Phased Dithered Watermarking for Physical Layer Authentication

By

Nathan West

Bachelor of Science in Electrical Engineering
Oklahoma Christian University
Edmond, OK
2011

Submitted to the Faculty of the
Graduate College of
Oklahoma State University
in partial fulfillment of
the requirements for
the Degree of
Master of Science
May, 2014

Phased Dithered Watermarking for Physical Layer Authentication

Thesis Approved:

George Scheets

Thesis Advisor

Keith Teague

Jim West

ACKNOWLEDGMENTS

Thanks goes to my family for their support in this (admittedly extended) segment of my education. In response to the many questions regarding when I will finally finish my project/thesis, I present a quote from Larry Augustin,

> There's always this thought you get as a graduate student, "Gee if I could work from home [author commentary: or if I could get X software to work] I would be so much more productive I would graduate sooner because I would finish my thesis sooner." Is it true? Well, you can judge. Most people end up spending a lot of their time becoming more productive so that if they ever actually worked on their thesis they would finish it in a day.

I would also like to thank my adviser, Dr. Scheets, for valuable guidance and feedback through this process. I've learned a lot in the past two and a half years, which was made possible by the opportunities gained by working alongside Dr. Scheets. Similarly thanks to the Doug, Gautam, and Kellen at the NRL for the many different ways they have supported me. I'll never forget my first meeting with Doug (and my surprise), and am grateful for the events that followed.

Finally, as my first serious introduction to RF signal processing this project has introduced me to the GNU Radio project and community. In my short time as a contributor and working group chair I already feel like I could not give back as much as I receive in terms of education from the project and community there. I am excited to see the future of this project and the interesting paths it will take.

Name: Nathan West

Date of Degree: May, 2014

Title of Study: Phased Dithered Watermarking for Physical Layer Authentication

Major Field: Electrical Engineering

Wireless protocols can have authentication added at the physical layer without breaking the protocol for unaware clients. This study develops closed form expressions for the probability of bit errors when a technique called phase-dithered watermarking is used to add such an authentication message. The probability of bit errors is found for both message and authentication signals using phase-dithered watermarking on BPSK, QPSK, QAM, and DBPSK. When applicable results are compared to similar studies and confirmed with computer simulations.

TABLE OF CONTENTS

LIST OF TABLES

Table Page

LIST OF FIGURES

CHAPTER 1

Introduction

Communication systems attempt to address what was said and who said it. There are many modulation and encoding techniques for machines to transmit information, and many protocols such as GSM, IP, Ethernet require the source of a message to include an identifying address. In wired communications the closed nature of the media provides a modicum of trust between clients. Wireless communications change the trust-paradigm since the media is accessible by any party in close proximity. This opens a number of security risks since an adversary can easily claim an identity or address of a known client. The security is a concern because the address or identity claimed by a user could be used for routing, authentication, or billing. Recently there have been major wireless protocols with exposed weaknesses based on spoofing.

NFC (Near Field Communications) is a technology currently being advertised on many smart-phones to share music play lists, contacts, and other data. Charlie Miller [3], has shown how attackers can exploit NFC on Android-based phones from Samsung and Nokia to run malicious code without the owner's consent . Although this exploit does not specifically spoof an identity it does demonstrate how the latest wireless communications are actively being exploited by assuming trust in an un-trustworthy media.

GSM (Global System for Mobile communication) operates a PLMN (Public Land Mobile Network) that cell phones connect to [13]. Each cell phone has an identity number that the network operator checks for billing and switching. Each network also has an identity number, the MNC (Mobile Network Code). Both sides of the network, the operator and the client, have been shown to be insecure and vulnerable to spoofing [7, 12, 13]. Security researchers have demonstrated how to spoof phone clients to generate calls to expensive toll numbers [7]. Independently some researchers have created GSM base stations that can claim any MNC [13]. Since a cell phone in a PLMN doesn't authenticate a base station beyond the MNC, attackers can route traffic through fake stations and collect any information on the link [12].

The prevailing wireless LAN technology, IEEE 802.11, is also vulnerable to spoofing and traffic decryption [1]. The first encryption offered by the IEEE 802.11 standards, WEP (Wired Equivalent Privacy), is known to be insecure and required replacement with WPA [5]. IEEE 802.11 requires transmitters to identify themselves with a MAC address, which can easily be spoofed. Similarly, some phone vendors have partnered with carriers to offload phones to public IEEE 802.11 networks when available, based purely on SSID. Attackers are able to use so called honeypot attacks to lure such phones in to their networks and perform man-in-the-middle attacks making the entire data session vulnerable to eavesdropping and packet manipulation [15].

1.1 Physical Layer Authentication

Authentication requirements can be satisfied with many approaches, depending on design constraints. New protocols with authentication bits could be designed, which would obsolete legacy clients and decrease throughput efficiency. Yu et al [24] refers to this type of authentication as multiplexing since the message and authentication are multiplexed in time. Recent research [2, 19–21] has used multi-path fading to uniquely identify users via channel-estimation.

Using multi-path effects and other physical layer perturbances to authenticate users is typically called fingerprinting. Physical layer fingerprinting, developed by Yu et al. [20, 21] can be used to identify if a current user is the same as a previous user. This does not intentionally modify a signal, but instead relies on natural degradation by multi-path and other fading. Yu [26] and others [2, 19] also demonstrate the use of synthetic channels to intentionally perturb the signal in ways that look like environmental affects, which can be used to authenticate users using the inverse of the synthetic channel. Yu [24] calls this technique embedded authentication because the authentication signal is embedded in the transmitted message.

Embedding authentication messages within the physical layer preserves existing protocols and legacy clients while adding link specific authentication. Off the shelf protocols can be modified to include authentication and still be used with existing hardware [25]. Furthermore, each wireless link on a network can meet different security specifications. Modifying the physical layer will generally lead to a reduction in signal quality, which means reducing the probability of detecting the correct bit. Using the physical layer for detecting a specific

user dates back to World War II when armies on both sides of the war were able to identify wireless telegraphy operators by their fist [17]. The fist of a telegraph operator is the unique cadence used to key messages, similar to an individual's voice [9]. Since an operator stays with a ship or platoon, different armies were able to intercept telegraphs, identify the operator, and triangulate position to track enemy troop movement [17]. In modern communications the signals are machine-generated and are designed to have no variance between radios. All signals are degraded in some way, either due to fading, AWGN (Additive White Gaussian Noise), or multi-path effects. These characteristics rapidly decorrelate in space, which is the fundamental idea behind the fingerprinting method previously mentioned [20].

1.1.1 Watermarking

Deliberately adding degradation before transmission is also called watermarking, which has subtle differences from active channel emulation and fingerprinting [4]. RF watermarking is similar to image, video, and paper watermarking in that a low energy signal is added on to the primary signal. Currently two types of watermarking are being researched: baud dithering and constellation dithering [6, 8]. Both watermarking techniques embed a bitstream, the watermark, on top of the RF message that will uniquely identify the transmitter in some way. This can be done a number of ways, and there are several proposed algorithms to create a key that two clients can use to identify each other [26]. The watermarked signal is referred to as the tag, which is generated as a function of the transmitted message and a secret key [23].

Baud Dithering

Baud dithering changes the symbol timing on the transmitter, according to the tag [6]. This creates a specific type of bit-noise called jitter, which naturally occurs in digital communications. When the receiver detects the incoming waveform a decision is made based on the received symbol time so that the watermark can be recovered. The decoded message is hashed with the secret key on the transmitter side so the tag is verified.

Constellation Dithering

Constellation dithering changes the constellation in some way that creates two decision regions around each constellation point: one decision region defines the message hypothesis and another region defines the watermark hypothesis. Constellation dithering could change

the amplitude or phase of a signal to embed the watermark. Since phase shift keying is known to be the most energy-efficient binary modulation we chose to focus on phase dithering as a watermark method. The message stream can be modulated with any digital modulation scheme; after modulation a small phase is added or subtracted, based on the watermark tag. This creates smaller constellations around each message symbol. Similar to phase dithered watermarking, [18] has used similar techniques to do hierarchical modulation.

Hierarchical Modulation

In hierarchical modulation two or more bit streams with different priorities are combined into a single signal. The main bit stream may be mission critical or require a higher bit rate while the secondary bit stream is of lower priority or bit rate. Hierarchical modulation embeds one signal on top of another allowing both signals to transmit on the same carrier without increasing the bandwidth [18]. Phase dithered watermarking is similar to hierarchical watermarking, but has an added goal of stealth [10]. Since watermarking has the appearance of adding noise, a figure of merit for link analysis is the probability of bit and tag recovery errors.

1.1.2 Phase Dithered Watermark

For the purpose of finding the probability of bit errors, constellation watermarking is hierarchical watermarking where the message is the primary bit stream and the watermark tag is the secondary bit stream.

QAM/QAM Watermarking

[27] uses hierarchical QAM (Quadrature Amplitude Modulation) to create higher order QAM constellations transmitting independent bit streams, then uses OFDM (Orthogonal Frequency Division Multiplexing) to inverse multiplex the signal onto slower speed subchannels. [27] also provides P(BE) expressions for message and watermark symbols in an AWGN channel in terms of the distance between constellation points. Figure 1.1 shows the hierarchical QAM constellation used in [27]. In Figure 1.1 d_1 is half the distance between the adjacent message symbols, and d_2 is half the distance between adjacent watermark symbols in the same hierarchy. The final distance relevant to bit error probability, d_1', is defined as the distance between adjacent watermark symbols in adjacent hierarchies. Using this hierarchical QAM constellation for watermarking, [27] gives the probability of message

bit error defined in Equation 1.1. The tag is only decoded if the entire frame or packet is correct, since there is no point in decoding the tag if the message is in error. Given that the message is correct, the probability of a tag bit being decoded properly is given in Equation 1.2 [23, 27].

$$P_{message}(BE) = \frac{1}{4}\left(\text{erfc}\,\frac{d_1'}{\sqrt{N_0}} + \frac{d_1' + 2d_2}{\sqrt{N_0}}\right) \tag{1.1}$$

$$P_{tag}(BE) = \frac{1}{4}\left(\text{erfc}\,\frac{d_2}{\sqrt{N_0}} + \text{erfc}\,\frac{2d_1' + d_2}{\sqrt{N_0}} - \text{erfc}\,\frac{2d_1' + 3d_2}{\sqrt{N_0}}\right) \tag{1.2}$$

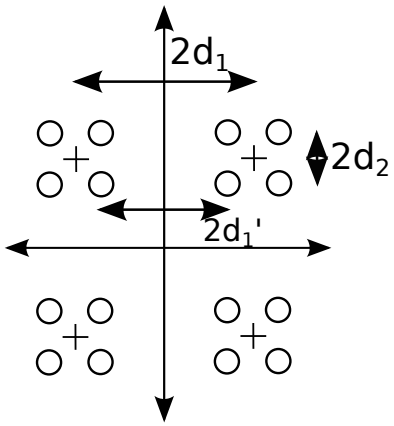

Figure 1.1: The hierarchical QAM constellation has '+' denoting where a message symbol is located, which is surrounded by a low energy watermark constellation. The valid constellation symbols are marked with circles. The distances marked show distance between message constellations, watermarks for a given message, and watermarks for a different message.

PSK/PSK Watermarking

Other researchers have used PSK modulation for bipodal phase shift keying as the watermark. [18] analyzes hierarchical PSK modulation to come up with exact bit error probabilities. The notation 2/4-PSK denotes a primary channel that is BPSK modulated with a secondary channel that is also BPSK modulated. The secondary channel symbols are modulated on top of the primary channel symbols, and hence there are two secondary channel symbols for every primary channel symbol. [18] analyzes the phase error of hierarchical PSK signals to find probabilities of bit and tag errors for 2/4-PSK given in Equations 1.3 and 1.4, respectively. The γ term is the common figure of merit, $\frac{E_b}{N_0}$. The ϕ is the angular distance from a straight BPSK constellation point and the watermarked constellation point. This distance is illustrated for a 2/4/8-PSK constellation as the angular distance for a BPSK

watermarked signal from a QPSK constellation in Figure 1.2.

$$P_{message}(BE) = Q\left(\sqrt{2\gamma}\cos(\phi)\right) \tag{1.3}$$

$$P_{tag}(BE) = Q\left(\sqrt{2\gamma}\sin(\phi)\right) \tag{1.4}$$

The notation is extended to 2/4/8-PSK to refer to three independent channels that transmit one bit each at the same time. Each channel is BPSK modulated on top of another channel. Since the energy of each channel can be different, each channel will have a different P(BE), allowing three different priorities for three different bit streams on a simultaneous communication. The same authors have done similar work analyzing hierarchical QAM constellations [18]. The probability of bit error for each channel is defined in terms of the Pawula F-function, the phase-error probability distribution. To find the probability of bit error for any given channel in a hierarchical PSK scheme can be found using a recursive algorithm defined in [18].

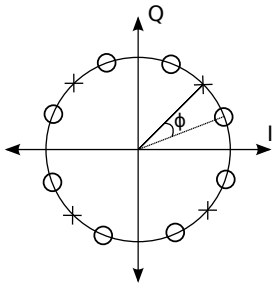

Figure 1.2: The hierarchical PSK constellation adds or subtracts a phase shift compared to a straight PSK constellation. The circles are watermarked constellation points that have a small phase difference, ϕ, from a standard QPSK constellation.

Hierarchical PSK has been previously used in watermarking for authentication. [6] uses 2/4-PSK to watermark OFDM signals using QPSK and DQPSK, and compares the results to baud-dithering the same signals. The QPSK and QPSK signals are modulated using OFDM for better P(BE). [6] provides plots for the watermark bit error rate for baud-dithering and constellation dithering. The results show for an equivalent watermark bit-rate the baud dithering has a lower probability of bit error, but comes with a trade-off in complexity and compatibility with non-aware receivers.

DPSK/PSK Watermarking

Another effort, [8], uses DBPSK as the message modulation and a rotated 8-PSK constellation to determine the watermark, which could be described as a 2/8-PSK hierarchical modulation. This method aimed to use existing blocks in a software framework called GNU Radio to implement watermarking a non-coherent DPSK system. The rotated 8-PSK constellation limits ϕ, the watermark angle, since the 8-PSK constellation points are already defined to be equidistant. [8] uses Monte-Carlo simulations to find the theoretical probability of bit errors for the message and watermark followed by over-the-air testing.

1.2 Stealth, Security, and Robustness

This thesis is focused primarily on signaling aspects of watermark authentication rather than cryptographic concerns, but it is worth mentioning works which do focus on cryptographic concerns related to watermarking. In the hypothetical cast of characters commonly used in cryptography Alice and Bob are watermark-aware transmitters and receivers communicating with authentication [9]. Carol is an watermark-unaware receiver that is also communicating with Alice or Bob. Eve is an eavesdropper that tries to determine if authentication is present, and to attack the authentication if it exists. [23, 25] both use this cast and define the stealth and robustness of the watermark authentication method. The authentication system is said to be stealthy if it is difficult to detect by Eve and if Carol is still able to communicate [23, 25]. The authentication system is robust if it is difficult for Eve to disrupt [23,25].

[23,24] describes a general framework of measuring the stealth and impact of a physical-layer watermark. Any receiver, such as Eve, is able to estimate the SNR of a given channel. If the SNR for given blocks of the communication change rapidly and discretely then Eve will suspect that a watermark authentication mechanism is being using [24].

[24] proposes a number of fitness tests, such as Kolmogorov-Smirnov or Lilliefors test, as being able to detect a watermark with given watermark powers. With a priori knowledge of the watermark and collaboration between Bob and Alice the watermark power can be set to a level that is within the noise parameters, effectively hiding the watermark from Eve, and improving Carol's signal [24]. [10] tests this approach in GNU Radio using the QAM/QAM watermark described in [27] where the watermark is randomly placed on a fraction of the transmitted signal. Using the SNR estimated from pilot symbols the impact

of the watermark on Carol and the presence of the watermark to Eve was tested. The results show that packet errors were not adversely affected for select watermark power levels, indicating that Carol's communication is not affected [10]. In addition, the SNR estimates show that Eve cannot determine the presence of the watermark with significant confidence [10]. [10] also experimentally determined the probability of correctly authenticating packets at select watermark power levels and found in many cases the probability of authentication approaches 1. Using a small, but unfinished experiment with falsely watermarked signals to test the robustness against an attacker [10] found (although inconclusively) that there is a small probability of falsely authenticating a user.

CHAPTER 2

Thesis Layout and Definitions

The scope of this thesis is in deriving closed-form expressions for the expected bit errors of message and watermark signals in phase-dithered watermarking. This chapter provides a layout of this thesis as well as definitions of terms and conventions used in the following chapters. Chapters 3-5 derive probability of bit errors for phase-dithered coherent modulation schemes; respectively covering BPSK, QPSK, and QAM. Chapter 6 shows the probability of bit errors for non-coherent DBPSK. Chapter 7 concludes with suggestions for continued research in this area. The appendices repeat existing proofs that are useful references for standard modulations.

2.0.1 Contributions

This work makes the following contributions to existing knowledge:

- Independently verifies existing closed form expressions for message and watermark BERs for phase-watermarked BPSK and QPSK
- Develops closed form expressions, verified by simulation, for the message and watermark BERs for phase-watermarked QAM
- Develops closed form expressions, verified by simulation, for the message and watermark BERs for phase-watermarked DBPSK

2.0.2 Conventions

The rest of this document will use the following terms and symbols.

Watermark

The term watermark will be used as a noun to refer to the specific bit that is represented by a post-modulation phase shift. The encoding of this bit is referred to as the watermark, and the process of encoding the bit is referred to as watermarking. Recovering the watermark is

referred to as watermark recovery and there will be a watermark error rate and probability of watermark error, P_W. This is deliberately unique terminology than that used in some related literature to emphasize the difference between the cryptological aspects of watermarking and the physical process of embedding and decoding data. The watermarking literature that studies cryptological aspects of embedding low power data, [10,25,26] will use the term *key* to refer to the bit being transmitted. The relation is that a key will have meaning in an authentication sense, but a watermark is a bit that may be used for any purpose.

$\frac{E}{N_0}$

$\frac{E}{N_0}$ is the symbol energy to noise ratio. This is used to describe the signal to noise ratio normalized by symbol rate over bandwidth. The symbol $\frac{E}{N_0}$ is commonly used in communications literature; now we introduce the subscripts that will be used in the remainder of this thesis.

