EXPLOITING OFDM FOR COVERT COMMUNICATION

by

Zaid Hayyeh

Submitted to the graduate degree program in Electrical Engineering
and the Graduate Faculty of the University of Kansas
in partial fulfillment of the requirements for the degree of
Master of Science.

Thesis Committee

____
Chairperson: Dr. Victor S. Frost

____
Dr. David Petr

____
Dr. Erik Perrins

Date Defended: __________________

The Thesis Committee for Zaid Hayyeh certifies
that this is the approved Version of the following thesis:

EXPLOITING OFDM FOR COVERT COMMUNICATION

Committee:

____
Chairperson*

____

____

____

____

Date approved:________________________

To my family for helping raise me up

To Dr. Frost for taking me under his wing

Acknowledgments

I would first and foremost like to thank God. “We have no knowledge except what he has taught us”.

The person I am most grateful to is Dr. Frost. His guidance and supervision were as good as it gets. I have always felt that it was a huge blessing to have him as my adviser and that it was an honor to work with him. Dr. Frost is one of the easiest and kindest people I have ever worked with. His expertise and knowledge are invaluable.

I would also like to thank Dr. Perrins for his help and advice with the simulation. Being able to consult and seek his advice was of great value.

Thanks are also in order for Dr. Petr, for serving on my committee, and Dr. Blunt for his help as well. The ITTC staff was very helpful and gracious. I would also like to thank them.

In closing, I am very grateful to my family for their love, support, and patience in my absence.

Abstract

Both LTE and WiMAX (802.16) 4th generation wireless systems (4G) utilize orthogonal frequency division multiplexing (OFDM). These technologies will become more wide spread as time goes on. Therefore, it would be beneficial to study covert communication in the presence of OFDM systems. OFDM is becoming more utilized due to a number of advantages it has over other techniques in wireless communication. OFDM can help to mitigate inter symbol-interference (ISI) resulting from multipath propagation. The lower rate of the sub-carriers is what makes this possible. OFDM takes several narrow-band lower-rate signals, and using the discrete Fourier transform, combines them into one high rate wide-band signal. The orthogonality of the OFDM signal eliminates co-channel interference. OFDM combined with adaptive modulation can be very effective in frequency selective environments. Most OFDM standards call for unused sub-channels for channel spacing and synchronization of transmitter and receiver. The effects we will be discussing in this thesis pertain to inserting a narrow band signal, that will be used for covert communication, in one of the unused sub-carrier locations of the OFDM signal and analyzing its effects on the OFDM signal. Although this signal is in an unused "slot", it is no longer orthogonal. We will also examine the effect of the OFDM signal on the covert signal. It would also be beneficial to study the ability to recover the information in the covert carrier in the midst of an OFDM signal. It will be important to view the effects of the covert signal on the OFDM signal by varying both its power and bandwidth and noting the results of the bit-error rate of the OFDM signal. This will allow us to deduce the amount of information we can transmit with a relatively low probability of detection (LPD) and the losses incurred by the OFDM user.

TABLE OF CONTENTS

1. INTRODUCTION..1

1.1 RESEARCH GOALS..4

1.2 CONTRIBUTIONS..7

1.3 THESIS ORGANIZATION...7

2. INTRODUCTION TO OFDM...9

2.1 OFDM FEATURES..9

2.2 OFDM SPECIFICATIONS..12

2.3 IMPLEMENTATION OF OFDM SYSTEM...14

2.4 BIT AND POWER ALLOCATION ALGORITHM...............................17

3. LTE WAVEFORM..21

3.1 LTE BACKGROUND..21

3.2 TIME & FREQUENCY DOMAIN STRUCTURE................................24

3.3 WAVEFORM SPECIFICATIONS..26

4. WiMAX WAVEFORM..28

4.1 WiMAX BACKGROUND...28

4.2FREQUENCY DOMANAN STRUCTURE...31

4.3WiMAX SIGNAL..33

4.4SUMMARY..34

5. COVERT EFFECT ON NON-COVERT OFDM COMM....................36

5.1PREMISE OF THE COVERT COMMUNICATION.............................36

5.2 SYSTEM PARAMETERS..37

5.3 SIMULATION INPUTS AND OUTPUTS...45

5.4 COVERT EFFECT ON NON-COVERT IN THE PRESENCE OF INCREASING NOISE...46

5.5 EFFECT OF INCREAING COVERT POWER ON NON-COVERT OFDM SIGNAL...49

5.6 EFFECT OF SYNCHRONOUS OFFSET ON NON-COVERT SIGNAL...55

6. LIMITATIONS OF COVERT SIGNAL..57

6.1EFFECT OF SPECTRAL POSITION ON COVERT SIGNAL..............57

6.2 EFFECT OF SYNCHRONOUS OFFFSET ON COVERT....................62

7. CONCLUSION...67

8. FUTURE WORK..70

TABLE OF FIGURES

FIGURE 1.1: TYPICAL BER CURVE OF SIMULATED OFDM SYSTEM..................4

FIGURE 1.2: BIT ALLOCATION FOR 5 MHZ OFDM SYMBOL................................6

FIGURE 2.1: NON-IDEAL CHANNEL MAGNITUDE & PHASE RESPONSE...........9

FIGURE 2.2: DIVISION OF BANDWIDTH..11

FIGURE 2.3: MULTI-CARRIER COMMUNICATION SYSTEM...............................16

FIGURE 2.4: OPTIMUM POWER DISTRIBUTION BASED ON WATER FILLING.17

FIGURE 2.5: BIT AND POWER ALLOCATION, N = 256, P_{TOTAL} = 1.........................20

FIGURE 3.1: LTE TIME-DOMAIN STRUCTURE...24

FIGURE 3.2: THE LTE DOWN-LINK PHYSICAL RESOURCE................................25

FIGURE 3.3: LTE DOWN-LINK FREQUENCY DOMAIN STRUCTURE................25

FIGURE 3.4: CYCLIC PREFIX INSERTION...26

FIGURE 4.1: EVOLUTION OF WIRELESS STANDARDS..30

FIGURE 4.2: WIMAX OFDM SUB-CARRIER SPACING FOR 20 MHZ...................34

FIGURE 5.1: TRANSMITTER/RECEIVER PAIRS & CHANNELS...........................40

FIGURE 5.2: NON-COVERT CHANNEL MAGNITUDE AND PHASE....................41

FIGURE 5.3: COVERT CHANNEL MAGNITUDE AND PHASE..............................41

FIGURE 5.4: NON-COVERT TO COVERT CHANNEL MAGNITUDE AND PHASE..42

FIGURE 5.5: COVERT TO NON-COVERT CHANNEL MAGNITUDE AND PHASE

…...42

FIGURE 5.6: COMPARISON OF BER CURVE WITH AND WITHOUT COVERT....49

FIGURE 5.7: PSD AT COVERT RECEIVER FOR INCREASED COVERT SIGNAL POWER...51

FIGURE 5.8: BASE-BAND SPECTRUM AT NON-COVERT RECEIVER..................52

FIGURE 5.9: *E_b/N_o* COVERT VS. BER NON-COVERT...54

FIGURE 5.10: SYNCHRONOUS OFFSET (Ʈ) VS. NON-COVERT BER...................56

FIGURE 5.11: SYNCHRONOUS OFFSET (Ʈ) VS. NON-COVERT BER...................56

FIGURE 6.1: COVERT SUB-CARRIER INDEX VS. COVERT BER..........................59

FIGURE 6.2: PSD AT NON-COVERT RECEIVER...60

FIGURE 6.3: COVER BER VS. SYNCHRONOUS OFFSET FOR SUB-CARRIER 103 …...64

FIGURE 6.4: COVER BER VS. SYNCHRONOUS OFFSET FOR SUB-CARRIER 146 …...65

FIGURE 6.5: PSD AT NON-COVERT RECEIVER FOR SUB-CARRIER 146...........66

LIST OF TABLES

TABLE 3.1: COMPARISON OF WIRELESS TECHNOLOGIES................................23

TABLE 3.2: LTE PARAMETERS...27

TABLE 4.1: OFDMA DOWN-LINK CARRIER ALLOCATION – OPTIONAL FULL USAGE OF SUB-CARRIERS...32

TABLE 4.2: OFDMA DOWN-LINK CARRIER ALLOCATION – OPTIONAL PARTIAL USAGE OF SUB-CARRIERS...32

TABLE 4.3: OFDM PARAMETERS IN WIMAX...35

1. Introduction

As demand for wireless communication devices has grown substantially, so has the amount of information needed to be carried by service provider networks. Wireless carriers have also marketed smart phones as the device of choice [11]. These devices offer companies the opportunity for greater revenue by being able to charge for additional services such as email, internet access, and video. These types of devices put even more pressure on networks. The applications that run on them require more resources compared to traditional voice services.

The increased number of users in addition to more resource hungry and higher order modulation applications has forced communication system designers to increase the capacity of their networks. This can be achieved through use of increased spectrum or use of various modulation techniques such as quadrature phase shift keying (QPSK) or M-ary quadrature amplitude modulation (M-QAM), for coding methods such as Reid-Solomon (RS) or low density parity check codes (LDPC) also yield increased efficiencies. Limited spectrum has caused engineers to come up with other solutions to solve this problem. The “Shannon Limit” [10] [3] for channel capacity clearly demonstrates the amount of bits/second/channel theoretical capacity limit. OFDM, in combination with various modulation and coding schemes, allows channels to achieve very high data rates (100 Mbps soft-input soft-output - SISO) [12] that are near capacity.

All fourth generation wireless communication systems (4G) currently being proposed involve the use of OFDM. Every major wireless carrier in the United States [11], Europe, and Asia [13] will migrate to either WiMAX (802.16) or LTE systems for 4G [14]. In the future, these modulation standards will be in wide use across the globe's wireless networks in order to help cope with the demand.

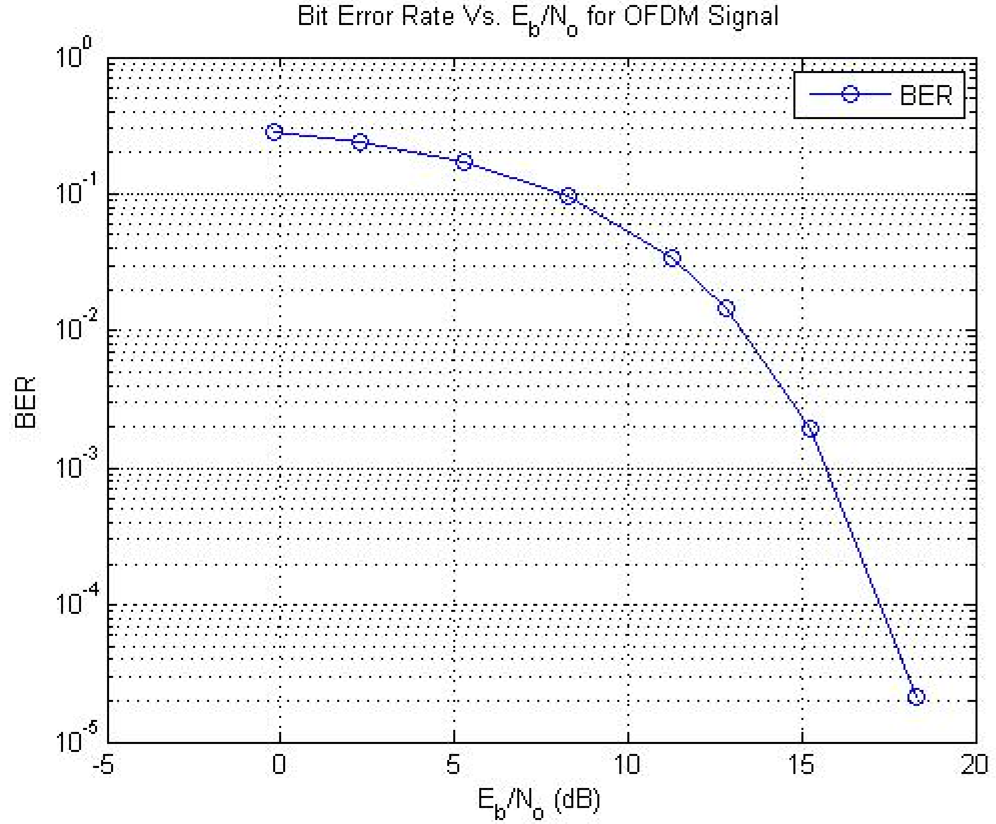
The purpose of covert communication is to hide, with a low probability of detection (LPD), the transmission of information; sometimes the covert signal can be embedded within an existing non-covert communication. A recent article in IEEE Spectrum [31] on stenography discusses several covert methods of transmitting information. These methods vary greatly from ancient examples of using a human scalp to embed a hidden message to modern times where covert information can be hidden in the flow of data packets transmitted over the internet. Also discussed in [31] are some of the reasons behind covert communication as well as a few historical examples of covert communication. Therefore, covert communications methods are of interest not only to those willing to exploit the characteristics of the system for covert communication, but also to those managing the systems and protecting them from vulnerabilities.

It is therefore beneficial to study the potential of covert communication embedded in OFDM signals. Clearly there will be wide spread deployment of OFDM systems and the degree to which people will depend on them will be significant. There has been either little or no research in the area of covert communications with regard to OFDM. Through this study we will be able to deduce how OFDM systems will respond to this type of exploitation.

1.1 Research Goals

This research seeks to show the potential effects of a covert communication signal embedded within an OFDM based wireless communication waveform (non-covert signal). The performance of the non-covert communications system is commonly characterized by the bit error rate (BER) versus a signal-to-noise ratio (SNR) or bit energy to noise ratio (E_b/N_o) as shown in Figure 1.1 for a typical OFDM system with the following parameters.

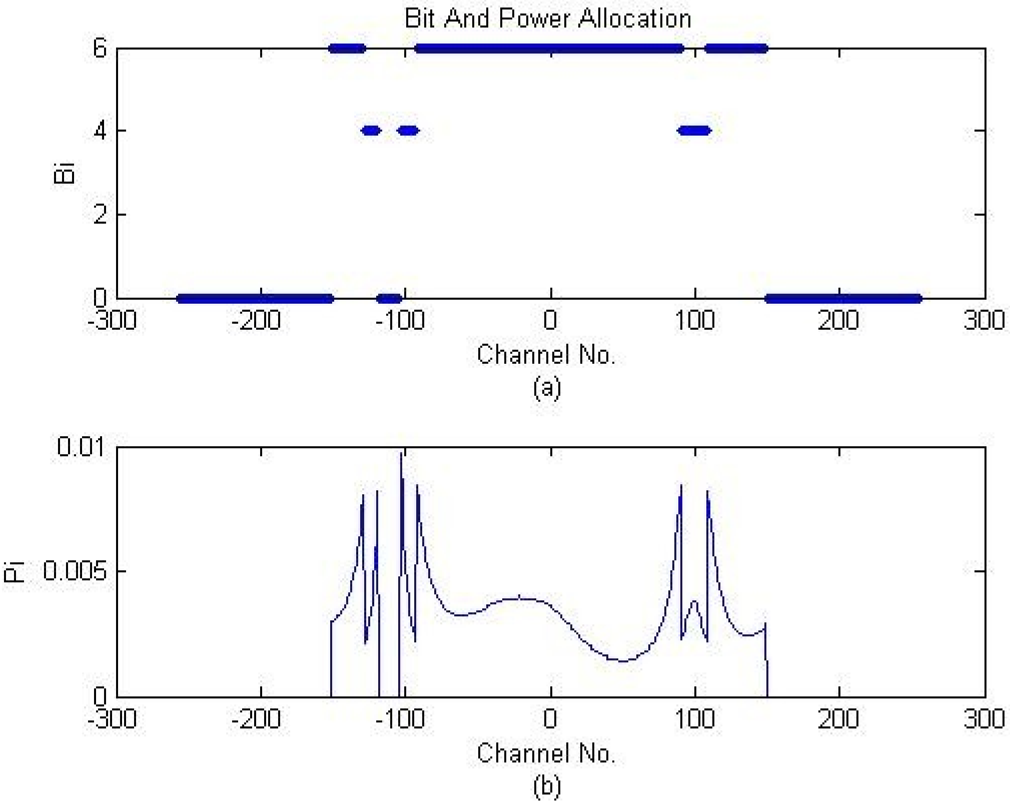
Figure 1.1: Typical BER Curve of Simulated 5 MHz OFDM System



A simulation model has been developed in Mat Lab to characterize the OFDM waveform in a noisy channel, for varying SNR or E_b/N_o in the presence of a covert signal. We will use this tool to evaluate the target (non-covert) OFDM system performance (BER) with and without the presence of the covert signal. This analysis will provide an estimate of the degradation in the BER of the target non-covert user as a function of the characteristics of the covert signal. The effect on the target user's error rate is crucial since most systems are designed to adapt to higher BER by lowering the data rate [1] [2], thus lowering the capacity of the channel and consuming more of the networks resources.

In this study the covert communications system will use BPSK modulation; evaluation of higher order and more complex modulation and coding is left for future work. The covert signal specifically seeks to use, as its bandwidth, some of the unused spectrum of the OFDM waveform. Both LTE and WiMAX have spectrum allocated for pilot tones for the purpose of timing and synchronization and/or guard bands to protect against spectral bleeding from adjacent signals in the spectrum and to prevent its signal from bleeding onto adjacent signals in the spectrum as well [1] [2]. There can also exist unused sub-carriers in between utilized sub-carriers due to poor channel response. For example, Figure 1.2a shows the guard bands of a 5 MHz 512 sub-carrier OFDM symbol along with some unused sub-carriers due to channel response in figure 1.2b.

Figure 1.2: Bit Allocation for 5 MHz OFDM Symbol



The performance of the covert communications system in the presence of the OFDM signal will also be determined. Providing BER performance of the covert communications system will establish the effectiveness and practicality of the proposed concept.

1.2 Contributions

This work makes the following contributions:

1 - Development of a simulation model for covert communication embedded in a OFDM waveform.

2 - Characterization of BER performance of LTE/WiMAX type OFDM signal in the presence of covert signal with varying power and bandwidth.

3 - Characterization of performance and limitations of covert communications systems in the presence of an OFDM signal.

1.3 Thesis Organization

In this thesis, we first cover the topic of OFDM and its implementation with an emphasis on the mathematical model and its benefits. We also discuss the bit and power allocation algorithm widely used in most OFDM schemes in the first section. In section two, we cover the LTE standard waveform in detail. Then, in section four, we cover the WiMAX standard waveform in detail. In these two sections we will also discuss some of there current and future applications in commercial wireless systems. In the next section we present the system performance of an LTE/WiMAX like OFDM waveform in the presence of a covert signal. These simulations will have as a reference for comparison, the same waveforms without the covert signal. The following section will focus on the performance of the covert signal. Then, in section seven, we present our results and our conclusions. In the final section, suggestions are made for future work connected to this subject.

2. Introduction to OFDM

2.1 OFDM Features

Typical single carrier wide-band modulation suffers from a number of phenomena that cause distortion of the signal and hence, the data at the receiver becomes very complex to recover. As opposed to the ideal channel, a typical single carrier wide-band modulation can suffer from attenuation, interference, and fading due to multi-path propagation. Multi-path propagation and the non-ideal response of channels can result in inter-symbol-interference (ISI).

Figure 2.1: Non-Ideal Channel Magnitude & Phase Response

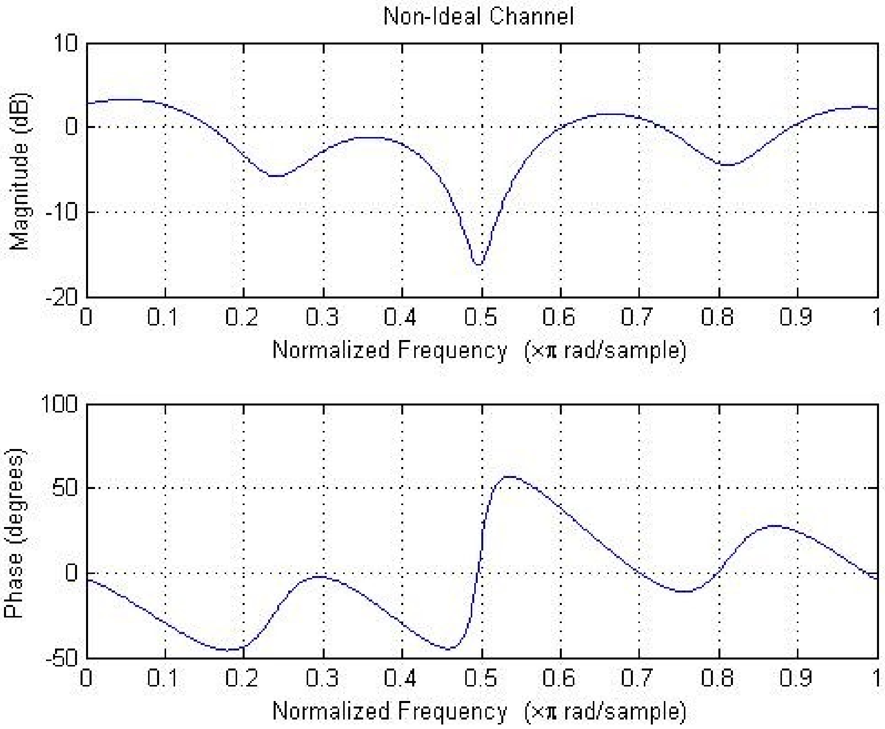


Figure 2.1 shows the magnitude and phase response of a random non-ideal channel potentially causing a signal to have ISI. It can be seen clearly how the attenuation and phase response varies throughout the spectrum of this channel. Equalization can become difficult to implement for a single carrier signal propagated through such a channel suffering from ISI such as this.

As an alternative to single carrier modulation, multi-carrier modulation can help to minimize the negative effects of multi-path and result in a more bandwidth-efficient scheme. In multi-carrier modulation, the bandwidth of a wide-band single carrier is divided equally among several narrow band sub-carriers [3]. Equation 2.1 shows the relationship between the bandwidth of the sub-carrier (Δf-Hz), the total bandwidth of the OFDM symbol (W-Hz), and the number of sub-carriers (N).

$$\Delta f = \frac{W}{N} \quad (2.1)$$

The dividing of bandwidth into equal sub-channels results in a response that is nearly ideal across each sub-channel. The OFDM symbol time ($T_{s,OFDM}$) must be larger than the channel's time dispersion in order for this assumption to hold. The response within each sub-band therefore can be treated as approximately constant if Δf is chosen to be small enough. The inter-symbol-interference then becomes negligible for each sub-carrier [3].

Figure 2.2: Division of Bandwidth from [3].

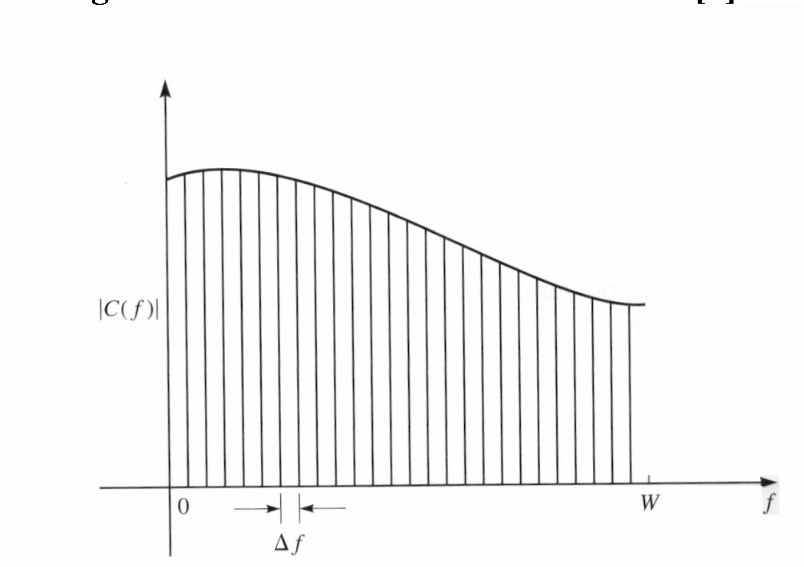


Figure 2.2 demonstrates the division of bandwidth amongst several sub-carriers versus the magnitude of the channel response. While the response is clearly non-ideal across the entire bandwidth, it can be visualized that response across each individual sub-carrier bandwidth is closer to ideal.

