Security Issues for Modern Communications Systems: Fundamental Electronic Warfare Tactics for 4G Systems and Beyond

Matthew Jonathan La Pan

Dissertation submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
in
Electrical Engineering

T. Charles Clancy, Chair
Robert W. McGwier
Jeff Reed
Sandeep Shukla
Kathleen Hancock

October 27, 2014
Blacksburg, Virginia

Keywords: Communications, Jamming, Cognitive Radio

Security Issues for Modern Communications Systems: Fundamental Electronic Warfare Tactics for 4G Systems and Beyond

Matthew Jonathan La Pan

(ABSTRACT)

In the modern era of wireless communications, radios are becoming increasingly more cognitive. As the complexity and robustness of friendly communications increases, so do the abilities of adversarial jammers. The potential uses and threats of these jammers directly pertain to fourth generation (4G) communication standards, as well as future standards employing similar physical layer technologies.

This paper investigates a number of threats to the technologies utilized by 4G and future systems, as well as potential improvements to the security and robustness of these communications systems. The work undertaken highlights potential attacks at both the physical layer and the multiple access control (MAC) layer along with improvements to the technologies which they target.

This work presents a series of intelligent, targeted jamming attacks against the orthogonal frequency division multiplexing (OFDM) synchronization process to demonstrate some security flaws in existing 4G technology, as well as to highlight some of the potential tools of a cognitive electronic warfare attack device. Performance analysis of the OFDM synchronization process are demonstrated in the presence of the efficient attacks, where in many cases complete denial of service is induced.

A method for cross ambiguity function (CAF) based OFDM synchronization is presented as a security and mitigation tactic for 4G devices in the context of cognitive warfare scenarios. The method is shown to maintain comparable performance to other correlation based synchronization estimators while offering the benefit of a disguised preamble. *Sync-amble* randomization is also discussed as a combinatory strategy with CAF based OFDM synchronization to prevent cognitive jammers for tracking and targeting OFDM synchronization.

Finally, this work presents a method for dynamic spectrum access (DSA) enabled radio identification based solely on radio frequency (RF) observation. This method represents the framework for which both the cognitive jammer and anti-jam radio would perform cognitive sensing in order to utilize the intelligent physical layer attack and mitigation strategies previously discussed. The identification algorithm is shown to be theoretically effective in classifying and identifying two DSA radios with distinct operating policies.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Wireless communication systems are prevalent across a range of platforms. Their applications are continuing to increase with time, often times substituting for wired communications systems due to their inherent benefits. The increasing need for wireless technology presents a distinct set of challenges and requirements based upon the available resources.

The availability of wireless communication resources is a good starting point for understanding the issue. There are a variety of resources which are important and essential to any communications system, however, in the context of modern wireless communications the one that always seems to pop up in conversation is spectrum. Spectrum refers to the available bandwidth appropriated for wireless communications applications along the usable radio frequency spectrum. In order for any wireless communication system to operate, it must have some spectrum to operate on. But in todays society the demand for spectrum is starting to exceed the supply, which has led to spectral crowding. Figure 1.1 depicts the limited availability of spectrum in the United States.

At the same time that spectral limitations have started to become a concern, wireless applications that require an increasing amount of capacity and throughput continue to develop. This problem is perhaps most visible in the realm of cellular communications, where the emergence of smart phones, tablets and similar devices have brought forth an overwhelming demand for high data rates. In order to meet the demands of cellular networks, there are a number of emerging technologies which have been developed to maximize spectral efficiency. In particular, there is the set of fourth generation (4G) wireless standards which are shaping the way that available communications resources are utilized.

The strategies for improving efficiency in wireless communication both offered by 4G systems and that are being developed for future systems are numerous. The research in this paper is centered around some of the most important technological developments made at the fundamental layers of the Open Systems Interconnection (OSI) network architecture stack. Figure 1.2 illustrates an example of how this stack loosely defines the layers of a

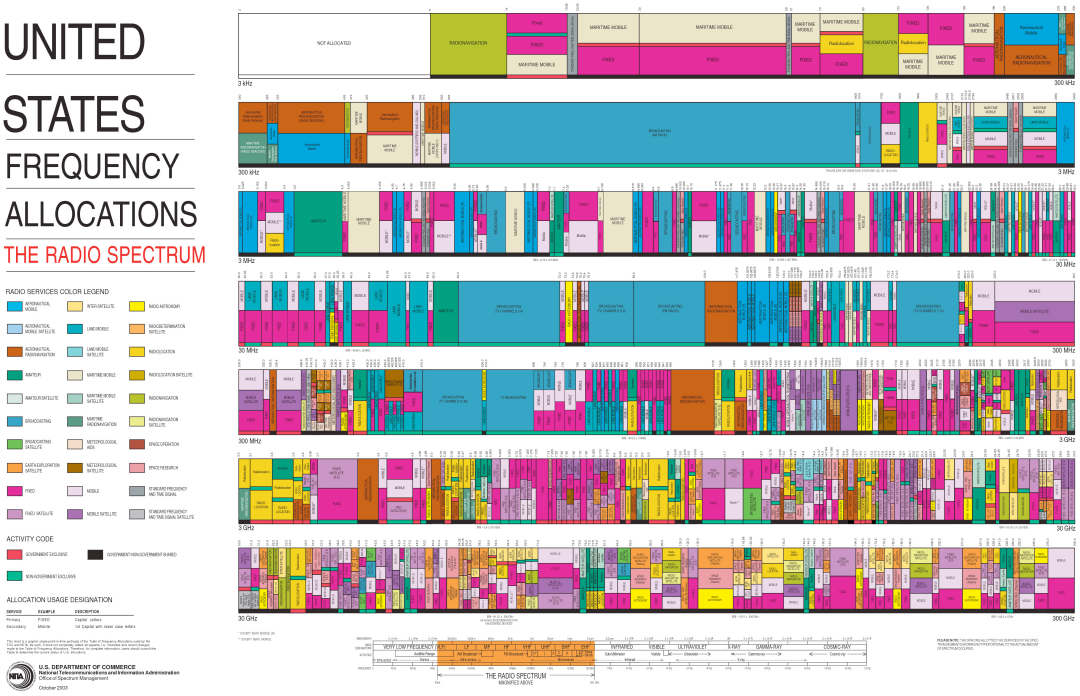

Figure 1.1: Illustration of spectrum allocation in the United States from 2003. This diagram of the radio spectrum frequency allocations in the United States illustrates the problem of spectral crowding at as the demand for wireless applications increases.

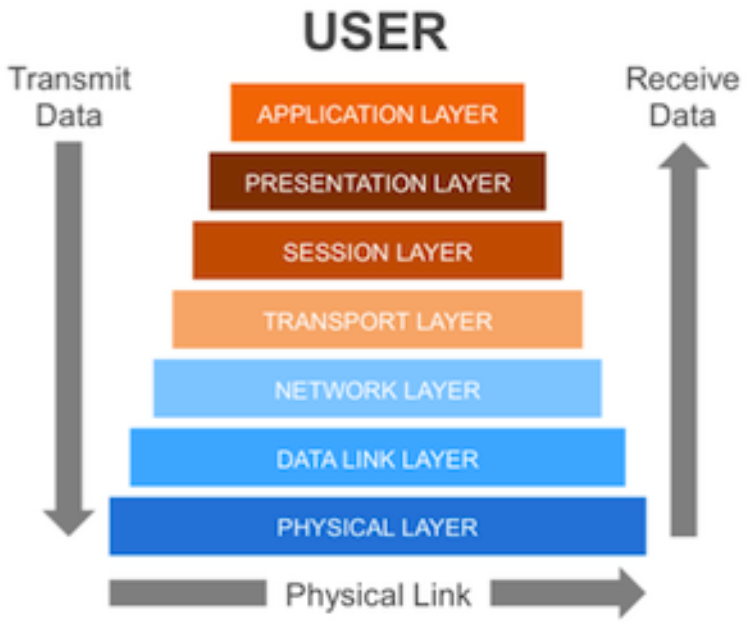

Figure 1.2: Open Systems Interconnection (OSI) network architecture model for communications systems. The fundamental level encompasses the digital modulation structure of a system, which is OFDM for the wireless systems analyzed in this work. The data link layer is an abstraction of processes like multiple user access (MAC) and is sometimes referred to as the MAC layer. The concept of DSA for wireless systems refers to this second layer.

communications system from user to user. Specifically, we will analyze the use of orthogonal frequency division multiplexing and multiple access (OFDM/A) in current implementations, as well as dynamic spectrum access (DSA) technology and for future implementations of wireless systems. OFDM, which is already a part of 4G standards [3, 4], offers a wealth of advantages to 4G systems at the physical layer. DSA is at the forefront of future communications technology, and will most likely be incorporated in either later 4G or 5G standards at the MAC layer.

While the feasibility of OFDM and DSA for modern systems offers significant advantages to users, many of the techniques for implementing these technologies have been developed for commercial systems where capacity and throughput demand is placed at a higher premium than security concerns. The emergence of electronic warfare for wireless communication systems has put a square focus on security issues for 4G systems. The emergence of OFDM and DSA for 4G systems gives rise to a wealth of problems on both the offensive and defensive side of electronic warfare tactics. This research is focused on a particular set of those problems, with emphasis on incorporating electronic warfare considerations in to system implementations.

The novel contributions of this work are as follows:

- A suite of power efficient jamming attacks that target OFDM synchronization at both the timing acquisition and carrier frequency offset estimation processes.
- An efficient cross ambiguity function based OFDM synchronization approach.
- A dynamic spectrum access radio classification and identification approach using stochastic modeling and machine learning algorithms.

These items, as well as the accompanying mathematical analysis, are the original work of the author, and it should be pointed out that the use of *we* in this paper is in general reference to the audience. In addition, the remainder of this work will be organized as follows. Chapter 2 presents the theoretical foundations and relevant literature to the presented research. Chapter 3 analyzes the performance of OFDM synchronization security and presents a number of possible security threats in the form of efficient jamming attacks. Chapter 4 discusses OFDM attack mitigation and security strategies, including synchronization with the cross ambiguity function and frame level 'sync-amble' randomization. Chapter 5 covers an algorithm for dynamic spectrum access radio identification. Finally, Chapter 6 contains the conclusions of this work as well as proposed future work.

Chapter 2

Foundations and Literature Review

Orthogonal frequency division multiplexing (OFDM) is a multicarrier digital modulation scheme. As suggested by its name, OFDM utilizes an orthogonal basis for performing frequency division multiplexing. There are multiple motivations for this technique, perhaps the most basic being the avoidance of intersymbol interference (ISI). ISI occurs when one or more symbols in a wireless communication system interferes with another symbol. ISI can be a catastrophic detriment to any communication symbol if it is not mitigated. OFDM uses the discrete Fourier transform (DFT) as an orthogonal basis. This approach also ensures spectral efficiency because OFDM does not require guard bands between subcarriers, as opposed to traditional FDM where they needed to protect against co-channel interference. In addition, the structure of OFDM allows for lower complexity equalization in the frequency domain. This is an important feature of OFDM that ties in to mitigating ISI that is caused by multipath interference.

Based on the evolving landscape in the world of wireless communications, OFDM is becoming a popular choice for physical layer modulation. In order to grasp this migration, it is essential to understand the fundamentals, advantages and disadvantages of OFDM for wireless communications. Since a portion of the basis for choosing OFDM as a physical layer modulation scheme is rooted in its compatibility with DSA schemes, it makes sense to cover the foundation of both technologies.

2.1 Fundamentals of Orthogonal Frequency Division Multiplexing/Multiple Access

Frequency division multiplexing (FDM) is the basis for the development of OFDM technology. FDM is predicated on the transmission of multiple streams of data over the same medium via frequency domain separation. For digital modulation schemes, baseband signals

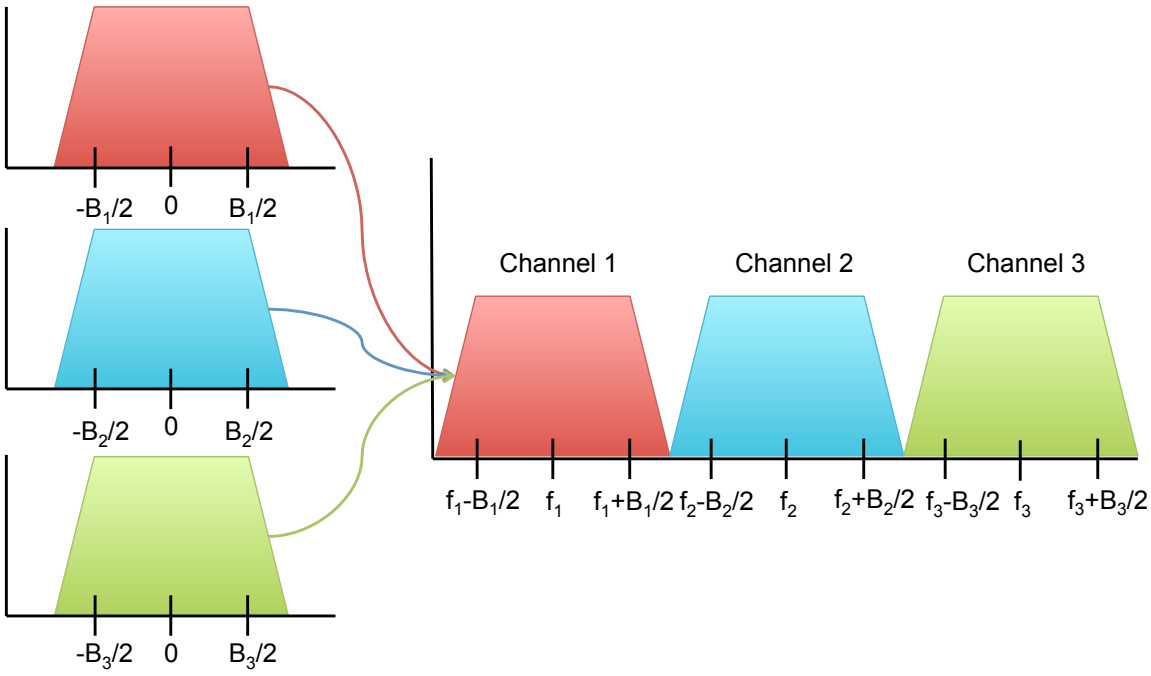

Figure 2.1: Frequency division multiplexing.

are modulated to carrier frequencies via

$$p_k = \sum_{k=0}^{K-1} \mathrm{Re}(b_k(t)) \cos(2\pi f_k t) + \mathrm{Im}\, b_k(t) \sin(2\pi f_k t) \tag{2.1}$$

and transmitted simultaneously according to

$$s = \sum_{k=0}^{K-1} p_k(t). \tag{2.2}$$

In order for these signals to be recoverable, they must be separable in the frequency domain. This means that each separate passband signal p_k with bandwidth B_k must satisfy

$$f_k + \frac{B_k}{2} \leq f_{k+1} - \frac{B_{k+1}}{2}. \tag{2.3}$$

In practical scenarios, however, the signals p_k will have some amount of energy outside of their bandwidths B_k. Extra frequency domain spacing, often referred to as guard bands, are used in order to ensure minimal interference between adjacent channels.An example of this technique is shown in Figure 2.1.

While this technique is effective for the transmission of multiple signals over a single medium, the frequency spacing and the use of the guard bands make it somewhat spectrally inefficient,

in terms of bits per second per Hertz (bits/s/Hz). In 1966, Robert Chang proposed using orthogonal signals in order to transmit multiple streams of data simultaneously [5]. His work, along with the incorporation of the discrete Fourier transform [6], would eventually give rise to the modern concept of orthogonal frequency division multiplexing (OFDM).

In an OFDM system, M-ary in-phase and quadrature (IQ) symbols X_k are modulated on to k orthogonal baseband subcarriers using a discrete-time Fourier transform (DTFT) according to

$$x(t) = \frac{1}{N}\sum_{k=0}^{N-1} X_k e^{j2\pi kt/T}, \quad 0 \leq t < T. \tag{2.4}$$

The selection of the symbol period as T guarantees that each of the subcarriers will be orthogonal to one another, which can be proven quite easily. By definition, the set of functions f are orthogonal if for the inner product $\langle f_i, f_j \rangle$ of any functions from the set

$$\langle f_i, f_j \rangle = \int_a^b f_i(x) f_j^*(x)\, dx = \|f_i\|^2 \delta_{i,j} = \|f_j\|^2 \delta_{i,j} \tag{2.5}$$

where

$$\delta_{i,j} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases} \tag{2.6}$$

and

$$\|f\|^2 = \langle f, f \rangle. \tag{2.7}$$

For OFDM subcarriers

$$f_i(t) = e^{j2\pi k_i t/T}. \tag{2.8}$$

These functions are orthogonal over any multiple of a symbol period T, meaning

$$a, b \in \{zT | z \in \mathcal{Z}\}. \tag{2.9}$$

We can show that

$$\|f\|^2 = \int_a^b e^{j2\pi kt/T} e^{-j2\pi kt/T}\, dx = \int_a^b 1\, dx = (b-a). \tag{2.10}$$

Incorporating this information in to (2.5) we see that

$$\langle f_i, f_j \rangle = \int_a^b e^{j2\pi k_i t/T} e^{-j2\pi k_j t/T}\, dx \tag{2.11}$$

which simplifies to

$$\langle f_i, f_j \rangle = \int_a^b e^{j2\pi (k_i - k_j) t/T}\, dx = (b-a)\delta_{i,j}. \tag{2.12}$$

These orthogonal bases form the foundation for transmission using OFDM. Each OFDM subcarrier will transmit one digital symbol, X_k, per OFDM symbol. These symbols are

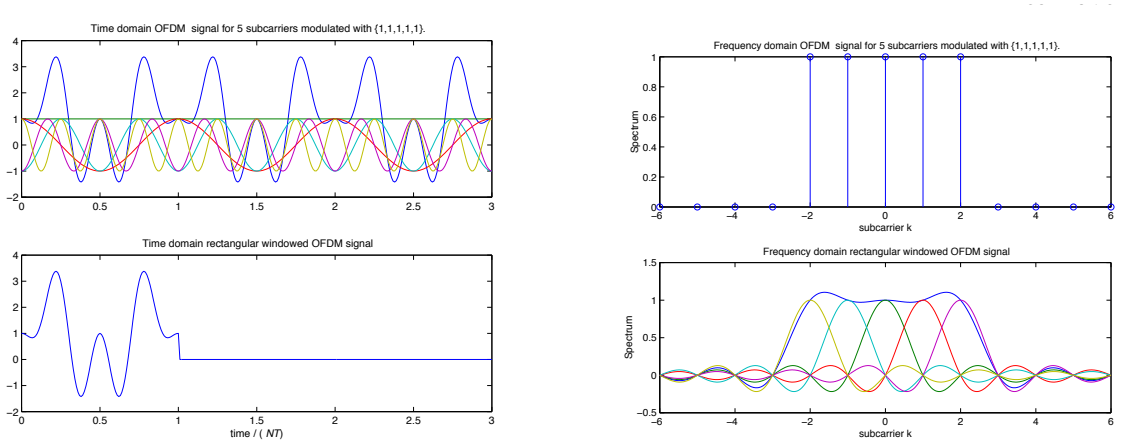

Figure 2.2: Synthesis of OFDM symbols and their fundamental representation in both the time and frequency domain [1].

typically chosen from an M-ary digital symbol mapping used to modulate binary data. OFDM is able to transmit using phase-shift keying (PSK) and amplitude shift keying (ASK), as well as quadrature amplitude modulation (QAM), which is a combination of the two.

While the relationship in equation 2.4 is useful for analyzing subcarrier orthogonality, OFDM symbols are actually generated discretely according to the DFT

$$x[n] = \frac{1}{N} \sum_{k=0}^{N-1} X_k e^{j2\pi kn/N}, \quad n = 0, 1, ..., N-2, N-1. \tag{2.13}$$

The sequence $x[n]$ represents a single OFDM symbol over a the symbol period T, where

$$N = f_s T \tag{2.14}$$

where f_s is the sampling frequency in Hz for a given system. In an OFDM system, N represents both the number of samples per symbol and the number of subcarriers.

The baseband signal $x[n]$ is sent to a digital-to-analog converter (DAC) then either to the receiver either at baseband, or to RF an modulation stage, the latter being the case for wireless systems. The receiver recovers the modulated symbols X_k using the conjugate transform

$$X_k = \sum_{k=0}^{N-1} x[n] e^{-j2\pi kn/N}, \quad n = 0, 1, ..., N-2, N-1. \tag{2.15}$$

The resulting IQ symbols are then estimated, processed and demodulated at the receiver, where the underlying information bits can ultimately be decoded.

As shown in Figure 2.2, OFDM is a highly spectrally efficient modulation scheme. It has been shown that OFDM is up to twice as spectrally efficient as single carrier modulation [7].

The spectral efficiency, η, of OFDM is given by the equation

$$\eta = \frac{NR_s}{(N+1)f_o} \tag{2.16}$$

where R_s is the symbol rate and f_o represents the bandwidth of a single subcarrier. From this equation we see that as $N \to \infty$, $\eta \to \frac{R}{f_o}$. Alternatively, the spectral efficiency of single carrier modulation schemes is given by

$$\eta = \frac{R_s}{2f_o}. \tag{2.17}$$

It should be noted that single carrier modulations can be windowed in order to somewhat improve spectral efficiency, while OFDM subcarriers can not be windowed due to the orthogonality requirement. However, the efficiency gain from windowing is much less significant than the factor of 2.

Increase in spectral efficiency is a major motivation for the movement of modern systems toward utilizing OFDM technology at the physical layer, however, it is not the only reason. As described in equation (2.13), OFDM symbols are typically generated using a DFT. This is a major advantage for OFDM on two fronts. The first is that there are a large number of efficient algorithms for computing the DFT. The algorithms within this family are often referred to communally as the fast Fourier transform (FFT). While explicit computation of an N point DFT requires $\mathcal{O}(N^2)$ computations, existing efficient algorithms like the radix-2 Cooley-Tukey algorithm can compute the FFT of a complex sequence in $\mathcal{O}(N\log(N))$ computations. The second advantage–which is really an extension of the first–is that there is a wide range of low cost signal processing hardware designed specifically to compute the FFT, making OFDM modulators and demodulators relatively inexpensive. And, as we will discuss in subsequent sections, the FFT based structure of OFDM will allow for portions of the modulation control processes of synchronization and equalization to be performed efficiently in the frequency domain.

The choice of an orthogonal basis for OFDM means that there is zero inter-symbol interference (ISI) and zero inter-carrier interference (ICI) in an ideal communication setting. In order to modulate baseband symbols with the FTT, an OFDM transmitter first takes a serial stream of digital samples and parallelizes them. The symbols are then converted to baseband digital symbols, also called IQ symbols. The specific digital modulation used on the subcarriers depends on the transmitter, and can be varied from low order modulations–such as binary phase-shift keying–to modulations with much higher bits per symbol like 256 bit quadrature amplitude modulation (256 QAM). The symbols are then modulated on to the individual subcarriers by assigning each one to a frequency bin and performing an inverse FFT (IFFT). Intuitively, the signal is being 'constructed' in the frequency domain and then the time domain signal is generated via IFFT. The real and imaginary parts of the signal are then split and can be transmitted on the carrier frequency using IQ modulation. The OFDM receiver is simply the inversion of this process. The basic block diagrams of the OFDM transmitter and receiver are shown in Figures 2.3 and 2.4.

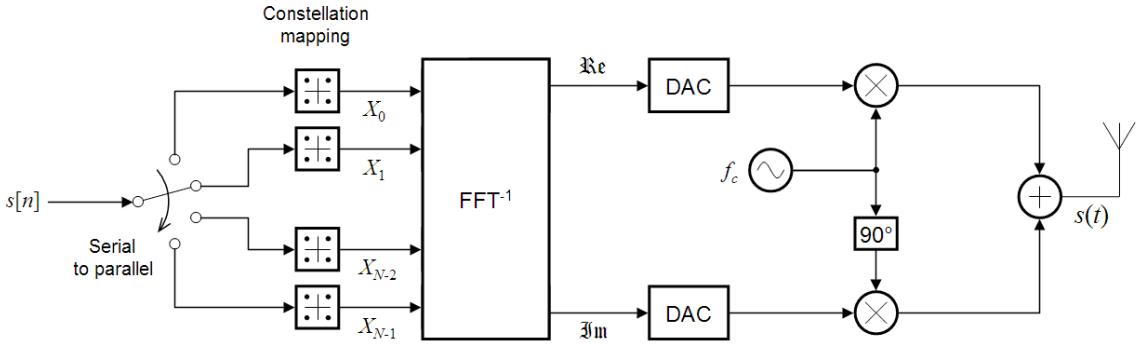

Figure 2.3: OFDM transmitter.

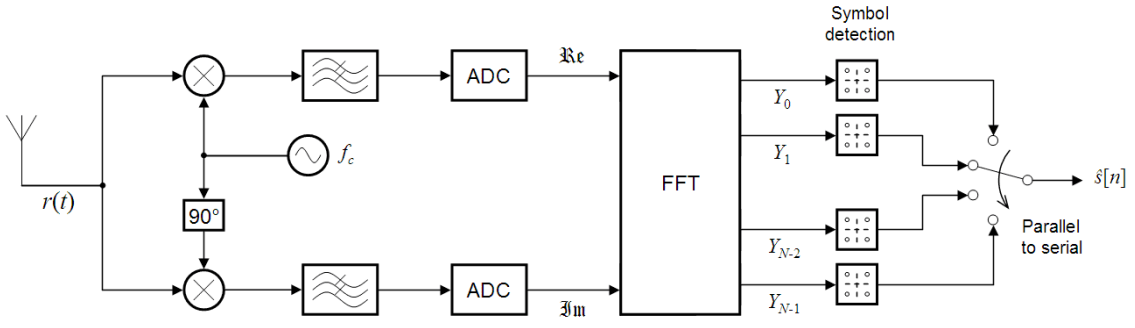

Figure 2.4: OFDM receiver.

While these simplified models of an OFDM transmitter and receiver covers the basic functions of modulation and demodulation, there are important processing blocks required for coherent OFDM communication which are omitted. In order for an OFDM transmitter and receiver to communicate in dynamic, wireless environments, it is necessary to facilitate synchronization between the two, and equalization at the receiver due to multipath channel effects. These processes, detailed in the next couple of sections, add complexity at both the transmitter and receiver. The transmitter is generally tasked with injecting control symbols in to outgoing data streams in order to enable synchronization and equalization at the receiver. The receiver is tasked with processing these overhead symbols in order to mitigate timing and frequency offsets that result in loss of subcarrier orthogonality and subsequent ICI, as well as multipath effects that can lead to ISI at the receiver. While idealized OFDM transmitter and receiver models are useful for explaining the underlying theory and motivation for using OFDM, communication with OFDM in most realistic wireless settings requires these added processes.

2.1.1 Orthogonal Frequency Division Multiplexing Synchronization

All practical wireless communications systems are susceptible to timing and frequency errors between the transmitter and the receiver. This is due to clock differences between the two ends and the uncertainty of symbol start times in burst communications. For this reason, synchronization between the terminals is required for certain communication systems, depending on their design.

Assuming that the synchronization symbol sent resembles an ordinary data symbol, and that the channel from the transmitter to the receiver can be modeled as an AWGN multipath channel with finite length impulse response, the sampled signal at the receiver after baseband conversion is represented as

$$r_n = \left(\sum_{k=0}^{C-1} x_{n-d-k} h_k \right) e^{2\pi j \frac{f}{f_s} n} + n_n \tag{2.18}$$

where the subscript n represents the sample index and spans the search area for the training symbol, d is the delay value and timing point of the symbol, C is the length of the channel approximation, f represents the carrier frequency offset and n is the noise term.

Synchronization is both critical and prerequisite to successful communication using OFDM. Without properly accounting for timing and carrier frequency offset at the receiver, OFDM system performance will be massively degraded [7, 8]. The resulting inter-symbol interference (ISI) and inter-carrier interference (ICI) in many cases can prevent communication altogether.

There are various methods for performing OFDM synchronization [9, 10, 11, 12, 13]. However, one method that is very frequently employed for OFDM systems is presented in [14].

This method is employed in 802.11 standards, as well as WiMAX. The synchronization method presented by Schmidl and Cox provides a high level of performance–the method provides the maximum likelihood (ML) estimate for the OFDM synchronization symbol *including* channel effects–and is therefore the method analyzed for comparative analysis in this paper. It is important to note, that while this method is not used in every OFDM system, it is one of the most practical high performance algorithms available for synchronization, making it a great point of reference for performing mathematical analysis on the synchronization process.

The synchronization method proposed in [14] has three main stages–symbol timing estimation, fine carrier frequency offset estimation and correction, and coarse carrier frequency offset estimation. These stages are performed sequentially in the order listed. This algorithm is based on the use of specific *preamble* symbols, transmitted at the beginning of every frame. Because of the particular structure of this synchronization algorithm, the preamble symbols have a very specific structure as indicated in [14].

The first step in the synchronization process is the estimation of symbol timing. Only the first preamble symbol is used for the timing stage. Once the complex time domain samples are obtained after radio frequency (RF) down conversion then the timing estimation algorithm is carried out. A sliding window of L samples is used to search from the preamble, where L is equal to the length of half of the first preamble symbol excluding the cyclic prefix. Two terms are computed for timing estimation. The first according to

$$P(d) = \sum_{m=0}^{L-1} (r_{d+m}^{*} r_{d+m+L}) \tag{2.19}$$

and the second according to

$$R(d) = \sum_{m=0}^{L-1} |r_{d+m+L}|^2 \tag{2.20}$$

where d is the time index which corresponds to the first sample taken in the window and r is the length-L vector of received symbols. The $(\ )^*$ notation represents complex conjugation. These two terms are used to compute the timing metric $M(d)$ according to

$$M(d) = \frac{|P(d)|^2}{R(d)^2} \tag{2.21}$$

which determines the symbol timing.