$\frac{E_b}{N_0}$ describes the energy per *bit* to the noise power spectral density per bit. Similarly, $\frac{E_s}{N_0}$ will describe the energy per *symbol* to the noise energy per symbol. The relation is that a key will have meaning in an authentication sense, but a watermark is an arbitrary bit.

P_b

P_b is used as a shorthand for the probability of a message bit error occurring at the receiver. This is normally expressed as a function of $\frac{E_b}{N_0}$.

$$P_b\left(\frac{E_b}{N_0}\right) \tag{2.1}$$

P_S

P_S is the short hand for the probability of a message symbol error occurring. Normally this will be a function of $\frac{E_S}{N_0}$, for example,

$$P_S\left(\frac{E_S}{N_0}\right) \tag{2.2}$$

Miscellaneous

Some terminology useful for discussing bit detection will be introduced in the first derivation and will then be consistently used for remaining bit detectors using other modulation schemes.

T is the bit (symbol) length after modulation, measured in seconds.

θ is used as a message modulation angle.

ϕ is used as the watermark modulation angle.

l_n refers to a random variable, hereafter called statistic in keeping with terminology used by [22], used by a bit detector for making decisions, which is the n^{th} output of a matched filter in the receiver.

CHAPTER 3

Phase Dithered BPSK Error Rates

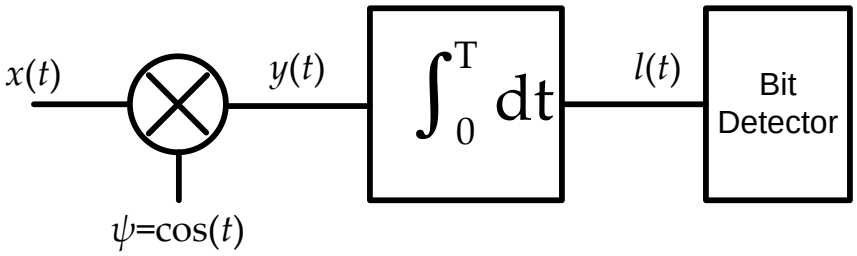

Figure 3.1: A typical coherent BPSK receiver with input $x(t)$ makes a bit decision on $l(t)$.

BPSK uses anti-podal phase-shifting to encode a single bit into a symbol for transmission. A typical receiver, shown in Figure 3.1, requires only a single basis function to determine the phase.

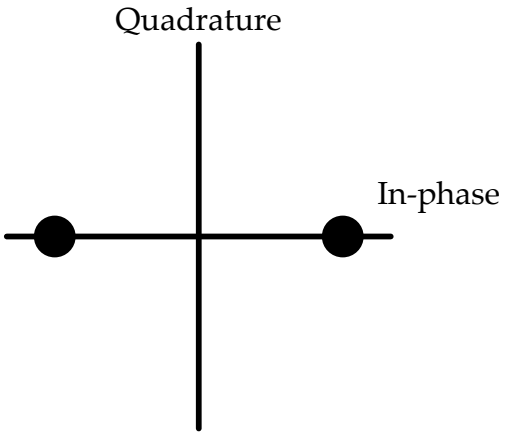

Figure 3.2: A typical coherent BPSK constellation diagram.

3.1 Standard BPSK

A BPSK signal is modeled as shown in Equation 3.1. θ is a representation of the message bit and will be either 0 or π. The constellation diagram for this signal is shown in Figure 3.2.

$$x(t) = \cos(\omega t + \theta) \tag{3.1}$$

The bit decision is made using the statistic $l(t)$ from Figure 3.1. This statistic is a bi-modal Gaussian random variable with variance depending on the noise power spectral density, N_0, shown in Equation 3.2. The relation between the variance and noise output of a correlator and matched filter detector is shown in Appendix A.

$$\sigma^2 = \frac{N_0 T}{4} \tag{3.2}$$

The $P_b\left(\frac{E_b}{N_0}\right)$ for BPSK, Equation 3.3, is well known in the literature [16,22]. The derivation of the standard P_b equation will be a useful building block for deriving probability of bit errors for watermarked BPSK.

$$P_b\left(\frac{E_b}{N_0}\right) = Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \tag{3.3}$$

3.2 Watermarked BPSK

Building from Equation 3.1, a watermarked BPSK symbol will appear in the form of Equation 3.4. Due to this being BPSK the same constraint remains on θ, the message modulation angle will be either 0 or π.

$$x(t) = \cos\left(\omega t + \theta + \phi\right) \tag{3.4}$$

The watermark angle, ϕ, is selected to give the desired trade-offs in watermarking; the most obvious being stealth which is related to signal degradation. The larger angle will improve probability of correct detection for the watermark but lower the probability of detecting the correct message bit, thus reducing the watermark's stealthiness. Introducing a binary watermark will split each existing message symbol in to two watermarked symbols. With BPSK this results in four symbols as seen in the constellation diagram in Figure 3.3.

A standard BPSK receiver is capable of detecting watermarked message bits properly, although with a lower $\frac{E_b}{N_0}$. The standard BPSK receiver is not capable of detecting the watermark bits because the watermark moves symbols orthoganl to the basis function used in demodulation. To overcome this a watermark-aware BPSK receiver must add in a quadrature path for bit and watermark decisions.

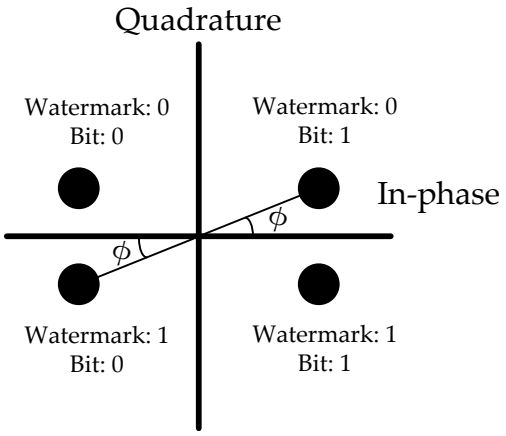

Figure 3.3: Watermarked BPSK constellation. The watermark creates two more constellation points.

3.2.1 Non-Watermark Aware BPSK Error Probability

Analysis shows the non-watermark aware BPSK receiver will result in the same bit error probability for the message as the watermark aware receiver. Using the standard BPSK receiver from Figure 3.1 the received signal is $x(t)$. The output statistic for determining the message bit is

$$l = \int_0^T (x(t)\cos(\omega t))\, dt \tag{3.5}$$

Substituting Equation 3.4 in to Equation 3.5 yields

$$l = \int_0^T ((\cos(\omega t + \theta + \phi))\cos(\omega t))\, dt \tag{3.6}$$

After using common trigonometric identities this simplifies to the following form

$$l = \pm\frac{1}{2}\int_0^T (\cos(\phi) + \cos(2\omega t + \phi))\, dt \tag{3.7}$$

The double frequency term goes to zero because the integral limits, $[0, T]$, cover an integer number of sinusoid periods. The result becomes the mean of a random variable used to determine the bit.

$$l = \pm\frac{T}{2}\cos(\phi) \tag{3.8}$$

Notice that the plus/minus of l indicates the message bit, and ϕ can be either positive or negative depending on the watermark, resulting in the four symbols shown in Figure 3.3. The results from Appendix B are now useful since we can substitute Equation 3.8 in to

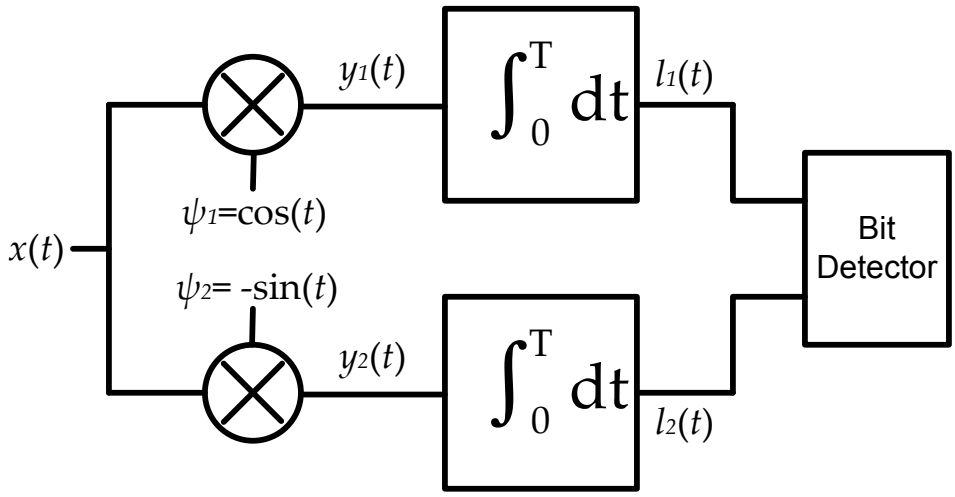

Figure 3.4: A quadrature style receiver is capable of providing information about the bit and watermark.

Equation B.9 and get

$$P_b\left(\frac{E_b}{N_0}\right) = Q\left(\frac{0 \pm \frac{T}{2}\cos(\phi)}{\sqrt{\frac{N_0 T}{4}}}\right) \tag{3.9}$$

This is the same form used in the derivation of standard BPSK in Appendix B, but the watermark introduces the cos term. After simple algebra the P_b for watermarked BPSK is found to be

$$P_b\left(\frac{E_b}{N_0}\right) = Q\left(\sqrt{\frac{2E_b}{N_0}}\cos(\phi)\right) \tag{3.10}$$

3.2.2 Watermark Aware BPSK Message and Watermark Error Probability

It is possible to construct a watermark aware BPSK receiver with a single basis function with an expected watermark phase offset to receive the message bit and the watermark. This is sub-optimal because it reduces the received signal quality. A better solution is adding another basis function that is orthogonal to the first, making a quadrature receiver, shown in Figure 3.4. The advantage of the quadrature receiver comes from simplicity of analysis and the fact that quadrature receivers are readily available.

Using the quadrature receiver results in two statistics used to determine watermark and message bits. They are,

$$l_1 = \pm\int_0^T \left[\cos(\omega t + \phi)\cos(\omega t)\right] dt \tag{3.11a}$$

$$l_2 = \pm\int_0^T \left[\cos(\omega t + \phi)\sin(\omega t)\right] dt \tag{3.11b}$$

Using common product-to-sum trigonometric identities yields,

$$l_1 = \pm\frac{1}{2}\int_0^T \left[\cos\left(2\omega t + \phi\right) + \cos\left(\phi\right)\right] dt \tag{3.12a}$$

$$l_2 = \pm\frac{1}{2}\int_0^T \left[\sin\left(2\omega t + \phi\right) - \sin\left(\phi\right)\right] dt \tag{3.12b}$$

After integrating the final statistics for determining message bits and watermark the result is

$$l_1 = \pm\frac{T}{2}\cos\left(\phi\right) \tag{3.13a}$$

$$l_2 = \pm\frac{T}{2}\sin\left(\phi\right) \tag{3.13b}$$

l_1 only varies in the in-phase direction and l_2 only varies in the quadrature direction. l_1 contains information on the presence of a watermark from the $\cos\phi$ term, but since $\cos\phi = \cos -\phi$ the watermark bit, represented by the sign of ϕ cannot be determined from l_1. The result of this is that l_1 effectively only provides information about the message bit and l_2 only provides information about the watermark. A decision on the message bit uses the same criteria as Equation B.8.

Equation 3.13a is the same as Equation 3.8, so the P_b remains the same (Equation 3.10). The probability of a watermark error, P_W, is

$$P_W\left(\frac{E_b}{N_0}\right) = Q\left(\sqrt{\frac{2E_b}{N_0}}\sin\left(\phi\right)\right) \tag{3.14}$$

Comparison to Hierarchical 2/4-PSK

[18] uses a different approach to derive a closed from expression for hierarchical BPSK in terms of The results from [18] are also presented for 2/4-PSK in terms of the Q-function, which match exactly

3.2.3 Computer Simulations

MATLAB was used to verify the derived Q-functions. Standard toolboxes were used to create a custom BPSK modulator and demodulator as well as watermarking and watermark recovery blocks. 10^4 random bits were used with a random binary watermark using a watermark angle of $\phi = \frac{\pi}{8}$. Each bit was modulated with each symbol being a single period and a sampling rate of 100 samples/symbol. The decision boundary for a message bit was

set to be the Quadrature axis. The watermark decision boundary is set to be the In-Phase axis. Figure 3.5 shows three lines:

- Black dots showing error rate averaged over 10^4 watermarked symbols with simulated AWGN.
- A green dotted line showing the expected P_b for unwatermarked BPSK, shown for reference. Calculated using Equation 3.3.
- A blue dashed line showing the expected $_b$ for watermarked BPSK with watermark angle $\phi = \frac{\pi}{8}$, calculated using Equation 3.10

The watermarked BPSK bit detection is a very close match to what is expected. Watermarked BPSK bit detection results in approximately 0.69 dB degradation in the message $\frac{E_b}{N_0}$ when $\phi = \frac{\pi}{8}$.

The watermark recovery rates are shown in Figure 3.6. This comes from the same simulation as Figure 3.5 with 10^4 bits with a watermark angle $\phi = \frac{\pi}{8}$. Combining the watermark and bit into a tuple, <watermark, bit>, the watermark was placed such that the tuple of symbols is gray coded. For example the message bit 1 is in quadrants 1 and 4. A watermark of 0 moves the message bit 1 symbol to quadrant 1, and a watermark of 1 moves that symbol to quadrant 4. A watermark of 0 moves the message bit 0 symbol to quadrant 2, and a watermark of 1 moves that symbol to quadrant 3. This is illustrated in Figure 3.3. The simulation for P_W provides a very close match to the expected watermark error rate from Equation 3.14.

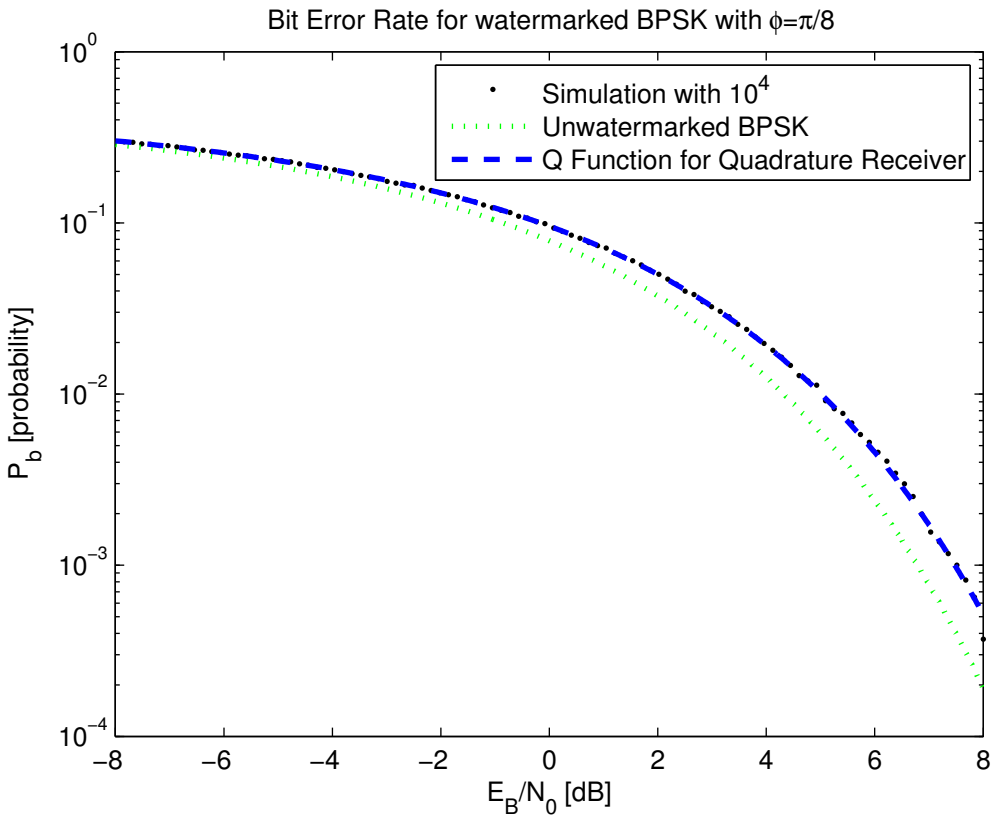

Figure 3.5: BPSK P_b for a simulated watermarked signal, expected P_b for a watermarked signal with $\phi = \frac{\pi}{8}$, and standard BPSK P_b. The black dots are simulated with 10^4 bits averaged in to each dot.

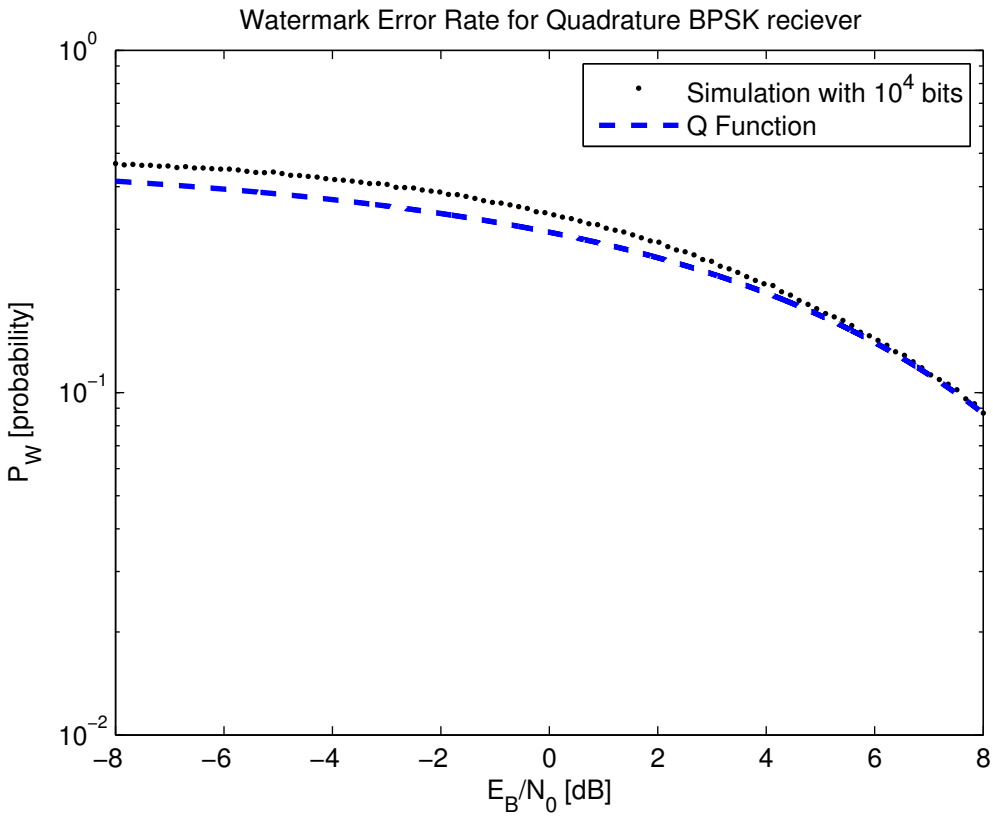

Figure 3.6: Watermark recovery error rates, P_W for $\phi = \frac{\pi}{8}$. The blue dashed line is the expected probability of watermark error. The black dots are simulated with 10^4 watermarked bits for each dot.

