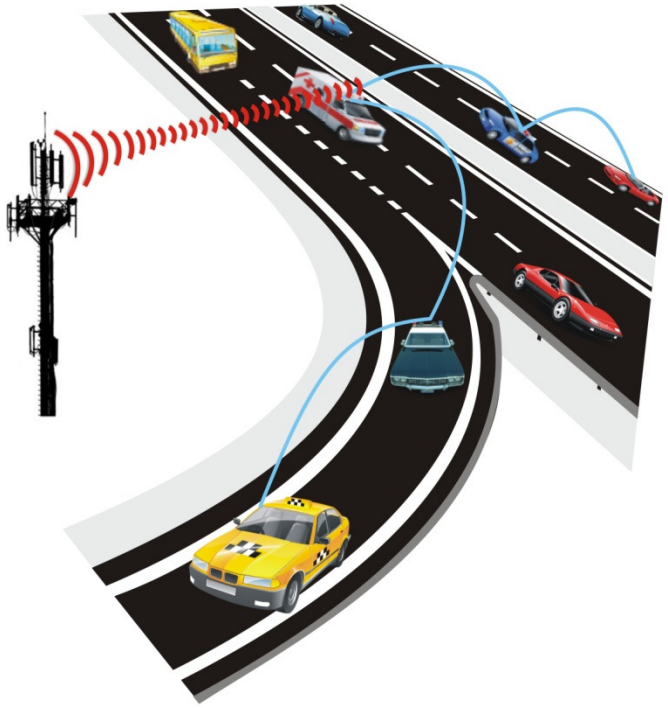
CHALMERS



Effects of Jamming on IEEE 802.11p Systems

Master of Science Thesis in Communication Engineering

Muhammad Tilal
Rashid Minhas

Report # EX 086/ 2010

Chalmers University of Technology
Department of Signals and Systems
Göteborg, Sweden, November 2010

Effects of Jamming on IEEE 802.11p Systems

Muhammad Tilal and Rashid Minhas

Examiner: Prof. Erik Ström

Chalmers University of Technology
Department of Signals and Systems (S2)
SE-412 96 Göteborg
Sweden
Telephone + 46 (0)31-772 1000

Both authors contributed equally in this research work.

Cover image depicts jamming scenario in the vehicular environment.

Department of Signals and Systems
Göteborg, Sweden, November 2010

Abstract

Intelligent Transportation Systems (ITS) is a standardized infrastructure based on DSRC/ WAVE. The recent approval of IEEE 802.11p standard is an important milestone in materializing the dream of communicating vehicles. In the context of ITS, the applications of IEEE 802.11p extend far beyond road safety including transport efficiency and infotainment applications. For the development of a secure and dependable infrastructure for these applications, IEEE 802.11p has to be resilient against different kinds of threats. One of these threats is the jamming or denial of service threat. This thesis is primarily focused on the study of different types of jamming that can hamper operations of a WAVE based system by corrupting physical layer operations between the transmitter and the receiver. The main objective is to check the resilience of the physical layer of IEEE 802.11p transceivers against different kinds of jamming signals and evaluate system performance under the effects of jamming, specifically in vehicular environments.

This study considered both intentional as well as unintentional jamming (interference). The jamming scenarios examined here were developed after studying the structure of the IEEE 802.11p transceiver and selecting the best jamming candidate among several in order to put IEEE 802.11p to the hardest tests and check potential vulnerabilities. In order to consider practical scenarios, simulations were specifically performed for vehicular channels where fading effects pose a real challenge for reliable communications to occur. The vehicular channels employed were based on contemporary research published in a peer reviewed study [1]. The channels considered were time and frequency selective empirical channels. The scenario investigated was a one assuming moving vehicles and a stationary jammer.

For the vehicular channels considered, the partial band noise jamming technique proved to be the most fatal to the system under the given circumstances. Other jamming techniques are not as effective, owing to the facts like amount of jammed bandwidth, shape of the jamming waveforms etc. The results with different frame sizes suggest that the frame error rate (FER) for larger frame size attains its maximum value at a lesser jammer power as compared to the smaller frame size.

Key Words: ITS, IEEE 802.11p, WAVE, DSRC, Vehicular, Jamming, Partial Band, IT++

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AGC	Automatic Gain Control
AGN	Additive Gaussian Noise
AWGN	Additive White Gaussian Noise
B	Bandwidth
BBNJ	Broadband Noise Jamming
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
C	Channel Capacity
DSRC	Dedicated Short Range Communications
DSSS	Direct Sequence Spread Spectrum
FEC	Forward Error Correction
FER	Frame Error Rate
FHSS	Frequency Hopping Spread Spectrum
GI	Guard Interval
IEEE	Institute of Electrical and Electronic Engineers
IFFT	Inverse Fast Fourier Transform
ISM	Industrial, Scientific and Medical
ITS	Intelligent Transportation Systems
JSR	Jammer to Signal Power Ratio
LOS	Line of Sight
LT	Long Training Sequence
MAC	Medium Access Control
MTJ	Multi Tone Jamming
N_{BPSC}	Number of Coded Bits per subcarrier
N_{CBPS}	Number of Coded Bits per OFDM Symbol
N_{CBPS}	Number of Data Bits per OFDM Symbol
N_t	Number of Jamming Tones
NLOS	Non Line of Sight
OFDM	Orthogonal Frequency Division Multiplexing
PBNJ	Partial Band Noise Jamming
PER	Packet Error Rate
PHY	Physical Layer
PLCP	Physical Layer Convergence Procedure
PPDU	PLCP Protocol Data Unit
PSD	Power Spectral Density
PSDU	PLCP Service Data Unit
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
R	Code Rate
RPJ	Repeat Back Jamming
RTV	Roadside to Vehicle
RX	Receiver
SNR	Signal to Noise Ratio
ST	Short Training Sequence

TX	Transmitter
V2V	Vehicle to Vehicle
VOIP	Voice over IP
WAVE	Wireless Access in Vehicular Environments
WBSS	Wave Mode Basic Service Set

Acknowledgements

We want to convey our deepest gratitude to our supervisor Prof. Erik Ström, especially, for giving us the opportunity to work with him and being a mentor to us throughout the thesis. He supported us, all the way along, to this point, with patience and knowledge while being very flexible in handling matters. Whenever we were stuck in something, he was available to guide us with his years long technical experience and knowledge.

We owe a bundle of thanks to our thesis coordinator Dr. Stylianos Papanastasiou, for his guidance, efforts and time he provided. He was courteous enough to overlook our mistakes and was always there to help us. His guidelines regarding the simulations and report writing proved to be of great help.

We definitely have to thank our parents and family, whose selfless and gentle support was always the reason for us to carry on throughout the graduate tenure and specifically the master's thesis. We are also thankful to all our teachers, colleagues and peers, who contributed, either directly or indirectly, to our work by any means.

We remain indebted and grateful to all of you

Chapter 01: Introduction

This chapter describes the background, objectives, methodology and organization of the thesis

1.1. Background

Commercial applications of wireless communications have experienced a significant growth in a relatively short time span. Interestingly, the IEEE 802.11 specification has become the nominal standard for deployment in Wireless Local Area Network (WLAN). The IEEE 802.11p is an amendment to the standard which is at the verge of deployment. This standard mainly focuses on communication in vehicular environments. This standard is also named as Wireless Access for Vehicular Environment (WAVE) and naturally fits in the context of Intelligent Transportation Systems (ITS).

Intelligent Transportation Systems (ITS) involve two basic vehicular communication scenarios, namely Vehicle to Vehicle (V2V) and Road Side to Vehicle (RTV) communication. Based on communication and cooperation between vehicles and roadside infrastructure, ITS safety applications offer great potential to avoid traffic accidents or at least reduce their impact [2]. This communication system claims for making transportation system safer and intelligent. The safety related applications are mainly focused to enhance the road safety by employing the tools like cooperative collision warnings, pre crash sensing, lane change warning, traffic violation warnings etc.

Two other major categories of potential applications include transport efficiency and information/entertainment (infotainment) applications. Transport efficiency can be enhanced by optimizing the flow of the vehicles by reducing the travelling time and avoiding traffic jam situations by using the tools like enhanced route guidance/navigation, optimal traffic light scheduling, lane merging assistance etc. These kinds of applications don’t have the strict delay requirements. The applications included in infotainment category aim to make the journey more comfortable and pleasant by enhancing the multimedia entertainment, VOIP calls, parking information and billing, maps downloads, toll collection etc. The biggest challenge in this kind of communication is highly mobile environment and rapidly changing conditions especially in the case of V2V communication [3].

Specifically IEEE 802.11p's communication is known as Dedicated Short Range Communication (DSRC). The DSRC band ranges from 5.850 GHz to 5.925 GHz. The DSRC works within a range of up to 1000 m with 10 MHz channel spacing, attaining the data rate ranging from 6 to 27 Mbps depending upon modulation type and service used [4] [5].

As described before, IEEE 802.11p overlaps with non licensed ISM band so obviously interference from other technologies operating in the same band is expected. Previously IEEE 802.11p has not been analyzed for its robustness against interferences and jamming. Originating from different technologies these interferences could be of various types, so in this research different types of interfering signals (Details are provided in Chapter 3) were simulated to see how these interfering signals could corrupt the communication. Apart from interference from co-band technologies, intentional jamming cannot be neglected as the system promises to provide safer transportation by using communication means. For example, one might want to jam public safety messages broadcasting or emergency vehicle information. To analyze the severity of these contaminations the Physical Layer (PHY) of 802.11p standard was studied to achieve objectives of this Master thesis. Different possible scenarios was modeled and simulated, i.e. V2V communication to see the effects of different interfering signals.

1.2. Objective and Scope

The aim of this thesis is to investigate the susceptibility of 802.11p compliant transceivers to jamming signals under various channel conditions. The proposed research took into account, different types of interfering signals and evaluated their effectiveness in hindering 802.11p communications. Performance measurements have been collected using a physical layer simulator, which closely mimics the operation of an 802.11 transceiver at the time sample level. The scope of this thesis includes the exposition of possible interferers which could harm or corrupt the system. This jamming could be of many kinds like introducing fixed or random interfering signal patterns or by using high power interfering transmitter.

1.3. Methodology

The research was carried out in several phases. It started with the literature study towards the implementation and evaluation. For implementation, evaluation and simulation purposes two tools were used. Firstly a simulator, already developed, in C++ at the signals and systems department of Chalmers University, was utilized as a main simulating tool. This simulator mimicked the physical layer operations of IEEE 802.11p. Further development was done in the same simulator for the purposes of the thesis. Several types of jamming techniques like noise jamming, tone jamming and follower jamming were implemented and simulated on different channels. These channels included AWGN and vehicular channels. The performance of 802.11p system was analyzed and compared in the presence of different jammers. MATLAB was used for plotting and comparison of results.

1.4. Thesis Organization

This thesis report comprises of six chapters. Chapter 2 gives a brief description of IEEE 802.11p physical layer model in accordance with the scope of the research work. Chapter 3 gives a detailed description of jamming signals and their predicted effects. In Chapter 4, all the channels used for the simulations are discussed along with the parameters used. Chapter 5 is written to provide the simulation results for different jamming techniques and their comparison. Chapter 6 provides conclusions, drawn from the gathered results, and suggestions for future work.

Chapter 02: System Model for IEEE 802.11p

This chapter gives a brief description of IEEE 802.11p PHY model. Instead of describing the complete physical layer structure of IEEE 802.11p, the scope of this chapter is limited to the scope of research carried out.

2.1. Introduction

IEEE 802.11 is a family of wireless LAN (WLAN) standards that use the over the air modulation techniques and have the same basic protocol. The initial version of 802.11 standard emerged in 1997 but 802.11b was the first widely accepted standard. With the passage of time different amendments were made to enhance and adapt the WLAN standard for specific applications and in 2007 a new edition was published to encompass all these amendments. As such IEEE 802.11- 2007 is the most recent and currently used WLAN standard. IEEE 802.11n- 2009 is an amendment of IEEE 802.11- 2007 to improve the throughput over the previous standards.

802.11 PHY supports different modulation types including Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS) and Orthogonal Frequency Division Multiplexing (OFDM). It uses the frequencies of 5.9 GHz and the 2.4 GHz in unlicensed ISM band. The OFDM physical layer specification defines three different types of channel spacing including 20, 10 and 5 MHz and almost all 802.11 compliant devices support these.

The IEEE 802.11p amendment proposes some minor changes in order to allow IEEE 802.11 technology to be used in very high speed, rapidly changing radio environments encountered by cars and other vehicles on the express and high ways as well as densely occupied urban areas. It defines the amendments to the PHY in order to deal with the severe Doppler shifts and rapidly changing multipath conditions experienced by vehicles communicating with each other or the road side infrastructure at speeds of approximately 200 km/h. It also incorporates MAC layer changes in order to satisfy the need of fast connection setup and a quick, reliable data exchange which arises due to fast moving vehicle going through multiple zones because of its high speed. The MAC layer amendments allow for a new mode for 802.11 which allows for a faster connection and handover, named as WAVE Mode Basic Service Set (WBSS).

The main challenge in vehicular environments is the mitigation of fading effects, which are typically worse than in ordinary fading channels. These pronounced fading effects arise because of an increased delay spread due to very high vehicular speeds. To mitigate these fading effects, OFDM operation of IEEE 802.11 standard is chosen as the best available candidate in the standard. But the choice of OFDM PHY has to be complemented with the increased symbol duration in order to get the desired results. As the original IEEE 802.11 standard is capable of using different channel bandwidths including 20, 10 and 5 MHz, so for IEEE 802.11p, 10 MHz channel bandwidth is used.

The 10 MHz channel spacing in obtained by half clocked operation as compared to full clocked operation in 20 MHz channel spacing. This increases the symbol duration thus providing a longer guard interval to cater for increased delay spread, leading to lesser inter symbol Interference (ISI) in the vehicular environments. However the price for this benefit is reduced system bandwidth, data rate and the OFDM carrier spacing.

2.2. OFDM PHY Description

This section gives a brief overview of the transmitter and receiver blocks of a typical 802.11p system based on the OFDM PHY. Most fundamental blocks for OFDM based IEEE 802.11p transceiver are shown in Figure 2-1.

In 802.11p, an OFDM symbol is formed by taking 64 point IFFT- an important point to note here is that not all the subcarriers are used for the data transmission. Out of 64, only 52 subcarriers are used in total, of which 48 are regarded as data subcarriers and 4 are used as pilot subcarriers. The pilot subcarriers, placed at the locations -21, -7, 7, and 21, are used for frequency offset and phase noise estimation. This is applicable regardless of any operating mode for the system. The unused subcarriers act as the guard band in order to prevent spectrum overlap with neighboring channels.

Like its parent standard, 802.11p also supports variable data rates which is possible by different combinations of adaptive modulation and multiple coding rates that are set according to the channel conditions.

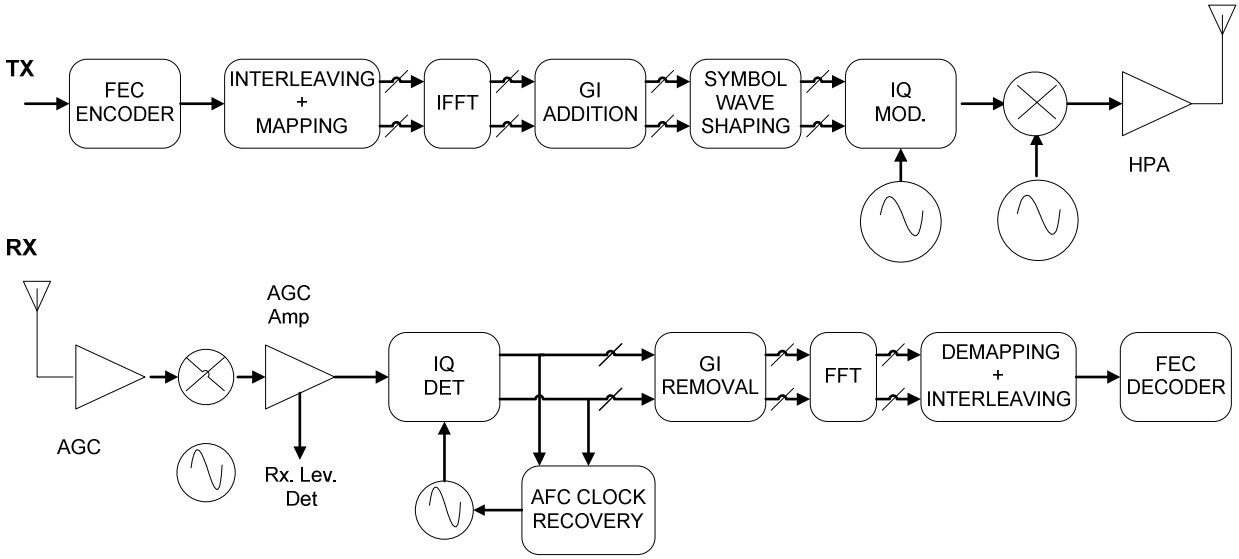


Figure 2- 1: Block diagram of 802.11p transceiver [4]

Modulation formats include BPSK, QPSK, 16 QAM and 64 QAM while the Forward Error Correction (FEC) code used is convolutional code with industry standard generator polynomials $g_o = 133$ and $g_1 = 171$. The supported code rate include 1/2, 2/3 and 3/4 where the code rates higher than 1/2 are possible by employing puncturing.

Table 2-1 summarizes the modulation dependent parameters for the system and table 2-2 gives an overview of IFFT/ FFT timing related parameters [4].

Table 2- 1: Summary of modulation dependent parameters [4]

Modulation	Coding Rate (R)	Coded Bits per Subcarrier (N_{BPSC})	Coded Bits per OFDM Symbol (N_{CBPS})	Data Bits per OFDM Symbol (N_{DBPS})	Data Rate (Mb/s) 10 MHz Channel Spacing
BPSK	1/ 2	1	48	24	3*
BPSK	3/ 4	1	48	36	4.5
QPSK	1/ 2	2	96	48	6*
QPSK	3/ 4	2	96	72	9
16 - QAM	1 / 2	4	192	96	12*
16 – QAM	3/ 4	4	192	144	18
64 – QAM	2/ 3	6	288	192	24
64 - QAM	3/ 4	6	288	216	27
*	Mandatory Data Rates				
	Parameters for System Under Consideration				

Table 2- 2: Summary of timing related parameters [4]

Parameter	Value (10 MHz Channel Spacing)
N_{SD}: Number of data subcarriers	48
N_{SP}: Number of pilot subcarriers	4
N_{ST}: Number of subcarriers, total	52 (N_{SD} + N_{SP})
Δ_F : Subcarrier Frequency Spacing	0.15625 MHz (10MHz/ 64)
T_{FFT}: Inverse Fast Fourier Transform(IFFT)/ Fast Fourier Transform (FFT) Time	6.4µs (1/ Δ_F)
$T_{PREAMBLE}$: PLCP Preamble duration	32 µs (T_{SHORT} + T_{LONG})
T_{SIGNAL}: Duration of SIGNAL (BPSK-OFDM symbol)	8.0 µs (T_{GI} + T_{FFT})
T_{GI}: Guard Interval Duration	1.6 µs (T_{FFT}/ 4)
T_{GI2}: Training Symbol Guard Interval Duration	3.3 µs (T_{FFT}/ 2)
T_{SYM}: Symbol Interval	8 µs (T_{GI} + T_{FFT})
B_{SIG}: Signal Bandwidth	8.3 MHz (53*10MHz/64)

2.3. PPDU Frame Format

With respect to the PHY, the communication between 802.11p transmitter and receiver takes place in the form of frames, termed as PPDU frames. These frames have a predefined structure with multiple

fields. Some of these fields are fixed while others are dependent on transmission related parameters. The length of the frame is variable depending upon the amount of the data that has to be exchanged.

