Exploiting OFDM Systems for Covert Communication

Zaid Hijaz

Information and Telecommunication Technology Center
Department of Electrical Engineering and Computer Science
University of Kansas
Lawrence, KS, USA
zhijaz@ku.edu

Victor S. Frost

Information and Telecommunication Technology Center
Department of Electrical Engineering and Computer Science
University of Kansas
Lawrence, KS, USA
frost@ittc.ku.edu

Abstract—Both Long Term Evolution (LTE) and WiMAX (802.16) 4th generation wireless systems (4G) utilize orthogonal frequency division multiplexing (OFDM) on the down-link. The advantages of OFDM over other wireless communication techniques are well known. These technologies will become more ubiquitous as time goes on. Here a study is presented of the potential for covert communication within an OFDM waveform. Most OFDM standards call for unused sub-channels for channel spacing, synchronization of transmitter and receiver and to mitigate poor channel response. Here we study the effects of 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 analyze its influence on the target OFDM signal as well as determining the communications capabilities of the covert link. The covert signal inserted in an unused sub-carrier locations or frequency "slot", is no longer orthogonal to the target OFDM waveform. Thus, there is potential for the covert signal to impact the target link. Here we examine the effect of the covert signal on the target OFDM system as a function of the location of the covert signal, its power, and bit rate. The communications capability of the covert link is also studied. The amount of information that can be transmitted covertly with minimal impact on the target OFDM user (i.e., relatively low probability of detection) is also presented.

I. Introduction

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. It is common in OFDM systems for sub-channels (frequency slots) to go unused to accommodate required channel spacing, synchronization of transmitter and receiver and to mitigate poor channel response. The premise of this work is that by using these empty slots for concealed communication the target OFDM signal can provide a "cover" for the covert system. With the increased deployment of OFDM in 4G systems there is the potential for this type of exploitation.

Here we demonstrate that such exploitation is possible by showing that the covert communication is possible while not appreciably impacting the target OFDM system. In this work a simulation model for covert communication embedded in an OFDM waveform was constructed and used to characterize a BER performance of LTE/WiMAX type OFDM signal in the presence of a covert signal with varying bit rate, power, and spectral location and describe the performance and limitations of the covert communications systems in the presence of an OFDM signal.

II. System Assumptions

The basic assumption behind the proposed concept for hidden communications is that there are unused slots available for the covert system to use. On the OFDM down-link channels, both LTE [3] and WiMax [3] standards specifies such slots. However, frequency slots within the OFDM spectrum are also not used in order to deal with channel conditions; the selection of these slots is determined by bit and power resource allocation algorithms. Placing the covert signal in one of the slots among the actively modulated sub-carriers will enhance its LPD, therefore one such resource allocation algorithm [1] is reviewed next.

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 [1] 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). The algorithm used for allocating bits and power assumes a linear time-invariant channel with AWGN. Each of the N sub-carriers will be using QAM ($M_i = 2^{B_i}$). Where M_i is the constellation size and B_i is the number of bits transmitted on the ith sub-carrier in a frame interval of T seconds. The bit rate of the OFDM signal is expressed in (1). The power allocated to the ith sub-carrier with respect to the average available power at the transmitter is given in (2).

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

$$P_{total} = \sum_{i=1}^{N} P_i \quad (2)$$

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 4-QAM ($M_i = 4$, $B_i = 2$). We start by dividing the total available power (P) equally amongst all the sub-carriers. Those that result in a probability of symbol error greater than our desired symbol error probability (SER) will not be used for transmission. We then allocate the total power amongst the remaining sub-carriers and compute M_i for the highest SNR channel based upon our desired probability of symbol error (SER). 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 [1]. Figure 1a shows the bit allocation for the non-covert OFDM channel and Figure 1b shows the power allocation for the non-covert OFDM channel. Note the sub-channels around slot -105 are not used.
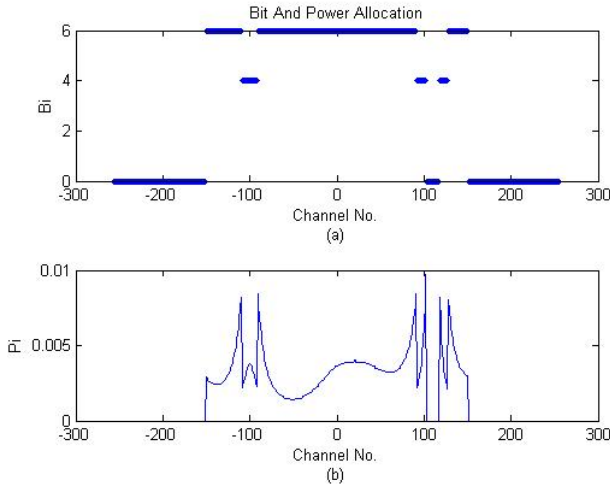

