ANTENNA-DRIVEN METHODS FOR INCREASED WIRELESS NETWORK SECURITY

BY

CARA YANG KATARIA

DISSERTATION

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Electrical and Computer Engineering
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2020

Urbana, Illinois

Doctoral Committee:

Professor Jennifer Bernhard, Chair
Professor Steven Franke
Professor Jonathan Makela
Professor José Schutt-Ainé
Assistant Professor Grace Xingxin Gao, Stanford University

ABSTRACT

Conventional techniques currently used for secure communications are subject to significant vulnerabilities, especially for wireless systems. Unauthorized interceptors have more computation power than ever before to record and potentially decode sensitive information, and there is very little protection against disruptive interference, i.e., jamming. Our research goals are to identify and characterize new methods using antenna design and radiation properties to increase the security of wireless networks.

Two major threats are addressed in this work—jammers and eavesdroppers. The problem space outlined for the first threat is the open broadcast of the Global Positioning System (GPS), and the solution is developed from the view of a receiver seeking a desired signal in the presence of potentially stronger interference. In the second case, we consider any system with a known transmission angle but possible eavesdroppers in other directions. The proposed solution is a novel modulation technique that we call secure antenna polarization modulation, or SAPM. For both cases, we share the theory, design justifications, and simulation results, as well as measurement data from prototypes. Based on the presented ideas, results, and analysis, there is high potential for these solutions in a variety of wireless applications, especially those that are limited in their ability to use traditional methods for security.

To Mama, Baba, Raj, and the 3Blues for their love and support.

ACKNOWLEDGMENTS

I would like to express my gratitude to Professor Jennifer Bernhard for her guidance through this uniquely rewarding process. Her mentorship provided me with technical advice and helpful connections, and I truly appreciate her trust in me. I value the friendship and patience that she has shown me when I so often needed it, and I could always count on the welcoming community that is our research group.

I am lucky to have my co-advisor Professor Grace Gao on my side, as she has always remained dedicated to my success. My heartfelt thanks go to the members of my doctoral committee. Professor Steven Franke has been an incredible source of expertise and a patient reviewer of my seemingly endless paper revisions. I was given my first university teaching job by Professor Jonathan Makela, who has taught me what effective and compassionate management is by example. And I will always be indebted to Professor José Schutt-Ainé, whose kindness and support convinced me to continue my graduate studies.

I would like to thank Professor Jessica Ruyle, John Meier, and the Advanced Radar Research Center at the University of Oklahoma for their generosity in sharing their well-designed analog beamformer, which facilitated this research.

Finally, I am incredibly grateful to have such an understanding family—my mother and father, and my husband Raj. Thank you for your unconditional love, patience, and support while I indulge in my extended vacation from adult life.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

The rapid growth of wireless communication services in recent decades has also led to a sharp increase in cybercrime, with recently reported victim losses totaling over $1 billion in the USA alone [1]. Malicious activity that specifically targets the vulnerabilities of wireless networks can be categorized into two types: denial of service attacks, such as jamming, and passive interception of information, or eavesdropping [2], [3]. These are attacks on the lowest layer of the Open Systems Interconnection (OSI) architecture, the physical layer, which specifies the hardware and signaling interface with the channel [4]. The physical layer for a wireless network has significantly higher security vulnerabilities compared to that of a wired system, where a malicious source must literally be wire-tapped to gain access. Physical layer attacks also constitute a kind of gateway offense in that they may enable other types of malicious activity at the upper protocol layers [5].

For the first category, denial of service attacks, the civilian Global Positioning System (GPS) provides an excellent ecosystem for our investigation. It is an open-access broadcast that is entirely reliant on receivers to implement counter-jamming measures. To combat these types of attacks under the constraints of GPS, we solely focus on a solution for the receiver. For the second category, eavesdropping, we assume design control over the entire end-to-end system to find a viable secure solution using the physical layer. The novel technique that we propose is not necessarily limited to any specific protocol or system. In this chapter, we provide the following:

- Definitions and discussion of the main physical layer security threats to a wireless network
- A summary of current techniques to mitigate these risks
- The problems with existing solutions and the contributions of this work

It is worthwhile to note that many other well-known types of cyberattacks, such as IP hijacking, masquerading, and general malware, actually target the upper layers of the OSI model and are just as easily unleashed on wired systems [3]. As such, they do not necessarily take advantage of the open nature of the wireless channel and will not be in the scope of this work.

1.1 Threats to wireless network security

In this section, we define the two categories of attacks that are the focus of this investigation: denial of service and eavesdropping. To narrow down the scope of the discussion, we will only concern ourselves with jamming as a representative of the first type of attack. Jamming is defined as the intentional transmission of interference to eliminate or disrupt a network's communications [2]. A typical jammer is a strong signal at the carrier frequency for some protocol, but one that does not carry any useful information. Its goal would be to "flood" every receiver within its range such that those nodes could not discern the true signal. More sophisticated jamming attacks may broadcast false data; usually this is referred to as spoofing. Section 1.2 includes several examples of jamming cases for civilian GPS and discusses the risks posed by an extended outage.