The PPDU frame format is shown in Figure 2-2. It has three main entities namely PLCP Preamble, SIGNAL and DATA fields. The combination of SIGNAL field with the SERVICE field is known as PLCP Header. A brief explanation of the fields in PPDU frame is given as under

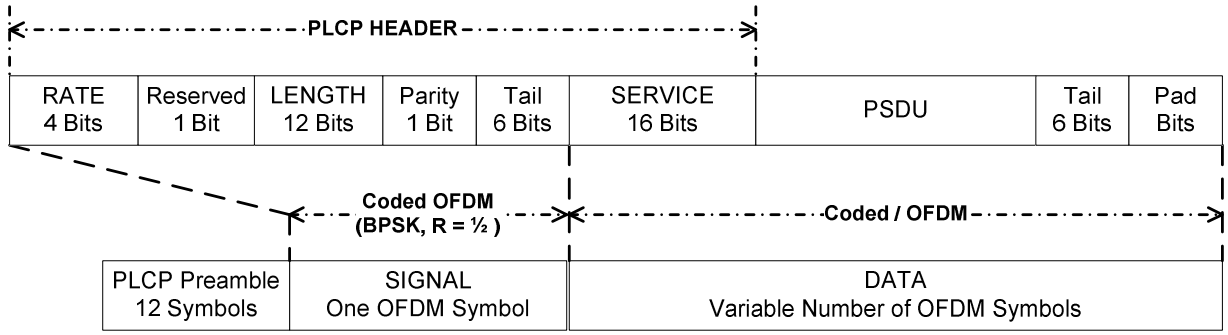


Figure 2- 2: PPDU frame format [4]

2.3.1. PLCP Preamble

The main purpose of PLCP preamble is synchronization. It consists of 10 short and 2 long training symbols. The PLCP preamble format is depicted in the Figure 2-3.

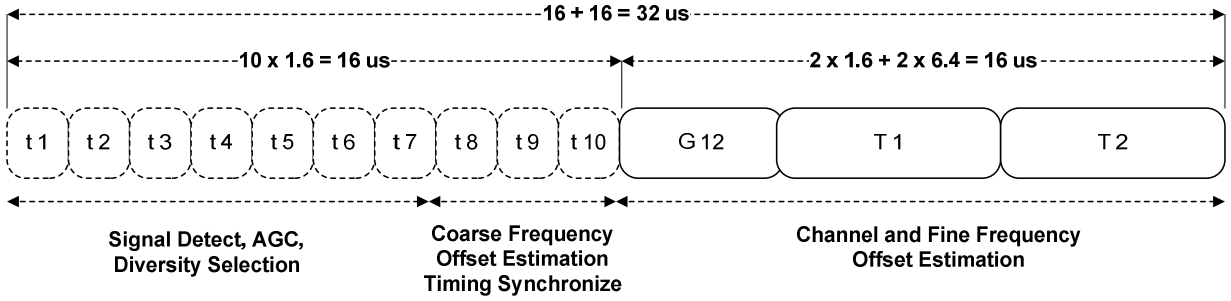


Figure 2- 3: PLCP Preamble [4]

The short training sequence is, primarily, used for signal detection; coarse frequency offset estimation and timing synchronization. Two long training symbols are placed after short training sequence, which serve the purpose of channel and fine frequency offset estimation. G12 is used as the guard interval for the long training sequence.

2.3.2. SIGNAL

The SIGNAL field contains the RATE and LENGTH of the transmitted data. The RATE field conveys the information about the modulation type and code rate used for the rest of the packet. LENGTH field is unsigned 12 bit integer indicating the number of octets in PSDU that are being sent by the MAC to PHY

(of transmitter) to transmit. The SIGNAL field is of critical importance because it contains crucial information about the length and code rate for the received frame. If receiver is unable to decode the SIGNAL field, rest of the packet is discarded because of lack of necessary information required for decoding.

Figure 2-4 shows the bit assignment of the SIGNAL field consisting of 24 bits. Bits 0 – 3 are used to encode the RATE, bit 4 is reserved for the future use. Next 12 bits ranging from 5 to 16 are used by LENGTH field and bit 17 is used as an even parity bit for the bits in the LENGTH field. The remaining bits in the SIGNAL field (bit 18 – 23) are tail bits and set to 0.

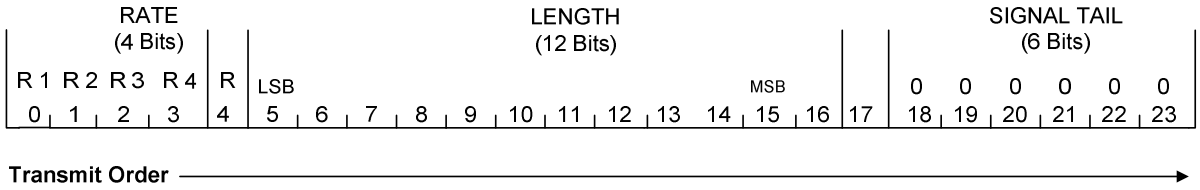


Figure 2- 4: SIGNAL field (Bit Assignment)

SIGNAL field is always encoded into single OFDM symbol using BPSK modulation along with the convolutional code with rate R= 0.5.

2.3.3. DATA

The DATA field consists of the SERVICE field, PSDU, TAIL bits and the PAD bits. The SERVICE field has sixteen bits, of which first six (0-5) are used to synchronize the descrambler at the receiver while the rest are reserved for the future use and set to zero.

There are six TAIL bits after PSDU which are required to return the convolutional encoder to zero state. This procedure enhances the error probability of the convolutional decoder, which depends on the future bits for decoding and which may not be available past the end of the message.

The bits in the DATA field must be the multiple of Number of coded bits per OFDM symbol (N_{CBPS}). To achieve this, the length of the message is extended using the PAD bits so that it becomes the multiple of N_{DBPS} (Number of data bits per OFDM symbol).

2.4. PPDU Frame Encoding

This section gives a brief overview of encoding a PPDU frame. The encoding process is mainly divided into three main steps which are 1) Preamble Generation, 2) The SIGNAL Field Generation and 3) DATA Field Generation.

As a first step, ten symbols of short training sequence (ST) and two symbols of long training sequence (LT) are generated. The short training sequence (ST) is appended in front of the long training sequence (LT) to make the Preamble field.

For the generation of the SIGNAL field, the first process is to get the required parameters such as RATE, LENGTH and PARITY. After putting together all the information required for the SIGNAL field the resulting bits are passed through the convolutional encoder and the interleaver. This encoded and interleaved SIGNAL field is mapped to frequency domain and the pilot subcarriers are inserted. As a final step the SIGNAL field is transformed into time domain.

For the DATA field generation, the data octets acquired from MAC layer are transformed into a bit stream followed by addition of the SERVICE field bits and pad bits. The resultant bits are then scrambled and tail bits are set to zero and then fed into convolutional encoder. The output of the convolutional encoder is then mapped to complex symbols depending upon the type of modulation i.e. BPSK, QPSK etc. Then the pilot subcarriers are inserted and frequency to time domain transformation is carried out followed by the addition of cyclic prefix.

After these three steps have been carried out; all the resulting OFDM symbols are concatenated to form a single time domain signal that has to be transmitted as shown in Figure2-5

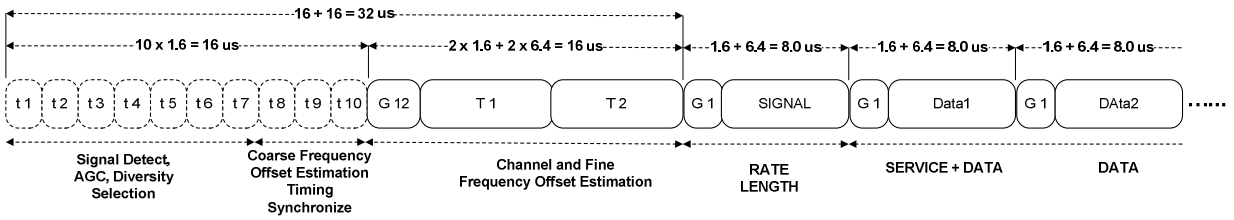


Figure 2- 5: Complete PPDU Frame for transmission [4]

When a PPDU frame is received, the training sequences are used for the channel estimation and other necessary purposes. The SIGNAL field is decoded in order to get the RATE and LENGTH parameters of the encoded data and using these parameters, DATA field is decoded to get the information being sent. If at any point, the receiver is unable to decode the SIGNAL field, the DATA field cannot be decoded.

Chapter 03: Jamming Signals

This chapter gives an overview of the jamming signals background and details. It includes detailed description on the different types of jamming signals and their predicted effects.

3.1. Background and Introduction

In a strict sense jamming is a (usually intentional) transmission of a signal to disrupt the communications by decreasing the SNR at the receiver. Unintentional jamming may occur when a transmission is being made, unknowingly, in the frequency band that is already occupied. Such kind of unintentional jamming is usually termed as “interference” [6].

History of the jamming dates back to World War II. In its simplest form, it is very similar to the spoofing attack. In such kind of jamming the pilots were mislead using the false commands in their own language. Since the cold war till now, a lot of development is made in this field resulting in a variety of jamming signals available today [7].

For successful jamming, a jammer has to fulfill two conditions, (I) to detect that the transmission is taking place and (II) to transmit the signal which is designed to confuse the receiver [8]. So the jamming is successful when the jamming signal denies the useful reception of communication transmissions. In digital communication systems, use is denied when the error rate of the transmission cannot be compensated by error correction. One thing that needs to be noted here, is, that the original transmission can never be altered. Jamming only hinders the reception of the intended signal at the receiver.

The effects of jamming depend upon the jammer to signal power ratio (JSR). Other major factors involve the modulation scheme, channel coding and interleaving of the target system [9]. Jammer power can be inserted in a desired band in number of ways depending upon the ultimate goal of jamming.

Most digital systems require synchronization and the channel state information for the proper functionality. Such systems are most vulnerable to jamming because jamming signal can be designed to affect the synchronization signals. Once the synchronization is lost, the system is unable to decode the signal properly as it can lock on to signal at any arbitrary point in time or actual signal duration is different than the one perceived by the system. Most modern communication systems are designed for maximum throughput by utilizing of channel state information via training sequences and pilots. These known sequences/ signals can be neutralized by jamming to make a communication system practically useless.

There are many jammer waveforms being used nowadays depending upon the suitability to the target system. Any single jamming waveform cannot be effective for all kind of communication systems as it depends upon the design of the target system. For instance, a waveform can be effective for jamming an OFDM based system but not in spread spectrum based system. For this study six different types of waveforms are considered which are presented along with their complete description in the following sections.

3.2. Noise Jamming

Noise is detrimental to almost every communication system and if it exceeds certain level it can hinder the communication effectively. This fact is exploited by using noise jamming as it increases the background noise for the system by injecting Additive Gaussian Noise (AGN), broadband or band limited, in addition to the thermal noise. This effectively makes it difficult for the communication system to operate and in some cases; communication is totally denied [10].

This can also be seen as an effect of noise jamming on channel capacity for a communication system. In presence of AWGN, the formula for channel capacity by Shannon is given as

$$C = B\ log2\ (\ 1 + \frac{S}{N}\ ) \qquad \text{(Eq. 3.1)}$$

Where
C = Channel Capacity in bits/second
B = Channel Bandwidth in Hertz
S = Average Received Signal Power over the bandwidth, measured in watts
N = Average noise/ interference power, in watts

It gives an upper bound on the data rate for which the communication is possible with a small error rate and if the data rate is increased beyond this level, the received signal will have significant amount of errors. Now keeping all other parameters constant if the noise N is increased by adding an extra amount of noise "J" using jammer, errors at the receiver can be increased beyond the acceptable range. This is true for the fading channels as well.

Noise Jamming is primarily classified into two major categories namely the Broadband Noise Jamming (BBNJ) and Partial Band Nose Jamming (PBNJ).

3.2.1. Broadband Noise Jamming (BBNJ)

The broadband noise jamming injects the noise power across the entire spectrum bandwidth of the target system and affects all the spectral components equally. Jamming signals using BBNJ are very similar to the AWGN and modeled as zero mean Additive White Gaussian Noise (AWGN) with jammer power denoted as "J" and power spectral density "N_j" (measured in Watts/ Hz). The main factor that limits the performance of BBNJ is that the finite amount of jammer power is spread over a larger bandwidth which results in low level of N_j. BBNJ can be viewed as a noise waveform having constant flat Power Spectral Density (PSD) over entire target system's bandwidth. The double sided power spectral density of the jamming signal is denoted as N_j / 2 and total jamming power "J" spread over a bandwidth "B" Hertz is given as

$$\mathrm{J} = 2\ \mathrm{B}\ \frac{\mathrm{Nj}}{2} = \mathrm{B}\ \mathrm{Nj} \qquad \text{(Eq. 3.2)}$$

Double sided power spectral density of the broadband noise is depicted Figure 3-1.

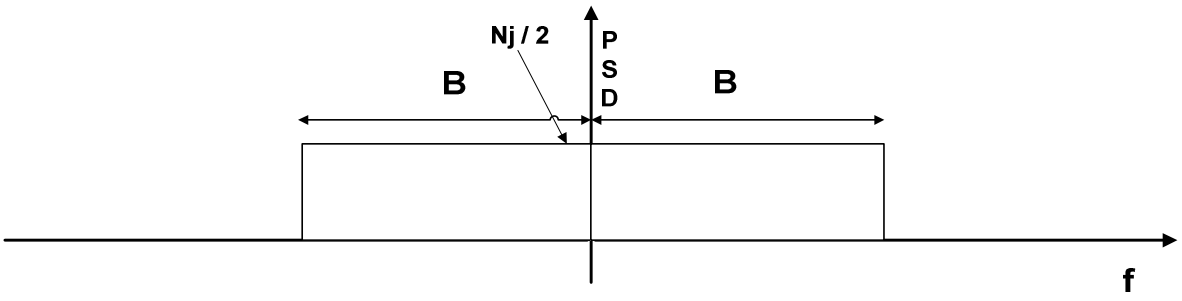


Figure 3- 1: Double sided Power Spectral Density (PSD) of BBNJ signal

For our purpose BBNJ signal is generated using "AWGN" channel class in IT++. This command is used to simulate the BBNJ signal, because, as mentioned earlier, BBNJ can be regarded as an AWGN signal. The input parameter for this command is the variance of the noise to be generated. For real valued signals, it denotes the noise variance per real dimension while for complex valued signals it is regarded as noise variance per complex dimension i.e. sum of the variances in real and imaginary parts. As our signal is a QPSK modulated and complex valued, the noise variance is set equal to the required jamming power spectral density N_j. Figure 3-6 shows the power spectral density of the generated BBNJ signal.

3.2.2. Partial Band Noise Jamming (PBNJ)

Partial Band Noise Jammer (PBNJ) is very similar to the BBNJ; however, PBNJ is band limited in nature. It is modeled as zero mean Additive Gaussian Noise (AGN) with most of its power concentrated in a limited portion of entire bandwidth. This is considered as more effective than BBNJ as more power is injected in smaller bandwidth to interfere with the original signal.

If we keep the total jamming power constant and reduce the bandwidth in Eq.3.2 then the resulting power spectral density (flat over the limited bandwidth) for PBNJ is higher than that of BBNJ. In practice the band limited Gaussian noise (PBNJ signal) can be generated by passing the additive white Gaussian noise (AWGN) through a filter of desired type and bandwidth. Such a filtering operation eliminates the whiteness of the noise and band limits it as illustrated in Figure 3-2.

Figure 3- 2: Generation of PBNJ Signal by filtering AWGN

The double sided PSD of the PBNJ is shown in Figure 3-3

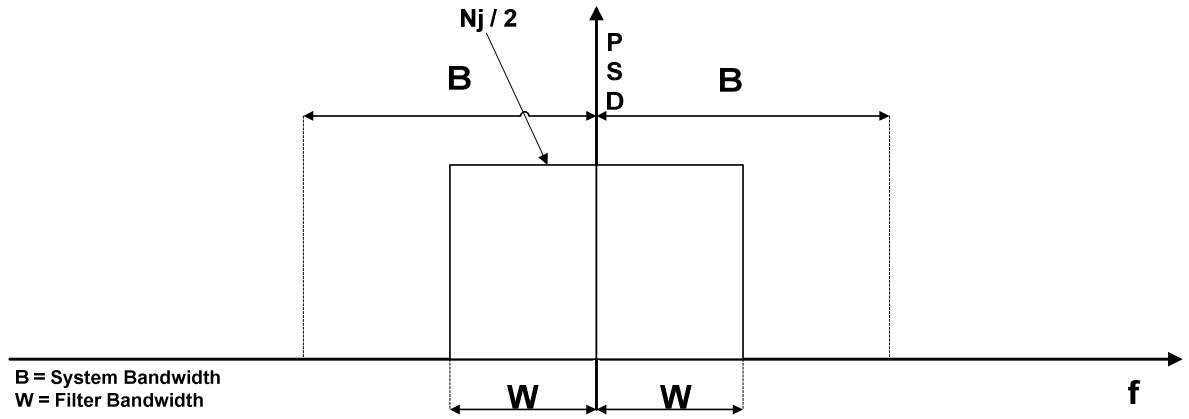


Figure 3- 3: Double sided Power Spectral Density (PSD) of the PBNJ signal

We designed the desired filter in MATLAB. Of many available choices, we chose to use a low pass filter for the sake of simplicity. An 6^{th} order low pass digital butterworth filter with the normalized cut off frequency Wn is designed using the command

[b,a] = butter(n,Wn,'ftype')

Where
n = Order of the filter
Wn = Normalized cut off frequency
ftype = Filter type i.e. lowpass, highpass etc.
b,a = Filter coefficients

Several low pass filters using the same command were generated with different cut off frequencies to investigate the effect of varying jamming bandwidth. Four different low pass filters with normalized cut off frequencies of 0.2, 0.4, 0.6 and 0.8 corresponding to the cut off frequencies of 1, 2, 3 and 4 MHz respectively were generated. These filters were tested for their effectiveness in order to select the bandwidth to give the optimal jamming performance. Figure 3-4 shows the plots of FER vs. the JSR for the PBNJ generated with low pass filters of different bandwidths. It turned out that the filter with the bandwidth of 2 MHz was the best performer so this was used for the simulations.