Figure 1: Bit and Power Allocation for 5 MHz OFDM Channel

The next assumption 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 as shown in Figure 2. 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. The cross channels will be unknown at each receiver. The non-covert transmitter (NCTx) and non-covert receiver (NCRx) will have

known CSI regarding the channel they will be utilizing. Note that channel estimation can be done effectively [4]. The four channel's magnitude and phase response will be held constant throughout this experiment. In reality, we know that wireless channel characteristics vary with time and location for mobile channels; however keeping the channels fixed eliminates one source of variation for this initial feasibility study; consideration of time varying channel can be considered later. Here we used fixed representative channels. These channels all differ in their magnitude and phase characteristics as they would in practice. These representative channels were generated at random. We compared the system performance of the representative channel to that obtained with several other randomly selected channel realizations and found there was little difference in system performance. The signal at the input to the non-covert receiver is given by (3). The equation shows the ith channel magnitude on the kth sub-carrier ($C_k^{(i)}$) and phase (ϕ_k) response. Equation (3) also shows the point in the symbol constellation chosen to represent the in-phase and quadrature components for the non-covert (A_{kc} and A_{ks}) as well as the covert (B_{kc} and B_{ks}), and the sub-carrier base-band frequency (f_k). The covert only transmits on the vth sub-carrier.
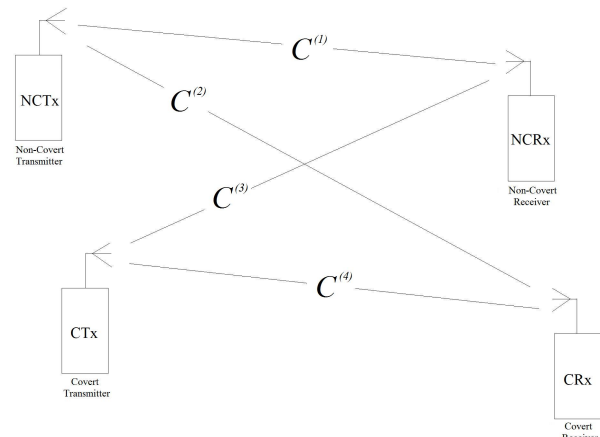

Figure 2: Transmitter/Receiver Pairs.

$$r(t) = \left(\sum_{k=0}^{N-1} \sqrt{\frac{2}{T}} \left| C_k^{(1)} \right| A_{kc} \cos(2\pi f_k t + \phi_k^{(1)}) + \right.$$
$$\left. \sqrt{\frac{2}{T}} \left| C_k^{(1)} \right| A_{ks} \sin(2\pi f_k t + \phi_k^{(1)}) \right) +$$
$$\left(\sum_{i=0}^{N-1} \sqrt{\frac{2}{T}} \left| C_i^{(3)} \right| B_{ic} \cos(2\pi f_i t + \phi_i^{(2)}) + \right.$$
$$\left. \sqrt{\frac{2}{T}} \left| C_i^{(3)} \right| B_{is} \sin(2\pi f_i t + \phi_i^{(2)}) \right) + n(t) \quad (3)$$

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

We assume that the covert communications system knows the sub-channels that are not used by the non-covert target

system. That is, we assume that the covert system has knowledge of Figure 1a through channel scanning and estimation [15].

Ideal phase and frequency recovery of the signals is assumed. This assumption is also similar to the above, 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 [4]. However we assume that the non-covert OFDM and covert systems are not in sync. Thus the covert signal is not orthogonal to the non-covert OFDM signal. This results in a synchronization offset, τ, between the two signals causing performance degradations which will be quantified later.