Eavesdropping, on the other hand, is a passive attack that could potentially lead to longer-term damage. When unauthorized users receive a signal intended for other parties, they are acting as eavesdroppers. It is intuitive that the larger the coverage area for a given transmission, the more susceptible it is to data interception [3]. Even if the unintended receiver does not decode the message, it may still analyze network traffic patterns to potentially launch another type of attack [5]. Data encryption, which is implemented at the upper OSI layers, is the most widespread existing form of protection against eavesdroppers. It has a number of flaws that newer security techniques involving the physical layer seek to address, which is discussed in Section 1.3.

1.2 Mitigation strategies for GPS jammers

It is no secret that GPS signals are highly vulnerable to interference in the form of jamming, in part due to their low power levels [6]. Interruptions in GPS service can have serious repercussions worldwide [7]–[9]. In a 2012 report, the Department of Homeland Security assessed this risk for the communications, emergency services, energy, and transportation sectors [7]. Among other things, it noted that advanced jamming attacks could compromise operations for the power grid, threaten mass transit safety and tracking, and cause cell service outages. The authors of [8] examine the characteristics and effects of interfering signals from "personal privacy devices" (PPDs) on the operation of Newark Airport's Ground Based Augmentation System (GBAS), which aids aircraft landings by providing highly accurate positioning via differential correction messages for GPS signals [10]. They find that interference can be detected intermittently from the nearby highway, and at certain surges of interfering signals, GBAS operations at Newark could be disrupted. In particular, a trucker with a PPD was able to interrupt GBAS testing on multiple occasions [9]. Since then, other airports besides Newark have adopted GPS-assisted aircraft landing systems including Houston's George Bush Intercontinental Airport, Charleston International Airport, and other locations worldwide, marking an increasing reliance on GPS [10]. As transportation and other services that are integral to our daily lives become more dependent on GPS for position, navigation, and timing, an outage has the potential to be catastrophic.

This investigation will be limited to the civilian GPS signals—the coarse acquisition (C/A) codes at the L1 (1.57542 GHz) band and potentially the L2C codes (1.2276 GHz) [6]. As noted, the responsibility of jamming risk mitigation falls on the receiver since any new GPS satellite launches would be both expensive and risky. Most proposed solutions necessitate the use of digital beamforming networks (BFNs) with antenna arrays, sometimes called controlled reception pattern antennas [11], [12]. Unfortunately, these are difficult to implement on cost-sensitive platforms due to an expensive set of frontend electronics—typically low-noise amplifiers, mixers, oscillators, and filters precede an analog-to-digital converter (ADC) for each antenna in the array [13].

1.2.1 Direction finding and its potential to aid GPS

One specific use of any array is to estimate an incoming signal's direction of arrival (DOA), which can provide validation for a satellite transmission in the presence of interference because the expected angle of arrival can be calculated using the GPS almanac broadcast [6]. Non-GPS signals (from jammers or otherwise) would be unlikely to reach receivers from a particular satellite's direction; in fact, true GPS signals mainly come from the sky, while interference is generally earth-bound.

The motivation for this investigation stems from the desire to build a low-cost, space-efficient solution for GPS that can still offer DOA functionality as a jamming deterrent. Work on direction finding by past authors often involves some variant of the multiple signal classification algorithm, or MUSIC, originally derived for arrays and later modified for single antennas [14], [15]. Unfortunately, the "single" antenna elements themselves, such as the ESPAR [15] and the leaky-wave antenna [16], are larger because they rely on a set of undriven dummy elements. The time-domain processing detailed in [15] requires that the incoming signal be sampled at a multiple of its own frequency, so sources of unknown frequency or with Doppler shifts cannot be identified—a critical problem for GPS. If time-averaging of received power is used without coherence, as in [16], multiple sources from different directions cannot be resolved reliably, especially if they vary slightly in frequency and amplitude. The planar four-arm spiral antenna used in [17] has the ability to avoid this problem and is physically smaller, but it requires four RF inputs for operation. It is consequently just as expensive as a four-element array, as it needs the same front-end electronics.

1.2.2 Our contributions to counter GPS jamming

The review of current technology has revealed that today's systems still suffer limitations from space and cost concerns, and within the realm of single-antenna DOA solutions, there is a lack of treatment for multiple sources. For GPS receivers that are severely constrained in size and/or budget, viable solutions need to better utilize the additional degrees of freedom that may be designed into their hardware. To address this need, we propose a hemispherical spiral ("hemispiral") antenna for GPS capable of direction finding [18].

The original contributions of this work include the design and measurement of the hemispiral, which is smaller than its one- or two-port predecessors and requires significantly fewer electronic components than arrays. In addition, we prescribe a methodology using this antenna to find the direction of more than one incoming source at shifted frequencies.

1.3 Risk management in the presence of eavesdroppers

When there is design control over both the transmitters and the receivers of a wireless network, much more involved security techniques may be employed. In general, protection against the threat of eavesdroppers requires some degree of design at the transmitter. Today, the most widespread solution for sensitive wireless transmissions uses cryptography to encrypt the content with a key known to authorized parties. This is done at one or more of the upper protocol layers and traditionally does not involve the physical layer [5]. Unfortunately, conventional encryption methods are still subject to significant vulnerabilities from interceptors that have enough computation power [19]. More importantly, there is considerable processing headroom needed for encryption and a separate secret channel must be created for sharing the key. These demands are at odds with the cost and latency requirements of many wireless networks, especially in the growing market of cheap, low-power Internet of Things (IoT) devices [20].