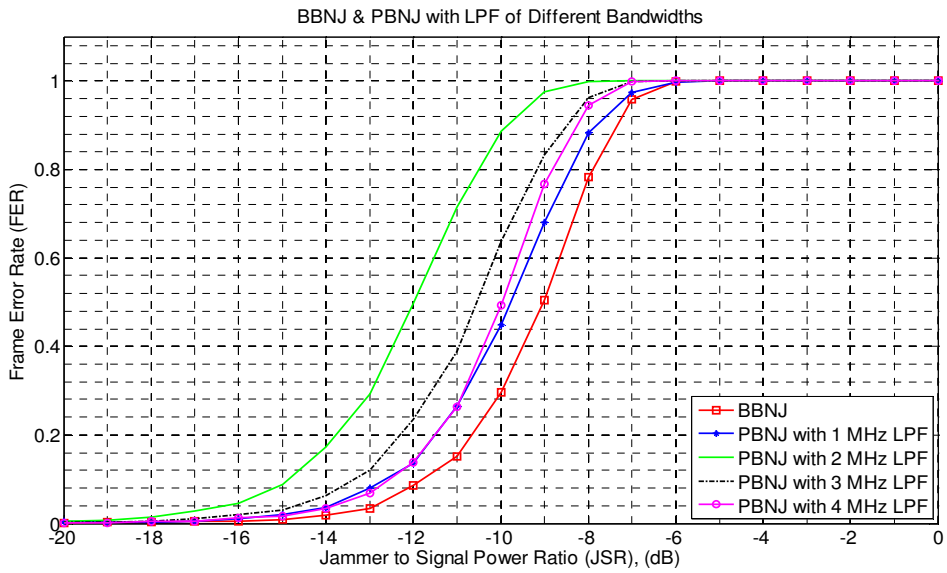


Figure 3- 4: BBNJ vs.PBNJ with Different Bandwidths

The filter coefficients from MATALB were then exported to the IT++ and a broadband noise signal was generated and filtered using the "filter" command from the IT++ library resulting in PBNJ signal. In the generation of PBNJ signal, an important thing to take care of was the power of the broadband noise signal fed to the input of the filter. In order to make a fair comparison, the total jamming power was kept constant for both BBNJ and PBNJ. This corresponded to a higher value of PSD in case of PBNJ as compared to BBNJ signal so power of the broadband noise at the filter input was adjusted to get the same average jamming power at the filter output.

Figure 3-5 depicts the transfer function of the designed low pass filter. The PSD of PBNJ signal compared to PSD of BBNJ signal is plotted in Figure 3-6.

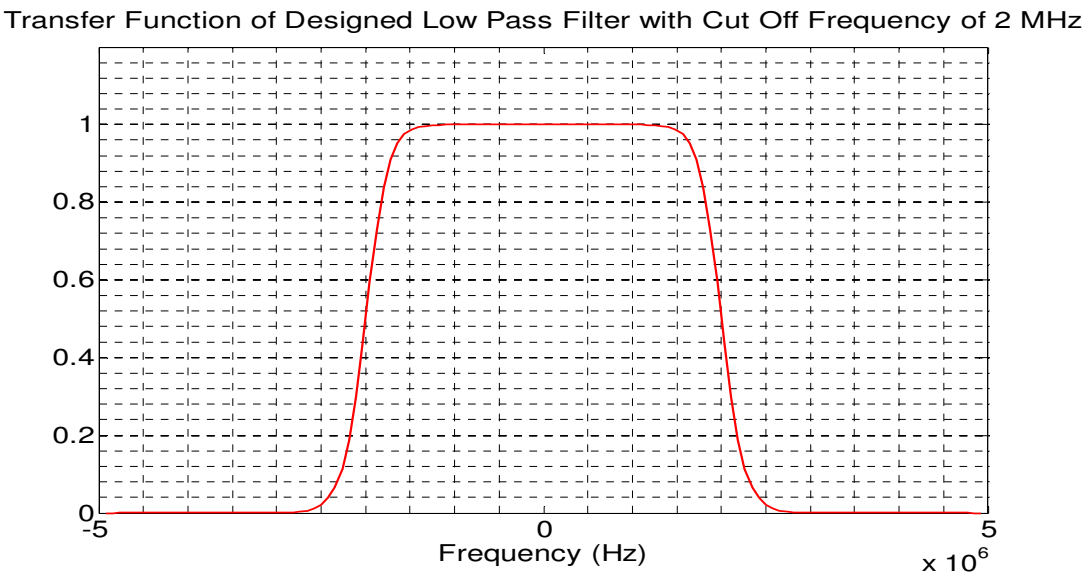


Figure 3- 5: The designed low pass filter transfer function (Cut off frequency = 2 MHz)

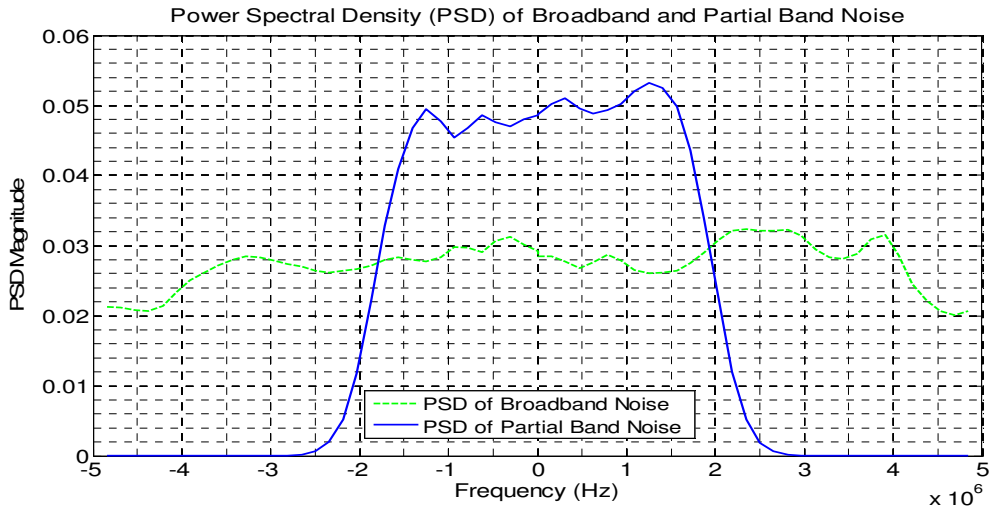


Figure 3- 6 : Power Spectral Density (PSD) of the generated PBNJ signal

From Figure 3-6, we can see that power spectral density is approximately flat over the desired bandwidth for both types of jamming signals. The small deviations from the constant behavior can be attributed to the lesser number of generated samples. It is investigated, using simulations, that as the number of generated noise samples increases, the PSD tends to be more flat.

3.3. Tone Jamming

Tone jamming is one of the numerous waveforms that can be considered to jam the desired signal. Tone jammer consists of N_t tones (N_t>0). These jammer tones are usually sinusoidal. To dominate target system jamming tones must have enough power [11] [12]. Mathematically tone jamming signal can be described as

$$j(t) = \sum_{m=1}^{Nt} A_m \, e^{(2\pi f_m t + \varphi_m)} \qquad \text{(Eq. 3.3)}$$

where N_t represents number of jammer tones, A_m is amplitude of the m^{th} tone at the frequency f_m and φ_m is the uniformly distributed phase between 0 and 2π. $j(t)$ is assumed to have total power J, which is evenly divided among N_t jammer tones. Following equation shows this mathematically.

$$P_m = \frac{J}{N_t} \qquad \text{(Eq. 3.4)}$$

where P_m represents the power of each tone and J is the total jammer power. Power spectrum is amplitude spectrum squared; this relationship is used to calculate the amplitude of each tone. As shown in Equation 3.5.

$$A_m = \sqrt{P_m} \qquad \text{(Eq. 3.5)}$$

As discussed in chapter 2, OFDM symbol consists of 64 sub carriers, 52 out of these are used for transmission and remaining 12 are used as a guard on both side of the band. For data transmission 48 sub carriers are used and remaining 4 are used as pilot sub carriers. Pilot sub carriers help the receiver to decode the data by providing channel knowledge. These 52 used sub carriers ranges from -26 to 26, where pilot sub carriers are present at sub carrier number -21,-7, 7 and 21 as shown in figure 3-7.

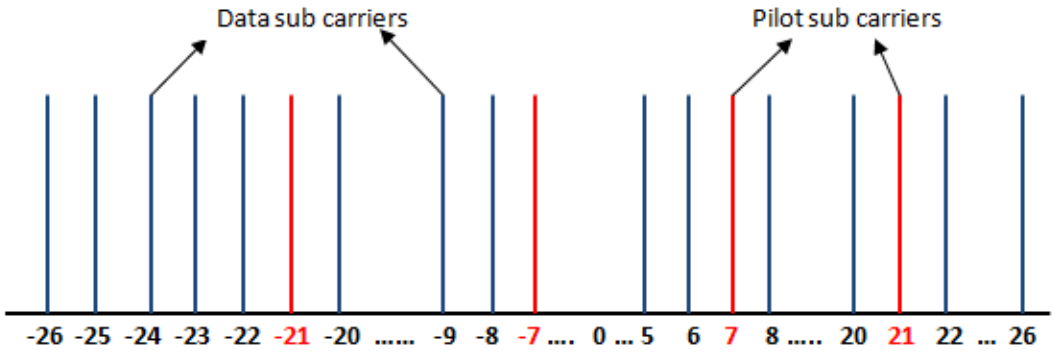


Figure 3- 7: Data and Pilot sub carriers

Figure 3-7 shows 52 equally distributed sub carriers, data sub carriers are shown in blue color and 4 pilot sub carriers are represented by red color. There is no sub carrier at '0' or in other words we can say there is no DC component. Each sub carrier has a specific frequency and these sub carriers are apart from each neighboring sub carrier by certain spacing in frequency.

If the original transmitted signal is observed in frequency domain, the frequencies where sub carriers are present are called as mark frequencies, where as frequencies those are not assigned to any sub carrier, are named as space frequencies [13]. Figure 3-8 shows the phenomenon, blue lines depict mark frequencies and gap between these lines are space frequencies. Now if we assume that the jammer has exact knowledge of the mark frequencies and the jammer tones have larger power than the transmitted tone then the probability of symbol to be jammed is quite high.

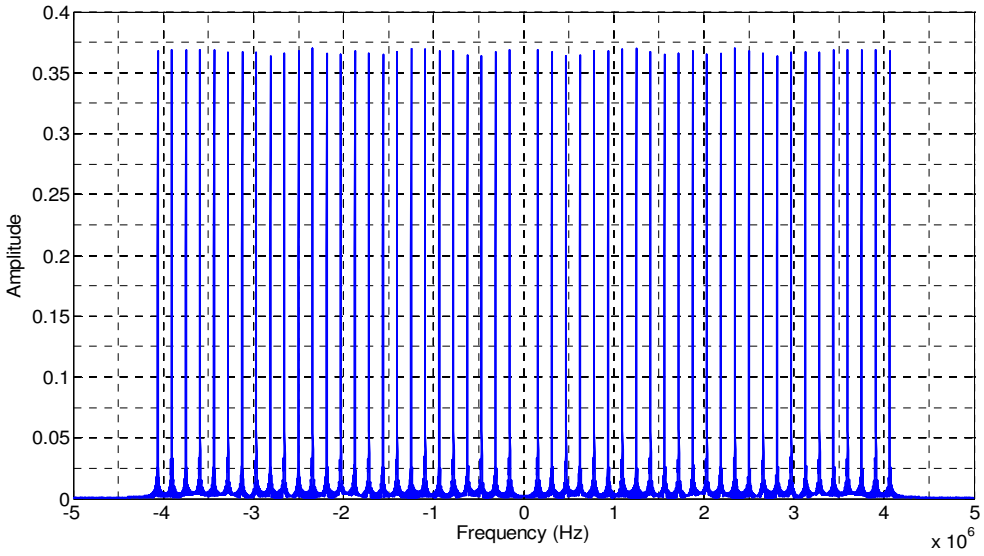


Figure 3- 8: The space & mark frequency

Tone jammer can be utilized in different ways. Following are some possible implementations of this technique utilized in this study.

3.3.1. Single Tone Jamming (STJ)

As mentioned earlier, Nt in the Eq. 3.3 represents number of jammer tones. In the case of Nt= 1, there will only be one jammer tone injected in the channel, and then this jamming technique is known as single tone jamming. Figure 3-9 shows the frequency spectrum of STJ. Mathematically STJ can be represented as

$$j(t) = A_m \, e^{(2\pi f_m t + \varphi_m)} \qquad \text{(Eq. 3.6)}$$

As there is only one tone, the power of the tone needs to be quite high to dominate the signal tone. Now for successful jamming it is required to have exact knowledge of mark frequencies. Choice of f_m is made by selecting f_m randomly from these 48 data carrier's frequencies, we call it randomly selected single tone jamming.

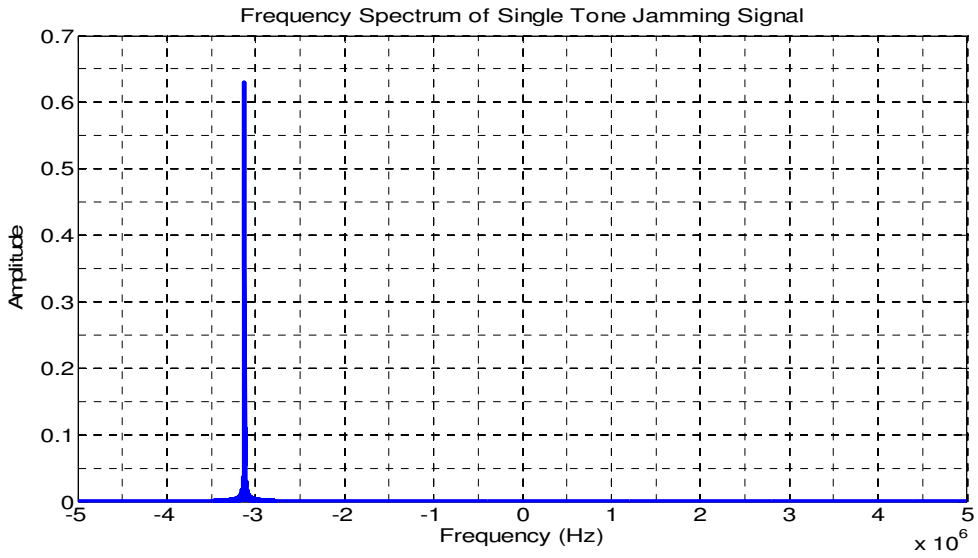


Figure 3- 9 : Single tone Jammer signal

3.3.2. Multi Tone Jamming (MTJ)

Multi tone jamming can be described in an identical manner as single tone jamming. Recall Eq. 3.3, now if Nt >1 then $j(t)$ will be called as multi tone jamming signal. When the value of Nt= 52, it means each sub carrier will have one jamming tone, Eq. 3.3 can be written as

$$\mathrm{j(t)} = \sum_{\mathrm{m=1}}^{52} \mathrm{A_m}\, \mathrm{e}^{(2\pi \mathrm{f_m t}+\varphi_{\mathrm{m}})} \qquad \text{(Eq. 3.7)}$$

Another possible way to analyze the performance of tone jamming could be jamming the pilot subcarriers. There are four pilot carriers in each OFDM symbol, so the jammer power for each tone will be quite high as a result of lesser number of jammer tones. Now if we assume that jammer has the knowledge of pilot subcarriers' locations and tones generated by jammer exactly hits the location, then the transmitted symbol will be probably corrupted. In this case, the total power J will be divided among 4 jamming tones. Eq. 3.3 can be written as

$$\mathrm{j(t)} = \sum_{\mathrm{m=1}}^{4} \mathrm{A_m}\, \mathrm{e}^{(2\pi \mathrm{f_m t}+\varphi_{\mathrm{m}})} \qquad \text{(Eq. 3.8)}$$

f_m (m= 1, 2, 3, 4) will be frequencies of pilot sub carriers. When a certain amount of power is divided among number of tones (N_t = 4), pilot jamming tones will have higher power than the other scenario where each sub carrier has one jammer tone (N_t = 52). Figures 3-10 and 3-11 show the difference between these two techniques.

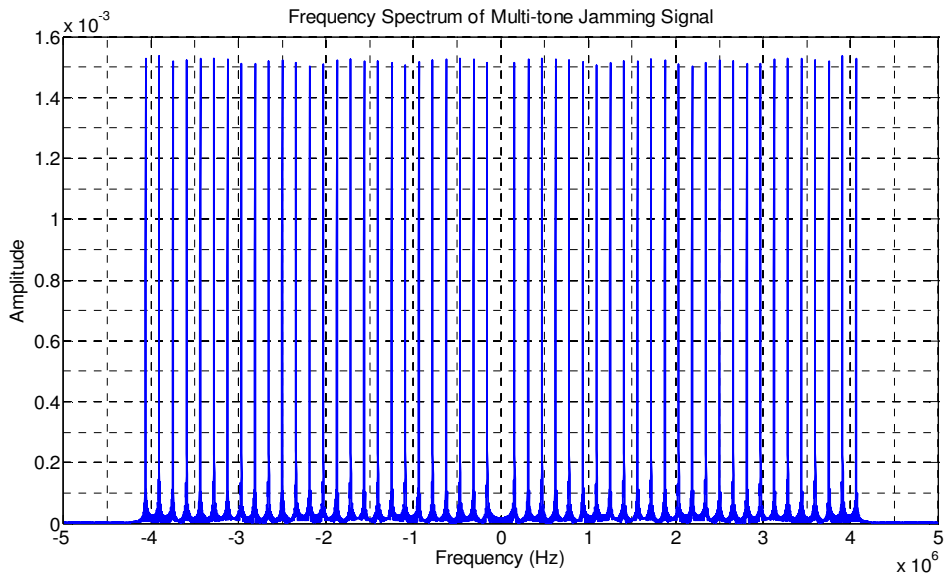


Figure 3- 10: Multi tone jamming, $\mathbf{Nt = 52}$

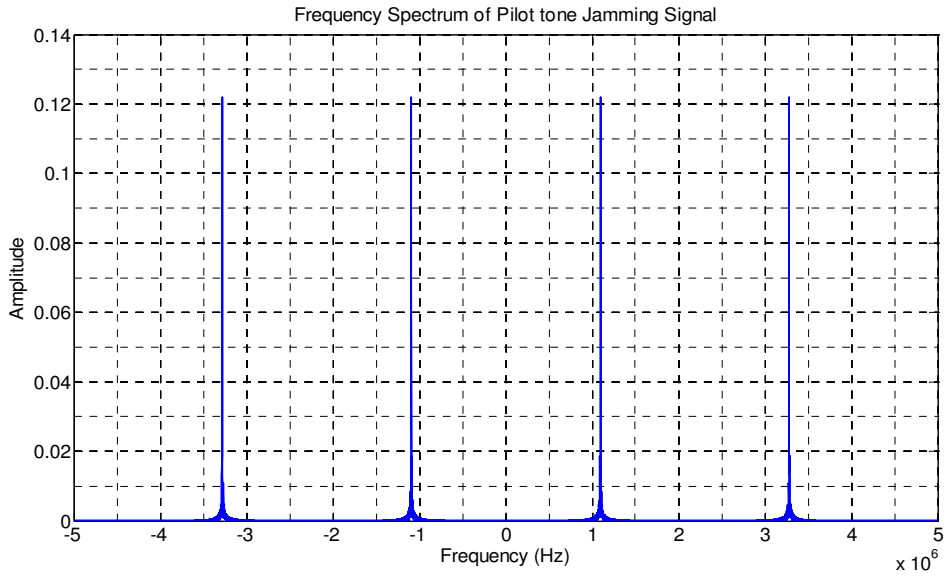


Figure 3- 11: Pilot tone jamming, $\mathbf{Nt = 4}$

3.4. Follower Jamming

In its most basic form, the follower jamming is transmission of replicas of the original signal. This kind of jamming can take two forms – Intercepting the original transmitted signal and retransmitting it with increased power or evaluating the different parameters of the original signal and transmitting artificially generated dummy replicas of that signal. The former type can actually be regarded as an intentional jamming situation while the latter can be categorized under both the intentional jamming scenario and

interference scenario. Either way, such kind of retransmission acts as interference by causing the multiple copies of the same signal at the receiver and degrades its decoding capabilities.