This metric will generate a plateaued peak where the maximum values begin at $d = \hat{d}$, with the point $\hat{d}$ being at the beginning of the preamble, and end when $d = \hat{d} + (T_{cp} - T_{ch})f_s$, where T_{cp} is the period of the cyclic prefix and T_{ch} is the length of the channel impulse response, corresponding to its delay spread. The symbol timing estimate can be taken from anywhere on the plateau, which will be the length of the cyclic prefix minus the length of the channel impulse response. This timing estimate will tell the receiver the starting point

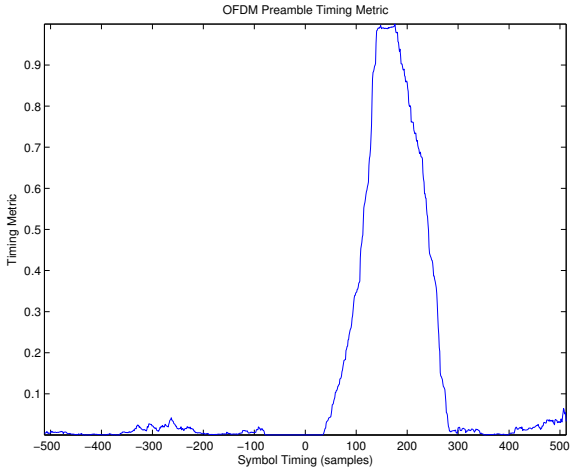

Figure 2.5: The timing metric $M(d)$ for an OFDM preamble symbol in a window of 3 symbols length

of the window of samples to grab in order to process an incoming frame. Once this stage is performed, the receiver will take the samples from the timing point and correct for the carrier frequency error between the transmitter and the receiver.

Carrier frequency offset estimation is the final step of the synchronization process. This stage corrects for the error introduced by the clocks at both the transmitter and the receiver. There are actually two sub-stages within frequency correction. The first is fine frequency correction and the second is coarse frequency correction. The fine frequency correction Δf is estimated using

$$\Delta f = \angle(P(d))/\pi T \tag{2.22}$$

where T is the period of a single preamble symbol without its cyclic prefix and d is taken from anywhere along the timing metric plateau.

The coarse frequency error estimation is the final step in the synchronization process, and finally employs the use of the second preamble symbol and the differentially modulated PN sequence. First, FFTs–the length of the symbol period without the cyclic prefix–of each of the symbols are taken. A coarse frequency metric is then computed in order to determine the number of bins that the symbols are shifted in either direction according to

$$B(g) = \frac{\left|\sum_{k\in\mathcal{X}} R^*_{1,k+2g} v^*_k R_{2,k+2g}\right|^2}{2(\sum_{k\in\mathcal{X}} |R_{2,k}|^2)^2} \tag{2.23}$$

where $R_{1,k+2g}$ and $R_{2,k+2g}$ represent the DFT of r_{d+m} and r_{d+m+L}, respectively. These terms are later defined explicitly in equation (3.20). The term g represents the circular shift of the frequency bins of each of the DFT terms. For this equation, the set $\mathcal{X}$ represents all of

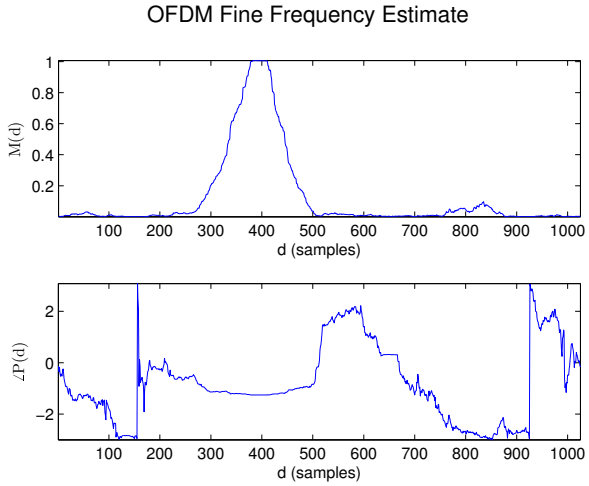

Figure 2.6: The timing metric $M(d)$ and the corresponding $\angle P(d)$ for an OFDM preamble symbol in a window of 3 symbols length. The phase value taken from the timing metric plateau will determine the fine frequency offset estimate.

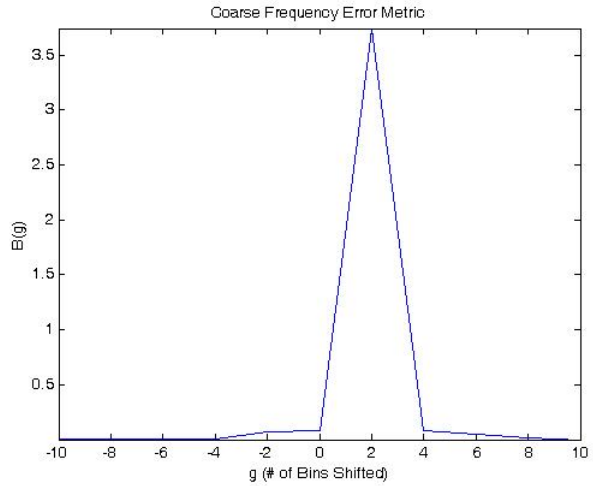

Figure 2.7: The coarse frequency metric $B(g)$ for an OFDM preamble symbol in a window of 3 symbols length

the subcarrier bins which are occupied by both preamble symbols (either even or odd). The differential PN sequence shows up as

$$v_k = \sqrt{2}\frac{X_{2,k}}{X_{1,k}}. \tag{2.24}$$

where the terms $X_{1,k}$ and $X_{2,k}$ represent the length L DFT of the first and second preamble symbols. It is important to note that

$$X_{i,k} = \sum_{n=0}^{2L-1} x_{n+N(i-1)} e^{-2\pi jkn/2L}. \tag{2.25}$$

The overall frequency offset is

$$\hat{\Delta f} = \angle(P(d))/\pi T + 2g_{\max}/T \tag{2.26}$$

where g_{max} is the value of g that maximizes $B(g)$ in equation (2.23), specifically $g_{max} = \frac{f}{2}$.

Once the overall frequency offset between the transmitter and the receiver has been determined, the signal acquisition process is complete and information symbols can be transmitted.

2.1.2 Orthogonal Frequency Division Multiplexing Equalization

Wireless channels present a number of distinct challenges for communications systems. There are a number of channel effects that can distort a wireless signal and impact fidelity at the receiver. In an ideal setting, the power loss from a transmitter to a receiver, termed free space path loss, is relative to the squared distance from the receiver according to the equation

$$\text{FSPL} = \left(\frac{4\pi df}{c}\right)^2. \tag{2.27}$$

Wireless communications are prone to a slough of other interference effects, though, that are often aggregated in to a simplistic general model for the path loss according to

$$\text{PL} = \left(\frac{4\pi df}{c}\right)^n \tag{2.28}$$

where the exponent n represents the 'lossy-ness' of a given channel. Larger values of n are used to represent relatively lossy channel environments, while values closer to 2 indicate channel conditions closer to free space propagation.

There are a number of challenges for land based wireless communications caused by the presence of physical obstacles, all of which can cause the value of n to increase for the path

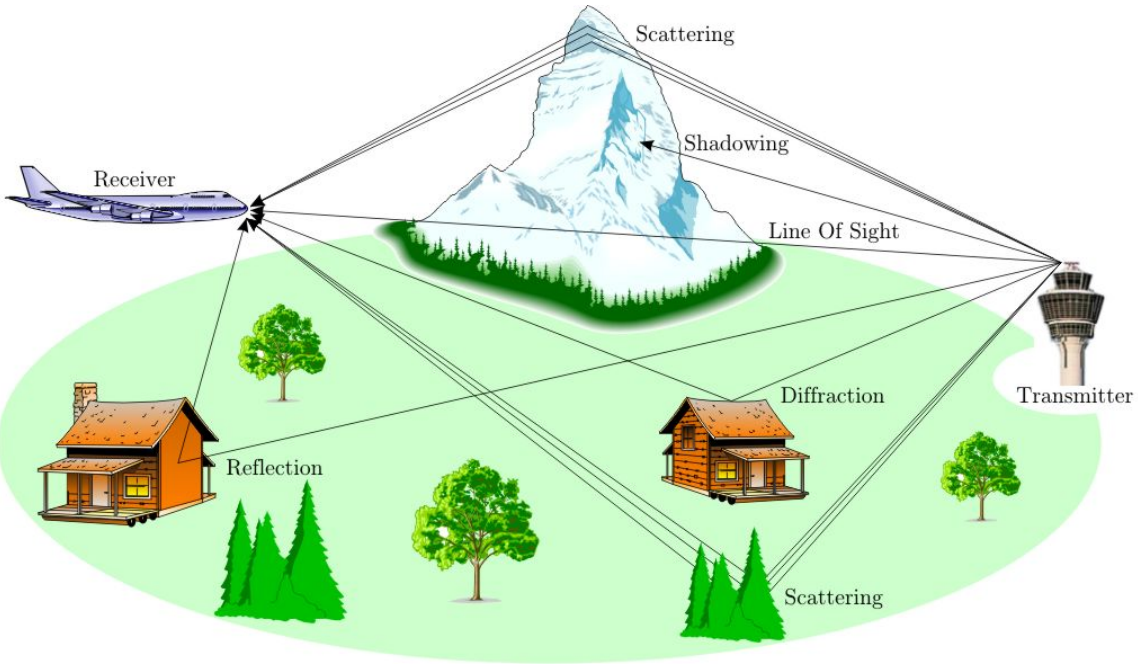

Figure 2.8: A hypothetical wireless channel environment, with examples of possible interference effects to a wireless signal.

loss estimate. Reflection, diffraction, scattering and shadowing–shown in Figure 2.8–are four important effects caused by physical obstructors in wireless systems that can be a detriment to a receiver's ability to successfully demodulate transmitted signals. For the purpose of this work, we will focus on the aggregated impact of these effects that result in multipath interference at the receiver.

The basic idea behind this approach is that any wireless channel can be modeled by its impulse response according to

$$h(t) = \sum_{k=0}^{K-1} h_k \delta(t - \tau_k) \tag{2.29}$$

where $h_k \in \mathbb{C}$, $\tau_k \in [0, \infty)$ and K represents the number of distinct signal paths from the transmitter to the receiver. $\delta(t)$ represents the continuous time Dirac delta function. An example of the magnitude of a multipath channel response is shown in Figure 2.9. The signal at the wireless receiver is mathematically represented by the convolution of the transmitted signal $x(t)$ and the channel response according to

$$y(t) = [h * x](t) \stackrel{\text{def}}{=} \int_{-\infty}^{\infty} h(\tau) x(t - \tau)\, d\tau. \tag{2.30}$$

Ideally, the received signal $y(t)$ will the same as the transmitted signal $x(t)$. For this to occur, it is required that $h(t) = \delta(t)$, which is often referred to as a flat channel with unity

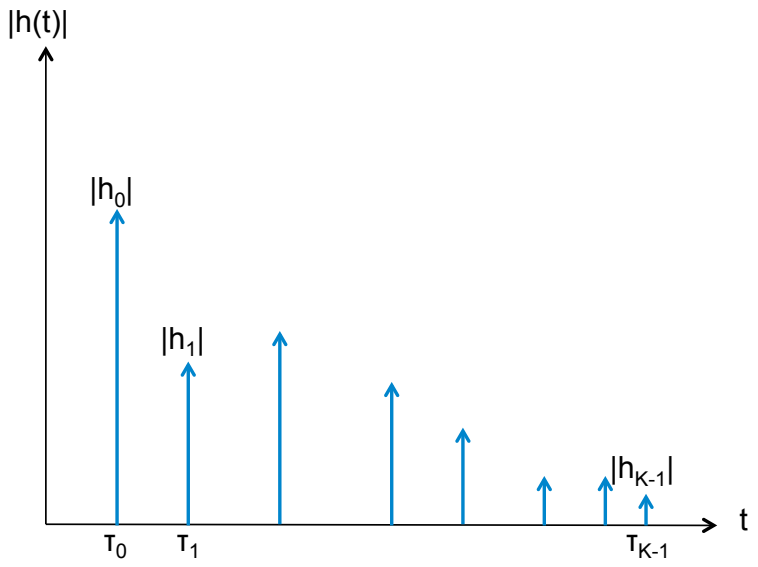

Figure 2.9: The continuous time magnitude response of a multipath channel. Each delta function is weighted with a complex coefficient corresponding to a specific signal path.

gain. However, in realistic scenarios the wireless channel will be very different from the unity gain case, imparting some level of distortion on the received signal. This distortion can cause inter-symbol interference (ISI) at the receiver, resulting in a severe degradation of that receiver's ability to successfully demodulate the signal of interest.

In order to mitigate the distorting effect that multipath channels will have on a wireless signal, it is necessary to perform equalization. Mathematically, the purpose of equalization is to undo the multipath channel distortion and recover as close to the original signal as possible according to

$$y(t) = \bar{x}(t) = [\bar{h}^{-1} * h * x](t) \tag{2.31}$$

where $\bar{h}$ represents an estimated inverse of the wireless channel.

Computing the inverse channel response $\bar{h}^{-1}$ in the time domain is very complex problem due to the convolution operation. However, the problem can be simplified in the frequency domain by utilizing the Fourier transform pair

$$\mathcal{F}\left[[h * x](t)\right] = \mathcal{F}\left[h(t)\right] \cdot \mathcal{F}\left[x(t)\right] \tag{2.32}$$

where $\mathcal{F}[*]$ represents the Fourier transform. In the continuous time domain, the Fourier transform of a signal $x(t)$ is defined as

$$\mathcal{F}\left[x(t)\right] = \int_{-\infty}^{\infty} x(t) e^{-2\pi j f t}\, dt \tag{2.33}$$

where f represents the domain across which the Fourier transform is defined.

Using the relationship from (2.32) in (2.31), we can see that the frequency domain representation of $y(t)$ can be represented as

$$Y(f) = \bar{H}^{-1}(f)H(f)X(f) \tag{2.34}$$

where the uppercase notations represent the frequency domain representations of the signals $Y(f) = \mathcal{F}[y(t)]$, $X(f) = \mathcal{F}[x(t)]$ and so on. Since the goal of equalization is to mitigate any distortion in the wireless channel in order to achieve $y(t) = x(t)$, we can see that it is desirable for

$$\bar{H}^{-1}(f) = \frac{1}{H(f)}. \tag{2.35}$$

So in its most basic form, frequency domain equalization is performed on a signal by estimating the wireless channel and then dividing out the channel frequency response in order to recover the undistorted signal.

This basic idea is applied to the concept of OFDM synchronization. In fact, the frequency domain synthesis structure of OFDM lends itself to the concept of frequency domain equalization very well. After successful acquisition and synchronization with negligible error, an OFDM symbol can be represented as

$$r_n = \left(\sum_{c=0}^{C-1} x_{n-d_o-c}h_c\right) + n_n, \quad n = 0, 1, ..., N-2, N-1 \tag{2.36}$$

where $\{d_o|\ d_o \in \mathbb{N},\ 0 \leq d_o \leq f_s T_{cp}\}$, meaning that the timing point is taken correctly from somewhere along the cyclic prefix range. This relationship is a discrete convolution of the transmitted signal and the discrete wireless channel response plus the noise term. Applying the DFT to this sequence will yield

$$R_k = e^{-j2\pi d_o k/N}H_k X_k + N_k, \quad k = 0, 1, ..., N-2, N-1. \tag{2.37}$$

The exponential term in this result is a linear phase shift, the frequency domain representation of a uniform time shift. Based on the frequency domain equalization method discussed earlier, it is desirable for the communications system to be able to estimate the discrete channel response H_k in order to mitigate the multipath channel distortion. However, the number of unknown terms in (2.37) makes the channel filter response H_k difficult to estimate.

In order to estimate the channel response at the receiver, OFDM systems make use of special control symbols, usually called 'pilots' or 'pilot tones'. These pilot tones are symbols inserted in to the data stream of an OFDM symbol in order for the receiver to make measurements of the signal x_n. These symbols are inserted in to an outgoing symbol via frequency domain synthesis, shown in Figure 2.10. This is performed by placing specific symbols–generally known at the receiver–in X_k at specific, usually uniformly spaced intervals, in k. In this case the receiver would know the sequence

$$X_{eq} = X_{mp},\ \{m|m \in \mathbb{Z}, m > 1\},\ \{p|p \in \mathbb{Z}, 0 \leq p \leq \lfloor\frac{N}{m}\rfloor\} \tag{2.38}$$

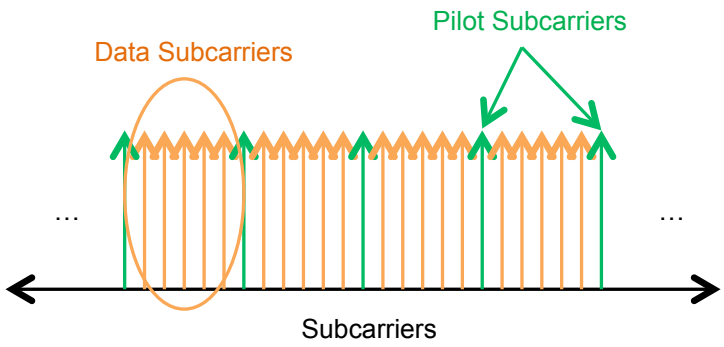

Figure 2.10: The use of pilot tones for OFDM equalization. The orange subcarriers are used to transmit data to the receiver, while the green subcarriers represent the pilots used at the receiver to take partial channel measurements for equalization. The symbols transmitted over the pilots are generally known at the receiver in order to construct a reliable channel estimate.

where m is chosen based on the coherence bandwidth

$$B_c \approx \frac{1}{D} \tag{2.39}$$

where$D$ is the delay spread, or the amount of time between the first significant signal path and the last. For example, in Figure 2.9 the delay spread is given by $D = \tau_{K-1} - \tau_0$. An OFDM equalization system measures the channel via the computation

$$\bar{H}_{mp} = \frac{X_{mp}}{R_{mp}} \tag{2.40}$$

resulting in a partial frequency domain equalization filter response of

$$\bar{H}_{k_o} = \begin{cases} \frac{1}{e^{-j2\pi d_o k/N} H_k + \frac{N_k}{X_k}} & : k \in mp \\ 0 & : o.w. \end{cases} \tag{2.41}$$

at the receiver.

A simple OFDM equalizer, called the *zero forcing equalizer*, interpolates the channel response using a low pass filter according to

$$\bar{H}_k = \bar{H}_{k_o} * h_{LP} \tag{2.42}$$

which is then applied to the received signal [15]. Assuming that the channel estimation at the receiver is accurate, the resulting frequency domain equalized signal will be

$$E_k = \frac{e^{-j2\pi d_o k/N} H_k X_k + N_k}{e^{-j2\pi d_o k/N} H_k + \frac{N_k}{X_k}}. \tag{2.43}$$

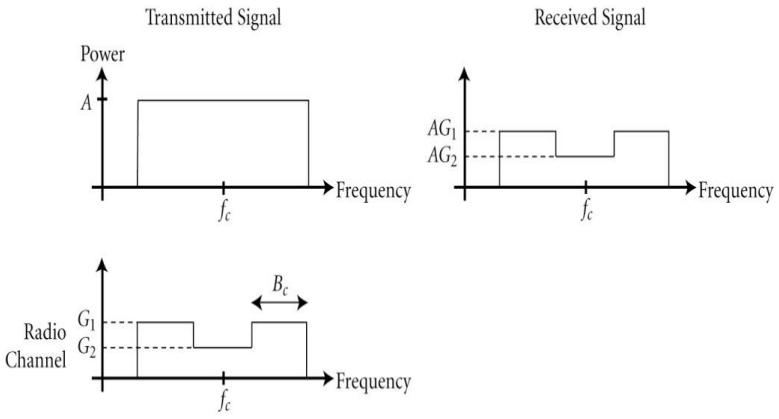

Figure 2.11: A frequency selective fading channel due to multipath interference. The diagrams on the left show the magnitude response of a transmitted signal and the frequency selective fading channel. The diagram on the right shows the magnitude response of the received signal after passing through the frequency selective channel. The coherence bandwidth, B_c, is shown on radio channel diagram.

In the noiseless case–meaning $N_k = 0$–the resulting signal will be $E_k = X_k$. However, the zero forcing equalizer does not account for the additive noise that is present in realistic systems. For this reason, minimum mean squared error (MMSE) channel estimation is often used for OFDM systems [16]. While the computational complexity of these methods is greater than the zero forcing equalizer, the MMSE methods account for additive noise, resulting in better overall channel estimation performance.

Additionally, mobile wireless communications–due to their mobile nature–present the problem of time varying channel fading. These effects are caused by movement of a mobile user, which results in variation of the multipath channel profile over time. In this case, equation (2.29) becomes

$$h(t) = \sum_{k=0}^{K-1} h(t)_k \delta(t - \tau_k), \tag{2.44}$$

meaning that $h(t)$ is no longer a time invariant system. In this case, the coherence time is defined as the amount of time over which the channel can be considered invariant, and is approximately

$$T_c \approx \frac{1}{f_m} \tag{2.45}$$

where f_m is the maximum delay spread caused by the movement of the transmitter and/or the receiver [17]. However, the correlation time is actually a measure the time interval over which the autocorrelation of the channel response is bounded by a certain value. For

example, 50% coherence time, where the autocorrelation $R_{hh}(T_c) \geq .5$ is defined as

$$T_c = \sqrt{\frac{9}{16\pi^2 f_m^2}}. \tag{2.46}$$

The correlation time of a fading channel in relation to the symbol period T_s for a given waveform is used to characterize the channel as a fast or slow fading channel–fast fading corresponds to $T_c < T_s$ and slow fading corresponds to $T_c > T_s$. Slow fading channels are much more desirable because the multipath channel can be considered constant over a symbol period, as in equation (2.29), greatly simplifying channel response estimation. However, OFDM symbols have a relatively long period due to the fact that

$$f_o = \frac{f_s}{N}. \tag{2.47}$$

Combining this fact with equation (2.14) yields the result

$$T = \frac{1}{f_o}. \tag{2.48}$$

While single carrier modulation symbol periods are dictated by the overall bandwidth, OFDM symbol duration is dictated by the bandwidth of a single subcarrier, also referred to as the subcarrier spacing.

The fact that OFDM symbols are much longer in duration than their single carrier counterparts, coupled with the fact that mobile systems introduce fading channels, it is required that mobile OFDM receivers perform channel estimation and equalization quite often. Generally these computations are performed for every single OFDM symbol and pilot tones are transmitted continuously. This not only adds control protocol overhead for OFDM systems, but it also presents an area for security vulnerability in OFDM systems [18, 19, 20].

While OFDM offers many advantages in terms of spectral efficiency and low cost implementation, the required control processes of synchronization and equalization pose a significant security vulnerability to OFDM based systems. This is not only based on the fact that both processes are prerequisite to demodulation at an OFDM receiver, but that both processes are generally performed relatively often in OFDM systems with highly visible control data. In the scope of this work, we will try to understand these security vulnerabilities and propose mitigations and solutions to physical layer based security threats.

2.2 Dynamic Spectrum Access

The allocation of spectrum resources is an important topic in relation to the history and future of both wireless technology as well as the wireless industries. This is because of

the fact that the amount of usable frequency spectrum for wireless technologies is limited. While the electromagnetic (EM) spectrum has not been proven to be explicitly limited by any upper bound on frequency, the range of frequencies that are usable for communications from a technological standpoint is on the order of hundreds of gigahertz. This has put a strain on the amount of available resources as the demand for wireless applications–such as mobile broadband–continues to grow at a breakneck pace. As the amount of available spectrum has dwindled over past decades–illustrated in Figure 1.1–there has been an important shift in the focus of wireless research to the emphasize the efficiency of how spectrum is utilized.

2.2.1 Time Frequency Access of the Spectrum

In order to discuss DSA problems, it is important to talk about the fundamental concepts that have led to the framework of DSA theory for wireless networks. While Figure 1.1 shows the macro-division of frequency bands, the way that these resources are divided amongst multiple users within a given band varies depending on the type of wireless technology employed for a particular network. For example, some wireless systems, such as the first generation Advanced Mobile Phone Standard, rely on dedicated channel FDMA for user resource allocation. An outline of this scheme as well as a simple diagram are provided in Section 2.1. Other systems like the second generation Global System for Mobile Communication (GSM) rely on time division multiple access (TDMA) MAC layer protocol in order to divide resources amongst users. There are also standards that use code division multiple access (CDMA), like the third generation CDMA2000 family of standards. While these examples all point out standards for cellular networks, any wireless system with multiple users requires a multiple user access scheme for resource allocation and management amongst users.

Looking at the scope of wireless systems just in the US–based on Figure 1.1–we can see that there are a plethora of applications for wireless networks. Each of these networks supports different types of wireless systems with different usage patterns, and those patterns are often dynamic. One popular example of this is the spectrum allocated to television broadcasting services. Due to the propagation characteristics of broadcast television, frequency reuse–the concurrent transmitting of different data over the same frequency band based on geographical separation–can only be performed over very large distances. This leaves a large portion of spectral resources unused in certain locations. These allocated but unused resources are termed *white space*. Both the IEEE 802.11af and 802.22 standards utilize the TV band white space in order to provide mobile broadband access to end users [21, 22].

While the large amount of unutilized spectrum is good news in terms of solving the problems posed by spectral crowding, the use of these white spaces presents a whole new set of challenges for the design of wireless systems. Because the resources that are available in the white spaces of the spectrum are already allocated to dedicated communications systems, networks wishing to access these resources have come under scrutiny for the potential interference risk they pose to these dedicated systems [23]. Due to the complexity of this problem, wireless

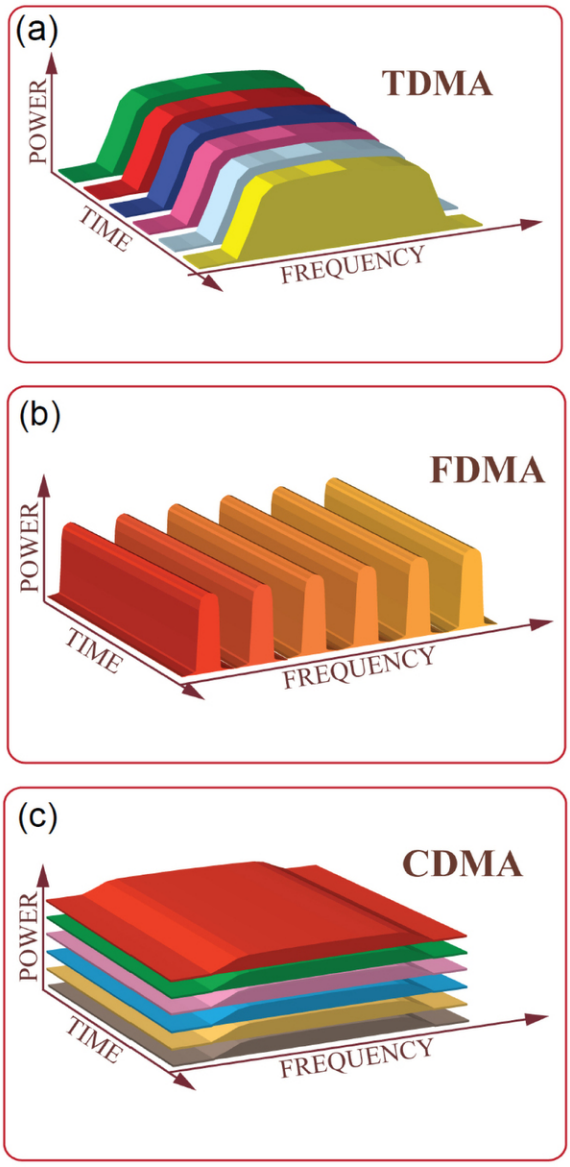

Figure 2.12: Visual comparison of three multiple access schemes. TDMA and FDMA divide user resources in time and frequency, respectively. CDMA uses orthogonal codes that allow multiple users to share concurrent time and frequency resources without interfering with one another [2].

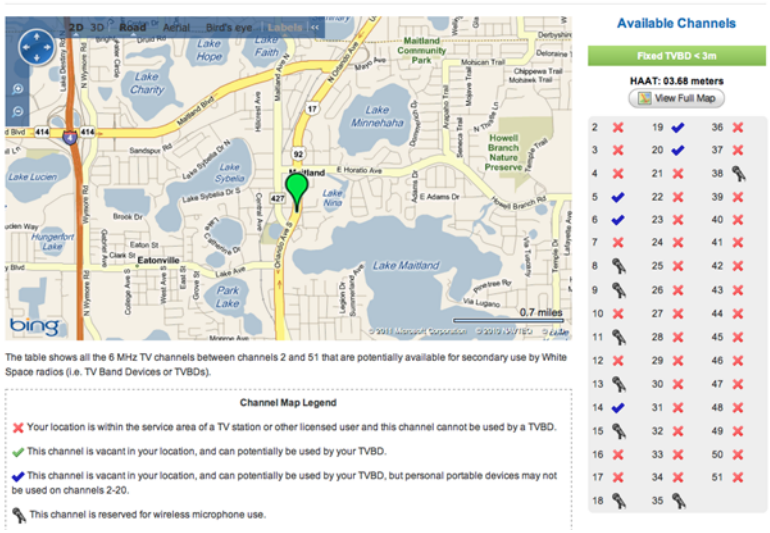

Figure 2.13: Example listing of available spectrum resources due to television band white space according to Spectrum Bridge's Show My White Space tool. The list on the right shows where television band devices could be used by television band devices (TVBDs).

networks that wish to utilize these white spaces require intelligent devices that can parse information about the surrounding RF environment in order to protect owners of licensed spectrum. This requirement has led to the idea of cognitive radios–devices that are a critical concept for dynamic spectrum access networks.