2.2 OFDM Specifications

Dividing allocated bandwidth (*W*) amongst a number (*N*) of equally spaced sub-carriers each having a bandwidth and center frequency spacing of Δ*f,* via the relationship in equation 2.1, and associating each sub-carrier with a sinusoidal carrier leads to the development of orthogonal frequency division multiplexing (OFDM). Equation 2.1 represents a single sub-carrier in the OFDM symbol.

$$s_k(t) = \cos(2\pi f_k t) \quad (2.2)$$

When adjacent carriers are located without sufficient spacing, spectral bleeding into adjacent carriers leads to the distortion of the signal. OFDM resolves this issue by insuring that the sub-carriers are orthogonal with respect to every other sub-carrier in the OFDM signal. This is achieved by having the carriers spaced by the reciprocal of the symbol period. When the signals are demodulated, they will have a whole number of cycles in the symbol period and their contribution will sum to zero [17]. This results in no interference contribution from the other carriers in the OFDM waveform. The orthogonal condition is represented in equation 2.3 and includes the received phase associated with each sub-carrier (ϕ_k).

$$\int_0^T \cos(2\pi f_k t+\phi_k)\cos(2\pi f_j t+\phi_j)=0 \quad (2.3)$$

$$k \neq j$$

The symbol rate ($1/T_s$) in an OFDM system is reduced by a factor of N as compared to a single carrier signal. *N* is the number of sub-carriers in the OFDM system. The symbol time for the OFDM symbol becomes $T_{s,OFDM}$ = N T_s, where T_s is the symbol time for a single carrier system.

As discussed in section 2.1, the channel response can be considered approximately a constant. The channel is modeled using *$C(f_k)$,* a complex-valued quantity, and is expressed in equation 2.4. The phase here is the same as in equation 2.3.

$$C(f_k) = C_k = |C_k| e^{j\phi_k} \quad (2.4)$$

We now consider modulating each sub-carrier with M-ary QAM. A_{kc} and A_{ks} represent the in-phase and quadrature parts of the QAM constellation point. This can be a 4, 8, 16, 32, or 64-QAM constellation. The effects of the sub-channel on the received signal are represented by the sub-channel magnitude response (C_k) and the sub-channel phase response (ϕ_k) which are the same as in equation 2.4. Therefore the received signal on the k_{th} sub-carrier may be expressed as

$$\begin{aligned} r_k(t) &= \sqrt{\frac{2}{T}}|C_k| A_{kc}\cos(2\pi f_k t+\phi_k) \\ &+ \sqrt{\frac{2}{T}}|C_k| A_{ks}\sin(2\pi f_k t+\phi_k) + n_k(t) \end{aligned} \quad (2.5)$$

This takes into account the channel response, the M-ary QAM modulation, and the noise. We assume $n_k(t)$ to be zero-mean Gaussian and spectrally flat across the k_{th} sub-channel [3].

2.3 Implementation of OFDM System

Key to the implementation of the OFDM symbol is the inverse discrete Fourier transform (IDFT). Each of the sub-carrier signals is sampled once per OFDM symbol sample time ($T_{s,OFDM}/N$) at the appropriate sampling instant. We refer to these complex valued points as X_k. These points are taken from the individual sub-carriers. The transmitted signal on the kth sub-carrier may be expressed as

$$\begin{aligned} u_k(t) &= \sqrt{\frac{2}{T}} A_{kc}\cos(2\pi f_k t) + \sqrt{\frac{2}{T}} A_{ks}\sin(2\pi f_k t) \\ &= \Re\left[\sqrt{\frac{2}{T}} X_k e^{j2\pi f_k t}\right] \end{aligned} \quad (2.5)$$

Then the *N* sub-carriers are modulated using a *N*-point IDFT which results in *N* discrete time samples. A mathematical representation of the *n*-th discrete time sample can be seen in equation 2.6. The relationship between the sub-carrier $u_k(t)$ and the discrete time sample x_n is seen in X_k.

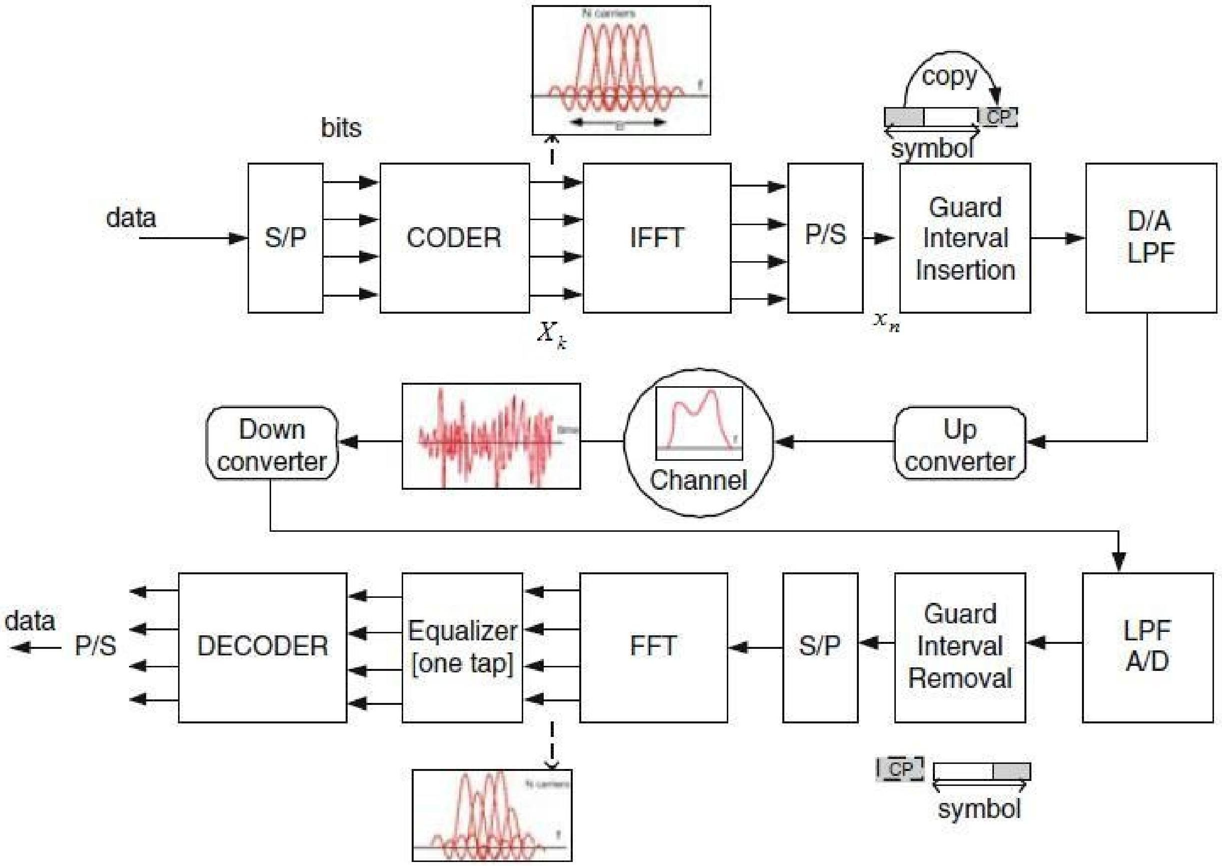
$$x_n = \frac{1}{\sqrt{(N)}} \sum_{k=0}^{N-1} X_k e^{j2\pi k n/N} \quad (2.6)$$

The IDFT can be efficiently calculated using the FFT algorithm. Figure 2.3 shows an example of this kind of multi-carrier communication system. The stream of input data enters a serial to parallel converter (S/P) which divides the data between amongst the sub-carriers. After encoding the sub-carrier data (X_k), the IFFT is applied to each sub-carrier. The parallel to serial (P/S) gives us the OFDM symbol samples (x_n). The sequence of x_n samples form the the sum *x(t)* of *N* sub-carrier signals. Before the samples are sent to the digital to analogue converter (D/A), the guard time (TG) or cyclic prefix (CP) is appended to the symbol samples. One of the methods used to combat ISI in an OFDM signal is to append a CP to the *N* samples. The number of samples, υ, that are appended are taken to be the last υ samples in the OFDM symbol $\{x_{N-\upsilon}, x_{N-\upsilon+1}, \ldots.., x_{N-1}\}$. This additional data increases the length of the block to *N* + υ. The length of υ depends on the number of samples related to the channel dispersion. For LTE/WiMAX type OFDM symbols, the υ is equal to 6 for normal CP and 7 for the extended CP.

On the receiver side, the channel effects are compensated for by the one tap equalizer. A one tap equalizer can be used because the sub-channel magnitude is nearly ideal due to the lower rate of the sub-carriers.

$$x(t)=\frac{1}{\sqrt{(N)}}\sum_{k=0}^{N-1} X_k e^{j2\pi kt/T} \quad (2.7)$$

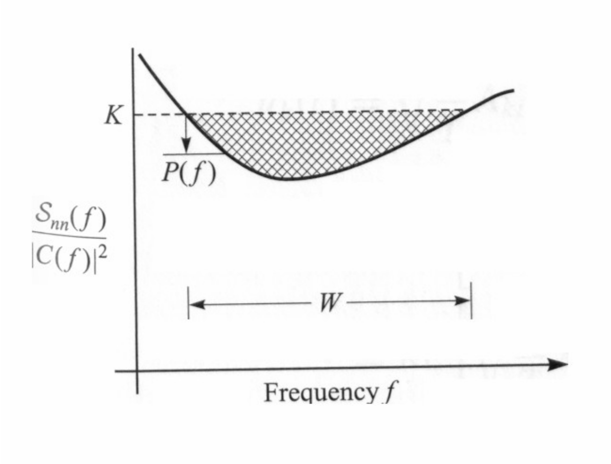
Figure 2.3: Multi-carrier Communication System from [19].



2.4 Bit and Power Allocation Algorithm

In order to more fully take advantage of the multi-carrier modulation scheme, the power and number of bits allocated to each sub-channel is varied. The algorithm that computes this allocation takes into account the signal-to-noise ratio of each individual sub-channel, the average available power of the transmitter, and the channel response (C_k). This approach will allow us to increase the channel capacity (bits/s/Hz).

Figure 2.4: Optimum power distribution based on water-filling from [3].



In Figure 2.4, we can see a visualization of the *water-filling interpretation* for Holsinger's work (1964). Channel noise-to-signal ratio ($S_{nn}(f)/|C(f)|^2$)is represented on the vertical axis with the frequency (*f*) on the horizontal axis. The simple interpretation of Holsinger's findings are that signal power should be high when signal to noise ratio are low. Here, *K* (signal power at the receiver for frequency *f*) represents the Lagrange multiplier used to satisfy the constraint and *P(f)* is the signal power at frequency *f*.

We begin to consider the algorithm used for allocating bits and power over a linear time-invariant channel with AWGN. Each of the *N* sub-carriers will be using QAM ($M_i = 2^{Bi}$). Where M_i is the constellation size and B_i is the number of bits transmitted on the *i*th sub-carrier in a frame interval of *T* seconds. The bit rate (R_b) of the OFDM symbol is expressed in equation 2.7. The power allocated to the *i*th sub-carrier with respect to the average available power at the transmitter is expressed in equation 2.8.

$$R_b = \frac{1}{T} \sum_{i=1}^{N} B_i \quad (2.7)$$

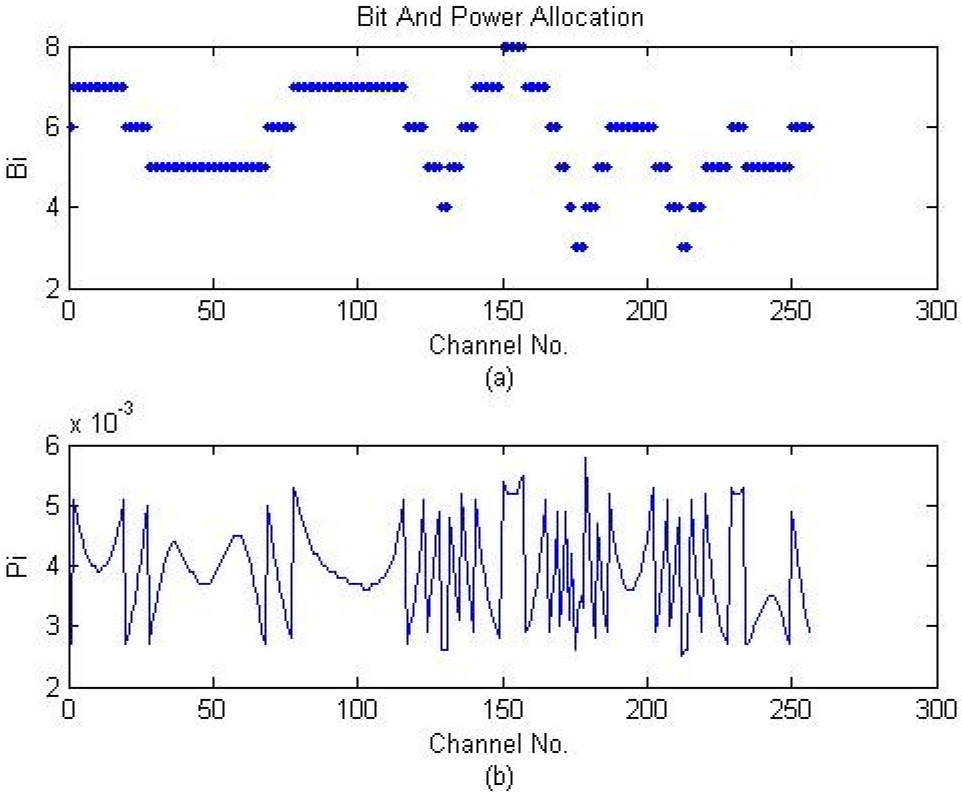
$$P_{total} = \sum_{i=1}^{N} P_i \quad (2.8)$$

The first step in allocating bits (B_i) and power (P_i) amongst the sub-carriers is to eliminate the channels which cannot support at least 4M-QAM here we consider $M_i = 4$, $B_i = 2$. We start by dividing the total available power (P) equally amongst all the sub-carriers. Those that result in probability of symbol error greater than our desired symbol error probability (typical $P_e = 10^{-3}$) will not be used for transmission. Equation 2.9 [3] approximates the symbol error probability for QAM.

$$P_e \approx 4Q\left(\sqrt{\frac{3P_i|C_i|^2}{N_o(M_i-1)}}\right) \quad (2.9)$$

We then allocate the total power amongst the remaining carriers and compute M_i for the highest SNR channel based upon our desired probability of symbol error. We then quantize M_i corresponding to an integer number of bits B_i. Next, we recalculate P_i based upon the quantized M_i and subtract the power (P_i) for the current channel from the total remaining unallocated power. Finally, we repeat this procedure for the rest of the channels beginning next with the channel having the highest remaining SNR until the allocation procedure is complete for all channels [3]. Figure 2.5a shows the bit allocated for each sub-carrier (B_i) for an OFDM symbol consisting of 256 sub-carriers based upon the algorithm described in this section. Figure 2.5b shows the amount of power allocated to each sub-carrier (P_i) in watts. Figure 1.2 shows a bit and power allocation for a channel where N = 512. There are channels that fail to meet the probability of error requirement that could potentially be exploited for covert communication.

Figure 2.5: Bit and Power Allocation, N = 256, $P_{total} = 1$.



Now that we have looked at OFDM in general, we will present two technologies that utilize OFDM specifically. Although they are very similar, LTE and WiMAX do have significant differences between them.

3. LTE Waveform

3.1 LTE Background

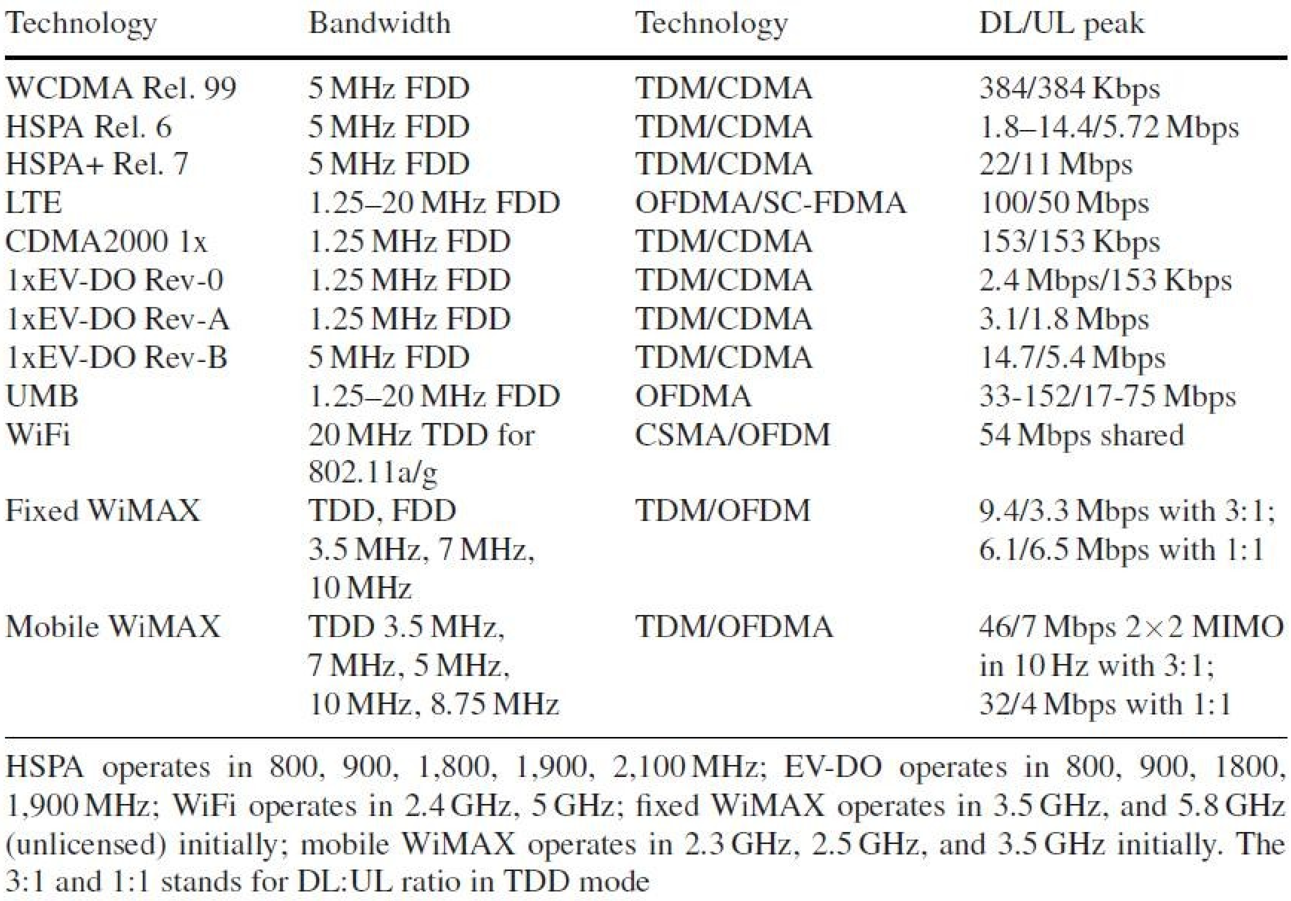
OFDM is used in Long Term Evolution (LTE) the standard for next generation cellular systems. The next generation of OFDM is key to the LTE standard which is an all IP based technology [20]. The LTE standard has been developed by the 3rd Generation Partnership Project (3GPP) in its eighth release [19]. This release focuses on 4th Generation (4G) mobile communication technology. The 3GPP is a group of telecommunication associations that have come together to develop a universal standard for the migration and advancement of communication standards throughout the world. These standards will also allow for the interoperability of receivers on multiple local networks as well as on other networks internationally. This also simplifies the manufacturing of the mobile devices as the manufacturers need to make fewer models to function on different networks. LTE will be the next step in advancement of wireless networks for many telecommunications operators worldwide. In the United States, for example, AT&T, Verizon, and T-Mobile have already chosen LTE as the next technology standard for their wireless 4G networks. Although LTE is marketed as 4G, it does not fully comply with International Mobile Telecommunications (IMT) Advanced 4G requirements.

The part of the LTE standard that concerns us is the waveform specifications. The specifications for the physical layer (PHY) will allow us to set the conditions for the system analysis described later in this report. These specifications will give the details of proposed OFDM waveforms used in LTE and help us to more closely reproduce the conditions in wireless communication under which it will be used. We will not concern ourselves with the other layers of LTE outside of the waveform specifications.

The use of OFDM in LTE enables links to reach very high data rates up to 100Mbps per 20MHz of spectrum from the base station to the mobile receiver, otherwise known as the down-link. This is a substantial increase in capacity over current 3G systems. Current High Speed Packet Access (HSPA) rates peak at 14Mbps. OFDM is only used on the down-link. Single carrier-frequency division multiple access (SC-FDMA) is used from the mobile end user to the base station known as the up-link. The deployment of LTE will help carriers to cope with the increased demand caused by the growing number of users and applications that go beyond traditional voice traffic that lead to bottlenecks, dropped calls, and a generally poor wireless experience for mobile users in some networks.

Table 3.1 allows us to compare LTE with some of the other wireless technologies. LTE has the largest down-link and up-link speeds of any other technology listed and is only specified for frequency division duplexing (FDD). There is no time division duplexing specified for LTE. It also has a variable bandwidth of 1.25 to 20 MHz. LTE uses OFDM on the down-link only.

Table 3.1: Comparison of Wireless Technologies from [19].



