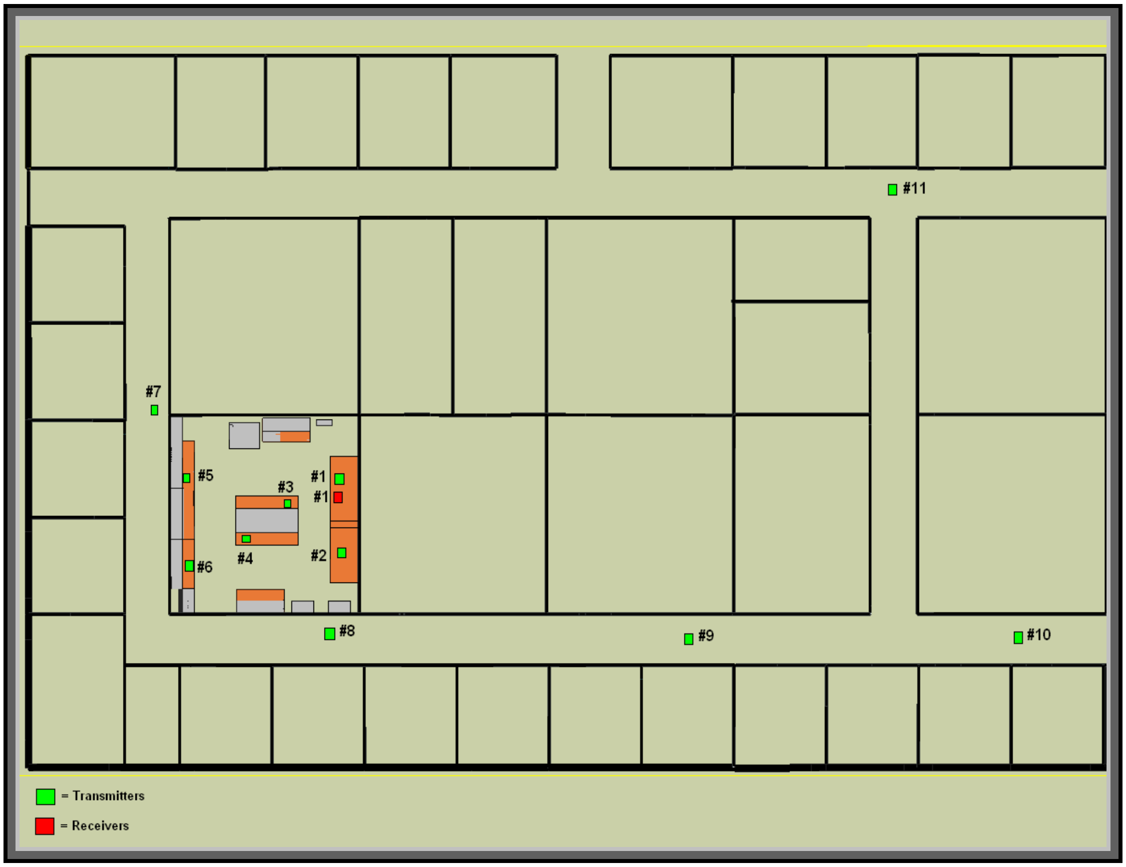
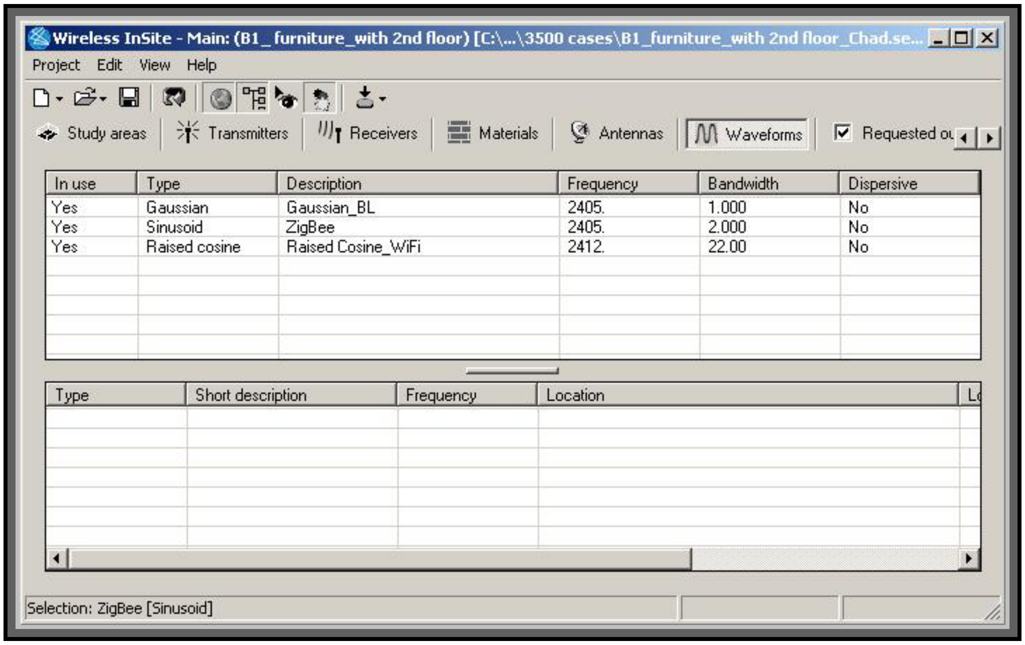


Figure 5.1- Transmitter and Receiver locations


Wireless InSite - Main: (B1_furniture_with 2nd floor) [C:\...\3500 cases\B1_furniture_with 2nd floor_Chad.se...
Project
Edit
View
Help
Study areas
Transmitters
Receivers
Materials
Antennas
Waveforms
☑ Requested ou

In use	Type	Description	Frequency	Bandwidth	Dispersive
Yes	Gaussian	Gaussian_BL	2405.	1.000	No
Yes	Sinusoid	ZigBee	2405.	2.000	No
Yes	Raised cosine	Raised Cosine_WiFi	2412.	22.00	No

Type	Short description	Frequency	Location	Lo

Selection: ZigBee [Sinusoid]

Figure 5.2 – Waveform Properties

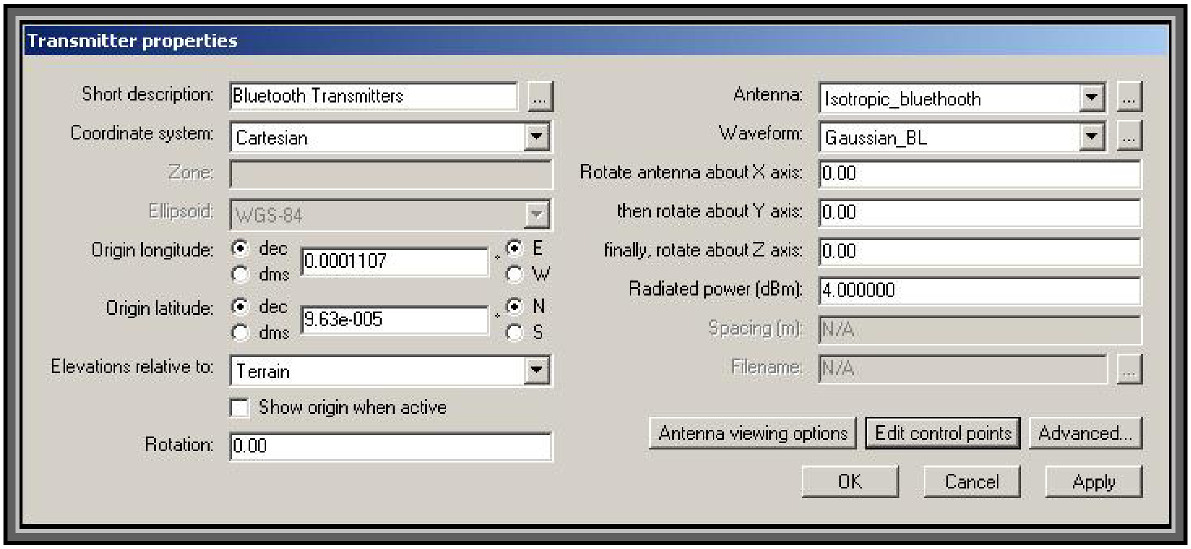
After specifying the waveform for each transmitter and receiver, several other parameters must also be chosen. A second window from Wireless Insite can be found in Figure 5.3. This figure shows the specifics for a Bluetooth transmitter, the only difference between the selection of the properties for the transmitter and the receiver is that of the selection of transmitter power level. From the figure, the transmitter uses the Bluetooth waveform along with an isotropic antenna, all antennas in this simulation are isotropic. The other consideration that is only specific to the transmitter is the radiated power, in Figure 5.3, this is set to 4dBm as specified for Bluetooth. The other two protocols use different values, Zigbee transmits at 0dBm, while Wifi radiates at a much higher 17dBm.

5.1.4 Wireless Insite Output

After selection of various parameters for the simulation of the propagation paths, a proper understanding of how to identify and interpret the results is needed. Two different transmitters, Wifi transmitters #5 and #7, which are in close proximity to each other, will have their outputs presented to show the difference caused from having to deal with obstructions located in the path of propagation, in this case a wall.

Wifi transmitter #5 is a LOS transmitter located in the upper left hand corner of the room under study from Figure 5.1. The resulting propagation paths associated with the transmitter will be composed of one direct path with nine supporting paths, which contain one or more reflections. The NLOS Wifi transmitter #7 is located within the same area of transmitter #5 except it is outside the room, thus the direct paths must transmit through the wall to reach the receiver. Therefore, all secondary will also contain a transmission through a wall to go along with their multiple reflections. The propagation paths can be found in Figure 5.4 for transmitter #5 and Figure 5.5 for transmitter #7. In these figures, the paths are not only shown but they also describe the relative power contained within each path. The lighter colored lines indicate more power contained within the path while the darker lines correspond to a lower received power, as specified by the bar indicator along the bottom of the figures.

The power contained within each path can also be shown in a graphical form. Figure 5.6 and Figure 5.7 show the relative received power of each path versus the delay associated with each path for transmitter #5 and #7 respectively. This is used to reinforce the notion of the advantage in power that a LOS transmitter has over a NLOS transmitter, and also the power advantage that



Transmitter properties

Short description: Bluetooth Transmitters

Coordinate system: Cartesian

Zone:

Ellipsoid: WGS-84

Origin longitude: ● dec ○ dms 0.0001107 ° ● E ○ W

Origin latitude: ● dec ○ dms 9.63e-005 ° ● N ○ S

Elevations relative to: Terrain

□ Show origin when active

Rotation: 0.00

Antenna: Isotropic_bluethooth

Waveform: Gaussian_BL

Rotate antenna about X axis: 0.00

then rotate about Y axis: 0.00

finally, rotate about Z axis: 0.00

Radiated power (dBm): 4.000000

Spacing (m): N/A

Filename: N/A

Figure 5.3 – Transmitter Properties

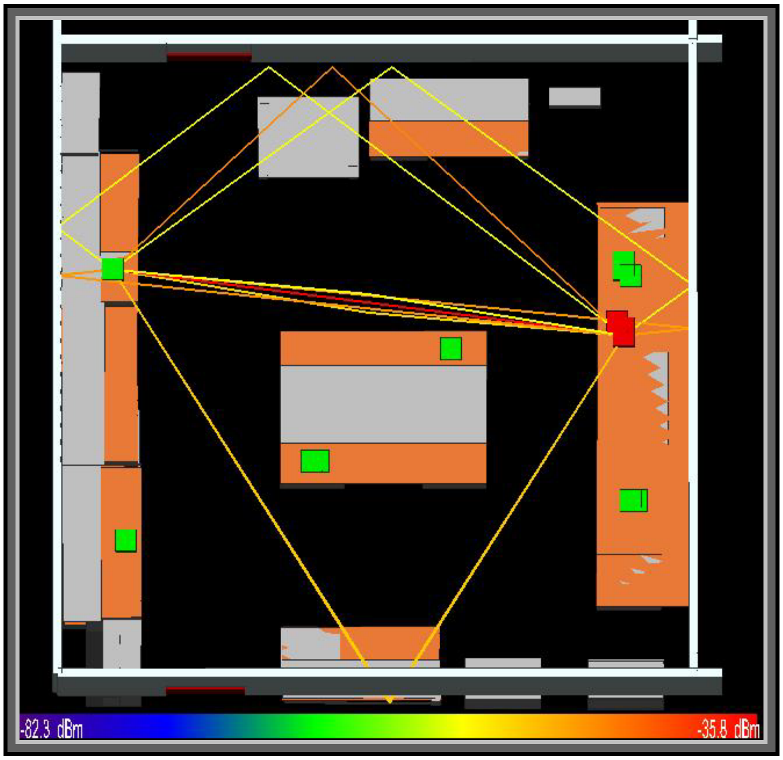


Figure 5.4 – Propagation Paths for Wifi Transmitter #5

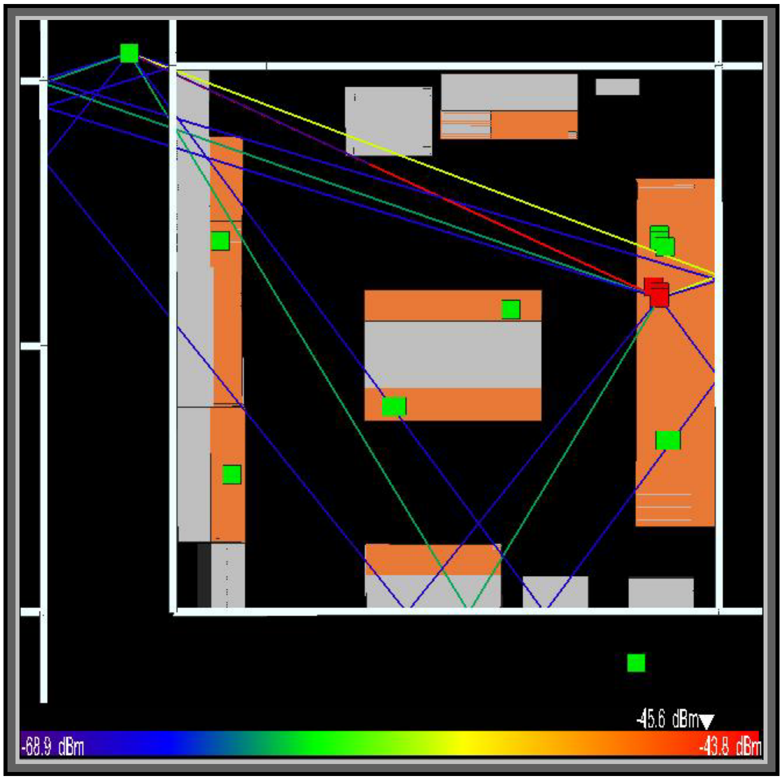
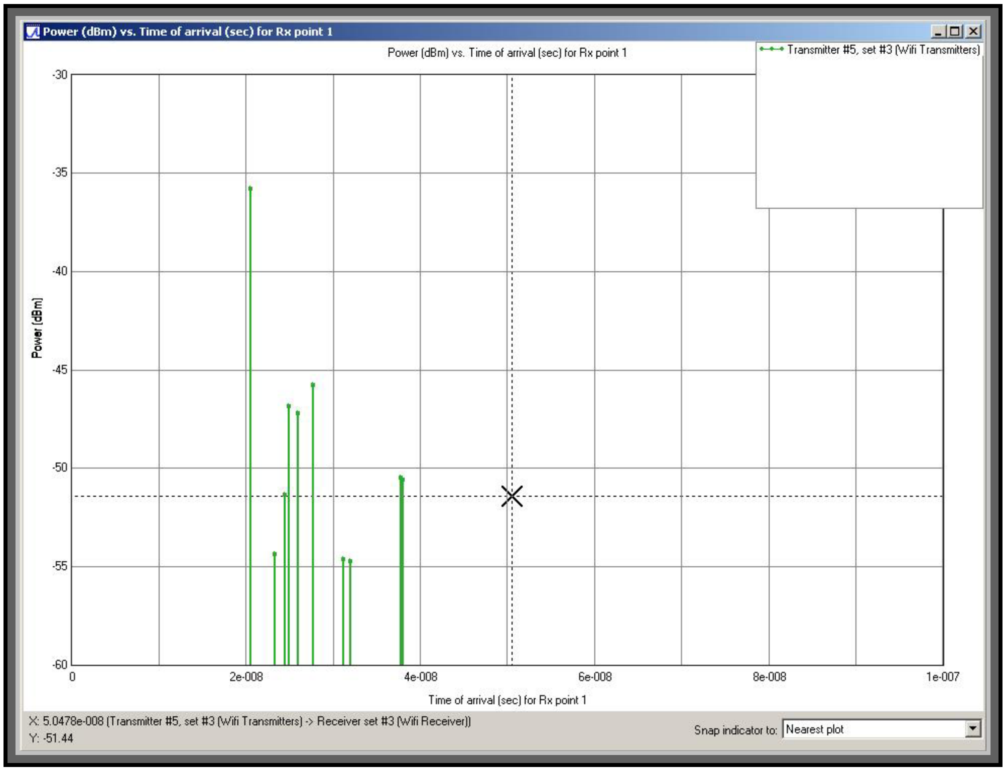
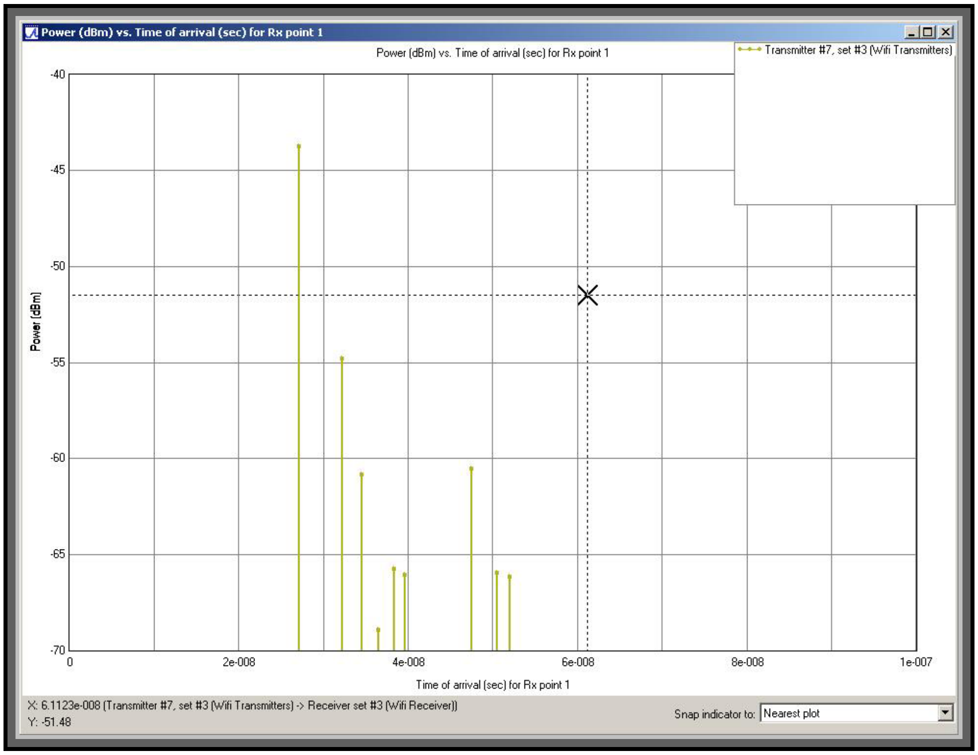


Figure 5.5 – Propagation Paths for Wifi Transmitter #7



X: 5.0478e-008 (Transmitter #5, set #3 (Wifi Transmitters) -> Receiver set #3 (Wifi Receiver))
Y: -51.44

Figure 5.6 – Power vs. Delay – Wifi Transmitter #5



X: 6.1123e-008 (Transmitter #7, set #3 (Wifi Transmitters) -> Receiver set #3 (Wifi Receiver))
Y: -51.48

Figure 5.7 – Power vs. Delay – Wifi Transmitter #7

the first arriving path has over all secondary paths, which undergo reflections. The results of the plots are given in tabular form found in Table 5-1 showing the results of transmitter #5 and Table 5-2 presenting the results for transmitter #7. Upon inspection, it can be seen that the LOS path of the #5 transmitter has a 7dB advantage over the performance of the single transmission path of transmitter #7, therefore a transmission can cause a decrease in power of approximately 7 dB. When looking from the first path to the second path for each set of results, this implies that a reflection has occurred, thus it appears that a reflection inflicts a 10dB drop in power. These results are only approximate and are only valid for concrete walls and when considering a Wifi signal, but the trend of a transmission harming the power of a signal less than a reflection is a valid observation within this study.

5.2 Results

The resulting BER curves can be grouped into three different categories, one for each protocol, showing the effects that an interfering signal has on a given protocol. Furthermore, each separate protocol can be broken down into its LOS and NLOS situations. Since eleven different transmitter points were chosen with three different devices located at each position, and for each protocol there are three separate interference cases, that corresponds to ninety-nine different BER curves being produced. To conserve time and space, and also to account for redundancy, only a select portion of them will be included within the results, with a collection of all BER curves available in the APPENDIX.

5.2.1 Transmitter/Receiver Performance

Before presenting the results for each device, it is important to look at the propagation characteristics from Wireless Insite for each transmitter location. This will aid in an effort to determine if the protocol should be able to perform at an acceptable level even before the interference has be introduced. Depending on the powers and phases of the subsequent paths after the first arriving path, these secondary paths may in fact decrease the overall performance of the system. Therefore the propagation path properties of the three protocols from Wireless Insite have been summarized in the following tables: Table 5-3 for Bluetooth, Table 5-4 for Wifi, and Table 5-5 showing the results of Zigbee. The three tables show the three different devices

Table 5-1 – Wifi Transmitter #5 Propagation Paths

Path Number	Phase (deg.)	Time (s)	Power (dBm)
1	-151.852	0.205496E-07	-35.804
2	-104.970	0.277587E-07	-45.809
3	-173.928	0.249576E-07	-46.864
4	-15.263	0.260218E-07	-47.225
5	-148.987	0.378032E-07	-50.521
6	27.667	0.380144E-07	-50.603
7	19.466	0.244994E-07	-51.385
8	-64.001	0.233424E-07	-54.371
9	1.848	0.311631E-07	-54.649
10	-18.962	0.320198E-07	-54.746

Table 5-2 - Wifi Transmitter #7 Propagation Paths

Path Number	Phase (deg.)	Time (s)	Power (dBm)
1	173.318	0.271163E-07	-43.755
2	-71.842	0.321982E-07	-54.803
3	-44.896	0.474554E-07	-60.570
4	-21.160	0.345179E-07	-60.840
5	-157.689	0.383456E-07	-65.787
6	-15.598	0.505357E-07	-65.973
7	113.873	0.396962E-07	-66.063
8	125.829	0.520404E-07	-66.180
9	125.829	0.520404E-07	-66.180
10	-77.880	0.364853E-07	-68.938

Table 5-3 - Bluetooth Propagation Paths

Bluetooth Transmitter Number		Propagation Path Number										
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**Total**
	1	1.000	0.008	-0.008	-0.005	0.003	-0.002	0.001	0.001	0.001	-0.000	**0.997**
	2	1.000	0.253	-0.120	0.108	0.006	0.017	0.004	0.004	-0.005	-0.007	**1.260**
	3	1.000	-0.020	0.000	-0.029	0.000	-0.003	-0.003	-0.003	0.004	-0.003	**0.944**
	4	1.000	-0.725	0.056	-0.042	-0.035	0.022	0.014	0.000	-0.006	0.006	**0.290**
	5	1.000	-0.102	0.070	-0.047	-0.026	0.025	-0.027	0.001	-0.002	-0.007	**0.885**
	6	1.000	0.724	-0.077	0.038	0.048	-0.063	-0.058	0.043	-0.001	-0.001	**1.653**
	7	1.000	-0.014	0.037	-0.018	0.006	-0.002	0.000	0.004	0.004	0.004	**1.023**
	8	1.000	-0.364	-0.048	0.037	0.028	0.025	0.013	-0.008	0.009	-0.001	**0.691**
	9	1.000	-0.011	-0.011	0.350	-0.182	-0.152	-0.068	-0.043	-0.043	-0.003	**0.837**
	10	1.000	0.242	-0.069	0.082	-0.075	-0.009	-0.020	0.012	-0.011	0.010	**1.161**
	11	1.000	0.053	0.012	0.000	-0.012	0.003	0.001	0.002	-0.001	0.002	**1.060**

Table 5-4- Wifi Propagation Paths

Wifi Transmitter Number		Propagation Path Number										
		1	2	3	4	5	6	7	8	9	10	Total
	1	1.000	-0.017	-0.008	-0.005	0.003	-0.001	0.001	-0.000	-0.000	0.000	**0.972**
	2	1.000	-0.296	-0.156	0.104	0.026	-0.018	0.004	-0.004	0.005	0.003	**0.668**
	3	1.000	-0.014	0.006	-0.029	-0.004	-0.007	0.001	0.001	0.004	0.001	**0.958**
	4	1.000	-0.828	0.057	0.004	-0.004	0.019	0.022	0.013	-0.005	0.006	**0.285**
	5	1.000	0.068	0.073	-0.052	0.034	-0.033	-0.027	0.001	-0.012	-0.009	**1.042**
	6	1.000	0.741	-0.049	0.054	0.062	-0.052	-0.044	0.002	-0.011	-0.011	**1.692**
	7	1.000	-0.033	-0.016	-0.019	0.006	-0.006	0.003	0.004	0.004	-0.001	**0.941**
	8	1.000	-0.411	-0.047	0.035	0.029	0.029	0.018	0.015	0.012	-0.002	**0.677**
	9	1.000	0.208	0.448	0.267	-0.143	-0.069	-0.044	-0.019	0.031	-0.005	**1.675**
	10	1.000	0.241	0.060	0.083	-0.094	-0.017	-0.016	0.012	0.009	0.010	**1.289**
	11	1.000	0.165	0.052	0.007	0.010	-0.001	-0.004	0.002	-0.001	-0.001	**1.228**

Table 5-5 - Zigbee Propagation Paths

Zigbee Transmitter Number		Propagation Path Number										
		1	2	3	4	5	6	7	8	9	10	Total
	1	1.000	-0.002	-0.008	-0.005	0.003	0.002	0.000	0.000	0.000	0.000	**0.991**
	2	1.000	0.501	0.148	0.106	-0.032	-0.010	0.004	-0.007	0.005	-0.003	**1.713**
	3	1.000	0.024	0.03	0.006	-0.013	-0.009	-0.003	-0.003	0.003	0.002	**1.036**
	4	1.000	-0.769	0.048	-0.027	-0.026	-0.011	-0.018	-0.003	0.002	0.003	**0.200**
	5	1.000	-0.045	0.067	0.060	-0.032	0.031	-0.017	0.009	0.012	0.005	**1.090**
	6	1.000	0.746	0.072	0.010	0.069	-0.067	-0.015	-0.039	0.012	0.011	**1.7981**
	7	1.000	0.071	0.024	-0.019	0.006	-0.006	0.006	0.005	0.003	0.003	**1.092**
	8	1.000	-0.299	-0.050	-0.009	0.025	0.013	-0.021	-0.017	0.010	-0.002	**0.651**
	9	1.000	-0.127	0.227	-0.173	-0.164	0.103	-0.065	-0.042	0.043	-0.035	**0.768**
	10	1.000	0.250	-0.155	0.072	-0.058	-0.003	-0.022	-0.004	0.008	0.010	**1.098**
	11	1.000	-0.380	-0.039	-0.054	0.084	-0.005	-0.008	-0.001	-0.002	-0.14	**0.599**

with each of the eleven different transmitters for each protocol. Along the top of the table are the 10 different paths along with the contribution that each path makes to the overall signal. The contribution of each signal is found by taking the normalized path power of the individual path and multiplying it by the cosine of the arriving phase of the path. Therefore the number can be positive or negative depending on relative phase of each path with the first arriving path. After totaling all individual path contributions, a total is given which yields the total power contained within the received signal.

In Table 5-3, depicting the summation of the Bluetooth paths, the transmitters whose signals are able to be received and demodulated have their total path powers highlighted. All transmitters will a total contained power greater than 0.885 are able to be recovered, while all transmitters with values less than that are unusable. This can be accounted to the fact that the secondary paths took too much information away from the first arriving path.

Upon inspection of Table 5-4, the results are somewhat different for Wifi then they are for Bluetooth. Even though the total received power for transmitter #2 is equal to 0.668, the signal is still able to be received, however, transmitter #7 has a total value of 0.941, yet it yielded unacceptable performance. This discrepancy can be attributed to the fact that the dominant LOS path of transmitter #2 carries a strong unfaded path between the transmitter and receiver, the secondary paths which take information away from the signal are faded and have varying fluctuations within the signal, therefore their effect on the overall signal was able to be minimized. But when considering the NLOS path of transmitter #7, the effects of the faded secondary signals have a greater effect on the overall signal because the dominant signal is also faded and cannot maintain a solid power level. This causes the performance of transmitter #7 to be unacceptable. The results of the Zigbee transmitters, found in Table 5-5, are on par with the results for the Bluetooth transmitters in that all transmitters with a total combined power over 0.8 generate acceptable results, even though not all of the same transmitters between Bluetooth and Zigbee performed in the same manner.