2.2.2 Cognitive Radio

Cognitive radio is a concept first proposed by Joseph Mitola [24] that expands upon the capabilities of modern software defined radios. Software radios are modern devices that are crafted to be reconfigurable, flexible devices capable of transmitting multiple waveforms. The parameters of these waveforms–including modulation type, forward error correction coding and frequency band to name a few–can vary greatly. This is possible because of the reconfigurability of the signal processing software used to handle processing in software defined radios. The concept of cognitive radio expands upon the advent of software radio in that it adds a layer of cognition and decision making capability to the device by harnessing the processing abilities of software radio.

The *cognitive engine* model for cognitive radios is used to describe their intelligence architecture. This architecture is based off of the OODA–observe, orient, decide and act–coined by John Boyd. Figure 2.14 depicts a general decision flow architecture for a cognitive radio based on the OODA loop structure. A cognitive radio will use its sensing ability to assess its RF environment. It can then use policy knowledge to orient itself to an environment

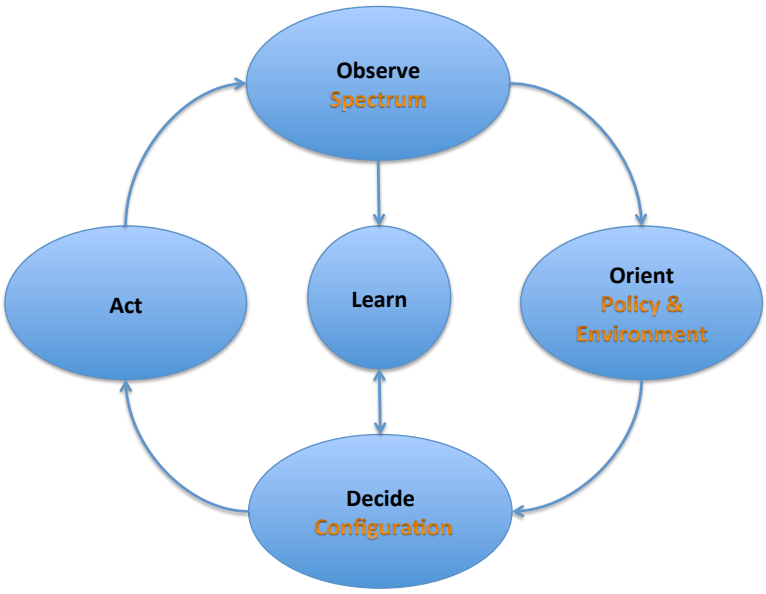

Figure 2.14: Cognitive radio decision flow architecture. A cognitive radio is constantly going through this loop in order to make decisions in and learn from its RF environment. Cognitive radios have the ability to sense their surrounding spectrum and make decisions, but they also theoretically have the ability to learn and update their strategies and policies.

and make a decision on the best course of action–be it to transmit in a certain band, leave a certain band, frequency hop, turn down transmit power, etc. The radio can then carry out this action by reconfiguring its own software. Cognitive radios also possess a unique capability to learn based on the observations and previous its observations and decisions and the impact that they have on one another.

The theoretical model of a cognitive radio lends itself to the idea of dynamic spectrum access networks. Radios utilizing DSA capabilities have to be able to perform rapid sensing and decision making in a dynamic RF environment in order to adhere to spectrum policy. Specifically, it is paramount that DSA radios using white space in licensed frequency bands avoid interference to licensed users. There have been a number of works on how to best measure to this interference and perform this task [25, 26, 27, 28, 29], and recent implementations have shown successful integration of DSA based devices in to TV white space [30, 31].

Advances in software defined radio capability through cognitive radio principles have allowed for dynamic spectrum access schemes to become realizable for wireless systems. This has in turn led to more a more complex range of application and capability ideas for DSA networks. With the expansion of this technology comes the challenges of securing these networks from malignant users. But in order to develop electronic warfare theory for DSA networks, it is necessary to understand the specific challenges and vulnerabilities that these networks present.

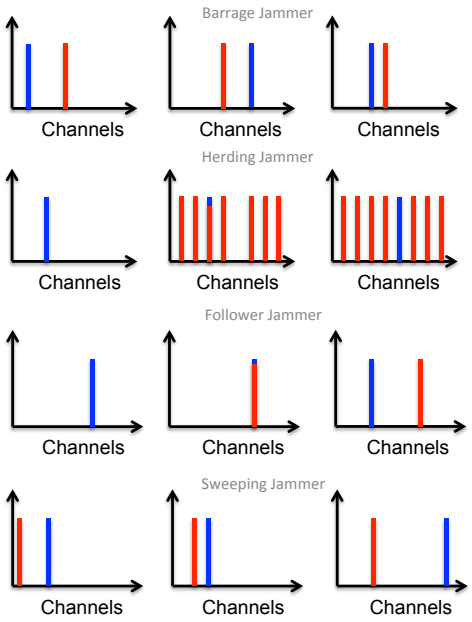

Figure 2.15: High level examples of DSA radio jammers. The blue bars represent DSA user energy and the red represents the malicious device. Four attacks are shown that target the DSA radios sensing capability. The barrage jammer occupies a single channel so that the DSA radio perceives it as unavailable, the herding jammer guides the DSA radio to a chosen channel, the follower jammer frequency hops with the DSA radio and the sweeping jammer moves incrementally across the channels in a given band.

2.2.3 Dynamic Spectrum Access Security Challenges

Dynamic spectrum access networks present a number of security challenges pertaining to network and device design. Because a dynamic spectrum access user will attempt to avoid interference to both itself and to licensed users, DSA device sensing becomes a target for jamming. A simple example is shown in Figure 2.15, where a DSA users policy is to not transmit on a channel where there is detectable interference present. An adversarial radio can perform a variety of attacks–including denial of service–by utilizing some of the attacks shown. Scenarios like these highlight the importance of critical sensing and analysis of an RF environment by the radios in a DSA capable network.

This type of scenario gives rise to the necessity of DSA radio identification algorithms. It is of interest for DSA radios to be able to classify different categories of radios in order to learn and update policy that impacts their cognitive process. While ideally this type of system could be developed using database knowledge as a reference point, the threat of unknown malicious radios requires the use of real time learning in order to identify and mitigate potential threats.

There are a couple of methods by which a DSA radio could automatically classify other devices through sensing information–this problem is of great interest to both the attack and security sides of the electronic warfare theory. Waveform classification and specific emitter identification (SEI) are areas which aim to solve this problem of radio classification.

However, for DSA radios we already have a behavioral architecture from Figure 2.14 that lends itself to stochastic classification algorithms. Due to the fact that cognitive radios with different intentions have a different set of parameters controlling their decision engine, it makes sense to use a behavior based identification system in order to classify these devices. In Chapter 5, we will discuss the underlying theoretical motivation for this type of classification model and show its viability even for radios with very similar decision engines.

Chapter 3

Orthogonal Frequency Division Multiplexing Synchronization Attacks

Orthogonal Frequency Division Multiplexing (OFDM) has become a leading modulation scheme in modern communications systems because of its spectral efficiency, achievable data rates, and robustness in multipath fading environments. However, it has been shown that current implementations of OFDM are susceptible to a variety of signal jamming attacks [18]. Various efficient jamming attacks which target the pilot tones used by OFDM communications systems have been derived. While this is one aspect of communicating with OFDM which must be improved, it is not the only area of weakness to an intentional adversarial attack.

As discussed in Section 2.1.1, one of the most important prerequisites for communicating using OFDM is synchronization between the transmitter and the receiver. Both timing and frequency synchronization are necessary in order to avoid inter-symbol interference (ISI), as well as inter-carrier interference (ICI) and loss of orthogonality among OFDM subcarriers. A number of algorithms have been developed in order to efficiently and robustly perform the synchronization [9, 10, 11, 12, 13].

While there has been some research conducted on analyzing and improving the robustness of OFDM synchronization algorithms [32, 33, 34, 35, 36], the majority of this work has been conducted under the assumption of uncorrelated or narrowband interference. In this chapter, we look at specific adversarial signals which are highly correlated to the synchronization symbols and designed with the intent of disrupting the communication of a transmitter and receiver using OFDM during the synchronization stage.

3.1 Synchronization Model Analysis

In order to determine the relative impact that the electronic warfare tactics presented in this paper, it is important to develop some frame of reference for the performance of OFDM synchronization without the presence of adversarial signals. In order to do this, the following section analyzes the performance of the OFDM synchronization estimators in the presence of only AWGN and multipath interference. We can then use the results from this section to measure the relative impact of the cognitive attacks presented in this paper.

3.1.1 Timing Acquisition Analysis

After baseband conversion and resampling, the OFDM will have a series of complex samples that compose the search range for the preamble symbol. These samples will be randomly shifted in frequency subject to the clock error between the transmitter and receiver, limited to the allowable range of offset between these two devices. We make the assumption that the offset is approximately constant over the duration of the training sequence. The sequence at the receiver is represented by

$$r_n = \left(\sum_{k=0}^{C-1} x_{n-k} h_k \right) e^{(2\pi j \frac{f}{f_s} n)} + n_n \tag{3.1}$$

where x is the samples of the training symbol sent, h represents the impulse response of the channel with length C, f represents the frequency offset between the transmitter and receiver clocks, and the term n represents noise. Substituting this term in to (2.19) yields

$$\begin{aligned} P(d) = \sum_{m=0}^{L-1} \left(\sum_{k=0}^{C-1} x^*_{d+m-k} h^*_k e^{(-2\pi j \frac{f}{f_s}(d+m))} + n^*_{(d+m)} \right) \cdot \\ \left(\sum_{k=0}^{C-1} x_{d+m+L-k} h_k e^{(2\pi j \frac{f}{f_s}(d+m+L))} + n_{d+m+L} \right) \end{aligned} \tag{3.2}$$

By approximating the cross correlation terms arising from the noise as zero, we can see that

$$P(d) = \sum_{m=0}^{L-1} \left(\sum_{k=0}^{C-1} x^*_{d+m-k} h^*_k \right) \left(\sum_{k=0}^{C-1} x_{d+m+L-k} h_k \right) e^{(2\pi j \frac{f}{f_s} L)} \tag{3.3}$$

Looking at the timing plateau where $\hat{d} \leq d \leq \hat{d} + (T_{cp} - T_{ch}) f_s$, we can simplify this expression based on the fact that the first preamble symbol is repeated over two half symbol periods, excluding the prefix, as indicated in [14]. This means that values spaced L samples apart are identical. This means that (3.3) can be simplified to

$$P(d) = \sum_{m=0}^{L-1} \left| \sum_{k=0}^{C-1} x_{d+m-k} h_k \right|^2 e^{(2\pi j \frac{f}{f_s} L)} \tag{3.4}$$

We can also use (3.1) to determine the what the receiver will estimate for $R(d)$ based on (2.20). Examining this result along the same plateau where $\hat{d} \leq d \leq \hat{d} + (T_{cp} - T_{ch})f_s$

$$R(d) = \sum_{m=0}^{L-1} \left(\left| \sum_{k=0}^{C-1} x_{d+m-k} h_k + n_{d+m} \right| \right)^2 \tag{3.5}$$

Applying the triangle inequality for complex numbers, this becomes

$$R(d) \leq \sum_{m=0}^{L-1} \left(\left| \sum_{k=0}^{C-1} x_{d+m-k} h_k \right| + |n_{d+m}| \right)^2 \tag{3.6}$$

Combining this result with (2.21) and (3.4) gives us

$$M(d) \geq \frac{\left(\sum_{m=0}^{L-1} \left| \sum_{k=0}^{C-1} x_{d+m-k} h_k \right|^2 \right)^2}{\left(\sum_{m=0}^{L-1} \left(\left| \sum_{k=0}^{C-1} x_{d+m-k} h_k \right| + |n_{d+m}| \right)^2 \right)^2} \tag{3.7}$$

We subsequently define

$$\sigma_{xc}^2 = \sum_{m=0}^{L-1} \left| \sum_{k=0}^{C-1} x_{d+m-k} h_k \right|^2 \tag{3.8}$$

as the total power of the entire channel affected OFDM symbol and

$$\sigma_n^2 = \sum_{m=0}^{L-1} |n_{d+m}|^2 \tag{3.9}$$

as the total noise power over one OFDM symbol period. We then utilize the fact that

$$2 \sum_{m=0}^{L-1} \left| \sum_{k=0}^{C-1} x_{d+m-k} h_k \right| |n_{d+m}| \leq 2\sigma_{xc}\sigma_n \tag{3.10}$$

with the relationship in (3.7) to obtain

$$M(d) \geq \frac{\sigma_{xc}^4}{\left(\sigma_{xc}^2 + 2\sigma_{xc}\sigma_n + \sigma_n^2\right)^2} \tag{3.11}$$

Rearranging terms and noting that

$$SNR = \frac{\sigma_{xc}^2}{\sigma_n^2} \tag{3.12}$$

produces the result

$$M(d) \geq \frac{1}{(1 + \frac{1}{\sqrt{SNR}})^4} \tag{3.13}$$

This lower bound gives an idea of the strength of the timing peak relative to SNR.

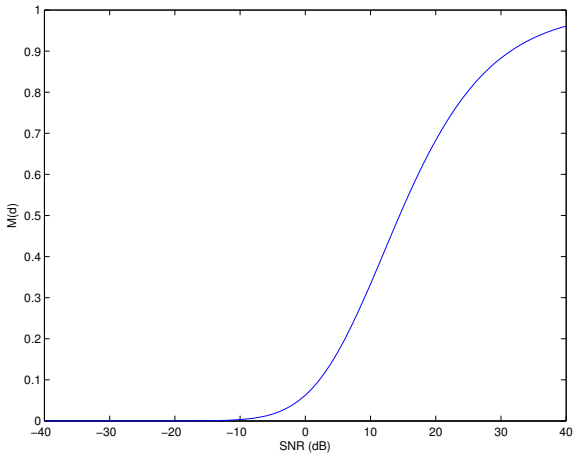

Figure 3.1: Lower bound on the peak value of the timing metric plateau relative to SNR

3.1.2 Carrier Frequency Offset Estimate Analysis

Assuming a multipath channel, white Gaussian noise and correct timing acquisition, the received preamble after conversion to baseband can be represented as

$$r_n = \left(\sum_{k=0}^{C-1} x_{n-k} h_k \right) e^{(2\pi j \frac{f}{f_s} n)} + n_n \tag{3.14}$$

where x_n represents the sampled preamble symbol, h_k represents a finite impulse response approximation of the multipath channel of length C, f represents the overall frequency error between the transmitter and receiver, f_s is the sampling frequency, and n_n represents the sampled additive Gaussian noise. We can analyze the fine frequency estimate in order to examine impacts of frequency domain attacks by substituting the signal as seen by the receiver in to the equation for $P(d)$; this yields

$$\begin{aligned} P(d) = \sum_{m=0}^{L-1} \left[\sum_{k=0}^{C-1} x^*_{d+m-k} h^*_k e^{-2\pi j \frac{f}{f_s}(d+m)} + n^*_{d+m} \right] \cdot \\ \left[\sum_{k=0}^{C-1} x_{d+m+L-k} h_k e^{2\pi j \frac{f}{f_s}(d+m+L)} + n_{d+m+L} \right]. \end{aligned} \tag{3.15}$$

This equation hinges on the assumption that the channel seen by the receiver is constant during one symbol period, an assertion that OFDM equalization is also based on. By expanding this equation and eliminating the cross terms, $P(d)$ approximates to

$$P(d) \approx \sum_{m=0}^{L-1} \left(\sum_{k=0}^{C-1} x^*_{d+m-k} h^*_k e^{-2\pi j \frac{f}{f_s}(d+m)} \right) \cdot \left(\sum_{k=0}^{C-1} x_{d+m+L-k} h_k e^{2\pi \frac{f}{f_s} f(d+m+L)} \right). \tag{3.16}$$

Coupling the assumption that a correct timing point is taken with the fact that the first preamble symbol repeats itself at a spacing of L samples over all the correct timing points, this equation becomes

$$P(d) \approx \sum_{m=0}^{L-1} \left| \sum_{k=0}^{C-1} x_{d+m-k} h_k \right|^2 e^{2\pi j \frac{f}{f_s}(L)}. \tag{3.17}$$

Equation (3.17) portrays the dominant term of the term $P(d)$ at any of the correct timing points. Noting that this result is in phasor form, along with the fact that

$$L = \frac{1}{2} T f_s \tag{3.18}$$

it is clear that the fractional frequency offset of the preamble symbol will be $\Delta f \approx \text{frac}\{f\}$. Since the exponential term can be divided in to two terms

$$e^{\pi j T f} = e^{\pi j T \text{frac}\{f\}} e^{\pi j \text{int}\{f\}} = \pm e^{\pi j T \text{frac}\{f\}}. \tag{3.19}$$

This term provides the fractional frequency offset only. The ambiguity due to the integer portion of the frequency offset can be disregarded as long as the partial frequency offset is always corrected in the same direction. The coarse frequency correction process will correct for the remaining frequency offset. The symbols can then be multiplied by a complex exponential to correct for the fine frequency error. In the frequency domain this represents the subcarriers being properly aligned in to bins. Once the fine frequency offset has been computed and corrected for, the frequency domain result will be the original symbol, with a frequency shift of an integer number of bins.

Once the fine frequency offset estimate is obtained and corrected for by multiplication of a complex exponential, the coarse frequency offset must be computed according to equation (2.23). The terms $R_{1,k}$ and $R_{2,k}$ represent the FFT of the first and second preamble symbol samples taken at the receiver after fine frequency correction, and are defined as

$$R_{i,k} = \sum_{n=0}^{2L-1} r_{n+N(i-1)} e^{-2\pi j k n / 2L}, \tag{3.20}$$

where

$$N = f_s \frac{T_{wp}}{2} \tag{3.21}$$

represents the number of samples in half of the preamble symbol period T_{wp}, which includes the cyclic prefix. Assuming perfect fine frequency correction, the received samples r_n are represented by

$$r_n = \left(\sum_{k=0}^{C-1} x_{n-k} h_k \right) e^{(2\pi j \frac{\text{int}_{(f)}}{f_s} n)} + n_n. \tag{3.22}$$

The first term in (3.22) is an approximation of the discrete convolution of the channel and the signal output by the transmitter. The length C in (3.22) and the complex weights h_k depend on the characteristics of the multipath channel. The channel affected signal is multiplied with a phase shift where $\text{int}(f)$ is an integer value corresponding to the remaining coarse frequency shift and uncorrelated noise is added.

Based on the structure of the preamble

$$|X_{1,k}|^2 = \begin{cases} p^2 & : k \in \mathcal{Y} \\ 0 & : k \notin \mathcal{Y} \end{cases} \tag{3.23}$$

and

$$|X_{2,k}|^2 = \begin{cases} \frac{1}{2}p^2 & : k \in \mathcal{B} \\ 0 & : k \notin \mathcal{B} \end{cases} \tag{3.24}$$

where $\mathcal{Y}$ is the subset of $\mathcal{X}$ which contains all even or odd subcarriers not part of the guard interval. $\mathcal{B}$ is the subset of all of the subcarriers excluding the guardband. The term p^2 is a constant proportional to the transmitted power of the preamble. The power on each subcarrier is halved for the second preamble symbol since it occupies both even and odd subcarriers. We also define

$$|N_k|^2 = p_n^2 \tag{3.25}$$

as the noise power over each OFDM subcarrier, which is assumed to be a constant. We define the total signal power of one preamble symbol at the receiver as

$$\sigma_{xc}^2 = \sum_{k\in\mathcal{X}} |H_k|^2|X_{1,k}|^2 = \sum_{k\in\mathcal{A}} |H_k|^2|X_{2,k}|^2, \tag{3.26}$$

where the set $\mathcal{A}$ represents all subcarriers, and the total noise power over one symbol as

$$\sigma_n^2 = \sum_{k\in\mathcal{A}} |N_k|^2. \tag{3.27}$$

By combining (3.23) with equations (2.23) and (2.24) with the fact that, we see that

$$B(g) = \frac{\left|\sum_{k\in\mathcal{X}} R_{1,k+2g}^* X_{1,k} X_{2,k}^* R_{2,k+2g}\right|^2}{p^4(\sum_{k\in\mathcal{X}} |R_{2,k}|^2)^2} \tag{3.28}$$

Incorporating equations (3.20) and (3.22) in the coarse offset estimator yields

$$B(g) = \frac{\left|\sum_{k\in\mathcal{X}} (H_{k-f+2g}^* X_{1,k-f+2g}^* + N_{1,k}^*) X_{1,k} X_{2,k}^* (X_{2,k-f+2g} H_{k-f+2g} + N_{2,k})\right|^2}{p^4\left(\sum_{k\in\mathcal{X}} |X_{2,k-f} H_{k-f} + N_k|^2\right)^2} \tag{3.29}$$

We can expand the numerator and rearrange the summations to show that

$$\begin{aligned}&\Bigg|\sum_{k\in\mathcal{X}}|H_{k-f+2g}|^2X_{1,k}X_{1,k-f+2g}^*X_{2,k-f+2g}X_{2,k}^*\\&+\sum_{k\in\mathcal{X}}X_{2,k-f+2g}X_{2,k}^*X_{1,k}H_{k-f+2g}N_{1,k}^*\\&+\sum_{k\in\mathcal{X}}X_{1,k}X_{1,k-f+2g}^*X_{2,k}^*H_{k-f+2g}^*N_{2,k}\\&+\sum_{k\in\mathcal{X}}X_{1,k}X_{2,k}^*N_{1,k}^*N_{2,k}\Bigg|^2.\end{aligned}\tag{3.30}$$

Due to the uncorrelated nature of the noise, the first term of the numerator will dominate. Therefore, it is reasonable to make the approximation that

$$B(g)\approx\frac{\left|\sum_{k\in\mathcal{X}}|H_{k-f+2g}|^2X_{1,k}X_{1,k-f+2g}^*X_{2,k-f+2g}X_{2,k}^*\right|^2}{p^4\left(\sum_{k\in\mathcal{X}}|X_{2,k-f}H_{k-f}+N_k|^2\right)^2},\tag{3.31}$$

noting that the numerator is only affected by the non-zero set of subcarriers $\mathcal{Y}$ which are not in the guardband.

There are two cases to consider regarding equation (3.30). The first scenario to analyze is when $2g=f$. In this case (3.31) becomes

$$B(g)\approx\frac{\left|\sum_{k\in\mathcal{X}}|H_k|^2|X_{1,k}|^2|X_{2,k}|^2\right|^2}{p^4\left(\sum_{k\in\mathcal{X}}|X_{2,k-f}H_{k-f}+N_k|^2\right)^2}\tag{3.32}$$

which, according to (3.24), simplifies to

$$B(g_{max})=\frac{\left|\frac{1}{2}\sum_{k\in\mathcal{Y}}|H_k|^2|X_{1,k}|^2\right|^2}{\left(\sum_{k\in\mathcal{X}}|X_{2,k-f}H_k+N_k|^2\right)^2}\tag{3.33}$$

or

$$B(g_{max})=\frac{\left(\frac{1}{2}\sigma_{xc}^2\right)^2}{\left(\sum_{k\in\mathcal{X}}|X_{2,k-f}H_k+N_k|^2\right)^2}.\tag{3.34}$$

The triangle inequality for complex numbers shows that

$$|X_{2,k-f}H_k+N_k|\leq|X_{2,k-f}H_k|+|N_k|.\tag{3.35}$$

Bounding the coarse frequency estimate at g_{max} by

$$B(g_{max})\geq\frac{\left(\frac{1}{2}\sigma_{xc}^2\right)^2}{\left(\sum_{k\in\mathcal{X}}(|X_{2,k-f}||H_k|+|N_k|)^2\right)^2},\tag{3.36}$$

then expanding, we see that

$$B(g_{max}) \geq \frac{\left(\frac{1}{2}\sigma_{xc}^2\right)^2}{\left(\sum_{k\in\mathcal{X}} |H_k|^2|X_{2,k-f}|^2 + 2|H_k||X_{2,k-f}||N_k| + |N_k|^2\right)^2}. \tag{3.37}$$

Utilizing the fact that

$$\sum_{k\in\mathcal{X}} |H_k||X_{2,k-f}||N_k| \leq \sqrt{\sum_{k\in\mathcal{X}} |H_k||X_{2,k-f}|^2 \sum_{k\in\mathcal{X}} |N_k|^2}, \tag{3.38}$$

we slightly relax the bound so that (3.37) takes the form

$$B(g_{max}) \geq \frac{\left(\frac{1}{2}\sigma_{xc}^2\right)^2}{\left(\frac{1}{2}\left(\sigma_{xc}^2 + 2\sqrt{\sigma_{xc}^2\sigma_n^2} + \sigma_n^2\right)\right)^2}. \tag{3.39}$$

Based on the definition

$$SNR = \frac{\sigma_{xc}^2}{\sigma_n^2}, \tag{3.40}$$

this equation results in the relationship

$$B(g_{max}) \geq \frac{1}{\left(1 + \frac{1}{\sqrt{SNR}}\right)^4}. \tag{3.41}$$

This bound yields an idea of how strong we can guarantee the peak of the coarse frequency correlation to be.

The second scenario is when $2g \neq f$, meaning that the coarse frequency estimate is incorrect. In this scenario, the values of $X_{1,k}$ and $X_{2,k}$ are an independent and identically distributed sequence of random variables. Specifically, we assume these values to be distributed according to

$$X_{i,k} = \frac{p}{\sqrt{2}^i} C_{i,k} + jD_{i,k}, \quad i = 1, 2; k \in \mathcal{Y}, \tag{3.42}$$

where

$$C_{i,k} = 2A_{i,k} - 1, D_{i,k} = 2B_{i,k} - 1, \tag{3.43}$$

and

$$A_{i,k}, B_{i,k} \sim \text{Bern}(\frac{1}{2}). \tag{3.44}$$

The channel frequency values H_k can be modeled as a set of complex dependent Gaussian random variables according to

$$H_k = C_k + jD_k, \tag{3.45}$$

where

$$C_k, D_k \sim \mathcal{N}(0, \frac{p_c}{2}). \tag{3.46}$$

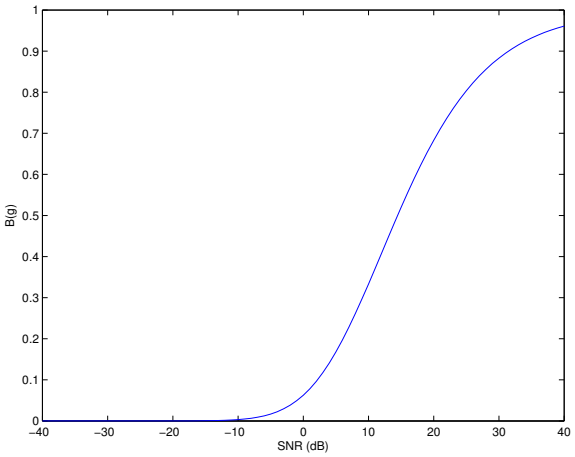

Figure 3.2: Lower bound on the coarse frequency offset estimator peak at the correct frequency offset relative to the effective SNR after channel fading.

The term p_c represents the average power of the wireless channel across all of the active subcarriers, specifically

$$p_c = \frac{1}{|\mathcal{B}|} \sum_{k \in \mathcal{B}} |H_k|^2 \tag{3.47}$$

where $|\mathcal{B}|$ represents the size of the set $|\mathcal{B}|$. Under this model, each computed channel power spectral density value $|H_k|^2$ will be a scaled chi-square distributed random variable according to

$$|H_k|^2 \sim \frac{p_c}{2} \mathcal{X}^2(2), \tag{3.48}$$

which is equivalent to the exponential distribution

$$|H_k|^2 \sim \frac{p_c}{2} Exp(\frac{1}{2}) = \text{Exp}(\frac{1}{p_c}). \tag{3.49}$$

This means that the interior portion of the numerator of (3.31) can be modeled according to

$$|H_{k-f+2g}|^2 X_{1,k} X^*_{1,k-f+2g} X_{2,k-f+2g} X^*_{2,k} = E_k + jF_k. \tag{3.50}$$

In addition, for the product of the subcarrier symbols

$$X_{1,k} X^*_{1,k-f+2g} X_{2,k-f+2g} X^*_{2,k} = W_k + jZ_k \tag{3.51}$$

a simple variance calculation yields

$$VAR[W_k] = VAR[Z_k] = p^4. \tag{3.52}$$

Due to the independence of the channel response and the frequency domain samples of the received signal the variance of E_k and F_k will be

$$VAR[E_k] = VAR[F_k] = 2p_c^2p^4. \tag{3.53}$$

From this expression, each of these terms is summed across all of the subcarriers $k \in \mathcal{X}$. Due to the extremely weak dependence of the random variables, we then apply the central limit theorem to show that

$$\sum_{k\in\mathcal{Y}} E_k + jF_k \Rightarrow \sqrt{|\mathcal{Y}|}\mathcal{N}(0, 2p_c^2p^4) + j\sqrt{|\mathcal{Y}|}\mathcal{N}(0, 2p_c^2p^4). \tag{3.54}$$

Noting that

$$\sqrt{|\mathcal{Y}|}\mathcal{N}(0, 2p_c^2p^4) = \sqrt{2|\mathcal{Y}|}p_cp^2\mathcal{N}(0, 1) \tag{3.55}$$

we can then make the same observations as equations (3.48) and (3.49) to obtain

$$\frac{1}{p^4}\left|\sum_{k\in\mathcal{X}} |H_{k-f+2g}|^2 X_{1,k}X^*_{1,k-f+2g}X_{2,k-f+2g}X^*_{2,k}\right|^2 \sim \text{Exp}(\frac{1}{2|\mathcal{Y}|p_c^2}). \tag{3.56}$$

This means that the expected value of the numerator for the case where the coarse frequency estimate is incorrect is

$$E[\text{Exp}(\frac{1}{2|\mathcal{Y}|p_c^2})] = 2|\mathcal{Y}|p_c^2 = |\mathcal{B}|p_c^2. \tag{3.57}$$

We then note, based on our definitions in (3.26) and (3.46), that

$$|\mathcal{B}|p_c^2 = \sum_{k\in\mathcal{B}} |H_k|^2. \tag{3.58}$$

We use equations (3.24) and (3.26) to derive

$$\sum_{k\in\mathcal{B}} |H_k|^2 = \frac{2\sigma_{xc}^2}{p^2}. \tag{3.59}$$

Since the denominator for both cases will be the same, we represent the numerator of (3.39) in these terms to show

$$\left(\frac{1}{2}\sigma_{xc}^2\right)^2 = \frac{1}{16}|\mathcal{B}|^2p_c^4p^4. \tag{3.60}$$

Taking the ratio of the numerator in (3.39) and the expected value of the numerator from (3.57), we see that the ratio of the lower bound on the estimate at the correct frequency to the expected value of the incorrect estimates is

$$\frac{min[B(g_{max})]}{E[B(g \neq g_{max})]} = \frac{1}{16}|\mathcal{B}|p_c^2p^4. \tag{3.61}$$

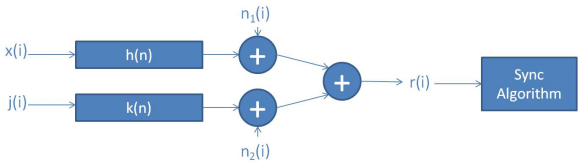

Figure 3.3: The physical jamming scenario

Converting this ratio to decibels yields

$$\frac{min[B(g_{max})]}{E[B(g \neq g_{max})]} \text{ dB} \approx 10\log(|\mathcal{B}|) + 20\log(p_c) + 40\log(p) - 12 \text{ dB}. \tag{3.62}$$

This result, combined with the lower bound from (3.41), helps to illustrate the performance of the correlation estimator in an environment without the presence of correlated adversarial signals.