Many researchers have thus turned to physical layer security, a family of techniques implemented directly at the lowest interconnection layer [3]. These include directional modulation (DM), artificial noise injection, and security-oriented beamforming [21], [22]. DM and artificial noise-aided solutions produce scrambled symbol constellations in most spatial directions relative to the transmitter, except in those of intended receivers, while BFNs concentrate as much power as possible toward intended receivers. Unfortunately for beamformers, if eavesdroppers have high sensitivity or enough information to implement processing gains, the transmission may still be demodulated correctly, especially from radiation sidelobes [23]. Artificial noise techniques bypass this issue by intentionally transmitting incorrect data to these angles, but they are computationally expensive. Additionally, they flood their environments (usually in all directions) with useless signals that can jam other communications and alert potentially unfriendly parties to transmitter locations [21]. DM, which could be considered a subset of this category, requires significantly less processing overhead but loses the ability to boost power in desired directions like BFNs, an efficiency hit that is often unacceptable [22].

1.3.1 Heightened security using wave polarization

Applying physical layer security concepts to an entirely different modulation method can help address many of these concerns. Our investigation is related to polarization-shift keying (PolSK) or polarization modulation (PM), where the state of polarization (SOP) is treated as the information-bearing parameter [24], [25]. Current polarization-related applications to security are very limited, but the inherently directional nature of a wave's SOP may increase secrecy with selective spatial distortion [26], [27]. The authors of [28] recognize this but do not exploit it fully, instead opting for a secret phase key that must be shared with receivers in a separate channel. The system proposed in [29] has purported reception in two directions, but in reality, information is shared over a range of transmission angles. More importantly, the spatial distortion is deterministic and potentially predictable [27]. This is also true of the solution in [30], which is strictly a PolSK system rather than one based on directional modulation as indicated. An adaptation known as polarization hopping is presented in [31], in which codes are transmitted in conventional schemes (QAM, PSK, etc.) with a secret pattern over two polarizations. While this provides one more proverbial hoop for an eavesdropper to jump through, the polarization mapping key still has to be provided to legitimate receivers in some form of authentication process. For interceptors with dual-polarized antennas, this is simply one more bit to decrypt.

1.3.2 Our contributions to counter eavesdropping

To date, the polarization-based methods proposed for improving security have had a propensity toward unnecessary complication or oversimplification, both of which can be traced back to the lack of a thorough and correct treatment for the system antennas. Wave polarization and how it varies over transmitter look angle is directly linked to the inherent physical structure of the antenna and its feed. We strive to further the knowledge in this area with the analysis presented in the investigation.

Based upon this analysis, we propose a novel technique for protecting sensitive wireless communication: secure antenna polarization modulation, or SAPM [32]. As with PolSK, dual-polarized antennas are used to transmit data, but SAPM spatial distortion is created with an element of randomness at all transmission angles except the intended ones. This is similar to DM; however, SAPM-based beamforming and beamsteering may be used to boost gain. SAPM also has the potential to be more robust than DM in multipath because there is no reliance on wave coherence between array elements for demodulation. Unlike artificial noise injection and the method from [28], a computationally heavy algorithm is not required and no secret keys need to be shared. As with most physical layer security and conventional beamforming systems, standard ways to find intended receivers must be employed [33]. To establish the proof-of-concept for SAPM, we derive expected performance using one intended receiver and line-of-sight (LOS) propagation in additive white Gaussian noise (AWGN) channels. We then simulate and measure a prototype to validate our theoretical framework for SAPM.

1.4 Dissertation outline

In this work, we present solutions to combat two major types of threats that plague the security of wireless networks: jammers and eavesdroppers. Our techniques improve upon prior methods as discussed in Sections 1.2.2 and 1.3.2. The organization of the dissertation is as follows:

Chapter 2 describes the design approach to optimize a receiving antenna for GPS and provides an overview of the DOA algorithm, along with simulation results. Measurement results and performance analysis in various configurations are presented in Chapter 3. We test direction finding at L1, where the most widely used civilian GPS signals reside, but the design and measurements encompass the L2C and L5 (1.17645 GHz) bands.

The chapters thereafter are focused on SAPM. Chapter 4 describes its theory of operation and includes performance characterization based on full-wave simulations. The design approaches for the ideal antennas for SAPM and other polarization-based methods are discussed in Chapter 5. An SAPM prototype to prove the concept is evaluated in Chapter 6. Chapter 7 concludes the work with several potential directions for further investigation.

CHAPTER 2

HEMISPIRAL ANTENNA DESIGN AND DIRECTION FINDING METHODOLOGY

In this chapter, we describe our approach and design justifications for the hemispiral, a miniaturized single RF-feed antenna for GPS. In addition to optimizing the geometry for general-purpose GPS reception, we must consider design requirements for the specialized DOA method to identify and protect applications from jammers.

For the purposes of DOA, the most critical requirement for the antenna is the ability to provide enough sufficiently different radiation patterns. We choose a modified two-arm Archimedean spiral antenna with this in mind, as it will support distinct patterns based on the phasing of its arms. When operated in the usual way, the arms are fed 180° out of phase and a broad circularly polarized (CP) pattern is produced, which we will refer to as the differential pattern. Feeding an in-phase signal on the arms produces a deep broadside null, which will be called the common-mode pattern. Adjusting the phase from 0° in either direction steers the null and effectively changes the pattern.