CHAPTER 4

Phase Dithered QPSK Error Rates

4.1 Standard QPSK

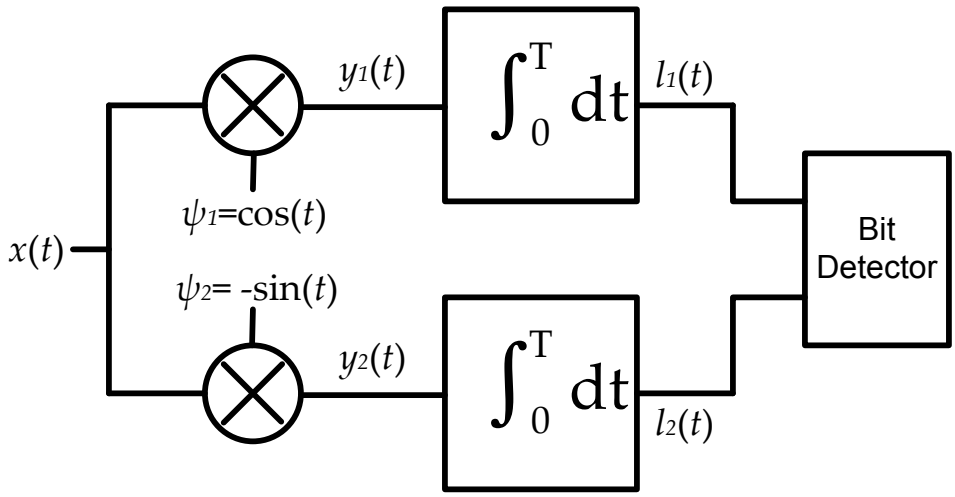

Figure 4.1: A typical quadrature-style demodulator for QPSK coherent demodulation.

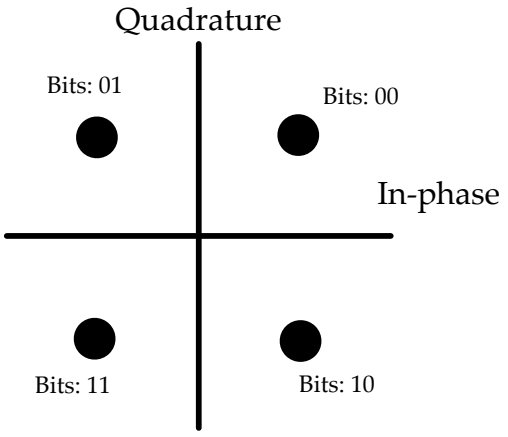

Figure 4.2: A grey-coded QPSK constellation. A pair of bits forms one of four symbols, each separated by 90°.

QPSK uses phase-shift keying to encode two bits into a symbol for transmission. QPSK is very similar to BPSK, and the transmitted signal can be modeled similarly because both

depend solely on a phase shift to encode information. The modeling equation for QPSK, Equation 4.1, is the same as for BPSK, Equation 3.1.

$$x(t) = \cos(\omega t + \theta) \tag{4.1}$$

Using QPSK the modulated phase angle θ can be one of four values, each separated by 90° and assummed equally likely. The constellation diagram for QPSK in this dissertation is shown in Figure 4.2. A common receiver is the quadrature style receiver pictured in Figure 4.1.

$$\sigma^2 = \frac{N_0 T}{4} \tag{4.2}$$

The variance and noise power density for this receiver is commonly known; a derivation is provided in Appendix A and the result repeated here in Equation 4.2. Since each symbol contains two bits we are interested in finding the P_S for QPSK which will be expressed in terms of $\frac{E_S}{N_0}$. For non-watermarked QPSK this is commonly known [16,22] and a derivation is provided in Appendix C.

$$P_b\left(\frac{E_b}{N_0}\right) = Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \tag{4.3}$$

The relationship between P_S and P_b for QPSK can be seen by comparing Equations 4.3 and 4.4 [22]. The difference between E_b and E_S in these two equations is subtle, but important; since each symbol has two bits $E_S = 2E_b$. The full derivation can be found in Appendix C; the final result from Equation C.15 is repeated here.

$$P_S\left(\frac{E_S}{N_0}\right) = 2Q\left(\sqrt{\frac{E_S}{N_0}}\right) - \left[Q\left(\sqrt{\frac{E_S}{N_0}}\right)\right]^2 \tag{4.4}$$

4.2 Watermarked QPSK

Phase-dithered QPSK splits each QPSK message symbol in to two watermarked symbols, the same way phase-dithered BPSK message symbols were split in to two symbols. The watermarked QPSK signal adds the phase offset ϕ so that the transmitted signal takes the form of Equation 4.5.

$$x(t) = \cos(\omega t + \theta + \phi) \tag{4.5}$$

The angle θ can be one of the same four values from Equation 4.1 representing one of the four possible message symbols. The watermark angle ϕ is a small angle that is either added or subtracted, depending on the watermark bit. The watermarked QPSK constellation with a gray-coded watermark is shown in Figure 4.3. In this context the gray-coding is seen when the bits and watermark are combined in to a 3-tuple; for example the transmitted tuple might be (high bit, low bit, watermark bit). Gray-coding the watermark improves the probability of correctly recovering the watermark.

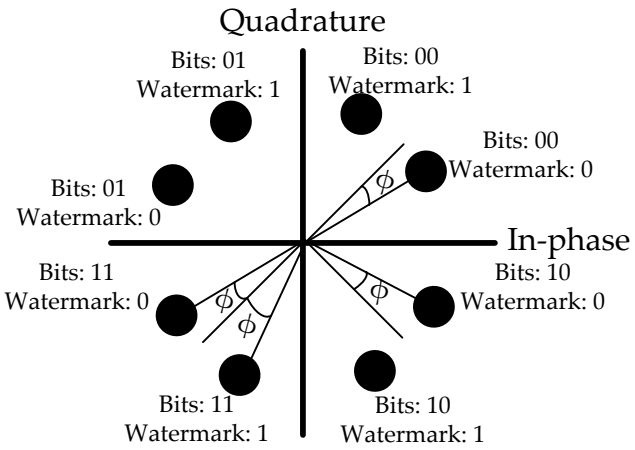

Figure 4.3: A phase-dithered QPSK constellation with a grey-coded watermark. Each watermarked symbol is ϕ radians from where the non-watermarked signal would be.

The same quadrature receiver used for standard QPSK is useful for receiving watermarked QPSK. Since the same receiver is used the P_S for a watermark-aware receiver is the same as that of a non-watermark aware receiver when a watermarked message is transmitted.

4.2.1 Watermarked QPSK Probability of Message Bit Error

Symmetry allows the error rate analysis to focus on a single symbol since all symbols will have the same probability of message and watermark errors. For simplicity the P_S derivation will be restricted to the symbol labeled with bits 00 and watermark 0 from Figure 4.3.

The decision region for this symbol are positive regions of the in-phase and quadrature axes, or quadrant 1. Equation C.3 from Appendix C shows the derivation of the decision statistic for non-watermarked QPSK. Similar to non-watermarked QPSK, the decision statistics, l_1 and l_2, for watermarked QPSK is found by correlating the received signal with

the demodulator's basis functions. The mean of those statistics is

$$\overline{l_1} = \int_0^T \left[\cos\left(\omega t + \frac{\pi}{4} - \phi\right)\cos\left(\omega t\right)\right] dt \tag{4.6a}$$

$$\overline{l_2} = -\int_0^T \left[\cos\left(\omega t + \frac{\pi}{4} - \phi\right)\sin\left(\omega t\right)\right] dt \tag{4.6b}$$

Trigonometric identities simplify this to an addition of cosines and sines to simplify integration. After integration the decision statistics evaluate to the results in Equation 4.7.

$$\overline{l_1} = \frac{1}{2}\int_0^T \left[\cos\left(2\omega t + \frac{\pi}{4} - \phi\right) + \cos\left(\frac{\pi}{4} - \phi\right)\right] dt \tag{4.7a}$$

$$\overline{l_2} = -\frac{1}{2}\int_0^T \left[\sin\left(2\omega t + \frac{\pi}{4} - \phi\right) - \sin\left(\frac{\pi}{4} - \phi\right)\right] dt \tag{4.7b}$$

The double frequency terms have an integer number of periods within the integral limits of $[0, T]$, which results in 0 after integration. After integrating the single frequency term the expected value of the decision statistics is

$$\overline{l_1} = \frac{T}{2}\cos\left(\frac{\pi}{4} - \phi\right) \tag{4.8a}$$

$$\overline{l_2} = \frac{T}{2}\sin\left(\frac{\pi}{4} - \phi\right) \tag{4.8b}$$

Bit decisions are made by comparing the sign of each decision statistic at the receiver. For example, Equation C.8 could be the decision criteria for the two message bits, and then the watermark bit is chosen by comparing l_1 and l_2. Equation C.8 shows the comparison to determine watermark bits that would match the constellation in Figure 4.3

$$bit_{watermark} = \begin{cases} 0 & |l_1| < |l_2| \\ 1 & |l_1| > |l_2| \end{cases} \tag{4.9}$$

Deriving the message error rate uses the PDF of the decision statistics l_1 and l_2. The expected values of these statistics, found in Equation 4.8, along with the noise PSD found in Appendix A is all that is required to define the PDFs (Equation 4.10) of l_1 and l_2, which

are f_{l1} and f_{l2} respectively.

$$f_{l1}(\lambda_1) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{\left(\lambda_1 - \frac{T}{2}\cos\left(\frac{\pi}{4} - \phi\right)\right)^2}{2\sigma^2}\right) \tag{4.10a}$$

$$f_{l2}(\lambda_2) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{\left(\lambda_2 - \frac{T}{2}\sin\left(\frac{\pi}{4} - \phi\right)\right)^2}{2\sigma^2}\right) \tag{4.10b}$$

The probability of symbol errors is the volume under the expected symbol region. As previously stated, the symbol with bits labeled 00 and the watermark labeled 0 in Figure 4.3 which has decision regions bounded by the I and Q axes. Now, Equation 4.10 is substituted in to Equation C.10 which gives the message symbol error rate for watermarked QPSK. The Q-function representation of this is a more useful and succinct representation of this probability. The Q-function of the message symbol error rate, Equation 4.11, is Equation C.11 with Equation 4.10 substituted in for l_1 and l_2.

$$P_S\left(\frac{E_S}{N_0}\right) = 1 - \left[1 - Q\left(\frac{0 + \frac{T}{2}\cos\left(\frac{\pi}{4} - \phi\right)}{\sigma}\right)\right]\left[1 - Q\left(\frac{0 + \frac{T}{2}\sin\left(\frac{\pi}{4} - \phi\right)}{\sigma}\right)\right] \tag{4.11}$$

Rearranging terms and using the relationship between symbol time, T, and symbol energy, E_S, gives the P_S in terms of $\frac{E_S}{N_0}$. The final result in a familiar form is the P_S in Equation 4.12. The product term is included here for completeness, but in practice can be omitted since it is sufficiently small for $\frac{E_S}{N_0} > 0$dB. The omission of the product term for standard QPSK is discussed by Fuqin while discussing the approximation of relating P_S to P_b [22]. The result is valid in this case because the relationship of P_S to P_b is the same in watermarked QPSK.

$$\begin{aligned} P_S\left(\frac{E_S}{N_0}\right) =& Q\left(\sqrt{\frac{4E_b}{N_0}}\cos\left(\frac{\pi}{4} - \phi\right)\right) + Q\left(\sqrt{\frac{4E_b}{N_0}}\sin\left(\frac{\pi}{4} - \phi\right)\right) \\ & - Q\left(\sqrt{\frac{E_S}{N_0}}cos\left(\frac{\pi}{4} - \phi\right)\right) \cdot Q\left(\sqrt{\frac{4E_b}{N_0}}\sin\left(\frac{\pi}{4} - \phi\right)\right) \end{aligned} \tag{4.12}$$

4.2.2 Watermark Recovery Error

The watermark error rate uses the same statistics (Equation 4.8) for decisions as the message recovery. For watermark error rate analysis the watermark is assumed to be grey-coded with the data as shown in Figure 4.3. The P_W analysis will also use the symbol drawn with bits 00 and a watermark of 0. The decision regions for the watermark that matches this constellation are:

$$bit_{watermark} = \begin{cases} 0 & |l_1| < |l_2| \\ 1 & |l_1| > |l_2| \end{cases} \tag{4.13}$$

Graphically this region forms a right angle between the angles $\frac{\pi}{4}$ and $\frac{\pi}{4}$. The watermark error probability is the volume of the joint density function (Equation 4.10 outside of this region.

$$P_W\left(\frac{E_S}{N_0}\right) = 1 - \int_0^{\infty} \int_{-\lambda_1}^{\lambda_1} f_{l1}\left(\lambda_1\right) f_{f2}\left(\lambda_2\right) d\, l_2 \; d\, l_1 \tag{4.14}$$

Substituting the probability density functions for l_1 and l_2 (Equation 4.15) in to Equation 4.14 and integrating will result in the P_W.

$$f_{l1}\left(\lambda_1\right) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{\left(\lambda_1 - \frac{T}{2}\cos\left(\phi - \frac{\pi}{4}\right)\right)^2}{2\sigma^2}\right) \tag{4.15a}$$

$$f_{l2}\left(\lambda_2\right) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{\left(\lambda_2 - \frac{T}{2}\sin\left(\phi - \frac{\pi}{4}\right)\right)^2}{2\sigma^2}\right) \tag{4.15b}$$

The result of this substitution is shown in Equation 4.16. The Q-function is not a convenient representation of this error probability because the limits of integration are not parallel to the axes. A transformation to rotate the entire function may be possible; however, it is much more convenient to leave the expression in Equation 4.16 and use numerical integration to generate BER curves.

$$\begin{aligned} P_W\left(\frac{E_S}{N_0}\right) = 1 - \frac{1}{\sigma^2 2\pi} \int_0^{\infty} \int_{-l_1}^{l_1} \Bigg[& \exp\left(-\frac{\left(\lambda_1 - \frac{T}{2}\cos\left(\phi - \frac{\pi}{4}\right)\right)^2}{2\sigma^2}\right) \\ & \times \exp\left(-\frac{\left(\lambda_2 - \frac{T}{2}\sin\left(\phi - \frac{\pi}{4}\right)\right)^2}{2\sigma^2}\right)\Bigg] d\lambda_2 d\lambda_1 \end{aligned} \tag{4.16}$$

The σ^2 here is the noise power spectral density at the bit decision maker, and $\frac{E_S}{N_0}$ is the message symbol energy to noise power spectral density.

4.3 Computer Simulations

The message and watermark error rates, respectively Equations 4.11 and 4.16, are confirmed using computer simulations in MATLAB. A custom QPSK modulator and demodulator pair was used without any dependencies on non-standard toolboxes. The watermarking was done with the same code using in BPSK simulations. Simulations used 10^4 randomly generated symbols ($2 \cdot 10^4$ bits) with a watermark angle $\phi = \frac{\pi}{16}$. Sampling rate was set to be 100 samples per symbol and the symbol duration was 1 sinusoid period. The simulations use $\frac{E_b}{N_0}$ as the controlled variable rather than $\frac{E_S}{N_0}$. The relationship is simply $2\frac{E_b}{N_0} = \frac{E_S}{N_0}$.

The simulated constellation is the same used in the previous derivations, shown in Figure 4.3. Figure 4.4 shows the results of the simulation. The three lines shown are

- black dots with the percentage of the 10^4 symbols received in error for the given $\frac{E_b}{N_0}$
- blue dashed line showing the expected symbol error rate for watermarked QPSK. Calculated from Equation 4.12
- green dotted line showing non-watermarked, standard QPSK symbol error rates. Calculated from Equation 4.4

The expected symbol error rate matches very close to the computer simulation. The watermark angle has a large affect on the symbol error. When the watermark angle puts the expected received symbol closer to the symbol decision boundary (I and Q axes) than the non-watermarked symbol location then the message bit error rate becomes higher than the watermark bit error rate. To prevent this the watermark angle should be kept lower than $\frac{\pi}{8}$.