While both LTE [3] and WiMax [3] standards specify the use of adaptive modulation and coding (AMC), the system under consideration here uses fixed modulation (after the execution of the resource allocation algorithm) and no forward error correcting coding. AMC as well as other higher layer considerations like hybrid ARQ [14] can be can be considered after the feasibility of the basic concept is proven.

III. SYSTEM PARAMETERS

This section describes the system parameters used in the study. Table 1 gives target non-covert OFDM system parameters.

Modulation	QPSK, 16-QAM, 64-QAM
RF Bandwidth	5MHz
Subcarrier spacing	15 KHz
Number of subcarriers	512 (512 FFT)
Cyclic Prefix	6 samples/symbol
Number of samples/symbol + CP	518
Symbol Time	13.5 (msec)
Number of modulated subcarriers	301
Normalized Power	1 Watt
Target SER	10^{-4}

Table 1: Target Non-covert OFDM System Parameters

Note that the location of each sub-carrier can be described by an integer index, k, where the k=0 is at the carrier frequency, f_c, e.g, 750 MHz for some proposed LTE deployments. Then given these parameters to the OFDM signal, the sub-carriers range from k= -256…. +256 with sub-carriers -150…150 modulated while subcarriers -256 to -151 and 151 to 256 are unused. For example, k = -152 corresponds to a sub-carrier at f_c -2.2725 MHz. The channel noise power is N_o=0.0002 W/Hz. The channel realizations used here are shown in Figures 3,4,5, and 6.

The covert communications system uses BPSK and mimics an OFDM signal by also being constructed using a 512 point IFFT and then selecting only one sub-carrier. A 6 samples/symbol cyclic prefix was also used. The premise is that the covert signal thus will exhibit the same properties as the non-covert OFDM system. Also this approach simplified the construction of the simulation model. The parameters of the covert communications system were varied as part of this study. The covert system is specified in terms of its bit rate-$R_{b-covert}$, spectral location-k, relative power-$E_{b,covert}/E_{b,non-covert}$ dB, and synchronous offset-τ.
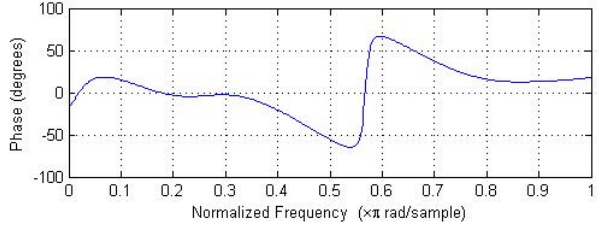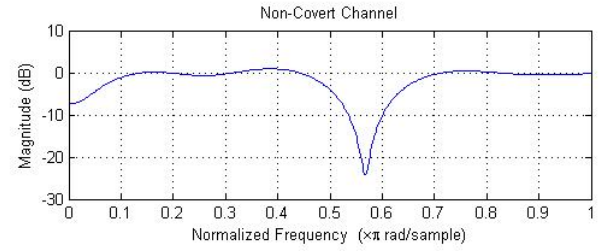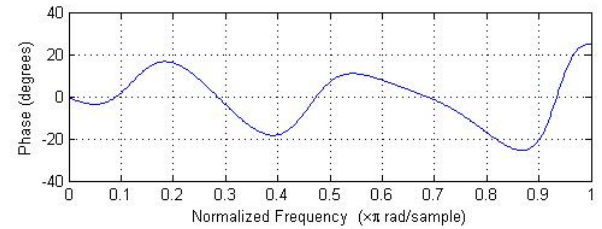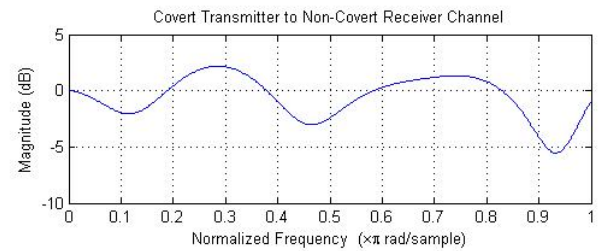

Figure 3: Non-Covert Channel ($C^{(1)}$)