Section 2.1 details the justifications for the most distinct part of the antenna, its shape, and the design tradeoffs made to receive signals efficiently in all operation modes. The model geometry and gain simulation results are shown in Section 2.2. Section 2.3 provides an overview of the algorithm for direction finding that leverages the hemispiral design, and Section 2.4 shares DOA simulation results. The reference frequency is L1 unless otherwise noted, but the spiral is sized for L5 as its lowest design frequency.

2.1 Antenna design for GPS reception

GPS satellites occupy six orbital planes at a 55° incline from the Equator, with a baseline of 24 or more active units at any given time [6]. A receiver with a good view of the sky would ideally see six to eight satellites (at minimum, four) at any given time. The receiving antenna should, therefore, offer good performance over as large a field of view (FOV) as possible in its upper hemisphere. The GPS signal is right-hand circularly polarized (RHCP) and the expected power levels received by a matched theoretical isotropic antenna on earth range from -154.9 dBW (civil, L5) to -164.5 dBW (military, L2), with a few dB variation depending on satellite elevation [6]. With such a weak signal of interest, it is critical for the antenna to have sufficient gain and be well-matched in both impedance and polarization. The latter can be quantified for a circularly polarized antenna by its axial ratio (AR). We address the work done to optimize the hemispiral for AR performance in Section 2.1.1.

Civil GPS signals occupy about 2 MHz centered at both L1 and L2, and about 20 MHz at L5 [6]. A well-designed general-purpose GPS antenna should have acceptable performance across the entire frequency range at each band. Since we operate the antenna in numerous modes based on the phasing between its arms, it is crucial to ensure an acceptable impedance match across these modes as well as over the frequencies of interest. Analysis regarding this aspect of the design is shared in Section 2.1.2.

2.1.1 Dome profile

The outer shape of the design is a dome that is nearly a hemisphere, hence the name of this antenna. While this design could be implemented with a planar spiral, and arrays of flat spirals have certainly been proposed for DOA [34], we assert that a larger field of view may be achieved with the dome. Under normal circumstances (no jammers), a GPS antenna ideally offers good RHCP reception from all directions above the horizon. To that end, we aimed to use the available solution volume more efficiently, with the expectation that the increased gain of the forward radiation would improve the AR across a larger range of look angles and increase our FOV. The link between antenna equivalent volume and gain (and bandwidth) has long been observed and characterized [35]. The idea of conforming a spiral to a hemisphere is not necessarily unique, but publications with prototypes and documented measurements are rare [36]. Conforming the spiral to a cone,

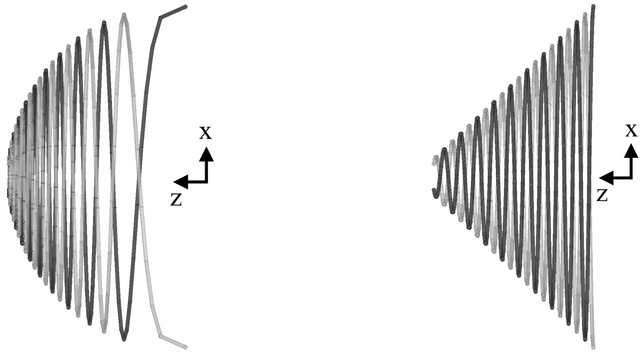


Figure 2.1: Dome (left) and cone (right) profiles used for conformal geometry studies; broadside at $\vartheta = 0°$

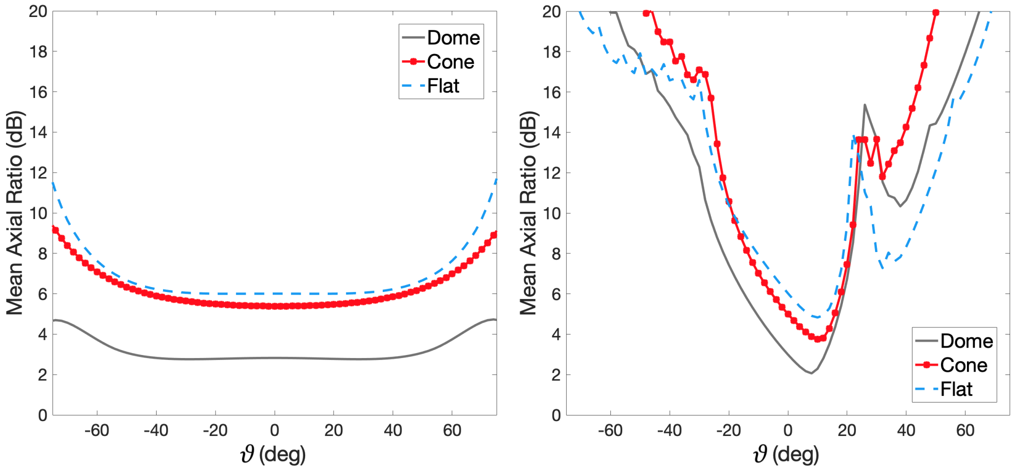
however, is a known method for reducing the planar spiral's back lobe [37], so this was used as a point of comparison.

To substantiate our hypothesis, three Archimedean spirals were simulated in Ansys HFSS with all geometries identical except the profile [38]. One was flat, serving as a reference. Side views of the other two, a cone and a dome, are shown in Figure 2.1. All three have a maximum z-dimension of 0.25λ, with an infinite ground plane at that distance. Figure 2.2 shows the resulting AR for two different modes versus angle off the z-axis (ϑ), averaged across all azimuthal cut-planes in φ. For the differential pattern, Figure 2.2a, used in normal operation, the dome shape provides significantly lower mean AR over elevation. This delta decreases and overall AR increases as we approach the common-mode pattern, where AR is roughly the same for all three profiles. Figure 2.2b shows an in-between mode with an obvious null. To a receiver, this results in decreasing RHCP power as input phasing approaches 0°.