The watermark error rate, shown in Figure 4.5, also matches very close to the simulation when $\frac{E_b}{N_0} > 0$dB. The gap between the simulation and expected rates for $\frac{E_b}{N_0} < 0$ exists because the expected rate, Equation 4.16, assumes anything outside of the decision region that the transmitted symbol exists in will be wrong. Using Figure 4.3 as a reference the constellation can be broken in to four decision regions for looking at the watermark. Opposite sides of the constellation have the same watermark, but the received signal would have to be dominated by noise for a symbol to land there. When $\frac{E_b}{N_0} < 0$dB the noise energy is at least half of the received energy, so the symbol is on the wrong half of the quadrant frequently. The difference between simulation and theory can be overcome by changing the limits of integration in Equation 4.16, but this increases the time of numerical integration

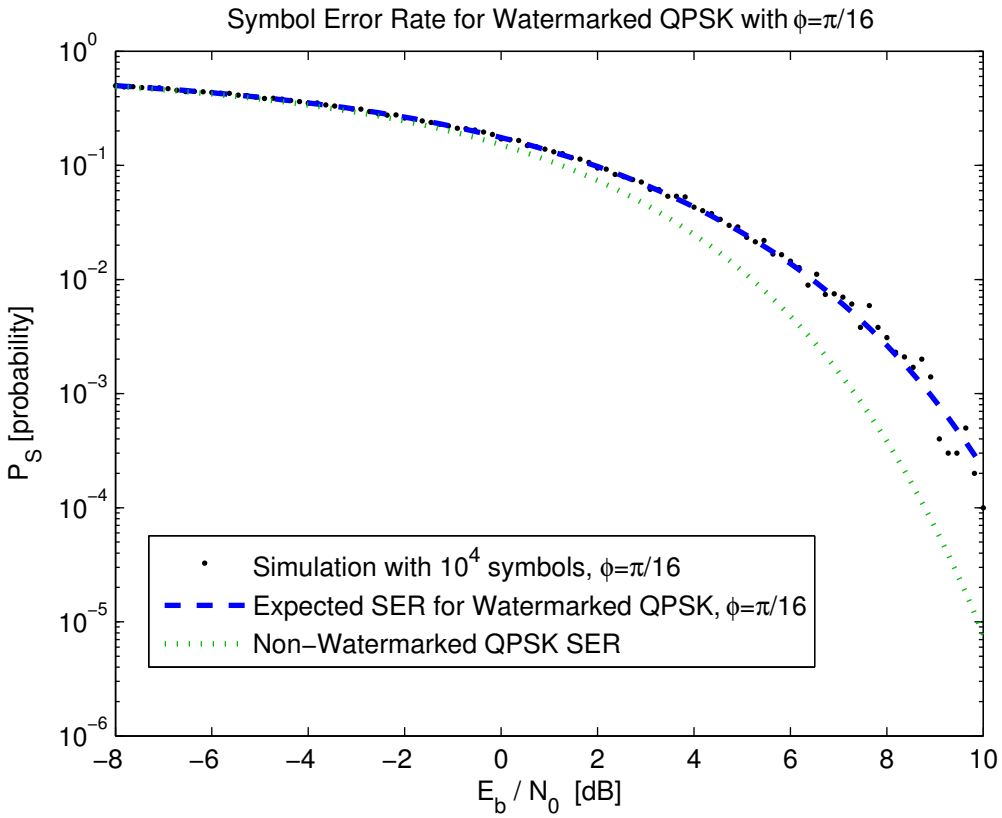

Figure 4.4: Symbol error rate for watermarked QPSK. $\phi = \frac{\pi}{16}$. Non-watermarked QPSK shown for reference.

and does not provide any insight since communication is unlikely with such low SNRs, and watermarks would not be effective.

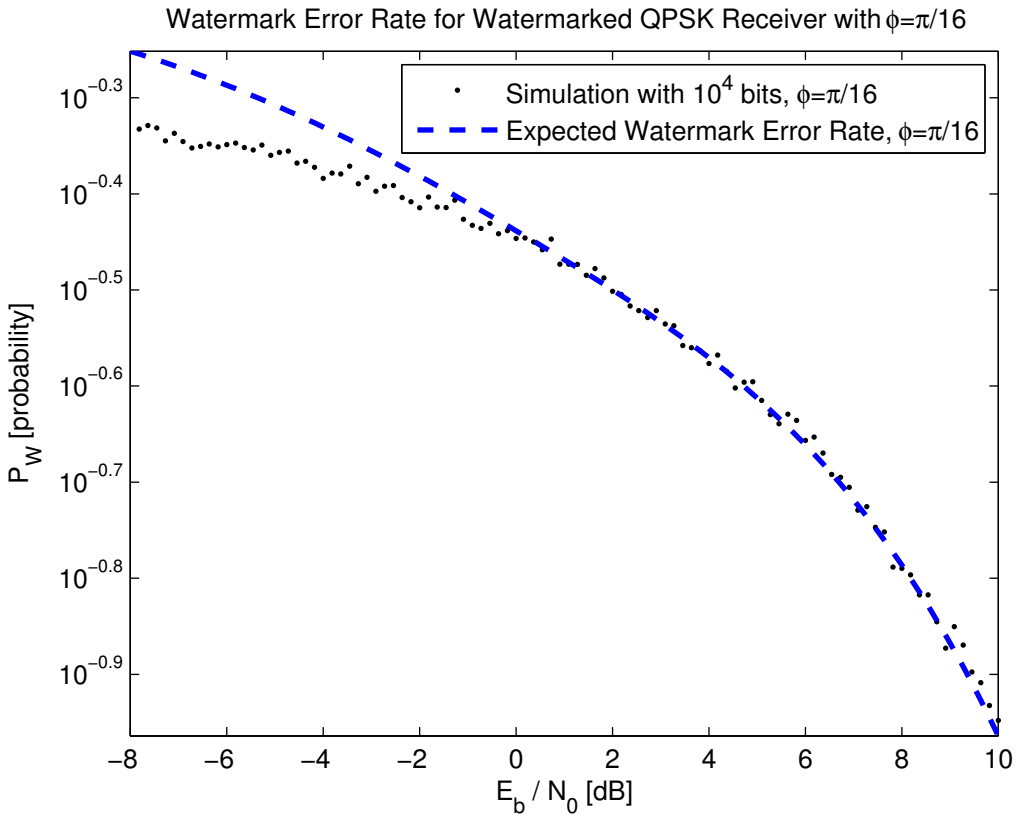

Figure 4.5: Watermark error rate for QPSK. $\phi = \frac{\pi}{16}$. The mismatch for $\frac{E_b}{N_0} < 0$ is due to a simplification used in the plotted 'Expected Watermark Error Rate'.

CHAPTER 5

Phase Dithered QAM Error Rates

5.1 16-QAM

QAM uses the sum of a weighted sine and cosine to form constellation symbols. There are a large number of possible constellations with varying numbers of constellation points [11,22]. This study chooses to focus on square 16-QAM. A 16-QAM constellation encodes four bits in to each symbol; a possible signal constellation is shown in Figure 5.1. The distance between adjacent constellation points, labeled d in Figure 5.1, will be important for the derivation of symbol error rates. Any of the transmitted symbols is formed using Equation 5.1, where $a(t)$ and $b(t)$ are pulses with four levels each (2 bits in $a(t)$ and 2 bits in $b(t)$).

$$r(t) = a(t)\cos(\omega t) + b(t)\sin(\omega t) \tag{5.1}$$

The quadrature demodulator used for watermarked BPSK and QPSK detection is also used for QAM symbol detection. A symbol decision is made by choosing the constellation point that is the closest (Euclidean distance) to the output of the demodulator. Using this decision rule creates squared decision regions around the inner symbols (labeled 5, 6, 9, and 10). The outer symbols have decision regions that are squared, but missing one or two edges on the outside of the constellation, depending on whether the point is on a corner (missing two edges) or on a side (missing one edge). These square decision regions, shown as the thin lines in Figure 5.1, are useful for deriving symbol error rates and provide a method of making symbol decisions faster than calculating 16 euclidean distances

For 16-QAM the probability of a symbol error is derived in Appendix D. QAM differs from the previously studied modulations by having symbols with several possibilities of energy. This introduces a new term used in the expression of symbol errors: E_{avg}, which represents the average energy of all possible symbols. The probability of symbol error for non-watermarked 16-QAM that is well known in the literature is repeated here from Equation D.20. The work in Appendix D will be referenced during the derivation of symbol

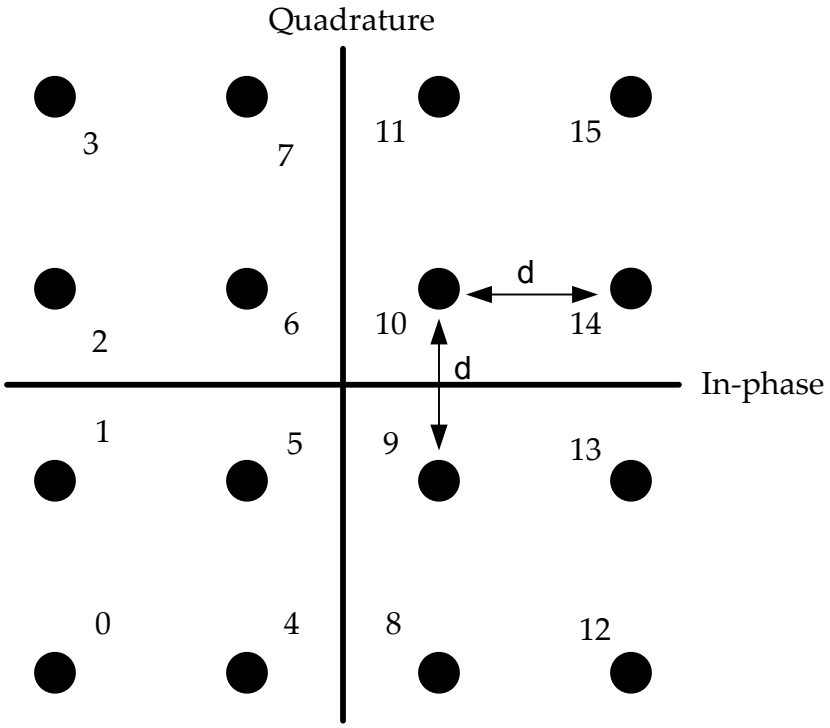

Figure 5.1: A square 16-QAM constellation with symbols numbered 0 through 15. The distance d is the distance between adjacent constellation points.

errors for watermarked QAM.

$$P_S\left(\frac{E_{avg}}{N_0}\right) = 4Q\left(\sqrt{\frac{E_{avg}}{5N_0}}\right) - 4Q\left(\sqrt{\frac{E_{avg}}{5N_0}}\right)^2 \tag{5.2}$$

5.2 Watermarked 16-QAM

Once again, this study is interested in phase-dithered watermarking, which splits each message symbol in to two watermark symbols (just as it did with BPSK and QPSK). This type of watermark applied to 16-QAM results in the constellation shown in Figure 5.2, which highlights the watermark decision regions with a gray and white background. The watermark angle alternates between adjacent bits so that large regions of the same color share a watermark bit. This arrangement is similar to a gray code in the sense that adjacent symbols have minimal differences.

In the constellation shown the white regions with gray symbols have a watermark of bit of 0 and the gray regions with white symbols have a watermark bit of 1. The watermark angle, defined as ϕ, is used to rotate the inner symbols. The remaining symbols must be shifted by an angle normalized by distance from the origin to keep the arc distance between the non-

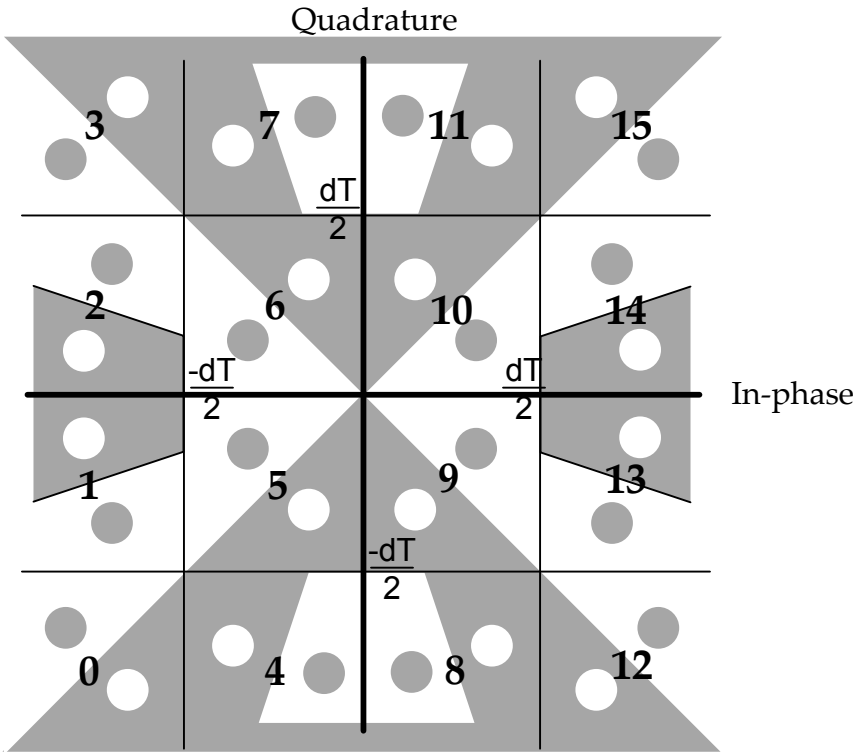

Figure 5.2: A watermarked square 16-QAM constellation as seen at the output of a receiver's matched filter detector. Each point is rotated by an angle scaled by distance from the origin.

symbol	radial distance	watermark angle	arc length
inner	$dT\frac{\sqrt{2}}{4}$	ϕ	$\phi dT\frac{\sqrt{2}}{4}$
outer edge	$dT\frac{\sqrt{10}}{4}$	$\frac{\phi}{\sqrt{5}}$	$\phi dT\frac{\sqrt{2}}{4}$
outer corner	$3dT\frac{\sqrt{2}}{4}$	$\frac{\phi}{3}$	$\phi dT\frac{\sqrt{2}}{4}$

Table 5.1: Summary of symbol radii, scaled watermark angles, and resulting arc-length distance from the non-watermarked symbol position.

watermarked symbol and the watermarked symbol constant for the entire constellation. Table 5.1 shows the radial distance, normalized watermark angle, and arc length after normalizing the angle for the three symbol locations (edge such as symbols 1 or 2, inner such as symbols 9 or 10, and outer corner such as 0) in 16-QAM. Normalizing watermark angles to keep constant arc lengths between non-watermarked symbols and watermarked symbols is necessary to prevent excessive errors on the outer symbols. Without normalizing the watermark angles even small angles could cause adjacent symbols to cross in to neighboring decision regions for the higher energy symbols.

The energy of a transmitted symbol is not changed by watermarking because the watermarked symbol is the same distance from the origin as the non-watermarked symbol. The

watermarked symbol at the receiver for the duration of a specific symbol, $r(t)$, is

$$r(t) = a\cos(\omega t \pm \phi) + b\sin(\omega t \pm \phi) \tag{5.3}$$

For the symbol error rate analysis the metrics for inner constellation points (points 5, 6, 9, 10) are used because they represent the worst case in terms of symbol errors. These symbols can have an error on all sides of their decision boundaries, unlike the outer symbols which have an unbounded region on the outer edges of the expected constellation.

5.2.1 Watermarked 16-QAM Probability of Message Symbol Error

QAM demodulation uses the same quadrature demodulator as QPSK and watermarked BPSK, shown in Figure 4.1. This demodulator splits the input to two paths, one (the I channel) is mixed with a cosine and the other (the Q channel) is mixed with a sinusoid. After mixing the channels go through a matched filter detector; for square pulses this is integrate and dump over the symbol length. Equation 5.6 shows this process. The matched filter outputs decision statistics, l_1 and l_2, that are used to determine symbol and watermark. These statistics will have a distribution matching the communication channel. Through an AWGN channel the means, $\overline{l_1}$ and $\overline{l_2}$, are the result of a noiseless signal through the demodulator which is shown in Equation 5.6.

$$\overline{l_1} = \int_0^T r(t) \cdot \cos(\omega t) dt \tag{5.4a}$$

$$\overline{l_2} = \int_0^T r(t) \cdot \sin(\omega t) dt \tag{5.4b}$$

Substituting in the received signal, $r(t)$, from Equation 5.3 gives Equation 5.5.

$$\overline{l_1} = \int_0^T \cos(\omega t) \left[a\cos(\omega t \pm \phi) + b\sin(\omega t \pm \phi)\right] dt \tag{5.5a}$$

$$\overline{l_2} = \int_0^T \sin(\omega t) \left[a\cos(\omega t \pm \phi) + b\sin(\omega t \pm \phi)\right] dt \tag{5.5b}$$

Some algebraic manipulation and product-to-sum trigonometric identities results in

$$\overline{l_1} = \frac{1}{2}\int_0^T a\left[\cos\left(2\omega t \pm \phi\right) + \cos\left(\pm\phi\right)\right] + b\left[\sin(2\omega t \pm \phi) + \sin(\pm\phi)\right] dt \tag{5.6a}$$

$$\overline{l_2} = \frac{1}{2}\int_0^T a\left[\sin\left(2\omega t \pm \phi\right) - \sin\left(\pm\phi\right)\right] + b\left[\cos(\pm\phi) - \cos(2\omega t \pm \phi)\right] dt \tag{5.6b}$$

The next step is to solve the integration. Each statistic has four sinusoidal terms summed together, which can each be integrated individually. The double frequency terms all result in 0 after integration because the limits of integration cover an integer number of periods. The remaining terms are all constant values, shown in Equation 5.8.

$$\overline{l_1} = \frac{aT}{2}\cos(\pm\phi) + \frac{bT}{2}\sin(\pm\phi)dt \tag{5.7a}$$

$$\overline{l_2} = \frac{bT}{2}\cos(\pm\phi) - \frac{aT}{2}\sin(\pm\phi)dt \tag{5.7b}$$

The following derivation will use the symbol labeled 10 in Figure 5.2 with the watermark $-\phi$. For this symbol the values of a and b are half the distance between adjacent symbols, denoted $a = b = {}^{d}/_{2}$. Equation 5.8 shows the decision statistics for this symbol with the previously mentioned substitutions.

$$\overline{l_1} = \frac{dT}{4}\cos(\phi) - \frac{dT}{4}\sin(\phi) \tag{5.8a}$$

$$\overline{l_2} = \frac{dT}{4}\cos(\phi) + \frac{dT}{4}\sin(\phi) \tag{5.8b}$$

The decision boundaries for this symbol form a square region bounded by limits shown in Equation 5.9. Q-functions can be used to express the symbol error rate because the decision region boundaries are parallel to the I and Q axes. These decision boundaries are illustrated along with Gaussian curve in Figure 5.3.

$$symbol_{10} = \begin{cases} 0 < l_1 < \frac{dT}{2} \\ 0 < l_2 < \frac{dT}{2} \end{cases} \tag{5.9}$$