An interesting phenomenon to note regarding the propagation paths, found common in all three of the protocols, deals with the second path of transmitters #2, #4, #6, and #8. As can been seen from the tables, these transmitters all have a secondary path with an absolute power greater than 0.25, even though the first path is either a LOS path an NLOS path consisting of just one transmission. This occurrence can be credited to the metal desk on which the second path bounces off of before entering the receiver. In the cases of transmitters #4 and #8, the energy caused by the second path, coupled with the phase shift associated with striking the metal surface, causes the transmitters to become inoperable. The second path cancels out too much power of the overall signal. The effect is totally opposite for transmitter #6. In this case the signal always constructively adds with the primary path, and increases the total energy by almost 75% of the energy found within the first path. For transmitter #2, the performance is enhanced for both the Bluetooth and Zigbee simulations, but the effects when considering the Wifi protocol tend to harm the signal. This illustrates that in harsh environments, where there are many metal objects, the performance is highly dependent upon how the signal interacts with those objects.

5.2.2 BER Curves

Now the focus will be shifted to the transmitters that yield more acceptable propagation paths and are more likely to result in successful outcomes. Beginning with the Zigbee LOS scenario, the performance should follow a Ricean behavior, due to the dominant LOS component, and further more, flat fading should be expected due to the delay aspect of the simulation being disregarded because of its minimal presence. After careful inspection of the LOS cases, which include transmitters one through six, the results can be represented by three different curves.

5.2.3 Zigbee LOS

A reasonable representation of the BER curves of all interferers for Zigbee transmitter #1 and transmitter #3 can be found in Figure 5.8, showing the plot of Zigbee transmitter #3 with Zigbee interferers. In this BER curve, the results of the separate interferers are undistinguishable from the case when no interferers are considered. All results reach a BER of 10^{-5} before an SNR value of 9dB. Due to the Ricean LOS component, the results can be approximated as coming from an AWGN environment since the LOS path was so dominant.

The previous example illustrated that the interferers had no, or little effect on the overall signal. Thus, the message can be received as if no interference is present. Even though the interferers may not have an effect on the signal, there are other factors, which can limit the performance. For transmitter #2 with any interferer, and transmitters #5 and #6 for the cases when either a Bluetooth or Zigbee device was presented as an interferer, the ability of the signal to resist the

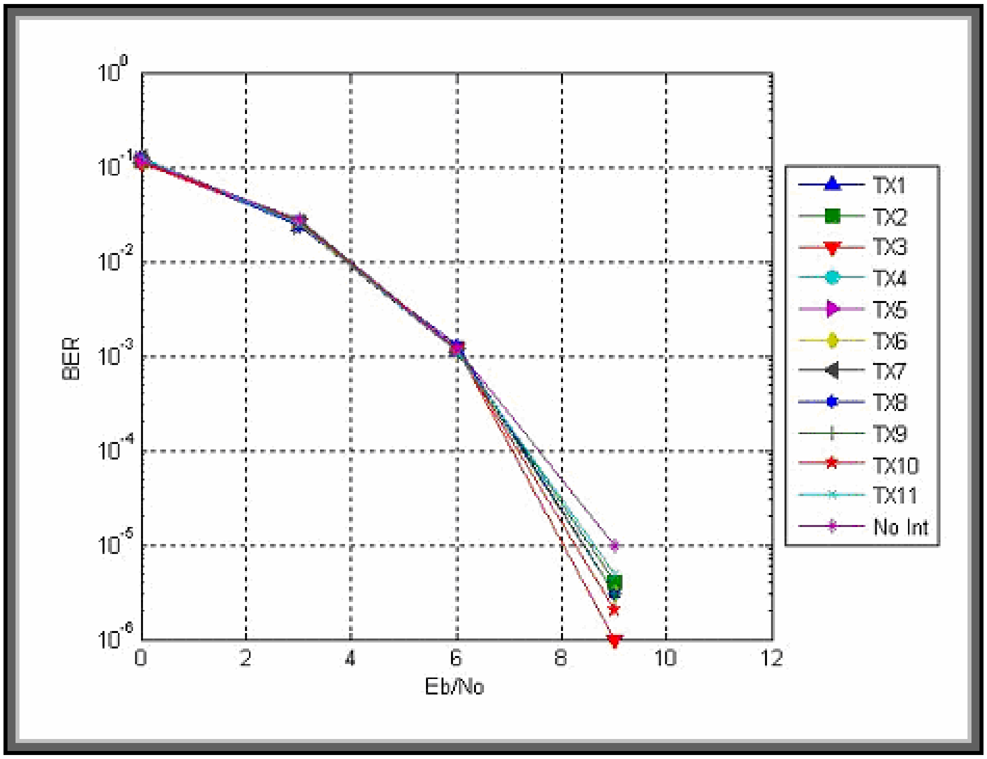


Figure 5.8 – Zigbee Transmitter #3 with Zigbee Interferers

affects of the interferers produces the same results as in the previous example of Figure 5.8 in that there is little deviation from the no interference setting. The difference however can be seen in Figure 5.9, which reflects the performance of Bluetooth interferers on the Zigbee transmitter #6. When comparing the two figures, the only variation is the curve at which the all the results are concentrated around. For Figure 5.9, the performance at 9dB is only approximately 5x10^{-4}, whereas it was 10^{-5} for the previous figure. In order for the performance to reach 10^{-5} for Figure 5.9, the SNR must now be equal to 11dB. This change in performance can be attributed to the relative characteristics of the propagation paths for the different transmitters. When compared to the first arriving path, it is obvious that transmitters #1 and #3 have more favorable secondary paths than do transmitters #2, #5, and #6.

Due to the power advantage that Wifi has over Zigbee, being radiated at an average power of 17dBm, as opposed to 0dBm for Zigbee. It follows that Wifi would affect the performance much greater than both a Bluetooth or Zigbee interferer. Unlike the previous examples when the interferers did not have any effect on the transmitted signal, in Figure 5.10 the Wifi interferers have begun to affect the operation of the protocol. The effects of the Wifi interferer on transmitter

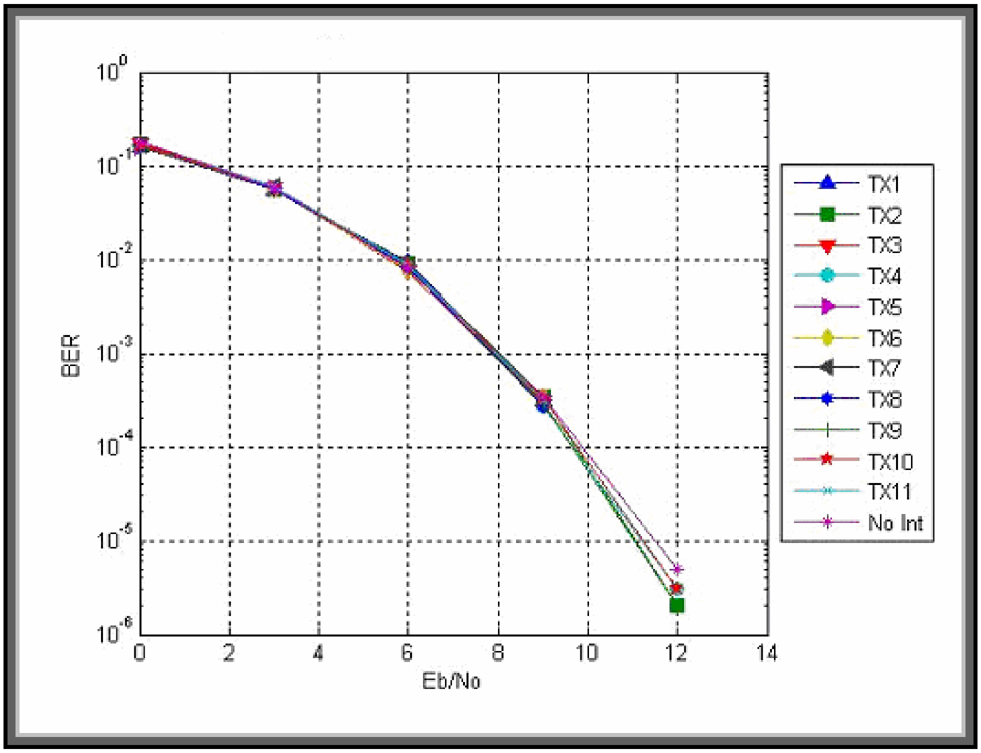


Figure 5.9 – Zigbee Transmitter #6 with Bluetooth Interferers

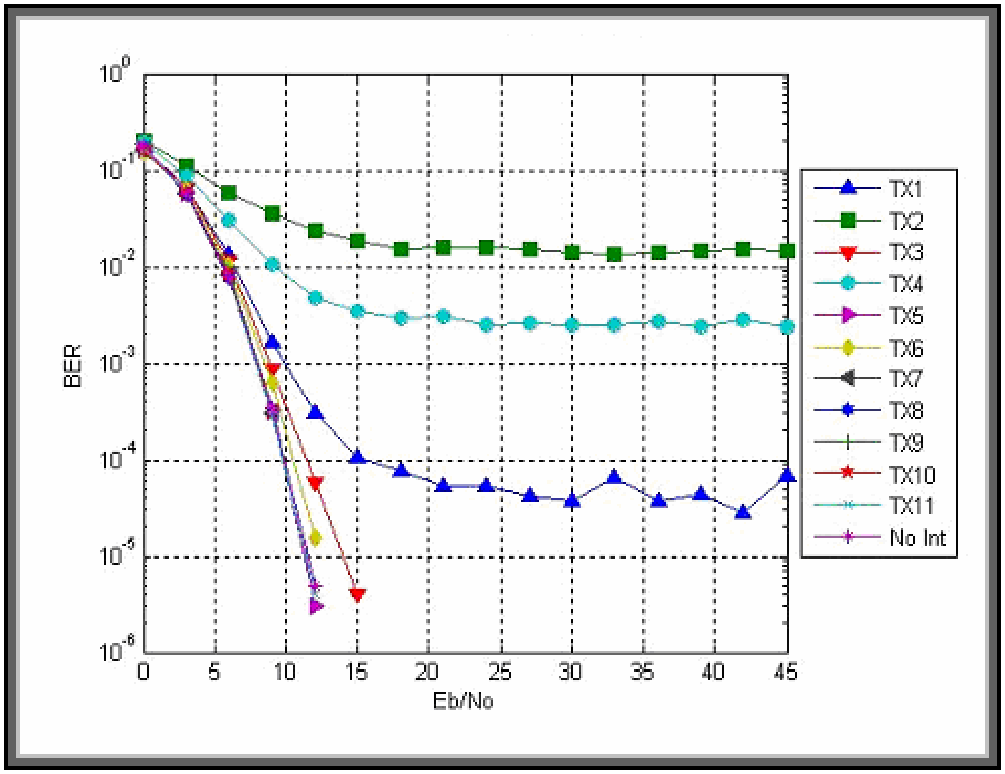


Figure 5.10 – Zigbee Transmitter #6 with Wifi Interferers

6, shown in Figure 5.10, and transmitter #5 are very similar. In the figure, it can be seen that only a few interferers cause the performance to diminish from the no interference case, those interferers are #1, #2, and #4. As a general rule of thumb, any performance which results in a BER greater than 10^{-3} will be considered to be undetectable. This means that from the figure, interferer #2 and interferer #4 cripple the performance and make those situations interference limited. On the other hand, even though interferer #1 limits the performance, the BER still maintains a probability of error less than 10^{-4}, so the signal can be received and demodulated. The question may arise why does interferer #1 not affect the performance as much as the other two interferers, even though is it closer in proximately to the receiver. This phenomenon can be explained by the relative phases of the two signals. Since the phase relation between the received signal of interferer #1 and that of transmitter #6 is on the order of 90 degrees, it minimizes the impact that interferer #1 has on the signal, more so than the other two interferers. This means that even though interferer #1 has more signal energy than the other two interferers, it is less correlated with the transmitted Zigbee signal and its affect is limited.

When comparing the results of Zigbee transmitter #5 when Wifi interferers are present with the results shown in Figure 5.10 for transmitter #6, the performances are very similar, when the interferers do not affect the signal the BER reaches 10^{-5} between SNR values of 10dB to 15dB. However, for transmitter #5, only interferers #2 and #4 cause the performance to be interference limited and flatten out. Interferer #2 causes the signal to be unrecognizable by generating too many errors, but interferer #4 does not completely distort the signal and the performance settles around 10^{-4}, which can be received.

5.4.4 Zigbee NLOS

The performance within the NLOS cases, Zigbee transmitters #7 thru #11 differ greatly from those when a LOS path is present. First and foremost, the performance of the system when only fading is considered, without interferers, has been degraded. For the LOS scenario, the system would reach a BER of 10^{-5} at 9dB, but now that crossing position has been pushed farther out, and the best performer is Zigbee transmitter #7 in which it's crossing point is at 20dB. Second of all, the performance has been corrupted because while the message signal has moved into the NLOS scenario, some of the interfering transmitters are still located within the LOS of the receiver, thus having greater received powers affecting the performance.

Looking at Zigbee transmitter #7, the performance when a Bluetooth or a Zigbee interferer is considered, stays relatively the same. By inspection of Figure 5.11, which shows the results obtained for Zigbee transmitter #7 with Bluetooth interferers, it can be seen that the NLOS interferers #7 thru #11 do not affect the signal in a substantial manner and the results appear to be within close proximity of the no interference case. This is also true for when Zigbee interferers are considered. All NLOS interferers follow the no interference case and reach a BER of 10^{-5} at 20dB, except for interferers #7 and #8. Their performance appears to settle to a value of $2x10^{-6}$. In Figure 5.11, the performance when any of the interferers are present, still reaches a point less than 10^{-3}. Therefore, all of the signals will be detectable. Interferers #1 and #2 keep the performance above the 10^{-4} level, while interferers #3, #4, and #6 can all maintain a BER nearer to 10^{-5}. Interferer #5 does not cause the signal to be interference limited and allows the BER to follow the performance of when the NLOS interferers are present. Very similar to these results, when Zigbee is assumed as the interferer, interferer #5 does not affect the performance, but the outcome of the other LOS interferers is a great deal different. First of all, interferers #1 and #2 cause the signal to no longer be detectable because they cause the BER to raise to 10^{-2}. Similarly, the performance when interferers #3, #4, and #6 also rise but still maintain a value near but less than 10^{-3}.

When looking at Wifi as an interferer for Zigbee transmitter #7, in Figure 5.12, it can be seen that due to the substantial increase in transmitted power between the two protocols, and the characteristics of the LOS path, each of the interferes located within the B1 room all have a considerable effect on the ability of the Zigbee receiver to demodulate the transmitted signal within an acceptable probability of error. The BER ranges from completely destroyed for interferers #1, #2 #3, #4, and #6, with nearly half of all received bits in error, to leveling out at a BER slightly above 10^{-4} whenever the 5th interferer is present. It should also be noted that both the #7 and the #8 interferers cause the BER to drop near 10^{-2}, meaning that they destroy the signal. Therefore it can be seen that between Bluetooth, Wifi, and Zigbee, Wifi has the most substantial affect on the interference, pushing the number of devastating interferers from zero for Bluetooth, to two for Zigbee, and finally the seven interferers of Wifi.

The final Zigbee example that warrants further examination is that of Zigbee transmitter #10. For each of the three groups of interferers, the BER curves are nearly identical to the ones shown in Figure 5.13, which include the presence of Zigbee interferers. What makes this curve interesting is that due to all of the interferers in and surrounding the B1 room, #1, #2, #3, #4, #5, #6, #7, and #8, the message is unrecognizable and approximately half of the bits are received in error.

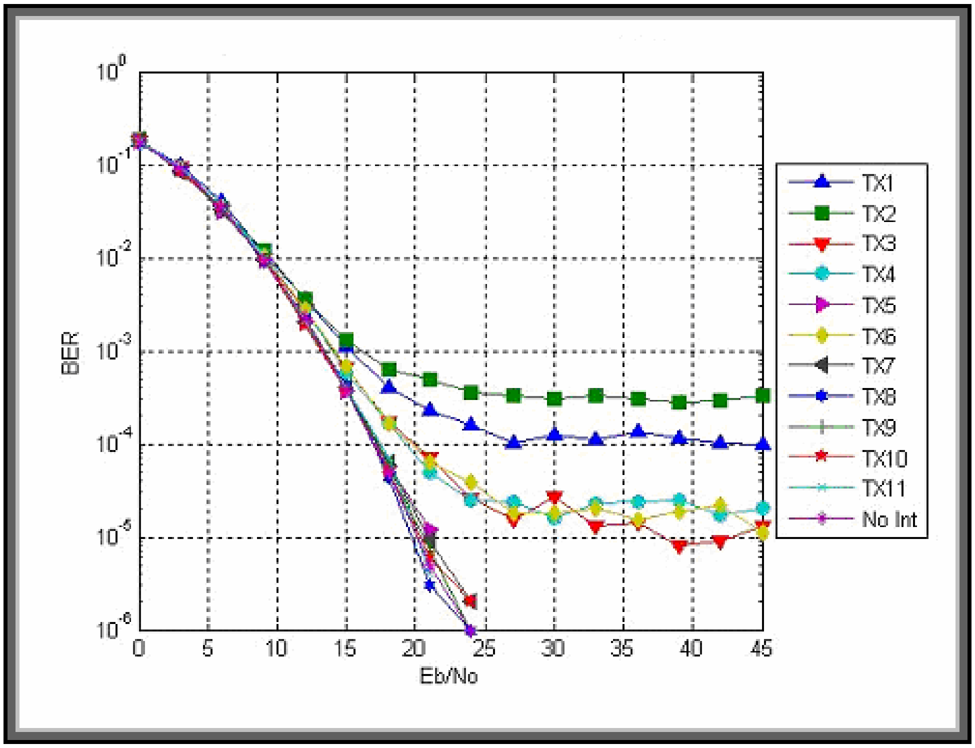


Figure 5.11 – Zigbee Transmitter #7 with Bluetooth Interferers

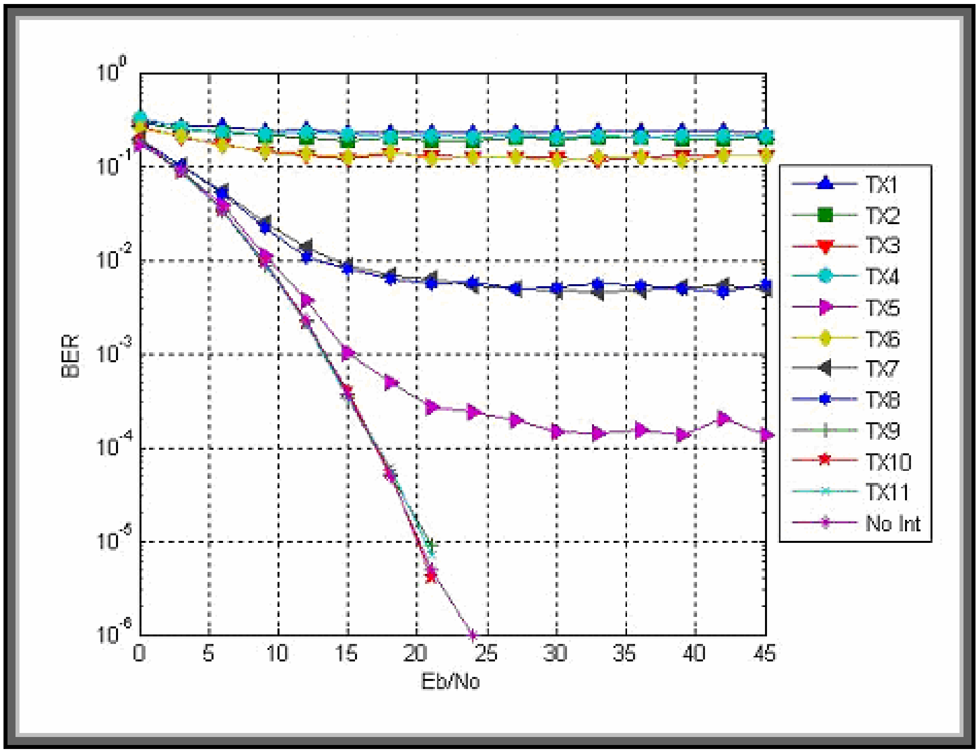


Figure 5.12 – Zigbee Transmitter #7 with Wifi Interferers

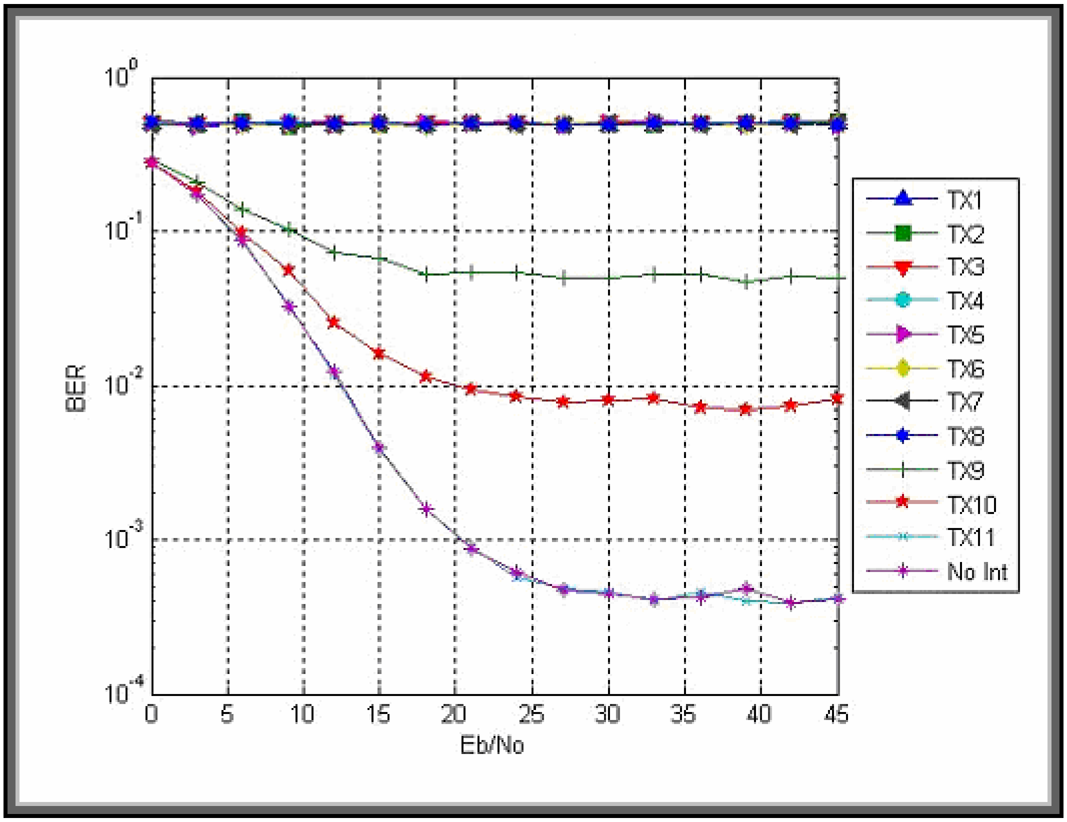


Figure 5.13 – Zigbee Transmitter #10 with Wifi Interferers

Conversely, for the interferers that are located a considerable distance away from the receiver, #9, #10, and #11, more on the order of the distance the Zigbee transmitter is, the performance follows that of the case when no interferers were used, meaning that those interferers have little effect on the reception of the transmitted signal. Two important details to observe however are the fact that the scenario when no interference was considered ever dropped below $4x10^{-4}$, and the other facet to notice is the location of the 9th and 10th interferers. The first feature can be attributed to the characteristics of the propagation paths for the transmitter. The location of the 9th and 10th interferer should be noted because for the case of when Bluetooth or Zigbee interferers were used, their performance modeled that of when no interference was considered, but their locations change when the Wifi interferers are present as seen in the figure. The level degenerates to an undetectable message for both interferers to a level near or below 10^{-2}, this can be attributed to the much higher transmitter power of Wifi

As a result, it appears that for Zigbee, Bluetooth is the least disturbing protocol, because in the presence of Bluetooth, the performance of the Zigbee transmitters does not tend to vary from the situation when no interferers are considered, with the exception of the NLOS transmitters with the

LOS interferers. Much like Bluetooth, Zigbee did not infringe upon the performance of another Zigbee device with a few exceptions. However, from the results of transmitter #7, it appears that Zigbee interferers affected the performance slightly more than the Bluetooth interferers did, therefore Zigbee is slightly more destructive than Bluetooth. Wifi on the other hand, seemed to have the most influence on the performance of the Zigbee devices, therefore Wifi appears to be the most damaging of the three protocols when considering its use in accompany with a Zigbee device, this realization can be attributed to Wifi having a high radiated power coupled with occupying a large bandwidth.

5.2.5 Wifi LOS

Moving from the Zigbee transmitter to the Wifi transmitter, the effects due to the interferers is expected to decrease dramatically. This is associated with the increase of radiated power from 0dBm of Zigbee, to the aggregate 17dBm of Wifi. The improved performance is most prevalent for the LOS transmitters, especially when dealing with either the Bluetooth or Zigbee interferers. Because of the 13-17dBm power advantage, the Zigbee and Bluetooth interferers do not have a profound impact on the operation of the Wifi receiver. The cases when the Wifi signal can be detected are for transmitters #1, #3, #5, and #6. When Bluetooth and Zigbee interferers are involved and only transmitters #1 and #3 for Wifi interferers, the performance looks very similar to Figure 5.14. This figure shows the effects of Zigbee interferers on Wifi transmitter #5. For each interferer, the performance crosses the 10^{-4} threshold between 10dB and 15dB. With the performance of the nearer transmitters pushing towards 10dB and the transmitter further from the receiver reaching the threshold more near 15dB. In some cases the performance due to interferers #1 and #3 push the curve out slightly further.

The results are considerably different when a Wifi interferer is introduced into the system for transmitters #5 and #6. This fact is obvious upon inspection of Figure 5.15, which shows the effects of the Wifi interferers on the #6 Wifi transmitter. While interferers #3, #5, and #7 through #11 behave in a manner similar to if a Bluetooth or Zigbee interferer was used, with the results approximate to that of the no interferer case, the #1, #2, and #4 interferers greatly affect the performance. The #2 interferer completely disrupts the Wifi signal making half of the signal unrecognizable while the interference from #4 causes the BER to lie between 10^{-2} and 10^{-3}. The effect of interferer #1 is that it produces a signal which may or may not be acceptable, due to the

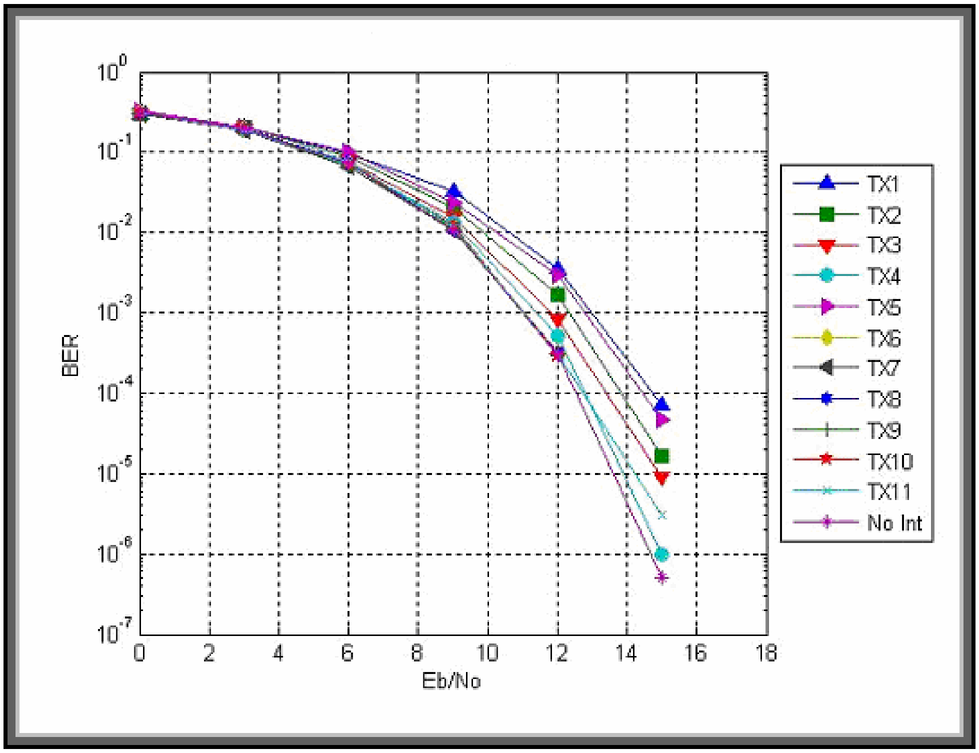


Figure 5.14 – Wifi Transmitter #5 with Zigbee Interferers

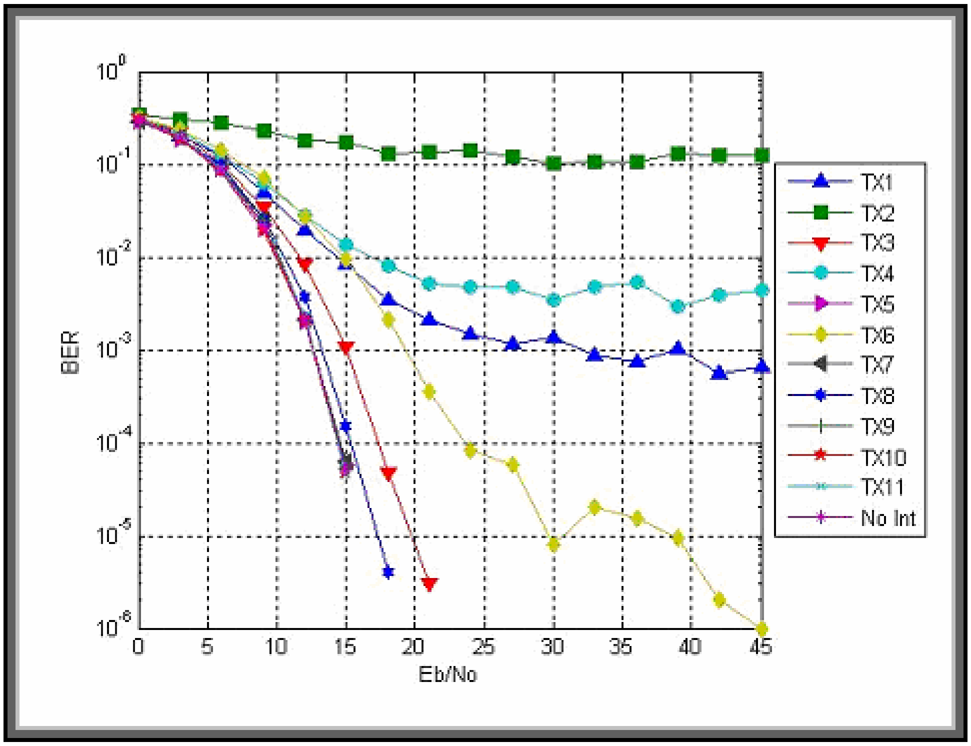


Figure 5.15 – Wifi Transmitter #6 with Wifi Interferers

fact that the BER settles near the 10^{-3} threshold. Interferer #6 pushed the BER curve so that the probability of error does not consistently stay below 10^{-5} until the transmitter reaches an SNR value of 40dB, an increase of over 20dB from the situation when no interference was considered.