Technology	Bandwidth	Technology	DL/UL peak
WCDMA Rel. 99	5 MHz FDD	TDM/CDMA	384/384 Kbps
HSPA Rel. 6	5 MHz FDD	TDM/CDMA	1.8–14.4/5.72 Mbps
HSPA+ Rel. 7	5 MHz FDD	TDM/CDMA	22/11 Mbps
LTE	1.25–20 MHz FDD	OFDMA/SC-FDMA	100/50 Mbps
CDMA2000 1x	1.25 MHz FDD	TDM/CDMA	153/153 Kbps
1xEV-DO Rev-0	1.25 MHz FDD	TDM/CDMA	2.4 Mbps/153 Kbps
1xEV-DO Rev-A	1.25 MHz FDD	TDM/CDMA	3.1/1.8 Mbps
1xEV-DO Rev-B	5 MHz FDD	TDM/CDMA	14.7/5.4 Mbps
UMB	1.25–20 MHz FDD	OFDMA	33-152/17-75 Mbps
WiFi	20 MHz TDD for 802.11a/g	CSMA/OFDM	54 Mbps shared
Fixed WiMAX	TDD, FDD 3.5 MHz, 7 MHz, 10 MHz	TDM/OFDM	9.4/3.3 Mbps with 3:1; 6.1/6.5 Mbps with 1:1
Mobile WiMAX	TDD 3.5 MHz, 7 MHz, 5 MHz, 10 MHz, 8.75 MHz	TDM/OFDMA	46/7 Mbps 2×2 MIMO in 10 Hz with 3:1; 32/4 Mbps with 1:1

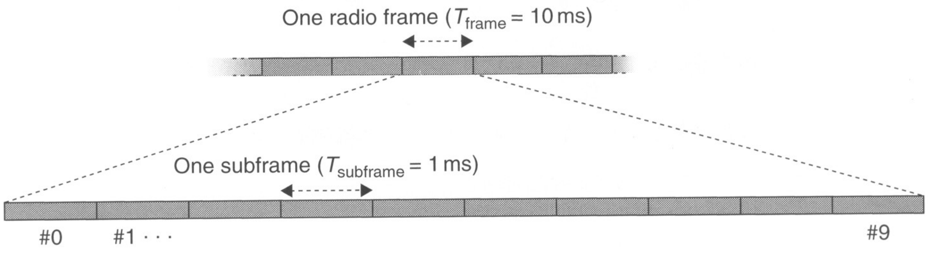
HSPA operates in 800, 900, 1,800, 1,900, 2,100 MHz; EV-DO operates in 800, 900, 1800, 1,900 MHz; WiFi operates in 2.4 GHz, 5 GHz; fixed WiMAX operates in 3.5 GHz, and 5.8 GHz (unlicensed) initially; mobile WiMAX operates in 2.3 GHz, 2.5 GHz, and 3.5 GHz initially. The 3:1 and 1:1 stands for DL:UL ratio in TDD mode

3.2 Time & Frequency Domain Structure

Understanding of the OFDM waveform in LTE requires presenting the specifications of both the time and frequency domain characteristics of the standard. As mentioned earlier, only the down-link employs OFDM. Each radio frame in LTE has a duration of T_{frame} = 10 ms. This frame contains ten equally sized sub-frames of duration

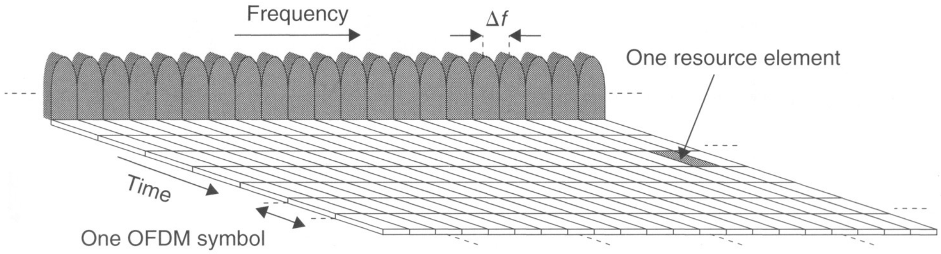
$T_{subframe}$ = 1 ms (Figure 3.1).

Figure 3.1: LTE Time-Domain Structure from [2].


One radio frame (T_{frame} = 10 ms)
One subframe (T_{subframe} = 1 ms)
#0
#1 · · ·
#9

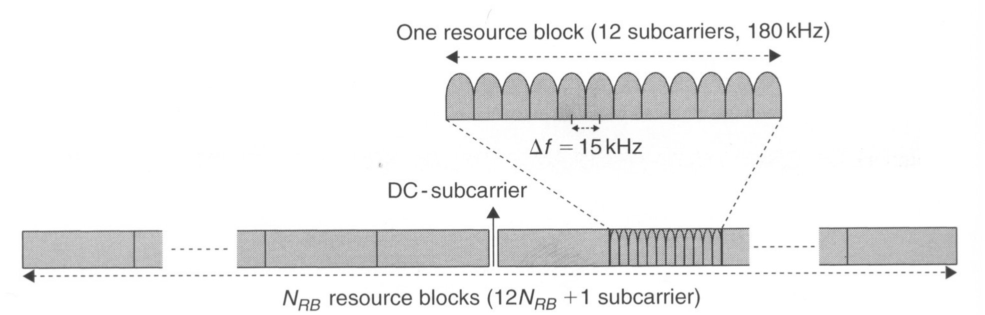
The sub-carrier spacing in LTE has been set at Δf = 15 kHz. An FFT based transmitter or receiver will have a sampling rate of f_s = 15000 * N_{FFT} , where N_{FFT} is the FFT size. The time frame and sub-carrier spacings allow us to view the down-link in a grid.

Figure 3.2: The LTE Down-link Physical Resource from [2].



The sub-carriers are then grouped into resource blocks which include a DC sub-carrier. The number of resource blocks depends upon the channel bandwidth. The LTE standard has several possible bandwidths choices which will be discussed in the next section.

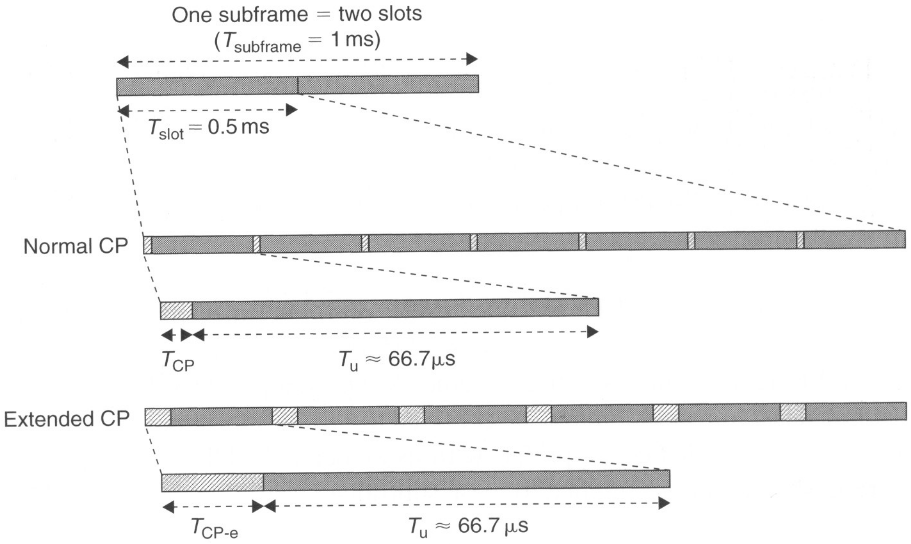
Figure 3.3: LTE Down-link Frequency Domain Structure from [2].


One resource block (12 subcarriers, 180 kHz)
$\Delta f = 15$ kHz
DC-subcarrier
N_{RB} resource blocks ($12N_{RB}+1$ subcarrier)

There are twelve sub-carriers in every resource block. Every resource block occupies 180 kHz (15KHz x 12) of spectrum. Each OFDM symbol includes the resource blocks and a centered DC sub-carrier.

Every sub-frame, in the time domain, consists of 7 OFDM symbols plus the cyclic prefix appended to each symbol. When the extended cyclic prefix (CP) is utilized, only six OFDM symbols per sub-frame plus their respective cyclic prefix are appended to every symbol. The extended CP is used for channels having a high channel dispersion at the cost of lowering the capacity of the channel. An example of the use of the two cyclic prefixes can be seen in Figure 3.4. Here the selected channel bandwidth is 30.72 MHz and the number of sub-carriers is 2048.

Figure 3.4: Cyclic Prefix Insertion from [3].

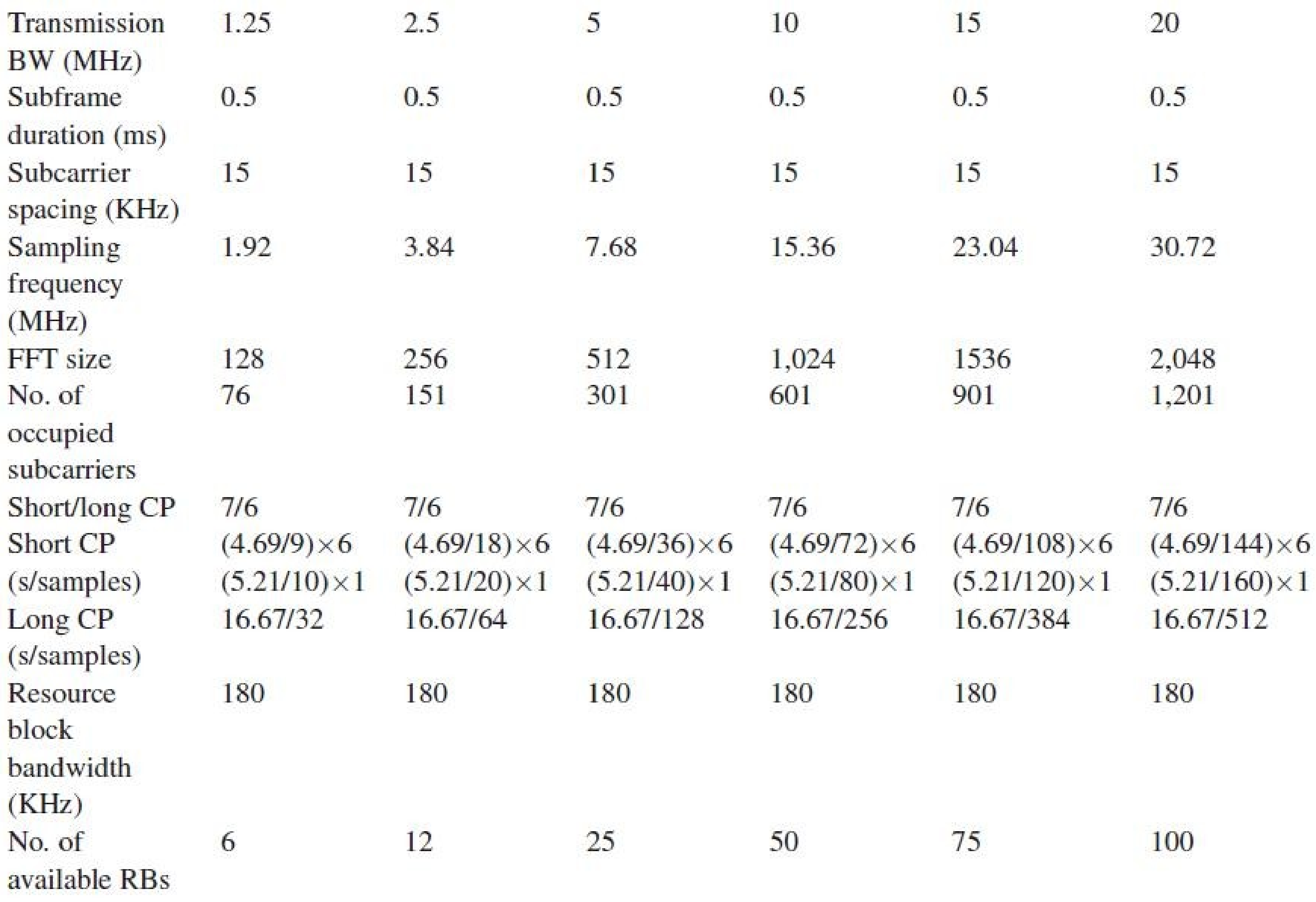


3.3 Waveform Specifications

The 3GPP has set the LTE standard and given system designers a number of options in meeting this standard. The system can have a single receiver and single transmitter design utilizing soft-input soft-output (SISO), dual receiver and dual transmitter (2X2

MIMO), or a quad array receiver and quad array transmitter (4X4 MIMO). By increasing the diversity, the capacity of the system is increased substantially. Table 3.2 lists the different bandwidth characteristics of LTE. As mentioned before, the waveform can be based upon channel bandwidths of 1.4, 3 5 10 15, or 20 MHz. The number of resource blocks and sub-carriers is directly related to the chosen bandwidth. Another important specification involves the supported modulation types of QPSK, 16-QAM, or 64-QAM which allow for 2, 4, or 6 bits per symbol respectively.

Table 3.2: LTE Parameters from [19].



Transmission BW (MHz)	1.25	2.5	5	10	15	20
Subframe duration (ms)	0.5	0.5	0.5	0.5	0.5	0.5
Subcarrier spacing (KHz)	15	15	15	15	15	15
Sampling frequency (MHz)	1.92	3.84	7.68	15.36	23.04	30.72
FFT size	128	256	512	1,024	1536	2,048
No. of occupied subcarriers	76	151	301	601	901	1,201
Short/long CP	7/6	7/6	7/6	7/6	7/6	7/6
Short CP (s/samples)	(4.69/9)×6 (5.21/10)×1	(4.69/18)×6 (5.21/20)×1	(4.69/36)×6 (5.21/40)×1	(4.69/72)×6 (5.21/80)×1	(4.69/108)×6 (5.21/120)×1	(4.69/144)×6 (5.21/160)×1
Long CP (s/samples)	16.67/32	16.67/64	16.67/128	16.67/256	16.67/384	16.67/512
Resource block bandwidth (KHz)	180	180	180	180	180	180
No. of available RBs	6	12	25	50	75	100

4. WiMAX Waveform

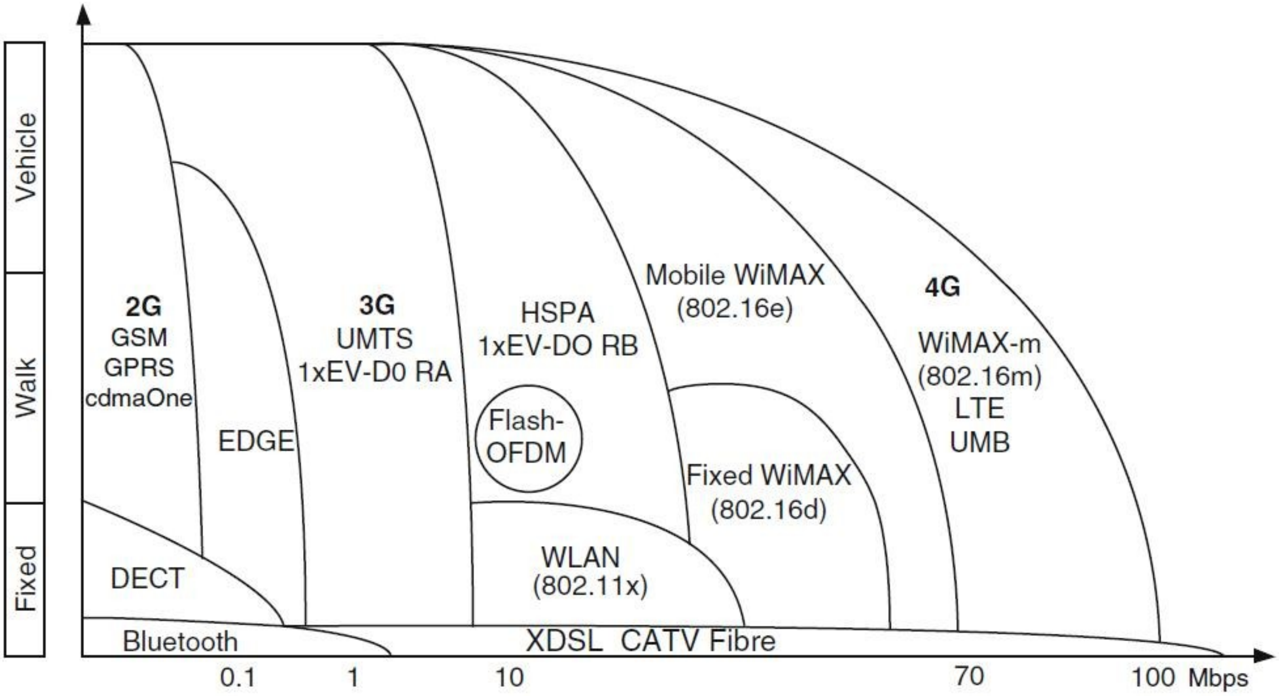
4.1 WiMAX Background

The WiMAX Forum is a non-profit industry based organization with the main goal to standardize WiMAX. Members include hundreds of communication operators, component vendors, and equipment vendors. WiMAX is the acronym for Worldwide Interoperability for Microwave Access. Among the forum's other goals are to promote the use and deployment of WiMAX and WiMAX certified products therefore insuring interoperability of wireless devices based upon this standard, developing a trusted certification process, and publishing the WiMAX standards. WiMAX certified products also meet government and industry standards [25]. This standard is an important step in the evolution of cellular standards. Figure 4.1 illustrates the growth of wireless technologies.

WiMax is envisioned to have many uses. It will connect Wi-Fi hotspots to the internet, provide an alternative to digital subscriber lines (DSL) or cable, provide portable connectivity to the internet, and can provide last mile connectivity. In the United States Sprint Nextel and Clearwire have already deployed WiMAX throughout several markets.

Korea's WiBro and Europe's Hyper Man were once considered competing technologies. They have now both been integrated into WiMAX and are no longer considered competitors [23]. The WiMAX air interface is based on 802.16 working group whose focus is on Broadband Wireless Access Standards. The WiMAX Forum Mobile System Specification is based upon the IEEE 802.16 – 2004, IEEE 802.16e – 2005, and IEEE 802.16 - 2009 standards. 802.16e-2005 (formerly known as 802.16e) specifies the MAC and PHY layers of the air interface. WiMAX Forum Mobile System Specification document covers all aspects and layers of WiMAX in detail while also allowing some flexibility [25]. It provides guidance for forum members in achieving the stated goals of the group. The part that concerns us in this research are those areas specifying the WiMAX waveform. Most of the material needed can be found in the PHY profile of the WiMAX Forum Mobile System Specification authored by the WiMAX Forum [25]. IEEE 802.16m will push data rates for mobile WiMAX up to 100 Mbps. It will meet International Mobile Telecommunications (IMT) – Advanced next generation (4G) requirements.

Figure 4.1: Evolution of Wireless Standards from [19].

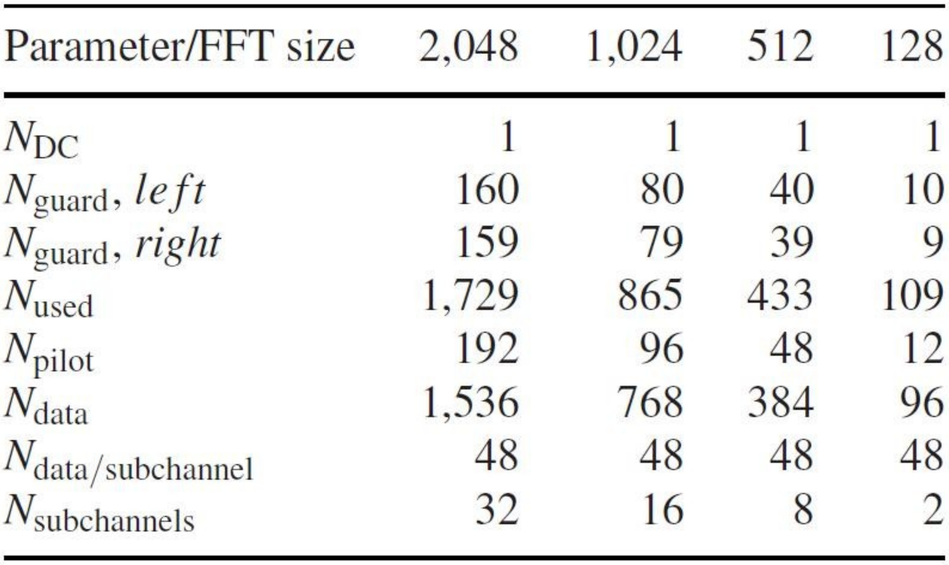


4.2 Frequency Domain Structure

WiMAX “Wave 3” is based upon IEEE standard 802.16m. “Wave 3” will have specifications for fixed and nomadic networks in it [32]. It supports use of orthogonal frequency division multiple access (OFDMA) on both the up and down-links with selectable channel bandwidths of 1.25 to 20 MHz and Fast Fourier Transform (FFT) implementation using 128, 256, 512, and up to 2048 N_{FFT}. Sub-carrier spacing is uniform for all Mobile WiMAX at Δf = 10.94 kHz. In order to achieve speeds close to that of LTE (100 Mbps), specifications for 4X4 MIMO smart antenna arrays have also been included in “Wave 3” [19].

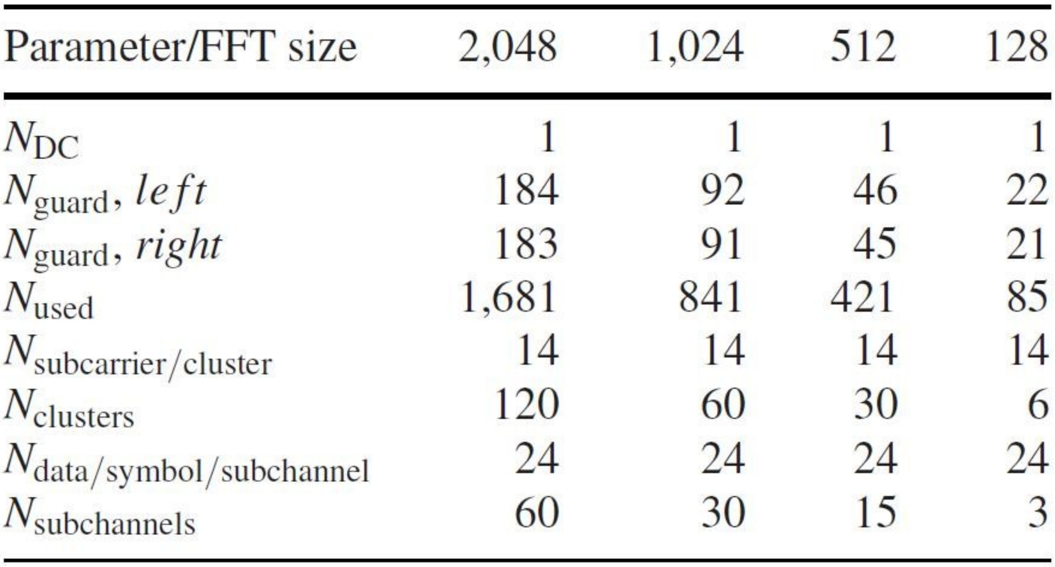
WiMAX utilization of OFDMA divides active sub-carriers into subsets. Each subset is termed a sub-channel with either distributed sub-carrier permutation or adjacent sub-carrier permutation [19]. This allows for scalability, multiple access, and use of advanced antenna array processing capabilities. Sub-carriers are allocated for data, pilot tones, and guard spacing. The following two tables describe the sub-carrier allocation for the down-link in case of full and partial usage of sub-carriers. Tables 4.1 and 4.2 show the allocation of the sub-carriers (N) for a number of FFT sizes.

Table 4.1: OFDMA Down-link Carrier Allocation – Optional Full Usage of Sub-Carriers from [19].



Parameter/FFT size	2,048	1,024	512	128
N_{DC}	1	1	1	1
$N_{\mathrm{guard}}, left$	160	80	40	10
$N_{\mathrm{guard}}, right$	159	79	39	9
N_{used}	1,729	865	433	109
N_{pilot}	192	96	48	12
N_{data}	1,536	768	384	96
$N_{\mathrm{data/subchannel}}$	48	48	48	48
$N_{\mathrm{subchannels}}$	32	16	8	2

Table 4.2: OFDMA Down-link Carrier Allocation – Optional Partial Usage of Sub-Carriers from [19].