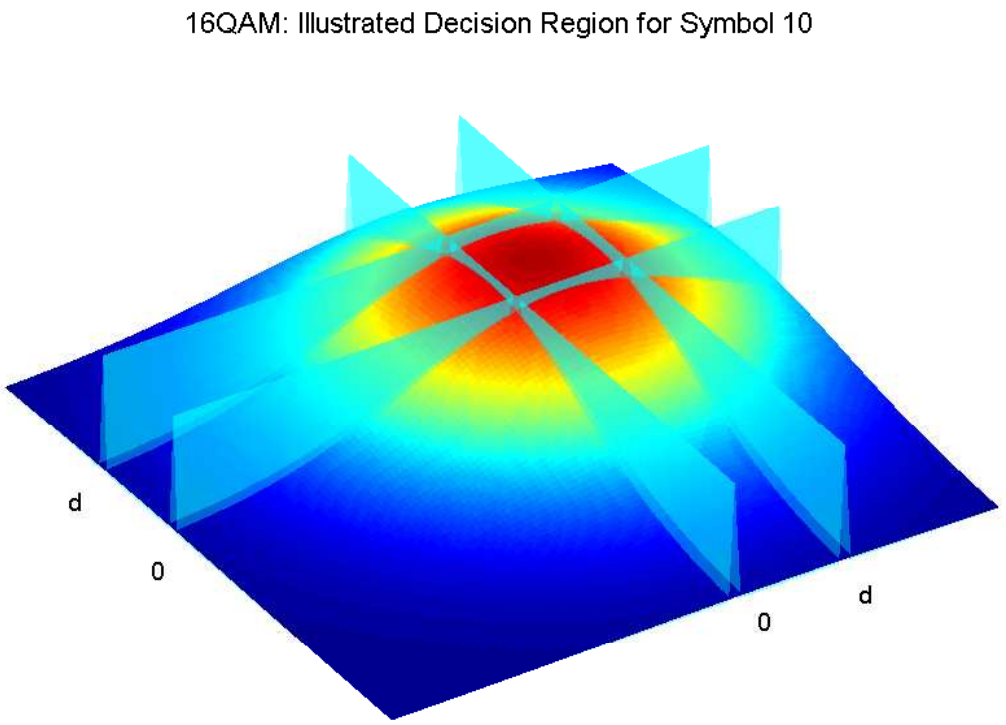

Figure 5.3: A 3-dimensional view of the probability density function of symbol 10. The teal planes coming vertically up are the message decision regions around the symbol.

$$P_S\left(\frac{E_{avg}}{N_0}\right) = 1 - \left[1 - \left[Q\left(\frac{\frac{dT}{2} - \overline{l_1}}{\sigma}\right) + Q\left(\frac{-\overline{l_1}}{\sigma}\right)\right]\right] \times \left[1 - \left[Q\left(\frac{\frac{dT}{2} - \overline{l_2}}{\sigma}\right) + Q\left(\frac{-\overline{l_2}}{\sigma}\right)\right]\right] \times \tag{5.10}$$

$$P_S\left(\frac{E_{avg}}{N_0}\right) = 1 - \left\{1 - \left[Q\left(\frac{\frac{dT}{2} - \frac{dT}{4}\cos(\phi) + \frac{dT}{4}\sin(\phi)}{\sqrt{\frac{N_0 T}{4}}}\right) + Q\left(-\frac{\frac{dT}{4}\cos(\phi) - \frac{dT}{4}\sin(\phi)}{\sqrt{\frac{N_0 T}{4}}}\right)\right]\right\} \times \left\{1 - \left[Q\left(\frac{\frac{dT}{2} - \frac{dT}{4}\cos(\phi) - \frac{dT}{4}\sin(\phi)}{\sqrt{\frac{N_0 T}{4}}}\right) + Q\left(-\frac{\frac{dT}{4}\cos(\phi) + \frac{dT}{4}\sin(\phi)}{\sqrt{\frac{N_0 T}{4}}}\right)\right]\right\} \tag{5.11}$$

$$P_S\left(\frac{E_{avg}}{N_0}\right) = 1 - \left\{1 - \left[Q\left(\sqrt{\frac{d^2 T}{4N_0}}\left(2 - \cos(\phi) + \sin(\phi)\right)\right) + Q\left(\sqrt{\frac{d^2 T}{4N_0}}\left(-\cos(\phi) + \sin(\phi)\right)\right)\right]\right\} \times \left\{1 - \left[Q\left(\sqrt{\frac{d^2 T}{4N_0}}\left(2 - \cos(\phi) - \sin(\phi)\right)\right) + Q\left(\sqrt{\frac{d^2 T}{4N_0}}\left(-\cos(\phi) - \sin(\phi)\right)\right)\right]\right\} \tag{5.12}$$

The average energy per symbol, from Equation D.9, has not changed from non-watermarked QAM since the watermark only rotates symbols around a circle. The average symbol energy is now substituted in $E_{avg} = {}^{5d^2T}/_4$.

$$
\begin{aligned}
P_S\left(\frac{E_{avg}}{N_0}\right) = 1 - & \\
& \left\{1 - \left[Q\left(\sqrt{\frac{E_{avg}}{5N_0}}\,(2 - \cos(\phi) + \sin(\phi))\right) + \right.\right. \\
& \left.\left. Q\left(\sqrt{\frac{E_{avg}}{5N_0}}\,(-\cos(\phi) + \sin(\phi))\right)\right]\right\} \times \\
& \left\{1 - \left[Q\left(\sqrt{\frac{E_{avg}}{5N_0}}\,(2 - \cos(\phi) - \sin(\phi))\right) + \right.\right. \\
& \left.\left. Q\left(\sqrt{\frac{E_{avg}}{5N_0}}\,(-\cos(\phi) - \sin(\phi))\right)\right]\right\}
\end{aligned}
\tag{5.13}
$$

Multiplying the terms results in

$$
\begin{aligned}
P_S\left(\frac{E_{avg}}{N_0}\right) = & Q\left(\sqrt{\frac{E_{avg}}{5N_0}}\,(2 - \cos(\phi) + \sin(\phi))\right) + Q\left(\sqrt{\frac{E_{avg}}{5N_0}}\,(-\cos(\phi) + \sin(\phi))\right) \\
& + Q\left(\sqrt{\frac{E_{avg}}{5N_0}}\,(2 - \cos(\phi) - \sin(\phi))\right) + Q\left(\sqrt{\frac{E_{avg}}{5N_0}}\,(-\cos(\phi) - \sin(\phi))\right) \\
& - \left[Q\left(\sqrt{\frac{E_{avg}}{5N_0}}\,(2 - \cos(\phi) + \sin(\phi))\right) + Q\left(\sqrt{\frac{E_{avg}}{5N_0}}\,(-\cos(\phi) + \sin(\phi))\right)\right] \\
& \times \left[Q\left(\sqrt{\frac{E_{avg}}{5N_0}}\,(2 - \cos(\phi) - \sin(\phi))\right) + Q\left(\sqrt{\frac{E_{avg}}{5N_0}}\,(-\cos(\phi) - \sin(\phi))\right)\right]
\end{aligned}
\tag{5.14}
$$

The previous general solution, Equation 5.14, can be approximated by the slightly less verbose form shown in Equation 5.17. This approximation assumes that the mean of the decision statistics, $\overline{l_1}$ and $\overline{l_2}$, are equidistant to the decision boundaries, which is close to being true for small watermark angles. For example, this symbol under consideration (symbol 10) has distance from the origin $r = dT\sqrt{2}/4$. The in-phase displacement, δ, of the symbol after watermarking can be found intuitively because the x-position (in-phase direction) of a point on a circle centered at the origin is $x = r\cos(\theta)$. For this symbol the in-phase displacement, or the in-phase difference between the watermarked symbol and a non-watermarked symbol, would be $\delta = dT\frac{\sqrt{2}}{4}(\cos(\pi/4) - \cos(\pi/4 - \phi/2))$. As long as this magnitude of displacement is much smaller than the total distance from one edge of the decision boundary to the other the approximation of Equation 5.17 is valid. An alternative form of this approximation is shown with only the terms required in Equation 5.16. If $\phi = \frac{\pi}{16}$, then the inequality becomes $0.09 << 1$, which is valid. The assumption begins to break down around for watermark angles larger than $\pi/14$, when the displacement is less

than an order of magnitude of the total distance between decision boundaries.

$$\left| dT \frac{\sqrt{2}}{2} (\cos(\pi/4) - \cos(\pi/4 - \phi/2)) \right| << \frac{dT}{2} \tag{5.15}$$

$$\left| \sqrt{2} (\cos(\pi/4) - \cos(\pi/4 - \phi/2)) \right| << 1 \tag{5.16}$$

$$\begin{aligned} P_S\left(\frac{E_{avg}}{N_0}\right) =& 2Q\left(\sqrt{\frac{E_{avg}}{5N_0}}\left(2 - [\cos(\phi) + \sin(\phi)]\right)\right) + \\ & 2Q\left(\sqrt{\frac{E_{avg}}{5N_0}}\left(2 - [\cos(\phi) - \sin(\phi)]\right)\right) - \\ & 4Q\left(\sqrt{\frac{E_{avg}}{5N_0}}\left(2 - [\cos(\phi) + \sin(\phi)]\right)\right) \times \\ & Q\left(\sqrt{\frac{E_{avg}}{5N_0}}\left(2 - [\cos(\phi) - \sin(\phi)]\right)\right) \end{aligned} \tag{5.17}$$

5.2.2 Watermarked 16-QAM Probability of Watermark Recovery Error

The watermark error probability for a 16-QAM constellation cannot be easily simplified to a Q-function form because the optimal decision boundaries are not parallel to the in-phase and quadrature axes. The decision boundaries used in this study, drawn in Figure 5.2, were chosen to create large areas that share a binary watermark value. This causes the actual watermark angle, either positive or negative, to be a function of the symbol and the binary watermark value. These large regions of shared binary watermark values will reduce the watermark error rate when compared to a constellation that does not take advantage of grouping similar bit patterns in adjacent symbols. The side-affect of this is there are several unique cases that must be considered to derive a general probability of a watermark error. The following sections cover the four possible cases, and symmetry is used to focus on a single quadrant.

From Figure 5.2 there is some symmetry in the watermark decision regions. The shaded regions all have the same binary watermark value, and the regions with a white background have the other binary value. The shaded regions also show the watermark boundaries; there are two unique shapes to consider for the watermark error probability. Both of these cases have one edge that extends to infinity, but for the sake of identification they will be called the triangular region and the extended trapezoid. The triangular region is an isosceles

triangle with a trapezoid missing from the unique edge; the triangle on the right side of the constellation in Figure 5.2 is bounded by $y = x$ and $y = -x$. The extended trapezoid is the area that is shaded gray in Figure 5.2, and is the trapezoid that is missing from the triangular section.

The probability of watermark error, derived in the following sections, must be left in integral form and calculated numerically. The probability that is used can either be found using the worst case, where the symbol closest to decision regions is used as representative of all symbols, or the probability for all symbols can be averaged together. The simpler approach of choosing the worst case symbol will give a slightly higher probability of error than will be observed and be a faster and simpler calculation. For completeness the more accurate estimate, averaging probability of error over all symbol possibilities, will be derived here. Using symmetry there are four unique probabilities that will be calculated: one of the watermarked symbols from symbol 10, both watermarked symbols from symbol 14, and one watermarked symbol from symbol 15 in Figure 5.2. All of the other symbols will have the same probability of a watermark error as one of these four symbols.

Case 1: watermark in triangular region

The first watermark region under consideration is bounded by the lines $y = x$ and $y = -x$ for $x > 0$. There is a region from $\frac{dT}{2} < x < \infty$ between the lines $y = x/3$ and $y = -x/3$ that needs to be subtracted from the previously mentioned region. The $\frac{dT}{2}$ bound is the message symbol decision boundary, which is shared by the watermark decision boundary. At the receiver each of these symbols is a normally distributed random variable. The mean, μ, and variance, σ^2, completely define the random variable, which allows the probability of a watermark error in this region to be written as shown in Equation 5.18. The limits of integration come from the watermark decision boundaries, and the means are determined by the decision statistics for the symbol under consideration.

$$P_W = 1 - \left[\int_0^{\infty} \int_{-x}^{x} \frac{1}{2} \mathrm{N}\left(\mu_x, \sigma^2\right) \mathrm{N}\left(\mu_y, \sigma^2\right) dydx - \int_{\frac{dT}{2}}^{\infty} \int_{\frac{-x}{3}}^{\frac{x}{3}} \mathrm{N}\left(\mu_x, \sigma^2\right) \mathrm{N}\left(\mu_y, \sigma^2\right) dydx \right] \tag{5.18}$$

With the symbols in this region there are three unique means, one for each of the three symbols types (inner, edge, outer corner) that give different probabilities of error. The

difference in the means is the coefficient used to weight the sine/cosine components. Again, we refer to the distance between message symbols at the receiver as $\frac{dT}{2}$.

Symbol 10 has already been analyzed in the previous section for the message error probability, and the means (μ_x for the in-phase mean and μ_y for the quadrature mean) are

$$\mu_x = \frac{dT}{4}(\cos\phi + \sin\phi) \tag{5.19a}$$
$$\mu_y = \frac{dT}{4}(\cos\phi - \sin\phi) \tag{5.19b}$$

For the remaining symbols the watermark angle must be normalized by their distance from the origin compared to symbol 10, as summarized in Table 5.1. Symbol 14 with a positive watermark angle is in this region and has the expected values

$$u_x = \int_0^T \cos(\omega t)\left[\frac{3d}{2}\cos(\omega t + \frac{\phi}{\sqrt{5}}) + \frac{d}{2}\sin(\omega t + \frac{\phi}{\sqrt{5}})\right]dt \tag{5.20}$$
$$u_y = \int_0^T \sin(\omega t)\left[\frac{3d}{2}\cos(\omega t + \frac{\phi}{\sqrt{5}}) + \frac{d}{2}\sin(\omega t + \frac{\phi}{\sqrt{5}})\right]dt \tag{5.21}$$

Which easily simplifies to

$$\mu_x = \frac{dT}{4}\left(3\cos\frac{\phi}{\sqrt{5}} + \sin\frac{\phi}{\sqrt{5}}\right) \tag{5.22a}$$
$$\mu_y = \frac{dT}{4}\left(\cos\frac{\phi}{\sqrt{5}} - 3\sin\frac{\phi}{\sqrt{5}}\right) \tag{5.22b}$$

Symbol 15 with a negative watermark angle has expected values

$$u_x = \int_0^T \cos(\omega t)\left[\frac{3d}{2}\cos(\omega t + \frac{\phi}{3}) + \frac{3d}{2}\sin(\omega t + \frac{\phi}{3})\right]dt \tag{5.23}$$
$$u_y = \int_0^T \sin(\omega t)\left[\frac{3d}{2}\cos(\omega t + \frac{\phi}{3}) + \frac{3d}{2}\sin(\omega t + \frac{\phi}{3})\right]dt \tag{5.24}$$

These expected values simplify to

$$\mu_x = \frac{3dT}{4}\left(\cos\frac{\phi}{3} + \sin\frac{\phi}{3}\right) \tag{5.25a}$$
$$\mu_y = \frac{3dT}{4}\left(\cos\frac{\phi}{3} - \sin\frac{\phi}{3}\right) \tag{5.25b}$$

Substituting any of the means from Equations 5.19, 5.22, 5.25 in to Equation 5.18 and doing a numerical integration over the probability density function will yield the probability of watermark recovery error for the corresponding symbols. The variance, σ^2, is the same well used variance utilized in the previous quadrature demodulators: $\frac{N_0 T}{4}$.

Case 2: the extended trapezoid

Symbol 14 gets watermarked in to a region that looks like a trapezoid that was previously subtracted from the large triangular region. The volume of the probability density function outside of this region, and thus the probability of a watermark error, is found with the integral, in Equation 5.26.

$$P_W = 1 - \int_{\frac{dT}{2}}^{\infty} \int_{\frac{-x}{3}}^{\frac{x}{3}} \mathrm{N}\left(\mu_x, \sigma^2\right) \mathrm{N}\left(\mu_y, \sigma^2\right) dydx \tag{5.26}$$

The expected values, μ_x and μ_y, for the probability density functions are the decision statistics at the receiver. Equation 5.28 shows the mean values to use.

$$u_x = \int_0^T \cos(\omega t) \left[\frac{3d}{2}\cos(\omega t - \frac{\phi}{\sqrt{5}}) + \frac{d}{2}\sin(\omega t - \frac{\phi}{\sqrt{5}})\right] dt \tag{5.27a}$$

$$u_y = \int_0^T \sin(\omega t) \left[\frac{3d}{2}\cos(\omega t - \frac{\phi}{\sqrt{5}}) + \frac{d}{2}\sin(\omega t - \frac{\phi}{\sqrt{5}})\right] dt \tag{5.27b}$$

$$\mu_x = \frac{dT}{4}\left(3\cos\frac{\phi}{\sqrt{5}} + \sin\frac{\phi}{\sqrt{5}}\right) \tag{5.28a}$$

$$\mu_y = \frac{dT}{4}\left(\cos\frac{\phi}{\sqrt{5}} - 3\sin\frac{\phi}{\sqrt{5}}\right) \tag{5.28b}$$

Summary

The four probability density functions for the unique symbol types are found in Equations 5.18 and 5.26 combined with the known expected values of the symbols.

The probability of watermark error for 16-QAM is complex because of the non-uniform constellation spacing created by the watermark and phase normalizing. Optimizing the chosen decision regions for successful watermark recovery creates four unique probabilities

in two decision areas that need to be computed numerically and averaged together. In practice it should be sufficient to choose one of the cases as representative and simplify the calculation to a single integral, but all four cases are shown for completeness. The following section will use a computer simulation to compare the average probability of watermark errors to the expected watermark error using only symbol 10's probability of watermark error. The complete equation for this error can be written by substituting Equation 5.19 in to Equation 5.18; the result is shown in Equation 5.29.

$$\begin{aligned} P_W = 1 - & \\ & \left[\int_0^{\infty} \int_{-x}^{x} \frac{1}{2} \mathrm{N}\left(\frac{dT}{4} \left(\cos\phi + \sin\phi \right), \sigma^2 \right) \mathrm{N}\left(\frac{dT}{4} \left(\cos\phi - \sin\phi \right), \sigma^2 \right) dydx \right. \\ & \left. - \int_{\frac{dT}{2}}^{\infty} \int_{\frac{-x}{3}}^{\frac{x}{3}} \mathrm{N}\left(\frac{dT}{4} \left(\cos\phi + \sin\phi \right), \sigma^2 \right) \mathrm{N}\left(\frac{dT}{4} \left(\cos\phi - \sin\phi \right), \sigma^2 \right) dydx \right] \end{aligned} \tag{5.29}$$

5.2.3 Computer Simulations

Using a custom modulator/demodulator pair in MATLAB the probability of symbol error and watermark error was tested and compared to the expected results. 10^5 symbols were randomly generated and watermarked before passing through an AWGN channel. The watermark angle, $\phi = \pi/16$, used in this simulation refers to the watermark angle for the inner symbols. The other symbols will be watermarked by another angle related to $\pi/16$ according to Table 5.1. The P_S rates are very close to the expected rates, as seen in Figure 5.4. In this figure the simulated probability of symbol error lies on top of the expected probability of symbol error from Equation 5.17. Both can be compared to the symbol error rate for standard 16-QAM constellation, plotted in green, using Equation D.20.