Similar results as found in Figure 5.15, dealing with Wifi transmitter #6, are prevalent for Wifi transmitter #5 when considering the presence of Wifi interferers. The difference being that since Wifi transmitter #5 is closer to the receiver, not as many interferers affect the performance. In this case only the first two interferers affect the performance in a significant way, but they both cause the BER to stay above the acceptance threshold and cause the signal to be undetectable. In the presence of all other interferers, the performance maintains a probability of error below 10^{-6} for an SNR above 20dB. The change in performance due to the Wifi interferer can be contributed to the fact that Wifi has a wide bandwidth, equal to 22 MHz, nearly a third of the 80 MHz wide ISM band. On average they could be transmitting on the same channel, if the selection of the channel was not based on availability and was completely random. It can also be contributed to the fact that even though Wifi has a power advantage over the other two protocols, when considering a Wifi interferer, they are transmitting at the same radiated power. Therefore when two Wifi transmitters are placed near each other, without the enhancements made through the upper network layers, such as CSMA/CA and channel assignment, the two devices may not be able to co-exist.

Unlike the Zigbee transmitter #2, the Wifi transmitter #2 did not produce an AWGN type BER curve. As can be seen in Figure 5.16, showing the performance of transmitter #2 with the existence of Bluetooth interferers, the systems performance levels off near a BER of 10^{-5}. This can be attributed to the propagation characteristics of the path between the transmitter and receiver. Zigbee with its superior coding gain over Wifi is able to overcome the effects of fading. However, Wifi could not combat the fading as effectively. In the figure, all LOS interferers except #4 and #6 cause the performance to be unacceptable and preside near a BER of 10^{-2}. All other interferers do slightly affect the performance and thus they are concentrated between the 10^{-4} and 10^{-5} error levels.

When changing from Bluetooth interferers to Zigbee interferers, the performance stays pretty uniform, with the performance settling into one of the two basic areas. This also holds true for the case when Wifi interferers are used except now a third trend line has emerged, with this performance hovering just below the 10^{-3} threshold. The two interferers located upon this new line are the #1 and #6 interferers, therefore the performance of Wifi transmitter #2 is better when

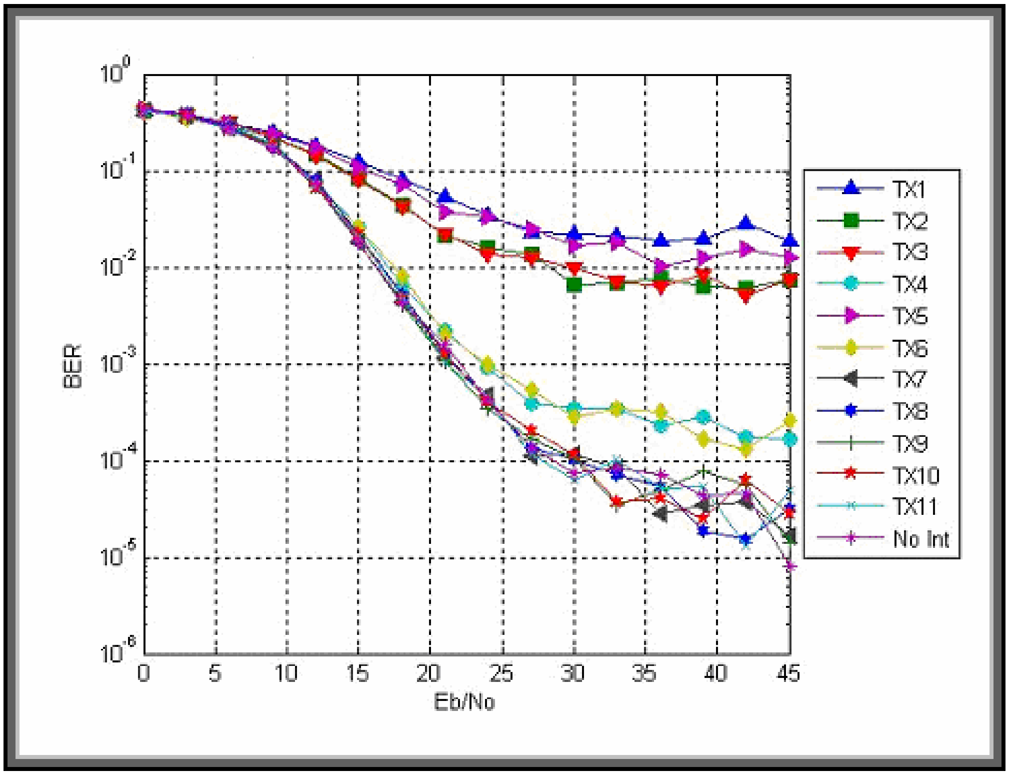


Figure 5.16 – Wifi Transmitter #2 with Bluetooth Interferers

considering the number one interferer of Wifi then when considering the number one interferer on the previous two standards. The results yield a performance that is acceptable in the presence of the Wifi interferer but not that of a Bluetooth or Zigbee interferer. This is just the opposite when considering the effects of the #6 interferer. Even though the #6 interferer does not cause the performance to become unacceptable when the Wifi interferer is presented, it does cause the performance to be inferior to when a Bluetooth or Zigbee interferer is considered.

5.2.6 Wifi NLOS

The performance of transmitter #2 is not the only difference between the performance of the two protocols, Zigbee and Wifi. When considering the NLOS scenarios for Zigbee, the only two transmitters that produced acceptable results are #7 and #10. Upon inspection of the NLOS results for Wifi, the #7 transmitter no longer can be used. However, the #9, #10, and #11 all produce acceptable results, which could be detected in a receiver. The trends between the three transmitters are fairly universal, for the cases of Wifi and Zigbee, the interferers either cause the receiver to be unable to demodulate the signal, or the performance roughly follows that of the no interference situation. The same cannot be said about the performance due to the Bluetooth interferers, the BER curves are spread out between the no interference case and when the signal in unrecognizable.

By looking at Wifi transmitter #9, Figure 5.17, which illustrates the effects due to the Bluetooth interferer, this spreading of the BER curves can be seen. The performance varies from the NLOS interferers being situated near the no interference case and maintaining a BER near 3x10^{-5} at 35dB, to the LOS interferers being spread from interferer #5 having a probability of error of 10^{-4} at 35dB. From there interferers #1, #2, and #4 all settle near the acceptable performance threshold for SNR values above 30dB. The only two interferers that cause the performance to be unacceptable are the #3 and #6 interferers.

The trends found in Figure 5.17 are very different than what can be seen for the other two interferers of Wifi and Zigbee. For the condition when Zigbee is the interferer, the only interferers which when considered, yield an acceptable performance, are the #9, #10, and #11. They all follow the no interference case, all other interferers distort the signal and cause nearly half of the bits to be in error. The same trend is found when Wifi interferers are being used; the only interferers not causing half of the bits to be in error are the #9 thru #11 interferers. For the case of Wifi, these interferers do not follow the no interference case, the #10 and #11 interferers settle to a BER slightly above 10^{-4} and the #9 interferer does not allow the BER to reach 10^{-2}, thus the effects of this interferer destroy the signal.

Nearly identical performance to that of transmitter #9 can be found in Figure 5.18, which depicts Wifi transmitter #10 with Bluetooth interferers. The difference being that instead of only two interferers causing the signal to become distorted beyond recognition, five of the LOS interferers damage the signal. The lone LOS interferer which when considered does not significantly corrupt the signal is the #4 interferer, even though its performance is limited to 3x10^{-4} at 30dB, which is greater than the values between 5x10^{-6} and 5x10^{-5} at an SNR of 35dB for the NLOS interferers and the situation when no interference was contained.

Again, when taking into account the effects of the Zigbee and Wifi interferers, the performances are very similar. For Zigbee, the LOS interferers all completely distort the signal along with the #7 and #8 NLOS interferers. Just as before, the #9 thru #11 interferers do not affect the signal and their performances are comparable to when no interferers are used. A difference occurs when

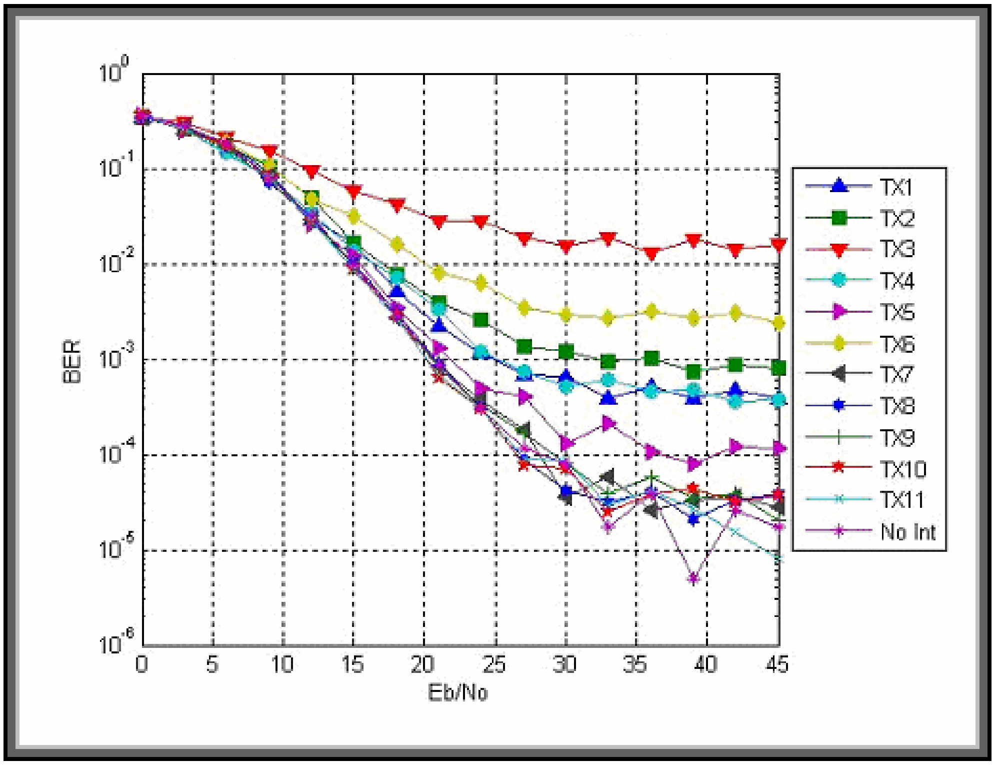


Figure 5.17 – Wifi Transmitter #9 with Bluetooth Interferers

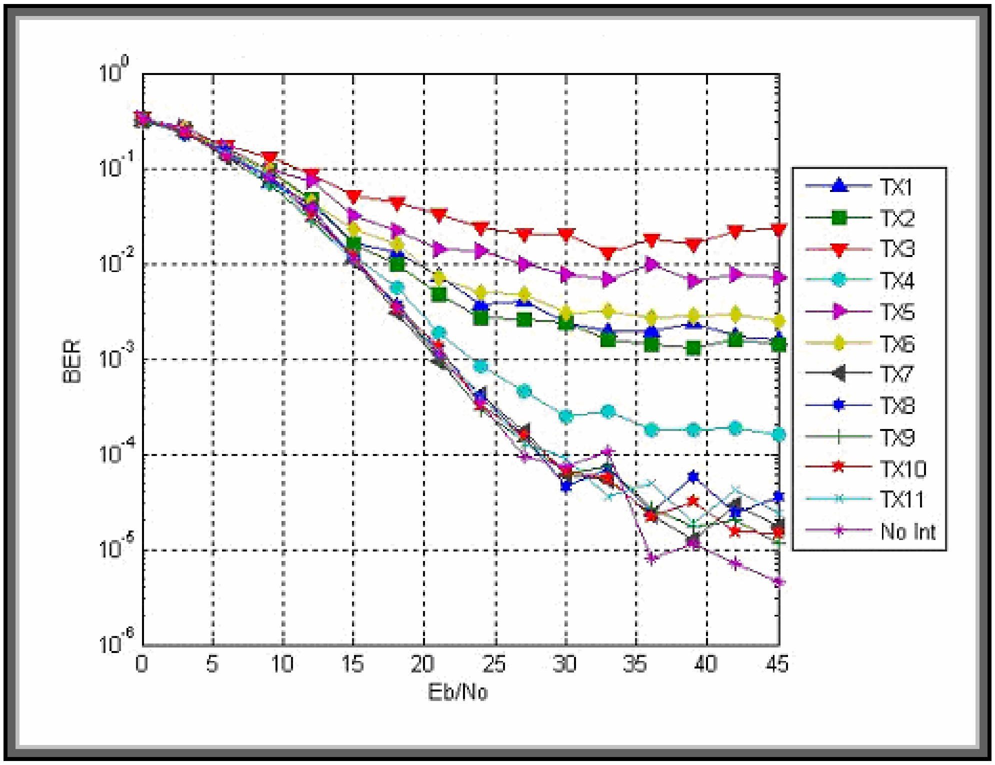


Figure 5.18 – Wifi Transmitter #10 with Bluetooth Interferers

moving toward the Wifi interferers, when transmitter #9 is being used, two of the interferers still allowed for an acceptable signal to be received. Although when moving to transmitter #10, none of the interferers allow for a signal to be detected and they all completely damage the signal.

The results of the final Wifi transmitter, #11, can be found in Figure 5.19, which portrays the effects of including a Wifi interferer. The first noticeable difference between the results of the previous two transmitters is that the line depicting no interference shows that the BER curve resembles the performance of a system noise limited and continues to slope downward. Whereas the previous two transmitters are appearing to flatten out to a constant level, a phenomenon that once again can be attributed to the unique propagation characteristics of this particular transmitter. Also, from the figure, it can be seen that the only interferers, which do not significantly affect the signal, are those of interferers #7, #8, and #9. With transmitter #11 being the furthest transmitter from the receiver, the effects of interferers #10 and #11 can be noticed because their power level is now within the same vicinity of the radiated power of transmitter #11. Therefore, when coupled with the relative phases, it appears that interferers #10 and #11 impair the signal. Conversely, interferers #7 and #8 do not impair the performance, they follow the same trend line as the no interference. Interferer #9 however, causes the BER to become interference limited and level off near a BER slightly less than 10^{-5}.

Comparing the results of transmitter #11 when both Bluetooth and Zigbee interferers are used can be compared to the previous two transmitters. For Bluetooth, the performance is spread between the LOS interferer's performance and that of the NLOS interferers. As before, the NLOS interferers do not cause the performance to vary considerably from the no interference instance. The LOS interferers however, cause the performance to fluctuate near the 10^{-3} threshold for the #1, #2, #4, and #5 interferers, while the #3 and #6 interferers cause the signal to be somewhat destroyed and unacceptable. When a Zigbee interferer is considered, the results are pushed to either one extreme or the other; half of all bits are received in error for the LOS interferers along with two of the NLOS interferers, #7 and #8. On the other hand, the performance follows the no interference situation whenever the other NLOS interferers are considered, interferers #9, #10, and #11.

Upon reflection of the results, the overall trend for Wifi is very similar to that of Zigbee, when considering the effects of the interferers. Like before, Bluetooth appears to be less intrusive upon Wifi than the other two interferers. The difference being that for the NLOS transmitters of Zigbee, the effects of Bluetooth for the most part do not cause the signal to be completely distorted.

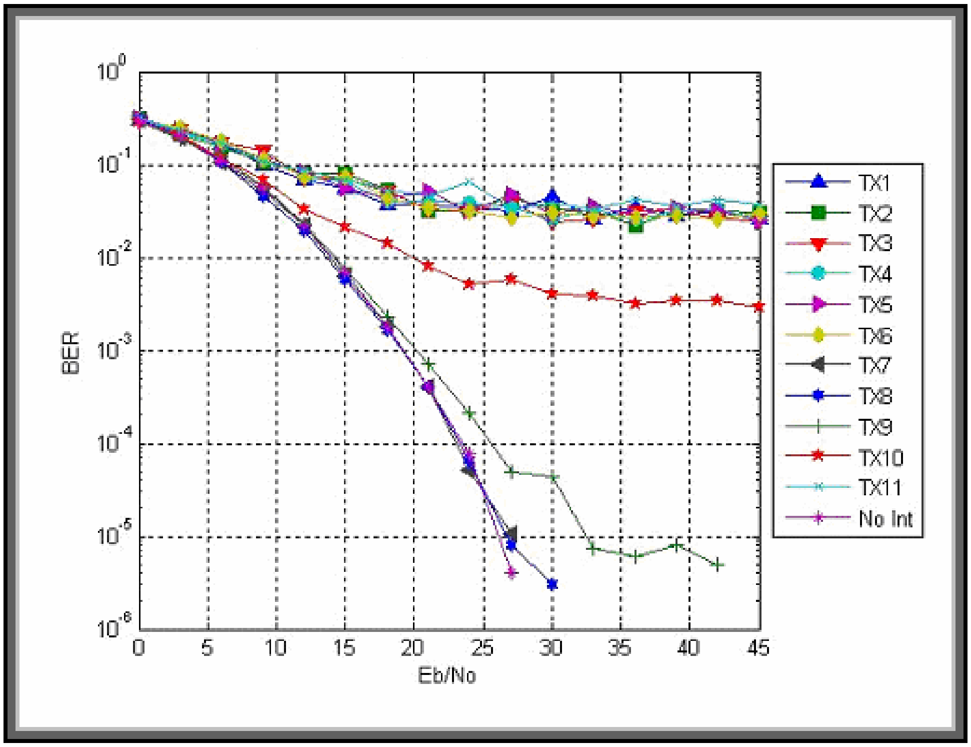


Figure 5.19 – Wifi Transmitter #11 with Wifi Interferers

When considering the NLOS transmitters of Wifi that is no longer the case. The LOS interferers affect the performance considerably, sometimes allowing the signal to still be detectable, and at other times causing the performance to go slightly above the threshold of acceptable performance. The NLOS interferers on the other hand do not affect the performance at all, allowing the signal to be received as if no interferers were present.

5.2.7 Bluetooth LOS

Unlike the previous two protocols, which used the advantage of spreading a signal over a wide bandwidth, Bluetooth uses a small bandwidth and jumps from one frequency to another. This aids in its ability to minimize interference by simply avoiding the interferers, the chances are small that the same interferer will interfere with consecutive hops. Whenever Bluetooth has a clear LOS path to the receiver, the other protocols do not have an affect on system at all. This fact is evident in all usable Bluetooth transmitters, #1, #2, #3, #5, and #6, for all cases when considering the interference associated with Bluetooth, Wifi and Zigbee interferers. The only differences in performance can be found in the changes in the no interference case across the five different transmitters.

The first example, Figure 5.20 shows the results obtained from Bluetooth transmitter #1 with Zigbee interferers. From this plot, it can be seen that the interferers do not affect the signal in a profound way, but upon inspection of the SNR when the BER crosses the 10^{-5} error level, the SNR is equal to 10dB. When going from Figure 5.20 to Figure 5.21, which shows the effects that Wifi interferers have on the signal of Bluetooth transmitter #3, the interferers have no impact. The curve does not reach 10^{-5} until an SNR of 11dB, this is the same as the performance for all the other interferers of both transmitter #3 and those of transmitter #2, but for this transmitter the SNR must exceed 12dB to exhibit the same performance. When going to the transmitters further from the receiver, the performance maintains the trend of pushing the curve to the right, which in turn means more energy is required to maintain the same performance. Inspecting the results of transmitter #6 with Bluetooth interferers in Figure 5.22 shows that the SNR must now be equal to 14 to achieve the 10^{-5} error rate, this is true for the other interferers as well. The results of transmitter #5 are very similar except that the SNR only needs to reach 13dB for the 10^{-5} BER.

5.2.8 Bluetooth NLOS

Once the Bluetooth transmitters are placed outside the B1 room, the performance varies greatly due to the interferers. There are three different transmitters that perform to at least a minimum acceptable standard, that standard being that the instance when no interferers were considered must at least surpass the 10^{-3} probability of error threshold. The three transmitters, which qualify under this standard, are the #7, #10, and #11 transmitters. Within these, the #7 and #11 transmitters reach a BER of less than 10^{-5}, while the #10 transmitter's performance only goes beyond the 10^{-3} level. Even though the actual values vary for these three transmitters, the tendencies for each can still be classified into three different categories when the interferers are considered. Those categories are when the interferers (1) cause the signal to be undetectable, (2) do not affect the signal, and (3) is somewhere in between the previous two. By and large, the interferers with a short LOS path to the receiver, #1 thru #4, can be placed into the first category. This is due to the fact that those interferers have a dominant path and that dominant path is received with a much higher total power than the signals received from outside the room. The second category of interferers consists of those that are not placed within close range of the

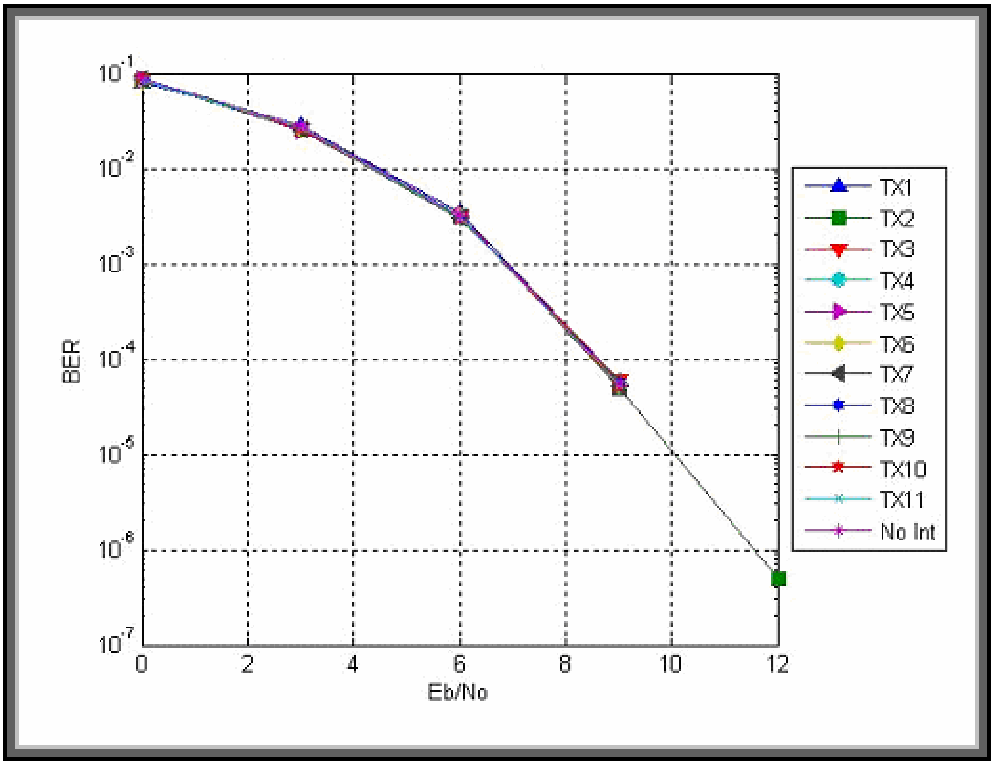


Figure 5.20 – Bluetooth Transmitter #1 with Zigbee Interferers

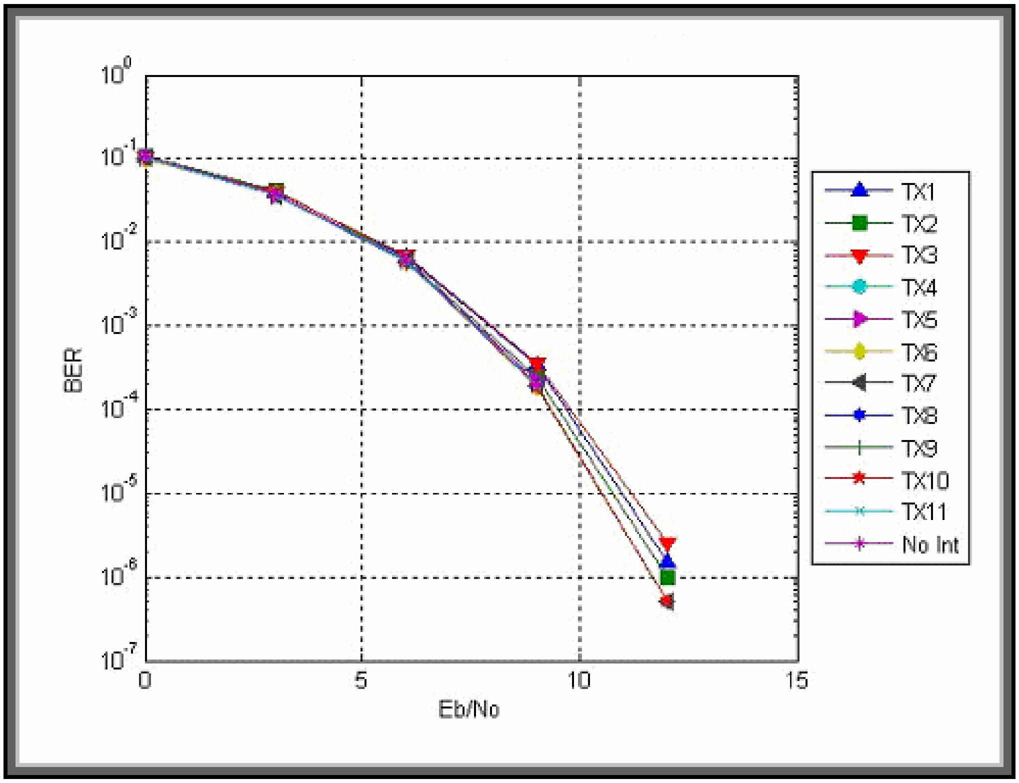


Figure 5.21 – Bluetooth Transmitter #3 with Wifi Interferers

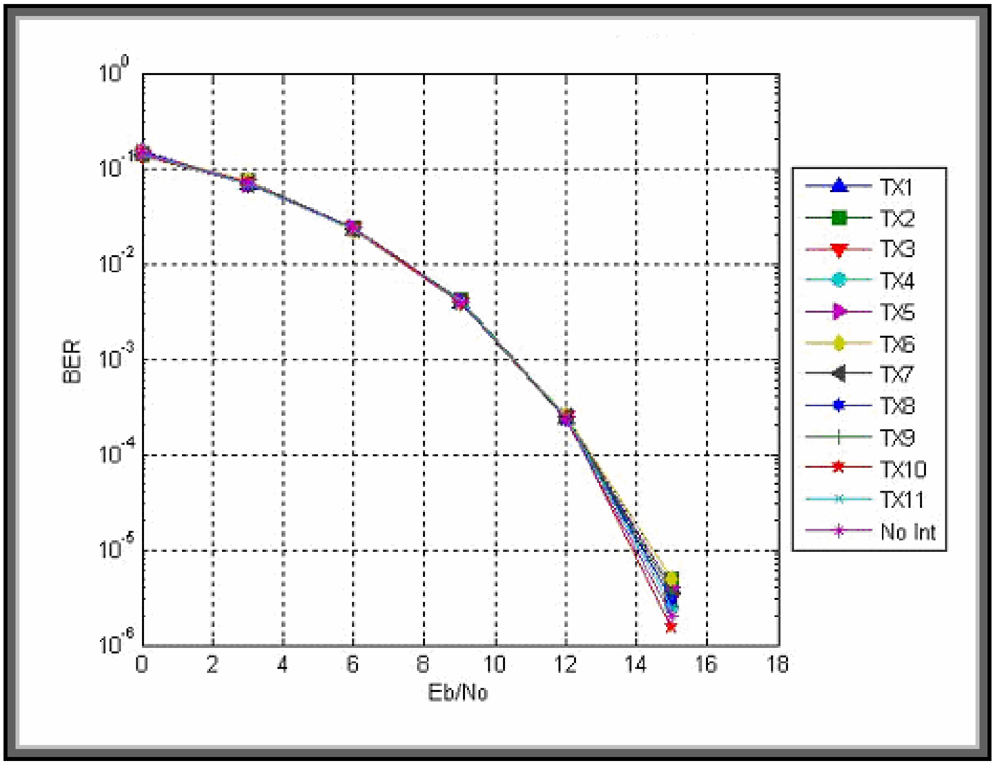


Figure 5.22 - Bluetooth Transmitter #6 with Bluetooth Interferer

receiver. This is because these interferers do not contain signal powers that can overwhelm the transmitted power of the Bluetooth signal because the propagation loss is too great. This category therefore consists of interferers #9, #10, and #11. Now that the two extremes have been accounted for, the middle ground must be considered. This would include the effects of the interferers, which are neither close to nor far away from the receiver. The performance of these interferers is fairly unpredictable. This group consists of both LOS and NLOS interferers, #5 thru #8. Therefore, the phase of the signals becomes more critical than the power because these interferers have power levels similar to those of the NLOS Bluetooth transmitters, so it matters if the signal and interferer have relatively close phases or if they are 180 degrees out of phase.