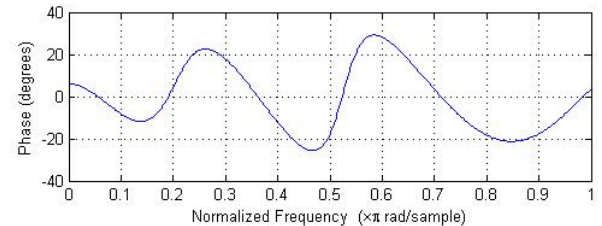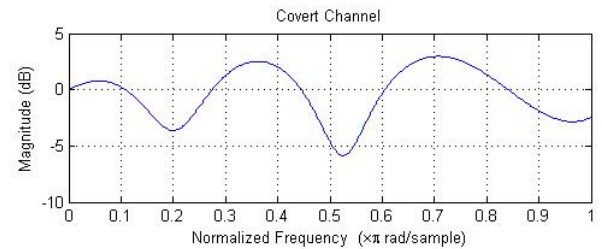Figure 4: Covert to Non-Covert Channel ($C^{(3)}$)
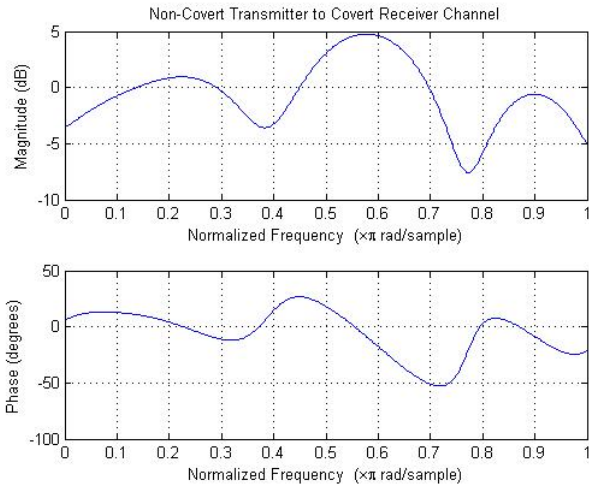

Figure 5: Covert Channel ($C^{(4)}$)

Figure 6: Non-Covert to Covert Channel ($C^{(2)}$)

IV. Covert Effect on Non-Covert for Increasing Noise

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 signal. Here sub-channel (k= -152) next to those utilized by the non-covert signal was chosen. It can be seen in Figure 7 that the presence of the covert signal has little effect on the target non-covert system this case.
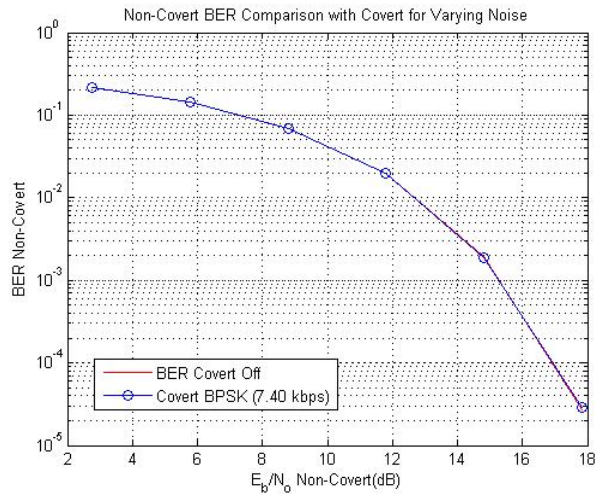

Figure 7: Comparison of BER Curve With and Without Covert ($R_{b,covert}$ = 7.40 kbps, Channel = -152 $E_{b,covert}/E_{b,non-covert}$ = -10.83 dB, τ = 128 samples/symbol)

V. Effect of Increasing Covert Power on Non-Covert OFDM Signal

For the next set of experiments, the covert signal power was increased and the effect on the non-covert OFDM signal

BER recorded. We increase the power of the covert thereafter from 5 x 10^-5, .0001, .001, .01, .1, 1, 5, 25, 100, and 250 Watts respectively.