2.1.2 Matching network

Given the observed AR increase over certain pattern modes, it is critical to minimize other losses. The discussion in this section addresses the two-wire matching section and its role in balancing performance across these modes.

The hemispiral is implemented with controlled distance to a ground plane slightly larger than its own outer diameter, which could represent the side of any platform that it would be mounted to for operation. Ordinarily, for the differential-mode pattern, this plane should be at a distance of 0.25λ to align the phase of the reflected back lobe [23]. In this state, the hemispiral's low



(a)

(b)

Figure 2.2: Axial ratio averaged over azimuth, φ, versus angle from the z-axis, ϑ, with (a) 180° and (b) 45° input phase

input reactance allows the use of a simple two-wire quarter-wave transformer from the outputs of a matched rat-race coupler behind the ground plane, leading to a single RF port on the receiver [39]. We may calculate the differential impedance Z_{diff} from the odd-mode characteristic impedance Z_d, which are described by the network's z-parameters in Equation (2.1) [40].

$$\begin{aligned} Z_{diff} &= 2Z_d \\ &= 2\big(z_{11} - z_{21}\big) \quad \text{for symmetric systems} \end{aligned} \tag{2.1}$$

However, as we deviate from 180° to generate the other patterns, the two-wire segment is no longer a transmission line due to the increasing common-mode components. At the extreme of zero phase, the same signal is seen on each arm of the two-wire *plus* the hemispiral. The common-mode impedance Z_{cm} may be calculated from the even-mode characteristic impedance, Z_e, described by the z-parameters in Equation (2.2) [40].

$$\begin{aligned} Z_{cm} &= \frac{1}{2} Z_e \\ &= \frac{1}{2}\big(z_{11} + z_{21}\big) \quad \text{for symmetric systems} \end{aligned} \tag{2.2}$$

The separate impedances seen by the differential and common-mode signal components vary with the antenna's distance to ground and, equivalently,

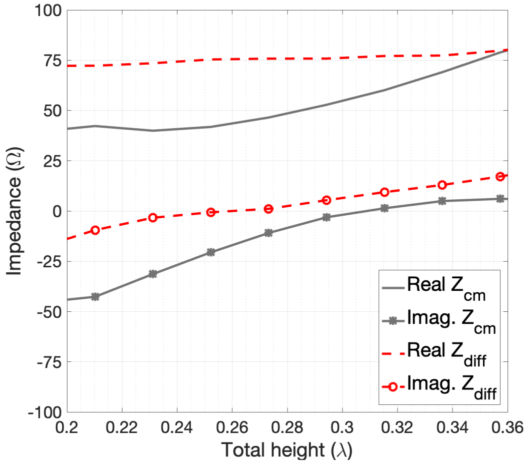


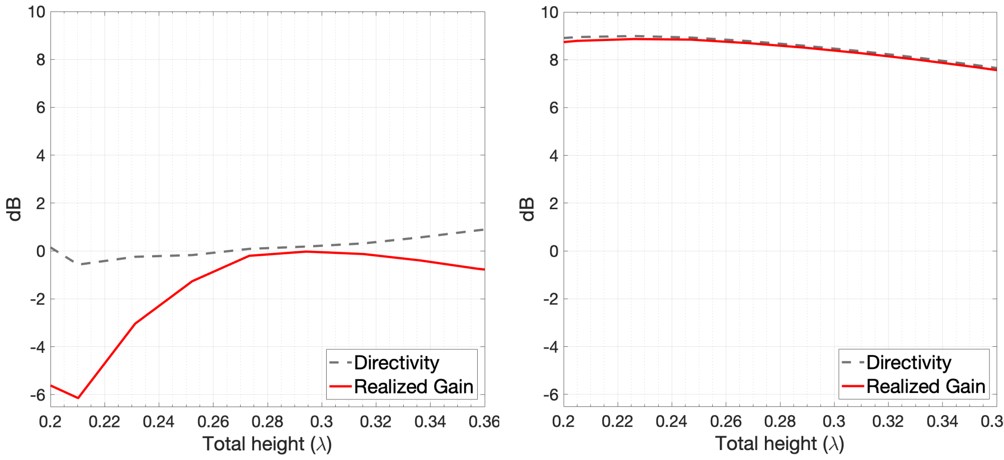
Figure 2.3: Common- and differential-mode impedance versus height (ground distance) for the modified dome model

the two-wire length. Figure 2.3 shows the real and imaginary parts of the common- (Z_{cm}) and differential-mode (Z_{diff}) impedances as this distance is increased, calculated from z-parameters generated in HFSS. The simulation model has an outer dome shape slightly modified from Figure 2.1. Evidently, for common-mode excitation, the two-wire length that yields the lowest mismatch loss is about 0.3λ, while the differential case is best matched at the usual quarter wavelength.