The probability of watermark error was simulated simultaneous to the symbol error. The simulated probability (black dots) compared to the expected (green and blue dashed lines) probability of watermark error is shown in Figure 5.5. The expected simplified P_W here is calculated using Equation 5.29, which uses watermarked symbols from symbol 10 as the worst-case. Noting that the watermark consists of two possible symbols (one bit) even though the message consists of 16 possible symbols (four bits) the expected watermark errors are greater than $1/2$ due to approximations used in the derivation of the watermark error rate, which obviously is not possible in implementation. Specifically, the watermark was assumed to be wrong outside of a single area. This is not the case with low $\frac{E_S}{N_0}$ since each watermark value has four distinct regions (refer to Figure 5.2 in which it will be correctly decoded.) A receiver may correctly give a watermark even if the received signal is far from

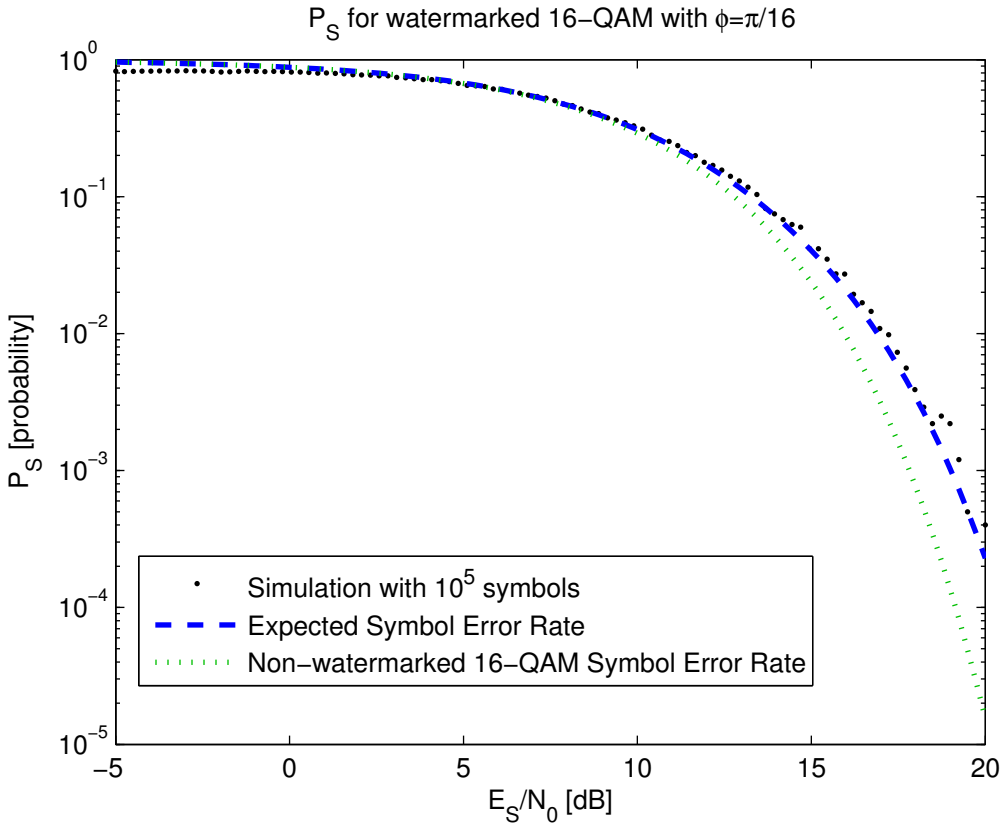

Figure 5.4: Simulated results of probability of symbol error compared to theory. 10^5 symbols were used to find the expected number of errors in each value of $\frac{E_S}{N_0}$ tested. The green line is non-watermarked 16-QAM for comparison.

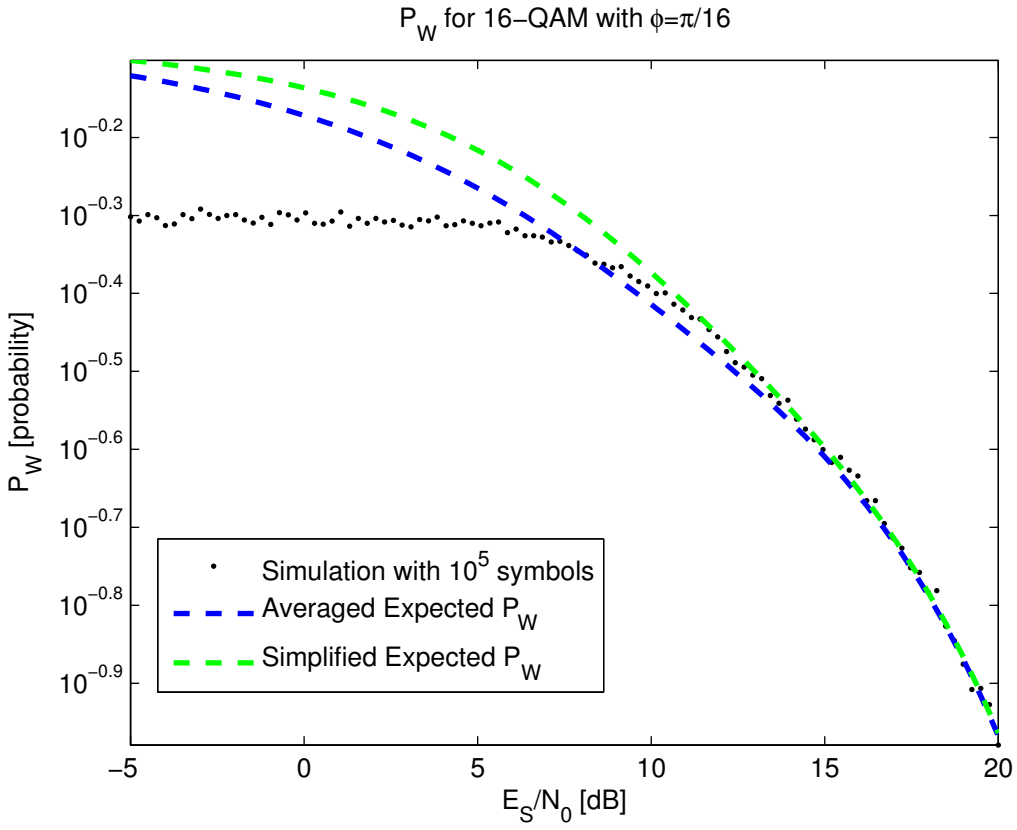

Figure 5.5: Simulated results of probability of watermark error compared to theory. Errors across 10^5 symbols average in to each data point. The green line is the simplified probability of watermark.

the correct symbol. This approximation is accurate at the higher $^{E_S}/_{N_0}$ values that yield a more reliably detected watermark symbol. The probability of watermark is only inaccurate when the P_W is close to 0.5, where the system would be unusable. As indicated previously a single integral could reasonably be substituted for the average over the four integrals given in Section 5.2.1.

CHAPTER 6

Phase Dithered Differential BPSK Error Rates

Differential BPSK (DBPSK) uses anti-podal signaling similar to coherent BPSK, but uses the previous symbol rather than a locally generated sinusoid as the reference signal. This technique increases the probability of bit errors, but reduces the receiver complexity by not requiring coherent phase synchronization. An optimal implementation of the process is shown in Figure 6.1 [22].

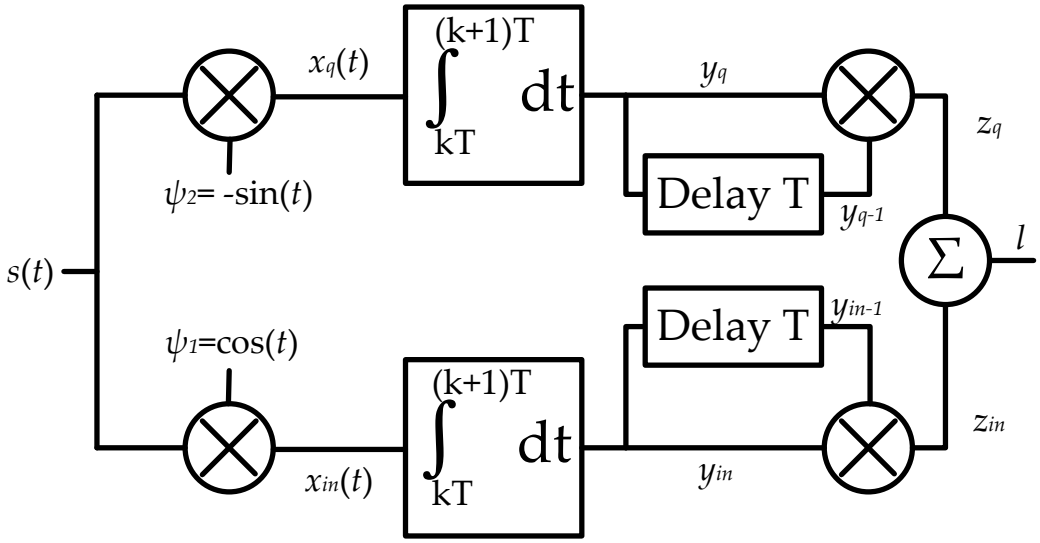

Figure 6.1: A non-coherent DBPSK receiver with input $s(t)$ makes message and watermark decisions on l.

6.1 DBPSK Receiver

The received signal, $s(t)$, is split in to quadrature and in-phase components respectively denoted $x_{in}(t)$ and $x_q(t)$. Equation 6.1 shows a model of what the received signal looks like where $M(t)$ is the binary PSK message bit, $W(t)$ is the watermark bit, and α is a phase offset assumed to be constant during the symbol duration from not being phase synchronized.

$$s(t) = \cos\left(\omega t + \pi M(t) + \phi W(t) + \alpha\right) \tag{6.1}$$

The pulse after integrating is referred to as $y_{in}(t)$ for the in-phase path and $y_q(t)$ for the quadrature path. These pulses are multiplied with the previous symbol pulse which will be referred to as $y_{in-1}(t)$ for the previous in-phase pulse and $y_{q-1}(t)$ for the previous quadrature pulse.

$$\begin{aligned} y_{in}(t) &= \int_0^T \cos\left(\omega t + \pi M(t) + \phi W(t) + \alpha\right) \cdot \cos(\omega t) dt \\ y_q(t) &= \int_0^T \cos\left(\omega t + \pi M(t) + \phi W(t) + \alpha\right) \cdot \sin(\omega t) dt \end{aligned} \tag{6.2}$$

Multiplying, integrating, and assuming an integer number of sinusoid cycles per symbol yields

$$\begin{aligned} y_{in}(t) &= \frac{T}{2} \cos\left(\pi M(t) + \phi W(t) + \alpha\right) \\ y_q(t) &= -\frac{T}{2} \sin\left(\pi M(t) + \phi W(t) + \alpha\right) \end{aligned} \tag{6.3}$$

The product of current symbols and previous symbols is $z_q(t)$ and $z_{in}(t)$. The notation $z_{in-1}(t)$ and $z_{q-1}(t)$ will be used for the previous symbol, which is equivalent to $z_{in}(t-T)$ and $z_q(t-T)$. Using the second notation, expressions for z are given in Equation 6.4.

$$\begin{aligned} z_{in}(t) &= y_{in}(t) y_{in}(t-T) \\ z_q(t) &= y_q(t) y_q(t-T) \end{aligned} \tag{6.4}$$

Substituting the integrator output from Equation 6.3 in to Equation 6.4 will give Equation 6.5.

$$\begin{aligned} z_{in}(t) &= \frac{T}{2} \cos\left(\pi M(t) + \phi W(t) + \alpha\right) \cdot \frac{T}{2} \cos\left(\pi M(t-T) + \phi W(t-T) + \alpha\right) \\ z_q(t) &= -\frac{T}{2} \sin\left(\pi M(t) + \phi W(t) + \alpha\right) \cdot -\frac{T}{2} \sin\left(\pi M(t-T) + \phi W(t-T) + \alpha\right) \end{aligned} \tag{6.5}$$

Now looking at all possible combinations of message and watermark bits will give all possible values for z, and eventually the expected values for l. The decision statistic, l, will be used to determine watermark and message bits which is the sum of z_q and z_{in}, shown in Equation 6.6.

$$l = z_{in}(t) + z_q(t) \tag{6.6}$$

With differential signaling of two bits (one message bit and one watermark bit) there

are four possible unique values for l. Keeping in mind that the actual bit transferred comes from bit changes, the possible events are

- The message and watermark bits do not change
- The message bit does not change, but watermark does change
- The message bit changes, but watermark does not change
- Both message and watermark bits change

The expected values for the decision statistic, l, will be found in the following four sections for each of these events.

6.1.1 Message and Watermark Bits do not Change

Starting with Equation 6.5, use $M(t) = M(t-T) = 0$ and $W(t) = W(t-T) = -1$.

$$\begin{aligned} z_{in}(t) &= \frac{T^2}{4}\cos(-\phi+\alpha)\cdot\cos(-\phi+\alpha) \\ z_q(t) &= \frac{T^2}{4}\sin(-\phi+\alpha)\cdot\sin(-\phi+\alpha) \end{aligned} \tag{6.7}$$

After using common trigonometric identities and algebra this simplifies to

$$\begin{aligned} z_{in}(t) &= \frac{T^2}{8}\left[1+\cos(-2\phi+2\alpha)\right] \\ z_q(t) &= \frac{T^2}{8}\left[1-\cos(-2\phi+2\alpha)\right] \end{aligned} \tag{6.8}$$

The sum of in-phase and quadrature components gives the decision statistic,

$$l = \frac{T^2}{4} \tag{6.9}$$

6.1.2 Constant Message with Changing Watermark

In this case the messages will be $M(t) = M(t-T) = 0$. The watermarks will be $W(t) = -1$ and $W(t-T) = 1$. Substituting these in to Equation 6.5 gives

$$\begin{aligned} z_{in}(t) &= \frac{T^2}{4}\cos(-\phi+\alpha)\cdot\cos(+\phi+\alpha) \\ z_q(t) &= \frac{T^2}{4}\sin(-\phi+\alpha)\cdot\sin(+\phi+\alpha) \end{aligned} \tag{6.10}$$

Trigonometric identities and algebra simplifies this to

$$\begin{aligned} z_{in}(t) &= \frac{T^2}{8}\left[\cos\left(2\phi\right) + \cos\left(2\alpha\right)\right] \\ z_q(t) &= \frac{T^2}{8}\left[\cos\left(2\phi\right) - \cos\left(2\alpha\right)\right] \end{aligned} \tag{6.11}$$

The expected value of l in this case is

$$l = \frac{T^2}{4}\cos 2\phi \tag{6.12}$$

6.1.3 Changing Message with Constant Watermark

In this case the messages will be $M(t) = 0$ and $M(t-T) = 1$. The watermarks will be $W(t) = W(t-T) = -1$.

From equation 6.5 the values for z are

$$\begin{aligned} z_{in}(t) &= \frac{T^2}{4}\cos\left(-\phi + \alpha\right) \cdot \cos\left(\pi - \phi + \alpha\right) \\ z_q(t) &= \frac{T^2}{4}\sin\left(-\phi + \alpha\right) \cdot \sin\left(\pi - \phi + \alpha\right) \end{aligned} \tag{6.13}$$

$$\begin{aligned} z_{in}(t) &= \frac{T^2}{8}\left[-\cos\left(-2\phi + 2\alpha\right) - 1\right] \\ z_q(t) &= \frac{T^2}{8}\left[+\cos\left(-2\phi + 2\alpha\right) - 1\right] \end{aligned} \tag{6.14}$$

The expected value of l,

$$l = -\frac{T^2}{4} \tag{6.15}$$

6.1.4 Changing Message and Changing Watermark

In the final case the messages are $M(t) = 0$ and $M(t-T) = 1$. The watermarks will be $W(t) = -1$, and $W(t-T) = 1$.

Substituting the message and watermark in to Equation 6.5 yields

$$\begin{aligned} z_{in}(t) &= \frac{T^2}{4}\cos\left(-\phi + \alpha\right) \cdot \cos\left(\pi + \phi + \alpha\right) \\ z_q(t) &= \frac{T^2}{4}\sin\left(-\phi + \alpha\right) \cdot \sin\left(\pi + \phi + \alpha\right) \end{aligned} \tag{6.16}$$

Which simplifies to

$$\begin{aligned} z_{in}(t) &= \frac{T^2}{8}\left[\cos\left(\pi + 2\alpha\right) + \cos\left(\pi + 2\phi\right)\right] \\ z_q(t) &= \frac{T^2}{8}\left[\cos\left(\pi + 2\phi\right) - \cos\left(\pi + 2\alpha\right)\right] \end{aligned} \tag{6.17}$$

Summing the in-phase and quadrature components for the expected value of l gives,

$$l = -\frac{T^2}{4}\cos(2\phi) \tag{6.18}$$

6.1.5 Decision Regions

Decision boundaries for determining the watermark and message bits are placed equidistant from the previously derived expected values for l.

The expected values of l when the message changed, Equations 6.15 and 6.18, are both negative of the expected values of l when the message changed. This results in $l = 0$ being the boundary of a message bit decision.

When the watermark bit changes l comes from Equations 6.12 and 6.18. When the watermark bit remains the same l comes from Equations 6.9 and 6.15. Assuming the watermark bits are equally probable a decision boundary comes from the average of Equations 6.9 and 6.12 and another boundary is formed by the average of 6.15 and 6.18. Based on this the decision boundaries are easily found and shown in Equation 6.19.

$$l = \pm\frac{T^2}{8}\left(1 + \cos(2\phi)\right) \tag{6.19}$$

6.2 Bit Error Rates

6.2.1 DBPSK Noise

The DBPSK receiver from Figure 6.1 is well known to have noise with a laplacian probability distribution. The laplacian distribution comes from the sum of the quadrature and in-phase components which each have a product normal distribution. The sum of two product-normal distributions will give a laplacian distribution [14]. For DBPSK the probability distribution function of the noise is

$$f_N(n) = \frac{2}{N_0 T} e^{-\frac{4|n|}{N_0 T}} \tag{6.20}$$

6.2.2 Message Bit Energy

Assuming 1 bit/symbol With a symbol time of T the bit energy is

$$E_b = \int_0^{2T} s^2(t) \tag{6.21}$$

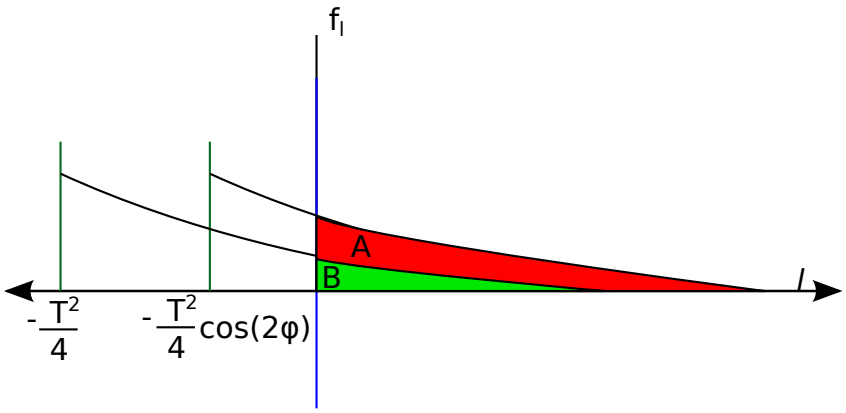

Figure 6.2: Green vertical lines show the two expected values for the message bits not changing between symbols. The black curves are half of the probability density function for received symbols. The message error rate is the sum of the green area labeled A and the red area labeled B.