3.2 System and Channel Model

In order to study some of the effects of adversarial signals on the OFDM synchronization process, a simple model was developed to imitate a realistic physical scenario. Within this basic model there are three main signals involved which represent the transmitter, receiver and the jammer. The transmitter and the jammer broadcast signals x and j, which then pass through two unique multipath channels h and k, respectively. These channels can be modeled as finite length digital filters white Gaussian noise is added to each signal at a fixed signal to noise ratio (SNR). The received signal is the aggregate of both the transmitter and jammer signal after the addition of channel effects and noise. In this case, the received vector r is

$$r_n = \left(\sum_{k=0}^{C-1} x_{n-k}h_k\right) e^{(2\pi j \frac{f}{f_s} n)} + \alpha \left(\sum_{i=0}^{K-1} j_{n-i}k_i\right) e^{(2\pi j \frac{f_j}{f_s} n)} + n_n \tag{3.63}$$

where h_k and k_i are the impulse responses of the channel that the receiver and the jammer sees, respectively, of lengths C and K. The values f and f_j represent the relative frequency offsets of the receiver with the transmitter and the jammer, and n is a vector of white Gaussian noise.

The power of the transmitter is assumed to be fixed, while the power output of the jammer can vary based on the attack signal. This scenario gives rise to the signal-to-jammer ratio (SJR)

$$SJR = 10\log(\alpha^2) = 20\log(\alpha) \tag{3.64}$$

which will be used as one metric of efficiency of an attack signal.

There are some underlying assumptions which help further describe the jamming scenario. It is, of course, assumed that there are clock errors between the transmitter and the receiver, but in a real environment there will also be clock error between the jammer and the other two parties. It is therefore assumed that the jammer has previous knowledge of the timing and frequency recovery algorithm. It is also assumed that the jammer has knowledge of the preamble structure used in OFDM synchronization[1]. These pieces of knowledge will be the baseline for all of the attacks presented (with the exception of channel whitening, which only requires knowledge of the channel frequency and bandwidth). Some attacks will require additional knowledge of the jamming environment, while other attacks will be effective based on only these assumptions.

The scope of this paper is focused on negatively impacting the symbol timing estimation at the first stage of the synchronization process. There are some important analytical models which help characterize the jamming signals impact on this metric. Substituting the aggregate of the transmitter and the jammer signal in to (2.19) yields

$$\begin{aligned} P(d) = \sum_{m=0}^{L-1} \left[\left(\sum_{k=0}^{C-1} x^*_{d+m-k} h^*_k \right) e^{-2\pi j \frac{f}{f_s}(d+m)} + \alpha \left(\sum_{i=0}^{K-1} j^*_{d+m-i} k^*_i \right) e^{-2\pi j \frac{f_j}{f_s}(d+m)} \right] \cdot \\ \left[\left(\sum_{k=0}^{C-1} x_{d+m+L-k} h_k \right) e^{2\pi j \frac{f}{f_s}(d+m+L)} + \alpha \left(\sum_{i=0}^{K-1} j_{d+m+L-i} k_i \right) e^{-2\pi j \frac{f_j}{f_s}(d+m+L)} \right] \end{aligned} \tag{3.65}$$

By expanding this equation, we can establish the basic analytical model which will describe each of the jamming signals' impact on the timing metric at the receiver.

$$\begin{aligned} P(d) = \sum_{m=0}^{L-1} \Bigg[& \left(\sum_{k=0}^{C-1} x^*_{d+m-k} h^*_k \right) \left(\sum_{k=0}^{C-1} x_{d+m+L-k} h_k \right) e^{2\pi j \frac{f}{f_s} L} \\ & + \alpha \left(\sum_{k=0}^{C-1} x^*_{d+m-k} h^*_k \right) \left(\sum_{i=0}^{K-1} j_{d+m+L-i} k_i \right) e^{2\pi j \frac{f_j - f}{f_s}(d+m)} e^{2\pi j \frac{f_j}{f_s} L} \\ & + \alpha \left(\sum_{i=0}^{K-1} j^*_{d+m-i} k^*_i \right) \left(\sum_{k=0}^{C-1} x_{d+m+L-k} h_k \right) e^{2\pi j \frac{f - f_j}{f_s}(d+m)} e^{2\pi j \frac{f}{f_s} L} \\ & + \alpha^2 \left(\sum_{i=0}^{K-1} j^*_{d+m-i} k^*_i \right) \left(\sum_{i=0}^{K-1} j_{d+m+L-i} k_i \right) e^{2\pi j \frac{f_j}{f_s} L} \Bigg] \end{aligned} \tag{3.66}$$

The noise terms have been left out in these derivations for the sake of brevity and simplicity. In these cases the noise term will have an impact, but if the transmitter and jammer signals are above the noise floor then the impact can be neglected in the interest of analyzing the impact of the jammer.

[1]If the jammer is targeting a known signal standard, then this information would readily be available when constructing the jamming attack.

In addition, we define the scenarios in which the jammer has channel knowledge. In this case, the jamming signal $\hat{j}_n$ is defined as

$$\hat{j}_n = \alpha \left(\sum_{l=0}^{K-1} p_{n-l} k_l^{-1} \right) e^{(2\pi j \frac{f_j}{f_s} n)} \tag{3.67}$$

where

$$p_n = \left(\sum_{i=0}^{C-1} j_{n-i} h_i \right) \tag{3.68}$$

where j_n is the jamming signal dependent on the attack, k^{-1} is the inverse jammer channel response such that $k^{-1} = \text{FFT}^{-1}(1/\text{FFT}(k))$, and $|\alpha| > 0$. In addition, f_j represents the frequency offset of the jamming signal at the receiver, which in most cases will be made to match the offset of the preamble at the receiver.

3.3 Jamming Attacks

While the synchronization process described by Schmidl and Cox can be considered robust within *friendly* communications environments, there are many weaknesses to the algorithm were it to be intentionally and intelligently attacked. These jamming strategies allow adversaries to be efficient relative to simple channel whitening. Even based on the importance of timing and frequency recovery alone, a more efficient attack than channel whitening presents itself as whitening only during preamble transmission. Some of the potential weaknesses lie both within the timing recovery and the frequency recovery. It is interesting to note that, while OFDM is much more sensitive to errors in the estimation of carrier frequency offset than symbol timing, there are still various ways in which synchronization could be disrupted by creating error in either or both values. While it is not yet clear which jamming strategy would be the most efficient against OFDM synchronization in terms of power and denial rate, there are many possible candidates.

3.3.1 Timing Acquisition Attacks

Symbol timing acquisition is generally the first stage of OFDM acquisition at a receiver. A malicious attack against this process can effectively prevent a transmitter and receiver from communicating. This section outlines a series of efficient attacks that are capable of denying service to an OFDM receiver by targeting the symbol timing acquisition process.

Barrage Jamming Attacks

There are two types of basic jamming attacks which perform barrage attacks. Though they are not explicitly covered in this paper, they are important to mention as the most basic attacks against OFDM. The first is a continuous white noise jammer which aims to raise the noise floor at the receiver in order to degrade communication. This is the most inefficient and least intelligent jammer, and can serve as a baseline for comparing the efficiencies of other jammers. The second type of barrage attack, preamble whitening, is slightly more efficient and intelligent, though it still relies on uncorrelated noise in order to disrupt communications. This jammer raises the noise floor only during the synchronization phase, effectively trying to drown out the preamble symbols in order to jam the receiver.

Continuous White Noise Jamming

The continuous white noise jamming method is the most basic and inefficient attack discussed in this paper. It consists of transmitting white noise across the entire bandwidth of the OFDM channel at a power such that the noise floor at the receiver is too high for any communication to occur. The effects of this jammer will not show up in the analytical model of the timing metric, due to the uncorrelated nature of the white noise. Instead, this *barrage jammer* will degrade the effective SNR at the receiver, preventing the receiver from ever obtaining the preamble symbols, or any OFDM symbols for that matter. The required transmit power of this attack will be a direct function of the OFDM transmitter power and the required SNR at the receiver for demodulation.

Preamble Whitening

This attack is identical in concept to the previous barrage attack, except that instead of continuously jamming an OFDM channel with white noise, the jammer in this scenario only focuses on the preamble symbols. Using this attack will improve upon the efficiency of a jammer proportional to the size of the frames sent out by the transmitter. Since the preamble symbols are sent out at the beginning of each frame, this jammer aims to prevent the receiver from ever synchronizing properly with the transmitter, causing massive degradation in the overall throughput of the system. This attack requires the knowledge of the preamble structure. Due to the distinct format of the preamble symbols used in this synchronization algorithm, it would not require a particularly sophisticated jamming system to be able to lock on to the preamble symbols and disable communication with this attack.

This attack does improve temporal efficiency, but the power requirement of the attack is still significant. Figure 3.4 shows that the required power output by a jammer to impact timing estimation can be significant. The timing estimate is not adversely affected by AWGN until the SNR drops below -10 dB. As an alternative, efficient jammers can offer superior

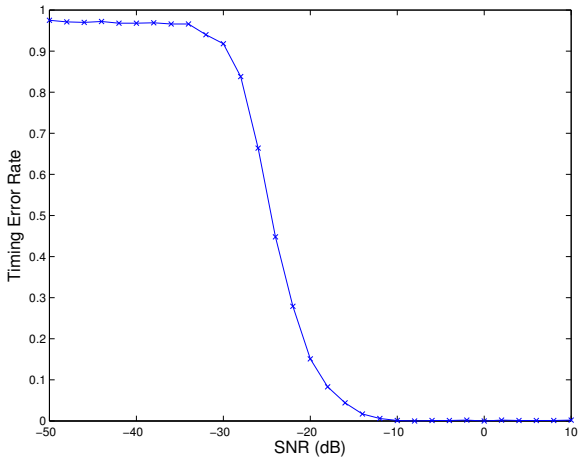

Figure 3.4: Timing estimate error as a function of the effective SNR at the receiver.

performance degradation to OFDM signals at much lower jammer powers by exploiting the inherent features of OFDM.

These barrage attacks can still provide a useful baseline for jammer efficiency. In a scenario where an OFDM transmitter and receiver synchronize once every n symbols, preamble whitening will offer a savings of

$$P_{sav} = 10\log(n\frac{P_{cw}}{P_{pw}}) \text{ dB} \tag{3.69}$$

in transmit energy compared with what a continuous white noise jammer would require. P_{cw} is defined as the average transmit power of the continuous white noise barrage jammer and P_{pw} is the average transmit power of the preamble whitening jammer. These terms will depend on the average power requirements of each jammer to accomplish its individual goal. This, of course, comes at the cost of the preamble whitener being able to sense and/or predict when the transmitter and receiver are attempting to perform synchronization. In general, the more efficient that these jammers become, the more cognition and implicit knowledge of OFDM systems they require.

False Preamble Timing Attack

The main opportunities to efficiently disrupt symbol timing estimation lie within either moving the peak of the timing metric, or destroying it altogether. The first method is to create a new timing metric peak. Based on the knowledge that the jammer has about the preamble, this can either be a retransmission of the preamble, a different preamble symbol altogether or the transmission of the correct preamble at the incorrect time. If the false

timing preamble is transmitted at a higher power, then the peak of the overall timing metric will be taken at the wrong place, and can destroy the symbol timing estimation.

The impact of this attack on the timing metric can be derived via (3.66). In this case, the attack signal can either be a copy of the preamble sent by the transmitter, or more generally can be a preamble symbol constructed with any PN sequence. The only requirement is that the jamming signal be of the preamble form. For this general case, the resulting timing metric numerator that the receiver sees will take the form

$$\begin{aligned} P(d) = \sum_{m=0}^{L-1} \Bigg[\left| \sum_{k=0}^{C-1} x_{d+m-k} h_k \right|^2 + \alpha \left(\sum_{k=0}^{C-1} x^*_{d+m-k} h^*_k \right) \left(\sum_{i=0}^{K-1} j_{d+m-i} k_i \right) \\ + \alpha \left(\sum_{i=0}^{K-1} j^*_{d+m-i} k^*_i \right) \left(\sum_{k=0}^{C-1} x_{d+m-k} h_k \right) + \alpha^2 \left| \sum_{i=0}^{K-1} j_{d+m-i} k_i \right|^2 \Bigg]^2 \end{aligned} \tag{3.70}$$

From this point there are two main cases: when the two preambles overlap and when they do not. We assume that the jamming symbol is sent so that there is significant separation between its timing metric plateau and the preamble's, specifically such that $\{N \in \mathbb{R} \mid |N| > T_{cp} f_s\}$ where N is the delay of the false preamble relative to the correct one. This is the optimal strategy for the jammer to make the receiver miss the timing point.

The first case is based around when $|N| > T_{sym} f_s$ and there is no overlap between the timing preamble symbols. This will simplify (3.70) to

$$P(d) = \sum_{m=0}^{L-1} \left| \sum_{k=0}^{C-1} x_{d+m-k} h_k \right|^4 + \alpha^4 \left| \sum_{i=0}^{K-1} j_{d+m-i} k_i \right|^4 \tag{3.71}$$

From here, we incorporate the lower bound from (3.13) and split the two plateaus to show that

$$M(d) > \begin{cases} \frac{1}{(1+\frac{1}{SNR})^2} & : d \in \hat{D} \\ \frac{1}{(1+\frac{1}{\alpha^2 JNR})^2} & : d \in \hat{D} - N \end{cases} \tag{3.72}$$

where $\hat{D}$ represents the range of the timing metric plateau for the preamble, $\hat{D} - N$ represents that range shifted by the delay N of the false preamble and JNR represents the jammer to noise ratio determined by the symbol and jammer channel but independent of α.

The second case is when $T_{cp} f_s < |N| < T_{sym} f_s$ such that the two preambles overlap. In this case, the two cross terms are a factor since the signals overlap in time. However, the terms represent single points in the cross correlation between the two preambles. If the jammer has no channel information and the symbols are independent, then they approximate to zero either way. However, the case where the jammer has channel knowledge and sends the same symbol as the transmitter requires further analysis. In this case the numerator of the timing

metric becomes

$$P(d) = \sum_{m=0}^{L-1} \left[\left| \sum_{k=0}^{C-1} x_{d+m-k} h_k \right|^2 + \alpha \left(\sum_{k=0}^{C-1} x^*_{d+m-k} h^*_k \right) \left(\sum_{k=0}^{C-1} x_{d-N+m-k} h_k \right) \right.$$
$$\left. + \alpha \left(\sum_{k=0}^{C-1} x^*_{d-N+m-k} h^*_k \right) \left(\sum_{k=0}^{C-1} x_{d+m-k} h_k \right) + \alpha^2 \left| \sum_{k=0}^{C-1} x_{d-N+m-k} h_k \right|^2 \right]^2 \tag{3.73}$$

In order to analyze this equation we define $R_{y(d)y(d)}(l)$ as the autocorrelation function

$$R_{y(d)y(d)}(l) = \sum_{m=0}^{L-1} y_{d+m} y^*_{d+m-l} \tag{3.74}$$

where $y(d)$ represents the function of interest and l is the lag between the two functions. If we define

$$y_{d+m} = \sum_{k=0}^{C-1} x_{d+m-k} h_k \tag{3.75}$$

then (3.73) becomes

$$P(d) = R_{y(d)y(d)}(0) + \alpha R_{y(d-N)y(d-N)}(-N)$$
$$+ \alpha R_{y(d)y(d)}(N) + \alpha^2 R_{y(d-N)y(d-N)}(0) \tag{3.76}$$

In order to accurately compute these terms, knowledge about the autocorrelation function of both the OFDM signal and the channel are necessary, as suggested in [37]. The autocorrelation of the OFDM symbol can be derived based on the power spectral density (PSD) via the Einstein-Wiener-Khinchin Theorem. This is based on the fact that an OFDM signal is cyclostationary. The PSD of an OFDM symbol is a rectangular function over all subcarriers other than the guardband. The autocorrelation of an OFDM symbol is simply the inverse Fourier transform of its PSD. The resulting PSD of an OFDM symbol is therefore a relatively narrow sinc function, whose width is proportional to the size of the guardband in a particular implementation. This can be seen in Figure 3.5, where the computed autocorrelation of half of the timing preamble symbol is shown, after the stripping of the cyclic prefix. The autocorrelation function has a narrow main peak and does not show significant correlation anywhere other than zero lag. The channel autocorrelation can be estimated with a 0^{th} order Bessel function using the Jakes' model. Based on this modeling, it can be shown that the cross correlation terms have a relatively small impact on the peak of the timing metric, so the numerator can be represented as

$$P(d) \approx R_{y(d)y(d)}(0) + \alpha^2 R_{y(d-N)y(d-N)}(0) \tag{3.77}$$

The most interesting case for the overlapping scenario is when $|N| = L$. In this case the numerator will take the form

$$\begin{aligned} P(d) &= R_{y(d)y(d)}(0) + \alpha R_{y(d\pm L)y(d\pm L)}(\pm L) \\ &+ \alpha R_{y(d)y(d)}(\mp L) + \alpha^2 R_{y(d\pm L)y(d\pm L)}(0) \end{aligned} \tag{3.78}$$

which, based on the preamble structure, becomes

$$P(d) = (1+\alpha)R_{y(d)y(d)}(0) + \alpha(1+\alpha)R_{y(d\pm L)y(d\pm L)}(0) \tag{3.79}$$

This result will create two different scenarios for the timing metric plateau based on the normalization term $R(d)$, dictated by $N = L, -L$.

$$M(d) > \begin{cases} \frac{1}{(1+\alpha)^2(1+\frac{1}{SNR})^2} & : d \in \hat{D}, N = L \\ \frac{(1+\alpha)^2}{\alpha^2(1+\frac{1}{JNR})^2} & : d \in \hat{D} - N, N = L \end{cases} \tag{3.80}$$

$$M(d) > \begin{cases} \frac{1+\alpha}{(1+\frac{1}{SNR})^2} & : d \in \hat{D}, N = -L \\ \frac{\alpha^2}{(1+\alpha^2)(1+\frac{1}{JNR})^2} & : d \in \hat{D} - N, N = -L \end{cases} \tag{3.81}$$

This result shows that the an optimal strategy for the false preamble jammer is to transmit with a delay equal to L. This maximizes the power normalization term $R(d)$ without contributing to the timing metric peak in $P(d)$ caused by the transmitter's preamble. This lowers the bound on the timing metric peak $M(d)$. While all delay values $L \leq N \leq 2L$ will have this effect, the delay $N = L$ maximizes it. In addition, this effect will still make an impact even without channel or symbol knowledge.

Preamble Nulling Attack

Another method for degrading symbol timing would be to destroy the timing symbol by inversion. This attack would be carried out by a technique called preamble nulling. This attack would be predicated on the fact that the jammer has perfect knowledge of the preamble as viewed by the receiver. By inverting the preamble symbol in time a jammer would be able to destructively interfere with the preamble at the receiver, wiping out the timing metric peak. However, this method is also dependent on the relationship between the channel that the transmitter sees and the channel that the jammer sees. If these channels are the same or similar enough, or if both are known to the jammer, then this attack can be effective. Without knowledge of these underlying conditions the attack becomes less feasible.

The analytical impact of this jammer can also be derived using the relationships in equations (3.66)-(3.68). The nulling jammer is sent by making $j_n = -x_n$ and $f_j = f$. Substituting the

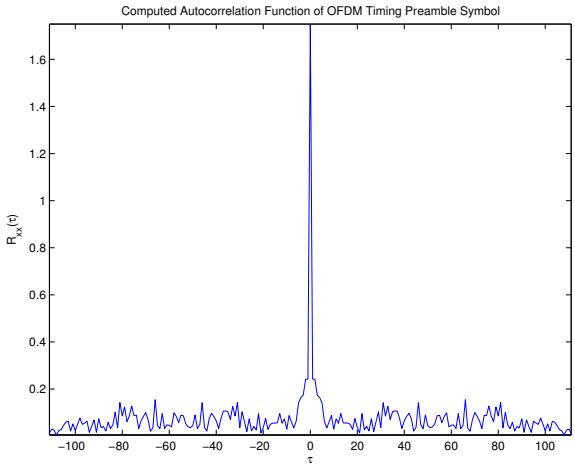

Figure 3.5: Computed autocorrelation of half of the first preamble symbol minus the cyclic prefix.

jamming waveform in to the (3.66) metric equations yields

$$P(d) = \sum_{m=0}^{L-1} \left[\left| \sum_{k=0}^{C-1} x_{d+m-k} h_k \right|^2 e^{2\pi j \frac{f}{f_s} L} - \alpha \left| \sum_{k=0}^{C-1} x_{d+m-k} h_k \right|^2 e^{2\pi j \frac{f_j - f}{f_s}(d+m)} e^{2\pi j \frac{f_j}{f_s} L} \right.$$
$$\left. - \alpha \left| \sum_{k=0}^{C-1} x_{d+m-k} h_k \right|^2 e^{2\pi j \frac{f - f_j}{f_s}(d+m)} e^{2\pi j \frac{f}{f_s} L} + \alpha^2 \left| \sum_{k=0}^{C-1} x_{d+m-k} h_k \right|^2 e^{2\pi j \frac{f_j}{f_s} L} \right] \tag{3.82}$$

The drawback with this attack is that in order to be effective, it requires that the power of the preamble symbol detected at the receiver be somewhere near the noise floor. However, (3.82), along with equations (3.67) and (3.68), show that there are various opportunities for error between the preamble and the nulling attack. In an implementation, it is hard to guarantee that α be such that $SJR = 0$ dB ($\alpha = 1$ in this case). In addition, there will be some slight errors in the channel estimation and inversion, plus some slight delay term based on the arrival of each signal.

Preamble Warping

Since the timing acquisition relies heavily on the correlation of the two halves of the first preamble symbol, another effective strategy for jamming is to destroy this correlation. This timing attack can be achieved by attacking the frequency domain structure of the preamble. As previously stated, the first preamble symbol can be created either with a half length IFFT and repeating it in the time domain, or by taking a full length IFFT in the frequency

domain where every other subcarrier is populated with a PN sequence. These methods are mathematically equivalent, so either one will result in a frequency domain representation where every other FFT bin is empty before the addition of the cyclic prefix. The idea behind the preamble warping attack is to transmit on the unused subcarriers of the preamble symbol in order to destroy time domain correlation.

Preamble warping essentially transforms the first symbol of the preamble in to a generic preamble symbol, albeit that the PN sequence is still present over one half-set of the subcarriers. By populating the unused subcarriers during timing acquisition, the attack aims to destroy timing correlation, causing the receiver to miss the timing point.

Analytically, the impact of the attack is actually better described starting from (3.66). In the case of the warping attack, the jamming signal will have the same form as the first preamble symbol. It is sent at the receiver frequency, but shifted over one frequency bin, such that

$$r_n = \left(\sum_{k=0}^{C-1} x_{n-k}h_k\right) e^{(2\pi j \frac{f}{f_s} n)} + \alpha \left(\sum_{i=0}^{K-1} j_{n-i}k_i\right) e^{(2\pi j (\frac{f}{f_s} + \frac{1}{2L}) n)} + n_n \tag{3.83}$$

Applying this result to the numerator of the timing metric, while once again disregarding the noise term, yields

$$P(d) = \sum_{m=0}^{L-1} \left[\left| \sum_{k=0}^{C-1} x_{d+m-k}h_k \right|^2 e^{2\pi j \frac{f}{f_s} L} + \alpha \left(\sum_{k=0}^{C-1} x^*_{d+m-k}h^*_k\right) \left(\sum_{i=0}^{K-1} j_{d+m+L-i}k_i\right) e^{2\pi j \frac{f}{f_s} L} e^{\pi j \frac{1}{L}(d+m+L)} \right.$$
$$\left. + \alpha \left(\sum_{i=0}^{K-1} j^*_{d+m-i}k^*_i\right) \left(\sum_{k=0}^{C-1} x_{d+m+L-k}h_k\right) e^{2\pi j \frac{f}{f_s} L} e^{-\pi j \frac{1}{L}(d+m+L)} + \alpha^2 \left| \sum_{i=0}^{K-1} j_{d+m-i}k_i \right|^2 e^{2\pi j \frac{f}{f_s} L} e^{\pi j} \right] \tag{3.84}$$

factoring out the constant phase term, using the time repetition properties of both sequences and noting that the middle terms are complex conjugates yields

$$\begin{aligned} P(d) = \sum_{m=0}^{L-1} \Bigg[& \left| \sum_{k=0}^{C-1} x_{d+m-k}h_k \right|^2 \\ & + 2\alpha \,\mathrm{Re}\left[\left(\sum_{k=0}^{C-1} x^*_{d+m-k}h^*_k\right) \left(\sum_{i=0}^{K-1} j_{d+m-i}k_i\right) e^{\pi j \frac{1}{L}(d+m+L)} \right] \\ & - \alpha^2 \left| \sum_{i=0}^{K-1} j_{d+m-i}k_i \right|^2 \Bigg] e^{2\pi j \frac{f}{f_s} L} \end{aligned} \tag{3.85}$$

The middle term represents a randomly phase shifted correlation between the transmitter symbol and the jammer symbol, which has an expected value of zero. Combining this with

the fact that the definition in (3.8) produces

$$P(d) = \sigma_{xc}^2 - \alpha^2 \sigma_{jk}^2 \tag{3.86}$$

For cases where σ_{xc}^2 and σ_{jk}^2 are close in value, it is optimal for the jammer to set $\alpha = 1$. This result shows that a jammer using this attack should adjust the value of α in order to match the power of the transmitted symbol at the receiver in order for this attack to be most effective. It also indicates that a scenario where the jammer has channel knowledge but does not use the exact same symbol as the transmitter is optimal. This way, the power terms for each of the symbols will be closest in value and the cross terms will still have an expected value of zero.

3.3.2 Carrier Frequency Offset Estimation Attacks

Carrier frequency offset estimation is the process by which an OFDM receiver mitigates the clock errors between itself and a transmitter. A malicious attack against this process can cause massive ICI, also destroying communication between a transmitter and receiver. This section outlines a series of efficient attacks that are capable of denying service to an OFDM receiver by targeting the carrier frequency offset estimation.

In order to measure the effectiveness of the attacks in this section, the root mean squared (RMS) error between the true frequency offset and the frequency offset estimation will serve as a metric for the effectiveness of the jamming attacks. This error is calculated as

$$e_{RMS} = \sqrt{< (f_{off} - f_{est})^2 >}, \tag{3.87}$$

where $< \cdot >$ is the mean, and will measure the accuracy of the frequency offset estimate.

This metric is important because it directly ties in with the degradation of SNR at the receiver, and subsequently synchronization system performance. This is because OFDM systems begin to suffer noticeable degradations in SNR for frequency offsets that are as little as 1% of the subcarrier spacing [7]. Based on the work done in [8], the degradation in SNR in dB at the receiver based on carrier frequency offset can be expressed as

$$D \approx \frac{10}{3ln(10)} (\pi \frac{\Delta F}{F})^2 \frac{E_s}{N_o}. \tag{3.88}$$

The term ΔF is defined as the frequency offset at the receiver, and the term F signifies the subcarrier or bin spacing in the OFDM symbols. The degradation is proportional to the E_s/N_o at the receiver, the ratio of energy per symbol to noise spectral density. This approximation assumes that the frequency offset is small relative to the bin spacing. Figure 3.6 illustrates the degradation in SNR for OFDM symbols based on the relative frequency offset using different digital modulations on the subcarriers. Using the marginal values for

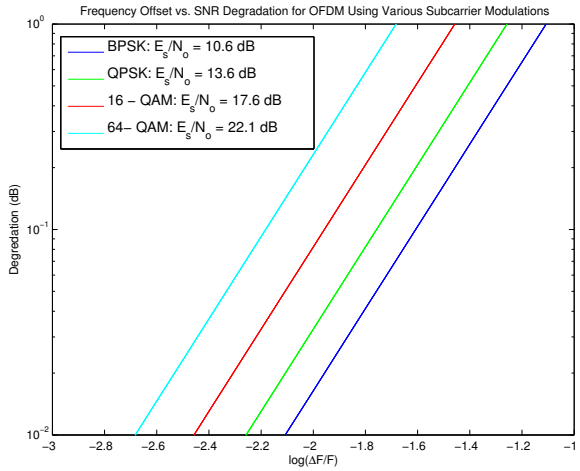

Figure 3.6: Degradation as a function of the relative frequency offset of received OFDM symbols using various subcarrier modulations

E_s/N_o for each of these modulations, it is clear that even slight errors in the fine frequency offset can have a significant impact on the effective SNR of an OFDM symbol at the receiver. This aspect of OFDM illustrates one of the glaring weaknesses of the synchronization process and highlights a definite susceptibility to adversarial signals.