Parameter/FFT size	2,048	1,024	512	128
N_{DC}	1	1	1	1
$N_{\mathrm{guard}}, left$	184	92	46	22
$N_{\mathrm{guard}}, right$	183	91	45	21
N_{used}	1,681	841	421	85
$N_{\mathrm{subcarrier/cluster}}$	14	14	14	14
N_{clusters}	120	60	30	6
$N_{\mathrm{data/symbol/subchannel}}$	24	24	24	24
$N_{\mathrm{subchannels}}$	60	30	15	3

4.3 WiMAX Signal

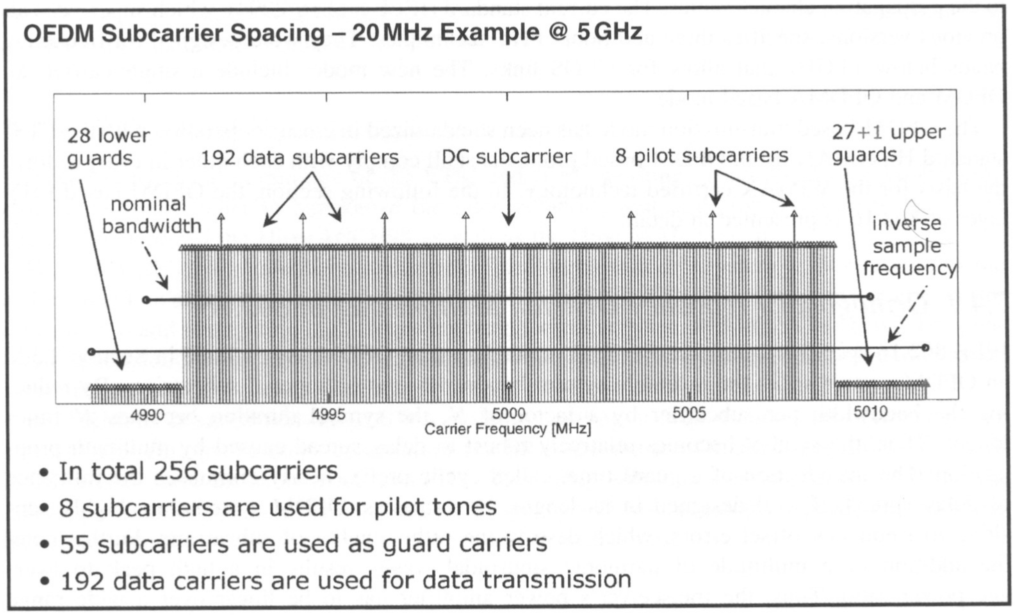
The WiMAX symbol time ($T_b = 1/\Delta f$) is the sum of the useful symbol time (T_s) and the guard time (T_g). The guard time is related to the Guard ratio (*G*) by equation 4.2. *G* has possible values of 1/32, 1/16, 1/8, and ¼. Its chosen value depends upon the channels time dispersion. Figure 4.3 relates the various parameters and options of the OFDM signal in WiMAX to one another.

$$T_s = T_b + T_g \quad (4.1)$$

$$T_g = G \cdot T_b \quad (4.2)$$

WiMAX supports adaptive modulation and coding of QPSK, 16-QAM, and 64-QAM on its individual sub-carriers. Figure 4.2 shows a possible sub-carrier allocation for a 20 MHz WiMAX OFDM signal at a 5 GHz carrier frequency. It shows the division of the sub-carriers used for pilot tones, DC sub-carrier, data sub-carriers, and guard bands.

Figure 4.2: WiMAX OFDM Sub-carrier Spacing for 20 MHz from [1].



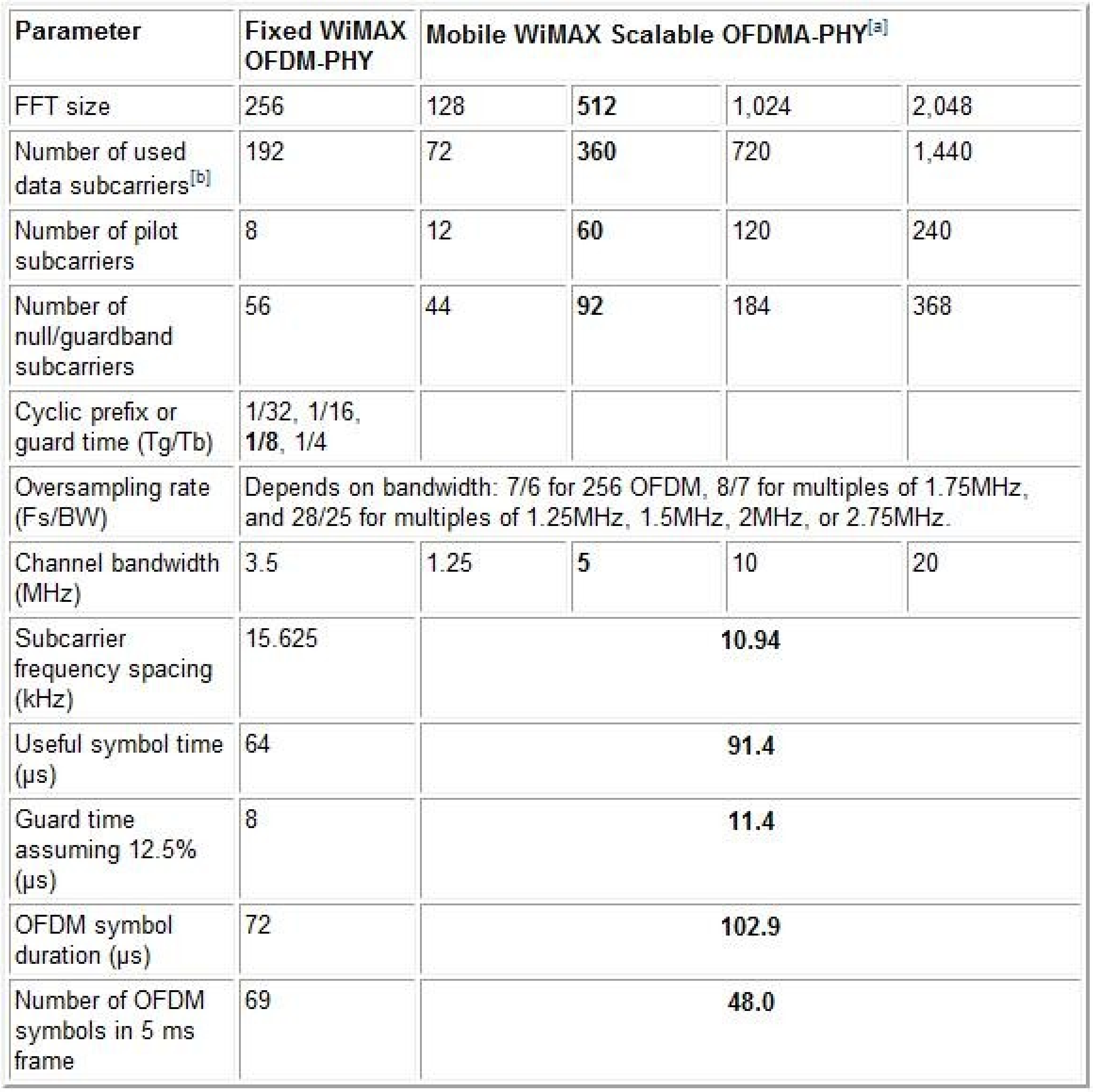
OFDM Subcarrier Spacing – 20 MHz Example @ 5 GHz

- In total 256 subcarriers
- 8 subcarriers are used for pilot tones
- 55 subcarriers are used as guard carriers
- 192 data carriers are used for data transmission

4.4 Summary

It is clear how important OFDM is to LTE and WiMAX. 4G networks will increase their capacity by utilizing OFDM technology. We have also discussed in the introduction some of the uses and benefits of covert communication. In the next sections we will propose a method for exploitation of these networks. In the next chapters we will examine the effects of the covert signal on the non-covert OFDM communication system as well as the effects and capabilities of the covert communications system in the presence of the OFDM signal.

Table 4.3: OFDM Parameters in WiMAX from from [27].



Parameter	Fixed WiMAX OFDM-PHY	Mobile WiMAX Scalable OFDMA-PHY[a]			
FFT size	256	128	**512**	1,024	2,048
Number of used data subcarriers[b]	192	72	**360**	720	1,440
Number of pilot subcarriers	8	12	**60**	120	240
Number of null/guardband subcarriers	56	44	**92**	184	368
Cyclic prefix or guard time (Tg/Tb)	1/32, 1/16, **1/8**, 1/4				
Oversampling rate (Fs/BW)	Depends on bandwidth: 7/6 for 256 OFDM, 8/7 for multiples of 1.75MHz, and 28/25 for multiples of 1.25MHz, 1.5MHz, 2MHz, or 2.75MHz.				
Channel bandwidth (MHz)	3.5	1.25	**5**	10	20
Subcarrier frequency spacing (kHz)	15.625	**10.94**			
Useful symbol time (μs)	64	**91.4**			
Guard time assuming 12.5% (μs)	8	**11.4**			
OFDM symbol duration (μs)	72	**102.9**			
Number of OFDM symbols in 5 ms frame	69	**48.0**			

5. Covert Effect on Non-Covert OFDM Communication

5.1 Premise of the Covert Communication

As we have seen, OFDM is utilized in 4G systems. These systems will become wide spread, and probably facilitate most of the wireless personal communication in the future. Therefore, it is beneficial to study covert communication that exploits wireless OFDM systems. In this chapter, we will examine the effects of the covert signal on the non-covert signal for variables of spectral base-band location with respect to the non-covert signal, covert signal power (*Watts*), and synchronous offset (*samples/symbol*).

OFDM symbols have a “slotted” structure. The bandwidth of the symbol is divided amongst the number of sub-carriers. For example, in LTE, a 5 MHz symbol specification has 512 sub-carriers. This results in 512 “slots” with a bandwidth of 15 KHz per sub-carrier [19]. WiMAX also uses a very similar structure. Both WiMAX and LTE offer a number of bandwidth and sub-carrier specifications. All specifications offer this type of “slotted” design. Several of the “slots” in these standards are not utilized for reasons of channel spacing or poor channel quality. We propose to occupy the unused spectrum of an OFDM sub-channel or an unused “slot” to support the transmission of a covert signal.

The existence of the OFDM symbol will provide a “cover” for the covert communication. By choosing spectrum for the covert signal from amongst the unused “slots” allocated for the non-covert OFDM signal, it will become more difficult to detect. It is crucial for covert communications to achieve a low probability of detection (LPD).

There are also a number of other challenges that must be examined with respect to correctly transmitting the covert information in this manner. We will look at these issues in detail in the next section. In this section we will only examine the effects of the covert signal on the non-covert OFDM signal. The non-covert BER is the measure we will use to determine if an acceptable performance is being achieved. The covert signal might draw attention to itself by causing the non-covert signal to have a noticeable increase in the BER. In a more extreme case, the covert could not only become detected, it could cause the non-covert receiver to be unable to recover significant amounts of the information in the signal due to interference from the covert signal. In this section we will seek to determine the BER of the non-covert communications system in the presence of the covert signal for varying covert signal power, synchronization offset between the non-covert and covert signals, noise power, and covert signal spectral location with respect to the non-covert spectrum.

5.2 System Parameters

The first assumption made for our simulation is the existence of known channel state information (CSI) for the channel in use by each transmitter/receiver pair. There are two sets of transmitters/receivers. A transmitter and receiver for the non-covert communication and a transmitter and receiver for the covert communication. There are four channels that must be represented in the model. Each transmitter will only account for the channel it intends to occupy. The cross channels will go unaccounted for at each receiver. Each receiver will see the intended communication as well as the signal arriving on the cross channel. The four channels are as follows:

1 - Non-covert transmitter to non-covert receiver channel-($C^{(1)}$)

2 - Non-covert transmitter to covert receiver channel-($C^{(2)}$)

3 - Covert transmitter to non-covert receiver channel-($C^{(3)}$)

4 - Covert transmitter to covert receiver channel-($C^{(4)}$)

The non-covert transmitter (NCTx) and non-covert receiver (NCRx) will have known CSI regarding the channel they will be utilizing. In practice, this does not occur. However, we know that channel estimation can be done effectively [33] thereby facilitating communication. Therefore it is not necessary to simulate channel estimation in order to validate our results. Channel estimation is not the topic of this study. The covert transmitter (CTx) and covert receiver (CRx) will also have the known CSI for the channel they will be utilizing. Neither transmitter/receiver pair will have knowledge of the cross channels or the signal arriving on them. Figure 5.1 depicts the channels as well as the transmitter/receiver pairs. Channel 1 (*$C^{(1)}$*) depicts the channel between the NCRx and the NCTx. Channel 4 (*$C^{(4)}$*) depicts the channel between the CRx and the CTx. Channels 3 and 4 depict the cross channels.

Ideal phase and frequency recovery of the signals is assumed. This assumption is also similar to the first, in that it is not necessary to model these effects in order to validate the results. We also know that phase and frequency can be recovered effectively [33].

The four channel's magnitude and phase response will be held constant throughout this experiment. Here we used fixed representative channels. Here we used fixed representative channels. These channels all differ in their magnitude and phase characteristics as they would in practice (see Figures 5.2, 5.3, 5.4, 5.5). These representative channels were generated at random. In reality, we know that wireless channel characteristics vary with time and location for mobile channels. We compared the system performance with the representative channel to that obtained with several other randomly selected channel realizations and found there was little difference in system performance.

Figure 5.1: Transmitter/Receiver Pairs & Channels.

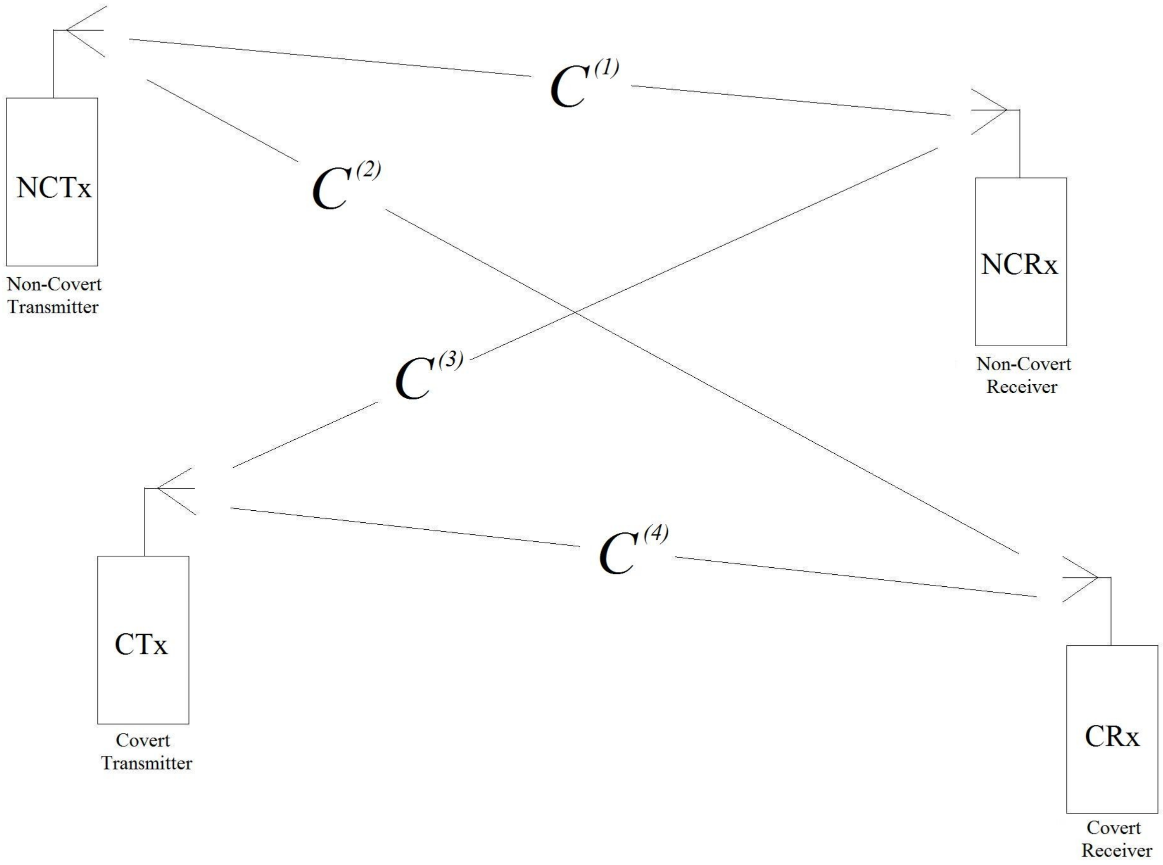


Figure 5.2: Non-Covert Channel Magnitude and Phase ($C^{(1)}$)

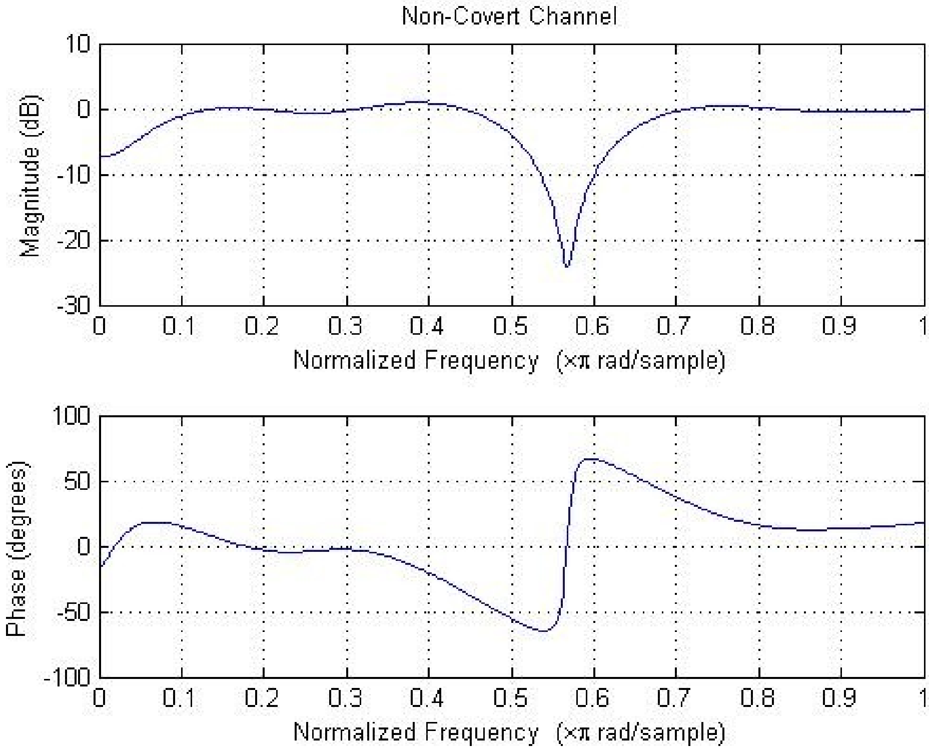


Figure 5.3: Covert Channel Magnitude and Phase ($C^{(4)}$)

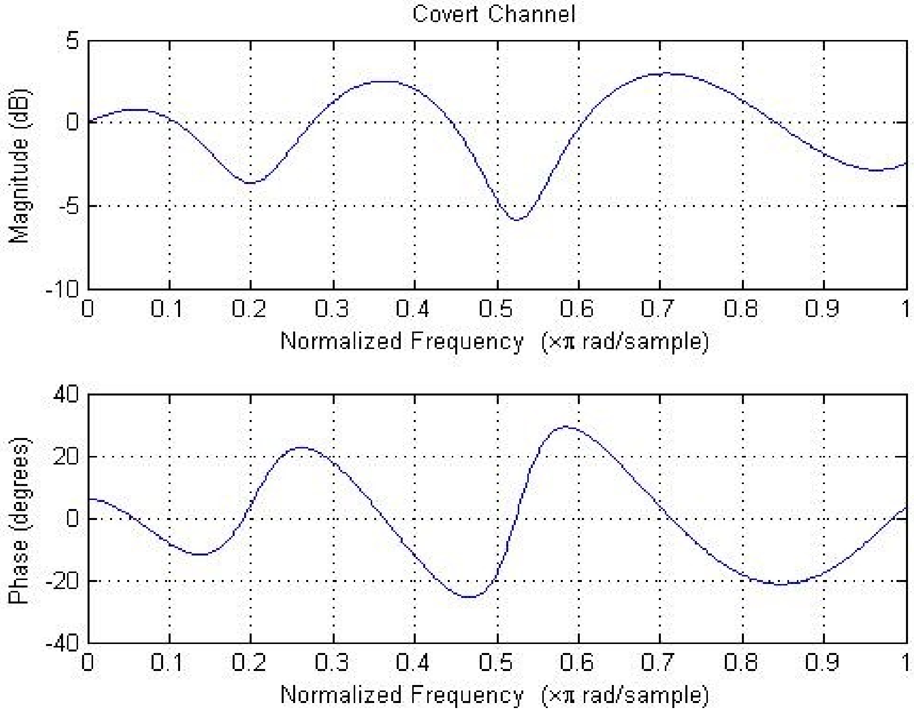


Figure 5.4: Non-Covert to Covert Channel Magnitude and Phase ($C^{(2)}$)

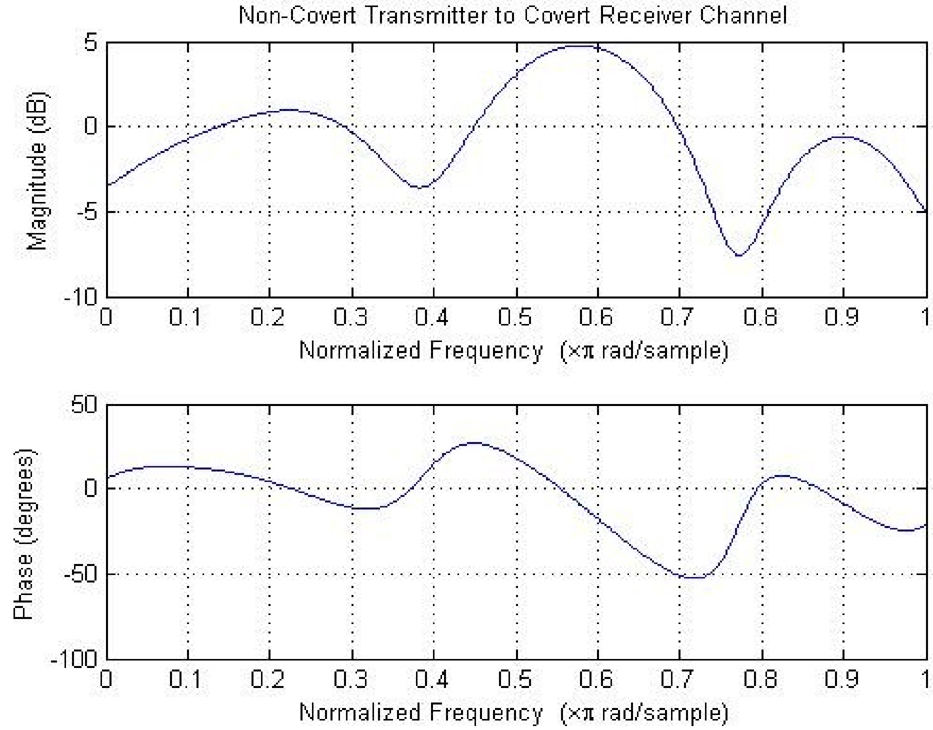
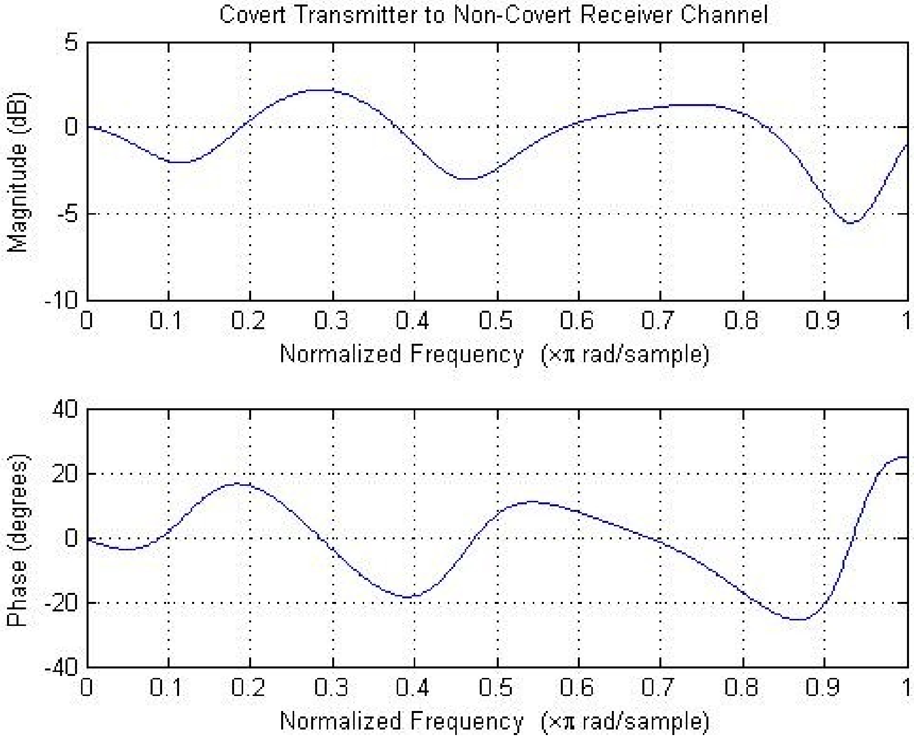


Figure 5.5: Covert to Non-Covert Channel Magnitude and Phase ($C^{(3)}$)



(See Appendix A) We assume that both Tx/Rx sets have the known CSI information. The simulation begins, in the NCTx, by executing the bit and power allocation algorithm described in section 2.4. All channels not achieving a desired symbol error rate (SER) will not be utilized by the NCTx and could potentially be used by the CTx. Both LTE and WiMAX use 4-QPSK, 16-QAM, or 64-QAM signal constellations on each sub-channel. After these allocations have completed, we generate an array of random data (0s & 1s), divide the data up amongst the sub-carriers, and convert to the appropriate point in the normalized symbol constellation (QPSK, 16-QAM, or 64-QAM). After the points have been multiplied by the power allocated for that channel, we apply the IFFT to the symbol points and then add the cyclic prefix (CP).