By examining Figure 5.23, these three categories can be illustrated by looking at how the different Wifi interferers affect the Bluetooth transmitter #7. As expected, interferers #1 thru #4 keep the BER near 10^{-3}, the threshold between detectable and undetectable signals. Also, interferers #9, #10, and #11 do not affect the signal in a considerable way, as was predicted,. Moving on to the four interferers that were questionable, it appears that the two LOS interferers, #5 and #6, affect

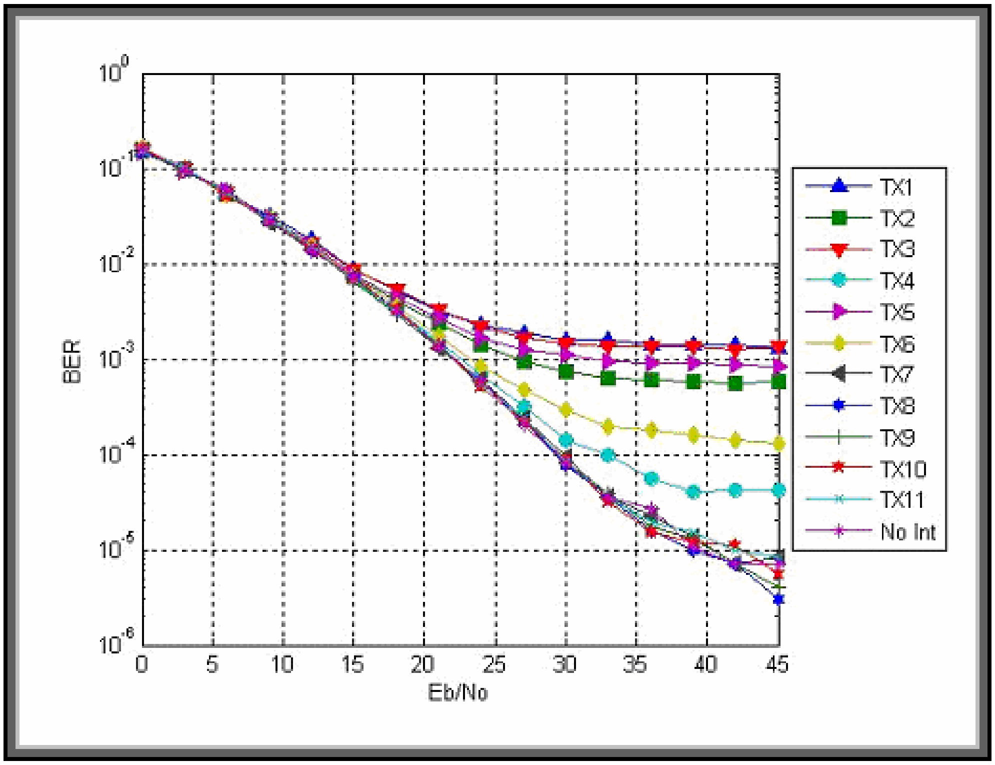


Figure 5.23 – Bluetooth Transmitter #7 with Wifi Interferers

the signal, but still allow the BER to fluctuate around 10^{-4}. The #7 and #8 interferers did not impinge on the signal and the performance paralleled that of the other NLOS interferers, #9 thru #11.

Comparing the results of the Wifi interference case of Bluetooth transmitter #7, with those of the other interferers, similar results were obtained for the Bluetooth interferers, although very different results were discovered for Zigbee. For the Zigbee interferers, both the second category and third category interferers performed in the matter that they should have. The second group, the #9, #10, and #11 interferers, did not affect the signal while the third group is unpredictable as expected because none of them appear to significantly influence the signal. The LOS interferers however did not perform as expected. The only two interferers, which changed the BER of the signal, were found to be the #1 and #2 interferers. Although their effect was not drastic, they only caused the BER to reach $2x10^{-4}$, rather than 10^{-5}, which the other signals reached at SNR values above 40dB. When considering the effects of a Bluetooth interferer upon transmitter #7, the results are as expected, interferers #9 thru #11 do not affect the performance, interferers #1, #3, #4, and #6 all cause the BER to settle to a value around $5x10^{-4}$, interferer #2 completely destroys the signal, and interferers #7 and #8 do not allow the BER to reach 10^{-5} and they remain near $3x10^{-5}$.

Moving to a transmitter farther away, the performance of the system as a whole changes, but the contribution due to each interferer is approximately the same. Looking at the results obtained in Figure 5.24 when a Zigbee interferer attacks the signal of Bluetooth transmitter #10, the results are almost an exact replica of the results for the other two interferers. Interferers #9 thru #11 do not affect the performance and they settle to a value of $4x10^{-4}$ for SNR values above 30dB, along with the no interference case. All other interferers cause the BER to be above the 10^{-3} threshold making the signals meaningless. The only difference is that for interferer #5 when being used as a Wifi interferer, it has a BER hovering around the 10^{-3} threshold, therefore the signal may or may not be acceptable, depending on the application.

Disregarding the effects of interferer #5 in the single instance from the previous results, the effects of the interferers on the results for transmitter #11 are the same as for transmitter #10. The no interference situations are completely different because transmitter #11 continues to decrease while transmitter #10 flattened out. All of the interferers, #1 thru #8, cause the signal to be irreconcilable. For interferers #9 thru #11, the performance follows the no interference case when the interferers are considered to be Wifi and Zigbee interferers. The performance changes however, when Bluetooth interferers are used, and the performance is depicted in Figure 5.25. In this figure, the three interferers have different effects on the transmitted signal of Bluetooth transmitter #11. Bluetooth interferer #9 causes the performance to be equal to 10^{4} for SNR values above 35dB. Interferer #10 appears to level off to a BER of 10^{-6} at an SNR of 45dB, while the effects of interferer #11 allow the performance to continue to decrease past a probability of error of 10^{-6}, very near the case of no interference.

From the results of the case when Bluetooth was the transmitted signal, Bluetooth appears to be the most well equipped protocol at resisting interference from other devices. At least for the LOS case since none of the interferers were able to affect the performance of Bluetooth. However, the performance when moving to a NLOS case fell in line with the performance of the previous two devices, when the interfering transmitter were located in proximity with the receiver, the signal was damaged, as long as the interferers were located an comparable distance with the Bluetooth transmitter, they did not affect the signal.

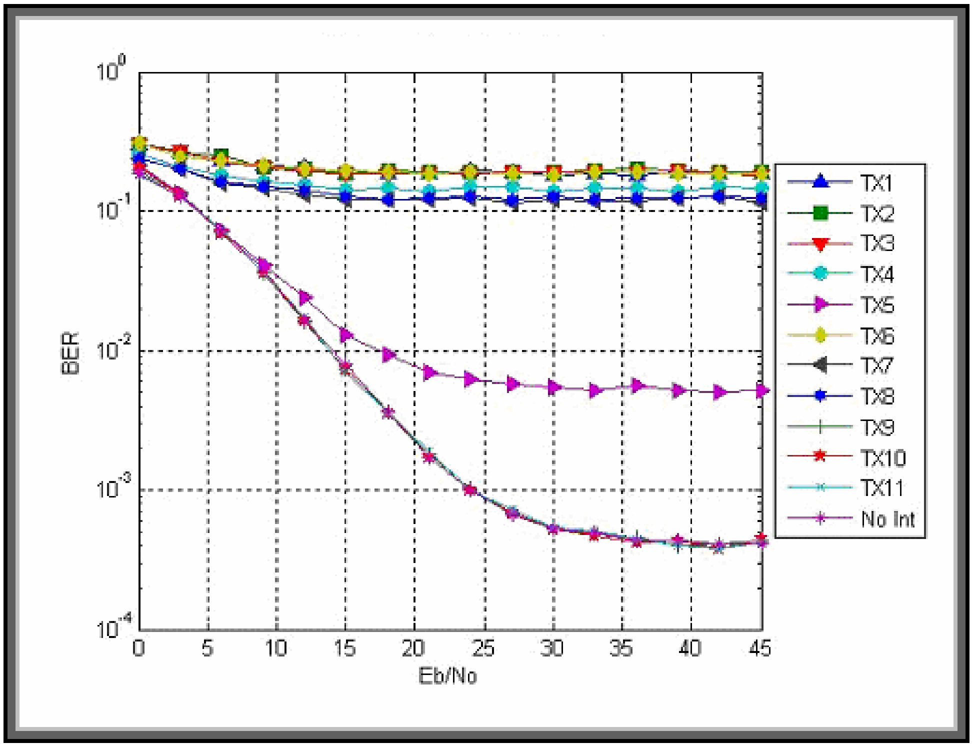


Figure 5.24 – Bluetooth Transmitter #10 with Zigbee Interferers

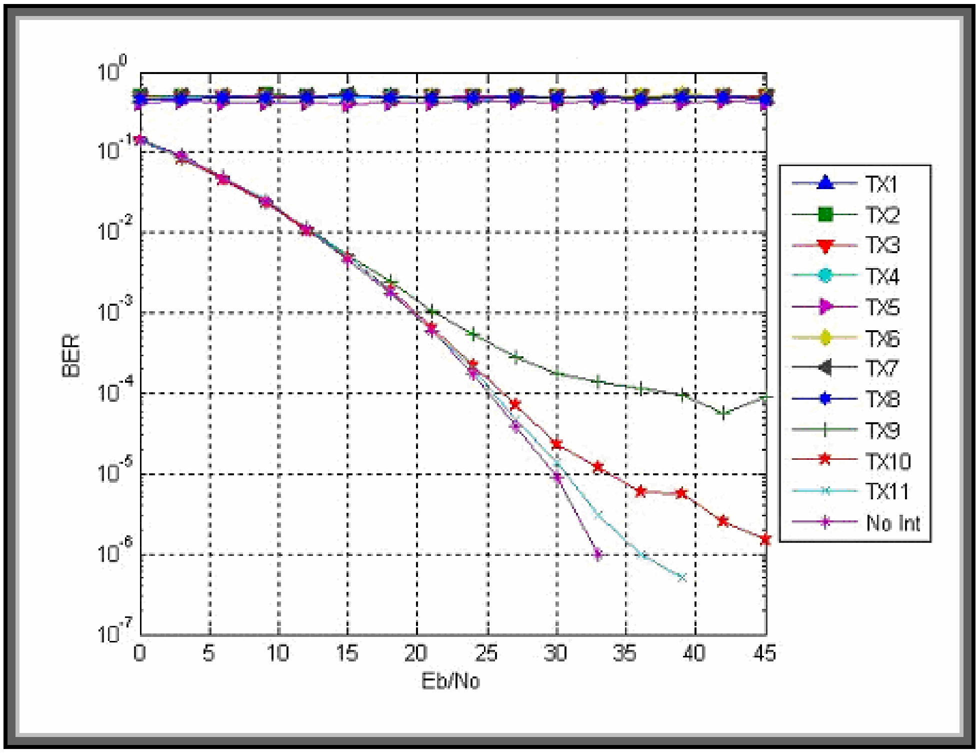


Figure 5.25 – Bluetooth Transmitter #11 with Bluetooth Interferers

One distinction from the previous two interferers though is that Bluetooth in the presence of another Bluetooth device seems to be a much harsher interferer than it was for the other two protocols. Now instead of the Bluetooth interferer hardly affecting the performance, it affects the performance as much, if not more than the other two interferers.

Chapter 6

Summary and Future Work

6.0 Summary

The finding from the general channel models and those of the site-specific channel model yield results which both reinforce while at the same time contradict each other. This effect can be explained due to the power levels that were assumed in each of the two different simulations. For the AWGN and Rayleigh fading of the general channel models, the relative powers of the three protocols were assumed to be equal, thus allowing for the variation of the interferer power level to determine the range of operability. On the other hand, in the site-specific channel model, the power level of both the signal and interferer were fixed according to their respective operating point. Therefore for the general channel models, the power is the variable, whereas in the site-specific model, the propagation paths between the transmitter and receiver are the variable, thus the characteristics of the physical environment influence the performance.

The effects of Bluetooth as an interferer will be studied first followed by the response of Bluetooth to interfering devices. For the most part, throughout all three channel models, the two generalized forms and also the site-specific model, Bluetooth intruded upon the performance of the other devices the least. This means that Bluetooth is a “good neighbor” and allows for the co-existence of devices within this frequency band. This statement can be attributed to the fact that Bluetooth not only transmits at a relatively low power level, 4 dBm, but also to the frequency hopping nature of the scheme in which Bluetooth employs. On average, most hops will not lie within the bandwidth of another signal. Even when these hops do occur within the wide bandwidth of Wifi, the nature of the narrowband signal that Bluetooth encompasses when compared to the wideband of Wifi, the effects are minimized when the Wifi signal is decoded.

When looking at the Bluetooth system in the presence of interferers, for the AWGN case, the performance is as good as Zigbee and better than Wifi, because of the minimal chance that the Bluetooth and the interferer are located within the same frequency space. However, the performance dips when the general Rayleigh channel is applied, more so than for Zigbee. Since the same flat fading effects are assumed to occur to each signal, this difference in performance can be attributed to the coding gain associated with the spreading of the Zigbee signal. When moving to the site-specific environment, Bluetooth shows the highest performance in the presence of a LOS signal or very strong single transmission NLOS signal. However, moving to the NLOS situations, Bluetooth becomes unable to overcome the effects of the interferers and performance is severely limited.

The overall performance of Zigbee in both the role of interferer and that of the transmitter is very similar to that of Bluetooth, although for different reasons. Zigbee does not seem to interfere with other devices because of its low radiated power level, being 4dBm below Bluetooth and 17dBm lower than Wifi. Zigbee also has a relatively small bandwidth, only 2 MHz, due to its low data rate, therefore the effects of Zigbee are also minimized upon a wide signal such as Wifi, and only occurs on 2 of the 79 channels of Bluetooth. That is why Zigbee did not appear to cause a significant disturbance to the other devices within the site-specific model.

When Zigbee is assumed to be the transmitting device, through the processing gain associated with the spreading of the Zigbee signal, it is able to defend itself from the effects of both the Bluetooth and Zigbee interferers with success, until the point that the interfering signal powers completely dominate the signal. Alternatively, because Wifi already begins with such a large power advantage over Zigbee, Wifi inadvertently hinders the performance of the Zigbee signal even when Zigbee has a LOS path to the receiver. Therefore the deployment of Zigbee devices within the presence of Wifi must be done with caution.

The final protocol, Wifi, has similar results between the general and specific cases when considering it as an interfering device. Wifi tends to limit the performance of other devices and does not allow for co-existence. In the general channel models, Wifi limits the performance of other transmitters due to its wide bandwidth and the likelihood for these devices to be located within the same frequency space. When moving to the site-specific scenario, this dominance is taken one step further due to the increased power advantage that Wifi has over the other protocols. Wifi limits the performance of a transmitting device long before the other interferers do. One reason for this can be attributed to the fact that Wifi was one of the first standards developed for products within the 2.4 GHz ISM band, therefore the presence of other devices was not considered. The only goal was to deliver the highest speed, along with the widest range possible.

When considering the effects that other devices have upon a transmitted Wifi signal, Wifi appears to be the least equipped to handle such interferers. In the case of the general channel models, Wifi is out-performed by the other two devices, by needing the highest SIR before being able to produce a detectable signal. Wifi seems to be sensitive to the small changes in the signal caused by an interferer. This result is shadowed in the results of the site-specific channel model due to the advantage in power that Wifi has over the interferers. Wifi uses a brute-force technique to obtain data communication, by just overpowering all other devices. The only interferer that can hinder the performance of a LOS Wifi transmitter is another Wifi device. Wifi cannot be completely blamed for this fault because at the time Wifi was being developed, mass production of other devices occupying the same frequency range as Wifi had not begun. In order to achieve a more efficient use of the ISM band, when other devices are produced they must make a conscience effort to minimize the effects that their device will have on the interference caused to other devices, similar to the way Bluetooth and Zigbee accomplish this, otherwise the entire band will suffer due to a degradation in the amount of throughput because of the amount of time a device must wait before being able to access a clear channel.

6.1 Future Work

Techniques for updating the current simulation have already been examined and implemented. Using the same floorplan layout, an increase in the number of transmitters and receivers has been accomplished, thus allowing for a greater coverage of the entire layout from which a more diverse set of results can be used to draw conclusions from. The new layout includes thirty-two transmitters, almost triple the original number of eleven previously used, also the number of receivers has been increased from one to fifteen. This produces an increase in the number of available BER curves from 99 to 4320. Figure 6.1 shows the location of the transmitters and receivers within the building floorplan, although the resulting BER curves have not yet been simulated, all procedures are completed for them to be conducted.

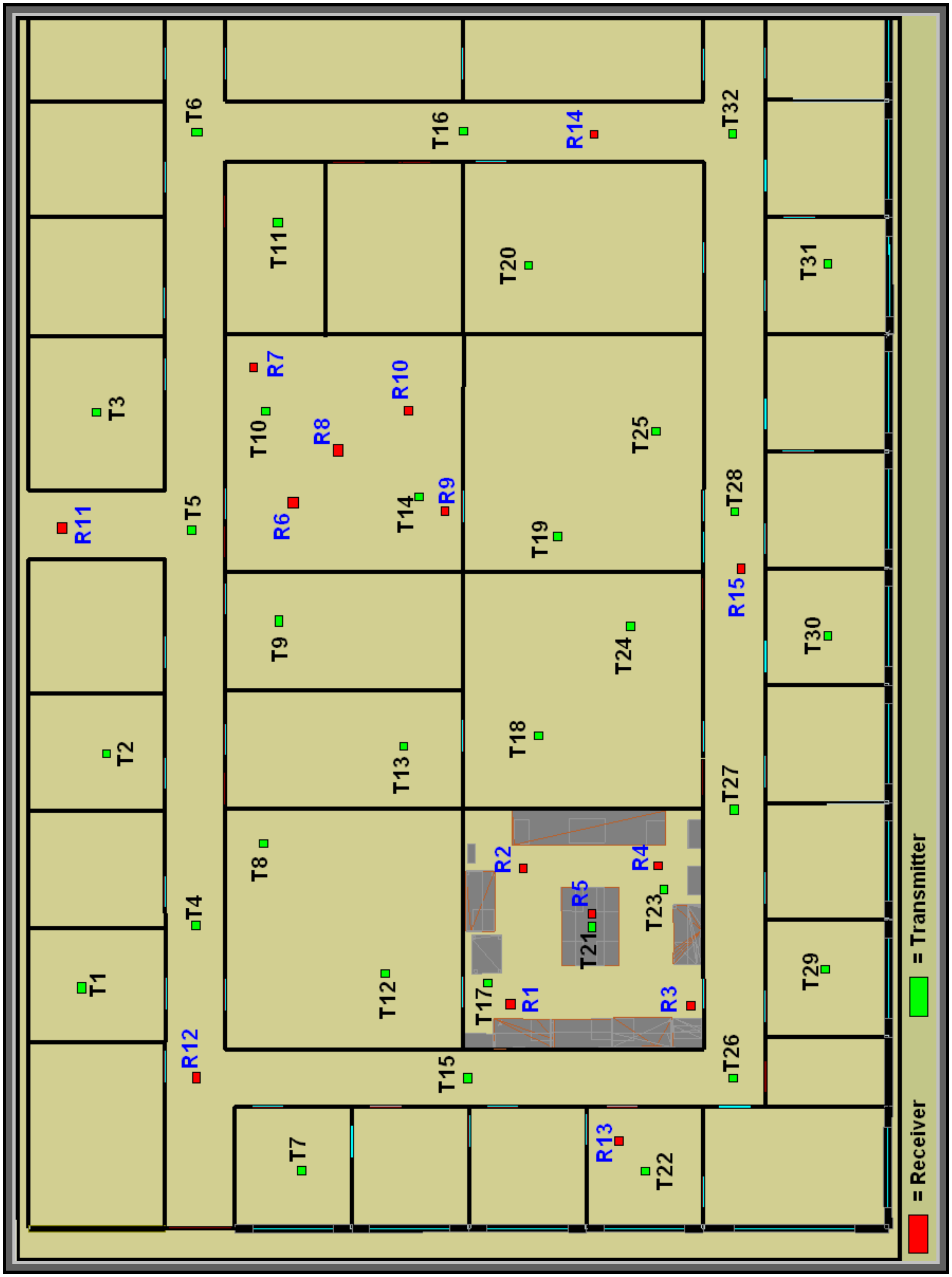


Figure 6.1 - Revised Tx/Rx Locations

Additional means to improve the current simulation can be grouped into two main categories. One category is a way to decrease the execution time of a simulation without having an effect on the performance of the system, and the second category contains ways in which the results of the simulation can be enhanced and thus become more reliable. After presenting the methods to improve the current simulation, a look into a totally different simulation process will be explored in which a highly advanced and effective technique could be enacted.

The first section to be discussed is ways in which the current simulation could become more efficient without changes to the results occurring. These techniques deal primarily with two of the receivers, the Zigbee and the Wifi receiver. These are two of the places where the simulations appear to bottleneck, with the Zigbee receiver impeding the performance much more so than the Wifi receiver.

The correlators found within the decoding of the Zigbee message hinder the speed performance of the Zigbee receiver. There are a total of 32 different correlations that must occur over the sixteen chips for in both the I and Q phase, so that one four bit symbol can be obtained. There is no algorithm that can be invoked such as will be seen for the Wifi receiver, therefore the correlators are necessary. However, if the process used within the correlators could be performed in parallel, the execution time could, in essence, be reduced by a factor of sixteen. The method of completing this task can feasibly be accomplished through the use of matrix algebra, although for this project, time did not permit to delve into such a task, therefore the improvement was secondary since it would not change the results. Nevertheless, for future simulations, this step would be vital to reduce the execution runtime of a single simulation using the Zigbee receiver from a few days to possibly a few hours.

As mentioned before, there is an algorithm that could be implemented to improve upon the efficiency of the Wifi receiver. The algorithm is commonly referred to as the Fast Walsh Transform (FWT). The FWT uses a butterfly technique in a similar manner as the one used for an FFT. The block diagram of the FWT can be found in Figure 6.2 taken from a Linksys white paper.[15] This technique reduces the combination of the number of multiplications and additions, thus allowing for a more effective method of simulation. Due to the limitations on time, coupled with the fact that the improvement in runtime was not significant for the number of simulations being performed, this upgrade was set aside so that the overall goal of the project could be realized.

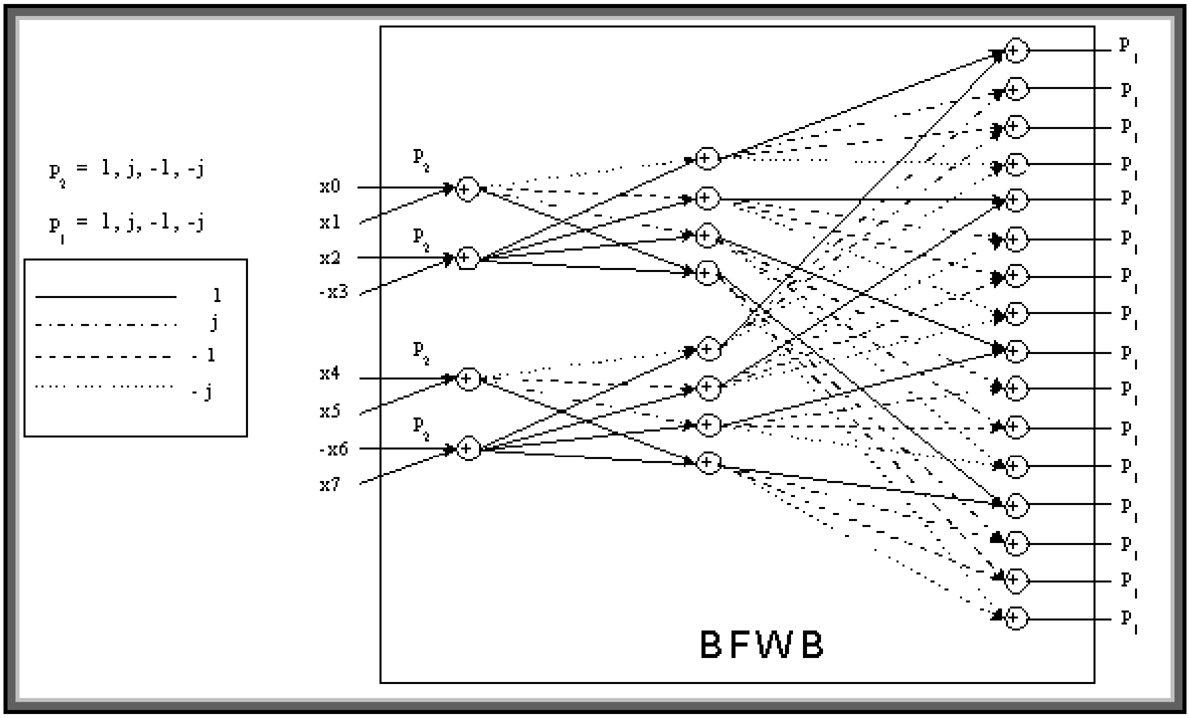


Figure 6.2 - Basic Fast Walsh Block

The second method, which is a way the simulation model can be improved to obtain better results, deals with the simulation of the GFSK system of Bluetooth. This system was modeled after a GMSK modulation technique, which is used on the GSM system for cellular phones, the difference between the two being the parameter for the modulation index, h. For the GFSK system of Bluetooth, h, is set to 0.35. For the modulation system for GSM, which is GMSK, h is equal to 0.5. Both the GMSK and GFSK systems use FSK modulation, however, when h is equal to 0.5, the FSK system can be modeled as MSK because of the minimum frequency separation. Although the approximation of assuming the GFSK had a modulation index of 0.5 is not true, it was suitable to make for the current simulation because of the need for the modulation to be in the direct and quadrature form. In order for the system to become more realistic, consideration of the GFSK system with a modulation index of 0.35 needs to be performed.

Although the Monte Carlo simulation is a very practical and widely used technique, the way in which the simulation could be greatly enhanced would be through the simulation of not only the physical layer of the protocols but also incorporate parts of their MAC layers as well. This would include using packets, CSMA/CA, and channel selection. Because of the complexion of incorporating all of these different details into the simulation, it might prove to be more effective to simulate the system in hardware rather than the present simulation which in done in software.

The vision of how the simulation should be implemented is as follows. Although numerous devices could be present, at the moment only three, one of each protocol, shall be regarded. Each protocol will have almost all of their characteristics fully simulated. For instance, Zigbee will be transmitting at 0dBm with half sine pulse shaping, to go along with Bluetooth having Gaussian pulses being transmitted at 4dBm. The protocols will consist of transmitting bits grouped into packets with the appropriate headers and other parameters specified in their standards. This will result in obtaining packet error rates along with information on the performance using the parameter of throughput. The FEC techniques for the individual standards could also be incorporated into the simulations to yield a more realistic packet error rate.

Once the simulation for each individual device has been created, the three protocols can be introduced into the system. First, the total 83.5 MHz spectrum of the ISM band should be considered. Bluetooth will follow its randomly generated hopping sequence to go from one channel to another. Zigbee and Wifi will both check the entire number of channels available and select a clear channel to transmit on. This is different from the current method in which it is assumed that the interferers could possibly be constantly changing channels thus leaving an on average result. In the new simulation, if all systems are operating within acceptable tolerances, then more devices can be added. This addition can continue until all channels are occupied for both the Wifi and Zigbee devices meaning that once more devices are added, two or more devices of the same protocol may be operating on the same channel, along with any interferers located in the frequency range. This will either result in more packets being in error due to the interference, less throughput do to the devices not being able to access the channel because of the “listen before talk” nature of the CSMA/CA not allowing the devices to transmit, or both. Going on step further, rather than only looking at individual devices, the devices could be used within their own piconets and be transmitting and receiving at the specified times as determined by the master devices. In either case, a more realistic depiction of what is occurring within the ISM band when considering interference would be presented. However, because of this added complexity and number of devices, it can be seen that there would be a lot of computational power needed for such a simulation. Although the current simulation method is primitive, it is an effective starting point in realizing the effects that interference will have on the coexistence of the protocols conforming to the WLAN and WPAN standards in the 2.4 GHz ISM band.

References

[1] “Industrial Wireless Technology for the 21st Century,” U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy. December 2002.

[2] Kevin Werbach, “Radio Revolutions – The Coming Age of Unlicensed Wireless,” New Age American, Public Knowledge. Washington, D.C.

[3] David G. Brenner, *UWB: The new frontier of wireless*, WiQuest Communications, White Paper.