We chose follower jamming as a signal with same parameters but different payload. With this configuration, the preamble and the header field are identical for the original and the jamming signal. The follower jammer signal is depicted in Figure 3-11

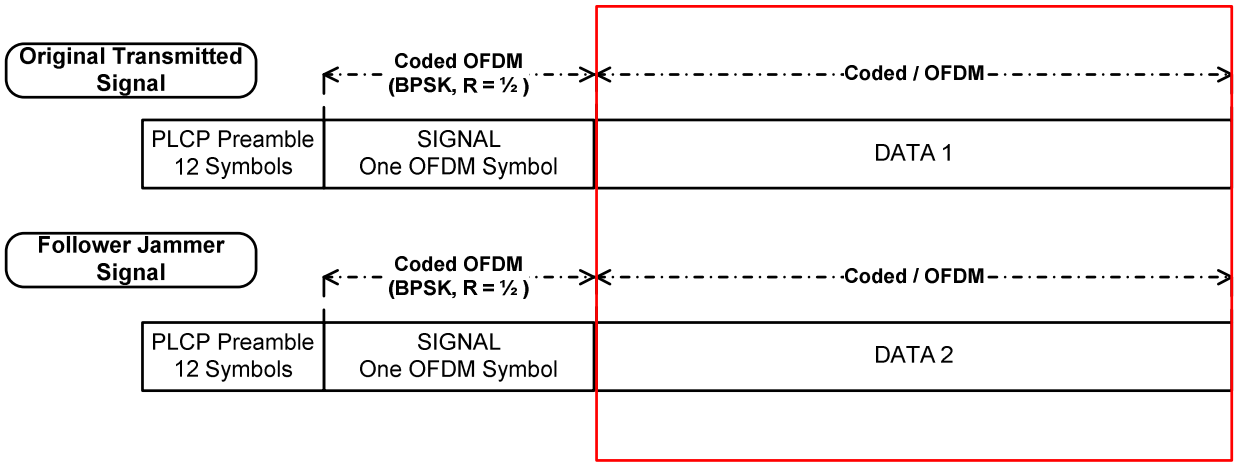


Figure 3- 12: Follower jammer signal

Chapter 04: Channels Description

This chapter deals the wireless channels used for the simulations. These include AWGN and vehicular channels

4.1. Additive White Gaussian Noise (AWGN) Channel

This channel is characterized by wide band noise alternatively known as white noise and simply added to the transmitted signal at the receiver. It has a constant power spectral density (PSD) over entire range of bandwidth under consideration. It has the amplitude distribution known to be Gaussian or normally distributed. This does not include the effects such as frequency and time selectivity, dispersion and non-linearities. Although this channel model is not very practical but it is used widely. The reasons for its use include understanding and modeling the communication systems in a simplest form before moving on to the complex channel models.

In order to have an idea about the behavior of our simulator, we started with AWGN channel following the reasoning as mentioned before. The following section gives the details of the more complex vehicular channels that were used for the simulations.

For AWGN channel, the received signal is simply the sum of the original signal, the channel noise and the jammer signal. This can be written as

$$r(t) = s(t) + n(t) + j(t) \qquad \text{(Eq. 4.1)}$$

Where

r (t) = Received Signal
s (t) = Transmitted Signal
n (t) = Noise Signal
j (t) = Noise Jammer Signal

4.2. Vehicular Channels

Recently Guillermo Acosta-Marum and Mary Ann Ingram of Georgia Institute of Technology have presented six different small scale fading models, presented in [1]. These small scale fading models as named in table 4-1 were created to support the IEEE 802.11p, wireless access in vehicular environments (WAVE)/ dedicated short range communications (DSRC). Another motivation behind these channels is the development of the basis for the certification of the compliant transceiver. A brief history of vehicular channel model development was also presented in the same study [1]

Table 4- 1: Six time and frequency varying channel models for vehicular WLAN

Sr. No	Scenario
01.	V2V- Expressway Oncoming
02.	V2V- Urban Canyon Oncoming
03.	RTV- Sub-Urban Street
04.	RTV- Expressway
05.	V2V- Expressway Same Direction with Wall
06.	RTV- Urban Canyon

The future applications of the IEEE 802.11p include transportation safety, toll collection, emergency services etc. In accordance with these applications, the vehicular channels can be classified into two major categories of interest namely vehicle to vehicle (V2V) and roadside to vehicle (RTV) channels. The presented models include both types. Each of these models was a tapped delay line model with each tap process characterized by Rayleigh or Rician fading and Doppler power spectral density (PSD). These small scale fading models included the multipath fading effects only and not the path loss and shadowing.

For our purposes we needed to have two channel models- one for the actual vehicle to vehicle communication of the target system to simulate the major vehicular channel characteristics where both the transmitter and receiver were moving. The second channel was required to incorporate the channel effects in the jamming signal where jammer was stationary and the target vehicle is moving. The choice of the both the channel was critically important in order to have a matching scenario such that both channels must be from expressway or an urban scenario. This was important because the channels were developed separately for the expressway and urban scenarios and thus had different characteristics. In order to develop a logical simulations scenario setup, the channels used for V2V and RTV should, both, fall under the same category.

A V2V- Expressway Oncoming and an RTV- Expressway (RTV) model were chosen to serve the needs respectively. The characteristics of these channel models can be viewed in detail in Table 4-2.

Table 4-2 summarizes the parameters for all the channel models developed originally. In this table, each set of parameters “frequency shift”, “fading Doppler” and “fading spectral shape” mean center frequency, frequency half width of the spectrum and the basic shape of the spectrum respectively and depict a single Doppler spectrum. The first two cells with the “Tap #” column are “1” and “1” while the first two cells in “Path #” columns are “1” and “2” which implies that all models have composite spectrum on the first tap, comprising at least two simple spectral shapes. Whereas for every six element vector, the *i* th element corresponds to the *i* th model as indicated below the table [1].

For vehicular channels the received signal can be described as

$$\mathrm{r(t)} = \mathrm{h1(t)} * \mathrm{s(t)} + \mathrm{n(t)} + \mathrm{h2(t)} * \mathrm{j(t)} \qquad \text{(Eq. 4.2)}$$

Where h1 (t) and h2 (t) are the impulse responses of the fading channels through which original and jammer signals are communicated.

Table 4- 2: Details on Vehicular channel models [1]

Tap #	Path #	Tap Power (dB)	Relative Path Loss (dB)	Delay Value (ns)	Rician K (dB)	Frequency Shift (Hz)	Fading Doppler	LOS Doppler (Hz)	Modulation (Hz)	Fading Spectral Shape
1	1	0.0	[0.0,-1.8, 0.0,0.0, 0.0,-1.4]	0	[-1.6,7.5, -5.3,4.0, 3.3,23.8]	[1451,574, 769,1145, 648,-55]	[60,165, 70,284, 152,1407]	[1452,654, 770,1263, 635,-60]	Rician	Round
1	2	0.0	[-24.9,-30.5, -36.4,-17.6, -21.5,-5.6]	1	n/a	[884,-97, -22,833, 171,-20]	[858,543, 600,824, 823,84]	n/a	Rayleigh	[R,C3, R,R, R,R]
[1,1, 1,2, 2,2]	3	[0.0,0.0, 0.0,-10 -9.3,-11.2]	[-25.5,-25.1, -30.0,-12.9, -11.8,-14.2]	[2,2, 2,100, 100,100]	[n/a, n/a, n/a, n/a, n/a, 5.7]	[1005,-89, 535,707, 582,-56]	[486,478, 376,871, 249,1345]	[n/a, n/a, n/a, n/a, n/a,40]	[Y,Y, Y,Y, Y,I]	[R,C3, R,R, R,C3]
2	4	[-6.3,-11.5, -9.3,-10 -9.3,-11.2]	[-13.1,-27.1, -12.3,-19.0, -18.8,-14.2]	[100,100, 100,101, 101,101]	n/a	[761,-549, 754,918, -119,0]	[655,174, 117,286, 515,70]	n/a	Rayleigh	[C3,R, R,C6, C3,R]
[2,2 3,3, 3,3]	5	[-6.3,-11.5, -9.3,-10 -14,-19]	[-7.5,-17.7, -21.7,-36.4, -17.6,-19.0]	[101,101, 101,102, 200,200]	n/a	[1445,559, 548,-250, 527,-87]	[56,196, 424,936, 223,358]	n/a	Rayleigh	[R,R, R,F, R,C6]
[3,2, 2,3, 3,4]	6	[-25.1,-11.5 -9.3,-17.8 -14.0,-21.9]	[-28.9,-19.5, -24.9,-25.8, -19.9,-21.9]	[200,102, 102,200, 201,300]	n/a	[819,115, -134,21, 62,-139]	[823,757, 530,166, 802,1397]	n/a	Rayleigh	[C3,C6, F,R, F,C3]
[3,3, 3,3, 4,5]	7	[-25.1,-19.0, -20.3,-17.8, -18.0,-25.3]	[-29.3,-17.6, -24.3,-21.2, -23.0,-27.9]	[201,200, 200,201, 300,400]	n/a	[1466,610, 761,677, 497,60]	[75,258, 104,726, 396,522]	n/a	Rayleigh	[F,C6, R,F, C6,C6]
[3,3, 3,3, 4,5]	8	[-25.1,-19.0, -20.3,-17.8, -18.0,-25.3]	[-35.6,-19.9, -25.4,-31.6, -20.8,-30.8]	[202,201, 201,202, 301,401]	n/a	[124,72, 88,-188, 87,-561]	[99,929, 813,538, 851,997]	n/a	Rayleigh	[R,F, C3,R, R,R]
[4,4, 4,4, 5,6]	9	[-22.7,-25.6, -21.3,-21.1, -19.4,-24.4]	[-25.7,-23.3, -26.8,-28.2, -19.4,-24.4]	[300,300, 300,300, 400,500]	n/a	[1437,183, 37,538, 43,50]	[110,653, 802,908, 747,529]	n/a	Rayleigh	[F,C6, C6,R, R,R]
[4,4,	10	[-22.7,-25.6,	[-34.4,-20.6,	[301,301,	n/a	[552,103,	[639,994,	n/a	Rayleigh	[C3,R,

4,4, 6,7]		-21.3,-21.1, -24.9,-28.0]	-28.5,-28.3, -24.9,-28.0]	301,301, 500,600]		752,41, 114,13]	91,183, 742,1572]			R,R, C6,R]
[4,5, 5,5, 7,8]	11	[-22.7,-28.1, -28.8,-26.3, -27.5,-26.1]	[-27.4,-29.8, -31.2,-28.5, -27.5,-31.5]	[302,500, 400,400, 60,700]	n/a	[868,720, 16,674, 38,-6]	[858,220, 807,723, 746,1562]	n/a	Rayleigh	[C6,F, C6,C6, C3,C6]
[n/a,5, 5,5 8,8]	12	[n/a,-28.1, -28.8,-26.3, -29.8,-26.1]	[n/a,-28.0, -41.8,-35.5, -29.8,-28.1]	[n/a, 501, 401,401, 700,701]	n/a	[n/a,-20, -755,-78, 8,4]	[n/a,871, 329,260, 743,81]	n/a	Rayleigh	[n/a,F, R,R, C3,R]

Notes:

1. Data Vector Format: [V2V-Expressway Oncoming, RTV-Urban Canyon,
   RTV-Expressway, V2V-Urban Canyon Oncoming,
   RTV-Suburban Street, V2V-Express Same Direction With Wall]
2. n/a means not applicable
3. Spectral Shapes are Flat(F), Round(R), Classic 3dB(C3) and classic 6dB(C6)
4. Modulation is Rician(I) and Rayleigh(Y)

Chapter 05: Simulation Results and Discussion

This chapter gives a brief description of simulator and simulation results. Simulation results have been categorized according to the channel models simulated.

5.1. Simulator Description

PhyLayerSim is an open source IEEE 802.11 simulator available at sourceforge website [14]. This simulator is being developed using C++ programming language and IT++ libraries, developed at Chalmers University of Technology. It has a collection of classes and functions that can be used to simulate the physical layer operations of 802.11 (a or p) transmitters and receivers along with the different channel models [14].

The source code of simulator has been divided into different sections accordingly, i.e. signal detection, channels etc. The source files which make actual executables can be found in the trials directory of the source. To meet the scope of the thesis we mainly worked with the trial files and rarely with the other files.

As described in the previous chapter, we simulated our interfering signals on different types of channels so multiple files have been added in the trials directory with names '*finalawgntrial*' and '*finalvechicularTrial'*. These files contain source code for jamming scenarios and jamming signals along with the other required code. Details about jamming signals and channel models were presented in chapter 3 and 4 respectively.

5.2. Simulations Setup

For simulation purposes, executables generated from source code, were used. These simulations were time consuming so help from cluster computing was taken to run these simulations in a better and faster way. A network of computers/ cluster C3SE was used. C3SE is a center for scientific and technical computing at Chalmers University of Technology in Gothenburg Sweden. Parallel or distributed computing options can be enabled. Depending upon nature of job, number of processors and number of nodes can be selected. The job runs until the maximum run time expires, or it finishes within the time specified by user. There will be no interruption or other risks, which can occur on personal computers. The details can be found at [15].

To run the desired simulations, two different types of script files have been used. Job script file, it contains parameters required for cluster computing, such as simulation time, number of nodes, number of CPUs etc. This file is linked with another script file called simulation script. Simulation script file is used to pass input parameters to the executable in the simulator. So it can be said that the job script drives the simulation script which is linked directly with the simulator. These script files are given in the appendix C.

5.3. Frame Decoding and Figures of Merit

The simulator is designed in a manner that a transmitted frame is divided into three main parts namely the preamble, the header and the payload/message just as described in the IEEE 802.11p physical layer specifications [5]. The receiver is designed so that it decodes the received frame step by step. It detects and synchronizes the start of frame and recognizes the preamble first. If it able to do so successfully, it will proceed to detect and decode the header otherwise it will regard it as a preamble error and abort

the decoding process. The same procedure is followed after detecting and decoding the header field. If the header is decoded successfully it goes on to decode the payload else it is considered as header error and the process is aborted. If the payload is not decoded properly, it is regarded as the frame error. The receiver considers a frame as successful if it is able to decode all the three parts of it perfectly.

To compare the performance of the system in the presence of jamming signals, the main quantity that we decided to compare was the Frame Error Rate (FER) because the simulator was designed in a way described above. It is plotted against the JSR. The FER and JSR are defined as

Frame Error Rate (FER) = Number of Unsuccessful frames/ Total number of transmitted frames
Jammer to Signal power Ratio (JSR) = Avg. jammer power/ Avg. signal power

In order to study the maximum effects of jamming on the target signal, a range of parameters was determined before running the actual simulations. So for this reason we determined the values of SNRs at which system performed best without jammer for every type of channel conditions used. Then we injected jamming signals to see the system behavior by varying the jammer to signal power ratio (JSR). These interfering signals are simulated number of times for certain values of JSR and frame size for each scenario. The output of these simulations was ".it" files containing the output parameters like Frame Error Rate (FER) and the range of JSR. These parameters are extracted from ".it" files using the MATLAB and plotted to draw the conclusions.

5.4. Results & Discussion

In this section the simulation results are discussed in detail with the help of plots obtained from the simulations. The result for every jamming type is primarily presented as a plot of FER vs JSR. The header error rate and preamble error rate are also plotted to aid in drawing some conclusions. The curve in the blue color is for preamble error rate, green curve depicts header error rate while red curve represent the frame error rate. The frame errors comprise of header, preamble and payload errors, as it can be also noticed from the figures below.

The frame sizes selected for the simulations are 300 and 800 bytes because these are the sizes of interest for the communication using IEEE 802.11p. In the simulations, each frame size is transmitted 4000 times for every value of SNR or JSR in range, to have a fair error accumulation. For all the simulations, QPSK modulation with convolutional encoder with rate ½ is used to achieve the date rate of 6 Mbps. In addition to that, hard decision decoding is used at the receiver. For the channel estimation, a simple channel estimator is used. This estimator uses a comb type pilot training sequence and at the receiver the linear interpolation is used to estimate the channel conditions for the OFDM symbols.

Six different jamming signals were simulated over AWGN and vehicular channel. The jamming techniques have been divided in to three major categories, noise jamming, tone jamming and follower jamming. The simulation results will be presented one by one in the in the proceeding part of the chapter.

5.5. AWGN Channel

The first step was to see the channel properties and to choose an optimum SNR value for simulations, where SNR here and afterwards is defined as E_b/N_o. In order to do this, simulations were carried out for frame sizes of 300 and 800 bytes in the absence of jammer signals. These were values where FER would approximately be 0. In both cases, as shown in Figures 5-1 and 5-2, this value was approximately 12 dB.