The upper bound of integration is $2T$ because each bit has energy spread across two symbols. The message and watermark values will not change the bit energy, so Equation 6.1 can be used with $M(t) = 0$ and $W(t) = 1$.

This substitution gives

$$E_b = \int_0^{2T} \cos\left(\omega t + \phi\alpha\right)^2 dt \tag{6.22}$$

Evaluating will give the bit energy,

$$E_b = T \tag{6.23}$$

6.2.3 Message Error Rate

The message error rate is the sum of the areas shown under the green (labeled B) and red (labeled A) areas in Figure 6.2. These areas can be calculated by shifting the density functions to be centered around 0 and finding $P(l > \beta)$, where β is the distance from the expected value to the decision region.

The area under a right-hand side of a curve from Equation 6.20 is found with

$$P_M(\lambda) = \int_\beta^\infty \frac{2}{N_0 T} e^{-\frac{4\lambda}{N_0 T}} d\lambda \tag{6.24}$$

Integrating gives,

$$P_M(\lambda) = \frac{2}{N_0 T}\left(-\frac{N_0 T}{4} e^{-\frac{4\lambda}{N_0 T}}\right)\Bigg|_{\lambda=\beta}^{\infty} \tag{6.25}$$

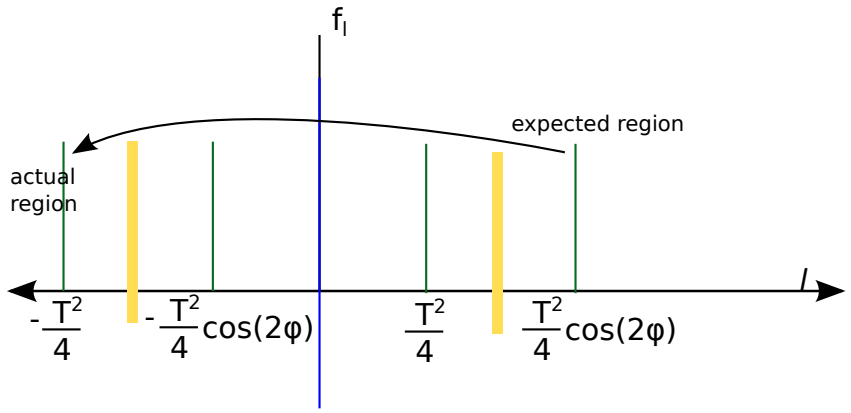

Figure 6.3: The worst, and most unlikely case, in terms of bit errors is the noise moves the received symbol in to the decision region furthest from where it would otherwise be expected. The green bars are expected values for decision statistics, and the watermark decision boundaries are shown with yellow bars. The message bit decision is based on the y-axis.

Evaluating will result in

$$P_M(\beta) = \frac{1}{2} e^{-4\frac{\beta}{N_0 T}} \tag{6.26}$$

β is the distance from an expected value to the decision boundary. There are four possible values for β that come from the expected values of l for message decisions. Two of these values are shown in Figure 6.2, the other two are positive, but have the same magnitude. Assuming that every combination of message bits is equally likely averaging the probability for each expected value of l is

$$P_M(\frac{E_b}{N_0}) = \frac{1}{4}\left(e^{-\frac{T}{N_0}} + e^{-\frac{T}{N_0}\cos 2\phi}\right) \tag{6.27}$$

Substituting the bit energy from Equation 6.23 gives

$$P_M(\frac{E_b}{N_0}) = \frac{1}{4}\left(e^{-\frac{E_b}{N_0}} + e^{-\frac{E_b}{N_0}\cos 2\phi}\right) \tag{6.28}$$

6.2.4 Watermark Error Rate

For the watermark error rate, analysis from the message error rate is valid up to Equation 6.26. From Equation 6.26 β is now made to be the distance between expected values of l and the decision boundaries for watermark bits, which were found in Equation 6.19

-

There are two expected values of l near each decision boundary that will dominate the watermark errors, and they are the same distance for all four combination of message

and watermark changes since the boundary was defined as the mean of these two expected values. A diagram of this event happening is given in Figure 6.3. If a watermark error occurs because the received signal is pushed beyond the far decision boundary then a symbol error also occurs and noise has totally dominated the signal. This is a case that will not be considered since it has a small effect on the error probability and will needlessly complicate the final expression.

The distance, β, to use in Equation 6.26 to find the watermark error rate is The distance β to use in Equation 6.26 is

$$\beta = \frac{T^2}{8}\left(1 + \cos(2\phi)\right) - \frac{T^2}{4}\cos(2\phi) \tag{6.29}$$

$$\beta = \frac{T^2}{8}\left(1 - \cos(2\phi)\right) \tag{6.30}$$

Using $E_b = T$ from Equation 6.23 and substituting it and Equation ?? in to Equation 6.26, the watermark error rate as a function of $\frac{E_b}{N_0}$ is

$$P_W(\frac{E_b}{N_0}) = \frac{1}{2}e^{-\frac{E_b}{2N_0}(1-\cos 2\phi)} \tag{6.31}$$

6.3 Comparison to Non-Watermarked DBPSK

Bit error rate curves in Figure 6.4 show predicted bit error rates for watermarked DBPSK using watermark angles of $\phi = \frac{\pi}{8}$ and $\phi = \frac{\pi}{16}$ along with non-watermarked DBPSK.

Predicted watermark error rates for DBPSK are shown in Figure 6.5, and are plotted using Equation 6.31. Watermark angles of $\phi = \frac{\pi}{8}$ (dashed line) and $\phi = \frac{\pi}{16}$ (solid line) are shown. Using these plots it is evident that small watermark angles require a very high SNR for usable reception.

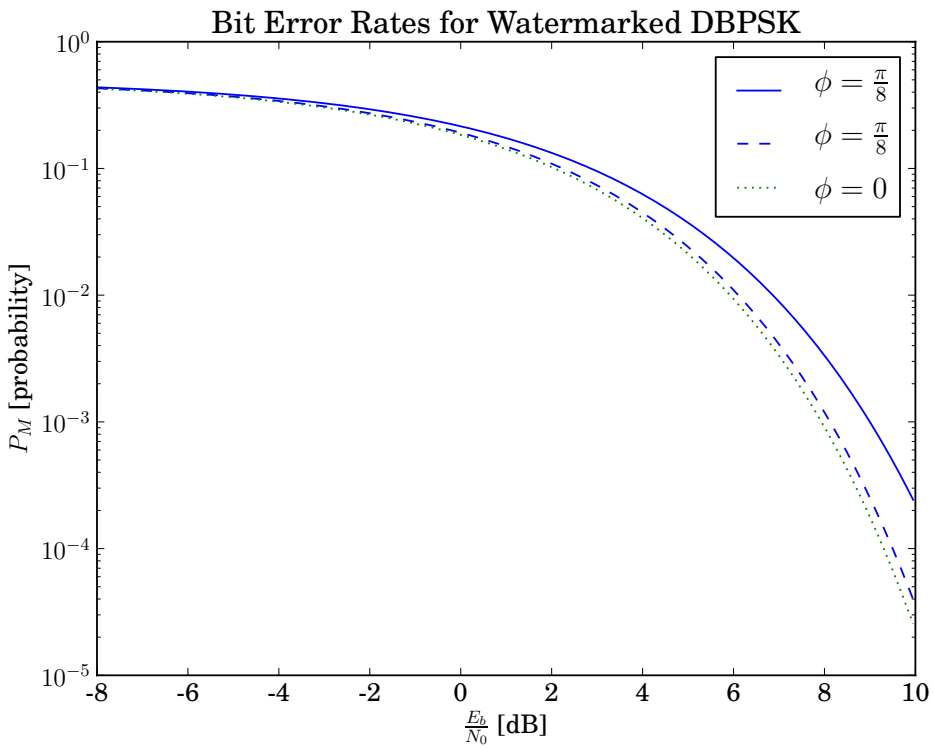

Figure 6.4: DBPSK P_M for different watermark angles.

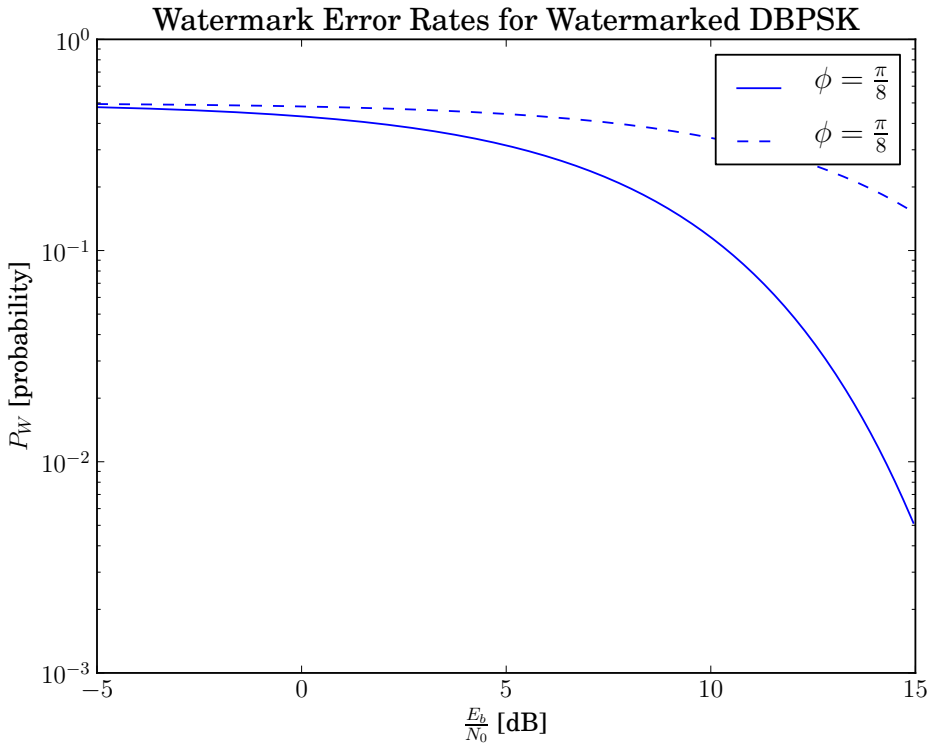

Figure 6.5: DBPSK P_M for different watermark angles.

CHAPTER 7

Conclusion

7.1 Conclusion

Closed form expressions to calculate the probability of bit errors for message and watermark signals with phase-dithered watermarked BPSK, QPSK, 16-QAM, and DBPSK have been presented. For coherent modulations the derived expressions have been verified with computer simulations. Although coherent BPSK results were found by [18], this study independently derived and verifi For BPSK, QPSK, and QAM results have been compared to similar studies.

The probability of bit errors presented enable decision making in authentication and quality of service applications. In authentication applications the phase-dithered watermark presented enables a balance between stealth and probability of authentication. The true probability of authentication would depend on cryptographic parameters such as key size that are outside the scope of this investigation. Other than authentication the watermark could be used as a side-channel with configurable priority based on the watermark angle, enabling quality of service for multiple data streams with overlapping channel usage.

7.2 Future Work

The proposed modulation schemes should be implemented and tested in over the air radios. Work has started on a watermarked BPSK constellation using GNU Radio 3.6, which should be updated to GNU Radio 3.7.

Additionally, this research focused on watermarks that use watermark symbol duration that is an integer multiple of the message symbol. Future work could investigate probability of bit errors for independent watermark and message symbol durations, which could increase stealth.

APPENDIX A

Noise Power Spectral Density

To find the variance of a statistic out of a correlator/matched-filter for BPSK the input signal is purely noise

$$x(t) = n(t) \tag{A.1}$$

The output is

$$l(t) = \int_0^T \cos(w_0 t)\, n(t) dt \tag{A.2}$$

Since the input, $n(t)$, is defined as white Gaussian noise the output is characterised completely by the mean and variance. The mean is set at 0. The variance is

$$\sigma^2 = \mathbf{E}\left[l^2\right] = \mathbf{E}\left[\int_0^T \cos(w_0 t)\, n(t) dt \int_0^T \cos(w_0 \tau)\, n(\tau) d\tau\right] \tag{A.3}$$

The τ symbol is introduced to make clear the independent dummy-variables for integration.

$$\sigma^2 = \mathbf{E}\left[\int_0^T \int_0^T n(t) n(\tau) \cos(w_0 t) \cos(w_0 \tau)\, dt d\tau\right] \tag{A.4}$$

Since integration and expectation are linear operators and $n(\cdot)$ is the only random part of this, it gets rearranged as follows

$$\sigma^2 = \int_0^T \int_0^T \mathbf{E}\left[n(t) n(\tau)\right] \cos(w_0 t) \cos(w_0 \tau)\, dt d\tau \tag{A.5}$$

The expectation here is the auto-correlation of a white Gaussian random variable, which by definition is

$$\mathbf{E}\left[n(t) n(\tau)\right] = \frac{N_0}{2} \delta(t - \tau) \tag{A.6}$$

Substituting this result back in to Equation A.5,

$$\sigma^2 = \frac{N_0}{2} \int_0^T \int_0^T \delta(t - \tau) \cos(w_0 t) \cos(w_0 \tau)\, dt d\tau \tag{A.7}$$

Now we use the sifting property of $\delta(\cdot)$

$$\sigma^2 = \frac{N_0}{2} \int_0^T \cos(w_0 t) \cos(w_0 t)\, dt \tag{A.8}$$

Using a common product-to-sum trigonometric identity and integrating,

$$\sigma^2 = \frac{N_0 T}{4} \tag{A.9}$$

APPENDIX B

BPSK BER Derivation

A BPSK demodulator will receive a signal of the form

$$x(t) = \pm \cos(\omega t) \qquad 0 \leq t < T \tag{B.1}$$

T is the bit time duration, and the $\pm$ comes from a π phase shift denoting the bit. At the receiver this signal gets multiplied by

$$\psi(t) = \cos(\omega t) \qquad 0 \leq t < T \tag{B.2}$$

The product goes in to a matched filter, an integrator giving

$$l(t) = \pm \int_0^T \left[\cos^2(\omega t)\right] dt \tag{B.3}$$

$$l(t) = \pm \int_0^T \frac{1}{2} \left[\cos(0) + \cos(2\omega t)\right] dt \tag{B.4}$$

The double frequency term goes to 0 after integration because the limits of integration, $[0, T]$, cover an integer number of periods. The result is

$$l(t) = \pm \frac{T}{2} \tag{B.5}$$

The result, l, is the mean of a normally distributed random variable with variance derived in Appendix A:

$$\sigma^2 = \frac{N_0 T}{4} \tag{B.6}$$

For convenience the Q-function will be used to express the P_b. The Q-function is the tail probability of a normally distributed random variable, that is the area under the right-hand

tail of a Gaussian curve. To review the definition:

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_0^\infty e^{-\frac{x^2}{2}} dx \tag{B.7}$$

Since the statistic going in to the bit detector of a BPSK demodulator has a non-zero mean and non-singular variance the Q-function has to be normalized. The bit detector will have a decision criteria, referred to as γ. The decision for a bit is made, for example, as

$$\text{bit} = \begin{cases} 1 & l > \gamma \\ 0 & l < \gamma \end{cases} \tag{B.8}$$

The P_b is

$$P_b\left(\frac{E_b}{N_0}\right) = Q\left(\frac{\gamma - l}{\sigma}\right) \tag{B.9}$$

Both symbols are assumed to be equally likely and are equidistant from the origin, so let $\gamma = 0$. Substituting in γ, l, and σ, we get

$$P_b\left(\frac{E_b}{N_0}\right) = Q\left(\frac{0 + \frac{T}{2}}{\sqrt{\frac{N_0 T}{4}}}\right) \tag{B.10}$$

After some algebra this becomes

$$P_b = Q\left(\sqrt{\frac{T}{N_0}}\right) \tag{B.11}$$

At this point knowing the E_b is useful. The energy of the transmitted bit is

$$E_b = \int_0^T \cos^2(\omega t)\, dt \tag{B.12}$$

After algebra,

$$E_b = \frac{T}{2} \tag{B.13}$$

Substituting Equation B.13 in to Equation B.11 results in the well known P_b

$$P_b = Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \tag{B.14}$$

APPENDIX C

QPSK SER Derivation

A QPSK demodulator will receive a signal of the form

$$x(t) = \pm \cos(\omega t + \theta) \qquad 0 \leq t < T \tag{C.1}$$

T is the bit time duration, and θ is the modulated phase shift denoting the transmitted bits. This analysis will use the quadrature demodulator shown in Figure C.1 so that the signal in Equation C.1 gets multiplied by

$$\psi_1(t) = \cos(\omega t) \qquad 0 \leq t < T \tag{C.2a}$$

$$\psi_2(t) = -\sin(\omega t) \qquad 0 \leq t < T \tag{C.2b}$$

The product goes in to a matched filter, an integrator giving

$$l_1(t) = \int_0^T [\cos(\omega t + \theta)\cos(\omega t)]\, dt \tag{C.3a}$$

$$l_2(t) = -\int_0^T [\cos(\omega t + \theta)\sin(\omega t)]\, dt \tag{C.3b}$$

$$l_1(t) = \int_0^T \frac{1}{2}[\cos(\theta) + \cos(2\omega t + \theta)]\, dt \tag{C.4a}$$

$$l_2(t) = \int_0^T \frac{1}{2}[\sin(\theta) - \sin(2\omega t + \theta)]\, dt \tag{C.4b}$$

The double frequency terms go to 0 after integration because the limits of integration, $[0, T]$, cover an integer number of periods. The result is

$$l_1(t) = \frac{T}{2}\cos(\theta) \tag{C.5a}$$

$$l_2(t) = \frac{T}{2}\sin(\theta) \tag{C.5b}$$

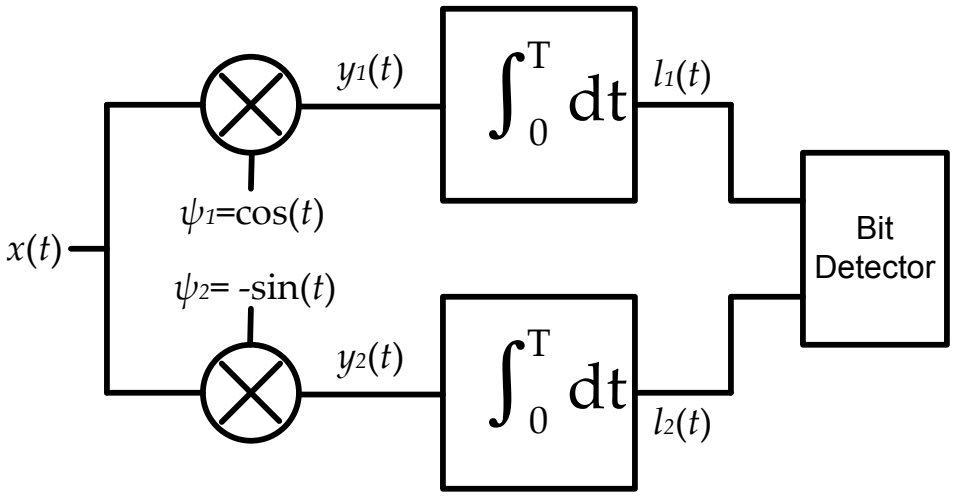

Figure C.1: Quadrature receiver used to demodulate QPSK signals.