[4] “Special Report: Wireless Networking,” IEEE Spectrum, September 2003. pg 24-27.

[5] Willie D. Jones, “Ultrawide Gap On Ultrawideband,” IEEE Spectrum, January 2004. pg 30.

[6] Vikki Lipset, “802.16e vs. 802.20,” Wi-Fi Planet, September 2004. http://www.wi-fiplanet.com/columns/article.php/3072471

[7] ”IEEE Establishes New Standards Group of Raise Mobile Broadband Wireless Experience to LAN-Like Levels,” IEEE, 2003. https://standards.ieee.org/announcements/p80220app.html

[8]Christian Patachia-Sultanoiu, “Deploying WiMAX Certified Broadband Wireless Access Systems,” Journal of the Communications Network, 2004.

[9] Homepage of ZigBee™ Alliance, http://www.zigbee.org/

[10] Ed Callaway, P. Gorday, L. Hester, J.A. Gutierrez, M. Neave, B. Heile, V. Bahl, "Home networking with IEEE 802.15.4: A developing standard for low-rate wireless personal area networks," *IEEE Communication Magazine*, vol. 40, no. 8, pp. 70-77, August 2002.

[11] John Notor, Anthony Caviglia, Gary Levy, *CMOS RFIC Architectures for IEEE 802.15.4 Networks*, White Paper dated 2003.

[12] 802.15.4 Standard

[13] Leon W. Couch, II. *Digital and Analog Communication Systems*, Prentice Hall 2001.

[14] 802.11b Standard

[15] Vocal Technologies, Ltd. IEEE 80211b White Paper, White Paper dated October, 27 2003.

[16] Bob Pearson, Complementary Code Keying Made Simple, White Paper dated May 2000.

[17] 802.11a Standard

[18] Linksys, A Comparison of 802.11a and 802.11b Wireless LAN Standards, White Paper dated October 6, 2004.

[19] William H. Tranter, K. Sam Shanmugan, Theodore S. Rappaport, Kurt L. Kosbar. *Principles of Communication Systems Simulation with Wireless Applications*, Prentice Hall 2004.

[20] K.V.S.S.S.S. Sairam, N. Gunasekaran, S. Rama Reddy, "Bluetooth in Wireless Communication," *IEEE Communication Magazine*, pp. 90-96, June 2002.

[21] Bluetooth Website – www.bluetooth.org

[22] Tech Lab Review Staff, “Bluetooth, ready for the big leagues?” *Tech-Edge.* October 31, 2002. http://homepage.mac.com/techedgeezine/networking_bluetooth1.htm

[23] Bluetooth Standard – 802.15.1 Standard

[24] Anthony C. Davies, *An overview of Bluetooth Wireless Technology^{TM} and some competing LAN Standards*, White Paper.

[25] Patricia McDermott-Wells, "What is Bluetooth?" *IEEE Potentials*, pp. 33-35, December 2004/January 2005.

[26] Theodore S. Rappaport. *Wireless Communications Principles and Practice*, Prentice Hall 2002

[27] Todor Cooklev, *Wireless Communication Standards – A Study of IEEE 802.11^{TM}, 802.15^{TM}, and 802.16^{TM},* IEEE 2004.

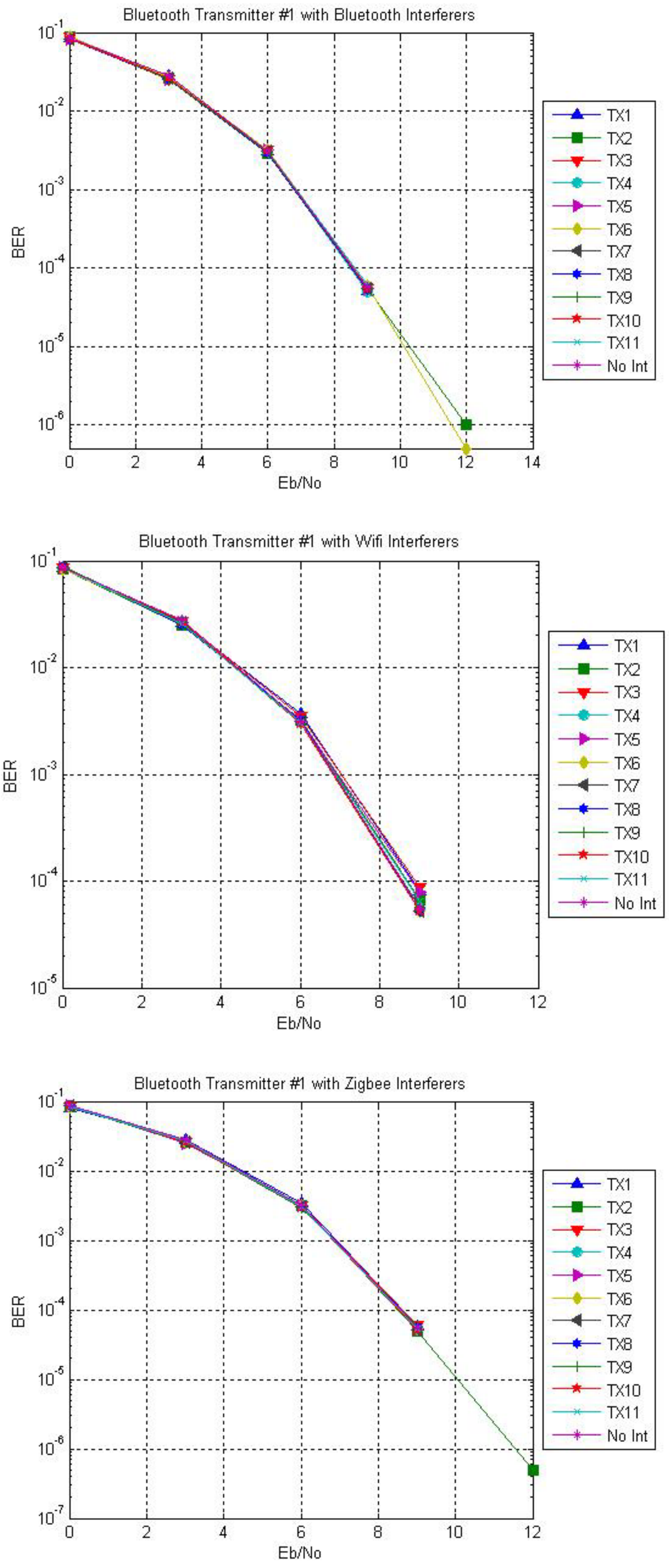
[28] Pravin Bhagwat, "Bluetooth: Technology for Short-Range Wireless Apps," *IEEE Internet Computing*, pp. 96-103, May/June 2001.

[29] T. Karhima, A. Silvennoinen, M. Hall, S.G. Haggman, "IEEE 802.11B/G WLAN Tolerance to Jamming," MILCOM Conference, 2004.

[30] C. Andren, M. Webster, "CCK Modulation Delivers 11 Mbps for High Rate IEEE 802.11 Extension," Wireless Symposium/Portable by Design Conference, Spring 1999.

Appendix

Site-Specific Channel Model BER Curves


Bluetooth Transmitter #1 with Bluetooth Interferers

Bluetooth Transmitter #1 with Wifi Interferers

Bluetooth Transmitter #1 with Zigbee Interferers

Figure A.1 - Bluetooth Tx #1

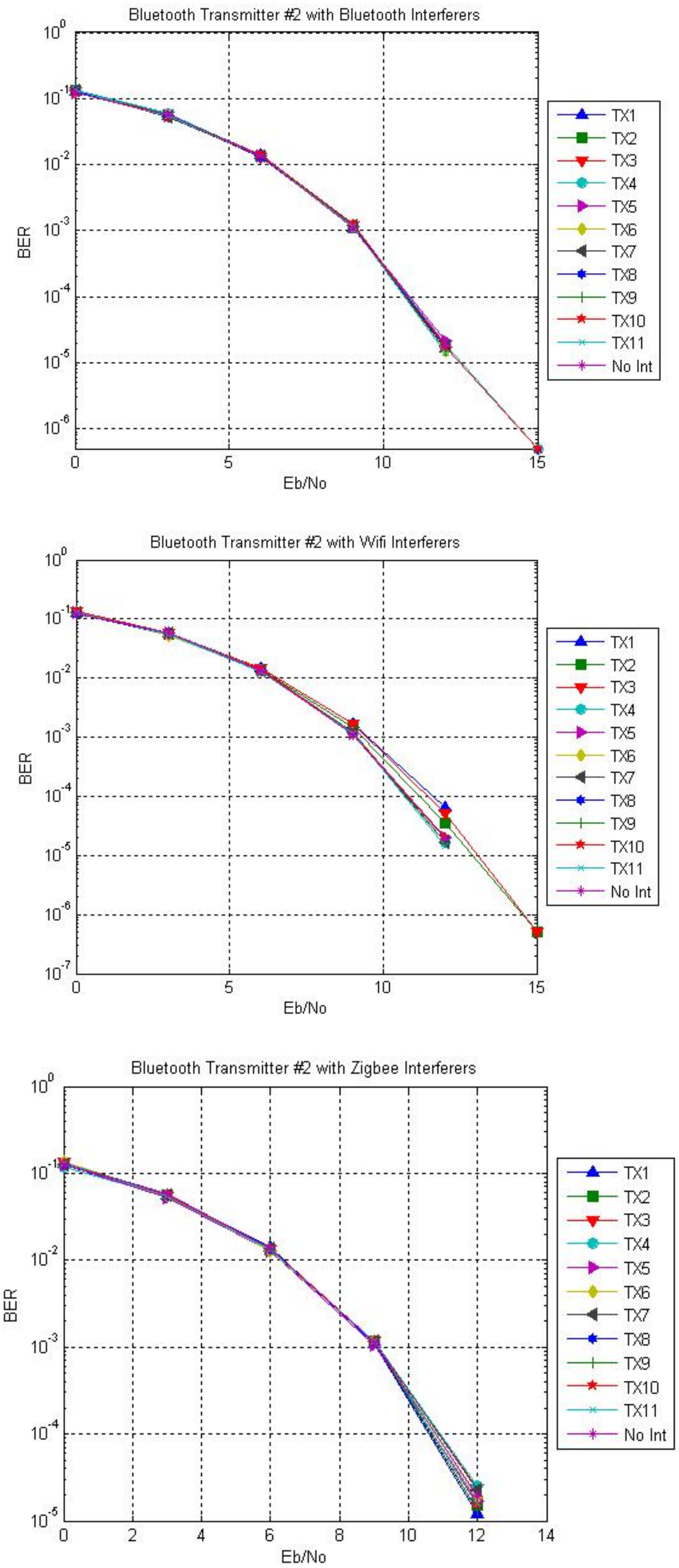
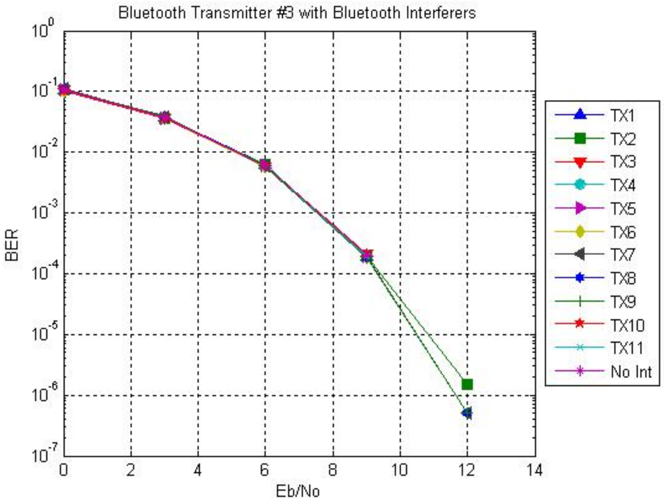
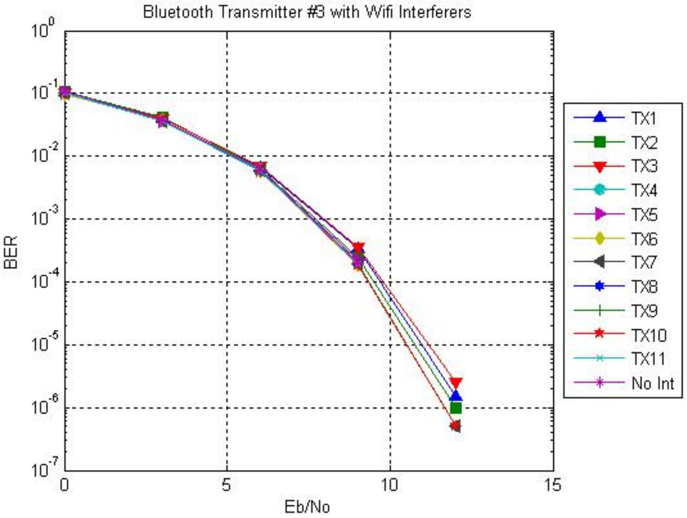


Figure A.2 - - Bluetooth Tx #2





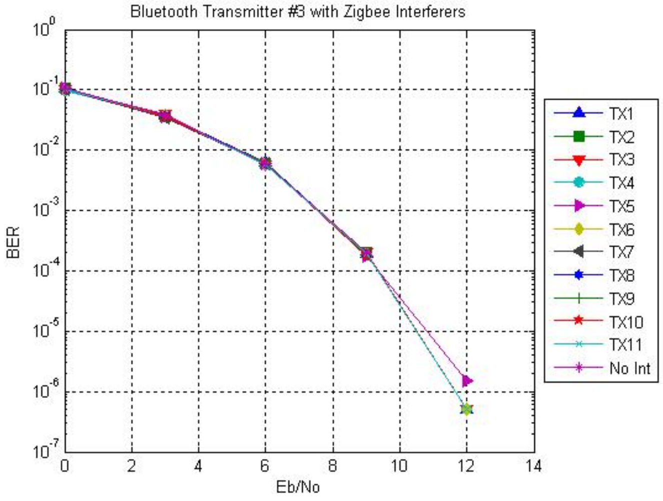
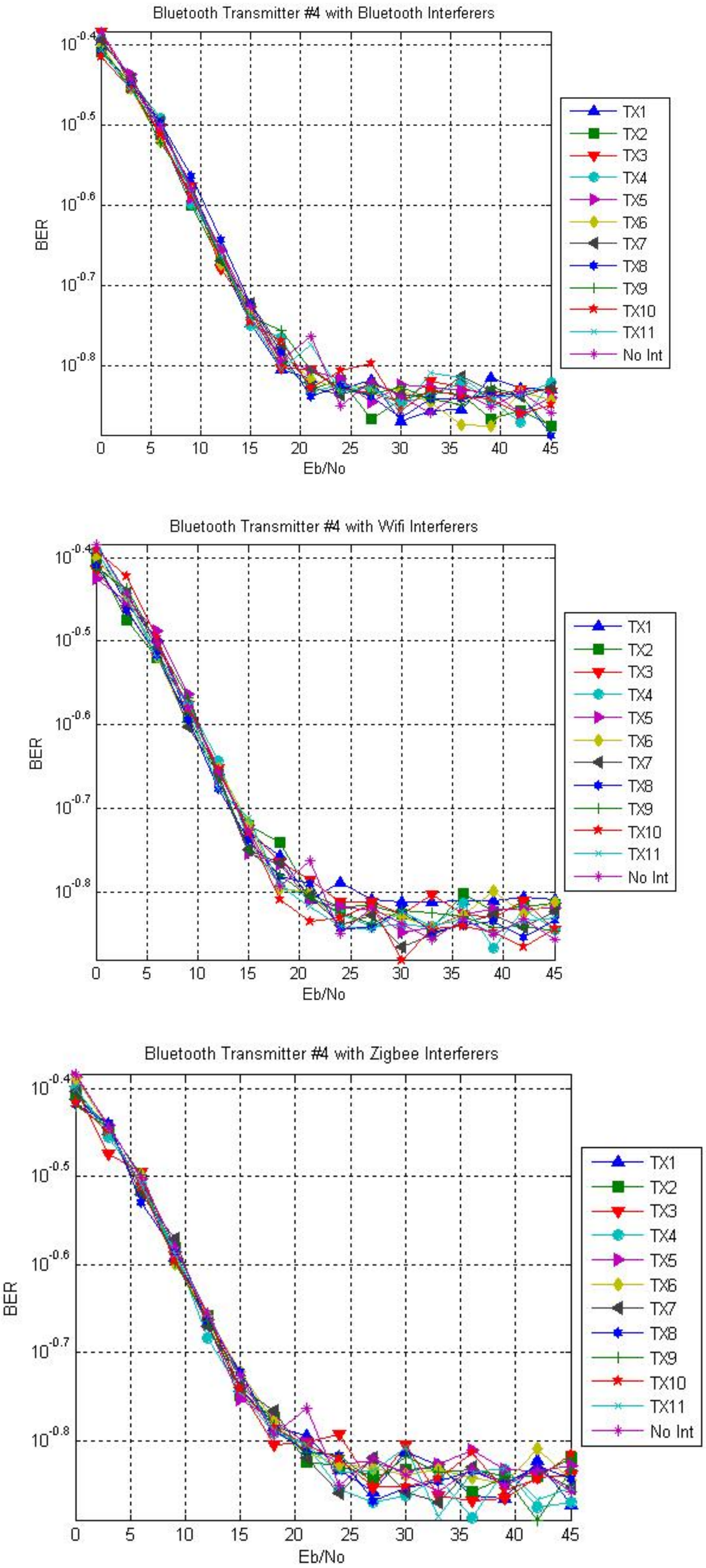


Figure A.3 - Bluetooth Tx #3



Bluetooth Transmitter #4 with Bluetooth Interferers

Bluetooth Transmitter #4 with Wifi Interferers

Bluetooth Transmitter #4 with Zigbee Interferers

Figure A.4 - Bluetooth Tx #4

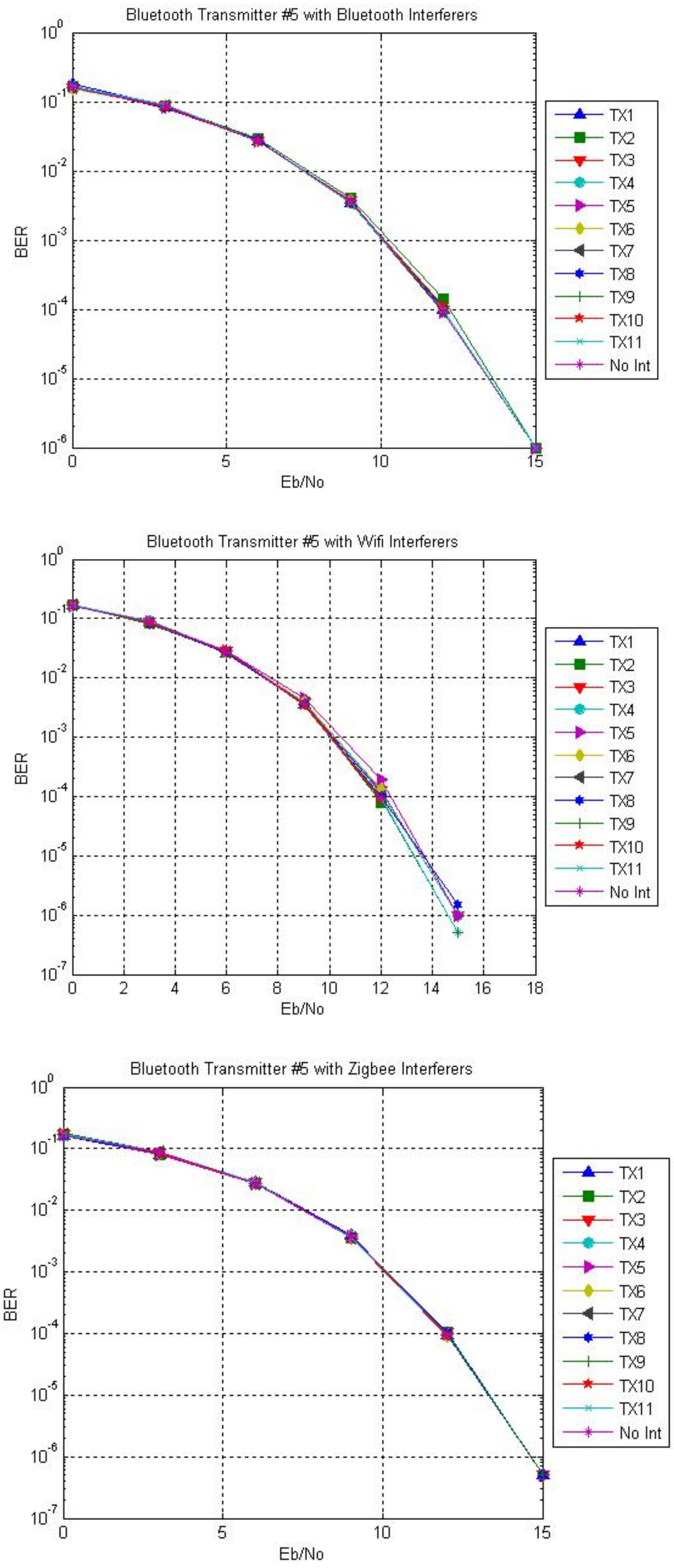
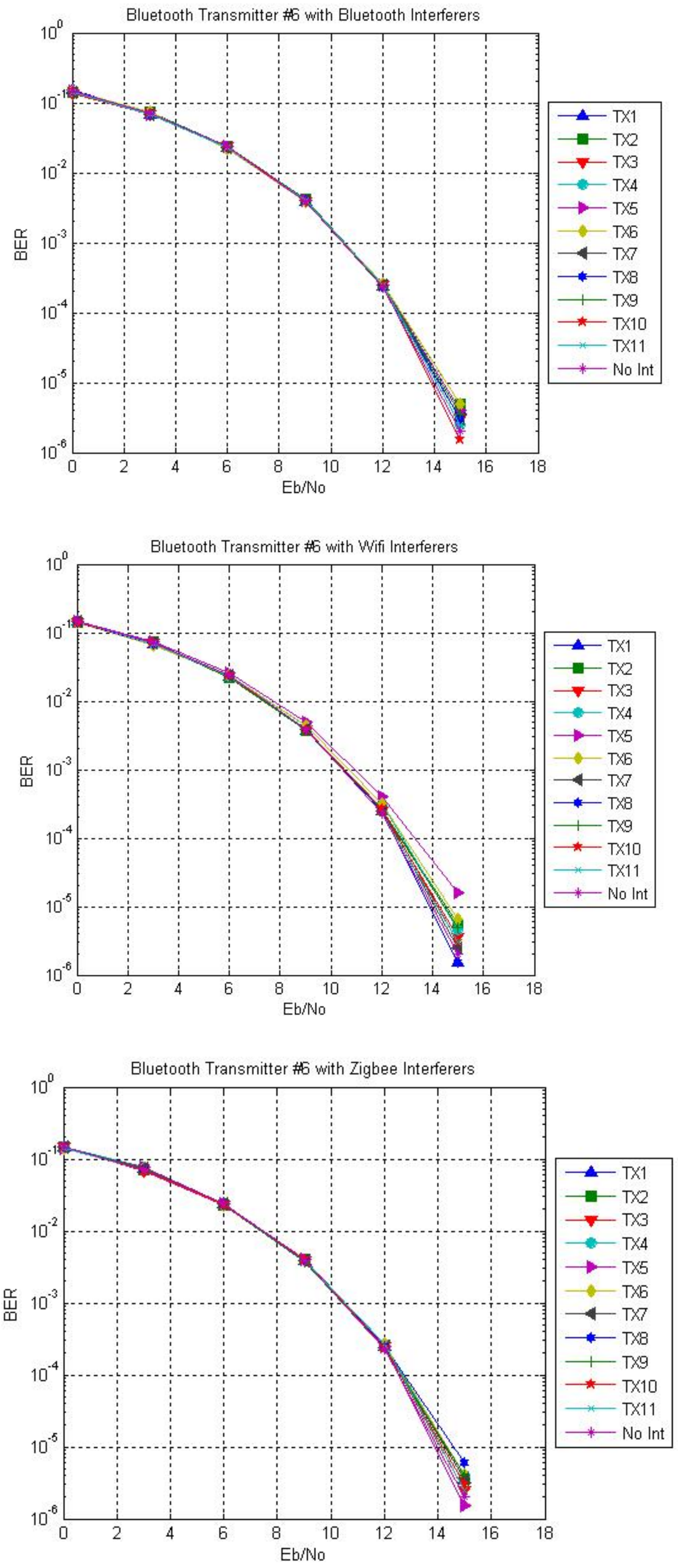


Figure A.5 - Bluetooth Tx #5

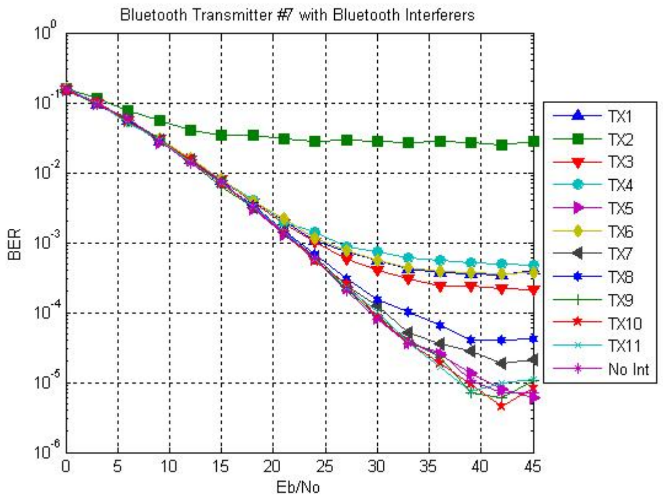


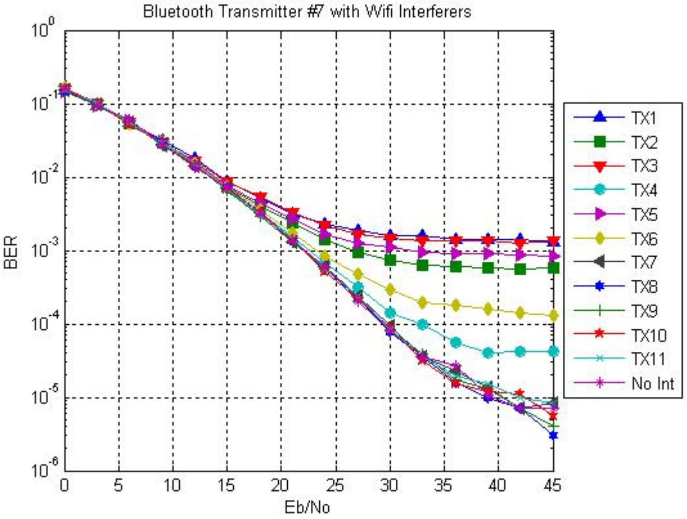
Bluetooth Transmitter #6 with Bluetooth Interferers

Bluetooth Transmitter #6 with Wifi Interferers

Bluetooth Transmitter #6 with Zigbee Interferers

Figure A.6 - Bluetooth Tx #6





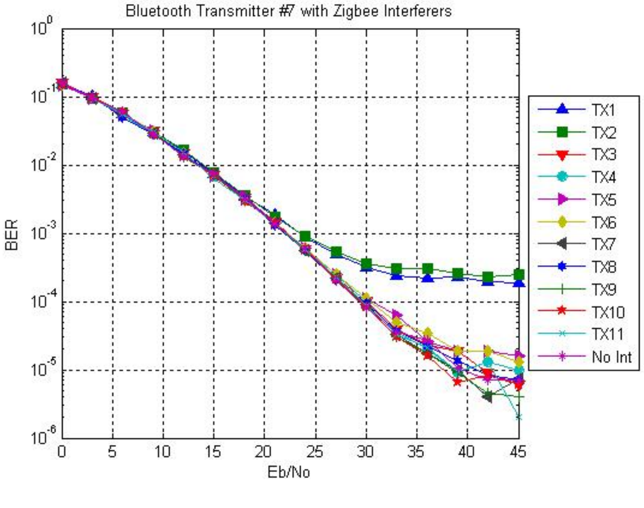
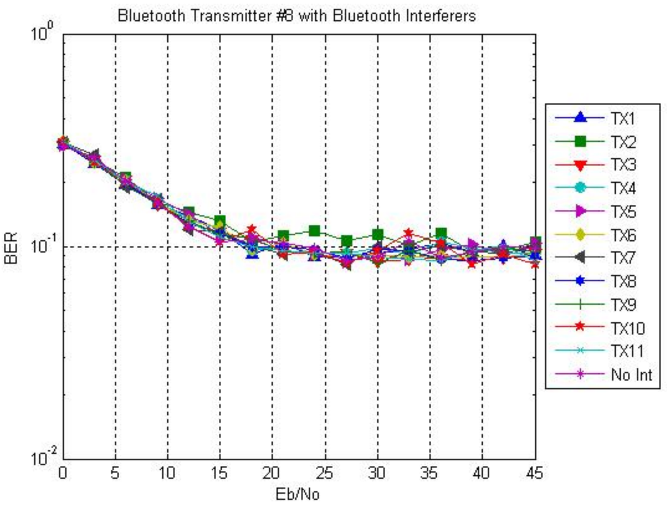
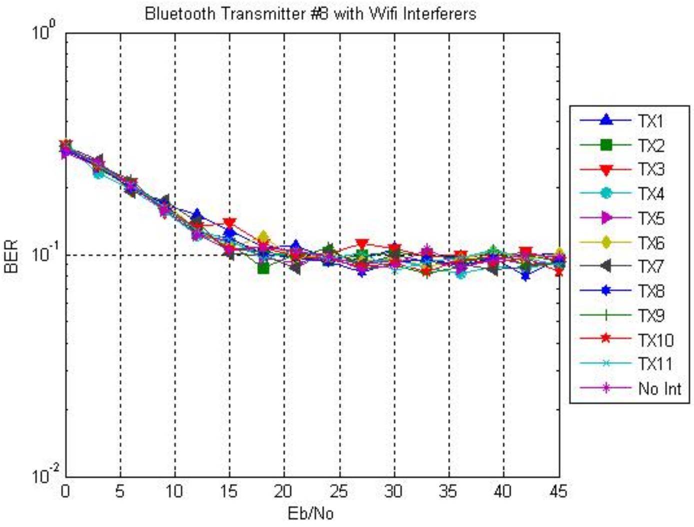