Preamble Phase Warping

The first of the frequency based synchronization jamming attacks is preamble phase warping. This attack aims to disrupt the frequency offset estimate of the receiver by sending a frequency shifted preamble symbol to the receiver. While it is important to note that this type of attack could be used to change the overall frequency error estimate at the receiver, another important use of the attack would be to degrade the fine frequency estimate. By altering the fine frequency offset, this jamming attack can prevent the receiver from properly lining up the subcarriers in to frequency bins at the receiver. This results in massive ICI and subsequent degradation of SNR.

This attack can be analyzed using equation (3.15) by adding in the term

$$w_n = \left(\sum_{i=0}^{K-1} y_{n-i} k_i \right) e^{(2\pi j \frac{f_j}{f_s} n)} \tag{3.89}$$

at the receiver. By ignoring the noise cross correlation terms as in the original derivation,

we can see that

$$P(d) = \sum_{m=0}^{L-1}\sum_{k=0}^{C-1} |x_{d+m-k}h_k|^2 e^{2\pi j \frac{f}{f_s}L} + \alpha \sum_{i=0}^{K-1} y^*_{d+m-i}k^*_i e^{-2\pi j \frac{f_j}{f_s}(d+m)} \sum_{k=0}^{C-1} x_{d+m+L-k}h_k e^{2\pi j \frac{f}{f_s}(d+m+L)}$$
$$+ \alpha \sum_{k=0}^{C-1} x^*_{d+m-k}h^*_k e^{-2\pi j \frac{f}{f_s}(d+m)} \sum_{i=0}^{K-1} y_{d+m+L-i}k_i e^{2\pi j \frac{f_j}{f_s}(d+m+L)}$$
$$+ \alpha^2 \sum_{i=0}^{K-1} |y_{d+m-i}k_i|^2 e^{2\pi j \frac{f_j}{f_s}L}. \tag{3.90}$$

From here, there are two cases of interest. The first is when the jammer has no channel knowledge and sends an arbitrary preamble symbol. In this case, the fine frequency estimate will be based off of

$$P(d) = \sum_{m=0}^{L-1} \left(\sum_{k=0}^{C-1} |x_{d+m-k}h_k|^2 e^{2\pi j \frac{f}{f_s}L} + \alpha^2 \sum_{i=0}^{K-1} |y_{d+m-i}k_i|^2 e^{2\pi j \frac{f_j}{f_s}L}) \right) \tag{3.91}$$

which results in a two polar form complex numbers. The peak autocorrelation value of the transmitter's symbol and channel are stochastically identical to that of the jammer's symbol and channel, so their impact on the weighting of the timing metric angle is negligible. The resulting angle is determined according to the addition of angles of complex numbers, which yields the equation

$$\angle(P(d)) = \arctan\left(\frac{\sin(2\pi \frac{f}{f_s}L) + \alpha^2 \sin(2\pi \frac{f_j}{f_s}L)}{\cos(2\pi \frac{f}{f_s}L) + \alpha^2 \cos(2\pi \frac{f_j}{f_s}L)} \right). \tag{3.92}$$

Given two random angles, this function versus α, which is proportional to SJR, the resulting function which determines the angle of $P(d)$ is an S-shaped curve which converges towards the angle of the preamble at high SJRs and converges towards the angle of the jammer at low SJRs.

The second case is when the jammer has channel knowledge and sends the same symbol as the transmitter. In this case, the cross terms in (3.90) do not go to zero. The two cross terms between the jammer and transmitter signal are represented by the expression

$$\sum_{m=0}^{L-1} \alpha \left(\sum_{k=0}^{C-1} |x_{d+m-k}h_k|^2 e^{2\pi j \frac{f-f_j}{f_s}(d+m)} e^{-2\pi j \frac{f_j}{f_s}L} + \sum_{k=0}^{C-1} |x_{d+m-k}h_k|^2 e^{2\pi j \frac{-(f-f_j)}{f_s}(d+m)} e^{2\pi j \frac{f_j}{f_s}L} \right). \tag{3.93}$$

The term $\sum_{m=0}^{L-1} e^{2\pi j \frac{f-f_j}{f_s}(d+m)}$ can be modeled as a phasor with a random angle which is dependent on the jammer and transmitter frequencies and their phases at the receiver. This

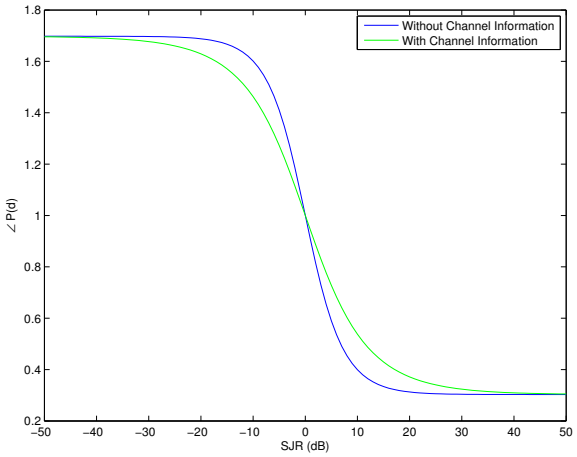

Figure 3.7: Estimate of the angle of $P(d)$ at the receiver based on the SJR of the phase warping attack with randomly generated frequency offsets. The estimate converges to the fractional frequency offset of the transmitter at high SJRs and the jammer at low SJRs.

term is represented as $a = e^{2\pi j\phi}$ where $\phi \sim U(0,1)$. The angle of these cross terms is then determined by

$$\arctan\left(\frac{\sin(2\pi(\frac{f}{f_s}+\phi)L)+\sin(2\pi(\frac{f_j}{f_s}-\phi)L)}{\cos(2\pi(\frac{f}{f_s}+\phi)L)+\cos(2\pi(\frac{f_j}{f_s}-\phi)L)}\right) \tag{3.94}$$

which, using sum to product identities, simplifies to

$$2\pi L\frac{\left(\frac{f}{f_s}+\frac{f_j}{f_s}\right)}{2} \tag{3.95}$$

which is the average of the two signals phase offset at the receiver. Incorporating this result with (3.90) and (3.92) shows that the fine frequency estimate at the receiver will be determined according to

$$\angle(P(d)) = \arctan\left(\frac{\sin(2\pi\frac{f}{f_s}L)+\alpha\sin(2\pi L\frac{(f+f_j)}{2f_s})+\alpha^2\sin(2\pi\frac{f_j}{f_s}L)}{\cos(2\pi\frac{f}{f_s}L)+\alpha\cos(2\pi L\frac{(f+f_j)}{2f_s})+\alpha^2\cos(2\pi\frac{f_j}{f_s}L)}\right). \tag{3.96}$$

Figure 3.7 shows the behavior of the fine frequency estimate at the OFDM receiver when exposed to the phase warping attack.

This attack can also be modeled stochastically based on a random frequency offset over a given range[2]. The frequency offset for any given system within the specified range can

[2]The frequency offset error for an OFDM system would have to be constrained within a specific range in order to not interfere with adjacent channels.

be modeled as a continuous random variable with a uniform distribution over the given frequency range. While there may be another distribution which models this offset more closely, a uniform distribution is a sufficient approximation for the purposes of this paper. For the model that we used, both the receiver frequency offset, X, and the phase warp offset, Y, are chosen from uniform distributions according to

$$X, Y \sim U(f_{Lo}, f_{Hi}) \tag{3.97}$$

where f_{Lo} and f_{Hi} are the lowest and highest possible frequencies based on the allowable clock error for a given system.

As previously stated, frequency estimation for OFDM is extremely sensitive to the extent that errors on the order of 1% of a subcarrier spacing can cause significant degradation to the effective SNR at the receiver. In an ideal jamming scenario where the attacker has knowledge of the exact preamble symbol, channel state information and frequency offset estimates, this attack effectively randomizes the frequency estimation within the range of possible offsets[3].

We can use the metric described in (3.87) to perform analysis of the ideal phase warping attack. Incorporating the model for the frequency offset and estimation in to this equation yields

$$e_{RMS} = \sqrt{< ((f_{Rx} - f_{Tx}) - (f_{Rx} - \hat{f}_{Tx}))^2 >}. \tag{3.98}$$

f_{Tx} in this equation represents the carrier frequency based on the transmitter clock, f_{Rx} represents the carrier frequency based on the receiver clock and $\hat{f}_{Tx}$ represents the estimate of the carrier frequency at the transmitter as made by the receiver. In this context we note that

$$f_{Rx} = f_{Tx} + X. \tag{3.99}$$

As shown in Figure 3.7, the receiver estimate for the phase angle will converge to the fractional frequency offset of the jammer at low SJRs. Equation (3.98) then converges to

$$e_{RMS} = \sqrt{< ((f_{Rx} - f_{Tx}) - (f_{Rx} - (f_{Tx} + Y)))^2 >}, \tag{3.100}$$

which simplifies to

$$e_{RMS} = \sqrt{< Y^2 >}. \tag{3.101}$$

As the sample size of the measured errors becomes sufficiently large, (3.101) will converge to

$$e_{RMS} = \sqrt{E[Y^2]}. \tag{3.102}$$

Noting that

$$E[Y]^2 = 0, \tag{3.103}$$

it follows that

$$e_{RMS} = \sqrt{VAR[Y]} = \sigma \tag{3.104}$$

[3]The range of possible frequency offsets is something that would be constrained by the signal standard.

where σ^2 is the variance of the random variables. For uniform distributions this variance is

$$\sigma^2 = \frac{1}{12}(f_{Hi} - f_{Lo})^2. \tag{3.105}$$

These results indicate that we would expect to see the RMS error for the frequency offset estimate approach the standard deviation of a uniform random variable with a support equal to the possible range of frequency offsets. In short, the ideal phase warping attack basically transforms the receiver frequency offset estimate in to a random variable over the range of possible offsets. This effect will have a dramatic impact on the OFDM synchronization process, the details of which are discussed later in this paper.

Differential Scrambling Attack

The other frequency estimation based, intelligent attack proposed in this paper is the differential scrambling attack. This attack is designed to disrupt the coarse frequency error estimation at the receiver. The coarse frequency error is simply a subcarrier misalignment at the receiver due to clock frequency discrepancies. The synchronization algorithm uses the phase error in the two halves of the first symbol in order to determine the fractional portion of the frequency discrepancy, and relies on the differential sequence of the common subcarriers of the first and second preamble symbol to determine the integer valued subcarrier offset. This sequence is determined according to (2.24), where $X_{1,k}$ and $X_{2,k}$ are the PN sequences on the common subcarriers of the first and second preamble symbols. The differential scrambling attack targets this differential sequence and prevents subcarrier alignment by interfering with the received symbols correlation to the sequence w_k. This jammer causes the received symbol from (3.14) to be

$$r_n = \left(\sum_{k=n}^{n+C-1} x_{n-k} h_k + \alpha \sum_{k=n}^{n+K-1} y_{n-k} k_k \right) e^{(2\pi j \frac{f}{f_s} n)} + n_n \tag{3.106}$$

where α is just a scalar term based on the power of the attack, y represents the sampled jamming signal, and K and k_k are based on the characteristics of the channel that the jammer sees.

The addition of this jammer has important implications in regard to the coarse frequency estimator from equation (3.29). The numerator of the term $B(g)$ becomes

$$\left| \sum_{k \in \mathcal{X}} (H^*_{k-f+2g} X^*_{1,k-f+2g} + \alpha K^*_{k-f+2g} Y^*_{k-f+2g} + N^*_{1,k}) X_{1,k} X^*_{2,k} (X_{2,k-f+2g} H_{k-f+2g} + N_{2,k}) \right|^2 . \tag{3.107}$$

The addition of the jammer will add a new set of cross correlation terms in to the numerator of $B(g)$. The analysis of this attack's impact on the coarse frequency offset is similar to the

derivation of the coarse frequency metric for the case $g \neq g_{max}$. The attack term will create another term, J, in the coarse frequency numerator, which will be distributed according to

$$J \sim \alpha^2 \text{Exp}(\frac{1}{2|\mathcal{Y}|p_k^2}) = \text{Exp}(\frac{1}{2\alpha^2|\mathcal{Y}|p_c^2}). \tag{3.108}$$

This term will severely impact the coarse frequency estimate for significant α. The ratio of the numerator of the correct coarse frequency estimate to the expected value of the incorrect estimates becomes

$$\frac{min[B(g_{max})]}{E[B(g \neq g_{max})]} \text{ dB} \approx 10\log(|\mathcal{B}|) + 20\log(p_c) + 40\log(p) - 20\log(\alpha) - 12 \text{ dB}. \tag{3.109}$$

In addition, this attack could also have an impact on the fine frequency estimate at the receiver.

The attack is carried out by either transmitting a constant or a random stream of symbols across the subcarriers used in the first preamble symbol. This attack is similar in structure to the false preamble timing attack proposed in [38]. Instead, the idea behind this attack is to distort the amplitude and phase of the received subcarriers in the first preamble symbol, in turn altering the differential sequence at the receiver. The symbols transmitted by the attacker on each subcarrier are constant based on the assumption that the PN sequence of the first preamble symbol is unknown. Assuming the sequence is random and its symbol values are uniformly distributed, transmitting a constant sequence has the same probability of altering the phase at each subcarrier as transmitting a random symbol. Differing this sequence will degrade the performance of the coarse frequency estimation and can result in subcarrier misalignment at the receiver.

3.4 Simulation and Attack Comparison

We developed synchronization simulations in order to test the performance of current synchronization algorithms in the face of symbol timing attacks. The tests were performed in multiple scenarios for each jammer in order to illustrate their individual capabilities. The minimum knowledge requirements for each of the jammers is displayed in Table 3.4.

The results of the false preamble timing attack follow the analytical results closely. The results in Figure 3.8 indicates that the false preamble timing attack is extremely effective in destroying the symbol timing estimate, especially in the case where the delay, N, of the false preamble is equal to the timing window length L. These results indicate that a jammer could force the receiver to synchronize with it as opposed to the true transmitter. This represents a relatively efficient method for disrupting OFDM-based communications.

The preamble warping results also reflect the analytical results as well. The attack is most effective when the two symbols are transmitted at identical power, which is the more likely

Table 3.1: Situational knowledge provided to each jammer for simulation

Jamming Attack	Structure	Symbol Timing	Frequency Offset	Channel
False Preamble	Yes	Window	No	No
Preamble Nulling	Yes	Exact	Yes	Yes
Preamble Warping	Yes	Exact	Yes	No

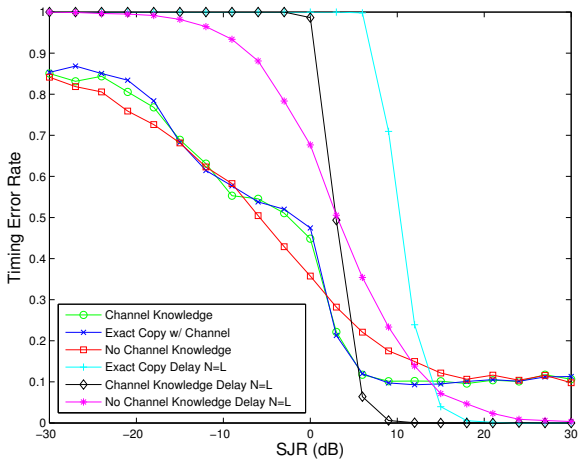

Figure 3.8: Symbol timing error rate as a function of the SJR of the false preamble timing attack.

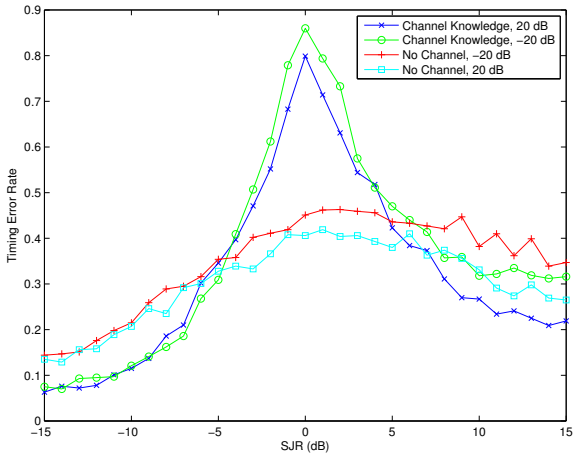

Figure 3.9: Symbol timing error rate as a function of the SJR at the receiver caused by the preamble warping attack at an SNR of 20 dB.

when the jammer has channel knowledge. However, even in the case where the jammer has no channel knowledge, Figure 3.9 shows that there is a significant disruption to acquisition at the receiver, producing error rates of almost .5.

In addition, Figure 3.9 indicates that the error rate is higher at higher SJRs. This is due to the fact that the signal power and the SNR were kept constant, while the jammer power was varied for comparison. This result signifies that increasing the jammer power too high will actually start to improve the timing acquisition at the receiver. This is because the warping attack is just a frequency shifted version of the timing preamble symbol, so sending a highly powered jamming signal will effectively increase the SNR seen at the receiver. However, the coarse frequency estimate would likely also be hampered, but as far as the timing estimation goes, this result is undesirable for a jammer. This is a useful result because it indicates that jammers using a warping attack are better off erring on the side of lower power than the transmitter signal, making this attack even more efficient.

We also developed some simulation scenarios in order to determine the impact of these frequency jamming attacks on OFDM synchronization. Each attack was tested under two different scenarios. The first scenario is assuming that the jammers have full channel knowledge of both their own channel and the transmitters. This means that the jammer can send a signal

$$\hat{y}_n = \alpha \left(\sum_{l=0}^{K-1} p_{n-l} k_l^{-1} \right) \tag{3.110}$$

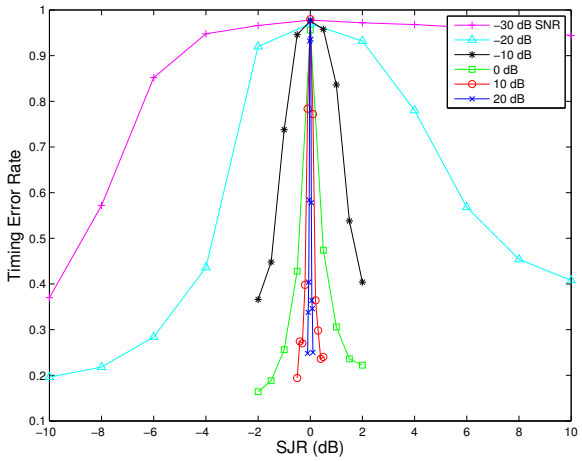

Figure 3.10: Timing estimate error rate as a function of SJR for the preamble nulling attack at an SNR of 20 dB.

where

$$p_n = \left(\sum_{i=0}^{C-1} y_{n-i} h_i \right) e^{(2\pi j \frac{f_j}{f_s} n)} \tag{3.111}$$

and α is determined by the SJR, and the frequency shift is a determined randomly and constrained to within a few subcarrier spacings. The term p_n is the jamming signal convolved with the channel response of the transmitter's channel at the given frequency offset. The term $\hat{y}_n$ represents the scaled convolution of signal p_n with k_i^{-1}, the inverse of the jammer's channel. This means that the received jamming signal will be p_n. The second scenario assumes no channel knowledge by the jammer, so that both the transmitter and jammer transmit across distinct multipath channels. We also included a simulation of the phase warping attack with perfect knowledge of the preamble symbol. This simulation provides a base line measurement for both the frequency estimation error rate and the RMS estimation error. Each of these scenarios were simulated a thousand times each over a range of SJRs.

The results for the phase warping attack show that it is highly disruptive to the frequency offset estimation at the receiver. Errors for these simulations were considered to be offset estimations at the receiver that were more than a tenth of a subcarrier away from their true value. This is more than enough estimation error to cause severe degradation to the effective SNR at the receiver. While the phase warping attack is extremely effective in causing errors when it has channel knowledge and transmits at equal or higher power as the transmitter, the phase warper with no channel knowledge actually out performs one with channel knowledge at high SJRs.

In terms of the ideal phase warping attack, where the jammer has exact knowledge of the

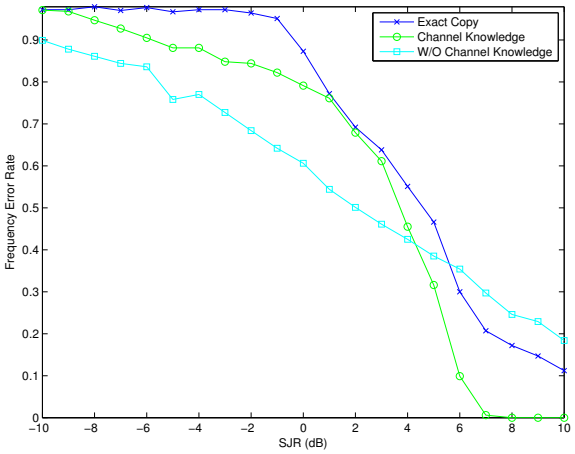

Figure 3.11: Frequency offset estimation error rate as a function of the SJR of three phase warping attacks with varying levels of situational knowledge.

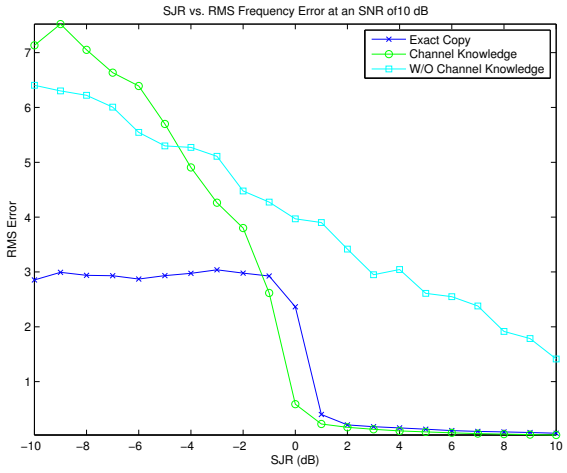

Figure 3.12: Frequency offset estimation RMS error as a function of the SJR of the phase warping attack with channel knowledge.

preamble symbol, the simulations show that the less cognitive attacks perform considerably well. The version of this attack with only OFDM standards knowledge–the least cognitive of these attacks–actually outperforms the idealized attack and the attack with channel knowledge at SJRs of 6 dB or higher. In scenarios where the jammer is transmitted at a higher power, the advantage of channel knowledge can provide an advantage of up to 6 dB. All three varieties of this attack seem to have certain advantages within different situations depending on the balance between the constraints of power and complexity.

In addition to the performance metric of estimation error rate, Figure 3.12 helps to illustrate some of the underlying impacts of each of these attacks on the preamble based frequency error estimation process. This graph shows the RMS error of the frequency offset estimation in terms of subcarrier bins. The results from this graph give very interesting insight in to the nature of the different attacks. First of all, the RMS error for the ideal phase warping attack highlights two important points about the synchronization process and this attacks impact. The first is that at relatively high SJRs, the ideal phase warping attack still causes significant degradation in the success rate of frequency synchronization despite the fact that the RMS error is extremely low (approximately .06 at an SJR of 10 dB). This speaks to the extremely sensitive nature of the frequency offset estimate. The second important result is that the error quickly converges to the standard deviation of the random distribution of possible frequency offsets as previously suggested. For these simulations both the frequency offset, X, at the receiver and the warping frequency, Y, were chosen from a uniform distribution spanning five subcarrier spacing in either direction

$$X, Y \sim U(-5, 5). \tag{3.112}$$

Calculating the standard deviation σ from (3.105) yields an approximate standard deviation of 2.89, which is in agreement with the results from Figure 3.12.

In the cases of the non-ideal phase warping attacks the RMS errors are much different. The attack that has full channel awareness without exact knowledge of the preamble demonstrates a similar RMS error as the ideal attack at SJRs of 0 dB or greater. However, once the power of the jamming signal starts to exceed that of the preamble the error for the non-ideal attack with channel knowledge continues to climb above the standard deviation for a uniformly random distribution of frequency offsets within the given range. This phenomenon–which also shows up in the RMS error for the blind attack–can be likened to the fact that these attacks can cause frequency estimation errors outside of the possible offsets. Fundamentally, this result suggests one of the main differences between the ideal attack and the other two versions of this attack. When the non-ideal attacks are successful in causing the frequency estimation process to miss, they cause it to miss bigger than the ideal attack. While the overall error rates are not as high for these attacks, the error margins tend to be wider and more spread out than the ideal attack. This aspect of the non-ideal attacks may or may not be desirable for the jammer, depending on factors such as the level of cognition of the target device. In either case, the RMS error results for all three versions of the phase warping jammer suggest that the attack is very effective in increasing the randomness of the

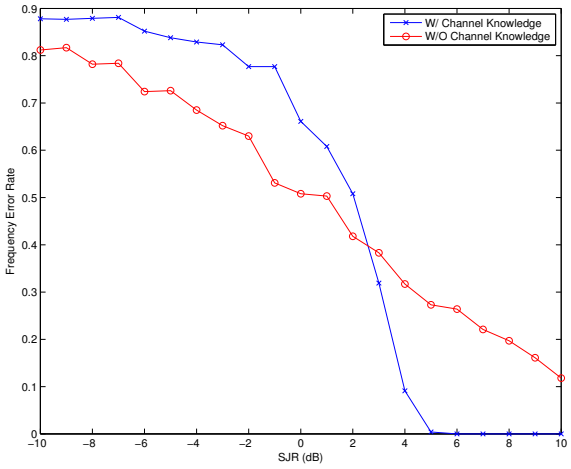

Figure 3.13: Frequency offset estimation error rate as a function of the SJR of the differential scrambling attack with channel knowledge.

frequency estimation process.

Using the same metric for estimation errors as the phase warping attack, the differential scrambling attack shows similar performance against the frequency estimation of OFDM. The attack without any channel measurements actually causes more acquisition errors at higher SJRs than the attack with perfect channel knowledge. At lower SJRs the more cognitive of the two attacks outperforms its counterpart, though the error ceiling on both attacks is not quite as high as the phase warping attack. It is important to note that at SJRs lower than 3 dB the attack with channel knowledge begins to produce a higher error rate than the simpler attack. This can be attributed to the fact that the differential scrambling attack only transmits a symbol that is half of the length of the entire preamble. The 3 dB threshold is therefore the point where the differential scrambler becomes more powerful than the first half of the preamble symbol. It is an interesting result that the performance the jammers with the addition of channel knowledge capabilities is tied in to this threshold.

The RMS errors that each jammer causes in the receiver follow a similar pattern as the phase warping jamming attacks. The jammer with channel knowledge causes estimation errors of a smaller variance, but at lower SJRs the errors are more consistent, resulting in the higher error rates. The jammer without channel knowledge causes errors with a wider variance, but on a less consistent bases as jammer power increases.

Although its seems somewhat surprising that the jammers without channel knowledge tend to perform slightly better at higher SJRs, the explanation is related to the estimation used by the receiver. It is important to note that the symbol timing estimator and fine frequency offset estimator coupled with the structure of the first preamble symbol creates a matched

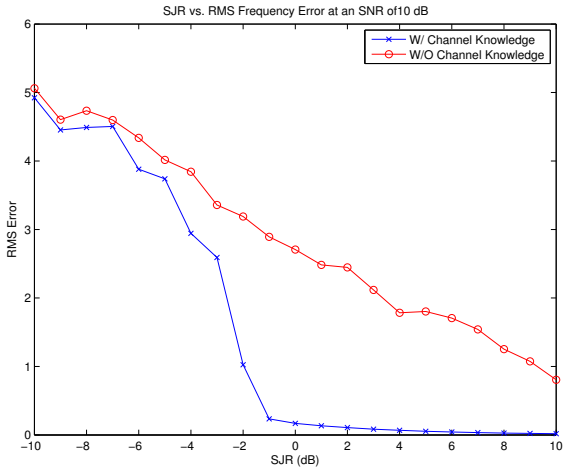

Figure 3.14: Frequency offset estimation RMS error as a function of the SJR of the differential scrambling attack with channel knowledge.

filter at the receiver since we have assumed the channel to be time-invariant over the period of the preamble. This means that–outside of noise–the estimated values at the receiver are much more deterministic for a given channel. In the case where the jammer and the transmitter see different channels, there receiver is not a matched filter for the cross terms between the two signals. This effect causes randomness in the numerator of the estimators, while the power normalization terms in the denominators still reflect the total power of both the jammer and transmitter preamble. This phenomenon seems to have the most impact specifically when both of these signals are transmitted with equal power.

Chapter 4

Attack Mitigation

Both OFDM timing and frequency synchronization are necessary in order to avoid inter-symbol interference (ISI), as well as inter-carrier interference (ICI) and loss of orthogonality among OFDM subcarriers. In addition, this process must be performed often in order to ensure accurate tracking of timing and frequency offsets between a transmitter and a receiver. A number of algorithms have been developed in order to efficiently and robustly perform the synchronization [14, 39, 40, 9, 10, 11, 12, 13].

However, as we have shown in previous sections, there are still many shortcomings of OFDM synchronization in the presence of efficient adversarial devices. It has been shown that current implementations of OFDM are susceptible to a variety of pilot jamming attacks [18]. There has been research conducted on analyzing and improving the robustness of OFDM synchronization algorithms under interference conditions [41, 8, 32, 33, 34, 35, 36], as well as on the performance of existing OFDM synchronization algorithms in the presence of targeted jamming attacks [42, 38, 43]. These works underscore the theme that OFDM implementations often require multiple, flexible security features in order to be robust.

In addition, due to the importance of OFDM synchronization and the high frequency at which it is calculated in realistic systems, it is important to develop algorithms that are efficient while still being secure. In this chapter, we present a novel method for performing OFDM synchronization utilizing the well known cross ambiguity function (CAF). We analyze the validity of this method for computing the timing point and carrier frequency offset in an OFDM system in addition to the CAF's performance in a realistic communications environment with multipath fading. In addition, we discuss how this synchronization method can be used in conjunction with a technique called 'sync-amble' randomization in order to vastly improve the overall security of the OFDM synchronization process.