We apply the channel as a discrete time filter and add the noise. The cross channel signal is also added at this point. The CTx follows similarly this process except that it will transmit its data on only one sub-carrier. A mathematical representation of this can be seen in equation 5.1. The equation shows the ith channel magnitude on the kth sub-carrier ($C_k^{(i)}$) and phase (ϕ_k) response, the point in the symbol constellation chosen to represent the in-phase and quadrature components for the non-covert (A_{kc} / A_{ks}) as well as the covert (B_{kc} / B_{ks}), and the sub-carrier base-band frequency (f_k). The covert only transmits on the vth sub-carrier.

$$r(t) = \left(\sum_{k=0}^{N-1}\sqrt{\frac{2}{T}}\left|C_k^{(1)}\right|A_{kc}\cos(2\pi f_k t+\phi_k^{(1)})+\sqrt{\frac{2}{T}}\left|C_k^{(1)}\right|A_{ks}\sin(2\pi f_k t+\phi_k^{(1)})\right) +$$

$$\left(\sum_{i=0}^{N-1}\sqrt{\frac{2}{T}}\left|C_i^{(3)}\right|B_{ic}\cos(2\pi f_i t+\phi_i^{(2)})+\sqrt{\frac{2}{T}}\left|C_i^{(3)}\right|B_{is}\sin(2\pi f_i t+\phi_i^{(2)})\right) + n(t) \qquad (5.1)$$

$$A_{vc} \,\&\, A_{vs}=0\,;\, B_{ic} \,\&\, B_{is}=0 \text{ except for } i=v$$

At the NCRx receiver, the CP is first removed. We then use the FFT to convert back to the frequency domain and "equalize" the signal by dividing it by the channels response. We use a maximum likelihood detector at the Rx to convert the received signal to constellation points for each sub-carrier. Then, the points are decoded back to 0s and 1s and compared to the original information to find errors in the data. The BER is tracked as the OFDM symbols are received. The CRx does the same for its covert signal. The mathematical representation of the signal at the CRx is seen in equation 5.2

$$r'(t) = \left(\sum_{k=0}^{N-1}\sqrt{\frac{2}{T}}\left|C_k^{(2)}\right|A_{kc}\cos(2\pi f_k t+\phi_k^{(3)})+\sqrt{\frac{2}{T}}\left|C_k^{(2)}\right|A_{ks}\sin(2\pi f_k t+\phi_k^{(3)})\right) +$$

$$\left(\sum_{i=0}^{N-1}\sqrt{\frac{2}{T}}\left|C_i^{(4)}\right|B_{ic}\cos(2\pi f_i t+\phi_i^{(4)})+\sqrt{\frac{2}{T}}\left|C_i^{(4)}\right|B_{is}\sin(2\pi f_i t+\phi_i^{(4)})\right) + n(t) \qquad (5.2)$$

$$A_{vc} \,\&\, A_{vs}=0\,;\, B_{ic} \,\&\, B_{is}=0 \text{ except for } i=v$$

The covert signal is specified by its bit rate (bits-per-second), spectral location, power, and synchronous offset. For example, the covert signal could be placed at channel no. -256 corresponding to f_c = -3.38325 MHz or channel no. -152 corresponding to f_c =

-2.2725 MHz. The relationship between the channel no. and the sub-carrier frequency is channel no. multiplied by the sub-channel bandwidth (15 KHz) minus half the sub-channel bandwidth (7.5 KHz). The power of the covert signal ($E_{b,covert}$) is specified with respect to the power in the non-covert signal ($E_{b,non\text{-}covert}$) in decibels (dB). The synchronous offset of the covert symbol is given with respect to the non-covert symbol (Tau).

5.3 Simulation Inputs and Outputs

The Mat Lab simulation of the non-covert OFDM system and the covert system has six inputs (See Appendix A):

1 - If the covert is on or off

2 - The number of OFDM symbols in the simulation run

3 - The noise power in Watts/Hz

4 - Synchronization Offset in samples/symbol

5 - The symbol constellation of the covert signal (BPSK, 4M-QAM, etc.)

6 - The covert signal rate with respect to the full rate allowed by the bandwidth

The simulation outputs the following;

1 - The running non-covert OFDM system BER

2 - The running covert system BER

3 - The non-covert signal-to-noise ratio (SNR)

4 - E_b/N_o dB non-covert signal

5 - E_b/N_o dB covert signal

6 - $E_{b,covert}/E_{b,non\text{-}covert}$ dB

7 - Non-covert OFDM system channel capacity (bps)

8 - Covert system channel capacity in (bps)

The simulation requires approximately 15 minutes to run for every 10,000 non-covert OFDM symbols. The simulation also plots the average PSD at the output of the NCTx and CTx as well as the average PSD at the input of the NCRx and the CRx.

5.4 Covert Effect on Non-Covert in the Presence of Increasing Noise

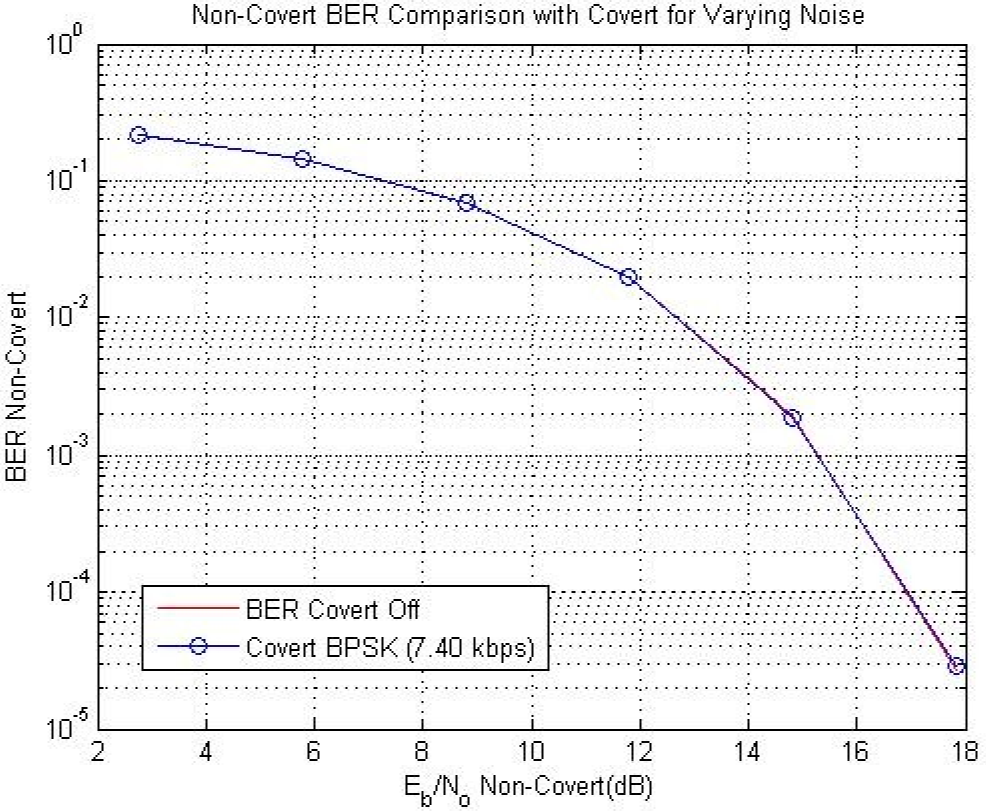
For all experiments conducted here, the bandwidth of the non-covert OFDM symbol was kept constant at the 5 MHz specification and utilizing a 512 point FFT [19]. The sub-carrier spacing is 15 KHz. The normal cyclic prefix (6 samples/symbol) will be used as opposed to the extended CP (7 samples/symbol). BPSK was used exclusively for the covert signal. The bandwidth of the covert is 15 KHz.

The first question addressed here is the effect of increasing the noise power while maintaining constant signal power on the non-covert system. We would expect that the

BER increases with increasing noise power (N_o). The non-covert OFDM signal power will remain constant while the noise power increases, thereby decreasing the E_b/N_o. The covert will occupy spectrum in a selected unused "slot" adjacent to the sub-carriers occupied by the OFDM symbol. A sub-channel (-152) next to those utilized by the non-covert signal was chosen for maximum effect on the BER of the non-covert OFDM system. We will see later that the BER of the covert system increases as its distance from the non-covert signal decreases. We can deduce from this that the effect of the signals on one another occurs when the distance in the spectrum decreases. This spectrum is not used by the non-covert signal for the reason of channel spacing. Signals are allocated more spectrum than there bandwidth for the reason of channel spacing. Channel spacing reduces the chance that the signal will interfere with adjacent signals in the spectrum. For example, in this experiment a 5 MHz OFDM symbol is used but 7.68 MHz of spectrum is allocated for the actual signal to prevent interference in the next 5 MHz signal in the spectrum. This simulation was run twice. The first curve was generated without the covert signal for the purposes of comparison. The second curve was generated with the covert signal maintaining constant power.

It can be seen that the two curves lie on top of each other. It must be noted that for this examination the power was adjusted per sub-carrier for a desired SER of 10^{-4} at a noise power of N_o = .00002 Watts/Hz using the bit and power allocation algorithm discussed in section 2.4 [3]. The average available power at the NCTx is 1 Watt. The noise was then increased while keeping the symbol power constant which results in a lower BER for the non-covert signal. This result shows that the covert has little to no effect, in this scenario, on the non-covert and is further proof validating the simulation because it is in line with theoretical BERs [33] [3]. We will not discuss the BER of the covert in this section. We will discuss it in depth in later sections. It is worth noting that the power on the covert was adjusted so that it could achieve a BER of 10^{-4}, while employing BPSK as its signal constellation for a noise power of N_o = .00002 Watts/Hz which results in a covert signal power of 5 x 10^{-5} Watts. The covert was placed in channel -152 and the synchronous offset was set 128 samples/symbol.

Figure 5.6: Comparison of BER Curve With and Without Covert ($R_{b,covert}$ = 7.40 kbps, Channel = -152 $E_{b,covert}/E_{b,non-covert}$ = -10.83 dB, Ʈ = 128 samples/sym)



5.5 Effect of Increasing Covert Power on Non-Covert OFDM Signal

For the next set of experiments, the covert signal power was increased (Figure 5.7) and the effect on the non-covert OFDM signal BER recorded. We were also able to view the power spectral density (PSD) at the CRx and NCRx. The noise power was held steady at N_o = .00002 Watts/Hz. The average available power at the NCTx was set to 1 Watt. In Figures 5.7 we can see the base-band PSD at the NCRx as the covert signal power increases for channel -152. Figure 5.7a shows the PSD without the covert. Figure 5.7b shows the covert with a signal power of 5×10^{-5} adjusted for a desired BER of 10^{-4}. We increase the power of the covert thereafter from .0001, .001, .01, .1, 1, 5, 25, 100, and 250 Watts respectively in Figures 5.7c through 5.7k . We can see clearly the spectral interference increase as the covert signal power increases.

Figure 5.7: PSD at the Input to the Covert Receiver for Increasing Covert Signal Power ($R_{b,covert}$ = 7.40 kbps, Channel = -152, Ţ = 128 samples/sym)

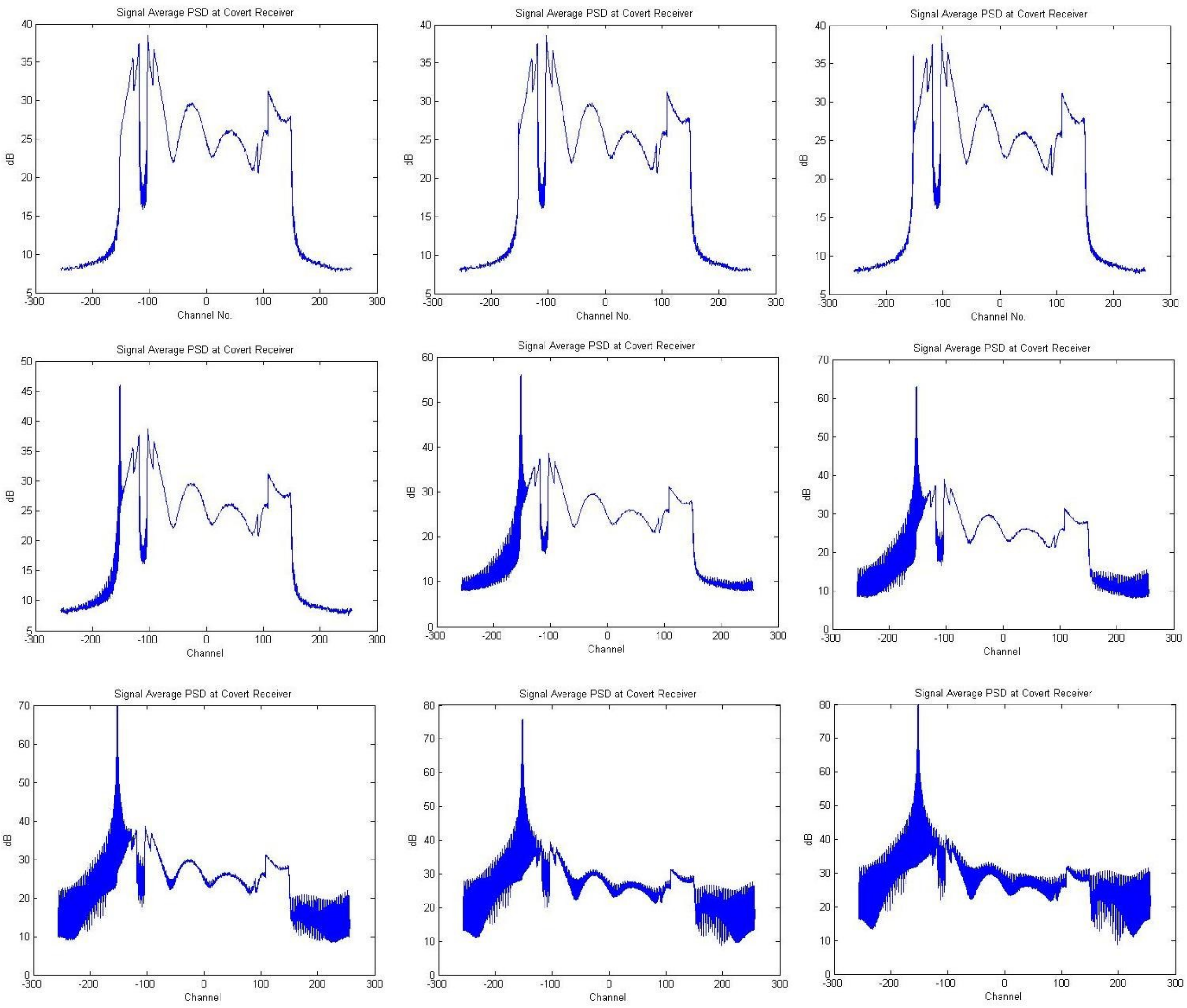
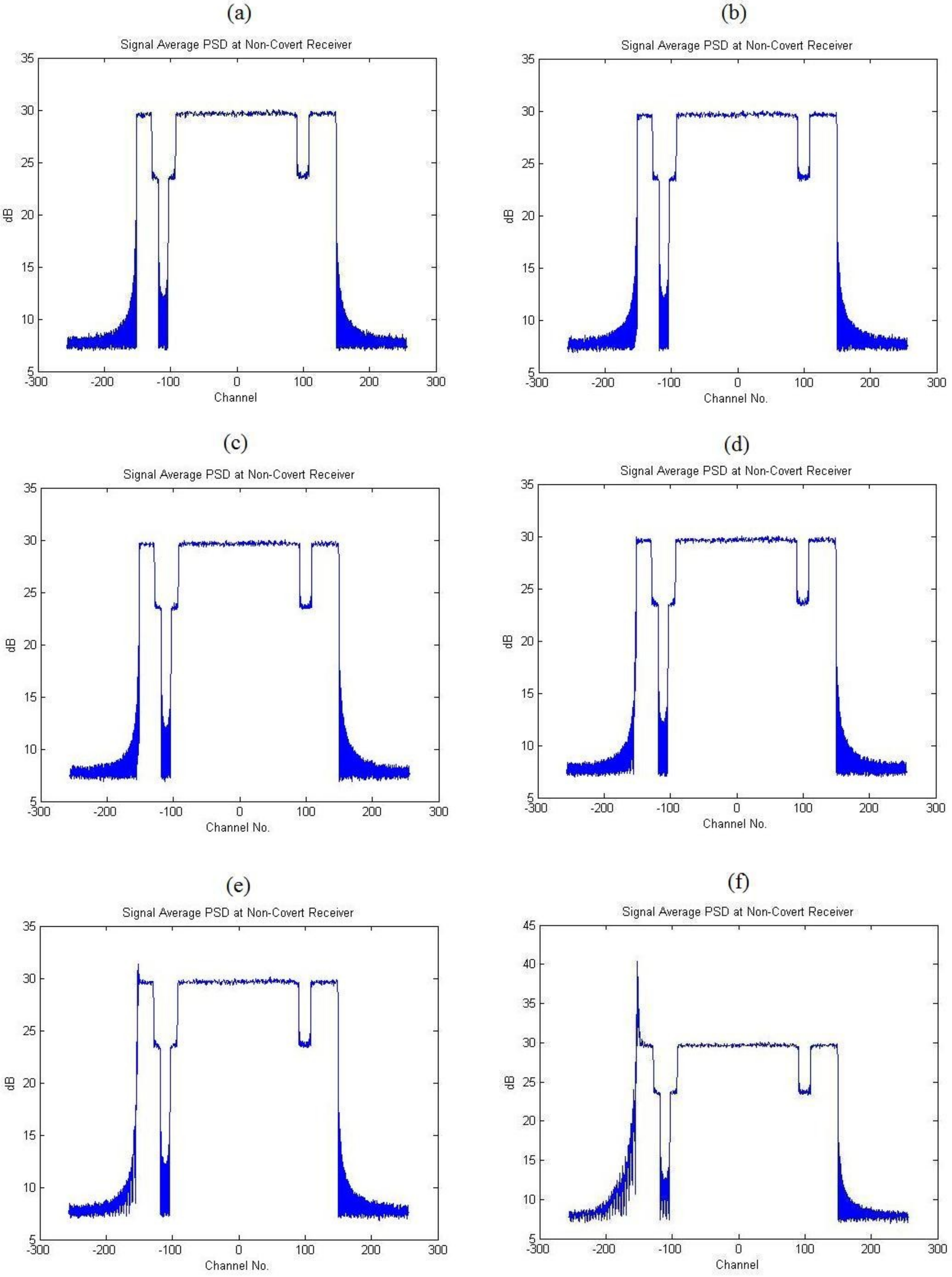
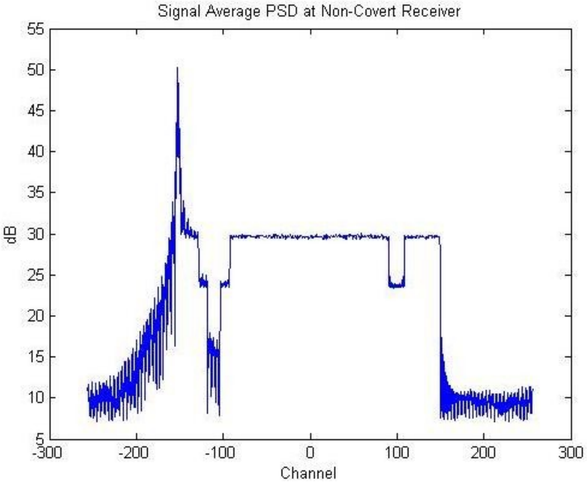


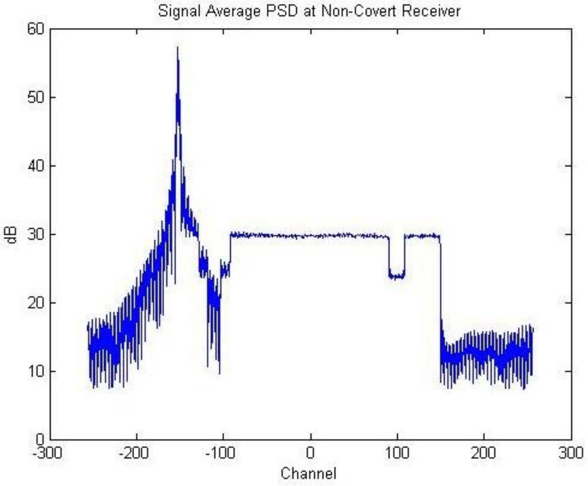
Figure 5.8: Base-band Spectrum at Non-Covert Receiver for Increasing Non-Covert Signal Power ($R_{b,covert}$ = 7.40 kbps, Channel = -152, Ʈ = 128 samples/sym)