The maximum directivity and realized gain in the upper hemisphere are plotted over ground distance for the common-mode pattern in Figure 2.4a, where there is a peak in realized gain around the same 0.3λ mark. This is consistent as the input phase is increased up to about 60°. Beyond that, the differential components of the current begin to take over until the system again presents as a spiral load with a two-wire transmission line, Figure 2.4b. The chosen z-height of 0.28λ represents a trade-off favoring common-mode, optimized at L1. Mismatch losses at L2/L5 were accounted for through simulation and verified with measurements in Section 3.1.

2.2 Model geometry and radiation patterns

Figure 2.5 shows the final model for the hemispiral, with relevant dimensions annotated or given in the caption. It is a design compromise between the differential and common-mode patterns that yields good performance through



(a) (b)

Figure 2.4: Maximum RHCP directivity/realized gain over (ϑ, φ) versus z-height for the (a) common-mode and (b) differential patterns

all in-between modes. The antenna's largest extent, its diameter, is 0.34λ at the lowest design frequency L5, comparatively smaller than those of the leaky-wave antennas used in [16] (1λ+), and the 0.5λ-diameter ESPAR used in [15].

Reference equations for the Archimedean spiral may be found in [23]. The dome curvature is given by the following parametric equation, which also defines the distance in z between the arms:

$$z(\varphi) = h \cos^p\left(\frac{\varphi}{\varphi_0}\right) \tag{2.3}$$

$$\text{where } h = 48 \text{ mm}, \ \varphi_0 = 11\pi \text{ rad}, \ p = 0.5$$

Decreasing the height h of the curvature generally worsens AR, while increasing it adds z-height and impacts the impedance discussed earlier. The exponent p defines the rate of curvature, with larger p resulting in more concavity at the edge. The p that produces the lowest mean AR over look angle changes with input phase. The variable φ_0 determines the number of turns and the outer radius of the spiral. These variables were assessed using analysis similar to Sections 2.1.1 and 2.1.2, and the values shown here are based on performance and size trade-offs over pattern modes.

The polar plots in Figure 2.6 show simulated 3D power patterns over the upper hemisphere for two modes. Since there are two arms, the null may

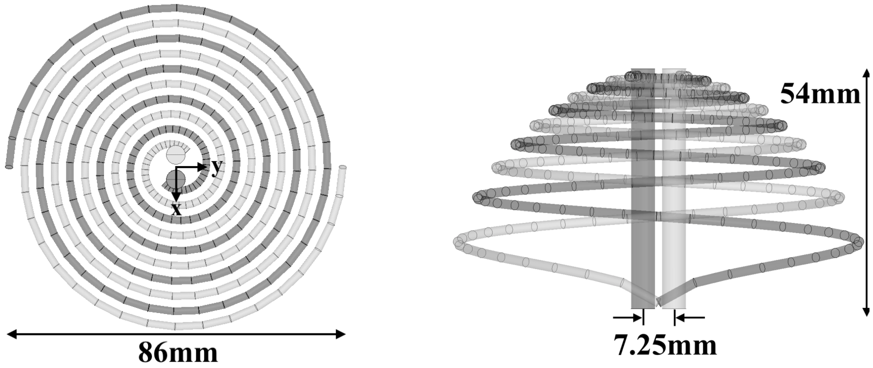


Figure 2.5: Top and side views of the ideal hemispiral geometry; two-wire feed radius = 2.5 mm, spiral wire radius = 1 mm

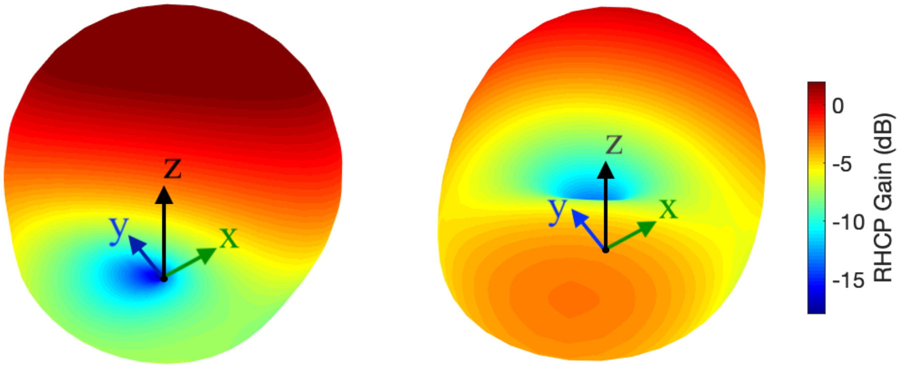


Figure 2.6: Power patterns (dB) over the upper hemisphere with input phase of 60° (left) and 10° (right)

not be arbitrarily steered to any angle; however, changing the input phase results in a set of distinct patterns in each azimuthal cut-plane, making it possible to estimate DOA. We describe our modified MUSIC DOA algorithm in Section 2.3.