Figure 8 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 comparable 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.
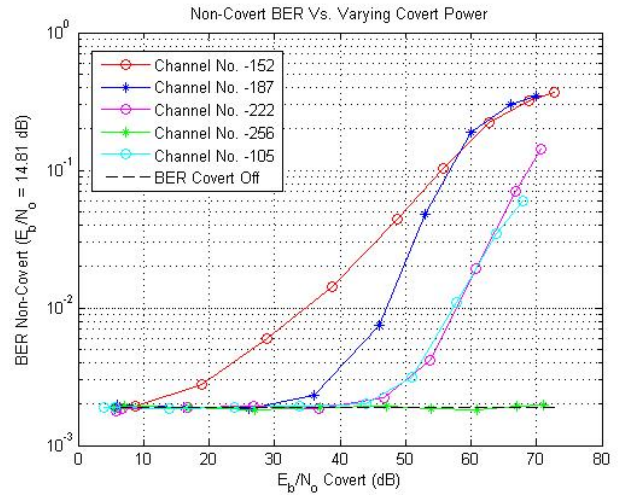

Figure 8: E_b/N_o Covert vs. BER Non-Covert ($R_{b,covert}$ = 7.40 kbps, , τ= 128 samples/symbol)

VI. Effect of Synchronous Offset on Non-Covert Signal

Another of the variables that must be examined is the synchronous offset between the two signals, τ. The OFDM signal sub-carriers are orthogonal to one-another. However, the non-covert will only achieve this orthogonality if its 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 may not be possible to achieve in practice.

In this section, we examine the effect synchronous offset in terms of the samples per symbol. When the covert signal is offset, it loses its orthogonality with respect to the other OFDM sub-carriers thereby resulting in interference. Figures 5 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 were held constant throughout this part of the study. Note Figure 1 shows that a set of sub-carriers around k = -105 inside the used spectrum of the target OFDM signal are unused. It was also verified that the synchronous offset between the covert and non-covert signals has little effect on the non-covert BER for a covert signal in the middle of the unused OFDM spectrum. This result also demonstrated that

the covert communication signal does not impact the target non-covert system even when the covert signal is embedded inside the modulated OFDM spectrum.

VII. Effect of Spectral Position on Covert Signal

Next we examine the communications capability of the covert system. 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 (k= -256 @ f_c = -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 @ f_c = -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 ($C^{(4)}$ in Figure 2) of the sub-channels varying. A synchronous offset of 128 symbols/second was used. We will see in later sections why this synchronous offset was chosen. For this study, the rate of the covert transmitter was also varied from 1.85 to 7.40 kb/s. Note 7.40 kb/s is the maximum rate of the covert system for the scenario studied was the maximum allowed by the bandwidth of the 15 KHz sub-channel. The rate was then lowered in order to achieve an improved BER for the covert communications system. In Figure 9, 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.

We can see that it is difficult to achieve an acceptable BER (10e-3) with the full rate for this scenario. 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 signal increases, the BER of the covert system 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 signal is from the non-covert signal while the detectability of the covert communications increases.

VIII. Effect of Synchronous Offset on Covert

Next we examine the effect the synchronous offset has on the covert BER. 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 (τ) is equal to n.

For Figure 11, we placed the covert in sub-channel number k = -105. From Figure 1, we can see that 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

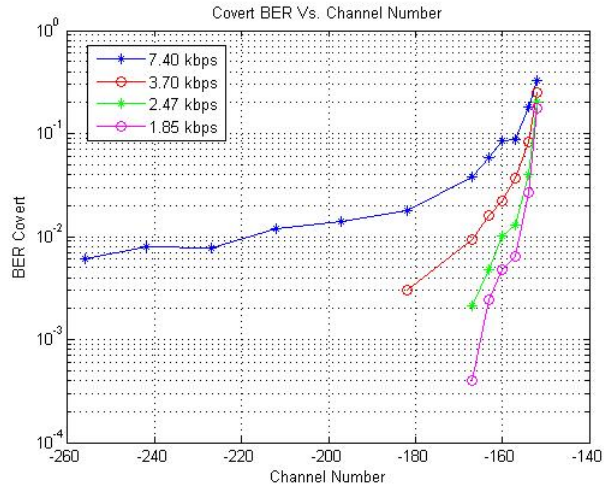the same reason of poor channel quality, thereby giving the covert signal good spacing.