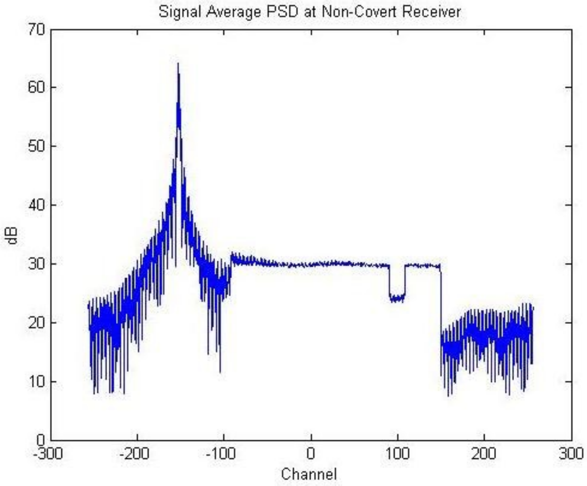
(g)


Signal Average PSD at Non-Covert Receiver
dB
Channel
55
50
45
40
35
30
25
20
15
10
5
-300
-200
-100
0
100
200
300

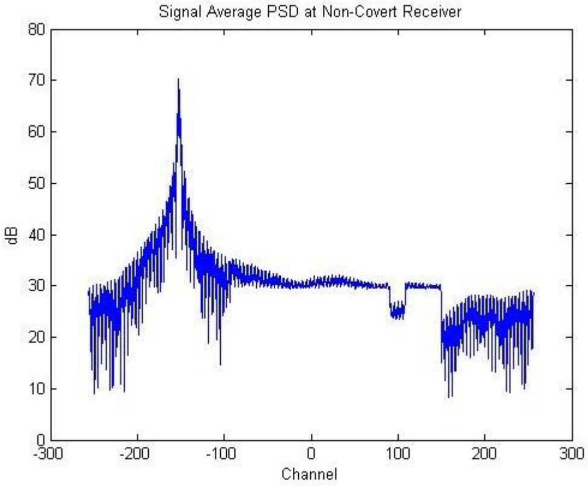
(h)


Signal Average PSD at Non-Covert Receiver
dB
Channel
60
50
40
30
20
10
0
-300
-200
-100
0
100
200
300

(i)


Signal Average PSD at Non-Covert Receiver
dB
Channel
70
60
50
40
30
20
10
0
-300
-200
-100
0
100
200
300

(j)


Signal Average PSD at Non-Covert Receiver
dB
Channel
80
70
60
50
40
30
20
10
0
-300
-200
-100
0
100
200
300

(k)

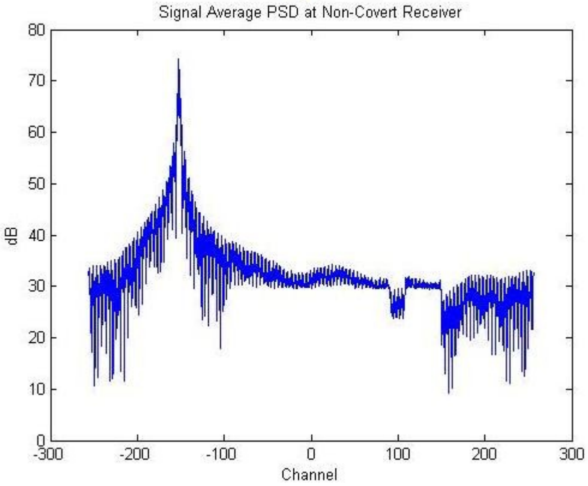
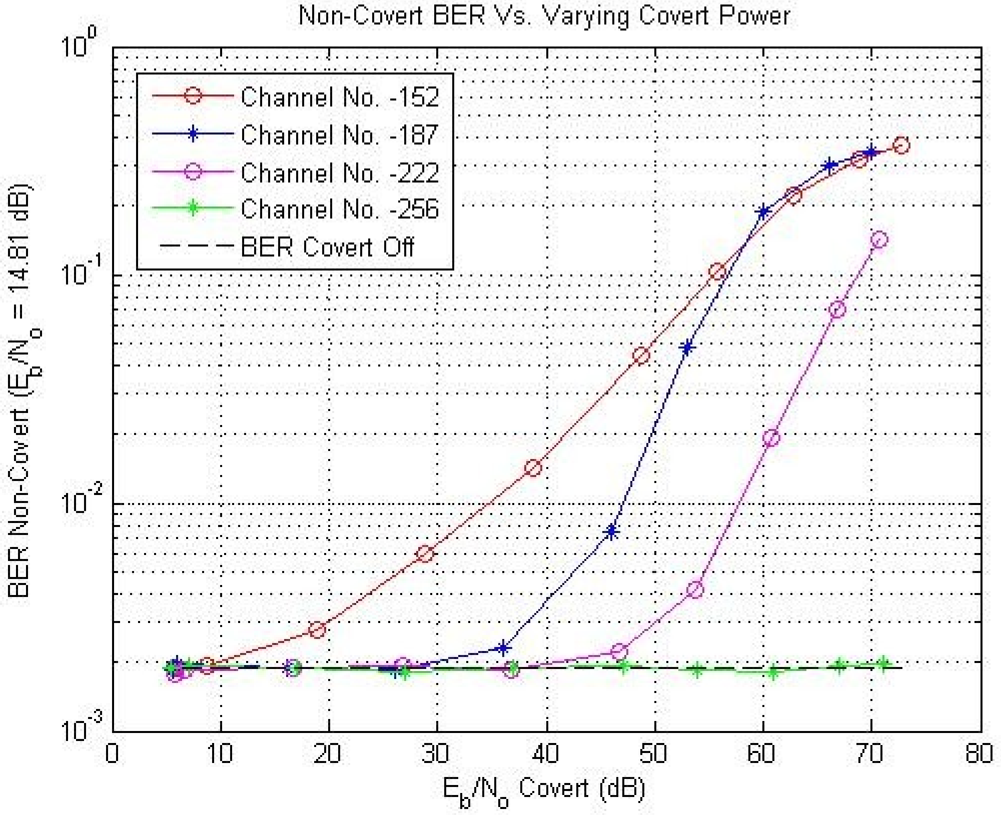

Signal Average PSD at Non-Covert Receiver
dB
Channel
80
70
60
50
40
30
20
10
0
-300
-200
-100
0
100
200
300

Figure 5.9 demonstrates the increase of non-covert BER as the covert signal power increases for several spectral locations. The dashed line is inserted for comparison. It provides us with a reference for the BER of the non-covert without a covert signal present. The BER rate increase is unchanged for a covert E_b/N_o less than 9 dB when placed in channel -152. This is the power required to achieve a desired SER equal to that of the non-covert system of 10^{-4}. Beyond that, the BER for the non-covert OFDM becomes more noticeable as covert power increases.

Figure 5.9: E_b/N_o Covert Vs. BER Non-Covert ($R_{b,covert}$ = 7.40 kbps,

Ʈ = 128 samples/sym)



5.6 Effect of Synchronous Offset on Non-Covert Signal

Another of the variables that must be examined is the synchronous offset between the two signals. The OFDM signal sub-carriers are orthogonal to one-another as discussed in Section 2.2. However, the non-covert will only achieve this orthogonality if its symbol timing is perfectly in line with the OFDM symbols. The covert symbol must arrive at the receiver at the exact same instant as the non-covert symbol. This is very unlikely and somewhat impossible to achieve.

For our experiment in this section, we measured the synchronous offset in terms of the samples per symbol. We want to determine the effects of the synchronous offset, tau, between the covert on the BER of the non-covert OFDM signal. When the covert is offset, it loses its orthogonality with respect to the other OFDM sub-carriers thereby resulting in interference. Figures 5.10 and 5.11 shows the effects of this interference on the non-covert OFDM signal for synchronous offsets of 0, 1, 4, 8, 16, 32, 64, 128, and 256 samples per symbol. The power of the signals and the noise power was held constant throughout the simulation. Figures 5.10 and 5.11 shows that the synchronous offset between the covert and non-covert signals has no effect on the non-covert BER for a covert signal on the edge (Figure 5.10) of the utilized OFDM spectrum and in the middle of the unused OFDM spectrum (Figure 5.11).

Figure 5.10: Synchronous Offset (Ʈ) Vs. Non-Covert BER ($R_{b,covert}$ = 7.40 kbps, Channel = -146, $E_{b,covert}/E_{b,non\text{-}covert}$ = -10.83 dB)

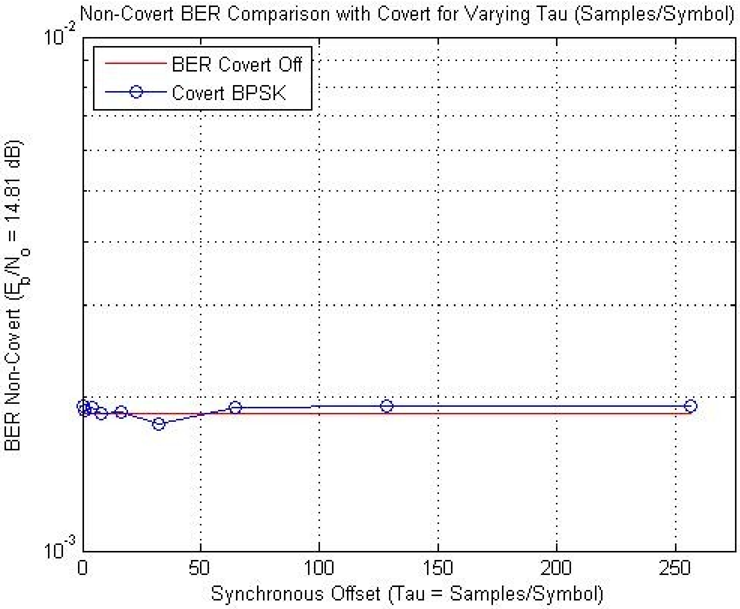
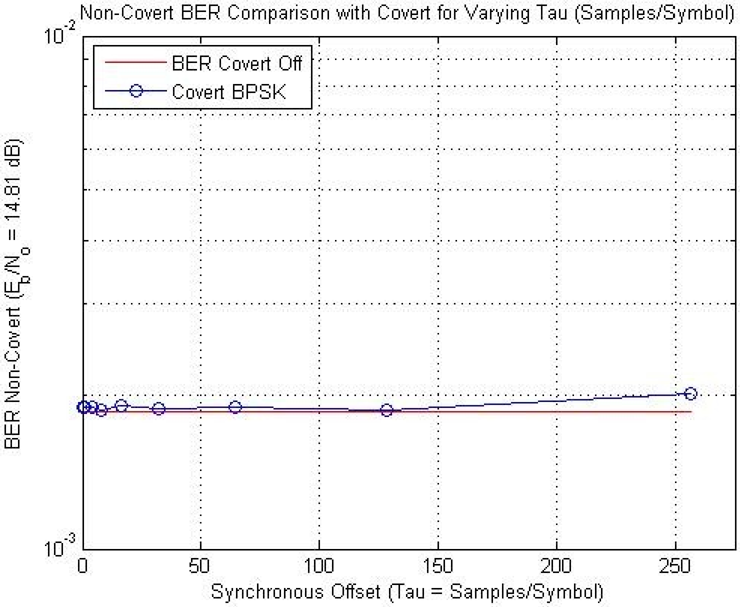


Figure 5.11: Synchronous Offset (Ʈ) Vs. Non-Covert BER ($R_{b,covert}$ = 7.40 kbps, Channel = -105, $E_{b,covert}/E_{b,non\text{-}covert}$ = -9.15 dB)



6. Limitations of the Covert Signal Communication System

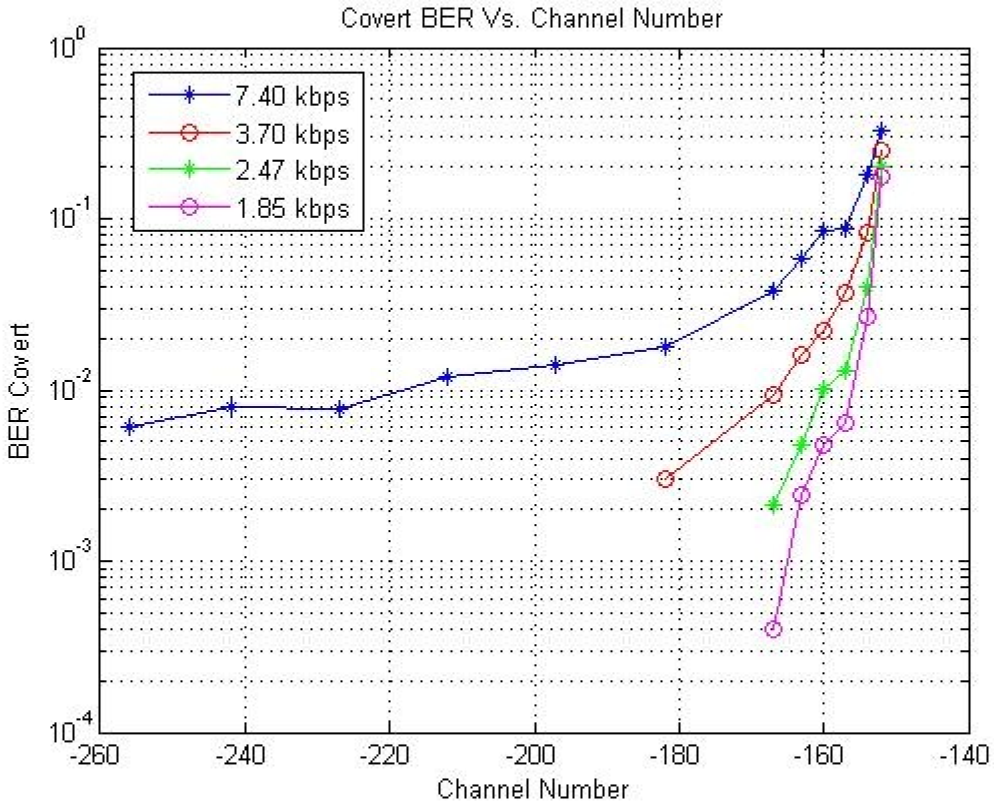
The previous chapter evaluated the effects of the presence of the covert signal on the non-covert communications system. In this chapter we will examine the effectiveness of the covert signal to send information in the presence of the non-covert OFDM signal. Here we ascertain if the interference from the non-covert is too great to allow a covert signal within its designated spectrum to communicate effectively. Also, this evaluation will allow us to view the effects of covert signal bandwidth (symbol rate), position in the spectrum with respect to the base-band non-covert signal, and synchronous offset for the covert signal on the performance of the covert communication and its potential.

6.1 Effect of Spectral Position on Covert Signal

The non-covert OFDM symbol has 512 sub-carriers. The 5 MHz specification in LTE calls for 301 of the 512 sub-carriers to be utilized [19]. For this study the covert signal will be placed in one of the non-utilized sub-channel "slots" in the base-band spectrum. It will move from the left most sub-channel (channel no. -256 @ -3.8325 MHz) until it reaches the sub-channel which lies next to the first sub-channel utilized by the OFDM waveform (channel no. -152 @ -2.2725 MHz)

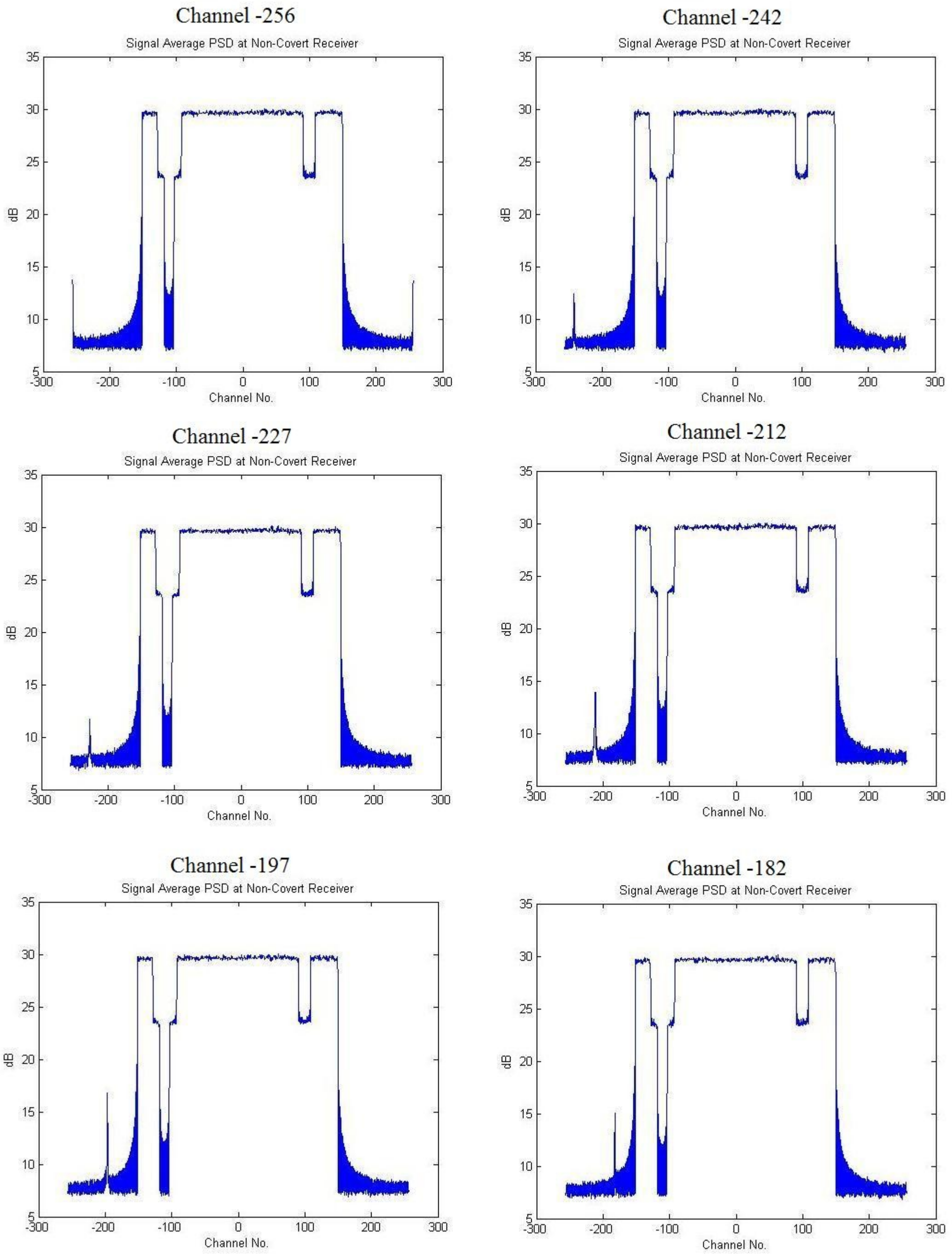
The power of the covert communications system is adjusted to reach a desired SER of 10^{-4}. The power with respect to the location of the covert will also vary due to the channel magnitude response of the sub-channels varying (see Figure 6.2). A synchronous offset of 128 symbols/second was used. We will see in later sections why this synchronous offset was chosen. The non-covert OFDM signal had an average available power at the transmitter of 1 Watt. For this study, the rate of the covert transmitter was also varied from 1.85 to 7.40 kbps. The maximum rate of the covert system for the scenario studied was the maximum allowed by the bandwidth of the 15 KHz sub-channel. When factoring in the CP the maximum rate for the covert communications system is 7.40 kilo-bits-per-second (kbps). The rate was then lowered in order to achieve an improved BER for the covert communications system. In Figure 6.1, we see that the rates of each individual curve, starting from the top curve, is the full rate (7.4 kbps), half the full rate, one third the full rate, and one quarter the full rate for a bandwidth of 15 KHz respectively.

Figure 6.1: Channel Number Vs. Covert BER (τ = 128 samples/sym)



We can see that it is difficult to achieve an acceptable BER (10e-3) with the full rate. For the lower rates, the BER rate improves dramatically for the same distances as the rate decreases. As expected, when the distance from the utilized sub-carriers of the OFDM symbol increases, the BER of the covert decreases. For example, if an acceptable BER is 10^{-2} and we have a bit rate of 1.85 kbps, then the covert can reside as close as sub-channel -157. If our rate is 2.47 kbps, then we need to be as far out as channel -160. It is also worth noting that the lower the channel number the further in the spectrum the covert is from the non-covert signal.