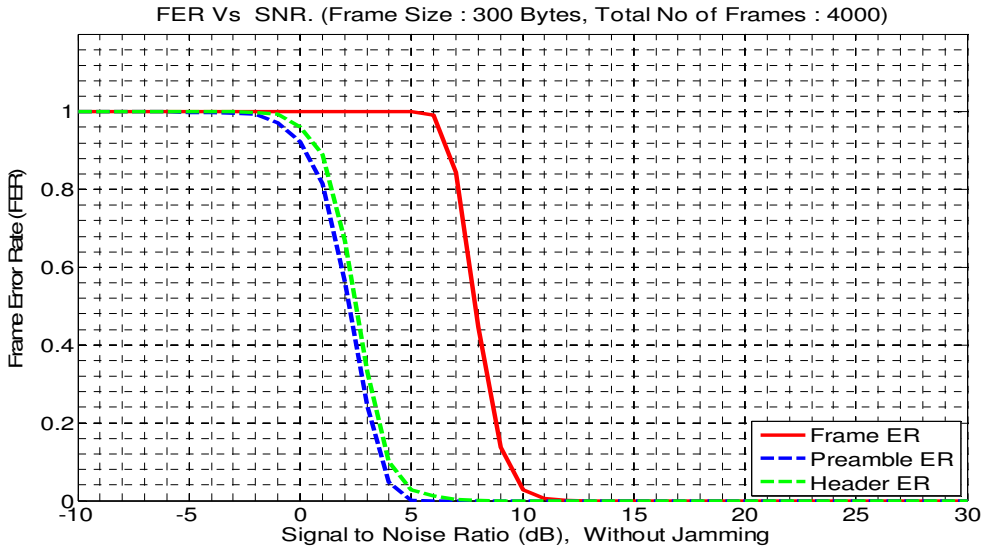


Figure 5- 1: FER vs SNR in AWGN channel without jammer (Frame size= 300 bytes)

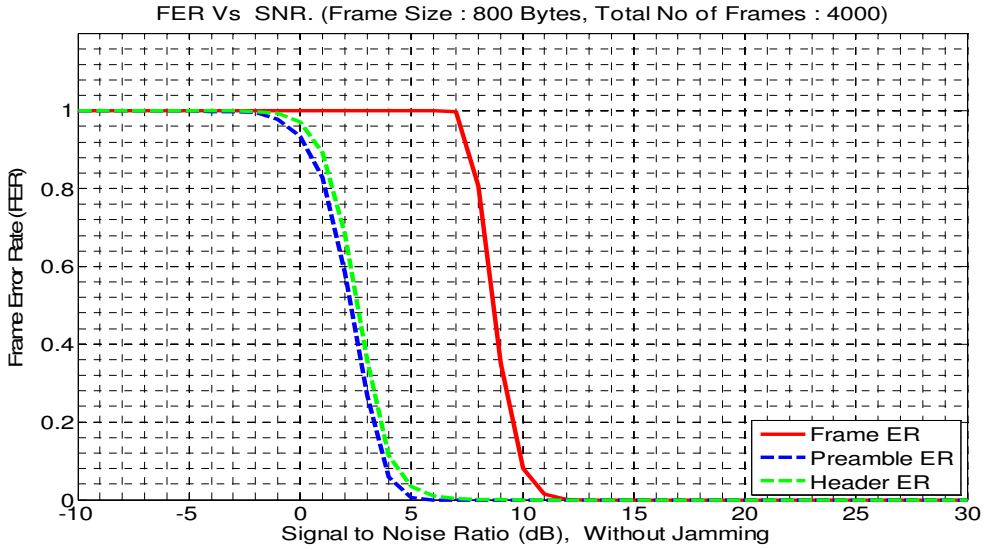


Figure 5- 2: FER vs SNR in AWGN channel without jammer (Frame size= 800 bytes)

5.5.1. Noise Jamming

Noise jamming technique has been discussed in detail in Section 3.2. All the simulations were carried out using the optimum parameters for both cases. In this subsection the results for the BBNJ are presented followed by the results of the PBNJ.

5.5.1.1. Broadband Noise Jamming

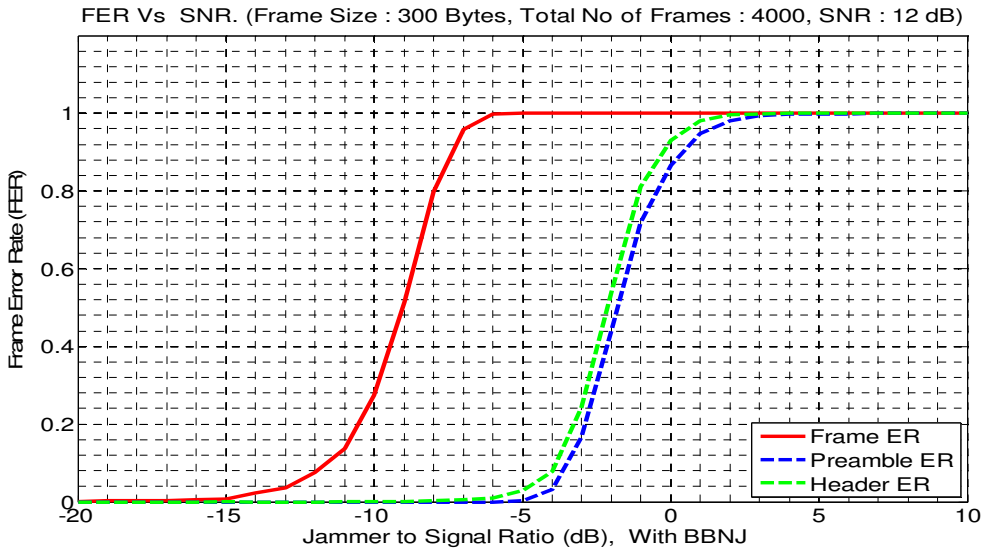


Figure 5- 3: FER vs JSR for BBNJ in AWGN channel (Frame size= 300 bytes)

Figure 5-3 shows the behavior of the IEEE 802.11p in presence of BBNJ with the frame size of 300 bytes. As noticed in previous part, the header and preambles are more resistant to the channel noise, and overall frame errors comprise of header, preamble and payload errors.

In this case the certain jamming noise is distributed over whole band. From Figure 5-3 it can be seen that at a JSR of -6 dB, the FER becomes 1 while header error rate and preamble error rate become 1 at JSR value of 2 dB and 4 dB respectively.

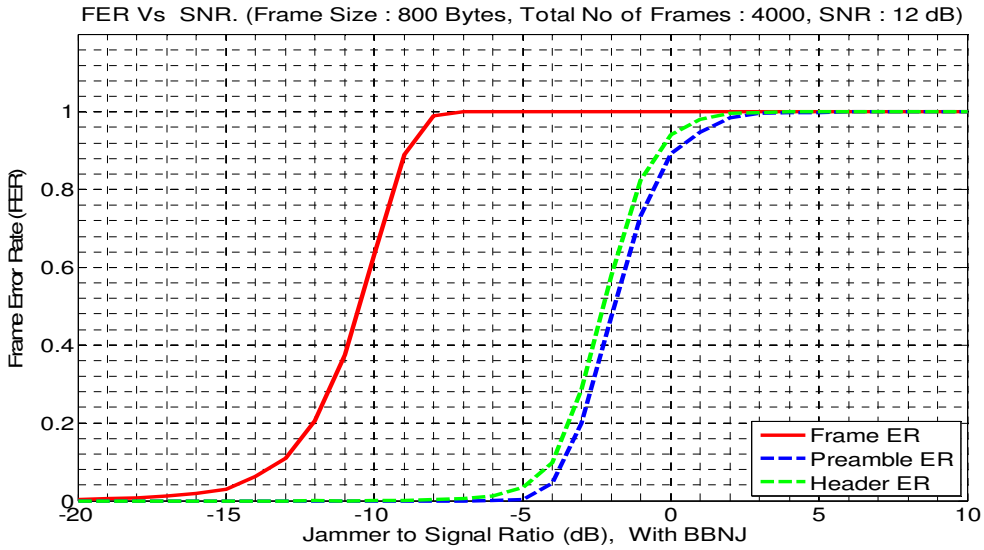


Figure 5- 4: FER vs JSR for BBNJ in AWGN channel (Frame size= 800 bytes)

With the frame size of 800 bytes, the FER becomes 1 at -7 dB and header error rate reaches 1 at a JSR equal to 3 dB and preamble error rate become 1 at a JSR of 4 dB as depicted in Figure 5-4. This represents a very minor effect on error rates, when the payload is increased.

5.5.1.2. Partial Band Noise Jamming

PBNJ signal, generated using a low pass filter with the cut off frequency of 2 MHz, is used for the simulations. The results for the PBNJ are presented in Figures 5-5 and 5-6. The SNR for PBNJ were kept the same as BBNJ. From the Figure 5-5, it can be seen that FER becomes 1 at JSR of -8 dB while header error rate attains the value of 1 at 8 dB and preamble error rate never becomes 1. It starts increasing from JSR of -5 dB and keeps on increasing till 8 dB. After 8dB it becomes saturated and fluctuates between 0.99 and 0.98 but never becomes exactly 1.

For the frame size of 800 bytes, the behavior of curves remains the same but they just got shifted. The FER reaches 1 at -9 dB but the header error rate gets a slight shift towards positive axis and 100% header error rate is achieved at 7 dB. The behavior of preamble remains same as it was in the previous case.

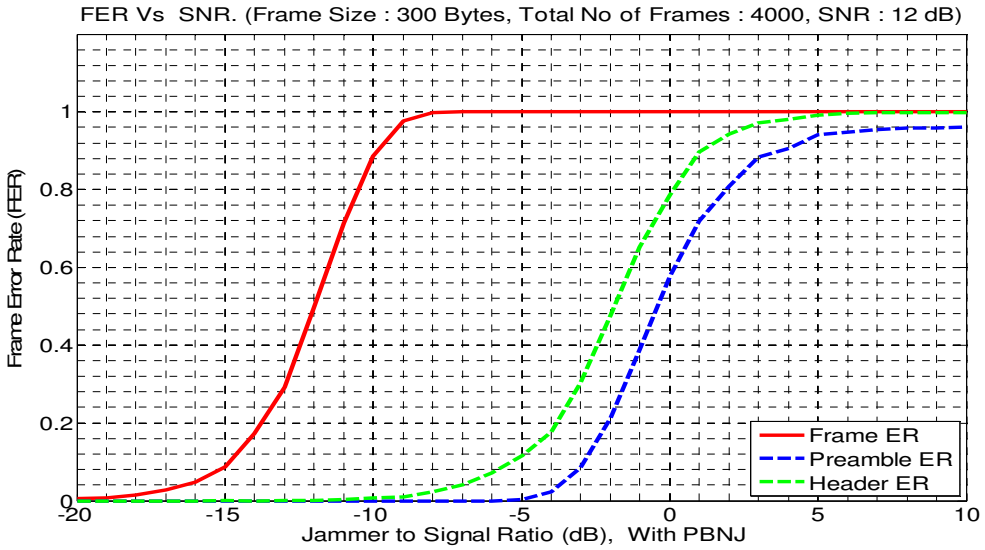


Figure 5- 5: FER vs JSR for PBNJ in AWGN channel (Frame size= 300 bytes)

Comparing the results with the BBNJ using Figures 5-3 and 5-5, it can be seen that the PBNJ is more effective than BBNJ as all the error rates achieve their maximum value at a smaller JSR in case of PBNJ. This phenomenon was described in detail in section 3.2.2 and depicted in Figure 3-6.

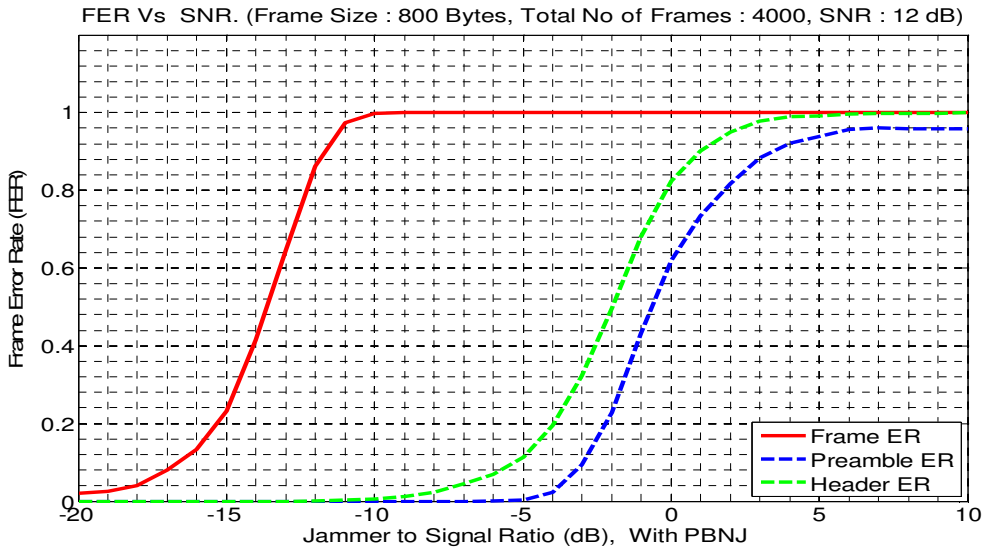


Figure 5- 6: FER vs JSR for PBNJ in AWGN channel (Frame size= 800 bytes)

5.5.2. Tone Jamming

Tone jamming was described in Section 3.3. Three different types of tone signals were simulated as jammer / interference to IEEE 802.11p on AWGN channel. The simulation results of these jamming signals are presented in the following part of this chapter.

5.5.2.1. Multi Tone Jamming

In this particular type of jamming, every subcarrier is subject to the jamming by injecting a tone in each of 52 subcarriers (data and pilot subcarriers). To do this simply a complex sinusoidal was transmitted on every frequency where logically a subcarrier existed.

Figure 5-7 depicts simulation results of multi-tone jamming, simulated on an AWGN channel. Unlike noise jammers, multi tone jamming signal doesn't affect transmission when jammer power is less than signal power. But as the jammer power dominates the signal power, the damage starts. The FER becomes 1 at a JSR of 11 dB. Although all headers become erroneous at 20 dB, but preamble error rate never becomes 1 and beyond 22 dB they fluctuate between 99 to 100%.

For the frame size of 800 bytes, the behaviors of curves remain same but they just get slightly shifted. The FER becomes 1 at 10 dB now instead of 11 dB. The same effect is observed in the header error rate also as, it becomes 1 at approximately 19 dB.

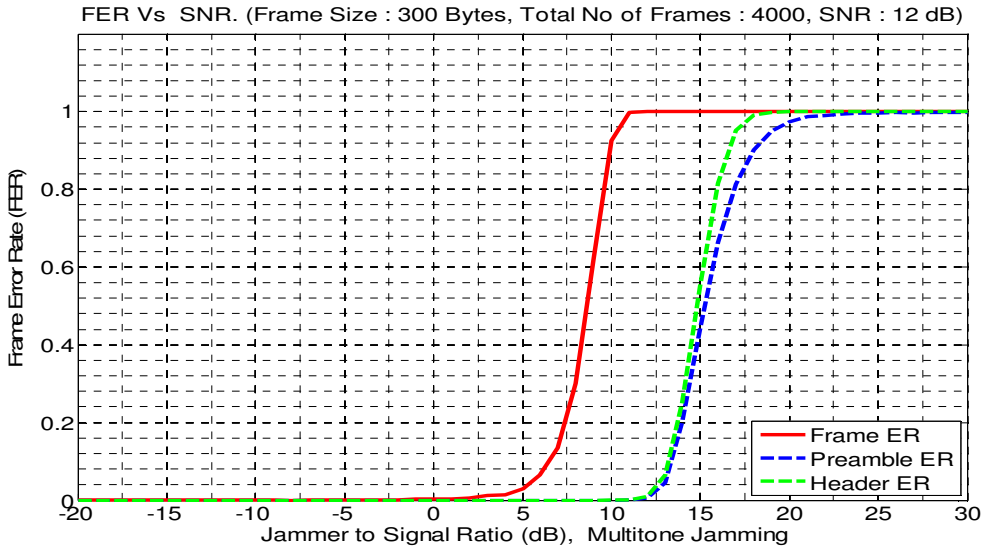


Figure 5- 7: FER vs JSR for Multi-tone jammer in AWGN channel (Frame size= 300 bytes)

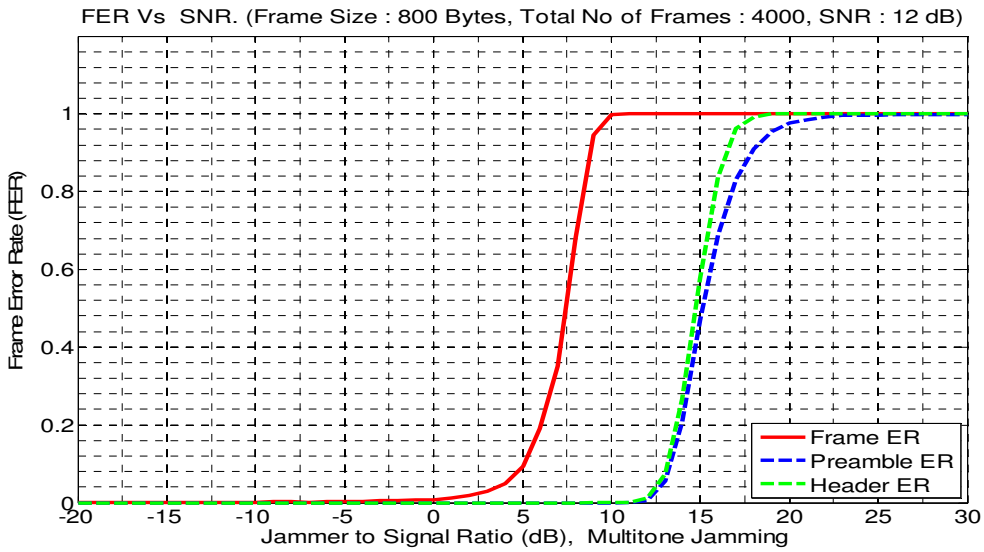


Figure 5- 8: FER vs JSR for Multi-tone jammer in AWGN channel (Frame size= 800 bytes)

5.5.2.2. Pilot Tone Jamming

Pilot jamming is another way of jamming inherited from tone jamming. The details on this type of jamming were described in Section 3.2.2. Figures 5-9 and 5-10 show the simulation results the frame size of 300 and 800 bytes.

Figure 5-9 shows the simulation results of pilot tone jamming, for AWGN channel. In case of multi-tone jamming the interfering tones are injected at all subcarriers which results in the FER increase only after jamming power dominates the signal power. On the contrary, in pilot tone jamming the FER starts to rise well before the jammer power dominates the signal power. This can be attributed to two reasons. First, the same amount of power is distributed between only 4 tones in case of pilot tone jamming scenario. Secondly pilot subcarriers contain channel information and aid in channel estimation so hitting these exactly causes more damage at low JSR. Figure 5-9 shows that FER became 1 at -8 dB and moving further right on the horizontal axis (JSR), header and preamble failure start contributing for high FER until both of these attain the value of 1 at 6 dB.