Figure 9: Channel Number vs. Covert System BER

It can be seen from Figures 10 and 11 that the BER of the covert improves as the rate decreases, as expected. For no synchronous offset, all rates perform well; however, this is may not be achievable in practice. Any synchronous offset causes the BER to increase significantly. When the bit rate was lowered to 462 b/s a BER of 10^{-4} or less was achieved for channels -105 and -154 for all synchronous offsets. These results demonstrate that the covert communication signal can be effectively hidden next to an OFDM signal as in Figures 12a, b, & c. The expanded PSD in figures 12b and 12c show the average PSD around channel k = -154. This demonstrates the difficulty in detection of the covert signal.
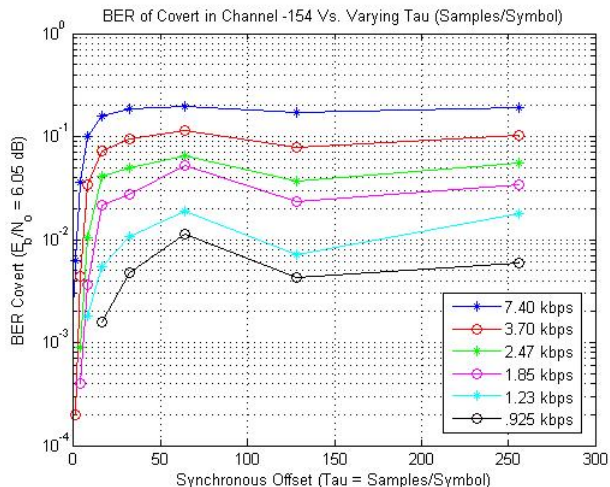

Figure 10: Cover BER Vs. Synchronous Offset for Sub-Channel -154
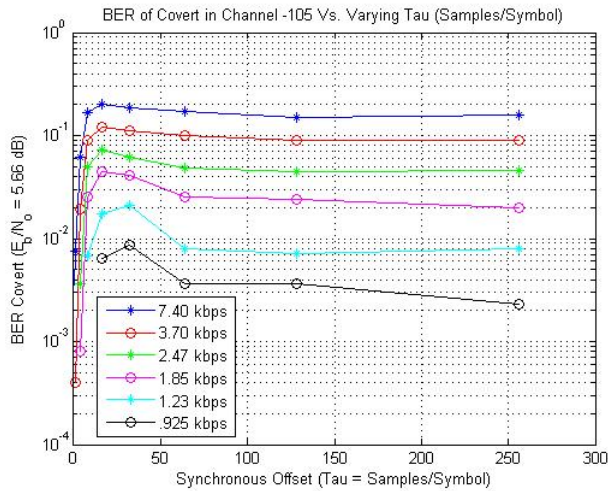($E_{b,covert}/E_{b,non-covert}$ = -8.76 dB)

Figure 11: Cover BER Vs. Synchronous Offset for Sub-Channel -105
($E_{b,covert}/E_{b,non-covert}$ = -9.15 dB)

IX. CONCLUSION

Widespread deployment of wireless 4G systems using OFDM is expected. Here a method of covert communication has been proposed that takes advantage of the OFDM spectral structure. 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 signal. Here we have demonstrated the potential and feasibility of this concept.
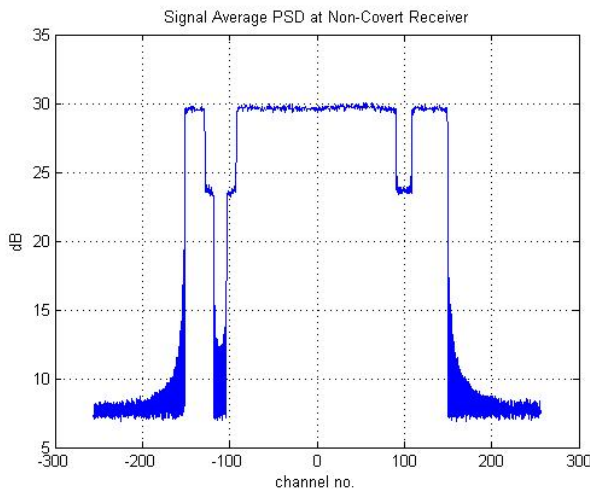