Figure 6.2: PSD at Non-Covert Receiver ($R_{b,covert}$ = 7.40 kbps, Ʈ = 128 samples/sym)


Channel -256

Channel -242

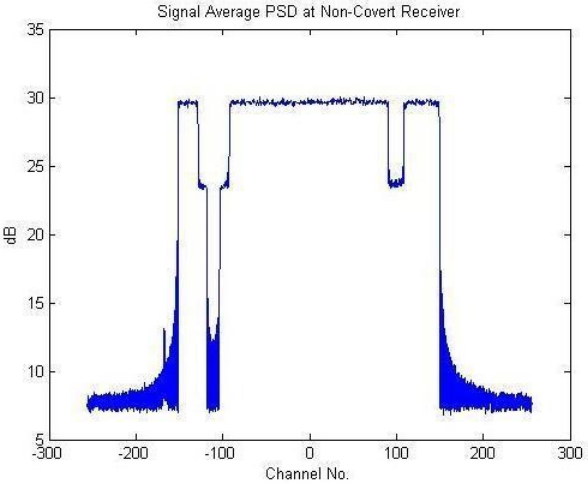
Channel -227

Channel -212

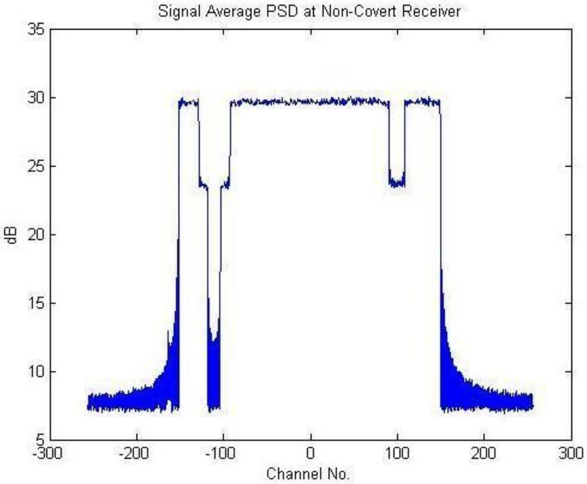
Channel -197

Channel -182

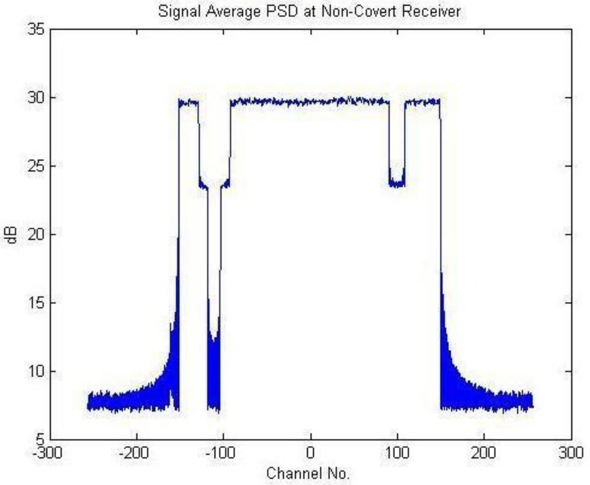
Channel -167



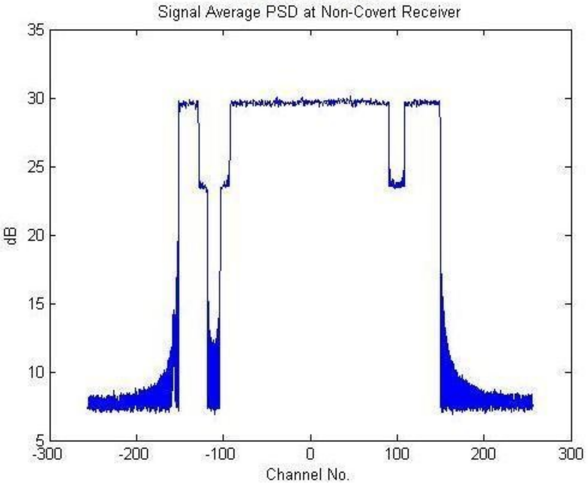
Channel -163



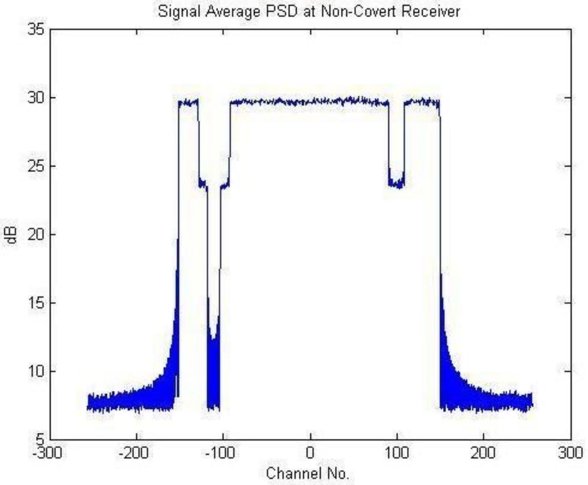
Channel -160



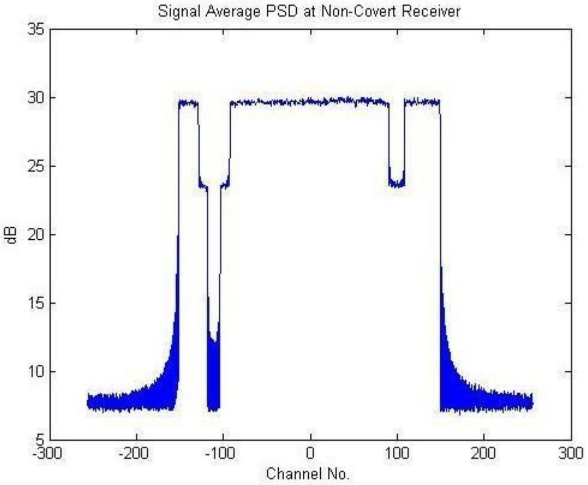
Channel -157



Channel -154



Channel -152



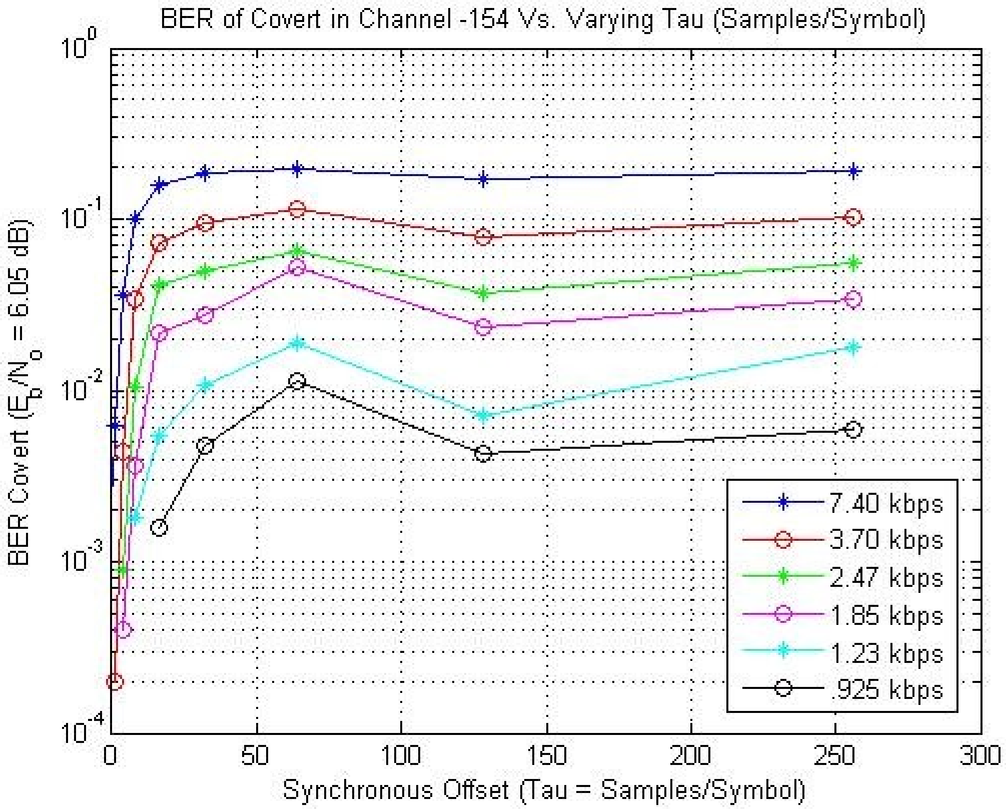
6.2 Effect of Synchronous Offset on Covert

Next we examine the effect the synchronous offset has on the covert BER. After applying the *N*-point IFFT on the sub-carriers at base-band, the resulting OFDM base-band symbol is comprised of *N* samples per symbol. Here a 512 point IFFT was utilized thereby giving a 512 sample symbol. The covert symbol operates in one of the unused sub-channels of the non-covert symbol. In practice, no IFFT/FFT is needed for the covert system. However, in this study utilizing an IFFT/FFT for the covert system simplified the implementation of the simulation. In the CTx, while in the frequency domain prior to the IFFT, we insert zero as the symbol for all sub-carriers except the covert sub-carrier. It has been verified that this is equivalent to transmitting the covert signal without the IFFT. The CP involves copying the last six samples of the symbol and placing them in front of the 512 samples of the OFDM symbol resulting in a symbol that is 518 samples long. The synchronous offset can be viewed in terms of the symbol samples. Using the first sample as a reference out of the *N* samples per symbol for the covert and non-covert, if both are received at the same sample time in the receiver, then there is no synchronous offset. If the covert sample is received n samples later, than the synchronous offset (Tau) is equal to n.

For Figure 6.3, we placed the covert signal in sub-channel number -154. The OFDM symbol in LTE does not utilize 210 of the sub-channels out of 512 for channel spacing and one DC sub-carrier [19]. That results in the non-utilization of the first 105 sub-channels. This location was chosen, as opposed to sub-channel -152 which would provide a better LPD than sub-channel -154, because as was seen in the previous section the BER improves significantly for any bit rate when the distance from the utilized sub-channels increases. The performance of the non-covert system for sub-channel -152 was poor at all rates for any synchronous offset and the covert remains difficult to view in the PSD for channel -154 as can be seen in Figure 6.2 for the plot labeled "Channel -154".

Figure 6.3: Cover BER Vs. Synchronous Offset for Sub-Channel -154

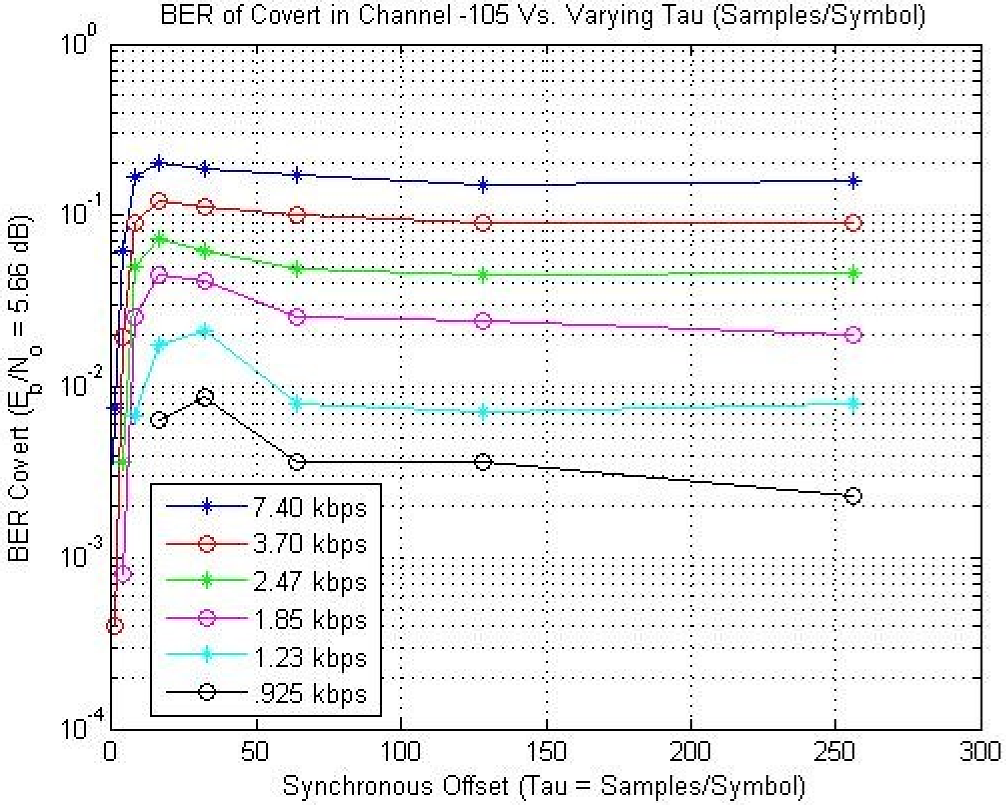
($E_{b,covert}/E_{b,non\text{-}covert}$ = -8.76 dB)



For Figure 6.4, we placed the covert in sub-channel number -105. Figure 6.5 shows the PSD at the NCRx. The NCTx does not utilize 14 consecutive (-111 to -98) sub-channels due to poor channel quality. We make the assumption that the CTx has prior knowledge of this and that six of the sub-channels on one side and 7 on the opposing side of -105 are also not utilized for the same reason of poor channel quality, thereby giving the covert siganl good spacing. The covert signal can be seen clearly amongst the utilized sub-channels.

Figure 6.4: Cover BER Vs. Synchronous Offset for Sub-Channel -105

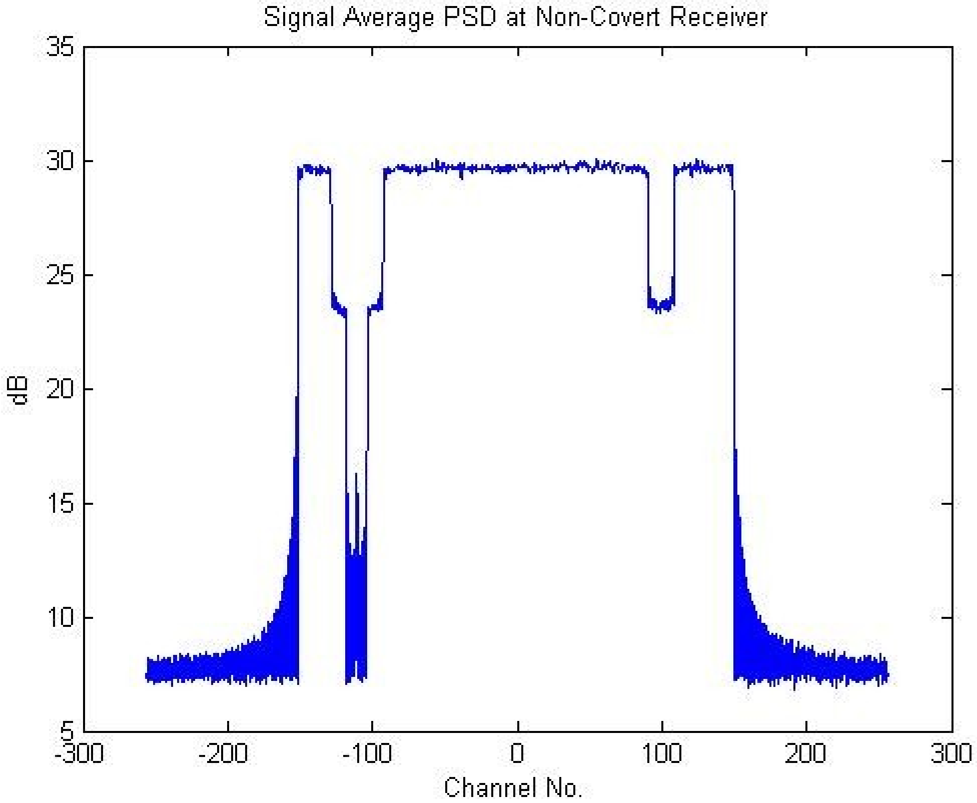
($E_{b,covert}/E_{b,non\text{-}covert}$ = -9.15 dB)



It can be seen from Figures 6.3 and 6.4 that the BER of the covert improves as the rate decreases. For no synchronous offset, all rates perform well. As we have stated, this is not achievable in practice. Any synchronous offset causes the BER to increase significantly. When the bit rate was lowered to 462 bps a BER of 10^{-4} or less was achieved for channels -105 and -154 for all synchronous offsets.

Figure 6.5: PSD at Non-Covert Receiver for Sub-Carrier -105

($E_{b,covert}/E_{b,non\text{-}covert}$ = -6.05 dB)



7. Conclusion

With the soon to be widespread deployment of wireless 4G systems, a method of covert communication has been proposed that takes advantage of the OFDM spectral structure of these systems. By inserting the covert signal in one of the unused sub-channels of the OFDM channel, the signal is potentially hidden or difficult to detect. In order to remain undetected, the covert signal must have little to no effect on the OFDM symbol. The standard of measurement of this effect is the BER of the non-covert information. Here we have demonstrated the potential and feasibility of this concept.

For this study a 5 MHz LTE waveform specification was chosen. This waveform has 512 sub-carriers and a sub-channel bandwidth of 15 KHz utilizing adaptive modulation [19]. In the case where the covert signal uses the full bandwidth of the sub-channel, 15 KHz, the power of the covert signal has a noticeable effect on the BER of the non-covert communication for a covert E_b/N_o greater than 9dB and $E_{b,covert}/E_{b,non\text{-}covert}$ less than -7 dB. The covert synchronous offset and location within the non-utilized base-band spectrum of the non-covert signal has no effect on the BER of the non-covert. Therefore, as long as the covert signal power is kept equal to or lower than the necessary power to achieve a SER equal to that of the non-covert system, in this case 10^{-4}, the synchronous offset and location have a negligible effect on the non-covert OFDM communication BER.

In order for the covert signal to be able to communicate with an acceptable BER ($< 10^{-3}$), the symbol rate must be several times below the bandwidth of the OFDM sub-channel it is occupying. Symbol synchronous offset, location in the base-band spectrum of the non-covert OFDM spectrum, and symbol rate all significantly affect the BER of the covert signal. In Figures 6.3 and 6.4, we can see that if the symbol rate of the covert is equal to or less than the 1/8th of the full rate for the 15 KHz bandwidth, or 935 bps for the 5 MHz LTE OFDM waveform specification, it can achieve an acceptable BER. If the symbol rate of the covert is lowered it can achieve an improved BER and the synchronous offset can be disregarded. Also, the closer the covert signal is in the spectrum to the utilized sub-channels of the non-covert OFDM symbol, the worse the performance. BER performance of the covert improves significantly by allowing the covert to reside in a sub-channel that is at least a few sub-channels distance from the utilized sub-channels of the non-covert OFDM symbol. Even at a relatively low symbol rate utilizing 1/8th the bandwidth of the sub-channel, the BER remains unacceptably high (> 0.1) for channels directly adjacent to those utilized by the non-covert signal. This is due to the interference from the non-covert symbol remaining high in those channels. For covert signals utilizing unused channels by the non-covert signal due to poor channel quality, such as in Figure 6.5, the covert system can achieve an acceptable BER if there at least a few sub-channels on both sides of the covert signal that are not used by the non-covert system and the rate of the covert signal is lowered to 1/8th the maximum rate allowed by the bandwidth or less.

If the covert signal power is increased beyond the power necessary to achieve a desired SER rate equal to that of the non-covert OFDM signal, it becomes noticeable in the power spectral density and causes the BER of the non-covert signal to increase noticeably as well. This will increase its probability of detection and defeat its purpose. In order to achieve a low probability of detection and communicate effectively, the covert system must adjust its signal power to achieve a SER equal to or less than that of the non-covert OFDM symbol, occupy a sub-channel that is at least a few sub-channels distance from the utilized non-covert OFDM symbol on both sides of the covert channel, and lower its rate to 1/8th that allowed in the bandwidth of a sub-channel or less. In the case of the 5 MHz LTE waveform which has 15 Khz sub-channels, it equates to 935 bps or less. If the desired SER of the covert system were lower than the non-covert system, it result in higher covert signal power. Higher covert signal power will cause the covert to become more easily detected. These conditions will allow the covert to operate with an acceptable BER and low probability of detection regardless of the symbol synchronous offset.

8. Future Work

While this study demonstrated the feasibility of covert communications within an OFDM signal; additional work is needed to explore the full potential of the concept. We have seen how the synchronous offset effects the covert BER significantly in section 6.2. For little to no synchronous offset, the BER of the covert signal improves drastically. This is because for no synchronous offset the covert becomes orthogonal to the sub-carriers in the non-covert OFDM symbol and eliminates the side-lobe interference from the other sub-carriers. A system for monitoring the synchronous offset and adjusting the symbol timing to achieve no synchronous offset could be developed to help improve the BER of the covert system.

In many systems utilizing OFDM, sub-channels are assigned to different end users. It would be beneficial to study the effect of the covert signal on the most adjacent sub-carriers to the covert signal as opposed to the entire OFDM signal. The effect on those sub-carriers is most probably greater than the sub-carriers that are at a greater distance in the spectrum. If the BER of the adjacent sub-carriers is increased significantly, it could lead to an unacceptable probability of detection for the covert signal thereby defeating the purpose.

Systems could also be developed to monitor and adjust for certain performance parameters of covert signal location in the spectrum, covert signal power, and bit rate. These could be three individual systems or a system that combines two or all of these parameters.

The systems studied here only took into consideration a covert signal utilizing BPSK. If the systems mentioned earlier were developed, thereby allowing the covert to improve its performance, other symbol constellations might be used. With a QPSK or higher bit per symbol constellation being employed, a higher data rate could be achieved while keeping the symbol power near that of a BPSK constellation for the same symbol rate. Using more bits per symbol can compensate for the lower symbol rate needed to achieve an acceptable BER.

Adaptive coding and modulation (ACM) are utilized by both LTE and WiMAX [19]. The communication systems utilizing LTE or WiMAX adjust the modulation type (QPSK, 16-QAM, and 64-QAM) and error control coding rate (e.g. 1/2, 1/3, etc.). In response to the changing channel conditions, ACM could enhance the ability of a covert signal to hide. Thus further study could focus on determining the system performance with AMC.

Now that the concept has been shown to be feasible, effort could be devoted to develop analytical performance models with increasing sophistication, starting with the basic scenarios studied here then moving on to models that capture the effects of channel dynamics and AMC.

References

[1] B. Walke, S. Mangold, L. Berlemann, *IEEE 802 Wireless Systems.* West Sussex: Wiley, 2006.

[2] E. Dahlman, S. Parkvall, J. Skold, P. Beming, *3G Evolution:HSPA and LTE for Mobile Broadband.* Oxford: Academic Press, 2007.

[3] J. Proakis, M. Salehi, *Digital Communications.* New York: McGraw-Hill, 2008.

[4] Leonard J. Cimini, Jr., "Analysis and Simulation of a Digital Mobile Channel Using Orthogonal Frequency Division Multiplexing," *IEEE Transactions on Communications,* vol. COM-33, pp. 665-675, July 1985.

[5] Irving Kalet, "The Mutitone Channel," *IEEE Transactions on Communications,* vol. 37, No. 2, pp. 119-124, February 1989.

[6] Irving Kalet, "Optimization of Linearly Equalized QAM," *IEEE Transactions on Communications,* vol. COM-35, No. 11, pp. 1234-1236, November 1987.

[7] S. Ye, R. Blum, L. J. Cimini, Jr., "Adaptive Modulation for Variable-Rate OFDM Sytems with Imperfect Channel State Information," *Vehicular Technology Conference,* vol. 2, pp. 767-771, May 2002.

[8] Y. H. Kim, H. G. Kim, I. Song, M. J. Lee, S. H. Yoon, "A Coded OFDM System for Time-Varying Multipath Rayleigh Fading Environment," *MILCOM 97 Proceedings,* vol. 2, pp. 867- 871, November 1997.

[9] C. W. Lee, G. J. Jeon, “An Efficient Adaptive Modulation Scheme for Wireless OFDM Systems,” *ETRI Journal,* vol. 29, no. 4, pp. 445-451, August 2007.

[10] C. E. Shannon, *“Communication in the Presence of Noise,”* Proceedings of the I.R.E., vol. 37, issue 1, pp. 10-21, January 1949

[11] S. Choney, *“Is 2010 the Year of Wireless Congestion?,”* web resource available at: http://www.msnbc.msn.com/id/34634571/ns/technology_and_science tech_and_gadgets/.

[12] I. Poole, *“What Exactly is LTE,”* Communications Engineer, pp. 46-47, June/July 2007.

[13] Moray Rumney, *"IMT-Advanced: 4G Wireless Takes Shape in an Olympic Year,"* Agilent Measurement Journal, September 2008.

[14] G. Blackwell, *“The Future of 4G:LTE vs. WiMAX,”* web resource available at: http://www.wi-fiplanet.com/news/article.php/3845111

[15] C. Krapichler, *“LTE, HSPA and Mobile WiMAX: A Comparison of Technical Performance,”* Hot Topics Forum: LTE vs WiMAX and Next Generation Internet, 2007 Institution of Engineering and Technology, pp. 1-31, September 2007.

[16] J. L. Holsinger, *“Digital Communications over Fixed-Time Continuous Channels with Memory, with Special Application to Telephone Channel,”* MIT Research

Lab of Electronics, Tech. Rep. 430, 1964.

[17] J. Davidson, *"LTE OFDM,OFDMA, and SC-FDMA,"* web resource available at: http://www.radio-electronics.com/info/cellulartelecomms/lte-long-term-evolution/lte-ofdm-ofdma-scfdma.php.

[18] F. Khan, *LTE for 4G Mobile Broadband.* Cambridge: Cambridge University Press, 2009.

[19] M. Ergen, *Mobile Broadband: Including WiMAX and LTE.* Berkley: Springer, 2009.

[20] D. McQueen, *"The Momentum Behind LTE Adoption,"* IEEE Communications Magazine, pp. 44-45, February 2009.

[21] E. Dahlman, S. Parkvall, D. Astley, A. Furuskar, Y. Jading, M. Lindstrom, *"LTE: The Evolution of Mobile Broadband,"* IEEE Communications Magazine, pp. 44-51, April 2009.

[22] L. Nuaymi, *WiMAX-Technology for Broadband Wireless Access.* West Sussex: John Wiley & Sons, 2007.

[23] IEEE Std. 802.16 - 2004, IEEE Standard for Local and metropolitan area networks, *"Part 16: Air Interface for Fixed Broadband Wireless Access Systems,"* 2004.

[24] W. Joseph, L. Martens, *"Performance Evaluation of Broadband Fixed Wireless System based on IEEE 802.16,"* Wireless Communications and Networking

Conference, vol. 2, pps. 978-983, April 2006.