Figure A.7 - Bluetooth Tx #7





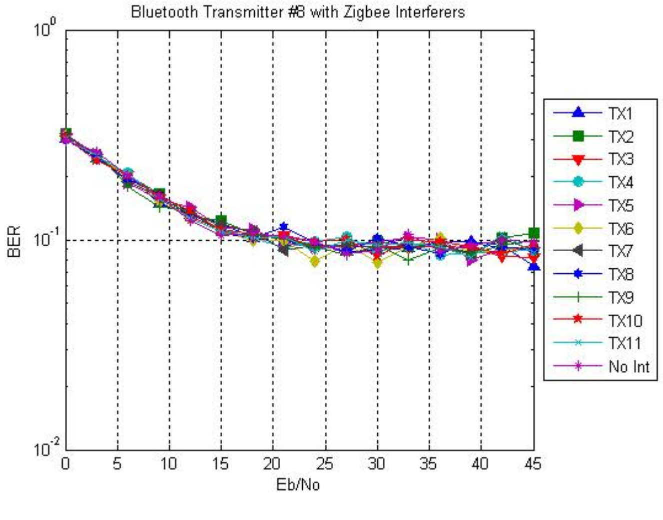


Figure A.8 - Bluetooth Tx #8

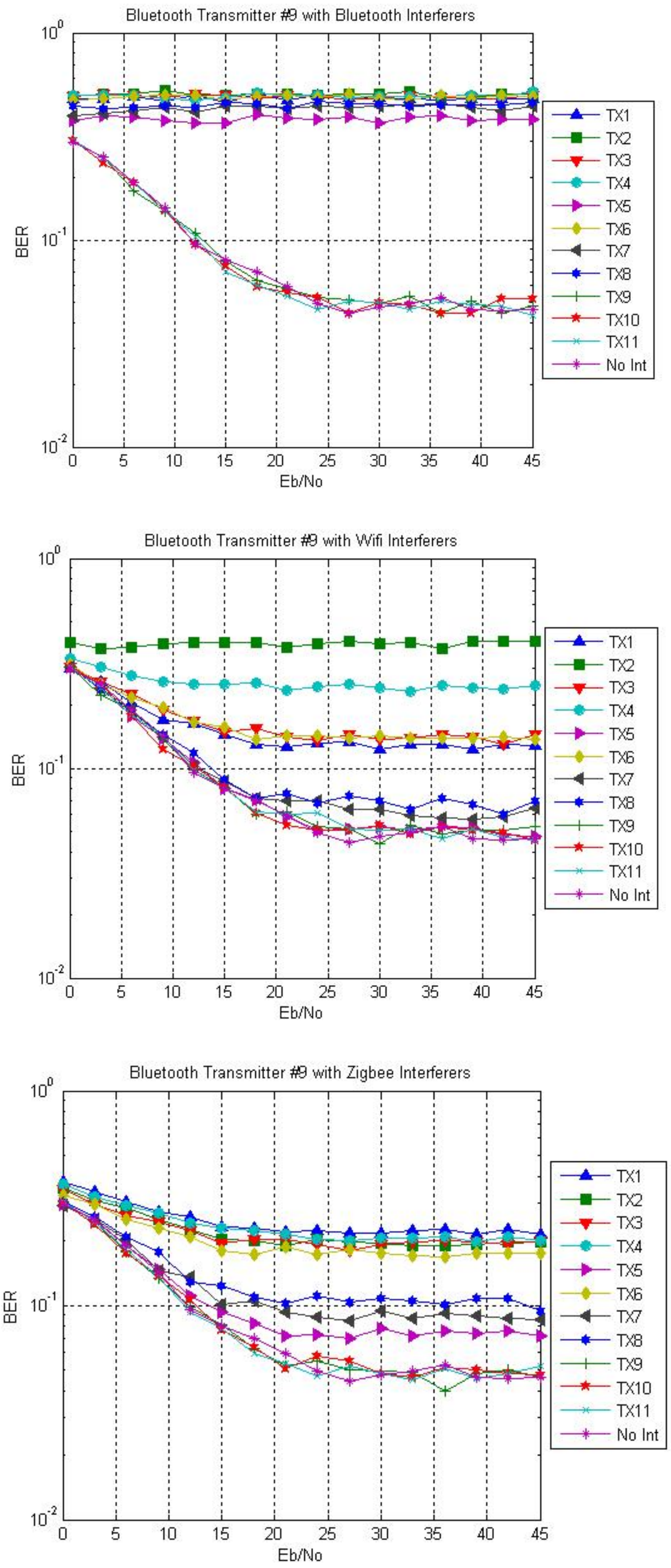
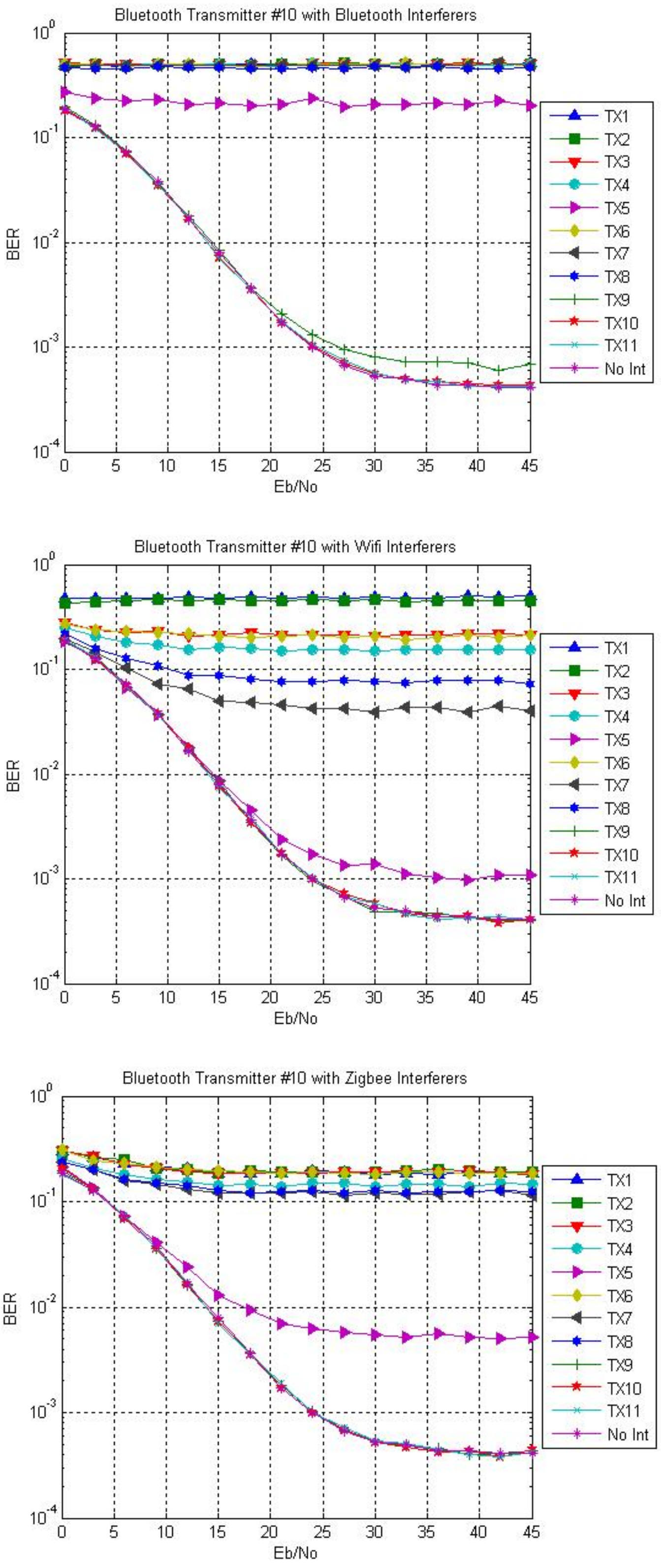


Figure A.9 - Bluetooth Tx #9



FigureA.10 - Bluetooth Tx #10

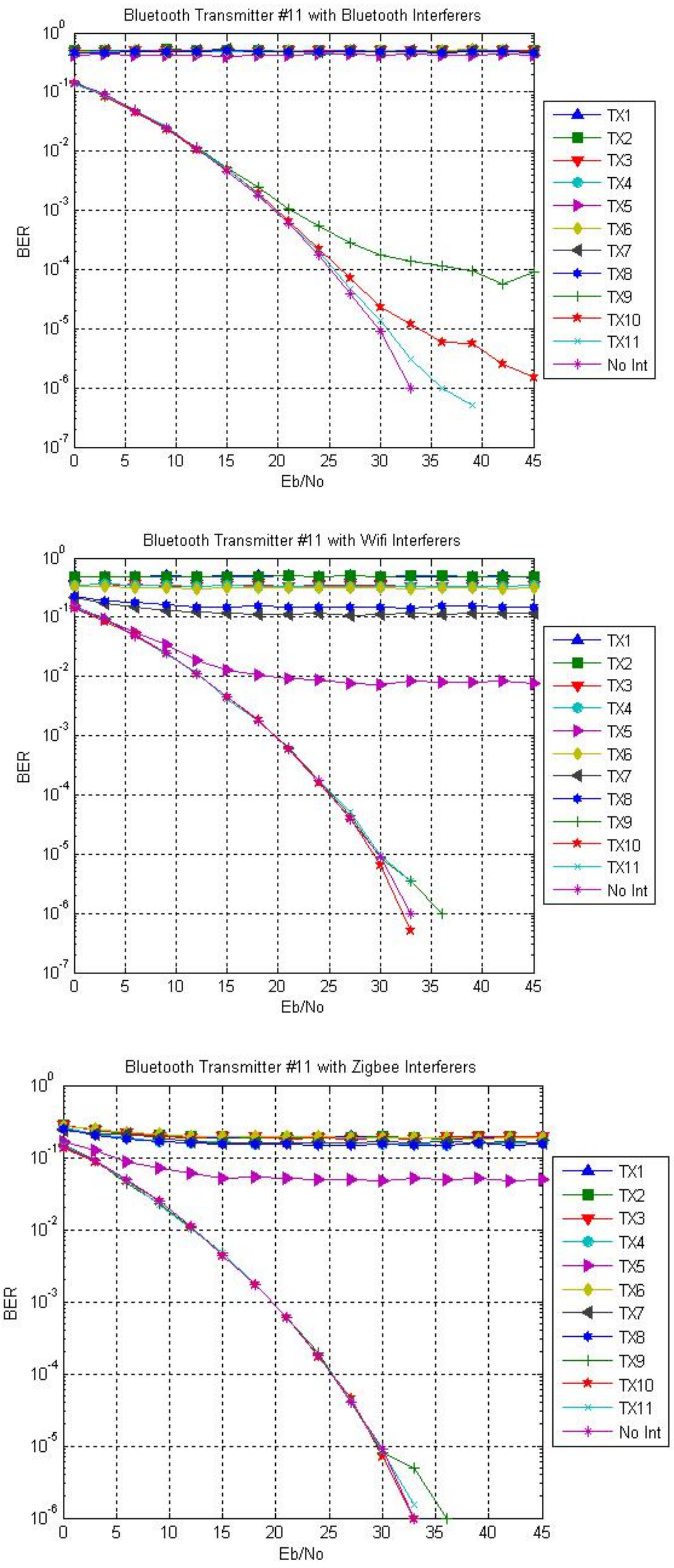
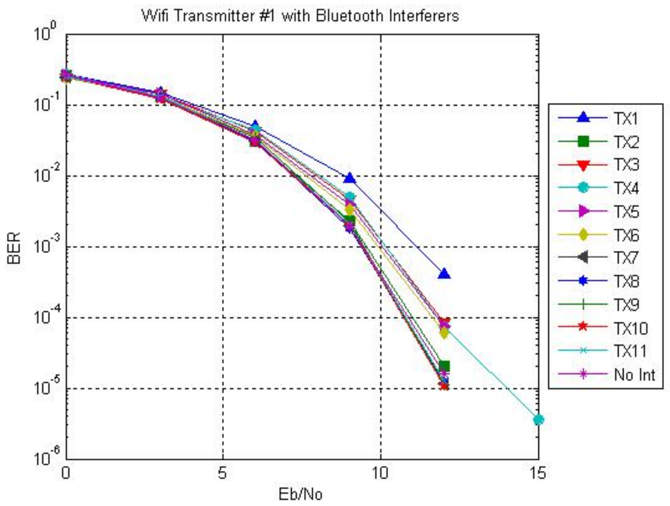
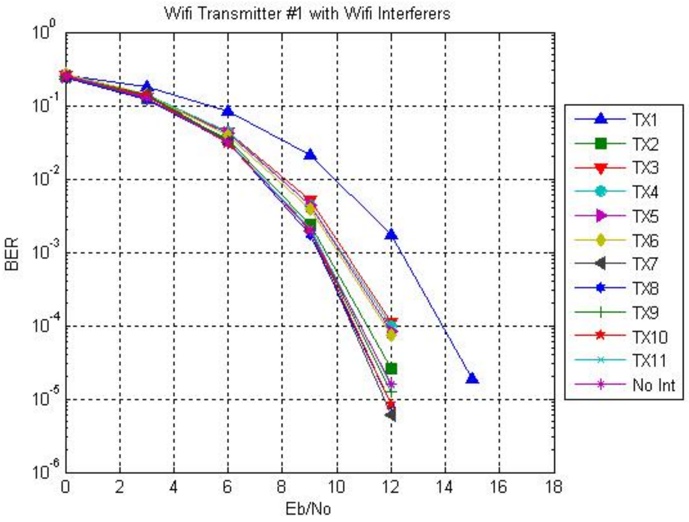


Figure A.11 - Bluetooth Tx #11





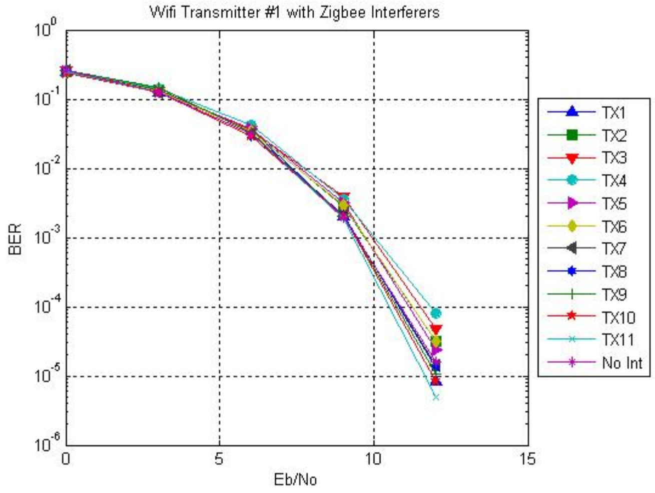
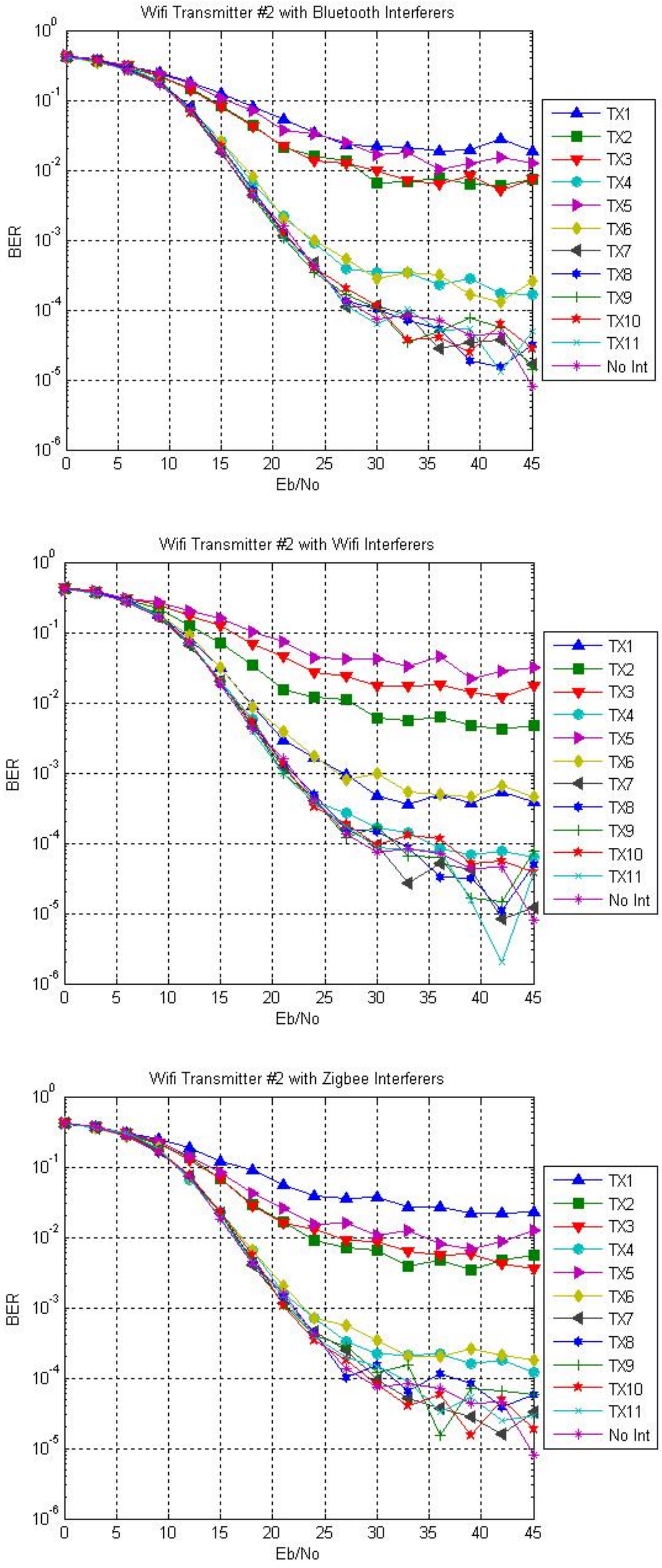


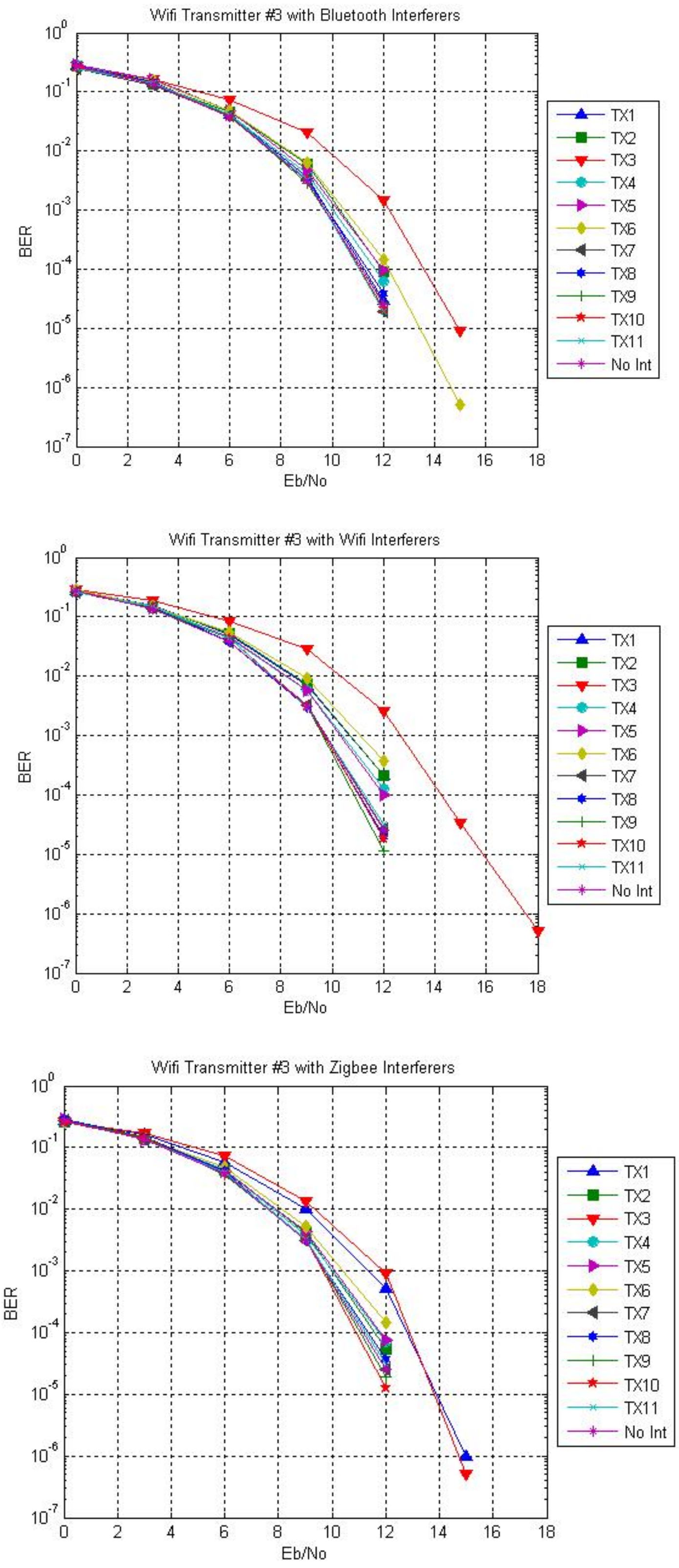
Figure A.12 - Wifi Tx #1


Wifi Transmitter #2 with Bluetooth Interferers

Wifi Transmitter #2 with Wifi Interferers

Wifi Transmitter #2 with Zigbee Interferers

Figure A.13 - Wifi Tx #2


Wifi Transmitter #3 with Bluetooth Interferers

Wifi Transmitter #3 with Wifi Interferers

Wifi Transmitter #3 with Zigbee Interferers

Figure A.14 - Wifi Tx #3

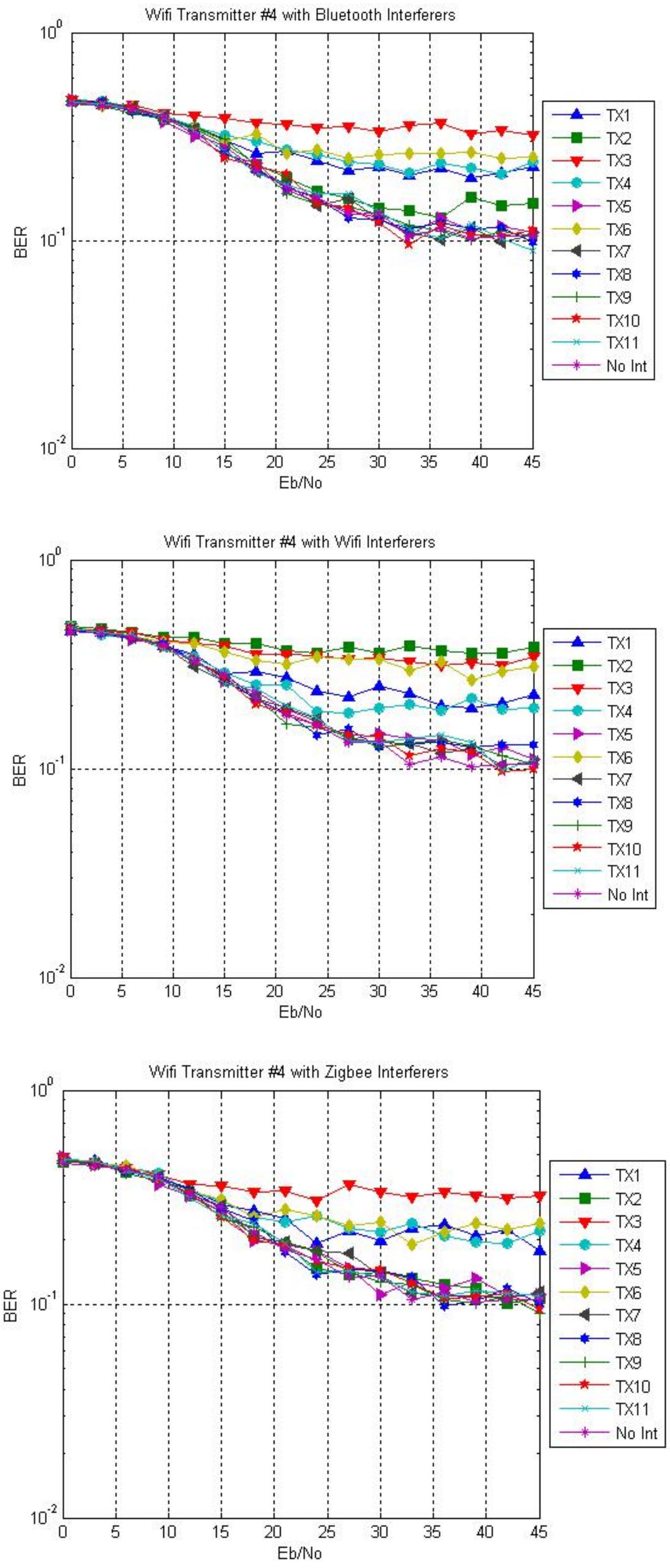


Figure A.15 - Wifi Tx #4

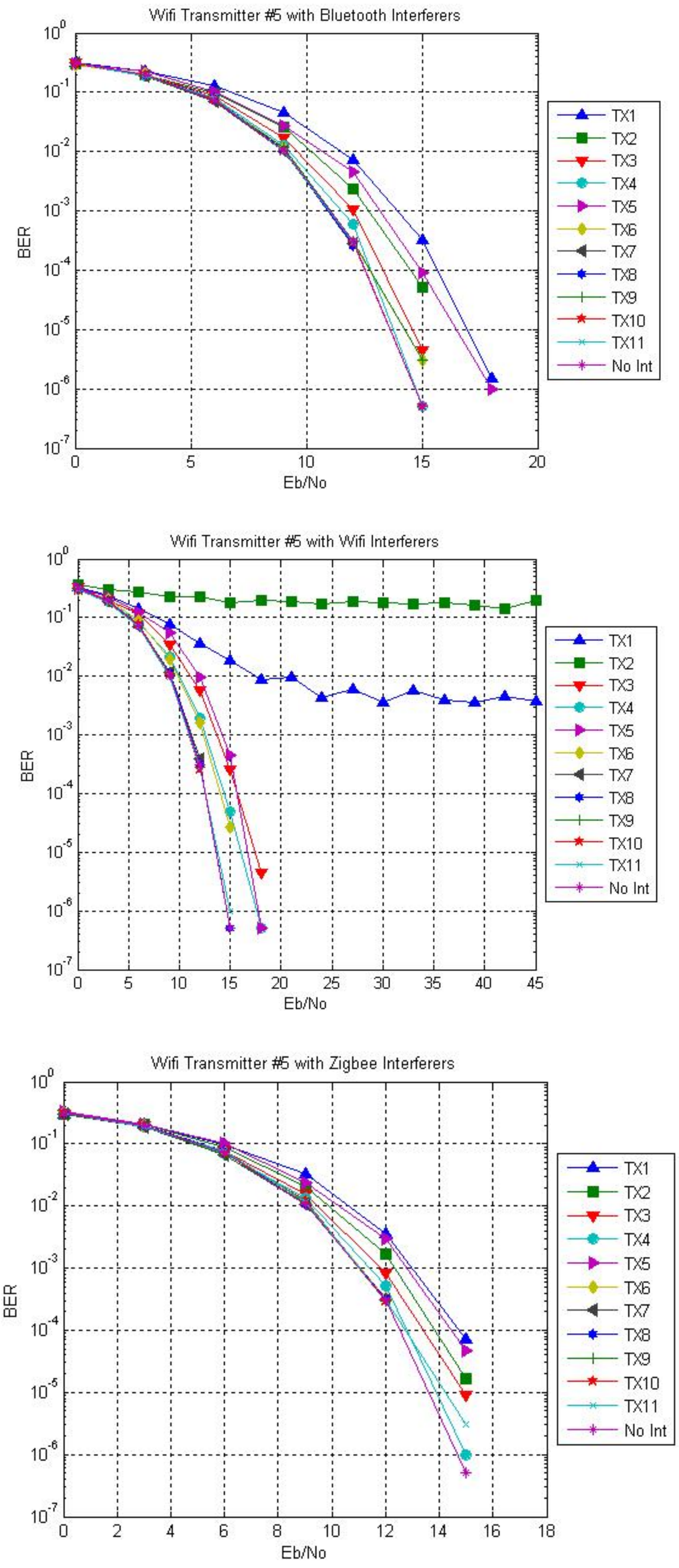
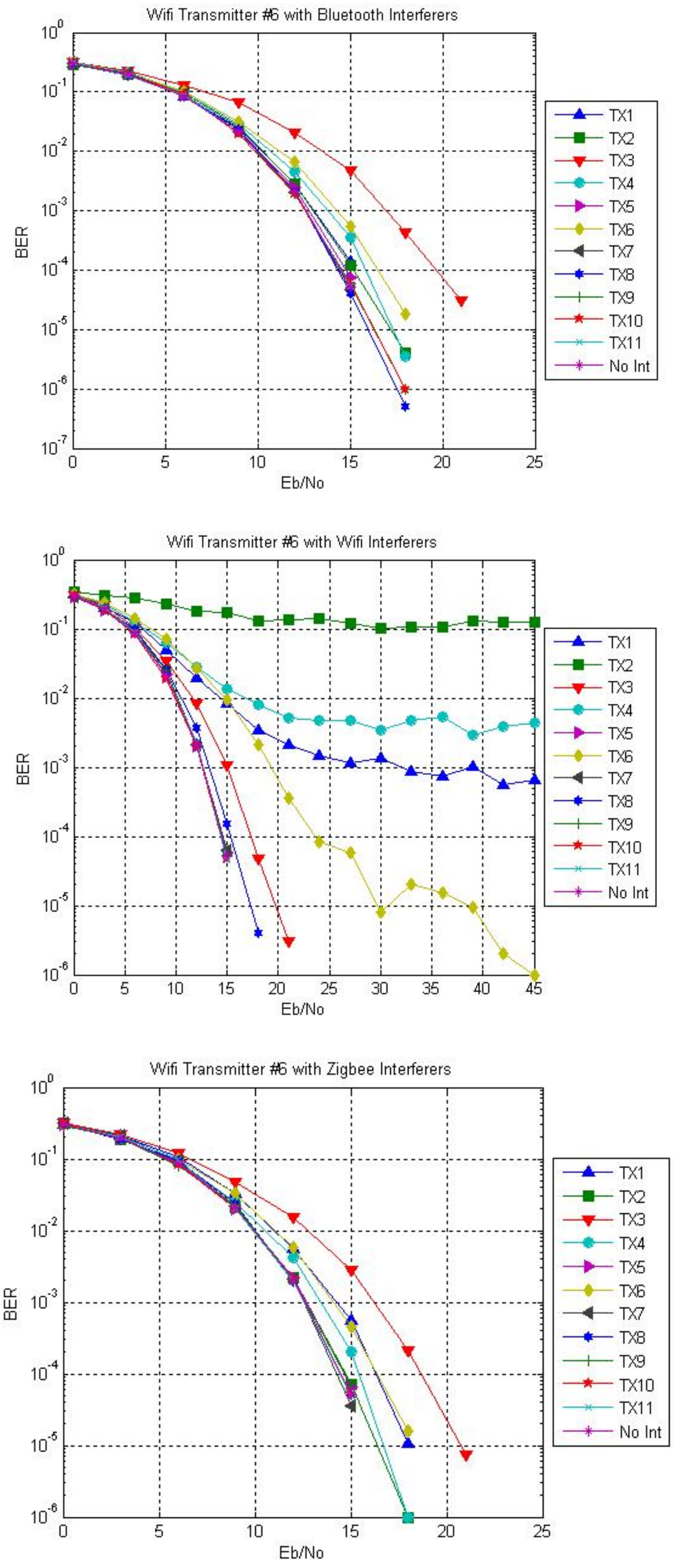