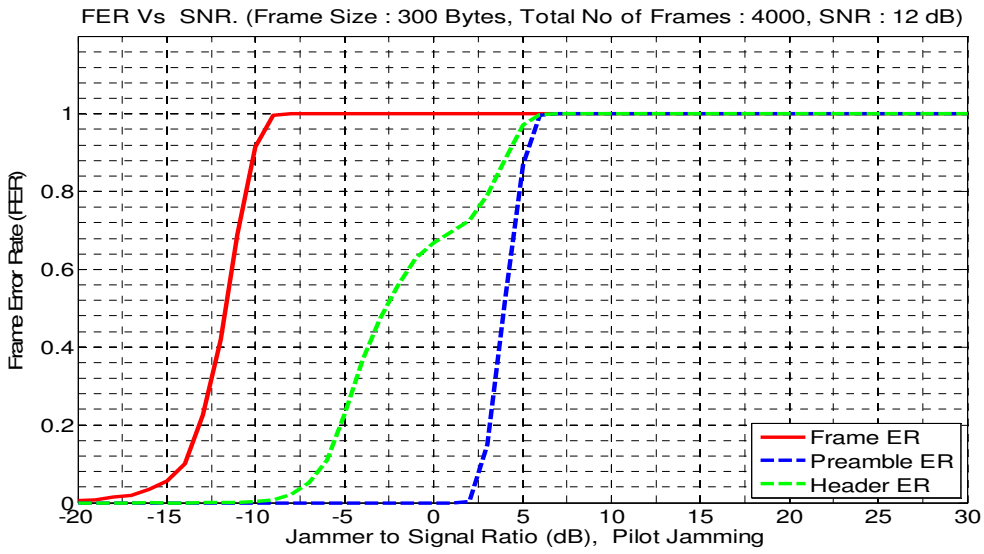


Figure 5- 9: FER vs JSR for Pilot tone jammer in AWGN channel (Frame size= 300 bytes)

Simulation results shown in Figure 5-10 are very much identical to the results shown in figure 5-9. The only noticeable difference in this case is that FER became 100 % at -9 dB. The header and preamble error rate also follow the same trend.

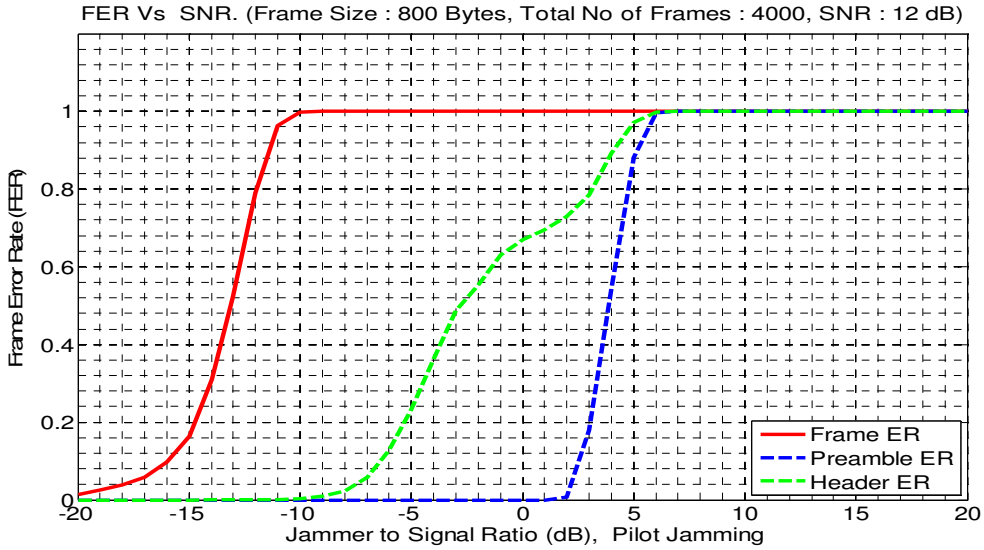


Figure 5- 10: FER vs JSR for Pilot tone jammer in AWGN channel (Frame size= 800 bytes)

5.5.2.3. Single Tone Jamming

In single tone jamming, a single tone is injected at any one of 48 data carrier's frequency selected randomly. The simulation results for frame size 300 and 800 bytes in Figure 5-11 and 5-12 show that frame and header error rate start increasing when the jamming power is quite large than signal power.

It has to be noted that if just one data carrier or pilot carrier is supposed to be jammed, it doesn't affect preamble at all for all JSR values in range. But on the same JSR if we increase number of carriers to be jammed we can see an observable decrease in the successful detection of preambles, as it can be seen in the case of pilot tone jamming. Preamble comprises of 10 short training sequences, assigned to 12 different subcarriers and 2 long training sequences are assigned to all 52 sub carriers.

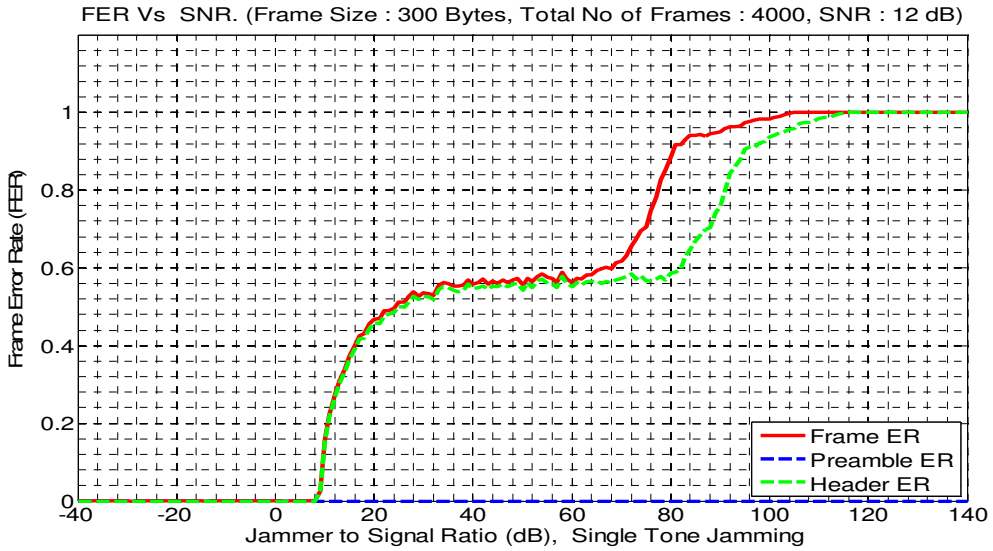


Figure 5- 11: FER vs JSR for Single tone jammer in AWGN channel (Frame size= 300 bytes)

One reason for this behavior could be the simulator structure. The signal detection algorithm was designed based on the correlator structure, discussed in [16]. The input sample was correlated with its delayed sample, according to the periodic characteristic of short training sequence caused by IFFT. The delay amount was 16 because there are 16 samples for a short training sequence. After that, the correlated samples were averaged over a period of time. The average energy of received signal is calculated, the correlation output was normalized. The correlation results were not affected by the signal with the sudden peak. The normalized magnitude of averaged correlated samples was compared with a given threshold. If it is higher than the given threshold then the received sample will be claimed as OFDM symbol [16]. It has been seen that just by jamming one sub carrier; it is not possible to have synchronization error in this setup.

For both 300 and 800 bytes frame size it is noticed the FER and header error rate remains constant for quite longer interval of JSR. The resultant curves show that in this interval, almost all the frame errors are caused by header failures. To completely disable or corrupt the transmission, single tone jammer is required to transmit quite high power. It is seen in simulation results the FER became 100% when JSR is beyond 100 dB which is quite high interfering power.

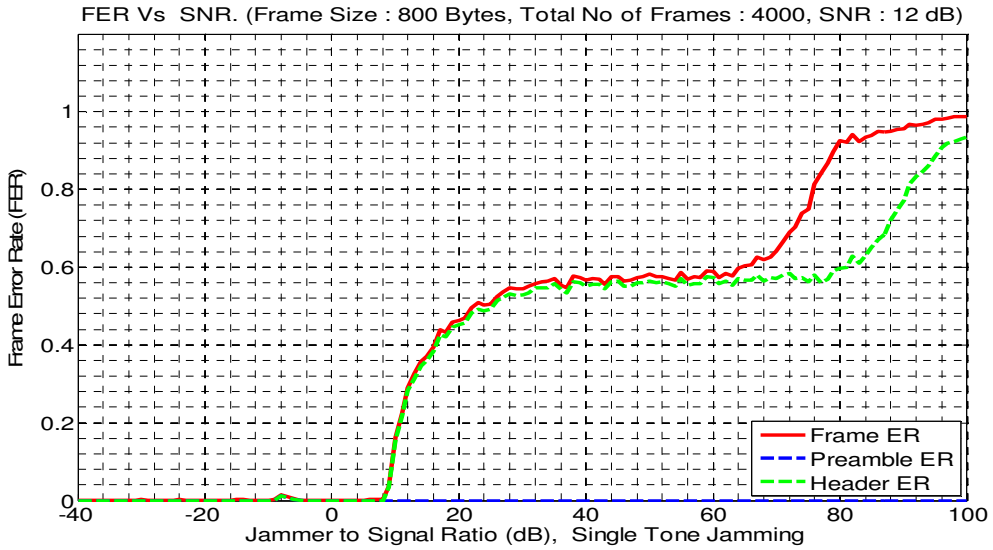


Figure 5- 12: FER vs JSR for Single tone jammer in AWGN channel (Frame size= 800 bytes)

5.5.3. Follower Jamming

The details of follower jammer can be seen in detail in Section 3.4. In Figure 5-13, the results for the follower jammer are presented. The FER attains the value of 1 at the JSR of -2 dB while the header error rate and preamble error rate remain constant at 0. This can be attributed to the fact that the jammer contains the preamble and header (as the RATE and LENGTH field are same) fields that are identical to the original signal. This causes the perfect signal detection and header decoding. The results for the frame size of 800 bytes follow the same pattern and the maximum FER is also achieved at approximately the same value, as shown in Figure 5-14.

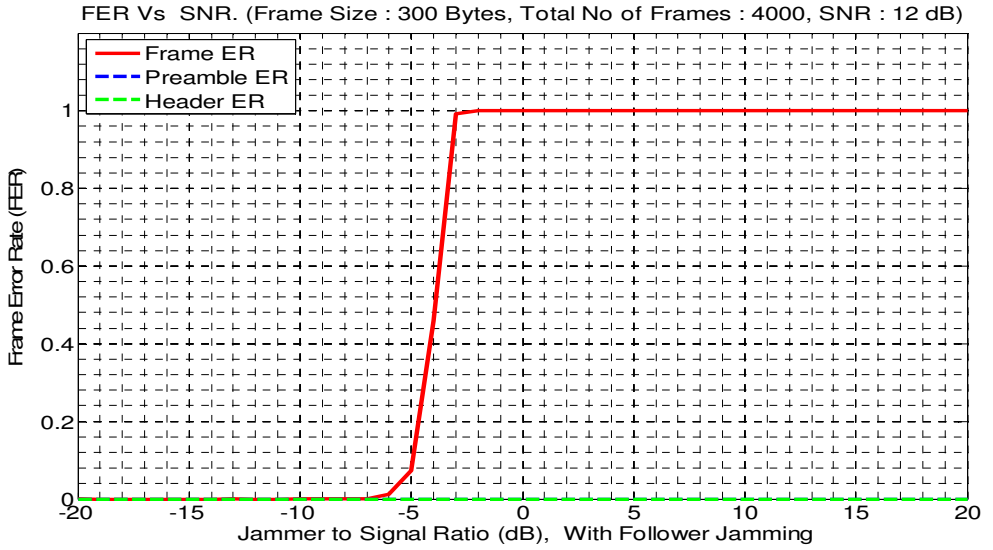


Figure 5- 13: FER vs JSR for follower jammer in AWGN channel (Frame size= 300 bytes)

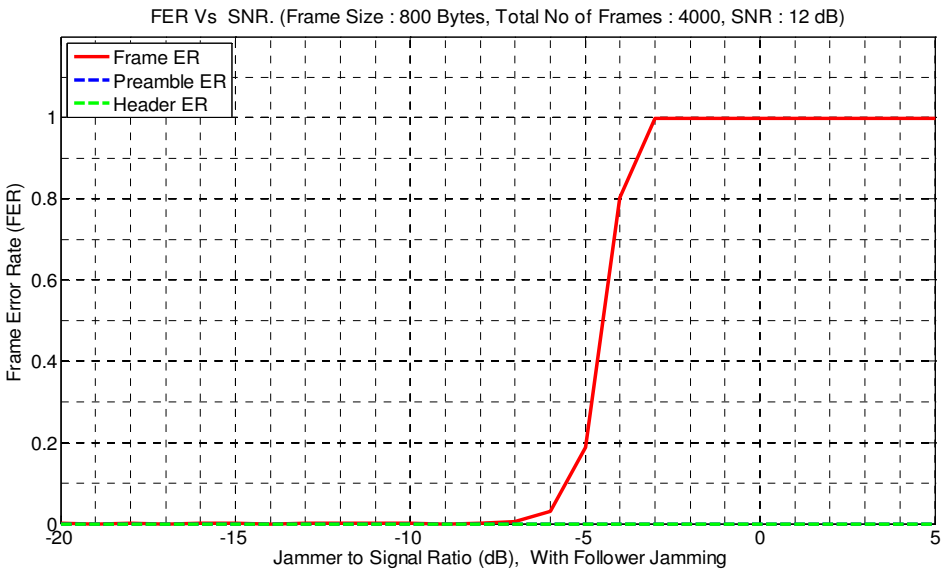


Figure 5- 14: FER vs JSR for follower Jammer in AWGN Channel (Frame size = 800 bytes)

5.6. Vehicular Channel

For the vehicular scenario, one V2V and one RTV channel is selected. The IEEE 802.11p's signal (target) was propagated through the V2V channel to mimic the communication between two oncoming vehicles moving on an expressway in opposite direction. The RTV channel was used for the propagation of the jammer signal to the target signal where jammer was stationary and target vehicle was moving on an expressway. The details about the channels were presented in Section 4.2.

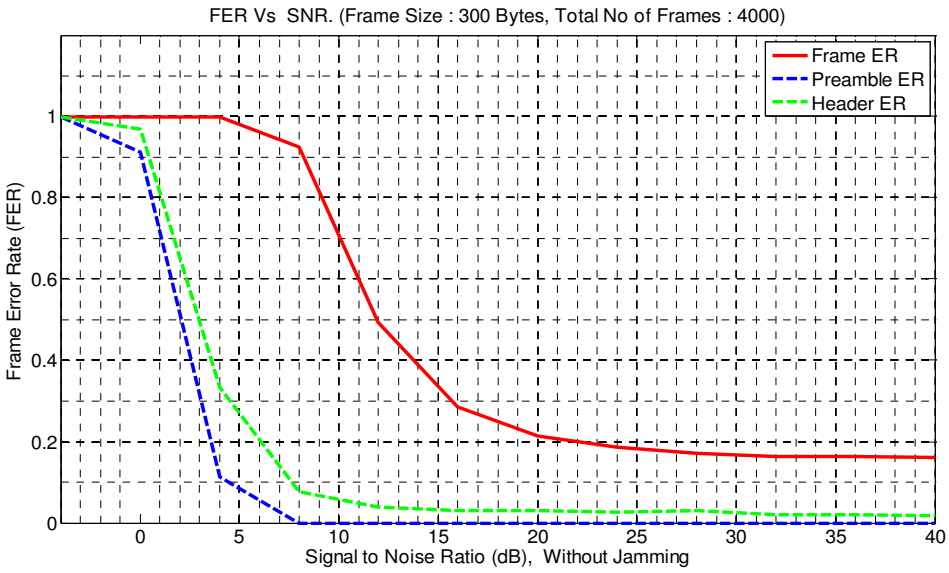


Figure 5- 15: FER vs SNR in vehicular channel without jammer (Frame size= 300 bytes)

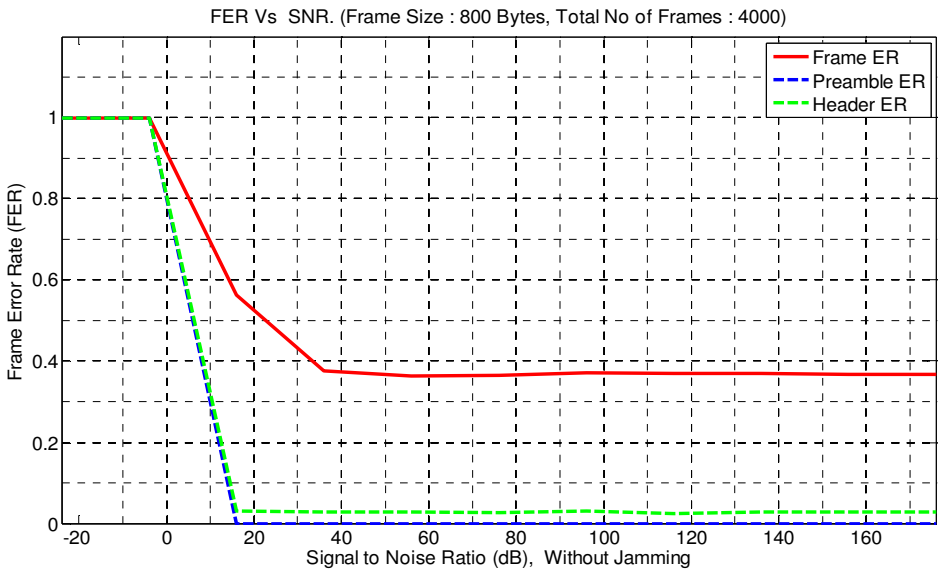


Figure 5- 16: FER vs SNR in vehicular channel without jammer (Frame size= 800 bytes)

The results for all six types of jamming signals are presented in the following subsections with the logical reasoning for their behavior. Figures 5-14 and 5-15 show the results of the simulations performed to find the optimal SNR values to be used in the simulations for the frame sizes of 300 and 800 bytes respectively. This value turns out to be 36 dB, so all the simulations with jammer are done with this SNR value.

In the Figures 5-15 and 5-16, there is an irreducible error floor caused by limited performance of the channel estimator. As mentioned earlier, a simple channel estimator with the linear interpolator is used for channel estimation which has limited estimation capabilities, due to which an irreducible error floor is observed for both frame sizes in the vehicular channels.

5.6.1. Noise Jamming

5.6.1.1. Broad Band Noise Jamming

The simulation results for BBNJ are presented in Figure 5-17 and it turns out that at a JSR of -5 dB the FER reaches its maximum value 1 while header error rate and preamble error rate are maximized at the JSR values of 3 and 4 dB respectively.

Figure 5-18 shows the jammer performance for the frame size of 800 bytes. The results show that all the curves follow the same behavior as observed in the case with the frame size of 300 bytes. The FER reaches its maximum value at a JSR of approximately -7.5 dB.