4.1 Cross Ambiguity Function Based Orthogonal Frequency Division Multiplexing Acquisition

The first improvement to physical layer security proposed in this paper is based on using the Cross Ambiguity Function (CAF) to compute the timing point and frequency offset estimation at the OFDM receiver. The main advantage of performing synchronization using the CAF is that it does not require an easily identifiable, time repetitive symbol as in [14]. The synchronization symbol will still have a cyclic prefix, but will not be physically discernible from any data bearing OFDM symbol.

4.1.1 Theoretical Analysis of Synchronization with the Ambiguity Function

Assuming that the synchronization symbol sent resembles an ordinary data symbol, and that the channel from the transmitter to the receiver can be modeled as an AWGN multipath channel with finite length impulse response, the sampled signal at the receiver after baseband conversion is represented as

$$r_n = \left(\sum_{k=0}^{C-1} x_{n-d-k} h_k \right) e^{2\pi j \frac{f}{f_s} n} + n_n \tag{4.1}$$

where the subscript n represents the sample index and spans the search area for the training symbol, d is the delay value and timing point of the symbol, C is the length of the channel approximation, f represents the carrier frequency offset and n is the noise term.

Since the receiver will not be able to use a delay line correlation as a matched filter for synchronization, it is required that the receiver have the baseband signal, x_n, of the OFDM training symbol in memory. This signal is the same as the one in (4.1), except that there is no frequency offset term and its length is exactly that of the training sequence, as opposed to the range that the receiver is searching. This means that the CAF method synchronization symbol will physically resemble any other data bearing OFDM symbol.

The receiver will then compute the CAF using the received baseband signal and the local baseband signal according to

$$A(u, v) = \left| \sum_{k=0}^{N-1} x_k r^*_{k+u} e^{-2\pi j k v / N} \right| \tag{4.2}$$

where r and x represent the low pass equivalents of the two sampled copies of a given signal, u and v represent the timing and frequency offsets in terms of samples and frequency bins, respectively, where $0 \leq u \leq d_{max}$ and $|v| \leq N f_{max}/f_s$. N represents both the length in

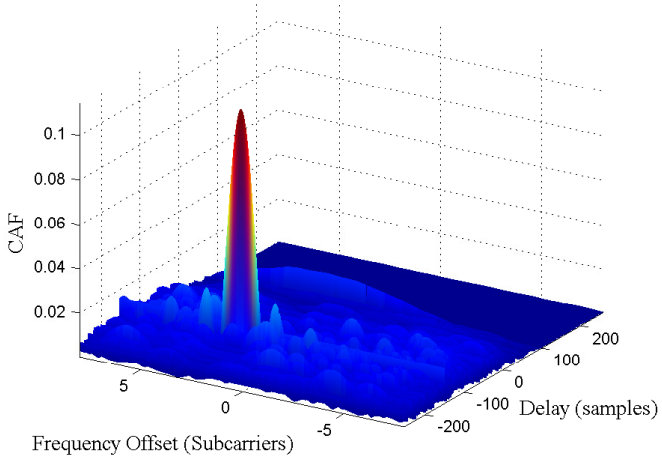

Figure 4.1: CAF surface used to perform timing and frequency offset estimation for OFDM synchronization. The location of the distinct peak in the CAF produces the values of the symbol timing point and the carrier frequency offset estimate used for synchronization at the receiver.

samples of the symbols as well as the number of subcarriers used in the OFDM system, while t_{max} and f_{max} are the finite range over which the offsets for timing and frequency are computed. The peak of this function over both timing and frequency offsets provide the timing and frequency offsets for the receiver. Figure 4.1 depicts a CAF surface for an OFDM system subject to AWGN and multipath interference.

A normalization term can also be computed using the reference copy of the preamble at the receiver according to

$$R_{xx}(0) = \sum_{k=0}^{N-1} x_k x_k^* = N\sigma_x^2, \tag{4.3}$$

where σ_x^2 is the average power of the preamble symbol, from the more general definition of the autocorrelation

$$R_{xx}(k) = \sum_{k=0}^{N-1} x_k x_{k-r}^*. \tag{4.4}$$

The normalized CAF is then computed as

$$A_n(u,v) = \frac{A(u,v)}{N\sigma_x^2}. \tag{4.5}$$

Normalization can also allow for thresholding of synchronization estimates in order to avoid errors. Figure 4.1 depicts a CAF surface for an OFDM system subject to AWGN and multipath interference.

The computed peak of the CAF will be located at the values of u and v that maximize A. Substituting Equation (4.1) in to (4.2) yields

$$A(u,v) = \left| \sum_{k=0}^{N-1} \left(x_k \left(\sum_{i=0}^{C-1} x^*_{k+u-d-i} h^*_i e^{2\pi j \frac{f}{f_s} k} + n_{k-d} \right) e^{-2\pi j k v/N} \right) \right| \tag{4.6}$$

The computed time and frequency offsets are determined according to

$$\arg\max_{\hat{d}_o, \hat{f}_o} A(\hat{d}_o, \hat{f}_o) := \{\hat{d}_o \mid \forall u, \hat{f}_o \mid \forall v : A(u,v) \leq A(\hat{d}_o, \hat{f}_o)\} \tag{4.7}$$

where $\hat{d}_o$ and $\hat{f}_o$ represent the computed delay and frequency offset values. If we assume favorable channel conditions, where the impact of noise is negligible and the channel between the transmitter and the receiver has unity gain with no phase distortion, then equation (4.10) simplifies to

$$A(u,v) = \left| \sum_{k=0}^{N-1} \left(x_k \left(x^*_{k+u-d} e^{2\pi j \frac{f}{f_s} k} \right) e^{-2\pi j k v/N} \right) \right| \tag{4.8}$$

In this case

$$\arg\max_{u,v} A(u,v) := (d, N\frac{f}{f_s}) \tag{4.9}$$

thus showing that the CAF will produce the appropriate timing point and frequency offset estimates under ideal conditions.

There are multiple assumptions in this scenario, however, that do not hold in a realistic wireless communication scenario. Effects like such as additive white Gaussian noise (AWGN) and multipath can not be ignored, nor can constraints on computational capabilities.

4.1.2 Cross Ambiguity Function Synchronization Performance

In order to assess the viability of the CAF synchronization method in a realistic wireless system, it is important to determine the system performance under realistic conditions. Revisiting equation (4.6) highlights two areas of concern regarding synchronization performance; multipath channel effects and AWGN. We can rearrange the terms in (4.6) to determine the theoretical CAF peak coordinates d_o and f_o

$$A(u,v) = \left| \sum_{k=0}^{N-1} \left(x_k \left(\sum_{i=0}^{C-1} x^*_{k+u-d-i} |h_i| e^{-j\theta_i} e^{2\pi j \frac{f}{f_s} k} + n_{k-d} \right) e^{-2\pi j k v/N} \right) \right| \tag{4.10}$$

where θ_i represents the i^{th} phase of the multipath channel response, specifically

$$\theta_i = \tan^{-1}(\frac{\mathrm{Im}(h_i)}{\mathrm{Re}(h_i)}). \tag{4.11}$$

Due to the autocorrelation properties of OFDM symbols [37]

$$R_{xx}(0) >> R_{xx}(r \neq 0), \quad \forall r \in \mathbb{Z}. \tag{4.12}$$

Incorporating this fact in to (4.10) means that the CAF will be maximized $u-d-i=0$. This essentially means that the multipath profile will produce multiple local maxima at points where $u = d + i$.

By using the relationship in (4.12), we can make the approximation that

$$R_{xx}(r \neq 0) \approx 0, \tag{4.13}$$

subsequently producing the values of the local maxima of the CAF function as

$$A(d+i, N\frac{f}{f_s}) \approx \left| \sum_{k=0}^{N-1} |x_k|^2 |h_i| e^{-j\theta_i} + x_k n_{k-d} e^{-2\pi j k \frac{f}{f_s}} \right|, \qquad i = 0, 1, ..., C-2, C-1 \tag{4.14}$$

These maxima can be bounded

$$A(d+i, N\frac{f}{f_s}) \geq \sum_{k=0}^{N-1} |x_k|^2 |h_i| - |x_k||n_{k-d}| \tag{4.15}$$

which, when incorporated with equation (4.4), simplifies to

$$A(d+i, N\frac{f}{f_s}) \geq |h_i|\sigma_x^2 - \sum_{k=0}^{N-1} |x_k||n_{k-d}| \tag{4.16}$$

We note that

$$\sum_{k=0}^{N-1} |n_{k-d}|^2 = N\sigma_n^2 \tag{4.17}$$

where σ_n^2 represents the average noise power present, based on the assumption that

$$n_k = \frac{\sigma_n}{2}(a_k + jb_k), \quad a_k, b_k \sim N(0,1) \tag{4.18}$$

where $N(0,1)$ represents the standard normal distribution. We also note that

$$\sum_{k=0}^{N-1} |x_k||n_{k-d}| \leq N\sigma_x\sigma_n. \tag{4.19}$$

Incorporating these relationships in to (4.16) yields

$$A(d+i, N\frac{f}{f_s}) \geq |h_i|N\sigma_x^2 - N\sigma_x\sigma_n. \tag{4.20}$$

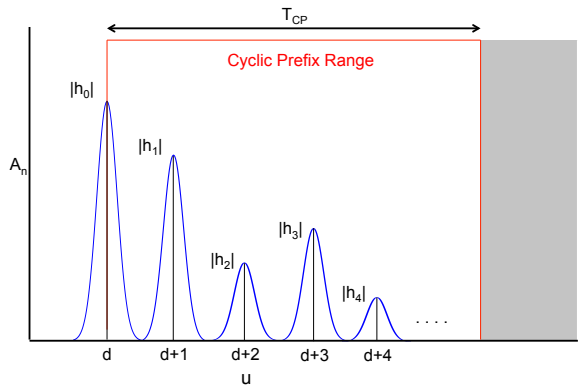

Figure 4.2: Theoretical snap shot of a normalized CAF plane at the frequency offset $N\frac{f}{f_s}$. The timing correlation peaks correspond to the magnitude and the location of the theoretical FIR filter taps of the multipath channel. As long as the strongest peak occurs within the range of the cyclic prefix–denoted by the red box–then the receiver will be able to estimate a valid timing point. If the strongest path falls after the cyclic prefix–marked by the gray area–then the timing point will be invalid.

Incorporating the normalization term we see that

$$A_n(d+i, N\frac{f}{f_s}) \geq |h_i| - \frac{\sigma_n}{\sigma_x}. \tag{4.21}$$

We subsequently define the average signal-to-noise ratio (SNR) of for the preamble symbol as

$$\text{snr} = \frac{\sigma_x^2}{\sigma_n^2} \tag{4.22}$$

then incorporate this in to (4.20) to obtain the inequality

$$A_n(d+i, N\frac{f}{f_s}) \geq |h_i| - \frac{1}{\sqrt{\text{snr}}} \tag{4.23}$$

or

$$A_n(d+i, N\frac{f}{f_s})_{dB} \geq 10\log\left(|h_i| - \frac{1}{\sqrt{\text{snr}}}\right) \tag{4.24}$$

where $\{*\}_{dB}$ is computed $10\log\{*\}$.

The multipath profile h will determine at what delay value u the peak of the ambiguity function A occurs. However, any timing estimation point taken over the range $u \in [d, d+T_{cp}f_s)$ can be considered a valid timing point that will allow for successful baseband processing and demodulation. Therefore, it is critical that the delay spread of the multipath channel, represented as i in our models, be less than length of the cyclic prefix $T_{cp}f_s$. More specifically,

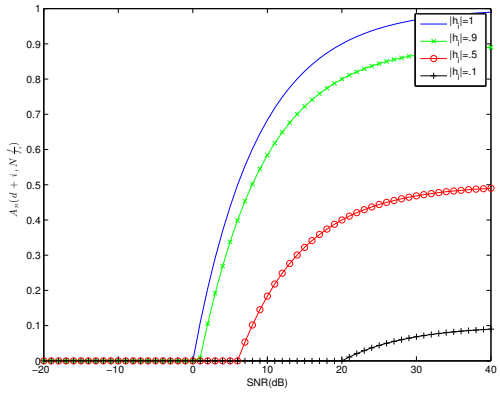

Figure 4.3: Lower bound on the normalized cross ambiguity function peak term relative to SNR. Results are shown over multiple values of $|h_i|$ in order to illustrate how multipath fading can impact the synchronization process.

the strongest signal path must be located within the range of the cyclic prefix according to

$$\underset{i\in\{0,1,...,C-1,C\}}{\arg\max} |h_i| \in \{0, 1, ..., \lfloor T_{cp} f_s \rfloor - 1, \lfloor T_{cp} f_s \rfloor\}. \tag{4.25}$$

Fortunately, this requirement coincides with the design motivations, in that OFDM systems typically choose a cyclic prefix longer than a specified maximum excess delay in order to avoid inter-symbol interference (ISI).

4.1.3 Efficient Cross Ambiguity Function Computation

In a realistic communications scenario, it is undesirable to directly compute the entire CAF due to computational constraints. It turns out that based on the characteristics of an OFDM system, the CAF can be computed rather efficiently. We will present two methods for computing the cross ambiguity function, and both of them can be incorporated in to an overall computationally efficient synchronization method for an OFDM system.

Coarse Time Domain Method

The first efficient method for computing the CAF is performed using the time domain signals given in equation (4.2). Figure 4.4 illustrates the main steps of this algorithm, which are described in this section.

The first step is to determine the delay values u over which to compute the lag products. The values of the delays are relative to the timing point of the system and are therefore a

matter of convention. In this work we simply define the range of u as

$$D = \{0, 1, 2, ..., d_{max} - 2, d_{max} - 1, d_{max}\}. \tag{4.26}$$

The correlation of a length N reference synchronization symbol over a space of n_f symbols–or $n_f N$ samples–results in a sequence of length $N(n_f + 1) - 1$, however $N - 1$ points from both sides of the sequence need not be computed as they represent the edges of the correlation function which are outside the search window, where n_f is the number of symbols in each OFDM frame. Therefore, in a typical synchronization scenario, a receiver will search over a total number of time delay values

$$|D| = N(n_f - 1) + 1 \tag{4.27}$$

where $|D| \in \mathbb{N}$. The lag products

$$f_u[k] = x_k r^*_{k+u}, \quad u \in D \tag{4.28}$$

can be computed in parallel.

The direct CAF computation method is carried out by simply taking the DFT of the lag products and finding the location of the maximum point along the resulting CAF plane. However, in order to reduce the computational burden at the receiver, we can first downsample the lag products, resulting in a greatly reduced number of overall computations. This is possible due to two factors. The first reason is that the lag products are inherently narrowband signals [44]. The second reason is due to the fact that in any practical OFDM system $f_s/2 >> f_{max}$, meaning that the DFT of the lag product spans a large number of points outside of the possible frequency offset range.

The maximum downsampling factor, m, for this stage is computed according to

$$m_{max} = \lfloor \frac{f_s}{2f_{max}} \rfloor, \tag{4.29}$$

however, in many cases it is computationally advantageous to downsample by a factor of 2[1]. The downsampling factor in this case would be

$$m_d = 2^{\lfloor \log_2 \left(\lfloor \frac{f_s}{2f_{max}} \rfloor \right) \rfloor}. \tag{4.30}$$

In either case, $m_{max} \geq 1$ and $m_d \geq 1$. Downsampling can be performed via filtering and decimation, though often times–depending on the constraints of a given system–decimating the signal with no filtering is sufficient due to the narrowband properties of the lag products [44].

[1]OFDM systems often employ a power of 2 number of subcarriers because of the optimality of the DFT for power of 2 length signals.

After the lag products have been downsampled, the CAF can be computed using the DFT according to

$$A(u,v) = \left| \sum_{k=0}^{M-1} f_u[km_d] e^{-2\pi jkm_d v/M} \right| \tag{4.31}$$

where $M = \lceil N/m_d \rceil$–in practice m_d should usually be chosen to be divisible by N, but if not then the last sample should be kept.

Taking a M point DFT across each of the lag products yields a frequency resolution of

$$R_f = \frac{m_d M}{f_s} = \frac{N}{f_s}, \tag{4.32}$$

in bin/Hz for A. However, it is more useful to express the normalized frequency resolution in bins per subcarrier as

$$R_{|f|} = R_f f_{sc}, \tag{4.33}$$

where due to the structure of OFDM symbols–namely the fact that N also represents the number of subcarriers

$$f_{sc} = \frac{f_s}{N} \tag{4.34}$$

and represents the Hz per subcarrier ratio of an OFDM system. This results in $R_{|f|} = 1$, while OFDM systems usually need a frequency offset estimation precision of less than a tenth of a subcarrier [7], so $R_{|f|}$ must be increased.

The receiver must perform interpolation in order to increase the frequency resolution and more accurately estimate the frequency offset error. There are various methods to perform this task, but given the nature of OFDM systems, it seems to make the most sense to leverage the efficiency of the DFT to perform this task. The minimum interpolation factor, s_{min}, for a required normalized frequency resolution $R_{|f|} = \sigma$, is conveniently

$$s_{min} = \sigma. \tag{4.35}$$

Noting again that it is computationally efficient to interpolate by a factor of 2, we can compute the actual interpolation factor

$$s = 2^{\lceil \log_2(s_{min}) \rceil}. \tag{4.36}$$

In both cases, $s_{min} \geq 1$ and $s \geq 1$. We then take the sM point DFT of the lag products

$$A(u,v) = \left| \sum_{k=0}^{sM-1} f_u[km_d] e^{-2\pi jkm_d v/sM} \right| \tag{4.37}$$

by appending $(s-1)M$ zeros to each of the lag products. The resulting CAF function A will have a normalized frequency resolution of

$$R_{|f|} = s. \tag{4.38}$$

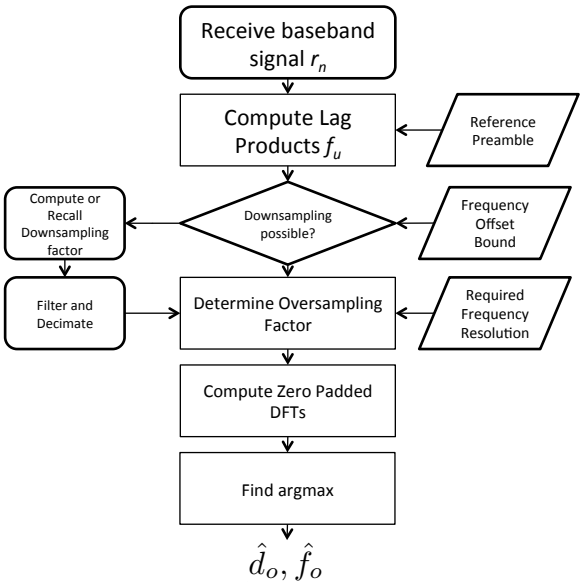

Figure 4.4: The coarse timing CAF method of determining the timing point and the carrier frequency offset for an OFDM system. Each of these values are subsequently outputted to timing and frequency correction blocks.

The values $\hat{d}_o$ and $\hat{f}_o$, defined in equation (4.7), are taken from this computed version of the CAF as the timing point estimate and frequency offset error estimate, respectively. While it is possible to compute a more precise, fractional timing point estimate with the CAF method, it is unnecessary due to the structure of OFDM symbols, where any starting sample taken along the cyclic prefix can be used as a valid timing point.

Coarse Frequency Domain Method

The second efficient CAF computation method for estimating timing and frequency offset errors for OFDM synchronization involves using the Fourier transforms of time signals in equation (4.2). Figure 4.5 illustrates the main steps of frequency domain CAF algorithm, which are described in this section.

The first step using this method is to compute the DFT of the received signal over the entire timing point search range according to

$$R_l = \sum_{n=0}^{2n_f N-1} \left[\left(\sum_{k=0}^{C-1} x_{n-d-k} h_k \right) e^{2\pi j \frac{f}{f_s} n} + n_n \right] e^{-2\pi j n l / N}. \tag{4.39}$$

This DFT is computed over $2n_f N$ points, twice the number of samples in the search range D, to avoid circular convolution during frequency domain computation. The DFT of the

receiver's reference copy of the preamble must also be computed according to

$$X_l = \sum_{n=0}^{2n_f N-1} x_n e^{-2\pi jnl/N}. \tag{4.40}$$

For both computations the sequences are zero padded to the appropriate lengths before DFT computation.

The CAF will subsequently be computed via the frequency domain representation of signals as

$$A(u,v) = \left| \sum_{l=0}^{2n_f N-1} X_l R^*_{l+v} e^{2\pi jul/N} \right| \tag{4.41}$$

The term R_{l+v} represents a v-point circular shift of the frequency bins of R_l–this is the coarsely frequency shifted term. The integer set F containing all of the shift values v is determined by the range of possible frequency offset values according to

$$F = \{-N\frac{f_{max}}{f_s}, -N\frac{f_{max}}{f_s}+1, ..., N\frac{f_{max}}{f_s}-1, N\frac{f_{max}}{f_s}\}, \tag{4.42}$$

where

$$f_{max} = \mu f_{sc}, \tag{4.43}$$

with μ defined as a system constraint on the maximum frequency offset between transmitter in receiver in terms of subcarriers. This means that $N\frac{f_{max}}{f_s}$ is the maximum possible frequency offset between a transmitter and a receiver in subcarriers.

In the case of the coarse frequency domain CAF, downsampling is not performed because it is necessary preserve the timing point search boundaries in the ambiguity function. However, the timing point search range for the computed CAF from equation (4.41) will span

$$u = \{-d_{max}, -d_{max}+1, ..., d_{max}-1, d_{max}\}. \tag{4.44}$$

This means that only half of the computed CAF over $u \in D$ is needed in order to search for a maximum timing point and carrier frequency offset. The locations of the discarded values of the computed CAF are dependent on the convention with which zero padding and Fourier transforms are performed.

The values of $\hat{d}_o$ and $\hat{f}_o$ are then obtained via the computed CAF over the values in equation (4.44) and $v \in F$ as defined in equation (4.42). While the computed timing point value will be computed with sufficient resolution, the frequency offset estimate will not be precise enough. Incorporating equations (4.34) and (4.43) in to (4.42) yields the set across which v is computed

$$F = \{-\mu, -\mu+1, ..., \mu-1, \mu\} \tag{4.45}$$

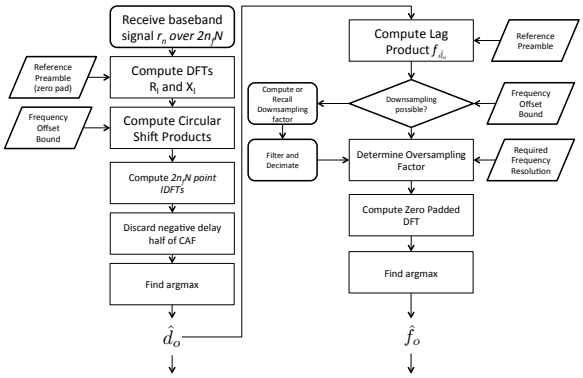

Figure 4.5: The coarse frequency CAF method of determining the timing point and the carrier frequency offset for an OFDM system. Each of these values are subsequently outputted to timing and frequency correction blocks.

resulting in an estimation precision on the order of subcarriers. However, OFDM systems typically require frequency offset estimation to a precision of hundredths of subcarriers[7]. This means that further computation is required to more precisely determine $\hat{f}_o$.

Increased resolution of the frequency offset estimate is best achieved via time domain computation of the CAF, as shown in Section 4.1.3. But since we already have a sufficiently precise estimate of the timing point, $\hat{d}_o$, it is unnecessary to compute the entire CAF. Instead we compute one 'slice' of the CAF function at the timing estimate $\hat{d}_o$ according to

$$A(\hat{d}_o, v) = \left| \sum_{k=0}^{N-1} x_k r^*_{k+\hat{d}_o} e^{-2\pi jkv/N} \right|. \tag{4.46}$$

The lag product computed in (4.46) must be zero padded to increase the frequency resolution of the resulting CAF function. The required frequency resolution and interpolation factor are computed exactly as in Section 4.1.3, resulting in a CAF 'slice' computation of

$$A(\hat{d}_o, v) = \left| \sum_{k=0}^{sM-1} x_k r^*_{k+\hat{d}_o} e^{-2\pi jkv/sM} \right|. \tag{4.47}$$

The resulting $\hat{f}_o$ computed from this equation, along with the previously computed value $\hat{d}_o$ can then be used to acquire the timing point of the system, perform frequency offset correction and subsequent baseband processing and demodulation operations.

4.1.4 Computational Complexity

Based on the performance of CAF synchronization the method appears viable, but it is also important to consider the computational cost of utilizing this strategy. Existing syn-

chronization methods such as [14] can be performed at a reasonable computational cost to the receiver, while maintaining adequate performance. As previously mentioned, the CAF synchronization method offers some advantages over existing algorithms, but in order to be a practical choice of algorithm it must be computed efficiently. While a brute force CAF synchronization approach would carry a heavy computational burden, utilizing efficient CAF computation methods makes the algorithm feasible.

In order to determine the computational complexity of CAF synchronization, it is first important to derive the computational complexities of each method, which will determine whether to compute the CAF via the coarse time domain method or the coarse frequency domain method.

We previously defined the search space D for the timing point in equation (4.26). This range represents all of the values of u for which a receiver would be required to compute the CAF. We also defined the search space F for the coarse frequency offset estimate in (4.42). This range represents the integer values of v that the receiver will be required to compute the CAF for. While the size of these search spaces alone can be used to determine the more efficient method of computation, further analyzing the computational complexity of each method will help to determine a more reliable threshold.

Coarse Time Method

Recalling the size of the time search space from equation (4.27), combined with the fact that each delay point will require N multiplication operations prior to the discrete Fourier transform (DFT) step, we can show that the number of operations required for the coarse timing method before the DFT stage can be expressed as

$$M_{t_1} = |D|N. \tag{4.48}$$

The downsampling stage will add another step to the computation of the CAF, but will decrease the number of overall operations. As previously noted, low pass filtering will usually not be required to downsample the lag products because of their narrowband properties. However, in the case that a low pass filter is used, a number of operations will be added on the order of $N_{LP}N$, where N_{LP} is the number of taps for the low pass filter. The number of operations after filtering and downsampling M_{t_2} can be approximated as

$$M_{t_2} \approx |D|N + |D|NN_{LP}. \tag{4.49}$$

The DFT computations are the final stage of the coarse time domain CAF computation algorithm. The total number of operations at this stage can be represented as

$$M_{t_3} \approx |D|N + |D|NN_{LP} + |D|\frac{sN}{m}\log_2\left(\frac{sN}{m}\right) \tag{4.50}$$

where m is the downsampling factor computed as per equation (4.30), and s is the oversampling factor computed in equation (4.36). It is assumed that the DFTs are efficiently computed via FFT, where the number of operations required will be $N \log_2(N)$ for a length N sequence, where N is a power of 2.

From this point the remaining operations will involve taking the absolute value of the CAF and perform a search for the maximum value, but these computations are common to both methods.

Coarse Frequency Method

The coarse frequency domain, on the other hand, requires pre-processing of a $2n_fN$ point DFT. While it is not guaranteed that n_f is a factor of two, it is still sufficient to approximate the operations required for the two DFTs at this stage as

$$M_{f_1} \approx 4n_fN \log_2(2n_fN) \tag{4.51}$$

for the purpose of this work, namely comparing the two methods of CAF computation. In addition, it should be noted that an DFT of length $2n_fN$ is not required to avoid circular convolution effects due to the reference copy of the preamble at the receiver being length N, but this choice simplifies derivations and helps minimize DFT complexity for cases where n_fN is a factor of 2. Using equation (4.42), we can see that the receiver will be required to search over a total number of integer frequency offset values

$$|F| = 2N\frac{f_{max}}{f_s} + 1. \tag{4.52}$$

Each frequency offset point will require $2n_fN$ multiplications before the IDFT stage is performed. This results in a total number of operations

$$M_{f_2} \approx 4n_fN \log_2(2n_fN) + 2n_fN|F|. \tag{4.53}$$

The next stage for the coarse frequency domain CAF computation method is to perform the inverse DFT (IDFT) of the frequency domain products, resulting in

$$Mf_3 \approx (|F| + 2)\, 2n_fN \log_2(2n_fN) + 2n_fN|F| \tag{4.54}$$

operations. The resulting CAF function after this stage yields a valid timing point, but the frequency offset estimate must be recalculated as described in Section 4.1.3. This timing point is used to compute one lag product, downsample and compute an oversampled DFT, resulting in one CAF slice from which the frequency offset error can be determined. The number of operations due to these computations can be determined from (4.50), resulting in a total number of operations

$$\begin{aligned} Mf_4 \approx{}& (|F| + 2)\, 2n_fN \log_2(2n_fN) + 2n_fN|F| \\ &+ N + N_{LP}N + \frac{sN}{m}\log_2\left(\frac{sN}{m}\right) \end{aligned} \tag{4.55}$$

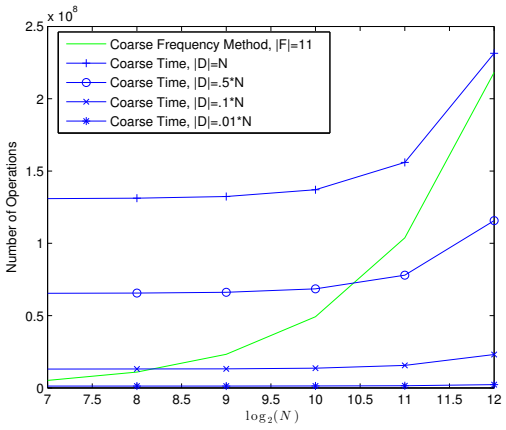

Figure 4.6: Comparison of the computational complexity between the coarse time CAF computation method and the coarse frequency computation method. The comparison is shown across a range of power of 2 subcarrier values and for differing values of the timing point search range —D—.

for the coarse frequency CAF computation method.