2.3 Overview of the DOA algorithm

Chosen for its high target resolution and tolerance to array geometry, MUSIC is a well-known subspace approach that employs eigendecomposition to separate the received data into signal and noise subspaces [14]. An array with L elements provides a set of directional mode vectors $\vec{a}$, which are simply the array's response to N valid look angles ϑ_n in the solution space. The mode vectors form the columns of a manifold $\mathbf{A}$ and define an L-dimensional space for the signal vectors, shown in (2.4) for 2D [14].

$$\begin{aligned}\mathbf{A} &= \begin{bmatrix}\vec{a}(\vartheta_1) & \dots & \vec{a}(\vartheta_N)\end{bmatrix} \\ &= \begin{bmatrix} a_1(\vartheta_1) & a_1(\vartheta_2) & \dots & a_1(\vartheta_N) \\ a_2(\vartheta_1) & a_2(\vartheta_2) & \dots & a_2(\vartheta_N) \\ \vdots & \vdots & \ddots & \vdots \\ a_L(\vartheta_1) & a_L(\vartheta_2) & \dots & a_L(\vartheta_N) \end{bmatrix}\end{aligned} \tag{2.4}$$

Although this algorithm was developed to be used with arrays, it has been adapted to work with single pattern-reconfigurable antennas by substituting the mode vectors (columns) with distinct radiation patterns over look angle (rows) [15], [16]. A more thorough discussion of our implementation of modified MUSIC is included in [41], but in this section we will review the original contributions of this work, i.e., specific changes that allow multiple source identification in the presence of Doppler.

Because single-input MUSIC is modified to compose a received vector over time, to guarantee coherence it must sample at the exact same point of the incoming waveform for each pattern, which can only be done in real time if sampling is at a multiple of the *lowest* source frequency [15]. For moving sources (or receivers) with changing Doppler shifts, this is impossible because Doppler is determined in the digital domain (after sampling). Noncoherent processing may be used in this case, where received power is time-averaged in each pattern mode, but if more than one source is present the results will be incorrect. To our knowledge, this is not addressed in the open literature for modified MUSIC. Conventional MUSIC for arrays does not have this limitation as long as each input is synchronously received.

The solution we propose is a phase alignment in post-processing, which can be done with an accurate understanding of the multi-source received signal's characteristics. For clarity, we illustrate with two waveforms in Equation

(2.5), but generalization to more sources is straightforward.

$$\begin{aligned}
R_l(t) =& B_l(\vartheta,\varphi)\cos\left(\omega_b(t-t_l)+\delta\right) \\
&+ C_l(\vartheta,\varphi)\cos\left(\omega_c(t-t_l)\right) \\
=& D_l\left[\cos\frac{(\omega_c+\omega_b)t-(\omega_c+\omega_b)t_l+\delta}{2}\right. \\
&\left.\times\cos\frac{(\omega_c-\omega_b)t-(\omega_c-\omega_b)t_l-\delta}{2}\right] \\
&+ F_l\left[\sin\frac{(\omega_c+\omega_b)t-(\omega_c+\omega_b)t_l+\delta}{2}\right. \\
&\left.\times\sin\frac{(\omega_c-\omega_b)t-(\omega_c-\omega_b)t_l-\delta}{2}\right] \qquad (2.5) \\
&\text{where } D_l = B_l(\vartheta,\varphi)+C_l(\vartheta,\varphi) \\
&\qquad\quad F_l = B_l(\vartheta,\varphi)-C_l(\vartheta,\varphi)
\end{aligned}$$

If the incoming waves have arbitrary radian frequencies ω_c and ω_b, constant amplitudes B_l and C_l, and a relative constant phase δ, we can represent the total received signal R_l in the time domain as (2.5) for the l^{th} sampling period. We may assume that $\omega_c > \omega_b$ and $B_l > C_l$ without any loss of generality. B_l and C_l are functions of their location and the delay term t_l can be referenced to any sampling period, as long as it is consistent. The term with amplitude D_l and only cosine terms includes a spectral component at the average of ω_c and ω_b multiplied by another component at half the difference of the frequencies. This is simply a lower frequency envelope modulated on a carrier, a basic AM waveform. The second sine-only term is the same waveform in quadrature that serves to adjust the modulation depth.

When $\omega_c - \omega_b$ is small, the delay term manifests as a larger phase offset in the carrier than the envelope. This would be a realistic scenario for most satellite communications, as carrier frequencies are generally fixed, channels are relatively narrow-band, and the range for expected Doppler shift is very small compared to the carrier. We align the envelopes first by taking the magnitude of $R(t)$ and its quadrature component, which is periodic at the envelope frequency. Each local peak may be detected and used as the starting point for aligning the carrier peaks. Conveniently, t_l may also represent

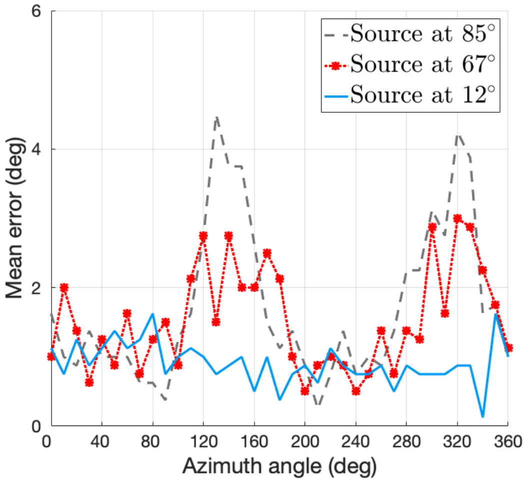


Figure 2.7: DOA error versus φ for 3 source angles in ϑ, averaged over SNR = 3 dB to 20 dB; 4 patterns with input phases = $[180°, 60°, 10°, -30°]$

the effect of dropped samples, which relaxes any timing synchronization requirements between the data capture and the pattern-switching mechanism.