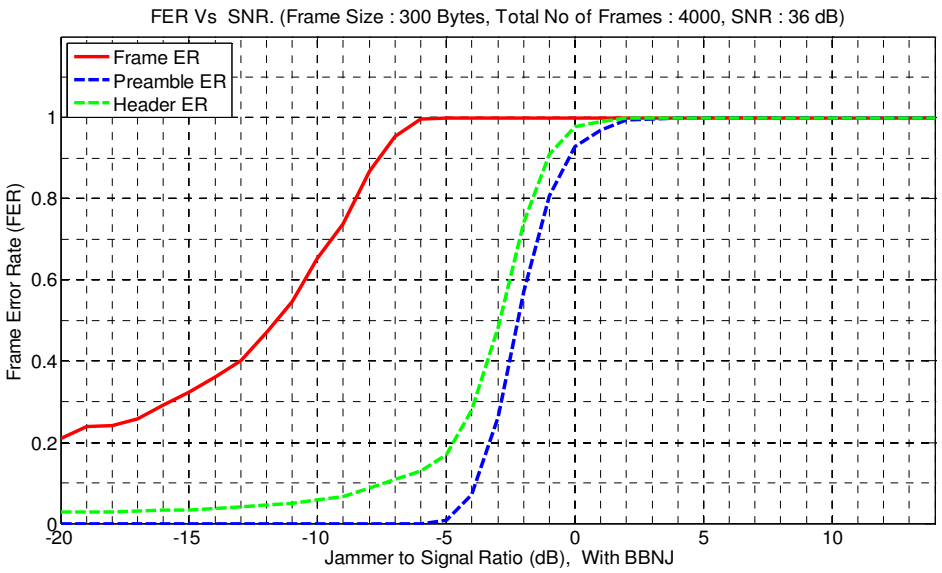


Figure 5- 17: FER vs JSR for BBNJ in vehicular channel (Frame size= 300 bytes)

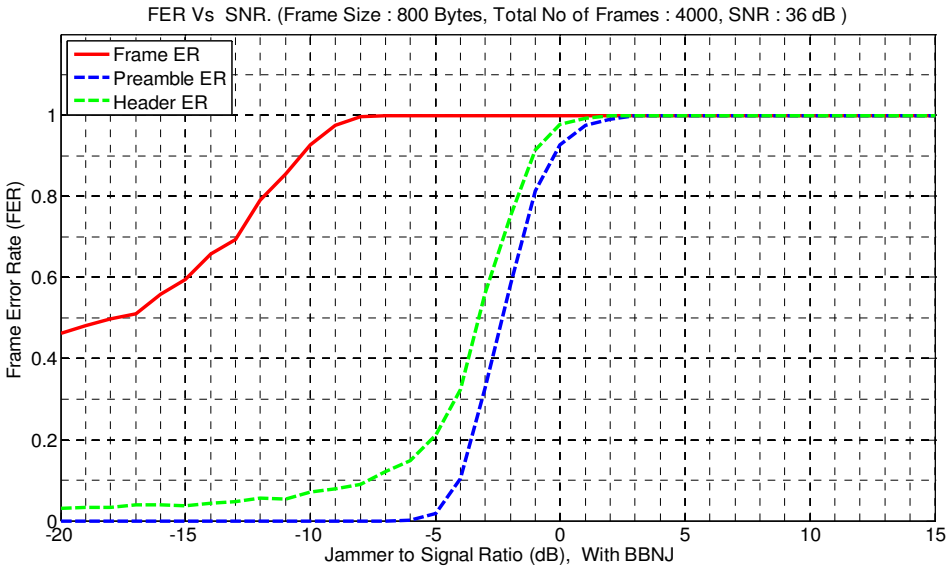


Figure 5- 18: FER vs JSR for BBNJ in vehicular channel (Frame size= 800 bytes)

5.6.1.2. Partial Band Noise Jamming

For PBNJ, the rate of rise of FER is quite high as compared to the BBNJ and it reaches its maximum value at a JSR of approximately -7 dB (Figure 5-19) which is, again, better than BBNJ. This performance edge is a result of the argument presented in the Sections 3.2.2 and 5.5.1.2.

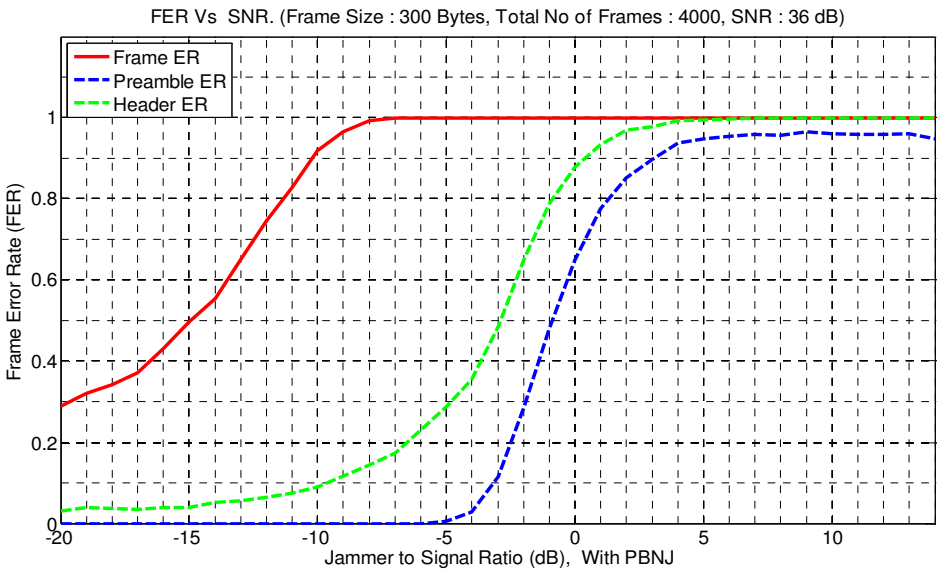


Figure 5- 19: FER vs JSR for PBNJ in vehicular channel (Frame size= 300 bytes)

The results with the frame size of 800 bytes are presented in Figure 5-20. These results are consistent with the results with the smaller frame size. The only difference is that 100% FER is achieved at a JSR of approximately -10 dB.

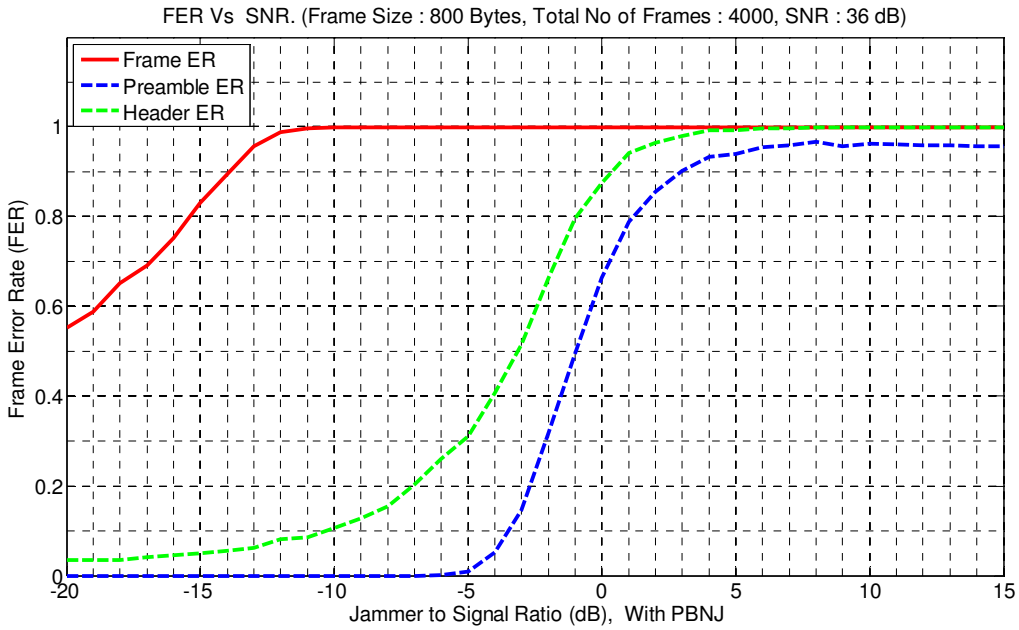


Figure 5- 20: FER vs JSR for partial band jammer in vehicular channel (Frame size= 800 bytes)

5.6.2. Tone Jamming

Tone jamming has been described in the Section 3.3. Three different types of tone signals have been simulated as interference to 802.11p in vehicular channel scenario. The simulation results of these jamming signals are presented in the following subsections.

5.6.2.1. Multi-tone Jamming

Figure 5-21 shows the simulation results for the system performance in presence of multi-tone jammer in the vehicular environment. The analysis shows that the FER reaches its maximum value at a JSR of 16 dB while header error rate and preamble error rate attain their 100 % values at JSRs of approximately 24 and 27 dB respectively. For the frame size of 800 bytes, FER reaches the 100 % value at JSR equal to 14 dB, as shown in Figure 5-22. The preamble and header error rate curves follow the behavior observed in the case of frame size equal to 300 bytes.

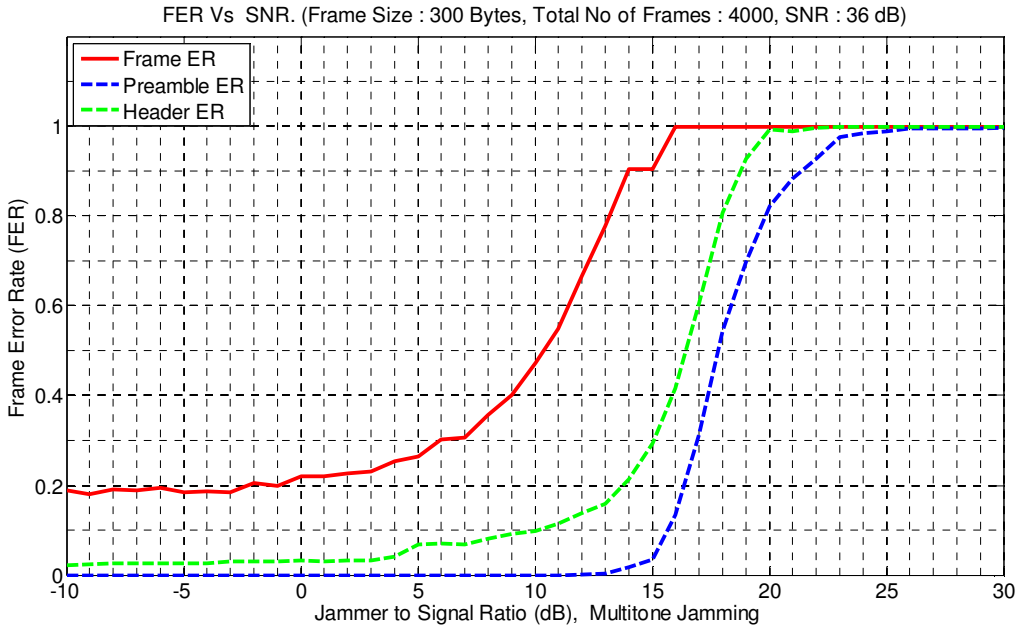


Figure 5- 21: FER vs JSR for multi-tone jammer in vehicular channel (Frame size= 300 bytes)

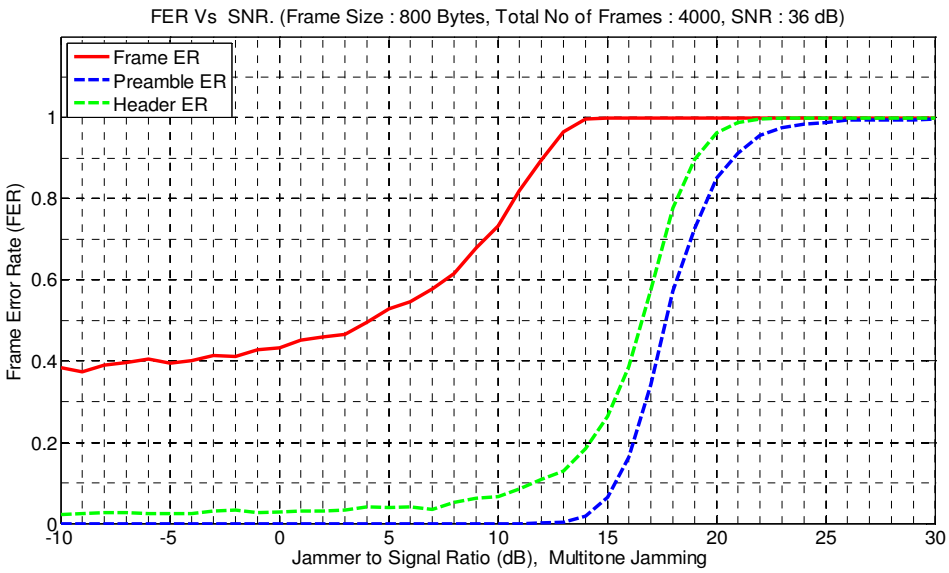


Figure 5- 22: FER vs JSR for multi tone jammer in vehicular channel (Frame size= 800 bytes)

5.6.2.2. Pilot Tone Jamming

In case of pilot tone jamming scenario, the results achieved show the superiority of pilot tone jammer over multi-tone jammer as it achieves the FER value of 1 at JSR of approximately -3 dB as shown in Figure 5-23. The header and preamble error rate also achieve their maximum values following the same reasoning presented in section 5.5.2.2.

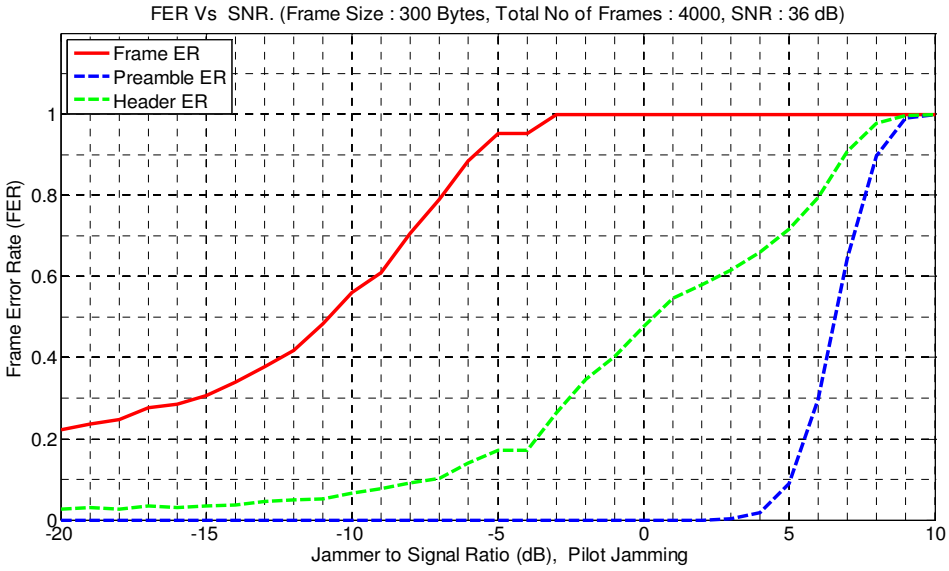


Figure 5- 23: FER vs JSR for Pilot tone jammer in vehicular channel (Frame size= 300 bytes)

The curves for the frame size of 800 bytes, in Figure 5-24, show the same response as those of smaller frame size with FER reaching 1 at a JSR of approximately -5 dB.

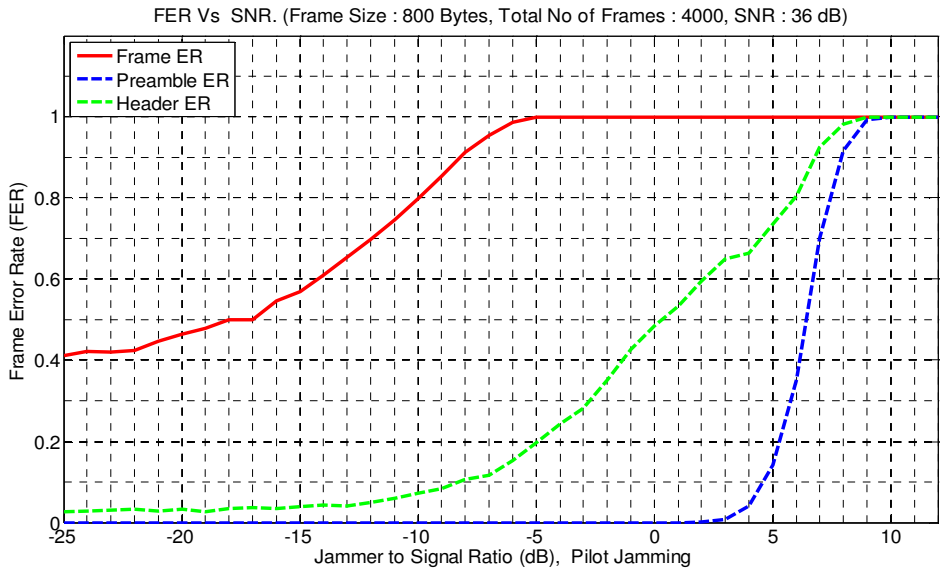


Figure 5- 24: FER vs JSR for Pilot tone jammer in vehicular channel (Frame size= 800 bytes)

5.6.2.3. Single Tone Jamming

Figure 5-25 shows the results for the case of single tone jammer where the maximum value of FER, 100%, is achieved at the JSR value of 41dB. The preamble error rate remains constant at a value of 0 following the reason/ justification presented in section 5.5.2.3. The results with the frame size of 800 bytes also follow the same behavior, as presented in Figure 5-26.