Cross Ambiguity Function Computation Method Threshold

We can use the complexity results for each of the two CAF computations to determine a reasonable threshold for choosing the most efficient method. Using the final results from equations (4.50) and (4.55), while rearranging the common terms due to the fine frequency offset computation in the coarse frequency method, we can define our computation decision threshold as

$$\begin{aligned} T_c = &(|F|+2)2n_f N \log_2(2n_f N) + 2n_f N|F| \\ &- (|D|-1)\left(N + NN_{LP} + \frac{sN}{m}\log_2\left(\frac{sN}{m}\right)\right) \end{aligned} \tag{4.56}$$

where

$$T_c \begin{cases} > 0 & : \text{use coarse time method} \\ < 0 & : \text{use coarse frequency method} \end{cases} \tag{4.57}$$

We can greatly simplify this metric by only considering the dominant terms, resulting in

$$T_c \approx (|F|+2)2n_f N \log_2(2n_f N) - (|D|-1)\frac{sN}{m}\log_2\left(\frac{sN}{m}\right) \tag{4.58}$$

It turns out that in most cases for burst OFDM when a receiver is searching for the start of a transmission, meaning that $|D| >> |F|$, the coarse frequency domain is orders of magnitude

more efficient than time domain synchronization computation. However, in cases where a receiver is only updating its synchronization after an OFDM frame–meaning the receiver has a much smaller time search space $|D|$–then the complexity comparison between the two methods becomes more meaningful. Figure 4.6 depicts the comparison of computational complexity for the two methods across a range of values for the number of subcarriers, N, in an OFDM system. The results indicate that the coarse time computation method is often more efficient for cases where the timing search window, $|D|$, becomes smaller, as is the case for continuous OFDM transmission. These results indicate that the coarse frequency method should be used for initial synchronization stages where $|D|$ is often very large, but the coarse time method can be much more efficient when updating synchronization values during continuous transmission where the search range $|D|$ becomes much more manageable.

In addition, it is important to point out that the CAF is parallelizable. The most expensive computations for both of the methods presented in this work involve computing across the timing search range $|D|$ and the frequency search range $|F|$. However, these computations can be performed completely in parallel in order to decrease overall computation time.

4.1.5 Security of Cross Ambiguity Function Based Synchronization

It is important to discuss some of the security features and implications of CAF OFDM synchronization. One important aspect of the method presented here, is that there are almost no requirements on the structure of the preamble. This is a marked difference from many other existing algorithms. From a security standpoint, this feature allows the training symbols to be structured similar to other data symbols in order to make them less recognizable as critical system information to a third party observer. In addition, it allows for important system information to be embedded within the symbol. Since any training symbol must be known at the receiver, it is possible that using a table of symbols could allow an OFDM transmitter to convey useful system information to the receiver based on symbol choice.

Another important security feature of the methods presented in this paper is the fact that the normalization term for the CAF as defined in equation (4.3) is computed locally at the receiver. This protects the CAF metric normalization from being tampered with by a malicious device. In addition, it also helps to enable the use of thresholding values that allow the receiver to determine whether or not computed synchronization values are valid. This could even provide a receiver with a measure of SNR based on the result in equation (4.24), if the receiver had an estimate of the channel $|h|$.

Lastly, this synchronization method allows for the relative movement of OFDM training symbols within a frame, as suggested in [43]. There are various possibilities for implementing this type of 'sync-amble' training, one of which involving signaling the training symbol position within an OFDM frame based on the symbol chosen from a fixed symbol set. The coarse

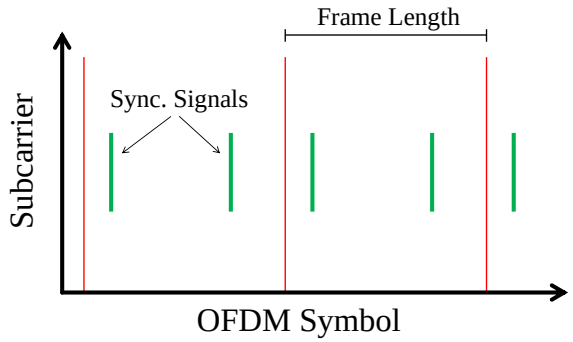

Figure 4.7: Example of Sync Signals within Frames

frequency method presented in this paper lends itself to this type of training symbol location randomization due to the fact that it requires the buffering of an entire frame. This means that a receiver could perform timing acquisition and carrier offset correction on the whole frame, then demodulate individual symbols in parallel. This 'sync-amble' randomization can be an important asset to OFDM security because it would prevent a malicious device from finding and locking on to a cyclostationary preamble symbol for continuous OFDM transmission.

4.2 Sync-amble Randomization

Many current implementations of OFDM rely on synchronization training symbols that are sent at the beginning of frame, or at a fixed location within the frame as shown in Figure 4.7. The receivers in these systems will locate these training symbols, perform error estimation and correction, and then proceed to demodulate the remainder of the OFDM frame. However, due to the block nature of OFDM waveforms, it is not requisite that the synchronization symbol be located at the beginning of the frame–it does not need to be a *pre*-amble.

This idea leads to the anti-jamming strategy termed preamble randomization. As shown in Figure 4.8, current OFDM systems insert the preamble at the beginning of a frame, both indicated by the name and represented by the green and yellow blocks. Data and control information is sent on the subcarriers in subsequent time blocks. It would be possible, however, for the preamble location to vary from frame to frame. Because this technique involves randomly varying the time position of the preamble within an OFDM frame, the training symbol is no longer strictly a preamble. In this case, the so called *sync-amble* will be located in a random time slot within a frame of OFDM symbols. There are multiple advantages to this strategy, as well as some limitations.

The first major advantage of randomizing the time location of the acquisition training symbol

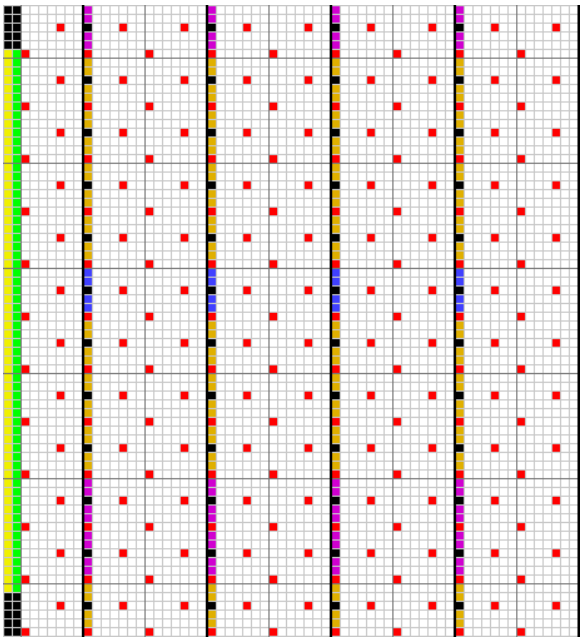

Figure 4.8: Time-Frequency diagram of an 4G frame using OFDM.

is that many of the attack presented in this paper, as well as in [38], rely on the jammer knowing when the preamble will be sent. The idea is that the jammer will not be able to lock on to a preamble location from one frame until the next, and by the time that the adversarial device does find the preamble within the frame, it will be too late to jam it. This means that the synchronization training symbols can be placed anywhere within the OFDM frame, and the location of these symbols can be varied from frame to frame in order to keep them from occurring periodically.

The optimal strategy for the transmitter would be do draw the location of the preamble randomly, according to $S_p \sim U(1, N_{fr})$ where N_{fr} is the number of symbols per frame, since this is the maximum entropy distribution for a discrete random variable with a finite support. In order to implement a randomly placed sync-amble, the synchronization strategy at the receiver would need to be updated. In order to minimize any increase in computational complexity, the transmitter and receiver would need shared, secret knowledge of the relative location of the sync signal within the frame. That way the search window for the timing point would be kept to a minimum, while allowing the receiver to identify the beginning and end of each frame.

Although this strategy presents an improvement over the predictability of current synchronization algorithms, the preamble is still detectable by adversarial communications devices. In addition, this attack could still be vulnerable to specific attacks such as the false preamble from [38]. This change to the OFDM synchronization would also require more processing at the receiver since the possible preamble location range becomes much greater. Despite

some minor drawbacks, sync-amble randomization would be a major improvement in OFDM synchronization security.

4.3 Simulation

In order to test the performance of the CAF OFDM synchronization method we conducted a number of simulations under practical wireless communication conditions. Both the coarse time and coarse frequency domain methods were implemented for an OFDM system using a single preamble symbol. The simulations were performed on an OFDM system with $N = 256$ subcarriers, with a timing point search range $|D| = 3 * N$ and a maximum frequency offset $N\frac{f_{max}}{f_s} = 5$ subcarriers for a total frequency search range $|F| = 11$ subcarriers. The cyclic prefix length was $N_{cp} = \frac{1}{8}N = 32$ samples.

The OFDM training symbols were sent within a miniature OFDM frame at an intermediate frequency through a simulated channel with both multipath channel effects and additive white Gaussian noise. Multipath effects were modeled as an FIR filter with tap weights determined by scaled normally distributed random variables, where the strongest path magnitude has an expected value of $E[|h_{max}|] = 1$, where $|h_{max}|$ represents the tap weight at the strongest path and $E[*]$ represents expected value. Simulations were conducted in order to determine the rate of successful symbol timing and carrier frequency offset estimations as computed via each of the CAF methods. Symbol timing acquisition points were tested against two criteria. The first criterion was that the timing point be estimated anywhere along the cyclic prefix in order to be considered correct, i.e. $\hat{d}_o - d < 0$ or $\hat{d}_o - d < 32$. The second criterion required that the exact timing point be computed at the receiver, but since timing point values were taken over a continuous interval either the floor or the ceiling of the delay value was considered correct, i.e. $|\hat{d}_o - d| > 1$. Carrier frequency offset estimates were considered incorrect if they were greater than five hundredths of a subcarrier away from actual frequency offset value, i.e. $|\hat{f}_o - f| > .05$.

Figures 4.9 and 4.10 illustrate the results of the simulations for each method. They show each method to be relatively robust even at low SNRs. These results make sense considering the weak bound in equation (4.24), which is illustrated in Figure 4.3. Estimation errors that would preclude the receiver from performing demodulation start to arise around -5 dB SNR.

In addition, we measured the performance of the each method's carrier frequency offset estimation against the Cramér-Rao lower bound (CRLB). The CRLB limits the accuracy of the frequency offset estimator in terms of the variance of the error between the estimated value and the true offset value. The relationship of this bound to computing the is discussed in detail in [45], but for the purposes of this work we only compute the standard deviation of the carrier frequency offset estimation error as

$$\sigma_f = \frac{\sqrt{3}}{\pi T}\frac{1}{\sqrt{BT\gamma}} \tag{4.59}$$

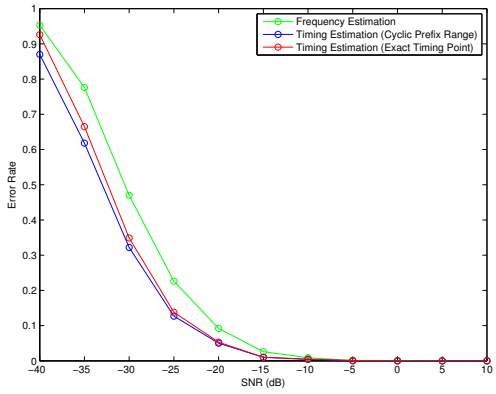

Figure 4.9: Symbol timing and carrier frequency offset estimation performance of the coarse frequency domain method. The plot shows the percentage of incorrect computed values, where errors are considered to be timing points outside of the cyclic prefix range and frequency offset estimates more than five hundredths of a subcarrier away from the actual frequency offset.

where B is the noise bandwidth at the receiver in Hz, T represents the length of the training symbol in seconds and

$$\frac{1}{\gamma} = \frac{1}{2}\left[\frac{1}{\gamma_1} + \frac{1}{\gamma_2} + \frac{1}{\gamma_1\gamma_2}\right] \tag{4.60}$$

where γ_1 and γ_2 represent the effective signal-to-noise ratios for each copy of the preamble. Since the reference copy at the receiver is noiseless–making γ_2 effectively infinite–the effective CAF SNR becomes

$$\gamma = 2\gamma_1 \tag{4.61}$$

where γ_1 is the SNR for the received training symbol.

The results for these simulations are shown in Figure 4.11. The plots show that, while the CAF estimator does not achieve the CRLB under multipath conditions, the carrier frequency offset estimation is still relatively accurate. It is important to note that the CRLB does not account for multipath. In addition, since the symbol timing point for OFDM systems is computed relatively imprecisely, the precision of the frequency offset estimate will suffer some as well.

In addition, the advantages OFDM CAF synchronization poses in adversarial jamming scenarios, we have simulated systems using both the method proposed in [14] and the CAF to perform OFDM acquisition. Each algorithm was tested using 224 subcarrier OFDM modulation with a cyclic prefix 1/8 of the symbol length. The timing point search was constrained to a three symbol window, while the maximum allowable carrier frequency offset was 5 subcarrier spacings. Timing estimation errors occur when a point is taken outside of the range

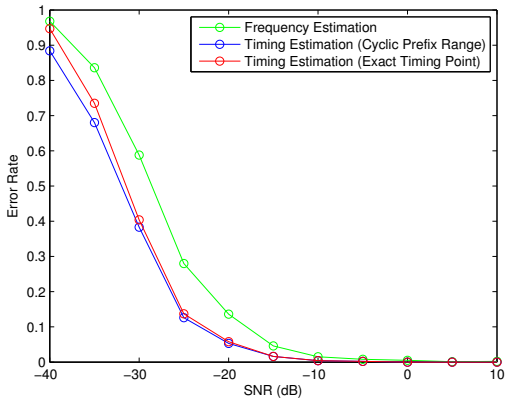

Figure 4.10: Symbol timing and carrier frequency offset estimation performance of the coarse time domain method. The plot shows the percentage of incorrect computed values, where errors are considered to be timing points outside of the cyclic prefix range and frequency offset estimates more than five hundredths of a subcarrier away from the actual frequency offset.

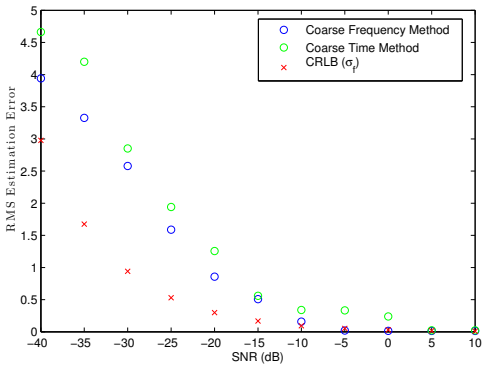

Figure 4.11: Performance of the carrier frequency offset estimation for both the coarse time and coarse frequency CAF computation methods vs. the Cramér-Rao lower bound. The measured values represent the root mean squared error values of the frequency offset estimates.

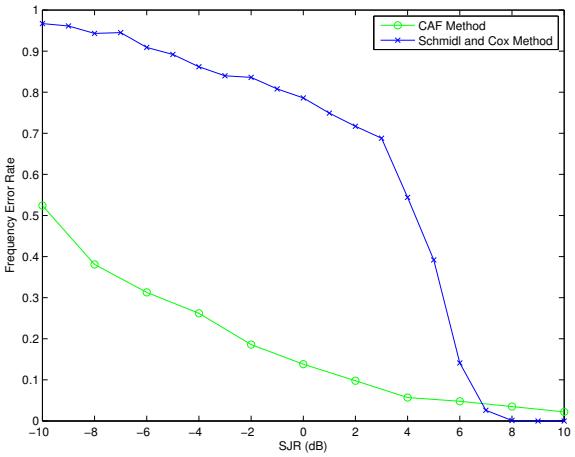

Figure 4.12: Comparison of performance between Schmidl and Cox's method and the CAF based synchronization algorithm in the presence of the phase warping attack

of the cyclic prefix. Frequency offset estimation errors occur when the disparity between the estimation and the true frequency offset is more than a five hundredths of a subcarrier.

We measured the CAF synchronization performance relative to the method from [14] in the presence of the phase warping attack proposed in [42]. This attack aims to disrupt the frequency offset estimation by sending a preamble symbol at a random RF within the possible search range. For this experiment, it was assumed that the jammer had knowledge of both its channel and the transmitters, but not the exact sequences used for the two synchronization symbols. Figure 4.12 demonstrates the advantages of using CAF synchronization in the presence of intelligent adversarial attacks. In any scenario where the jammer is transmitting at a power equal to or more than the synchronization symbol, the CAF demonstrates a significantly lower frequency error estimation rate. This can be attributed to the fact that the CAF synchronization relies on a specific sequence at the receiver, as opposed to a whole set of sequences conforming to the preamble structure described in [14].

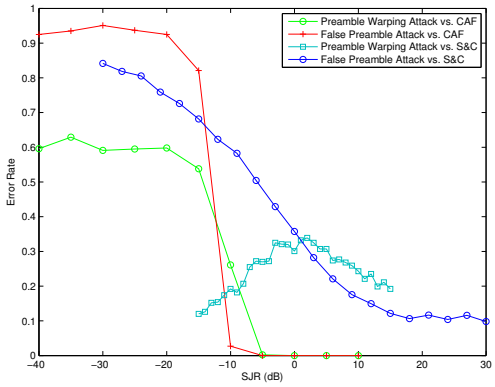

Figure 4.13: Timing estimate error rate as a function of SJR for the CAF synchronization algorithm vs. the Schmidl and Cox synchronization algorithm in the presence of various attacks. The CAF synchronization mitigates the power efficient attacks at the expense of acquisition complexity.

Chapter 5

Adaptive Dynamic Spectrum Access Radio Warfare

Looking towards future wireless systems, it is apparent that dynamic spectrum access will become an integral technology. This is because current policy has created a kind of fictional traffic jam on the radio frequency (RF) spectrum. On one hand it seems like there is no room for any frequency allocation, which is depicted in Figure 1.1. On the other hand, a significant portion of the spectrum goes unused depending at different times and frequencies. This phenomenon is illustrated in Figure 5.1 It is becoming clear that DSA technology is both a pertinent and viable solution to this issue, as described in Section 2.2. With the rise in importance of DSA technology, it is critical to investigate DSA interference and electronic warfare.

As demands on performance of wireless radio frequency networks increase, the availability of usable spectrum continues to diminish. Spectrum crunch has led to a significant increase in research geared towards spectrally efficient technologies. This area of work, coupled with the increasing flexibility and adaptability afforded to wireless devices by the advent of software defined radio and subsequently cognitive radio, has led to the idea of dynamic spectrum access for wireless networks.

Dynamic spectrum access is a broad term which encompasses various types of technology and networks. A core principle of all DSA networks, though, is that allocation of spectrum within a licensed frequency band varies in time between different users. A significant amount of work has been done to properly define both the term DSA and the different types of networks that the term refers to [46, 28, 29, 27].

Hierarchical DSA is one approach in particular with a number of advantages as well as a number of questions left to be explored. It is an appealing flavor of DSA because it incorporates licensing and policy–much like that which already exists–with spectrum sensing cognitive radio technology. Summarily, the idea is that 'primary' users in hierarchical DSA

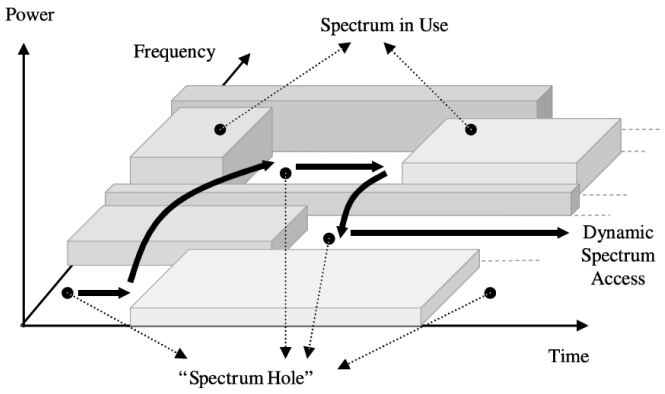

Figure 5.1: Time-frequency diagram illustrating 'holes' in the wireless spectrum due to inactivity.

have first rights to the spectrum over a given bandwidth. 'Secondary' users can then access spectrum at their discretion as long as they adhere to policies aimed to prevent interference for the primary users.

The definitions of users within realistic networks, however, are more nuanced than strictly two sets of users, labeled primary and secondary. For example, it is likely desirable for a network to place priority on emergency broadcast related transmission, critical military users or network critical information. In these cases, while it is important to protect the primary users of the network, it is critical that these secondary users are not denied service. These scenarios give rise to different types of DSA radios, or rather different operating modes.

In the context of a DSA network, it is very useful to consider the problem of radio identification. In a network where spectrum sharing and coordination is performed autonomously, sensing and policy are not the only factors which impact cognitive radio decisions. In addition, learning over time can help DSA radios better incorporate into the network while still adhering to the required radio policies. This building of radio 'etiquette' is critical to DSA networks. DSA network security is also a critical issue to consider as it relates to successful DSA deployment. Behavioral based identification algorithms can help identify and protect networks from malignant users and other security threats. Some work has been done in exploring alternative methods [47]. However, the majority of previous work is focused on identifying and tracking specific radios as opposed to identifying and classifying unknown radios using machine learning methods according to behavior within a DSA network framework.

The model used for this study comes from [48], where a radio is operating in a potentially hostile environment. The two modes used for this study are abstractions of the 'NIB' mode and 'Protection' mode, a useful and practical example of how secondary DSA radios might behave according to differing policy. While these modes are the example analyzed in this

work, we are hopeful that this work extends easily to many types of DSA radios.

5.1 Hierarchical Dynamic Spectrum Access Networks

Many of the problems involving multi-tiered DSA networks have been studied in detail [48, 49, 26, 50]. This work has given rise to the idea of different operating modes, which allow networks to assign a different level of priority to secondary user communication. The differences between the radio modes are best understood based on the inherent architecture of a secondary DSA radio.

Hierarchical DSA radios are effectively decision engines with input from a combination of policy based reference knowledge, plus spectrum sensing and observation based information. A simple incarnation of this decision engine can be modeled as a state machine of order 3, as shown in Figure 5.2.

This typical model for a DSA radio is a finite state machine. The scan state is where the radio combines spectrum sensing knowledge with policy knowledge to make a decision dictating what state it transitions to. The rendezvous state occurs after the radio has chosen a channel or piece of spectrum to transmit on; the radio rescans the RF environment then makes a transition decision. The transmit state represents the radio transmitting and receiving, but from the perspective of this model it represents a state where the radio holds until the RF environment induces a state change, similar to the scan state.

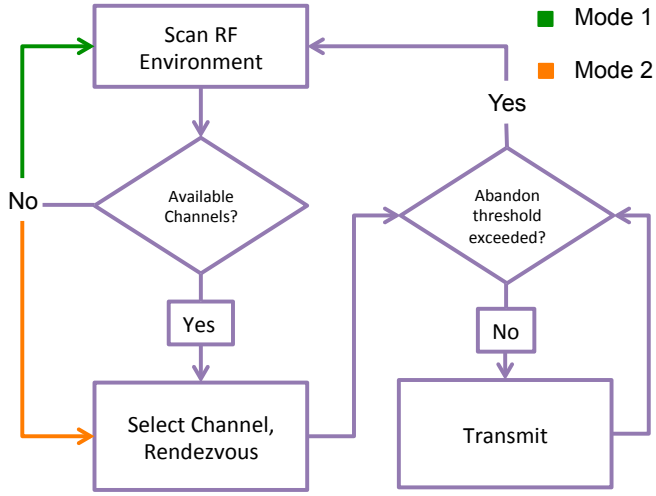

Figure 5.2: Generalized decision engine architecture for a secondary DSA radio. The radio evaluates the RF environment after each transition to determine the next one. The green and orange arrows show the single difference between the two radio modes' behaviors. The state transition behavior depends only on the current state.

The inherent difference between these two radio modes is the channel selection decision. The mode 1 decision engine is based on the policy of minimizing interference to primary users as its primary goal, illustrated in Figure 5.2. The mode 1 radio will not select a channel and begin to transmit until there is a channel available. This availability is determined based on the sampled power on a given channel being lower than an occupy threshold $\sigma_{o,f}$.

A mode 2 radio will go through the same decision flow as the mode 1 radio, with a different primary goal. Again referring to Figure 5.2, the mode 2 radio will always select a channel to transmit on, even if the power on every available channel is greater than the occupy threshold $\sigma_{o,t}$. This reflects the radio's primary objective of transmitting its information; minimizing interference to primary users is a secondary priority. In the event that all channels are determined occupied, the mode 2 radio will choose the channel with the lowest measured power in order to minimize interference to itself.

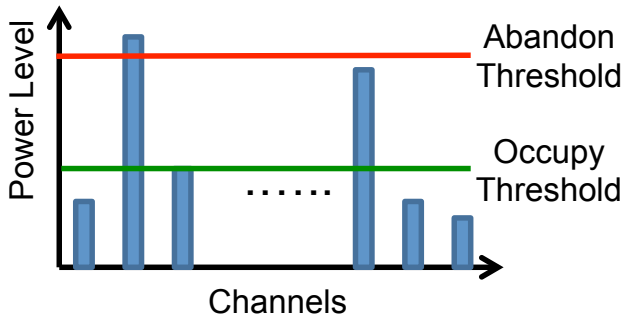

Figure 5.3: A visualization of the spectrum sensing information that secondary DSA radios use in their decision engine. Channel power measurements, in blue, are taken within the bandwidth of interest and compared to the decision thresholds.

Each radio mode also has a respective abandon threshold, defined as $\sigma_{a,f}$ and $\sigma_{a,t}$ for mode 1 and mode 2, respectively. The thresholds are constrained by

$$\sigma_a \geq \sigma_o > 0 \tag{5.1}$$

for both radio modes. Figure 5.3 is an example of the RF environment with the decision thresholds imposed to illustrate the secondary radios sensing. These power thresholds determine whether a DSA radio will leave a channel that it is occupying to revert to the scan state. These thresholds may or may not be the same depending on the policies assigned to the radio modes as well as the RF environment. After abandoning a channel, the secondary radio reverts to the scan state and loops until it's objective is achieved.

5.2 Traffic Modeling

One of the key factors dictating radio behavior in DSA networks is user traffic. Variables such as traffic density, resource availability and average resource usage are important in determining the behavior of the radios on the network. While radios on non-DSA networks are often modeled statically or piecewise in a stochastic sense, the probability distributions that govern DSA radio behavior can change rapidly depending on traffic patterns in a given network. Modeling this behavior starts with modeling the behavior of primary user traffic.

A network with m channels is modeled as an M/M/m queueing system. The arrival of traffic on the network is represented by a continuous random process $N(t)$ with a mean arrival time of λ. While the expected arrival time is not necessarily fixed, it is reasonable to assume that it is over the time period of analysis for modeling DSA radio behavior. The service times for each arrival are modeled as a continuous random variable t_s, with an expected value μ.

We also model the average power of the primary users with the chi-squared distribution

$$P_{prim} \sim \sigma_{prim}\chi^2(1) \tag{5.2}$$

where the scale factor σ_{prim} represents the average primary user power seen at the secondary DSA radio. This model is based on the average output of a DSA radio being modeled as a Gaussian random variable.

5.3 System Description

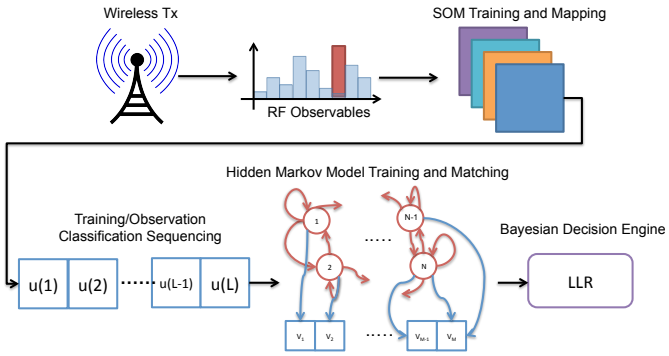

Figure 5.4: The high level architecture for the proposed system. The green arrows show the signal flow for both the training and identification phases of the system. Each different class of radio trains against this system in order for an unknown transmitter to be identified within a known class of radios.

The system model described in this paper can be broken down into three phases. The first stage of the system deals with the classification problem of the RF environment using a

self organizing map. The next stage utilizes the classified RF observations for the training of Hidden Markov Models that describe each radio. The final stage of the system uses a Bayesian decision metric in order to classify an unknown radio. Figure 5.4 describes the system architecture. It is important to note that the system operates in two ways–it has both a training stage and a classification stage which are identical in structure. The motivation for using a classification scheme for observations of an RF environment stems from the need for discrete emission HMMs.

5.3.1 Classification with Self Organizing Maps

In order to both classify radio behavior based on a given RF environment, as well as condense the space of RF observations in a given system, it is helpful to utilize unsupervised learning algorithms to perform clustering on multidimensional RF observation vectors. We define the observation vector

$$Y_1(n) = \begin{bmatrix} C(n) \\ p_1(n) \\ \vdots \\ p_m(n) \end{bmatrix} \tag{5.3}$$

where $C \in \{0, 1, .., m\}$ is the transmit channel of the secondary radio, where $C = 0$ represents no transmission. $p_i \in [0, \infty)$ for $i \in 1, 2, ..., m$ is the measured power on channel i out of m channels. Each of the components of the observation vector varies with time, which is denoted by the discrete index vector n.

In order to utilize this data to train a hidden Markov model, these observations vectors must be discretized, meaning that we need a function to perform the mapping

$$f : \mathbb{R}^{m+1} \to \mathbb{Z}. \tag{5.4}$$

The choice to map the observations to integers is explained in more detail in the next section. In many practical cases the dimensionality of Y_1 will be high, as will the entropy of its components. Subsequently, an ideal solution for this problem incorporates both dimensionality reduction and efficient quantization of the observation vectors.

A self organizing map (SOM) is an unsupervised learning tool that is well suited to this task. Self organizing maps are forms of artificial neural networks (ANN) that are trained via unsupervised learning to cluster high dimensional data into a discrete two dimensional space [51]. This discretization is ideal for converting observations from an RF environment into countable emissions suitable for training HMMs.