Figure 12a: PSD at Non-Covert Receiver
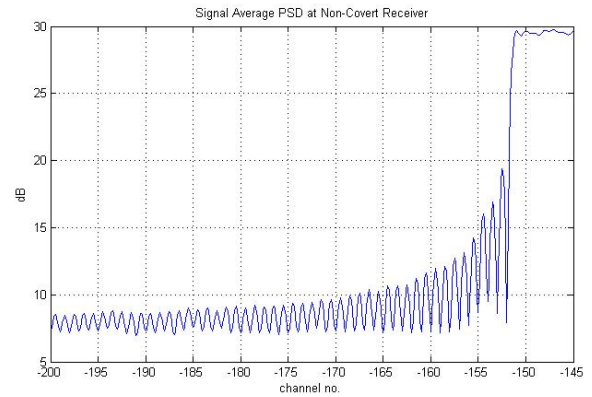($R_{b,covert}$ = 7.40 kbps, Channel = -154, $E_{b,covert}/E_{b,non-covert}$ = -10.83 dB, τ = 128 samples/symbol)

Figure 12b: Expanded PSD at Non-Covert Receiver with Covert Active
($R_{b,covert}$ = 7.40 kbps, Channel = -154, $E_{b,covert}/E_{b,non-covert}$ = -10.83 dB, τ = 128 samples/symbol)
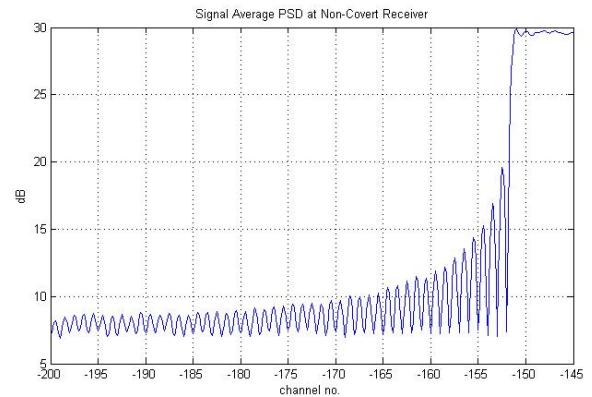

Figure 12c: Expanded PSD at Non-Covert Receiver, with Covert Signal Not Active

For this study a 5 MHz LTE like waveform specification was chosen. This waveform has 512 sub-carriers and a sub-channel bandwidth of 15 KHz [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 $E_{b,covert}/E_{b,non-covert}$ less than -7 dB. The covert synchronous offset and location within the non-utilized base-band spectrum of the non-covert signal has little effect on the BER of the non-covert system. 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 (e.g., $< 10^{-3}$), 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 7 and 8, 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 signal remaining high in those channels. For covert signals utilizing unused channels by the non-covert signal due to poor channel ($C^{(1)}$) quality 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. Therefore it is feasible for the covert communications system to operate within a OFDM signal.

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 signal, 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 results in higher covert signal power. Higher covert signal power will cause the covert to become more easily detected. Thus conditions exist that will allow the covert to operate with an acceptable BER and low probability of detection regardless of the symbol synchronous offset.

This study demonstrated the potential of exploiting OFDM systems for covert communications. Future work focusing on the synchronous offset between the two signals along with the phase and frequency recovery of the signals could be very beneficial in providing a basis for covert system improvement in terms of BER and LPD by developing a system that monitors and adjusts parameters of the covert signal. In this study, we examined the effects of the covert signal on the non-covert system. A study on the effects of the covert on the sub-carriers most adjacent to the covert could also be of benefit. A study could also be completed utilizing adaptive coding and modulation for the covert system in this study.

REFERENCES

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

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

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

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

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

[6] 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.

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

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

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

[10] 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.

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

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

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

[14] Dimitri Bertsekas and Robert Gallager, *Data Networks.* Prentice-Hall, Inc. Upper Saddle River, NJ, USA, 1992.

[15] R. Rouil, N. Golmie, "Adaptive Channel Scanning for IEEE 802.16e," IEEE Military Communication Conference (MILCOM), USA, 2006.