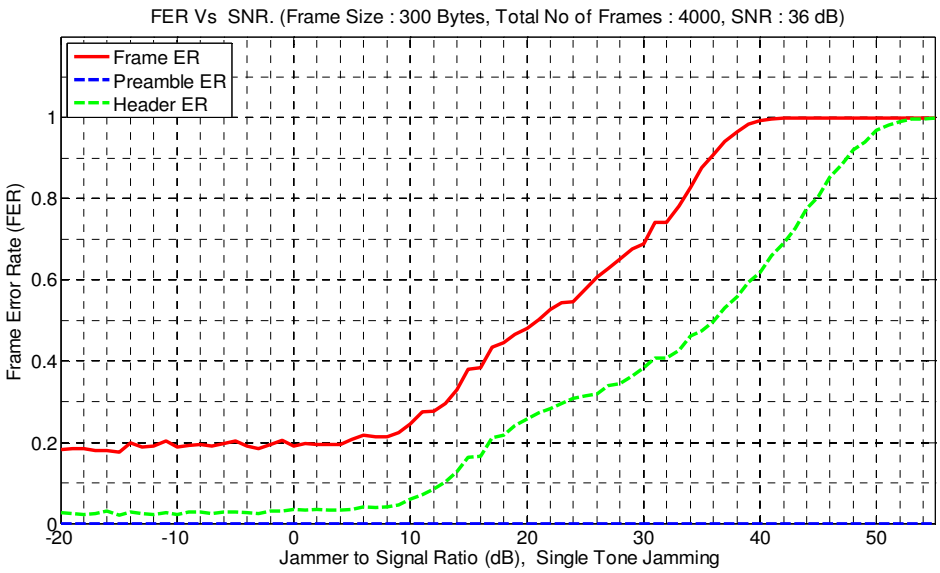


Figure 5- 25: FER vs JSR for single tone jammer in vehicular channel (Frame size= 300 bytes)

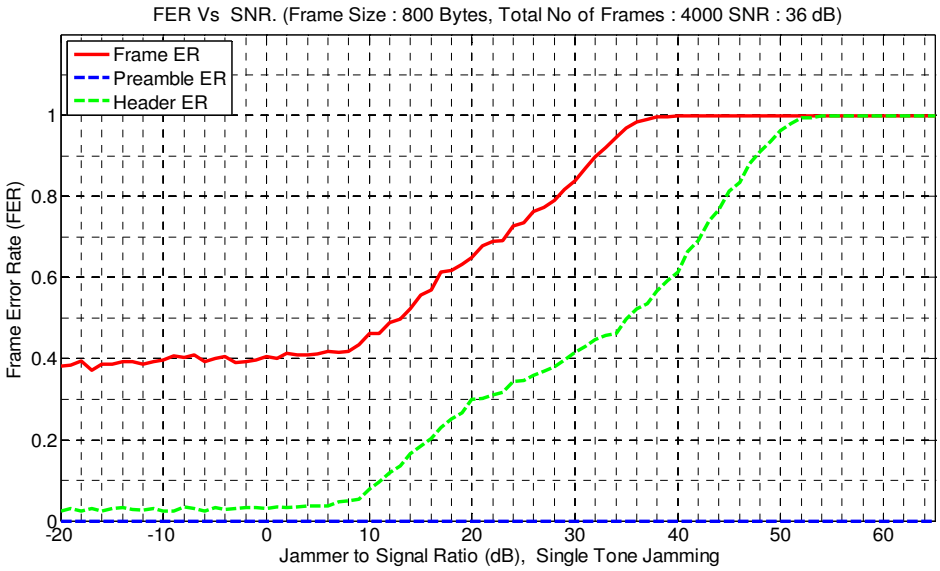


Figure 5- 26: FER vs JSR for single tone jammer in vehicular channel (Frame size= 800 bytes)

5.6.3 Follower Jammer

The performance of follower jammer is shown in Figure 5-27. The FER is reaches its maximum value at a JSR of -1.5 dB. The preamble and header error rate remain approximately 0, as expected. This is attributed to the fact that the preamble and header in jammer signal are exactly the same as the original signal. This enhances the receiver's ability to detect the preamble and decode the header.

The behavior remains the same for the frame size of 800 bytes but by increasing the frame size the FER reaches 1 at JSR of -4 dB (See Figure 5-28).

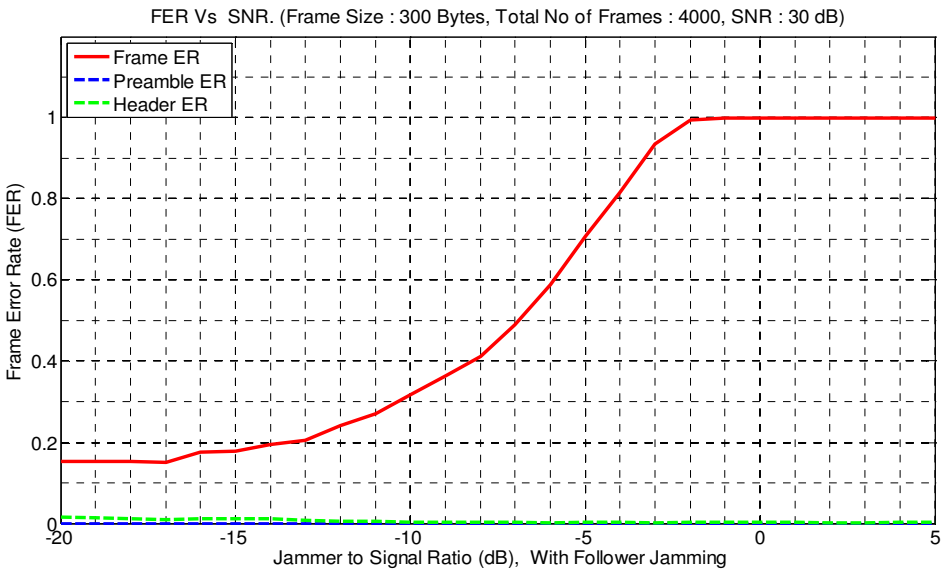


Figure 5- 27: FER vs JSR for follower jammer in vehicular channel (Frame Size= 300 bytes)

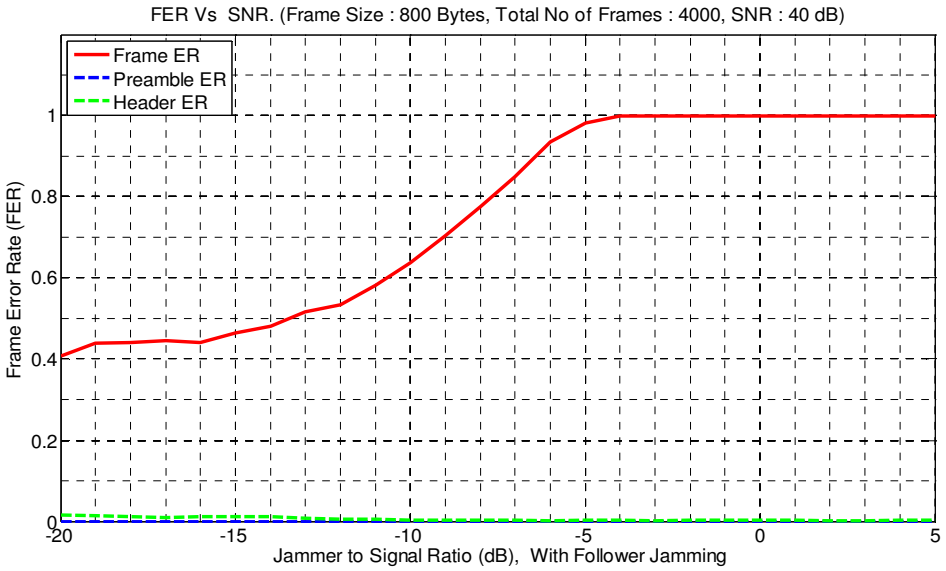


Figure 5- 28: FER vs JSR for follower jammer in vehicular channel (Frame Size= 800 bytes)

5.7. Summary

Table 5-1 summarizes the results for different jamming techniques in AWGN channel. The jammers are arranged in descending order depending upon their effectiveness in jamming IEEE 802.11p system. The results for the frame sizes of 300 and 800 bytes are approximately the same for the AWGN channel. The difference in JSR value for achieving FER of 1 for the frame sizes of 300 and 800 bytes is approximately 1 dB.

Table 5- 1: AWGN Channel; Comparison of different jammers on basis of attaining FER of 1

Sr. #	Jammer Type	JSR for FER of 100% (dB)	
		Frame Size 300 Bytes	Frame Size 800 Bytes
1.	Pilot Tone Jammer	-8	-9
2.	Partial Band Noise Jammer (PBNJ)	-8	-9
3.	Broadband Jammer (BBNJ)	-6	-7
4.	Follower Jammer	-2	-3
5.	Multi-tone Jammer	11	10
6.	Single Tone Jammer	100	100

For the vehicular channel scenario, the jammers are categorized in Table 5-2 based on their effectiveness. If the results are compared for the frames sizes of 300 and 800 bytes, for every type of jamming signals, it is observed that the behavior of the jammers remains the same. As mentioned earlier, an increase in the frame size increases the irreducible error floor so for the case of larger frame size 100 % FER is achieved at a lesser JSR. This can be observed in Table 5-2, where this value differs by approximately 2–2.5 dB for different frame sizes.

The preamble and header error rate curves are approximately identical for both frame sizes. This is because the PREAMBLE and SIGNAL fields are of the same size for both frame sizes.

Table 5- 2: Vehicular Channel; comparison of different Jammers on basis of attaining FER of 1

Sr. #	Jammer Type	JSR for FER of 100% (dB)	
		Frame Size 300 Bytes	Frame Size 800 Bytes
1.	Partial Band Noise Jammer (PBNJ)	-7	-10
2.	Broadband Jammer (BBNJ)	-5	-7.5
3.	Pilot Tone Jammer	-3	-5
4.	Follower Jammer	-1.5	-4
5.	Multi-tone Jammer	16	14
6.	Single Tone Jammer	42.5	40

Chapter 06: Conclusions and Future Work

This chapter contains the conclusions drawn from the simulation results and proposes some future endeavors that can be taken up as a next step to further this study

6.1. Conclusions

For the AWGN channel, pilot tone jammer and PBNJ and are the most effective jamming techniques. As mentioned earlier this performance categorization is attributed to the different factors in different cases. The pilot tone jammer outperforms PBNJ, even with small number of jamming tones, because of the placement of the jamming tones, which disables the receiver's capability to estimate and interpolate the channel conditions properly. While the other factors that affect the performance of jammers are the placement of jamming power and shape of the jamming waveforms.

For the vehicular scenarios, PBNJ is the best jamming technique followed by the BBNJ. Note that for vehicular channels the pilot tone jammer is not the outperformer. This is because, in the vehicular channel scenario, the pilot jammer undergoes the fading effects. This causes its characteristics to change causing its power to decrease at the locations of the pilot tones, thus jamming signal suffers a change in its effectiveness in hindering/ jamming the target signal.

For AWGN channels, the comparison of results shows that for the larger frame size, 100 % FER is achieved at a smaller JSR value. But this difference is not very evident in AWGN channel owing to the simplicity of the channel. In case of vehicular channel scenario, this difference is easily observed. For the case of larger frame size the FER attains it maximum values at a JSR that is approximately 2-2.5 dB lesser than its corresponding value for smaller frame size.

Summarizing we can conclude that IEEE 802.11p is vulnerable to the different kind of jamming signals. The degree of vulnerability is strongly dependent upon the type of jammer waveform used for the purpose. But, overall, PBNJ is most effective in hindering the IEEE 802.11p communications. The other jamming signals are less effective for the specific reasons and these reasons are already discussed in the respective sections.

6.2. Future Work

All the goals that were set at the planning stage of the thesis were achieved; nonetheless as work progressed, we noted potential further work opportunities to be taken up in the future. The following paragraphs give a brief idea about most important of these.

In order to meet the time line and thesis scope, we concentrated on designing a low pass filter in order to filter the AWGN to generate the colored noise (PBNJ). In practice, however, the jamming effects can be enhanced by determining the amount and location of bandwidth of the PBNJ signal. This can be divided into two parts; firstly determination of filter bandwidth to achieve the optimal jamming and secondly the type of filter to determine the location of jamming bandwidth by using the high pass or the band pass filter instead of low pass filter. More details on this can be found in [17].

The performance of multi-tone jamming can be optimized by determining the number of jammer tones to be generated along with the determination of their locations. This is important because the performance of the jammer depends upon the fraction of the bandwidth jammed and its location [17].

Bibliography

[1]. *Six Time and Frequency Selective Empirical Channel Models for Vehicular Wireless LANs.* **Guillermo Acosta-Marum, Mary Ann Ingram.** 4, s.l. : IEEE Vehicular Technology Magazine, December 2007, IEEE Vehicular Technology Magazine, Vol. 2, pp. 4-11.

[2]. **Böhm, A. and M. Jonsson,.** *Handover in IEEE 802.11p-based delay-sensitive vehicle-to-infrastructure communication.* School of Information Science, Computer and Electrical Engineering , Halmstad University. Halmstad, Sweden : s.n., 2007. Research Report. IDE-0924.

[3]. *Enhancing IEEE 802.11p/WAVE to provide infotainment applications in VANETs.* **Marica Amadeo, Claudia Campolo, Antonella Molinaro.** s.l. : ELSEVIER, 2010, Science Direct. Article in press.

[4]. **IEEE.** IEEE Standard for Information Technology - telecommunications and information exchange between systems- Local and metropolitan area networks- specific requirements; Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specification. New York (NY), USA : IEEE, June 12, 2007. IEEE 802.11p-2007.

[5]. *IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments.* **Daniel Jiang, Luca Delgrossi.** Singapore : IEEE, 2008. Vehicular Technology Conference, 2008. VTC spring 2008. pp. 2036-2040. ISSN 1550-2252.

[6]. **Sheila Frankel, Bernard Eydt, Les Owens, Karen Scarfone.** Establishing Wireless Robust Security Networks: A Guide to 802.11i. Gaithersburg, MD, USA : National Institute of Standards and Technology (Technology Admisnitration, US Department of Commerce), July 2008. NIST Special Publication 800-48, Revision 1.

[7]. *Wikipedia.* [Online] Wikimedia Foundation. [Cited: 11 02, 2010.] http://en.wikipedia.org/wiki/Radio_jamming#cite_note-1.

[8]. **Erik Ström, Tony Ottosson, Arne Svensson.** *An Introduction to Spread Spectrum Systems.* Department of Signals and Systems, Chalmers University of Technology. Göteborg : Chalmers University of Technology, 2002. URL to full text: https://regtransfers-sth-se.diino.com/download/arnechalmers/cpl/reports/s2_16_2002.pdf. ISSN 1403-266x; no R016/2002.

[9]. **Ståhlberg, Mika.** *Radio Jamming Attacks Against Two Popular Mobile Networks.* Department of Computer Science , Helsinki University of Technology. Helsinki : Helsinki University of Technology, 2000. Seminar Report. Seminar on Network Security, Fall 2000.

[10]. **Poisel, Richard. A.** *Modern Communications Jamming Principles and Techniques.* 2003. s.l. : Artech House Inc., 2003. ISBN-10: 1-58053-743-x, ISBN-13: 978-1580537438.

[11]. *Narrow-band Interference Rejection in OFDM-CDMA Transmission System.* **Hsu-Feng Hsiao, Meng-Han Hsieh, Che-Ho Wei.** Monterey, CA , USA : IEEE, 1998. IEEE International Symposium on Circuits And Systems (ISCAS). Vol. 04, pp. 437-440. Print ISBN: 0-7803-4455-3.

[12]. *Narrow- band Interference Rejection in Orthogonal Multi-carrier Spread Spectrum Communications.* **Fazel, K.** San Diego, CA , USA : IEEE, 1994. Third Annual International Conference on Universal Personal Communications. pp. 46-50. Print ISBN: 0-7803-1823-4 .

[13]. **Marvin K. Simon, Jim K. Omura, Robert A. Scholtz, Berry K. Levitt.** *Spread Spectrum Communications Handbook.* Electronic Edition : McGraw-Hill Inc., 2004. P/N 138225-8 Part of ISBN: 0-07-138215-1.

[14]. Sourceforge. *Sourceforge.* [Online] Geeknet, Inc. [Cited: November 02, 2010.] http://sourceforge.net/projects/physlayersim/.

[15]. Chalmers Center for Computational Science and Engineering. *C3SE.* [Online] Chalmers. [Cited: November 02, 2010.] http://www.c3se.chalmers.se/index.php/Ada_/_Kal.

[16]. *Design and evaluation of energy detection algorithms for IEEE 802.11a systems.* **Liu, Chia-Horng.** 2003. Radio and Wireless Conference, 2003. RAWCON '03. pp. 63 - 66 . Print ISBN: 0-7803-7829-6.

[17]. *Bit Error Rate Analysis of Jamming for OFDM systems.* **Luo, Jun, Andrian, J.H and Zhou, Chi.** Pomona, CA : s.n., 2007. Wireless Telecommunication Symposium, 2007, WTS 2007. pp. 1 - 8. Print ISBN: 978-1-4244-0696-8.

Appendices

Appendix A: Installation of Eclipse and IT++ on the Virtual Box

Uninstalling Previous Versions of Eclipse

If you already have eclipse installed on your system, you need to uninstall it first. To uninstall go to

→ Applications → Ubuntu Software Center → Installed software

Uninstall after locating eclipse in the list. Then open the terminal and execute

>> rm -r $HOME/.eclipse (if "/"doesn't work try "\")

The execution of the above mentioned command will remove the eclipse files completely from the machine. Also delete the workspace after taking backup of your previous work

Eclipse- Fresh Installation

Go to "Get Free Software" tab in the same window and select "Programming" and search for "Eclipse". Install it and close the window.

"JDE and "PDE" Installation

Open the terminal and execute

>> sudo apt-get install eclipse-jdt eclipse-plugin-cvs eclipse-pde

Now if you open Eclipse you should see options for the development of different java projects on the front page.

"CDK" Installation

Open Eclipse and go to "Help" tab and select "Install New Software". Add the following link http://download.eclipse.org/tools/cdt/releases/galileo and select the main C/C++ feature and don't select the optional features and complete the installation and then close Eclipse.

"BLAS, LAPACK & fftw3" Installation

The IT++ library needs some supporting libraries for its proper functionality. The following steps explain the installation of these libraries

Open the terminal and execute the following two commands and let the installation complete
>> sudo apt-get install libblas-dev liblapack-dev
>> sudo apt-get install libfftw3-dev

“ITPP” Installation

Now execute

>> sudo apt-get install libitpp-dev libitpp-doc
And let the installation complete. After completion of installation, also execute

>> sudo apt-get install libg++2.8-dev

Appendix B: Useful Commands for Virtual Box

Shared Directory

How to make a shared directory between windows host machine and Linux Guest machine

- Create a folder in the windows host machine that will serve the purpose of sharing the files and folders with the Linux guest machine. For example create a folder named “transient” in any drive of host windows machine.

- In Linux guest machine Go to the home directory using command

  >> cd home

- Create the folder in Linux guest machine. This folder has to be shared with the windows host machine. Use the following command in Linux terminal to create the folder

  >>mkdir name of the folder

  For example to create a folder named “transport” use
  >> mkdir transport

- Use the following command in Linux terminal to mount the shared folder

  >>sudo mount.vboxsf -o uid=UID,gid=GID [Name of the shared Folder in windows] [Name of the destination shared folder in Linux]

  With the folders created with names above the command can be used as

  >>sudo mount.vboxsf -o uid=UID,gid=GID transient transport

  Here
  User ID (UID) = 0
  Group ID (GID) = 0

  These is the default values that have all the rights and permissions, otherwise got to

  →System →Administration →Usergroups in the Linux and check the User ID for root

  OR type the following command in Linux terminal to get UID and GID
  >> id root

- The command executed in the last step has to be executed whenever the guest machine is turned on. There is a way to make this permanent, but can’t find the way to do that.