The self organizing map is initialized with a topology of $s \times s$ neurons. The map is trained using example vectors via the well known competitive learning algorithm. There are two different training vectors we utilize for this process, defined as

$$O_i = Y_i(n), \qquad i = 1, 2 \ , \ n = 0, 1, ..., L-1, L \tag{5.5}$$

where L is the length of the training sequence. This training set is a time series–in n–of data in the observation vector Y.

The second observation vector ($i = 2$) used to test this system is defined as

$$Y_2(n) = \begin{bmatrix} C(n) \\ ||p(n)||_1 \\ ||p(n)|| \\ ||p(n)||_\infty \\ s^2(p(n)) \\ \bar{p}(n) \end{bmatrix}, \tag{5.6}$$

consisting of multiple computed features of the observed RF spectrum. The second, third and fourth features, which are norms of the channel power observations, are defined as

$$||p(n)||_l = \left(\sum_{i=1}^{m} p_i^l(n) \right)^{1/l}, \tag{5.7}$$

where $||p(n)||$, the Euclidean norm, is computed for $l = 2$. In addition, the maximum norm $||p(n)||_\infty$ is computed

$$||p(n)||_\infty = \max(p_1(n), p_2(n), ..., p_m(n)). \tag{5.8}$$

The fifth feature, the unbiased sample variance, is defined

$$s^2(p(n)) = \frac{1}{m-1} \sum_{i=1}^{m} (p_i(n) - \bar{p}(n))^2 \tag{5.9}$$

where $\bar{p}(n)$ is the sample mean of the power observations, also the final feature, defined as

$$\bar{p}(n) = \frac{1}{m} \sum_{i=1}^{m} p_i(n). \tag{5.10}$$

We chose to use these feature vectors as an alternative basis for classifying the RF observations due to the nature of the SOM classification algorithm. Competitive learning tends to cluster samples that are close in vector space. However, RF observations that are similar are not necessarily close in vector space. For example, consider two possible observations, one at time $n = n_1$ where $p_1, p_2, p_3 \ll \sigma_o$ and $p_4, ..., p_m > \sigma_a$, and another at time $n = n_2$ where $p_1, ..., p_{m-3} > \sigma_a$ and $p_{m-2}, p_{m-1}, p_m \ll \sigma_a$. These scenarios are distant when represented in the observation vector Y_1, however to a DSA radio it represents two similar scenarios where there are three channels that seem unoccupied. For these reasons we trained the system with multiple observation vectors and compared overall performance in Section 5.4.

For either choice of the observation vector, both the SOM training and mapping will assign each example vector to a particular node on the $s \times s$ map. Formally, the SOM will map

$$Y_i(n) \to u_b, \quad n \in L, \tag{5.11}$$

for $u \in \mathbb{Z}$, specifically

$$u \in \{1, 2, .., s^2 - 1, s^2\}. \tag{5.12}$$

The term u is used as the SOM node index, where u_b represents the index of the node within the SOM that is the best match for an observation vector. The map not only groups similar observations together, but also develops a unified distance matrix (or a U-matrix) which topologically represents the distance between the nodes in the map. Examples of this classification process can be seen in Figures 5.5 and 5.6. The SOM can then output the node of each RF observation as a discrete value representing a particular cluster. This discretization of the observation space facilitates the use of HMMs as the model for the DSA radios.

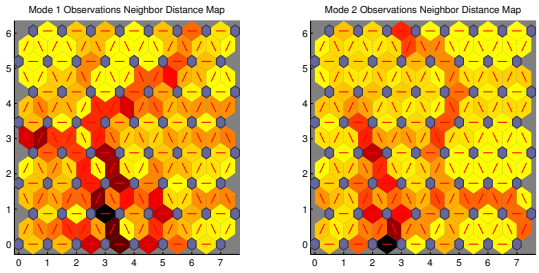

Figure 5.5: Neighbor distance maps for the self organizing maps constructed from the RF observations from each radio mode. These maps are an interpretation of the unified distance matrix that represents the topology of the self organizing map. Black represents the greatest distances between neurons and yellow represents the least distance.

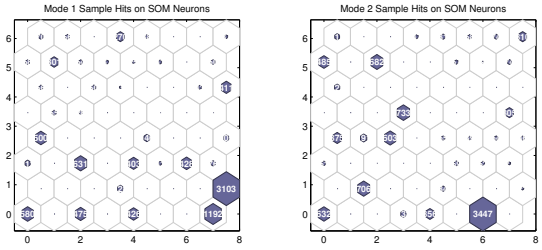

Figure 5.6: Sample assignments for each RF observation training vector to the self organizing map. These plots represent the discretization of the observation space via assigning observation samples to different neurons in the map. The size of the blue hexagon in each neuron represents the frequency of an observation being assigned to it.

5.3.2 Probabilistic Radio Representation Using Hidden Markov Models

Explicitly modeling DSA radios with different behaviors is a complex problem, especially for an outside observer with limited *a priori* knowledge of the radio architecture. For this reason, it is of interest to model these radios stochastically. Since DSA radio behavior is dynamic by definition, it is important to select a model that can preserve and sufficiently represent the transition in radio behavior. Mixture models are a well known method for describing similar systems. DSA radios in particular demonstrate state dependent behavior reminiscent of a Markov chain, shown clearly in Figure 5.2.

We probabilistically represent each of the two radio modes using hidden Markov models. The general underlying state structure of each of these models is described by the transition matrix

$$a_{ij} = P[q_t = s_j | q_{t-1} = s_i] \qquad 1 \leq i, j \leq N \tag{5.13}$$

where q_t is the current observation and q_{t-1} is the previous, and a_{ij} is the transition probability from state i to state j, subject to the constraints

$$a_{ij} \geq 0 \tag{5.14}$$

$$\sum_{j=1}^{3} a_{ij} = 1 \tag{5.15}$$

In this paper, we would like to consider the more general case $a_{ij} \in R^{NxN}$. Since it is feasible that the architecture and/or the policy that governs the radio is unknown to the observer, it is important to develop a system for identifying a radio with an unknown number of states. The ergodic state transition model of an unknown radio with N states is

$$a_{ij} = \begin{bmatrix} a_{0|0} & \cdots & a_{0|N} \\ \vdots & \ddots & \vdots \\ a_{N|0} & \cdots & a_{N|N} \end{bmatrix} \tag{5.16}$$

where the notation $a_{i|j}$ represents the state transition probability from i to j.

The emission probability matrices associated with these models are dependent on the method for observation quantization used in the HMM training. In order to determine the impact of the observation space on the accuracy of radio identification, it is important to compress the information from the RF environment to different levels. This idea comes from the unknown underlying complexity of the DSA radio system. The general emission matrix for the model is defined

$$b_{ij} = P[v_i(t) | q_t = s_j], \qquad 1 \leq j \leq N, 1 \leq i \leq M \tag{5.17}$$

where v is the set of the discrete positive integer observations and $M = |v|$. It is important to note that $v \subset u$ and $M \leq s^2$, meaning not necessarily all of the SOM nodes have observation vectors classified to them during mapping.

In this work, the value of M is determined by the number of neurons utilized in SOM training, as shown in Figure 5.6. The discretized training sequences O_i are then used to train hidden Markov models for each radio mode via the well known Baum-Welch algorithm. One of the most critical challenges of developing HMMs for these radio modes is the initial guess for the radio model. We avoided making too many assumptions about the underlying structure of the radios. The models are ergodic, with uniform state transition probabilities, meaning

$$a_{ij} = \frac{1}{N}, \qquad 1 \leq j \leq N, 1 \leq i \leq N. \tag{5.18}$$

The initialization of the emission probability matrix b is less trivial–the solution at which the HMM training algorithm converges is greatly dependent on the initialization of the emission probability matrix [52]. Initializing these probabilities randomly will usually cause the algorithm to converge on a model with uniform state transition probabilities and emission frequencies as the output probabilities. This essentially turns the HMM into a one state system, which is not the best model, as will be shown in Section 5.4. Instead, we initialize the emission probabilities with random perturbation to a uniform distribution, specifically

$$b_{ij} = \frac{1-\epsilon}{j} + \epsilon \frac{x_{ij}}{\sum_{j \in M} x_{ij}}, \quad 0 \leq \epsilon \leq 1. \tag{5.19}$$

The value of ϵ is the perturbation factor of the initial distributions, while x_{ij} is a set of standard uniform independent, identically distributed (i.i.d.) random variables. Any value of $\epsilon > 0$ will produce an initial uniform distribution with uniformly distributed perturbations. Once the best guess distributions are determined for the HMMs the models can be trained and used for classification of unknown radios.

5.3.3 Classifying Unknown Radios

The final stage of the radio identification system classifies unknown radios as either Mode 1 or Mode 2. The unknown radio observations are discretized via mapping to trained self organizing maps. The discrete observation sequences can be used to compute the probability $P(T|\lambda)$ that indicates how likely it is that the sequence came from a HMM described by the parameter λ. These probabilities are computed using the forward procedure of the Baum-Welch (or forward-backward) algorithm.

Given two radio models, with distinct parameters λ_1 and λ_2, we can use the log of the probabilities $P(U|\lambda_1)$ and $P(U|\lambda_2)$ for the unknown observation sequence U to compute the log likelihood ratio

$$LLR = \log\left(\frac{P(U|\lambda_1)}{P(U|\lambda_2)}\right). \tag{5.20}$$

The logs of the sequence probabilities are used for computations due to the fact that the actual probabilities can quickly approach zero. The sign of the log likelihood ratio is used

to determine the classification of the unknown radio via the Bayesian decision rule, while LLR's of zero are classified as undetermined.

5.4 Simulation and Analysis

In order to verify this model and determine it's performance, we implemented a MATLAB simulation of the two example radio modes, the primary user models and the RF environment. We set the occupy and abandon thresholds for both the federal and tactical mode radios at $\sigma_o = 10^{-6}$ and $\sigma_a = 10^{-4}$. Primary user arrivals were modeled as a homogenous Poisson process, with rate parameter $\lambda = .1$ and mean power determined by the random variable P_{prim} where $\sigma_{prim} = \sigma_a$. We modeled a m=10 channel network with exponential random variable service time t_s with a mean service time of $\mu = 1$. The channel noise power P_n was assigned a mean value of 10^{-9}. It is important to note that we carefully selected the traffic parameters to ensure a certain user density within the network. This is an important aspect of radio identification which greatly impacts the modeling of the radios. In DSA networks where secondary radio behavior is guided by policy that protects primary users' ability to access spectrum resources, secondary radio behavior will vary greatly based on primary user density, as well as overall user density. While investigating the effect of user density on this identification system is outside of the scope of this paper, it is an important part of our future work.

For HMM training we used variable length training sequences based on traffic from a fixed amount–10,000–users through the channel queue model. Each model was trained on 10 of these sequences. In order to simulate a scenario where the number of hidden states for a radio model is unknown, we simulated across a range of states from $N = 1$ to $N = 10$. While the model for $N = 1$ is trivial, it models the radios as having stationary distributions, which can be a simple identification technique if the radio modes demonstrate significantly different emission probabilities. While the initial guess for an unknown system can be greatly improved, the problem is not trivial and is a focus for future work.

Table 5.1: Radio Identification Success Rates Using O_1, 1 Map

	Number of States									
$s \times s$	1	2	3	4	5	6	7	8	9	10
4	.881	.653	.538	1.0	.484	.998	1.0	1.0	1.0	1.0
9	.958	.897	.806	.775	.991	.949	1.0	.861	.494	1.0
16	.923	.775	.766	.722	.489	1.0	.52	.999	.162	.885
25	.942	.809	.925	.653	.613	1.0	.594	.297	.507	.215
36	.948	.905	.939	.516	.564	.494	.731	1.0	.999	.205
49	.915	.809	.807	.711	.981	.999	.528	1.0	.156	1.0
64	.877	.782	.86	.648	.556	1.0	.93	.053	.994	.004

Tables 5.1-5.4 show the simulation results for this work. While there are a number of regions

Table 5.2: Radio Identification Success Rates Using O_1, 2 Maps

	Number of States									
$s \times s$	1	2	3	4	5	6	7	8	9	10
4	.913	.919	.624	.491	.490	1.0	.917	1.0	1.0	1.0
9	.666	.655	.593	.574	.672	.732	.739	.749	.944	1.0
16	.974	.840	.819	.645	.656	1.0	1.0	.987	.998	1.0
25	.469	.469	.469	.469	1.0	.530	.488	1.0	1.0	1.0
36	.513	.522	.5	.636	.5	.775	1.0	.871	.520	.580
49	.523	.520	.526	.596	.523	.621	.657	.714	.957	.990
64	.497	.496	.497	.497	.497	.998	.949	.961	.996	1.0

Table 5.3: Radio Identification Success Rates Using O_2, 1 Map

	Number of States									
$s \times s$	1	2	3	4	5	6	7	8	9	10
4	.878	.897	.498	.869	.474	.995	1.0	1.0	1.0	1.0
9	.946	0.911	.847	.665	.659	.517	.488	.997	1.0	1.0
16	.916	.87	.618	.825	.533	1.0	.966	.578	.999	.994
25	.872	.882	.676	.526	.614	.52	.88	.98	.508	.448
36	.929	.869	.955	.675	.525	.516	.893	.802	.994	.665
49	.915	.867	.796	.648	.687	.98	.996	.511	.984	.748
64	.886	.846	.803	.611	.93	1.0	.861	.992	1.0	1.0

where the identification system exhibits particularly poor performance–any identification rate around .5 essentially means the system is just guessing–there are also multiple combinations of SOM and HMM size that identify the unknown radios very accurately, in some cases with perfect accuracy. It is of interest to note that using a SOM size of 4 nodes, which vastly reduces the entire observation space to 4 discrete outputs, performed perfectly in all cases where $N > 7$. This result is encouraging because simpler implementations of this system are desirable for realistic implementation.

There seems to be two different regions in each table that demonstrate poor performance. The first is in the lower rows of the Tables 5.2 and 5.4. These regions show particularly low identification rates which seem to be attributed to lack of training data. Since two maps are used in these cases, each map is trained with half as much data as in the single map case. Choosing the correct amount of training data for these systems is a focus of further research. The second region demonstrating poor performance lies to the left hand side of each table, where a relatively low number of states is chosen for the HMMs. The last trend shown in the results is that there are significant drops in performance near many of the areas of peak performance when looking at the tables in a row-wise fashion. This result indicates that system parameters must be chosen carefully for a practical implementation of this system. Developing the mathematical framework for automatic parameter selection is a key area of future research.

There were some rather surprising results produced by these simulations as well. There are multiple cases–such as N=8 and $s \times s$=64 in Table 5.1–where the system trains poorly and

Table 5.4: Radio Identification Success Rates Using O_2, 2 Maps

	Number of States									
$s \times s$	1	2	3	4	5	6	7	8	9	10
4	.923	.902	.6	.469	.469	.976	1.0	1.0	1.0	1.0
9	.719	.697	.649	.605	.702	.993	.723	1.0	1.0	.932
16	.599	.61	.602	.57	.526	.978	1.0	1.0	.948	.563
25	.511	.511	.511	.511	.494	.746	.945	1.0	.861	.002
36	.518	.518	.518	.518	.518	.657	1.0	.534	1.0	1.0
49	.597	.583	.569	.561	.486	.869	.982	.947	.997	.984
64	.504	.505	.488	.51	.514	.519	.567	.123	.082	.386

identifies the radios almost perfectly incorrectly. In addition, many of the more successful simulations of the system occur when $N > 5$, despite the fact that the underlying decision engine for the radio modes seem simple. This result may very well be attributed to having no information about the initial guesses of the transition and emission matrices for the HMMs, indicating that there is a trade off between *a priori* knowledge and system complexity. In some example training for this system, we provided theorized initial guesses to the HMM parameters that we inferred from the behavioral model with much more success for values of $N = 3$. Developing better methods for model initialization is a priority for future research.

Chapter 6

Conclusion and Future Work

Physical layer security is an important topic as it relates to 4G and future generations of systems. It is important to consider these wireless security issues for a wide scope of systems and scenarios. As more cognition is introduced in to the realm of electronic warfare, it is critical to find optimal strategies for both attack and defense. In this work we have presented several strategies and solutions to problems regarding physical layer cognitive electronic warfare.

We have discussed how the synchronization process in any system employing OFDM is paramount to successful communications and how this process is also extremely sensitive to estimation errors [7]. While synchronization methods similar to those proposed in [14] perform very well against uncorrelated interference, the acquisition process can be severely degraded by intelligent jamming attacks [38, 42]. We have presented a number of these attack strategies that target the physical layer structure of OFDM synchronization symbols in order to cripple timing acquisition and carrier frequency offset estimation, along with theoretical and simulation based performance analysis of OFDM systems in the presence of these attacks. We have also demonstrated how the synchronization performance improves when using CAF synchronization in the presence of one of these smart jamming attacks. In addition, we have proposed a structure for securing OFDM synchronization via frame location randomization of training symbols. These tactics in conjunction with one another offer the possibility of dramatically improving OFDM synchronization security at the physical layer.

The CAF synchronization methods presented in this paper are a novel approach to performing training based symbol timing acquisition and carrier frequency offset estimation for an OFDM system. We have shown that this method is viable for robustly performing OFDM synchronization through both mathematical analysis and simulations that incorporate some of the realistic effects of a wireless communication environment. While the methods we presented are relatively costly from a computational standpoint, the algorithms are designed to utilize the efficiency of the DFT, which is inherent to the OFDM structure and lends to low cost hardware implementation. Furthermore, large portions of the computations can be run

in parallel, which increases the feasibility of these algorithms in conjunction with developments in parallel computing technology and the coinciding increase of affordability. These methods, along with future work for synchronization and other vital processing functions, can help to improve the overall security of OFDM based systems.

There are a number of areas for future work in the area of OFDM synchronization security and ambiguity function based synchronization. It is important to develop a functioning implementation of the CAF synchronization in order to both demonstrate its viability as processing method for OFDM acquisition and carrier frequency offset estimation, but also in order to test its performance under realistic multipath conditions and fading scenarios for the case of mobile OFDM based systems. In addition, the sync-amble randomization concept that applies to the OFDM control layer is a concept that can be further developed. This technology would most likely need to make use of a public/private key strategy in order to grant access to shared information about sync symbol locations.

Looking one layer higher to MAC layer security considerations for future systems, we have shown that by using a combination of machine learning techniques and probabilistic modeling for DSA radios that behavior based identification is possible. Cognitive approaches such as these are vital to developing cognitive radio technology with the ability to deploy in realistic communications environments with established infrastructure already in place. The problem of behavior based cognitive radio identification will be fundamental for both commercial and tactical DSA network security research.

By integrating machine learning approaches in to this technique, we have been able to greatly collapse the space of observations that would typically be available to a DSA radio. Utilizing sequence based stochastic techniques like hidden Markov models in order to model radios preserves the temporal fidelity of the behavioral statistics. HMMs are shown to be one such statistical tool that can provide this type of simplified mathematical representation for cognitive radio decision engine and outputs. We have shown that it is possible to train this system and automatically categorize DSA radios based on observable RF behavior with a high level of accuracy when model parameters are correctly chosen.

While the initial results are promising and warrant future work on this problem, this area of work represents a huge problem space with a plethora of future work. There are still a range of variables to consider that will impact the system, including primary user traffic density, observation noise and limitations and improved modeling and initial guesses for DSA radio HMMs. In addition, in order to optimize the system in terms of parameter selection, it will be important to incorporate some model selection methods based on information theoretic metrics of the observation space. In addition, there are a number of underlying theoretical concepts left to be formalized in order to fully develop this type of system.

The issues of OFDM synchronization and DSA radio security are important to consider for the future of wireless systems as both technologies become more prevalent. The challenges presented on both the attack and defensive sides of cognitive electronic warfare will only continue to increase in scope and complexity with the development of 4G and future generation

system capabilities. It will be vital for future implementations of OFDM systems to secure the physical layer control processes, particularly synchronization. Likewise, as DSA capabilities are realized for wireless systems, developing automated, cognitive algorithms for radios to assess their environments will be critical to the security of DSA capable networks. It is paramount that adequate wireless physical layer security features are developed to match the advances in physical layer technology for modern wireless systems.

Bibliography

[1] H. C. Keong. (2001, November) Overview of OFDM Design. National University of Singapore.

[2] J. Zhang, Y. Liu, S. Ozdemir, R. Wu, F. Gao, X. Wang, L. Yang, and F. Nori, "Quantum internet using code division multiple access," *Scientific Reports*, vol. 3, 2013.

[3] The IEEE 802.16 Working Group on Broadband Wireless Access Standards, *802.16e-2009*, The IEEE 802.16 Working Group on Broadband Wireless Access Standards Std., 2009.

[4] 3rd Generation Partnership Program (3GPP), *Long Term Evolution (LTE)*, The 3rd Generation Partnership Project (3GPP) Std., 2009.

[5] R. W. Chang, "Synthesis of Band-Limited Signals for Multichannel Data Transmission," *The Bell Systems Technical Journal*, vol. 45, pp. 1775–1796, 1966.

[6] S. Weinstein and P. Ebert, "Data Transmission by Frequency-Division Multiplexing Using the Discrete Fourier Transform," *IEEE Transactions on Communication Technology*, vol. 19, pp. 628–634, 1971.

[7] R. van Nee and R. Prasad, *OFDM for Wireless Multimedia Communications*. Boston, MA: Artech House, 2000.

[8] T. Pollet, M. V. Bladel, and M. Moeneclaey, "BER Sensitivity of OFDM Systems to Carrier Frequency Offset and Wiener Phase Noise," *IEEE Transactions on Communications*, vol. 43, no. 2/3/4, Feb/Mar/Apr 1995.

[9] H. Minn, V. Bhargava, and K. Letaief, "A Combined Timing and Frequency Synchronization and Channel Estimation for OFDM," in *IEEE International Conference on Communications (ICC)*, June 2004.

[10] M. Moretti and I. Cosovic, "OFDM Synchronization in an Uncoordinated Spectrum Sharing Scenario," in *IEEE Global Telecommunications Conference (GLOBECOM)*, November 2007.

[11] S. Patil and R. Upadhyay, "A Symbol Timing Synchronization Algorithm for WiMAX OFDM," in *Conference on Computational Intelligence and Communication Networks (CICN)*, October 2011.

[12] J. Kleider, S. Gifford, G. Maalouli, S. Chuprun, and B. Sadler, "Synchronization for RF Carrier Frequency Hopped OFDM: Analysis and Simulation," in *IEEE Military Communications Conference (MILCOM)*, October 2003.

[13] L. Nasraoui, L. Atallah, and M. Siala, "An Efficient Reduced-Complexity Two-Stage Differential Sliding Correlation Approach for OFDM Synchronization in the AWGN Channel," in *IEEE Vehicular Technology Conference (VTC)*, September 2011.

[14] T. Schmidl and D. Cox, "Robust Frequency and Timing Synchronization for OFDM," *IEEE Transactions on Communications*, vol. 45, no. 12, December 1997.

[15] J. Mark and W. Zhuang, *Wireless Communications and Networking*. Prentice Hall, 2003.

[16] P. Schniter, "Low-complexity equalization of OFDM in doubly selective channels," *IEEE Transactions on Signal Processing*, vol. 52, pp. 1002–1011, 2004.

[17] T. Rappaport, *Wireless Communications: Principles and Practice*. Prentice Hall, 2002.

[18] T. C. Clancy, "Efficient OFDM Denial: Pilot Jamming and Pilot Nulling," in *IEEE International Conference on Communications (ICC)*, June 2011.

[19] C. Shahriar, S. Sodagari, and T. Clancy, "Performance of pilot jamming on MIMO channels with imperfect synchronization," in *Communications (ICC), 2012 IEEE International Conference on*, 2012, pp. 898–902.

[20] C. Shahriar, S. Sodagari, R. W. McGwier, and T. C. Clancy, "Performance impact of asynchronous off-tone jamming attacks against OFDM," in *Communications (ICC), 2013 IEEE International Conference on*, 2013, pp. 2177–2182.

[21] *IEEE 802.11af-2013*, The IEEE Working Group 802.11- Wireless LAN Working Group Std.

[22] *IEEE 802.22-2011*, IEEE 802 LAN/MAN Standards Committee 802.22 WG on WRANs(Wireless Regional Area Networks) Std.

[23] B. Ray, "How to build a national cellular wireless network for 50m," The Register, April 2011.

[24] J. Mitola and G. Q. Maguire, "Cognitive radio: making software radios more personal," *IEEE Personal Communications Magazine*, vol. 6, pp. 13–18, 1999.

[25] T. C. Clancy, "Dynamic Spectrum Access in Cognitive Radio Networks," Ph.D. dissertation, University of Maryland, College Park, 2006.

[26] S. Chan, "Shared Spectrum Access for the DoD," in *New Frontiers in Dynamic Spectrum Access Networks (DySpan)*, 2007.

[27] B. Jabbari, R. Pickholtz, and M. Norton, "Dynamic Spectrum Access and Management," *IEEE Wireless Communications*, vol. 17, pp. 6–15, August 2010.

[28] B. S. Qing Zhao, "A Survey of Dynamic Spectrum Access," *IEEE Signal Processing Magazine*, vol. 24, pp. 78–89, 2007.

[29] M. Sherman, A. Mody, R. Martinez, and C. Rodriguez, "IEEE Standards Supporting Cognitive Radio and Networks, Dynamic Spectrum Access, and Coexistence," *IEEE Standards in Communications and Networking*, vol. 46, pp. 72–79, 2008.

[30] M. Zilis, "Californias Yurok Tribe Takes Advantage of White Spaces Technology," Radio Resource Magazine, June 2011.

[31] W. U. Relations, "Nation's first campus 'Super Wi-Fi' network launches at West Virginia University," Press Release, July 2013.

[32] L. Sanguinetti, M. Morelli, and H. V. Poor, "Frame Detection and Timing Acquisition for OFDM Transmissions with Unknown Interference," *IEEE Transactions on Wireless Communications*, vol. 9, 2010.

[33] K. Ramiah and M. Zivkovic, "OFDM Synchronization in the Presence of Interference," in *International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, 2013.

[34] L. Tao, W. H. Mow, V. K. N. Lau, M. Siu, R. S. Cheng, and R. Murch, "Robust Joint Interference Detection and Decoding for OFDM-based Cognitive Radio Systems with Unknown Interference," *IEEE Journals on Selected Areas in Communications*, vol. 25, pp. 566–575, 2007.

[35] P. Sun and L. Zhang, "Narrowband Interference Effect on Timing Synchronization for OFDM-based Spectrum Sharing System," in *International Conference on Wireless and Mobile Communications (ICWMC)*, 2010.

[36] M. Marey and H. Steendam, "Analysis of the Narrowband Interference Effect on OFDM Timing Synchronization," *IEEE Transactions on Signal Processing*, vol. 55, pp. 4558–4566, 2007.

[37] P. Klenner and K. Kammeyer, "Temporal Autocorrelation Estimation for OFDM with Application to Spatial Interpolation," in *IEEE Asilomar Conference on Signals, Systems and Computers*, October 2008, pp. 995–999.

[38] M. La Pan, T. C. Clancy, and R. W. McGwier, "Jamming Attacks Against OFDM Timing Synchronization and Signal Acquisition," in *IEEE Military Communications Conference (MILCOM)*, October 2012.

[39] P. Moose, "A Technique for Orthogonal Frequency Division Multiplexing frequency offset correction," *IEEE Transactions on Communication*, vol. 42, pp. 2908–2914, October 1994.

[40] J. van de Beek, "Low-Complex Frame Synchronization in OFDM Systems," in *International Conference on Universal Personal Communications (ICUPC)*, November 1995, pp. 982–986.

[41] M. Morelli and M. Moretti, "Robust Frequency Synchronization for OFDM-Based Cognitive Radio Systems," *IEEE Transactions on Wireless Communications*, vol. 7, pp. 5346–5355, 2008.

[42] M. La Pan, T. C. Clancy, and R. W. McGwier, "Phase Warping and Differential Scrambling Attacks Against OFDM Frequency Synchronization," in *International Conference on Acoustics Speech and Signal Processing (ICASSP)*, May 2013.

[43] ——, "Protecting physical layer synchronization: mitigating attacks against OFDM acquisition," in *Wireless Personal Multimedia Communications (WPMC), 2013 16th International Symposium on*, 2013.

[44] C. Yatrakis, "Computing the Cross Ambiguity Function : A Review," Master's thesis, Binghamton University, State University of New York, 2005.

[45] S. Stein, "Algorithms for Ambiguity Function Processing," *IEEE Transactions on Acoustics Speech and Signal Processing*, vol. ASSP-29, no. 3, pp. 588–599, June 1981.

[46] *IEEE Standard for Spectrum Sensing Interfaces and Data Structures for Dynamic Spectrum Access and other Advanced Radio Communication Systems.*, IEEE Std., April 2011.

[47] K. Kim, C. Spooner, I. Akbar, and J. Reed, "Specific Emitter Identification for Cognitive Radio with Application to IEEE 802.11," in *Gobal Telecommunications Conference (GLOBECOM)*, November 2008, pp. 1–5.

[48] T. C. Clancy, "Security Recommendations for Military Use of Dynamic Spectrum Access Technology," Office of the Assistant Secretary of Defense for Network and Information Integration, Tech. Rep., 2011.

[49] Y. Gottlieb, "Policy-controlled dynamic spectrum access in multitiered mobile networks," in *Military Communications Conference (MILCOM)*, 2010.

[50] K. Zhang, D. Swain, and M. Lin, "Dynamic Spectrum Access Enabled DoD Net-centric Spectrum Management," in *Military Communications Conference (MILCOM)*, 2007.

[51] T. Kohonen, "The Self-Organizing Map," *Proceedings of the IEEE*, vol. 78, no. 9, pp. 1464–1480, September 1990.

[52] L. Rabiner, "A tutorial on hidden Markov models and selected applications in speech recognition," *Proceedings of the IEEE*, vol. 77, pp. 257–286, 1989.