Figure A.16 - Wifi Tx #5



Wifi Transmitter #6 with Bluetooth Interferers

Wifi Transmitter #6 with Wifi Interferers

Wifi Transmitter #6 with Zigbee Interferers

Figure A.17 - Wifi Tx #6

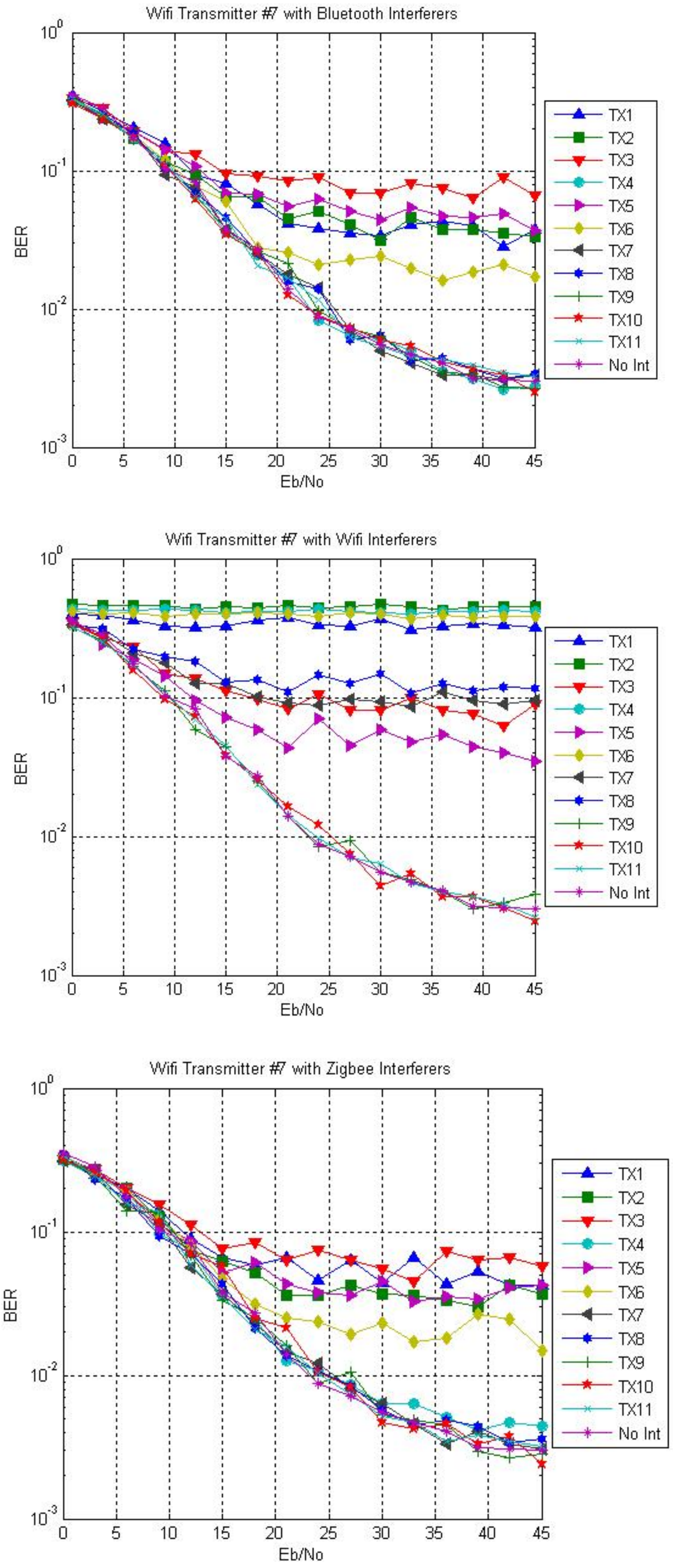


Figure A.18 - Wifi Tx #7

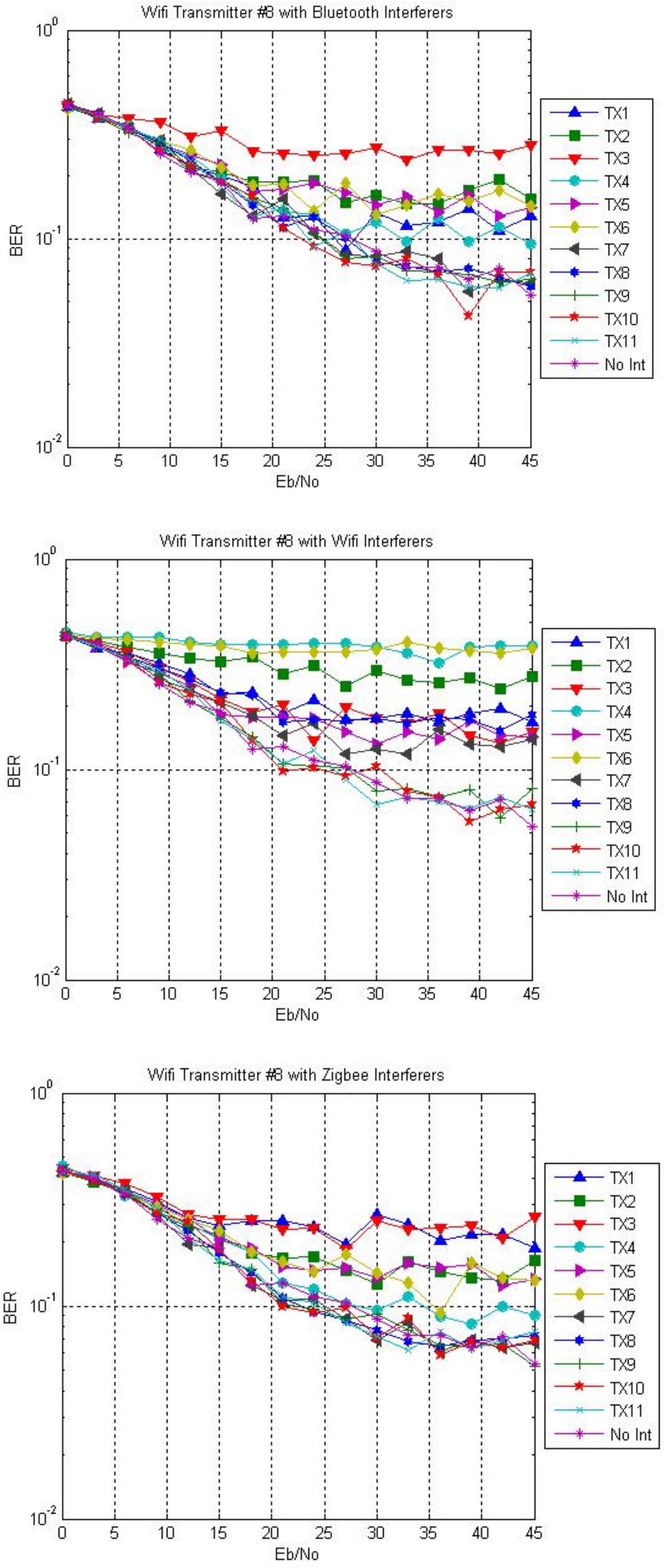
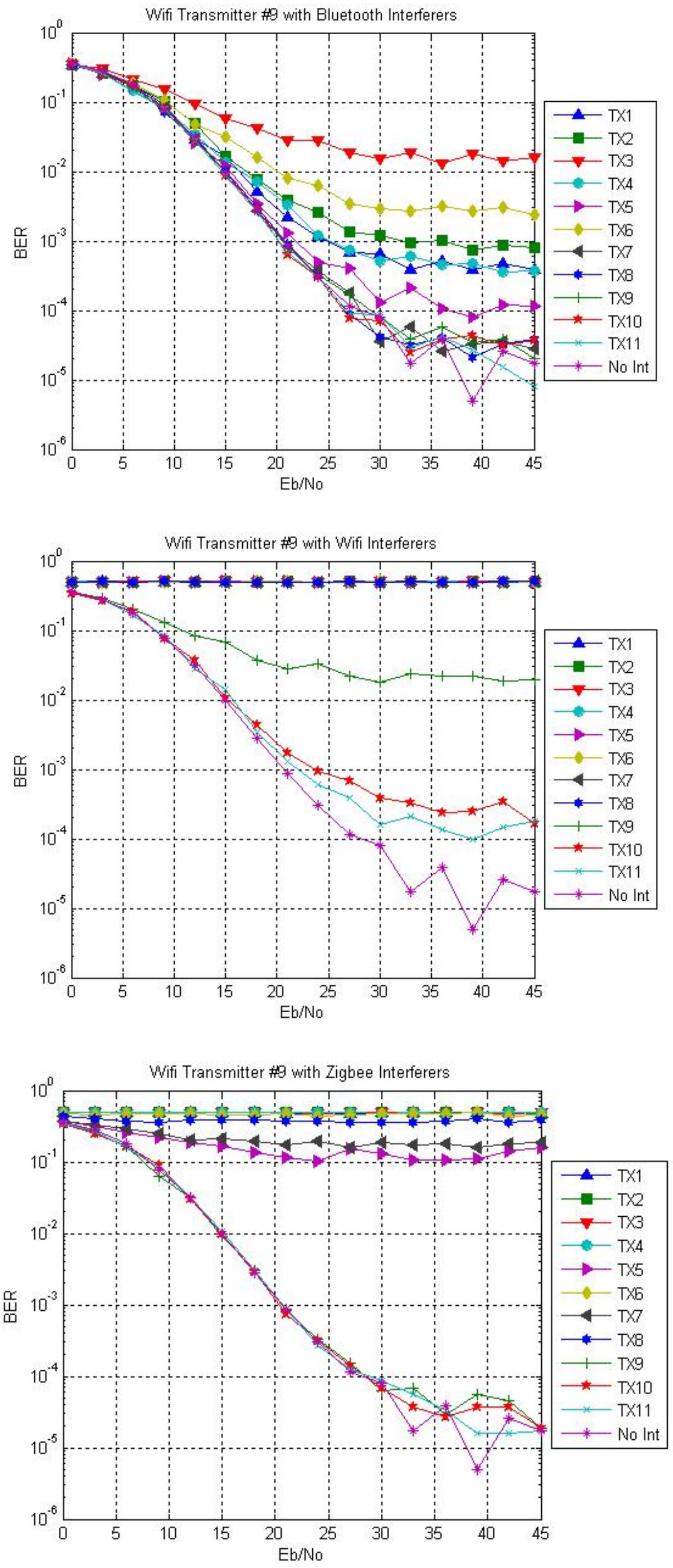


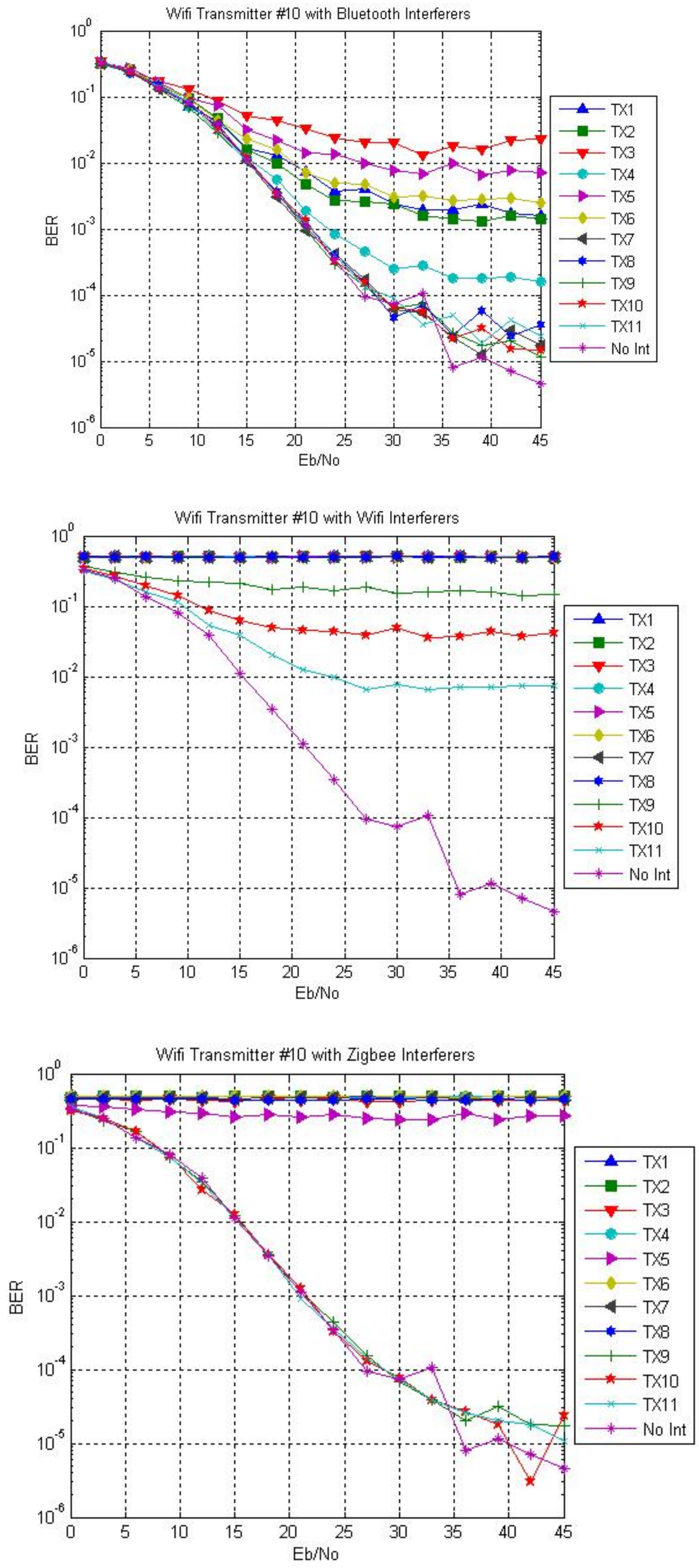
Figure A.19 - Wifi Tx #8


Wifi Transmitter #9 with Bluetooth Interferers

Wifi Transmitter #9 with Wifi Interferers

Wifi Transmitter #9 with Zigbee Interferers

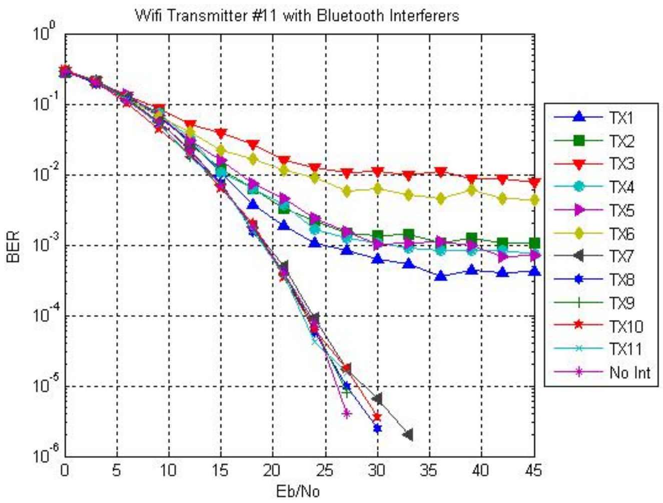
Figure A.20 - Wifi Tx #9

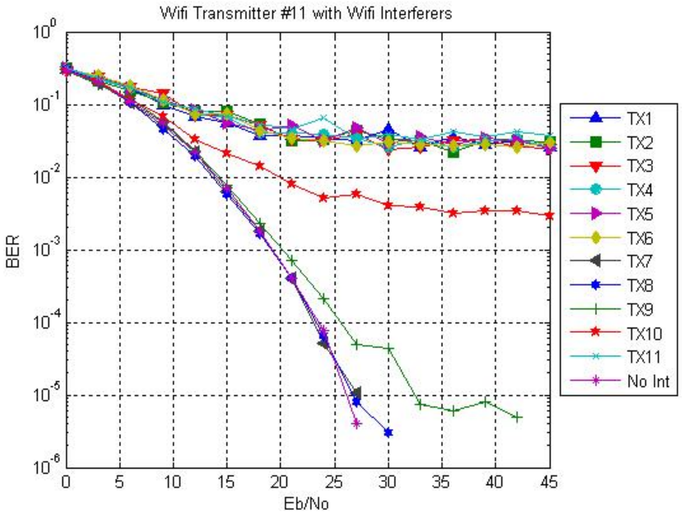

Wifi Transmitter #10 with Bluetooth Interferers

Wifi Transmitter #10 with Wifi Interferers

Wifi Transmitter #10 with Zigbee Interferers

Figure A.21 - Wifi Tx #10





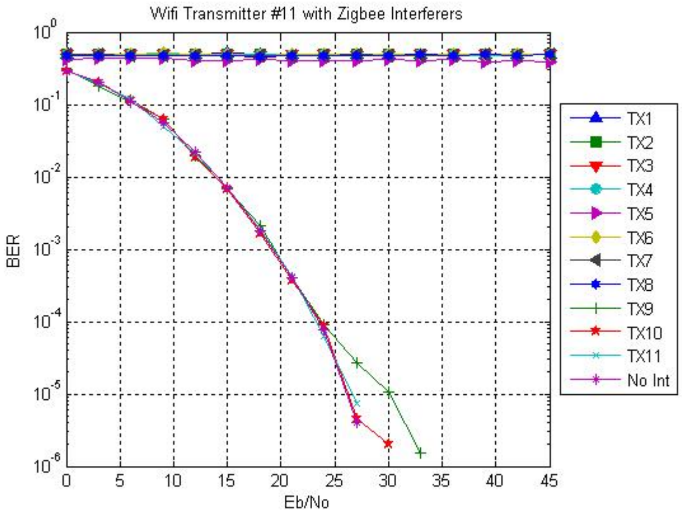


Figure A.22 - Wifi Tx #11

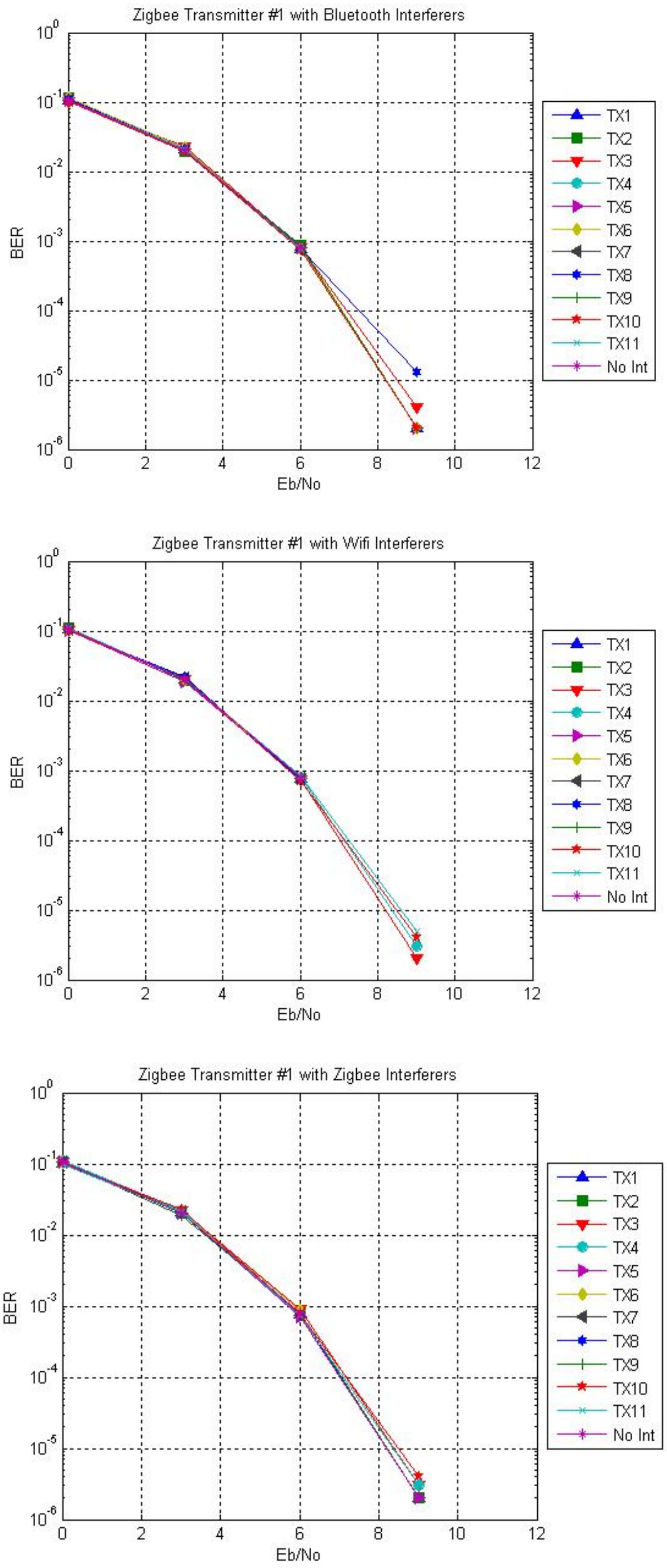
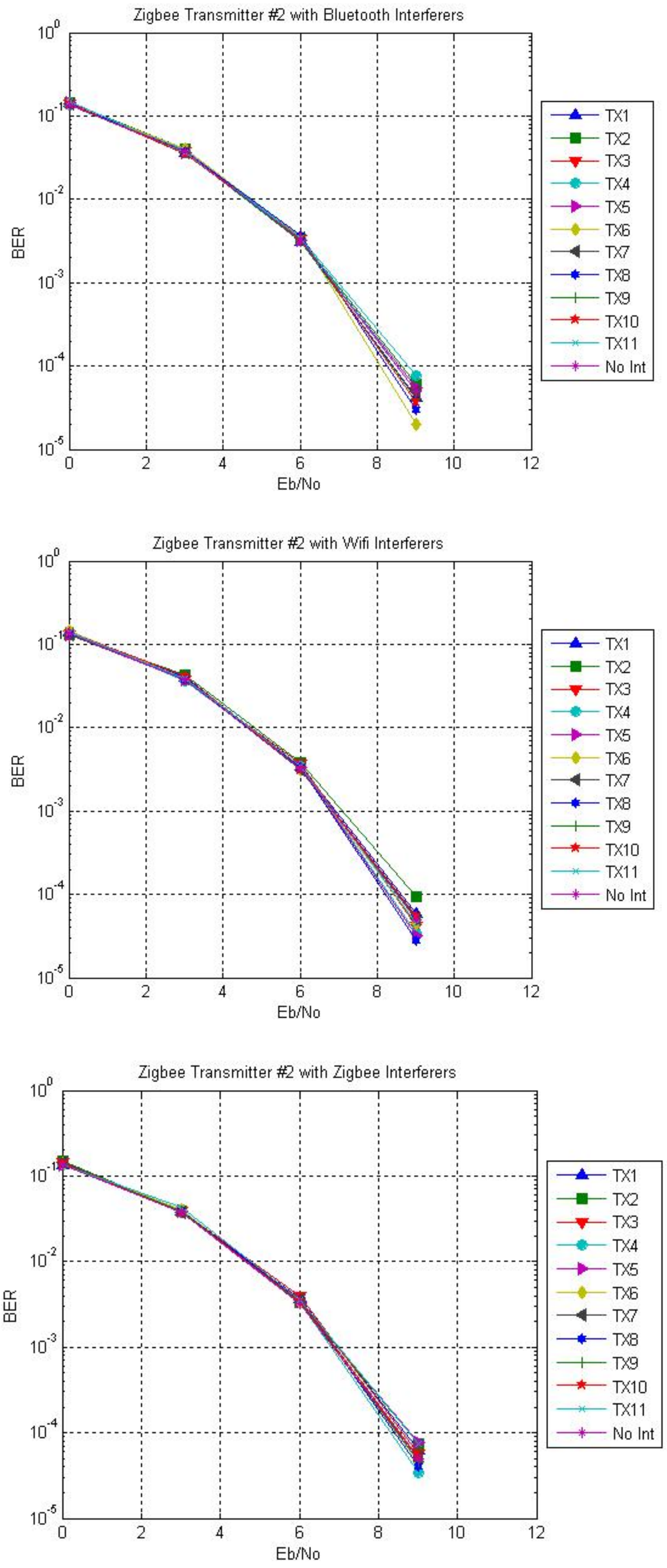