The results, l_1 and l_2, are the means of two normally distributed random variables each with variance derived in Appendix A:

$$\sigma^2 = \frac{N_0 T}{4} \tag{C.6}$$

For convenience the Q-function will be used to express the P_S. The Q-function is the tail probability of a normally distributed random variable, that is the area under the right-hand tail of a Gaussian curve. To review the definition:

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_0^\infty e^{-\frac{x^2}{2}} dx \tag{C.7}$$

Since the statistic going in to the bit detector of a QPSK bit detector has a non-zero mean and non-singular variance the Q-function has to be normalized. A symbol decision, and therefore bit decisions, can be made by comparing the I (l_1) and Q (l_2) channels to some threshold set to minimize P_S. The orientation of our constellation means that each quadrant is mapped to a single symbol. Bit decisions can be made by setting γ_1 and γ_2 to

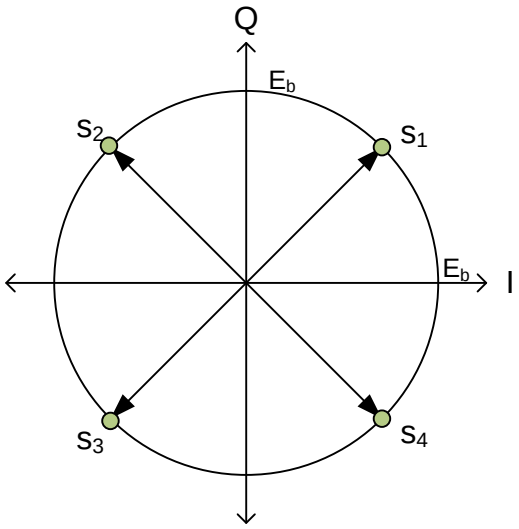

Figure C.2: The chosen QPSK constellation has a single constellation point in each quadrant.

0 and using the criteria in Equation C.8.

$$\text{bit}_1 = \begin{cases} 0 & l_1 > \gamma_1 \\ 1 & l_1 < \gamma_1 \end{cases} \tag{C.8a}$$

$$\text{bit}_2 = \begin{cases} 0 & l_2 > \gamma_2 \\ 1 & l_2 < \gamma_2 \end{cases} \tag{C.8b}$$

Now we will choose a constellation shown in Figure C.2 where each symbol is in a different quadrant. To calculate the P_S we will use the PDFs of l_1 and l_2.

$$f_{l1}\left(\lambda_1\right) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{\left(\lambda_1 - \frac{T}{2}\cos\left(\frac{\pi}{4}\right)\right)^2}{2\sigma^2}\right) \tag{C.9a}$$

$$f_{l2}\left(\lambda_2\right) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{\left(\lambda_2 - \frac{T}{2}\sin\left(\frac{\pi}{4}\right)\right)^2}{2\sigma^2}\right) \tag{C.9b}$$

At this point it is convenient to use symmetry to focus in on a single constellation point. We will choose the constellation point in quadrant 1. Notice for quadrant 1 in Figure C.2 $\theta = \frac{\pi}{4}$. The symbol is an error if the constellation is anywhere outside of the first quadrant; so we will integrate using the limits $[0, \infty]$.

$$P_S\left(\frac{E_S}{N_0}\right) = 1 - \int_0^\infty f_{l1}(\lambda_1)d\lambda_1 \int_0^\infty f_{l2}(\lambda_2)d\lambda_2 \tag{C.10}$$

This can be represented in a Q function as follows.

$$P_S\left(\frac{E_S}{N_0}\right) = 1 - \left[1 - Q\left(\frac{0+\overline{l_1}}{\sigma}\right)\right]\left[1 - Q\left(\frac{0+\overline{l_2}}{\sigma}\right)\right] \tag{C.11}$$

Substituting in the expected decision statistics:

$$P_S\left(\frac{E_S}{N_0}\right) = 1 - \left[1 - Q\left(\frac{\frac{T}{2}\cos\left(\frac{\pi}{4}\right)}{\frac{N_0 T}{4}}\right)\right]\left[1 - Q\left(\frac{\frac{T}{2}\sin\left(\frac{\pi}{4}\right)}{\frac{N_0 T}{4}}\right)\right] \tag{C.12}$$

Notice the switch from θ to $\frac{\pi}{4}$, because this derivation uses the symbol in quadrant 0 that is located at $\frac{\pi}{4}$.

One final substitution for the E_S should be made,

$$E_S = \int_0^T \cos^2(\omega t + \theta) \tag{C.13}$$

$$E_S = \frac{T}{2} \tag{C.14}$$

Now substituting in E_S and simplifying terms we get

$$\begin{aligned} P_S\left(\frac{E_S}{N_0}\right) =& Q\left(\sqrt{\frac{2E_S}{N_0}}\cos\left(\frac{\pi}{4}\right)\right) + Q\left(\sqrt{\frac{2E_S}{N_0}}\sin\left(\frac{\pi}{4}\right)\right) \\ & - Q\left(\sqrt{\frac{2E_S}{N_0}}\cos\left(\frac{\pi}{4}\right)\right) Q\left(\sqrt{\frac{2E_S}{N_0}}\sin\left(\frac{\pi}{4}\right)\right) \end{aligned} \tag{C.15}$$

The previous form of Equation C.15 intentionally leaves the cos and sin terms as they are as a reference for the watermarked QPSK derivation in this text. By simplifying the cos and sin terms and making the approximation that the product term is close to 0 we get the result commonly found in textbooks [16, 22].

$$P_S\left(\frac{E_S}{N_0}\right) = 2Q\left(\sqrt{\frac{E_S}{N_0}}\right) \tag{C.16}$$

This P_S can also be used to approximate the P_b. First, since there are two bits in each symbol the rate assume that each symbol error causes one bit error. This is a close approximation for gray-coded QPSK and gets rid of the 2 term. Next, the $E_S = 2E_b$ substitution is made. This gives the same P_b as BPSK,

$$P_b\left(\frac{E_b}{N_0}\right) = Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \tag{C.17}$$

This is an intuitive approximation for gray-coded QPSK with the chosen constellation considering Equation C.8.

APPENDIX D

QAM SER Derivation

Square 16-QAM uses a quadrature demodulator to make symbol decisions. The constellation is the same as that shown in Figure 5.1. The transmitted signal is

$$r(t) = a(t)\cos(\omega t) + b(t)\sin(\omega t) \tag{D.1}$$

$a(t)$ and $b(t)$ will hereon be replaced with equivalent values of d, the distance between adjacent symbols.

First, we find the energy in each symbol. Symmetry allows us to focus on a single quadrant.

Symbol 10 has symbol energy

$$E_{10} = \int_0^T \frac{d^2}{8}\left(2\cos(0) + \sin(2\omega_c t) - \sin(0)\right) dt \tag{D.2}$$

$$E_{10} = \frac{d^2 T}{4} \tag{D.3}$$

Symbols 11 and 14 have the same energy,

$$E_{11,14} = \int_0^T \left(\frac{3d}{2}\cos(\omega_c t) + \frac{d}{2}\sin(\omega_c t)\right)^2 dt \tag{D.4}$$

$$E_{11,14} = \frac{5d^2 T}{4} \tag{D.5}$$

$$E_{15} = \int_0^T \left(\frac{3d}{2}\cos(\omega_c t) + \frac{3d}{2}\sin(\omega_c t)\right)^2 dt \tag{D.6}$$

$$E_{15} = \frac{9d^2 T}{4} \tag{D.7}$$

The average symbol energy is

$$E_{avg} = \frac{E_{10} + 2E_{11,14} + E_{15}}{4} \tag{D.8}$$

$$E_{avg} = \frac{5d^2T}{4} \tag{D.9}$$

Next, the statistics of the output of the demodulator branches are calculated. The in-phase portion for symbol 10 can be written as

$$l_{10} = \int_0^T \left(\frac{d}{2} \cos(\omega_c t) + \frac{d}{2} \sin(\omega_c t) \right) \cdot \cos(\omega_c t)\, dt \tag{D.10}$$

After trigonometric identities and integration, the output statistic is

$$l_{10} = \frac{dT}{4} \tag{D.11}$$

Symbol 14, which neighbors symbol 10, has a mean in-phase value which can be calculated via

$$l_{14} = \int_0^T \left(\frac{3d}{2} \cos(\omega_c t) \cdot cos(\omega_c t) + \frac{d}{2} \sin(\omega_c t) \cdot cos(\omega_c t) \right) \tag{D.12}$$

Again, it can be shown that this integrates to

$$l_{14} = \frac{3dT}{4} \tag{D.13}$$

The decision boundary is in the middle of these two points, so

$$\gamma = \frac{dT}{2} \tag{D.14}$$

The other decision boundary in the in-phase direction is 0 because it is the mid-point between symbol 10 and symbol 6.

The probability of correct detection of symbol 10 is therefore

$$\int_0^{\frac{dT}{2}} \mathrm{N}\left(\frac{dT}{4}, \frac{N_0 T}{4} \right) \int_0^{\frac{dT}{2}} \mathrm{N}\left(\frac{dT}{4}, \frac{N_0 T}{4} \right) dxdy \tag{D.15}$$

Since the decision boundaries all run parallel to either the in-phase or quadrature axes

they can be represented as Q-functions.

$$\left[1-2Q\left(\frac{\frac{dT}{2}-\frac{dT}{4}}{\sqrt{\frac{N_0T}{4}}}\right)\right]\left[1-2Q\left(\frac{\frac{dT}{2}-\frac{dT}{4}}{\sqrt{\frac{N_0T}{4}}}\right)\right] \tag{D.16}$$

This simplifies to

$$\left[1-2Q\left(\frac{d\sqrt{T}/4}{\sqrt{N_0/4}}\right)\right]\left[1-2Q\left(\frac{d\sqrt{T}/4}{\sqrt{N_0/4}}\right)\right] \tag{D.17}$$

$$\left[1-2Q\left(\sqrt{\frac{d^2T/4}{N_0}}\right)\right]\left[1-2Q\left(\sqrt{\frac{d^2T/4}{N_0}}\right)\right] \tag{D.18}$$

Now substituting in the average symbol energy found earlier,

$$\left[1-2Q\left(\sqrt{\frac{E_{avg}}{5N_0}}\right)\right]\left[1-2Q\left(\sqrt{\frac{E_{avg}}{5N_0}}\right)\right] \tag{D.19}$$

The probability of a symbol error is the probability *outside* of this region. After rearranging terms this is the common formula.

$$P_S\left(\frac{E_{avg}}{N_0}\right)=4Q\left(\sqrt{\frac{E_{avg}}{5N_0}}\right)-4Q\left(\sqrt{\frac{E_{avg}}{5N_0}}\right)^2 \tag{D.20}$$

This is frequently presented in terms of k and M where k is the number of bits and $M=2^k$, or modulation order [11, 22].

BIBLIOGRAPHY

[1] Nikita Borisov, Ian Goldberg, and David Wagner. Intercepting mobile communications: the insecurity of 802.11. In *Proceedings of the 7th annual international conference on Mobile computing and networking*, MobiCom '01, pages 180–189, New York, NY, USA, 2001. ACM.

[2] N. Goergen, T.C. Clancy, and T.R. Newman. Physical layer authentication watermarks through synthetic channel emulation. In *New Frontiers in Dynamic Spectrum, 2010 IEEE Symposium on*, pages 1 –7, april 2010.

[3] Dan Goodin. Android, nokia smartphone security toppled by near field communication hack. *Ars Technica*, July 2012. http://arstechnica.com/security/2012/07/android-nokia-smartphone-hack/.

[4] S. Jain and J.S. Baras. Preventing wormhole attacks using physical layer authentication. In *Wireless Communications and Networking Conference (WCNC), 2012 IEEE*, pages 2712 –2717, april 2012.

[5] Peter Judge. Obsolete wep wi-fi gets new security shield. *Network World*, September 2007. http://www.networkworld.com/news/2007/091907-wep-wi-fi-security-shield.html.

[6] John E Kleider, Steve Gifford, Scott Chuprun, and Bruce Fette. Radio frequency watermarking for ofdm wireless watermarking. In *International Conference on Acoustics, Speech, and Signal Processing*, May 2004.

[7] Shawn Knight. Gsm security vulnerability affects 80 percent of mobile phones worldwide. *Techspot*, December 2011. http://www.techspot.com/news/46810-gsm-security-vulnerability-affects-80-percent-of-mobile-phones-worldwide.html.

[8] Bruce Lebold. Physical layer watermarking of binary phase-shift keyed signals using standard gnu radio blocks. Master's thesis, Oklahoma State University, 2009.

[9] David E Newton. *Encyclopedia of Cryptology*. ABC-CLIO, 1997.

[10] Brian Sadler Paul Yu, John Baras. An implementation of physical layer authentication using software radios. Technical Report ARL-TR-4888, Army Research Laboratory, 2009.

[11] J.G. Proakis. *Digital Communications*. McGraw-Hill series in electrical and computer engineering. McGraw-Hill, 2001.

[12] GNU Radio. Decrypting gsm phone calls. https://srlabs.de/decrypting_gsm/.

[13] GNU Radio. Gnuradio openbts network architecture, 2010. http://gnuradio.org/redmine/projects/gnuradio/wiki/OpenBTSNetwork_Architecture.

[14] Herman Rubin. E-mail Exchange, February 2013.

[15] Adi Sharabani. Wifigate – how mobile carriers expose us to wi-fi attacks. *Skycure Blog*, June 2013. http://www.skycure.com/blog/wifigate-how-mobile-carriers-expose-us-to-wi-fi-attacks/.

[16] Bernard Sklar. *Digital Communications: Fundamentals and Applications*. Prentice Hall, second edition, 2001.

[17] R.H. Spector. *Listening to the enemy: key documents on the role of communications intelligence in the war with Japan*. G - Reference, Information and Interdisciplinary Subjects Series. Scholarly Resources Inc., 1988.

[18] Pavan Kumar Vitthaladevuni and Mohamed-Slim Alouini. Exact ber computation of generalized hierarchical psk constellations. *IEEE Transactions on Communications*, 51(12), December 2003.

[19] H. Wen, P.-H. Ho, C. Qi, and G. Gong. Physical layer assisted authentication for distributed ad hoc wireless sensor networks. *Information Security, IET*, 4(4):390 –396, december 2010.

[20] Liang Xiao, L. Greenstein, N. Mandayam, and W. Trappe. Fingerprints in the ether: Using the physical layer for wireless authentication. In *Communications, 2007. ICC '07. IEEE International Conference on*, pages 4646 –4651, june 2007.

[21] Liang Xiao, Larry J Greenstein, Narayan B Mandayam, and Wade Trappe. Channel-based detection of sybil attacks in wireless networks. *IEEE Transactions on Information Forensics and Security*, 4(3), September 2009.

[22] Fuqin Xiong. *Digital Modulation Techniques, Second Edition (Artech House Telecommunications Library)*. Artech House, Inc., Norwood, MA, USA, 2006.

[23] Paul Yu. *Physical Layer Authentication*. PhD thesis, University of Maryland, 2008.

[24] Paul L Yu, John S Baras, and Brian M Sadler. Physical-layer authentication. *IEEE Transactions on Information Forensics and Security*, 3(1), March 2008.

[25] Paul L Yu, John S Baras, and Brian M Sadler. Physical-layer authentication. *IEEE Transactions on Information Forensics and Security*, 3(1), March 2008.

[26] Paul L Yu and Brian M Sadler. Mimo authentication via deliberate fingerprinting at the physical layer. *IEEE Transactions on Information Forensics and Security*, 6(3), September 2011.

[27] P.L. Yu, J.S. Baras, and B.M. Sadler. Multicarrier authentication at the physical layer. In *IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks*, june 2008.

VITA

Nathan West

Candidate for the Degree of

Master of Science

Thesis: Phased Dithered Watermarking for Physical Layer Authentication

Major Field: Electrical Engineering

Biographical:

Education:

- Oklahoma State University
  - Stillwater, OK
  - Master of Science, May 2014
  - Electrical Engineering
- Oklahoma Christian University
  - Edmond, OK
  - Bachelor of Science, May 2011
  - Electrical Engineering

Experience:

- U.S. Naval Research Laboratory, Mobile Systems Security (2012-Present)
- Oklahoma State University, Signal Processing and Communications Laboratory (2011-Present)
- AT&T Bell Labs, Systems Integration (Summer 2008,2010)
- Oklahoma State University, Radiation Dosimetry Laboratory (Summer 2009)

Professional Memberships:

- GNU Radio: core developer team and working group lead
- IEEE: Signal Processing, Communications, and Computer societies