[25] WiMAX Forum, *Mobile System Profile Specification,* Release 1.5 Common Part, August 2009.

[26] IEEE Std. 802.16 - 2009, IEEE Standard for Local and Metropolitan Area Networks, *"Part 16: Air Interface for Fixed Broadband Wireless Access Systems,"* 2009.

[27] J. Andrews, A. Ghosh, R. Muhamed, *Fundamentals of WiMAX: Understanding Broadband Wireless Networking.* Upper Saddle River: Prentice Hall, 2007.

[28] Carl Townsend, "Featured Whitepaper: Mobile WiMAX – The 4G Revolution Has Begun," web resource available: http://www.wimax.com.

[29] P. Lescuyer, T. Lucidarme, *Evolved Packet Sytem (EPS).* West Sussex: John Wiley and Sons, 2008.

[30] B. G. Lee, S. Choi, *Broadband Wireless Access and Local Networks: Mobile WiMAX and WiFi.* Norwood: Artech House, 2008.

[31] J. Lubacz, W. Mazurczyk, K. Szczypiorski, *"Voice Over IP",* IEEE Spectrum, pp. 42-47, March 2010.

[32] Xeno Phon, *"Many Questions About WiMAX,"* web resource available at: http://www.wimax360.com/forum/topic/show?id=610217%3ATopic%3A23718.

[33] M. Rice, *Digital Communications.* Upper Saddle River: Prentice Hall, 2009.

Appendix A

```
function RunOfdm(covert_on_off, NumOfdmSymbols, No, Tau, BiCov, CovRate)


% Load the design parameters
NoEst         = 1e-5; % This No is used to set Bi & Pi
DesiredPe     = 1e-4;
DesiredPecCov = 1e-4;



[c, d, f, g, N, Bi, Pi, Ci, Di, Fi, Gi, PiCov, IdxCov, BW, FiCov] =
DesignOfdm(NoEst, DesiredPe, DesiredPecCov, BiCov);

%PiCov = .001;

% Specify the simulation parameters
% An OFDM "symbol" is one long Tx over all N chan.
NumBitsPerSymbol = sum(Bi);
NumCovBitsPerSym = BiCov;

% Set up a cell array of QAM constellations with an average energy of unity!
Const{1} = UnitQamConstellation(1);
for ii=2:max(Bi)
    Const{ii} = UnitQamConstellation(ii);
end

% Necessary initializations
PAPR         = 0;
PiCv         = zeros(size(Fi));
XPand        = 8;
UpSample     = 1;
XAccum       = zeros(N*XPand*UpSample, 1);
RAccum       = zeros(N*XPand*UpSample, 1);
VAccum       = zeros(N*XPand*UpSample, 1);
WAccum       = zeros(N*XPand*UpSample, 1);
counter      = 0;
CovAccum     = 0;
CovBits      = (rand(1,NumCovBitsPerSym) > .5);

% Seed the random number generators with the current time
rand('state',sum(100*clock));
randn('state',sum(100*clock));

% Initialize the BER variables
TotalBerNum = 0;
TotalBerDen = 0;

% Initialize the covert BER variables
TotalBerNumCov = 0;
TotalBerDenCov = 0;

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% Loop on OFDM symbols
```

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

for kk=1:NumOfdmSymbols

    % Generate random information bits at the transmitter
    InputBits = (rand(1,NumBitsPerSymbol) > .5);

    % Generate random covert bits with a variable lower rate
    if counter >= CovRate
        counter = 1;
        CovBits = (rand(1,NumCovBitsPerSym) > .5);
    else
        counter = counter + 1;
    end;

    % Allocate an array of zeros for the QAM symbols
    X = zeros(N,1);
    V = zeros(N,1); % Covert Symbol

    % Loop through the subcarriers and initialize the QAM symbols
    FirstBitChan = 1;
    LastBitChan  = Bi(1);
    Bi           = [Bi;0];
    for ii=1:N
        % Convert each group of bits into a QAM symbol, taken from the
        % appropriate unit QAM constellation, and apply Pi
        if Bi(ii) > 1
            ThisConst    = Const{Bi(ii)};
            Xtemp        = (InputBits([FirstBitChan:1:LastBitChan]) *
2.^[0:1:Bi(ii)-1]') + 1;
            X(ii)        = sqrt(Pi(ii))*ThisConst(Xtemp);
            FirstBitChan = FirstBitChan + Bi(ii);
            LastBitChan  = LastBitChan  + Bi(ii+1);
        else
            FirstBitChan = FirstBitChan + Bi(ii);
            LastBitChan  = LastBitChan  + Bi(ii+1);
        end;
    end;
    Bi = Bi([1:1:N]);

    % Convert covert bits into QAM symbol and apply PiCov, and insert into the
    % covert frequency
    if (covert_on_off)
        ThisConst = Const{BiCov};
        Vtemp     = (CovBits * 2.^[0:1:BiCov-1]') + 1;
        V(IdxCov) = sqrt(PiCov)*ThisConst(Vtemp);
    else
    end;

    % Create the time-domain signal for non-covert and prepend the cyclic prefix
    x   = N*ifft(X);
    xCP = [x([(end-length(c)+2):1:end]);x];

    % Create the time-domain signal for covert and prepend the cyclic prefix
    if (covert_on_off)
        v   = N*ifft(V);
        if Tau < 1
```

```
            vCP   = [v([(end-length(c)+2):1:end]);v];
        else
            av  = v([(end+1-Tau):1:end]);
            bv  = v([(end-length(c)+2):1:end]);
            cv  = v([(1:1:(end-Tau))]);
            vCP = [av;bv;cv];
        end;
    else
        v  = 0;
    end;


    %%%%%%%%%%%%%%%%%%% This is where the transmitters end %%%%%%%%%%%%%%%%%%%%%

    %%%%%%%%%%%%%%%%%%% Non-covert channel + AWGN + Covert Signal %%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%
    if (covert_on_off)
        r = filter(c,1,xCP) + filter(d,1,vCP) +
sqrt(length(xCP)*No/2)*randn(length(xCP),2)*[1;j];
    else
        r = filter(c,1,xCP) + sqrt(length(xCP)*No/2)*randn(length(xCP),2)*[1;j];
    end;
    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

    %%%%%%%%%%%%%%%%%%% Covert channel + AWGN + Non-Covert Signal %%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%
    if (covert_on_off)
        w = filter(g,1,xCP) + filter(f,1,vCP) +
sqrt(length(xCP)*No/2)*randn(length(xCP),2)*[1;j];

    else
    end;
    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

    %%%%%%%%%%%%%%%%%%% This is where the receivers begin %%%%%%%%%%%%%%%%%%%%%%

    % Remove the cyclic prefix from non-covert
    r = r([length(c):1:end]);

    % Remove the cyclic prefix from covert
    if (covert_on_off)
        if Tau < 1
            w = w([length(c):1:end]);
        else
            w = [w([(Tau+length(c)):1:end]);w([1:1:Tau])];
        end;
    else
    end;

    % Transform to frequency domain using FFT
    R = fft(r)/N;
    if (covert_on_off)
        W = fft(w)/N;
    else
    end;

    % "Equalize" the received signal.  In other words, correct the
    % amplitude and phase of each subchannel
    REq        = R./Ci;
    REq        = REq./sqrt(Pi);

    % "Equalize" the received covert signal
    if (covert_on_off)
        WEq        = W./Fi;
        WEq        = WEq./sqrt(PiCov);
    else
    end;

    % Allocate an array of RxBits
    RxBits = zeros(size(InputBits));

    % Loop through the subcarriers and detect the QAM symbols
    FirstBitChan = 1;
    LastBitChan  = Bi(1);
    Bi           = [Bi;0];
    for ii=1:N
        % Convert each QAM symbol into a group of bits, taken from the
        % appropriate unit QAM constellation
        if Bi(ii) > 1
            ThisConst                            = Const{Bi(ii)};
            [Dist, Index]                        = min(abs(ThisConst - REq(ii)));
            RxBits([FirstBitChan:1:LastBitChan]) = dec2binvec(Index-1,Bi(ii));
            FirstBitChan                         = FirstBitChan + Bi(ii);
            LastBitChan                          = LastBitChan  + Bi(ii+1);
        else
            FirstBitChan                         = FirstBitChan + Bi(ii);
            LastBitChan                          = LastBitChan  + Bi(ii+1);
        end;
    end;
    Bi = Bi([1:1:N]);

    % Convert the covert QAM symbol into a group of bits, taken from the
appropriate
    % unit QAM constellation
    if (covert_on_off)
        if counter >= CovRate
            CovAccum               = (WEq(IdxCov) + CovAccum)/CovRate;
            ThisConst              = Const{BiCov};
            [Dist, Index]          = min(abs(ThisConst - CovAccum));
            RxBitsCov([1:1:BiCov]) = dec2binvec(Index-1,BiCov);
            CovAccum               = 0;
            % Compute the covert BER
            TotalBerNumCov = TotalBerNumCov + sum(CovBits ~= RxBitsCov);
            TotalBerDenCov = TotalBerDenCov + NumCovBitsPerSym;
        else
            CovAccum = WEq(IdxCov) + CovAccum;
        end;
    else
    end;

    % Compute the BER
    TotalBerNum = TotalBerNum + sum(InputBits ~= RxBits);
    TotalBerDen = TotalBerDen + NumBitsPerSymbol;
    % Compute PAPR
    CurPapr = 10*log10(max(abs(x).^2)/mean(abs(x).^2));
    if CurPapr > PAPR
        PAPR = CurPapr;
    else
    end;

    % Print some status to the screen; PAPR, etc.
    if (covert_on_off)
        fprintf(1, ...
            'OFDM Symbol %i of %i\n Running BER = %i/%i = %e\n Running CovBER = %i/
%i = %e\n PAPR = %i dB\n', ...
            kk, NumOfdmSymbols, TotalBerNum, TotalBerDen, TotalBerNum/TotalBerDen,
...
            TotalBerNumCov, TotalBerDenCov, TotalBerNumCov/TotalBerDenCov, PAPR);
    else
        fprintf(1, ...
            'OFDM Symbol %i of %i\n Running BER = %i/%i = %e\n PAPR = %i dB\n', ...
            kk, NumOfdmSymbols, TotalBerNum, TotalBerDen, TotalBerNum/TotalBerDen,
PAPR);
    end;

    % Use FftPadExpand() to compute the spectrum of x, r, v, w and
    % accumulate the magnitude-squared of these over time.
    [Xout,F1]  = FftPadExpand(x, XPand, UpSample);
    XAccum     = XAccum + abs(Xout).^2;

    [Rout,F2]  = FftPadExpand(r, XPand, UpSample);
    RAccum     = RAccum + abs(Rout).^2;

    if (covert_on_off)

        [Vout,F3]  = FftPadExpand(v, XPand, UpSample);
        VAccum     = VAccum + abs(Vout).^2;

        [Wout,F4]  = FftPadExpand(w, XPand, UpSample);
        WAccum     = WAccum + abs(Wout).^2;

    else
    end;

end;
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

% SNR calculation
SNR = pow2db(sum(Pi.*abs(Ci).^2/No)/length(Pi));
fprintf(1,'SNR = %f db\n',SNR);

% Eb/No calculation
EbNo = pow2db(sum(Pi)/(sum(Bi)*No));
fprintf(1,'Eb/No = %f db\n',EbNo);

% Covert Eb/No
if (covert_on_off)
    EbNoCov = pow2db((PiCov*FiCov)/(BiCov*No));
    fprintf(1,'Eb/No Covert = %f db\n',EbNoCov);
```

```
end;

% Covert vs. non-covert Eb/Eb
if (covert_on_off)
    CovNCov = pow2db((PiCov/BiCov)/(sum(Pi)/(sum(Bi))));
    fprintf(1,'Covert to Non-Covert Eb Ratio = %f db\n',CovNCov);
end;

% Print channel capacities
fprintf(1,'BW = %i MHz\n',BW/1e6);
fprintf(1, ...
    'Non-covert channel capacity = %i Mbps\nCovert channel capacity = %f kbps\n',
...
    (N/(N+length(c)-1))*(sum(Bi)*BW/(N*2e6)), (N/(N+length(c)-1))*BiCov*BW/
(2e3*N*CovRate));

% Plot the average PSDs computed inside the loop.
XAccumAv = 10*log10(XAccum./NumOfdmSymbols);

figure(6);clf;
plot(F1*15/1000,XAccumAv);
title('Non-Covert Transmitted Signal Average PSD')
ylabel('dB');
xlabel('Frequency (MHz)');
grid on;

RAccumAv = 10*log10(RAccum./NumOfdmSymbols);

figure(7);clf;
plot(F2*15/1000,RAccumAv);
title('Signal Average PSD at Non-Covert Receiver')
ylabel('dB');
xlabel('Frequency (MHz)');
grid on;

if (covert_on_off)
    VAccumAv = 10*log10(VAccum./NumOfdmSymbols);

    figure(8);clf;
    plot(F3*15/1000,VAccumAv);
    title('Covert Transmitted Signal Average PSD')
    ylabel('dB');
    xlabel('Frequency (MHz)');
    grid on;

    WAccumAv = 10*log10(WAccum./NumOfdmSymbols);

    figure(9);clf;
    plot(F4*15/1000,WAccumAv);
    title('Signal Average PSD at Covert Receiver')
    ylabel('dB');
    xlabel('Frequency (MHz)');
    grid on;
else
end;
```

```
function [c, d, f, g, N, Bi, Pi, Ci, Di, Fi, Gi, PiCov, IdxCov, BW, FiCov] =
DesignOfdm(No, DesiredPe, DesiredPecCov, BiCov)

IsiMagnitude = 0.2;
IsiDuration  = 6;

% Specify the channel
if(0)
    % Specify channel from non-covert transmitter to non-covert reciever
    c = [1;IsiMagnitude*exp(j*2*pi*rand(IsiDuration+1,1))];
    % Specify channel from covert transmitter to non-covert reciever
    d = [1;IsiMagnitude*exp(j*2*pi*rand(IsiDuration+1,1))];
    % Specify channel from covert transmitter to covert reciever
    f = [1;IsiMagnitude*exp(j*2*pi*rand(IsiDuration+1,1))];
    % Specify channel from non-covert transmitter to covert reciever
    g = [1;IsiMagnitude*exp(j*2*pi*rand(IsiDuration+1,1))];
else
    % Follow this branch to load the existing channels
    load c
    load d
    load f
    load g
end

% Specify the design parameters
N          = 512;       % Number of subcarriers
Ptotal     = 1;         % Total power available for allocation to the subcarriers

% Normalize the channels to have unit energy
c = c/(sqrt(abs(c'*c)));

d = d/(sqrt(abs(d'*d)));

f = f/(sqrt(abs(f'*f)));

g = g/(sqrt(abs(g'*g)));

% Compute the frequency and phase response of the channels & plot
%figure(1);clf;
%freqz(c);
%title('Non-Covert Channel')

[Ci,omega] = freqz(c,1,N,'whole');

%figure(2);clf;
%freqz(d);
%title('Covert Transmitter to Non-Covert Receiver Channel')

[Di,omega_d] = freqz(d,1,N,'whole');
```

```
%figure(3);clf;
%freqz(f);
%title('Covert Channel')

[Fi,omega_f] = freqz(f,1,N,'whole');

%figure(4);clf;
%freqz(g);
%title('Non-Covert Transmitter to Covert Receiver Channel')

[Gi,omega_g] = freqz(g,1,N,'whole');

% Allocate bits and power to the N subchannels
[Bi,Pi,PiCov,IdxCov,BW,FiCov]= BitAndPowerAllocation(DesiredPe, DesiredPecCov,
Ptotal,abs(Ci).^2/No, Fi, No, BiCov);

% Plot of bit and power allocations
figure(5);clf;
subplot(2,1,1)
plot([-256:1:255],Bi,'.');
title('Bit And Power Allocation')
ylabel('Bi');
xlabel({'Channel No.';'(a)'});
subplot(2,1,2)
plot([-256:1:255],Pi);
ylabel('Pi');
xlabel({'Channel No.';'(b)'});
```

```
function [Bi,Pi,PiCov,IdxCov,BW,FiCov]=BitAndPowerAllocation(DesiredPe,
DesiredPecCov, Ptotal, Ci2No, Fi, No, BiCov)

% Channel bandwidth (Hz)
BW = 7.68e6;

save('Ci2No')

% The length of CNo tells us the number of subchannels.
N = length(Ci2No);

% Initialize Bi and Pi to zero.
Bi = zeros(size(Ci2No));
Pi = zeros(size(Ci2No));

% Power per channel, equally divided
PTemp  = Ptotal/N;

% Calculate Pe assuming equal power distribution and M=4

Ci2No([1:105])   = 1e-4; % Left guard band
Ci2No([407:512]) = 1e-4; % Right guard band
```

```
PeTemp = zeros(size(Ci2No));


% Find channels that can support at least 4-QAM
for k = 1:1:N
    PeTemp(k) = 4*qfunc(sqrt(3*PTemp*Ci2No(k)/3));
end;
IdxRemaining      = find(PeTemp < DesiredPe);

% Select the covert channel
IdxCov = 107;   % Edge
%IdxCov = 146;  % Inner

% Adjust Pi for the covert channel, 4-QAM for the covert channel
Fi2NoCov  = abs(Fi(IdxCov))^2/No;
FiCov     = abs(Fi(IdxCov))^2;
PeCov     = 1e-5; % Probability of covert symbol error
PiTempCov = .1;

if BiCov > 1 % For QAM
    while (PeCov < DesiredPecCov)
        PiTempCov = PiTempCov - .00001;
        PeCov     = 4*qfunc(sqrt(3*PiTempCov*Fi2NoCov/((2^BiCov)-1)));
    end;
else         % For BPSK
    while (PeCov < DesiredPecCov)
        PiTempCov = PiTempCov - .00001;
        PeCov     = qfunc(sqrt(2*PiTempCov*Fi2NoCov));
    end;
end;
PiCov = PiTempCov + .00001;

% Next, we will run through the entries in IdxRemaining one-by-one, starting
% with the one with the largest Ci2No.  Each time through the loop we will:
%    * Allocate the remaining power evenly over the remaining subchannels
%    * Identify the remaining subchannel with the largest Ci2No
%    * Compute (unquantized) Mi that satisfies the Pe equation
%    * Quantize Mi to correspond to an integer number of bits
%    * Adjust Pi to satisfy the Pe equation
%--At this point Mi and Pi have been determined for the subchannel of interest--
%    * Move this index from the IdxRemaining set to the IdxAllocated set
%    * End of loop
IdxAllocated = [];

while(length(IdxRemaining) > 0)

    % Print a status message to the screen
    fprintf(1,'Subchannels remaining = %i\n',length(IdxRemaining));

    % Allocate the remaining power evenly over the remaining subchannels
    PRemain = Ptotal/length(IdxRemaining);

    % Identify the remaining subchannel with the largest Ci2No
    [Ci2NoHighest,IdxHighestCi2No] = max(Ci2No);

    % Compute (unquantized) Mi that satisfies the Pe equation
    m  = 0;
    Mi = 4;
    Pe = 0;
    while (Pe < DesiredPe)
        Pe = 4*qfunc(sqrt(3*PRemain*Ci2NoHighest/(3+m)));
        m = m + .0625;
        Mi = 4 + m;
    end;
    Mi = Mi - .0625;

    % Quantize Mi to correspond to an integer number of bits
    BiTemp = log2(Mi);
    if BiTemp < 3
        Bi(IdxHighestCi2No) = 2;
    elseif BiTemp > 3 && BiTemp < 5
        Bi(IdxHighestCi2No) = 4;
    else
        Bi(IdxHighestCi2No) = 6;
    end;

    % Adjust Pi to satisfy the Pe equation
    Pe     = 0;
    PiTemp = .01;
    while (Pe < DesiredPe)
        PiTemp = PiTemp - .0001;
        Pe     = 4*qfunc(sqrt(3*PiTemp*Ci2NoHighest/((2^Bi(IdxHighestCi2No))-1)));
    end;
    Pi(IdxHighestCi2No) = PiTemp + .0001;
    Ptotal              = Ptotal - Pi(IdxHighestCi2No);

    % Move IdxHighestCi2No from the IdxRemaining set to the IdxAllocated set
    IdxRemaining           = setxor(IdxRemaining, IdxHighestCi2No);
    IdxAllocated           = setxor(IdxAllocated, IdxHighestCi2No);
    Ci2No(IdxHighestCi2No) = 0;
end;
```

```
function [X,F] = FftPadExpand(x, PadFactor, ExpandFactor)

% Save the length of x as it is at the beginning
N    = length(x);

% Zero-pad x by the PadFactor.  If PadFactor = 4 and the length of x is N,
% then the zero-padded version will have one copy of x followed by three
% sections of zeros of length N (a total of 3*N zeros), so that the zero-padded
% version of x has a total length of 4*N.
xPad = [x;zeros((PadFactor-1)*N,1)];

% Increase the sample rate of x by the ExpandFactor.
xPadExp = resample(xPad,ExpandFactor,1);
```

```matlab
% Take the FFT of the zero-padded upsampled version of x
X = fft(xPadExp);

% Adjust the x-axis
F = [-N/2*PadFactor*ExpandFactor:N/2*PadFactor*ExpandFactor-1]'/PadFactor;
```

```matlab
function C = UnitQamConstellation(Bi)


% Check for the trivial cases of less than 1 bit (erroneous input) or 1 bit (the
% BPSK case).  All others should be OK with our main section of code.
if(Bi < 1)
    C = [];
    return;
elseif(Bi == 1)
    C = [-1;+1];
    return;
end


% When Bi is even, then M has the following properties:
%   * it has an integer square root
%   * the square root is an even number
% When Bi is odd, we want to round its square root up to the next even number,
% in order to find the smallest even-sided square that will hold our points.
EvenSquareRoot = ceil(sqrt(2^Bi)/2)*2;


% We need a PAM-type alphabet based on this even square root
PamM = EvenSquareRoot;

% Now, make the square QAM constellation using the basic PAM order:
%   * Start with the basic M-ary PAM constellation
%   * Make an M-by-M matrix where each row is the basic M-ary PAM constellation
%   * Make a copy of the M-by-M matrix, and then transpose the copy
%   * Multiply the first matrix by 1, and the second matrix by j, then add
PamConstellation = -(PamM-1):2:+(PamM-1);
SquareMatrix     = ones(PamM,1)*PamConstellation;
C                = SquareMatrix + j*SquareMatrix';
C     = C(:);
EavgC = sum(abs(C).^2) / length(C);
C     = C / sqrt(EavgC);

% If Bi is even, then we're done.  If Bi is odd, then we are dealing with a
% "cross" constellation, and we have to keep only the M points that are closest
% to the origin
if(mod(Bi,2) == 1)
    % There will be a few "ties" when we sort by minimum distance, so MATLAB
    % will use some sort of "tiebreaker."  Therefore, we will just grab the
    % constellation points in the first quadrant.  Then, we will replicate the
    % first quadrant 4 times.  This way we end up with a constellation that is
    % symmetric looking.
    FirstQuadrant = find( (real(C) > 0) & (imag(C) > 0) );
    C = C(FirstQuadrant);
    d = abs(C);
    [dSort,ISort] = sort(d);
    C = C(ISort(1:2^Bi/4));

    % Replicate the first quadrant 4 times
    C = [real(C) + j*imag(C);
         real(C) - j*imag(C);
        -real(C) + j*imag(C);
        -real(C) - j*imag(C);];
    EavgC = sum(abs(C).^2) / length(C);
    C     = C / sqrt(EavgC);
end
```