Figure A.23 - Zigbee Tx #1



Zigbee Transmitter #2 with Bluetooth Interferers

Zigbee Transmitter #2 with Wifi Interferers

Zigbee Transmitter #2 with Zigbee Interferers

Figure A.24 - Zigbee Tx #2

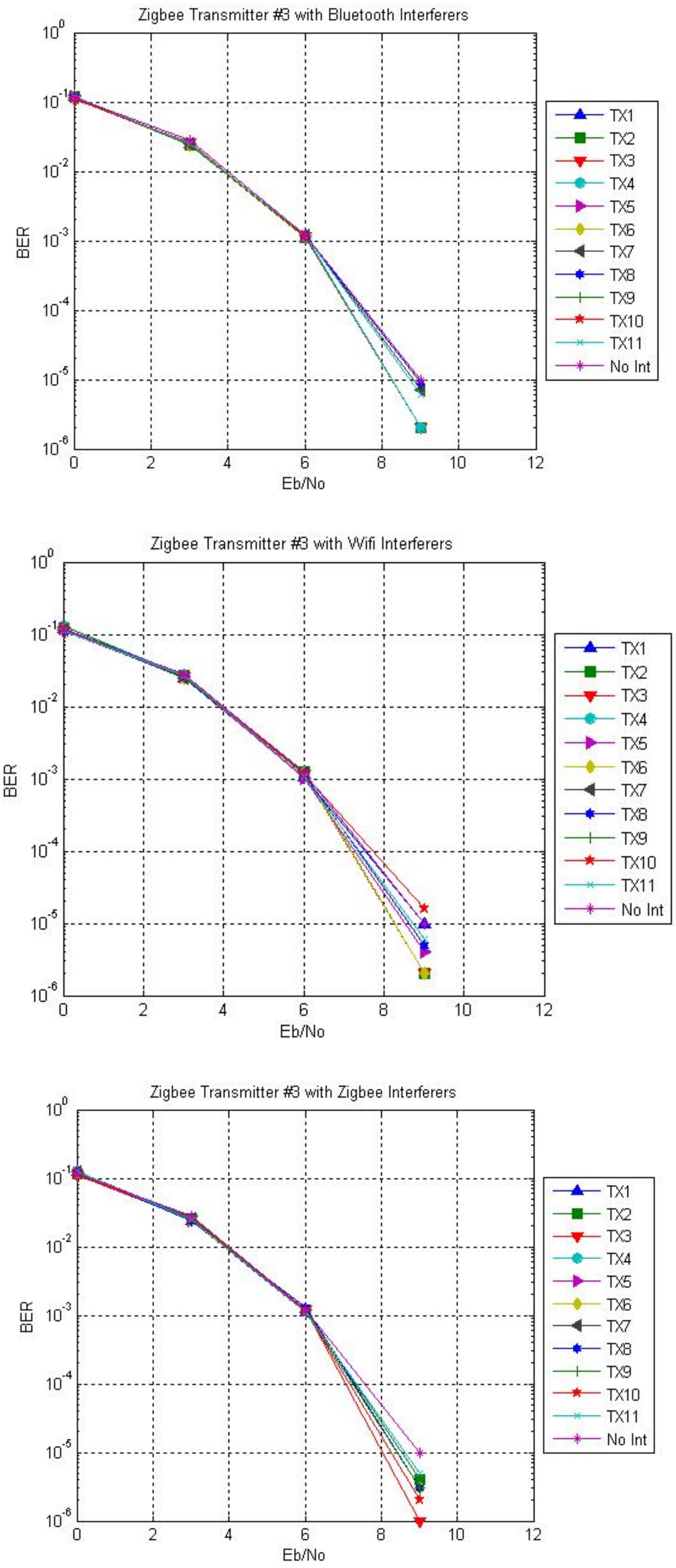
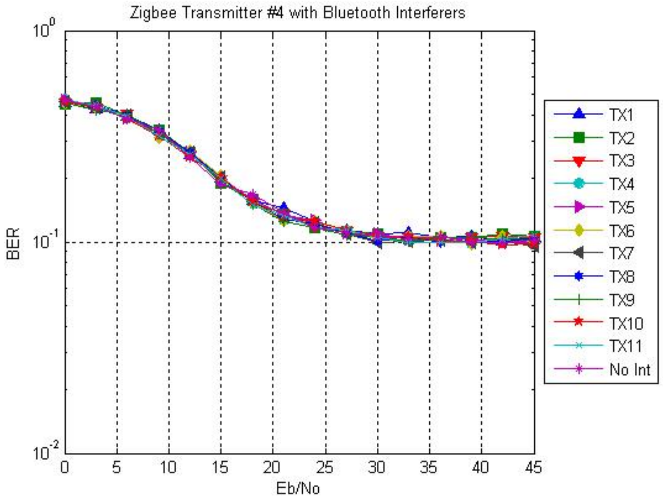
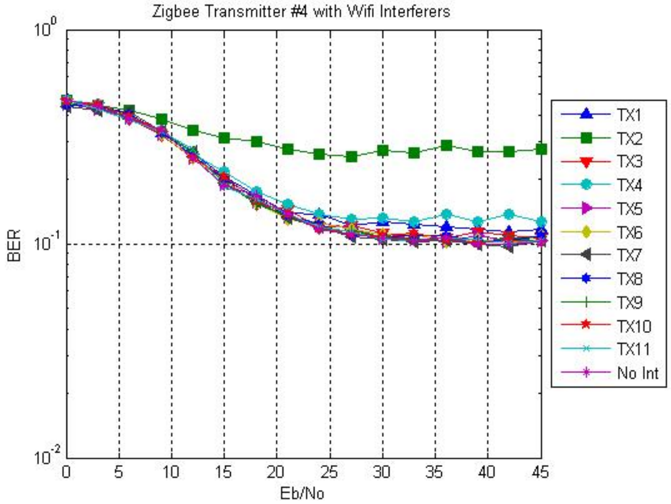


Figure A.25 - Zigbee Tx #3





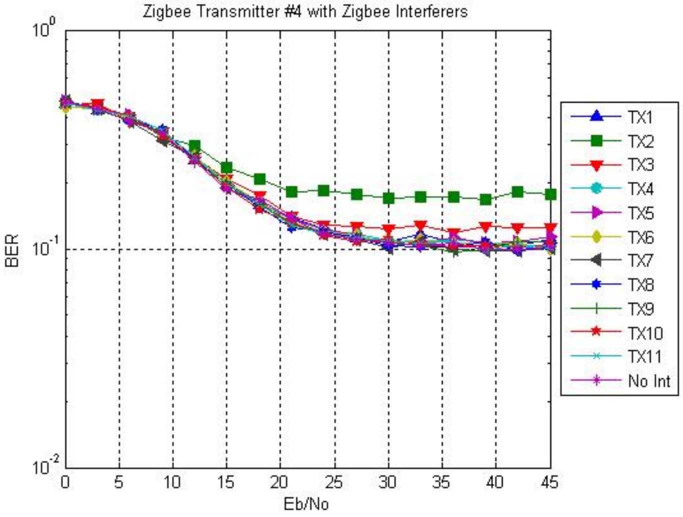


Figure A.26 - Zigbee Tx #4

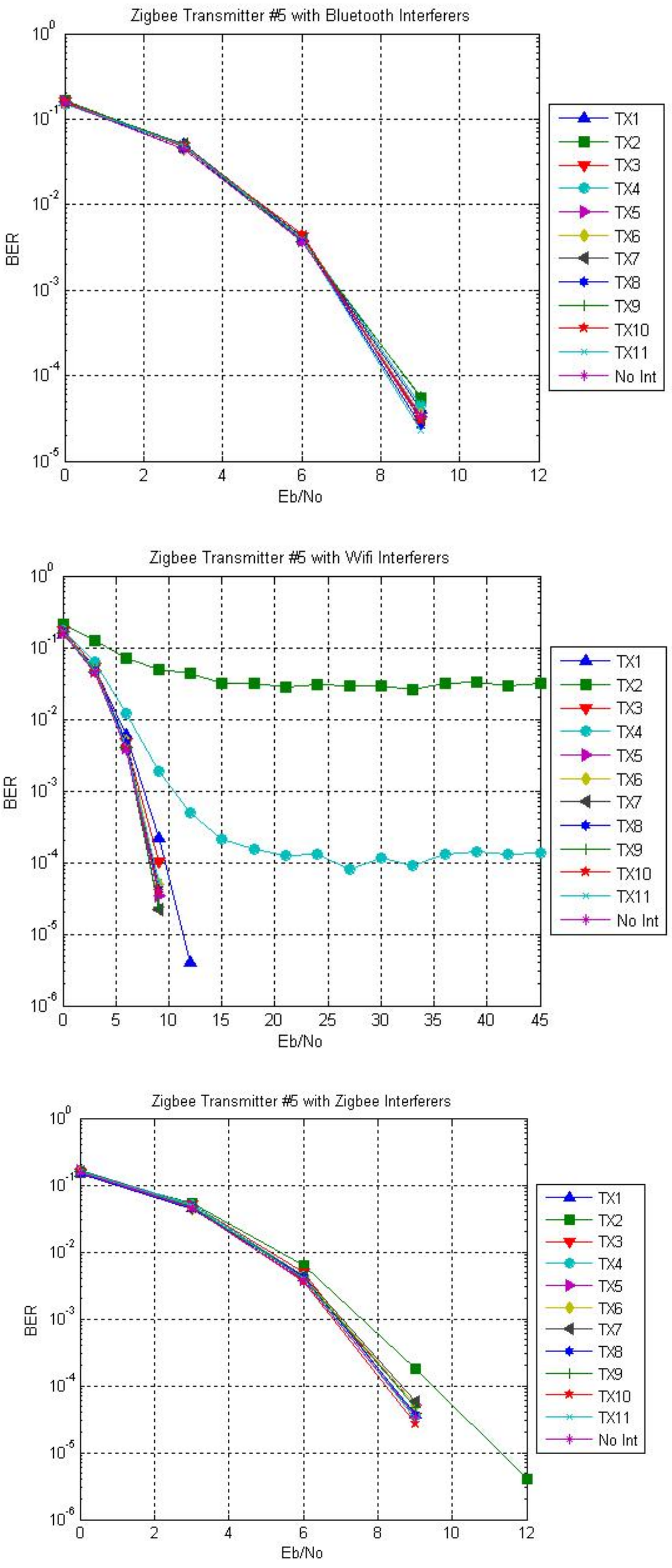
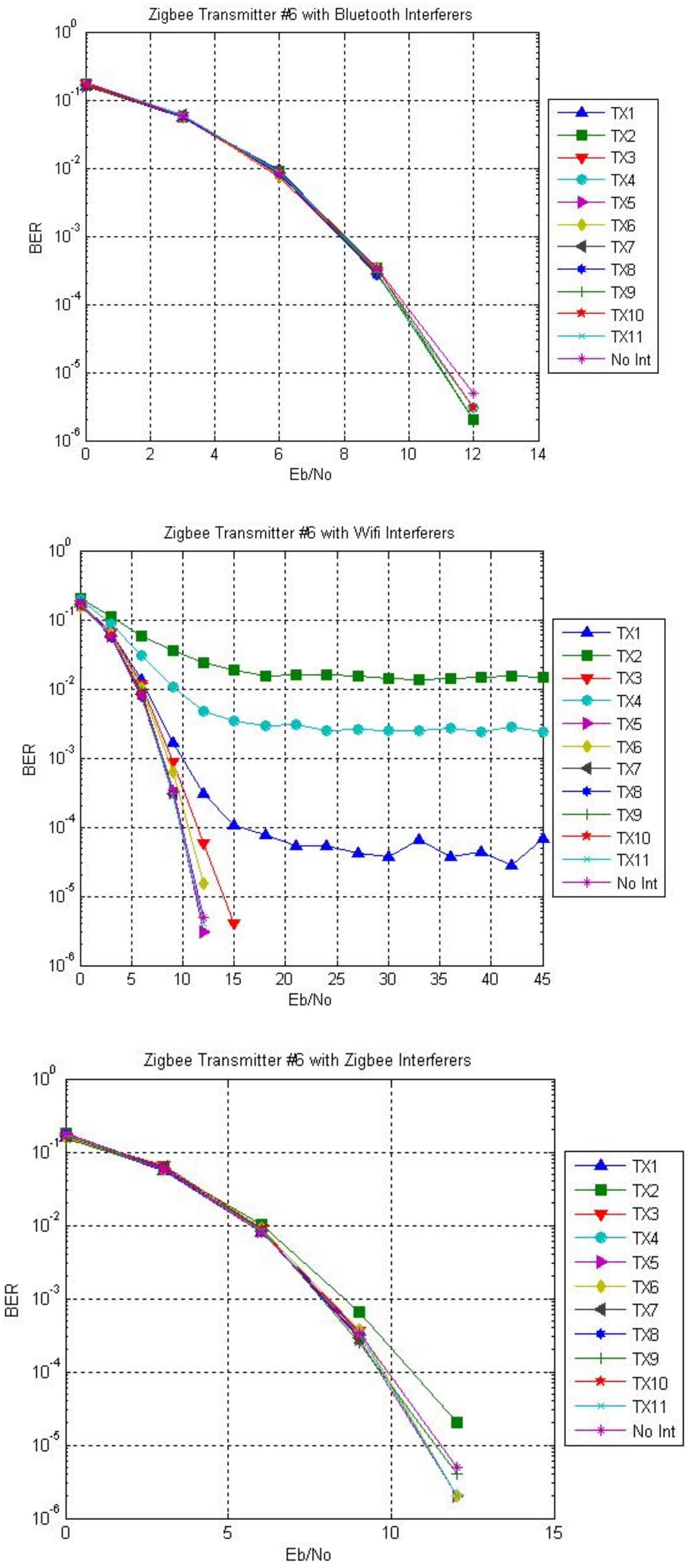


Figure A.27 - Zigbee Tx #5

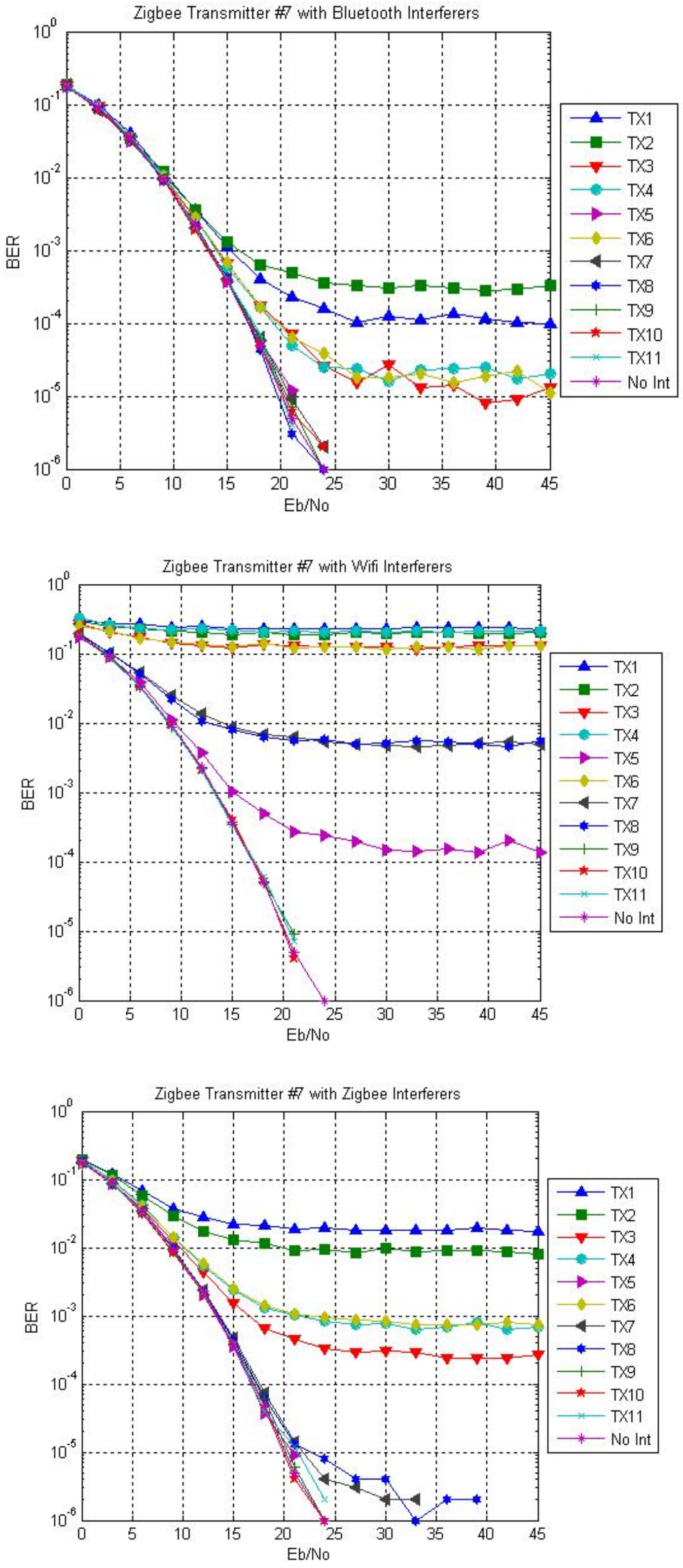


Zigbee Transmitter #6 with Bluetooth Interferers

Zigbee Transmitter #6 with Wifi Interferers

Zigbee Transmitter #6 with Zigbee Interferers

Figure A.28 - Zigbee Tx #6


Zigbee Transmitter #7 with Bluetooth Interferers

Zigbee Transmitter #7 with Wifi Interferers

Zigbee Transmitter #7 with Zigbee Interferers

Figure A.29 - Zigbee Tx #7

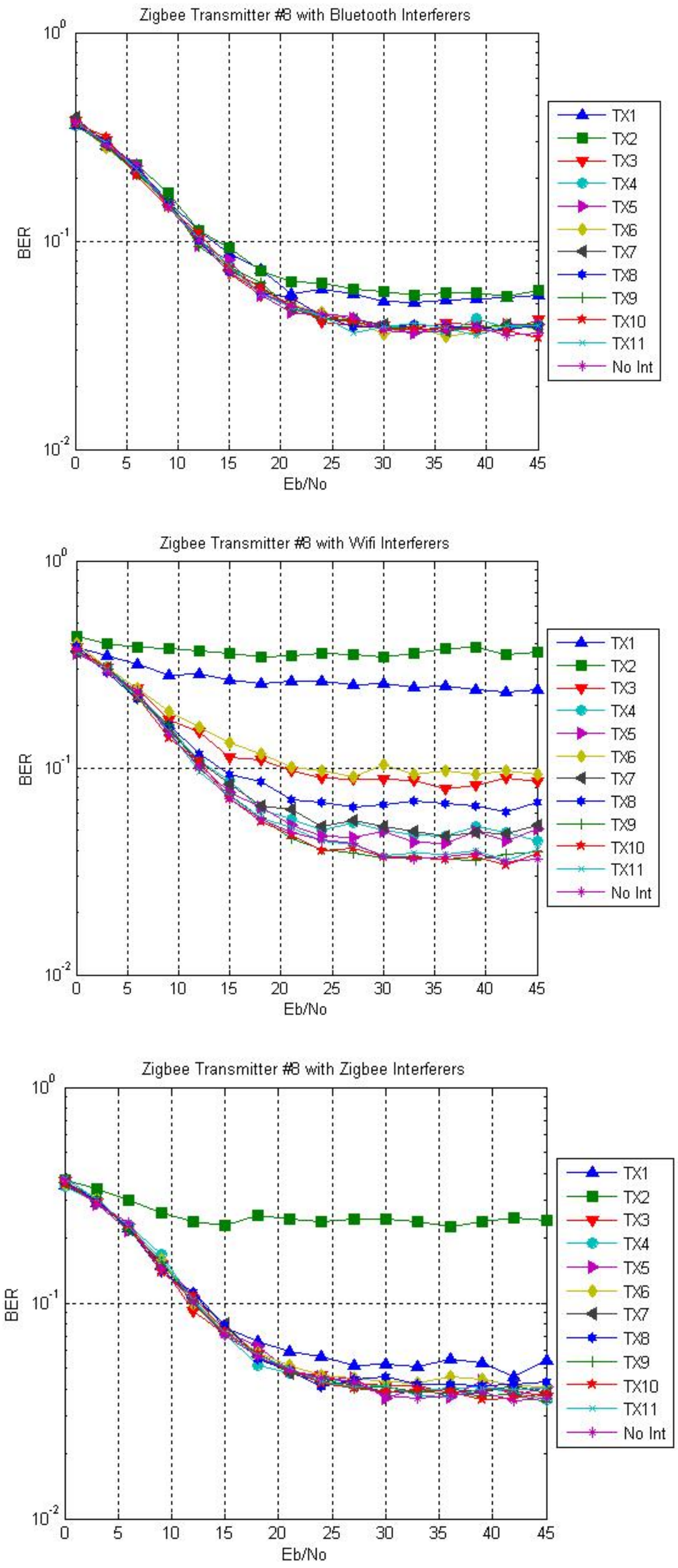


Figure A.30 - Zigbee Tx #8

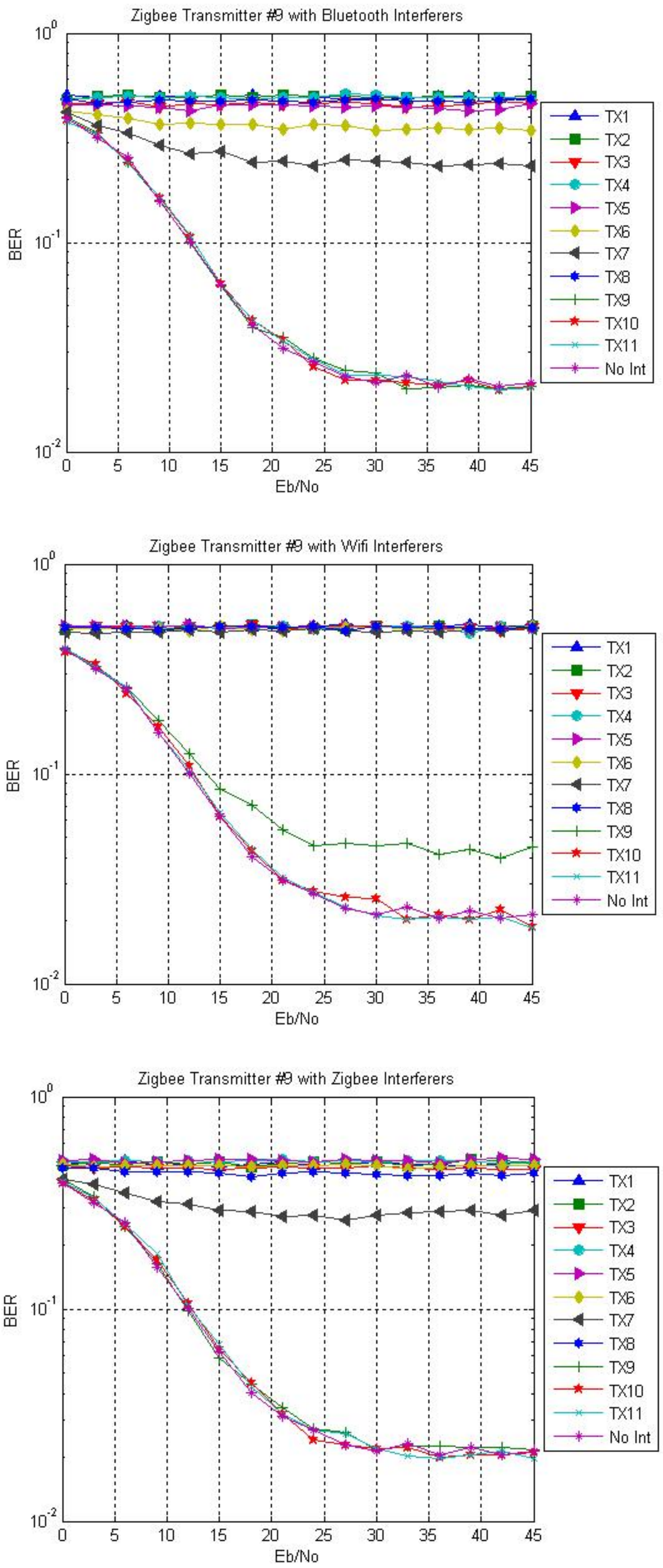


Figure A.31 - Zigbee Tx #9

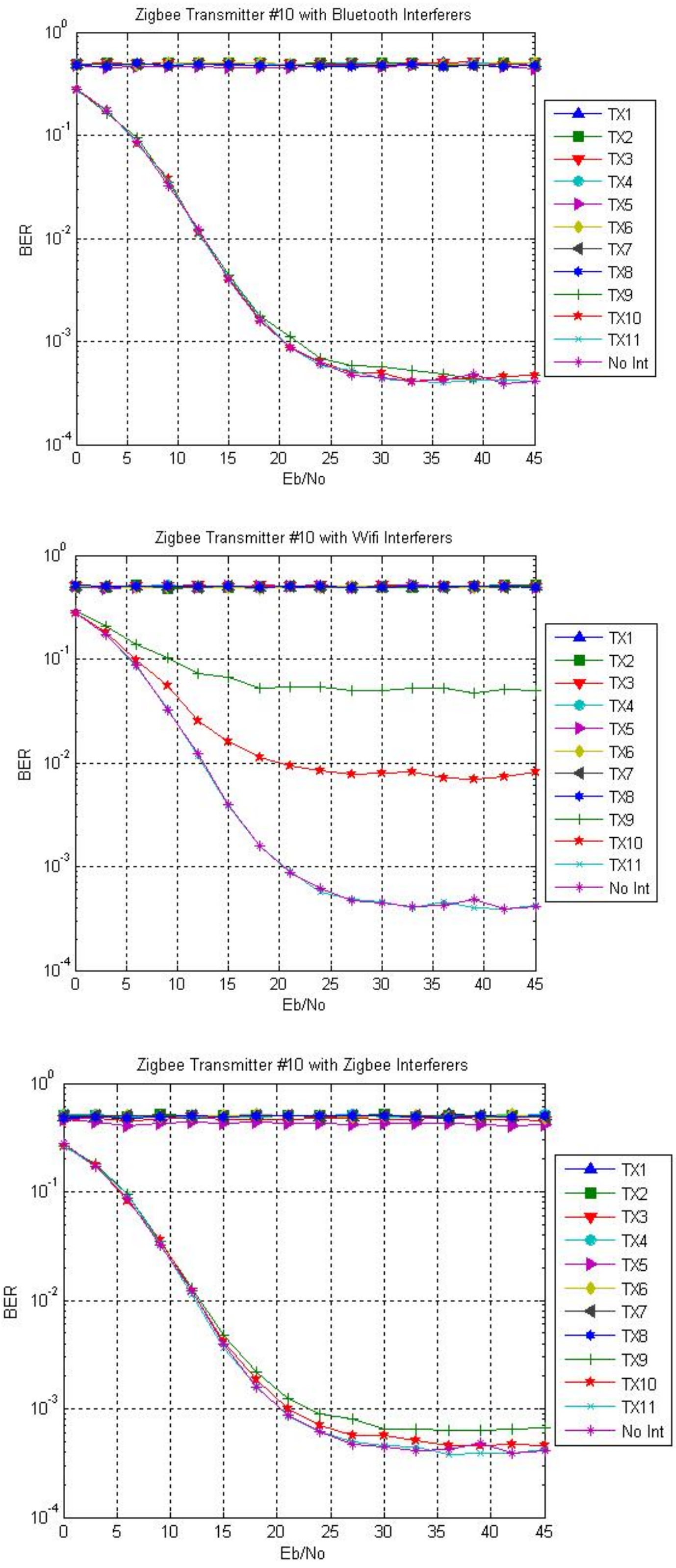


Figure A.32 - Zigbee Tx #10

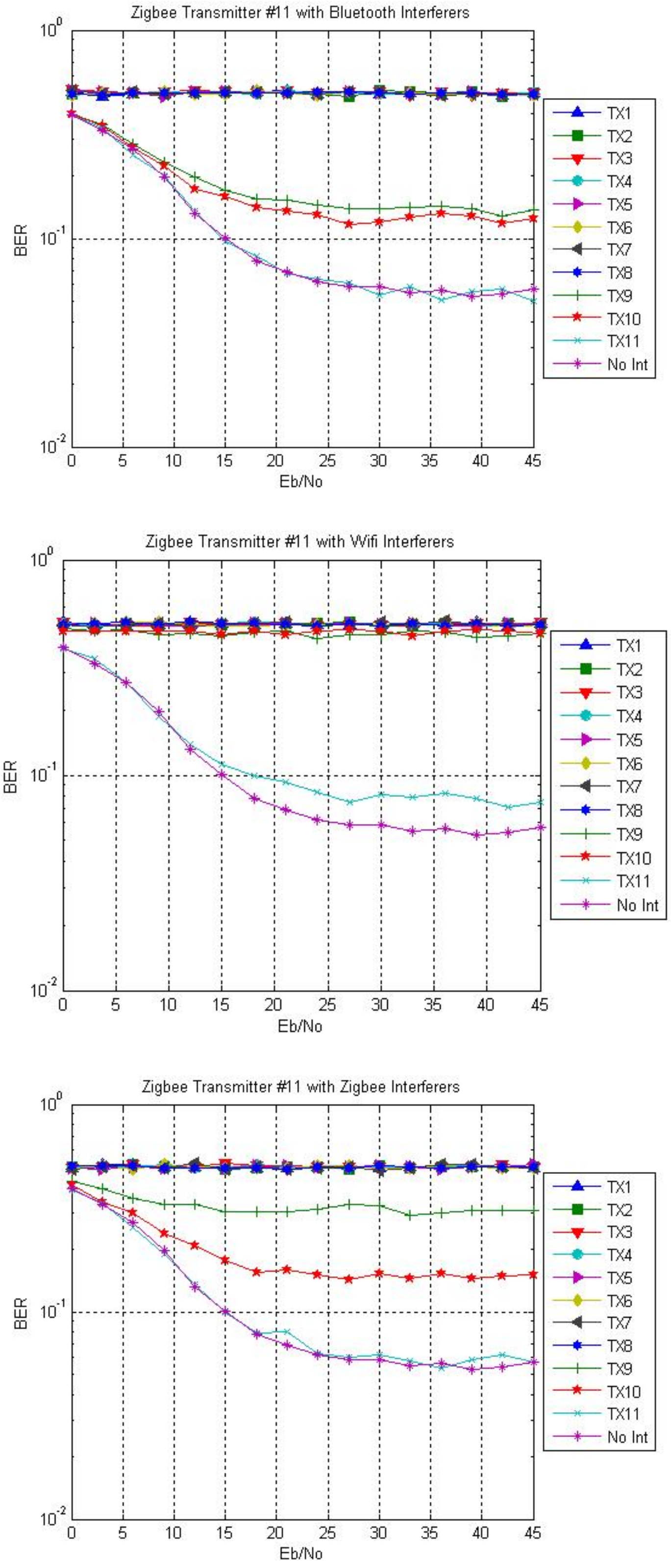


Figure A.33 - Zigbee Tx #11

Vita

Chad Joseph Kiger was born on January 31, 1981, in Ann Arbor, Michigan. He grew up in Milan, MI where he attended grade school at Paddock Elementary School, then Milan Middle School, and finally got his diploma from Milan High School in 1999. He obtained both his B.S. and M.S. degrees from the University of Tennessee, Knoxville, in May of 2004 and December of 2005 respectively. While pursuing his Master's degree, he was honored as being a Bodenheimer Fellow and was also a Student Research Assistant with the WCRG at the University of Tennessee, under the supervision of Dr. Mostofa Howlader.