This simple step is not addressed in previous authors' modifications of MUSIC to accommodate a single RF input instead of a vector from an array. It is critical, however, when adapting the method to a multi-source system, especially when transmitters and/or receivers are not necessarily stationary. In the absence of a highly tunable front end and pre-existing knowledge of the present frequencies, this method may act as a substitute for receiving data in each mode simultaneously.

2.4 Direction finding simulation results

Using the hemispiral design described in Section 2.2 to create four different patterns for use in the algorithm, we show simulation results in Figure 2.7 for 2D direction finding in ϑ for each φ-plane. Going forward, we define DOA error as the absolute difference between the true source angle and the MUSIC spectrum peak. White Gaussian noise is added to the incoming signal, and results are averaged over a broad SNR range that depends on receiver implementation [6]. We include a source near the horizon ($\vartheta = 85°$) to show the expected degradation in performance, which generally begins with SNR levels below 15 dB in our configuration.

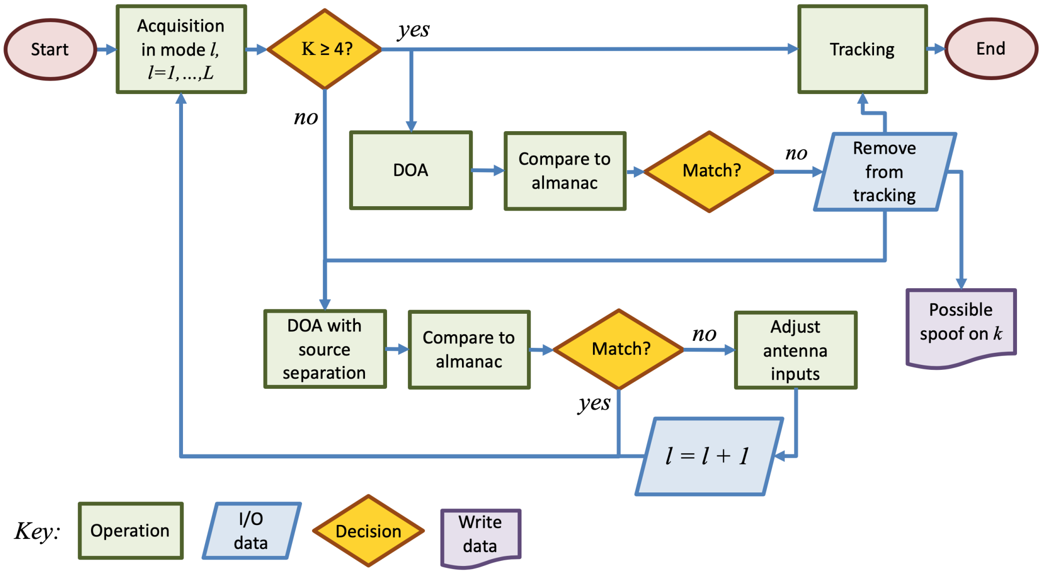


Figure 2.8: Potential DOA integration strategy for a GPS receiver; K total acquired satellite signals may be processed in parallel with GPS tracking

2.5 GPS receiver integration

Once an angle of arrival is estimated for a source, receivers may compare the result against the expected direction from the GPS almanac broadcast or the more accurate ephemeris data [6]. This would allow the identification of more sophisticated spoofed signals, where the data resembles a civilian GPS transmission (Gold codes, etc.). If there is only strong interference close to the carrier frequency, which is more typical of jamming scenarios, the hemispiral may potentially be adjusted to point a null at that source. Acquisition and tracking would proceed using this new pattern. Figure 2.8 shows a flowchart representing a possible receiver integration strategy.

During acquisition, a receiver finds the coarse estimate of each available satellite's Doppler frequency and code delay, usually via correlation with replicas on parallel channels. It then enters tracking operation, where finer estimates are found via one or more tracking loops, depending on the implementation [6]. This should initially be done with the preferred broad RHCP pattern without nulls ($l = 1$ in the flowchart, 180° phase on the feed).

We assume the receiver requires a minimum of $K = 4$ visible satellites to enter tracking. If this is the case, each of $k = 1, \ldots, K$ channels also enter DOA estimation, as described in Section 2.3. In this phase, the algorithm may use as few as three patterns depending on the expected or measured noise in the environment. The resulting angles of arrival are then compared to the expected angles calculated from the almanac (or ephemeris) for each k. If any of these fall outside a predetermined threshold of error, the channel is removed from tracking operations. These angles represent potentially spoofed signals because they passed the acquisition phase.

If the receiver acquires too few or no satellites, a more computationally heavy version of direction finding is used ("DOA with source separation"). Based on the large number of GPS satellites available today, we make the assumption that there is either significant physical blockage or interference. DOA is now done with several different sets of increasing numbers of patterns until an acceptable confidence level is reached in the estimates. The specific thresholds for confidence depend on the application, but several factors impacting estimation accuracy are discussed in Section 3.2. Again, the results are compared to the expected angles of arrival, and if they match, it simply means too few satellites are visible. If one or more of them do not match, the hemispiral inputs are adjusted to point a null in the direction output from the DOA algorithm. Using this pattern, acquisition is redone, and this step would be iterated over all the "no match" directions until either $K > 4$ satellites are acquired or all the null patterns/"no match" directions are exhausted.

2.6 Summary

In this chapter, we describe the design approach for the hemispiral antenna, particularly focusing on justifications for its peculiar shape and z-height. The initial spiral geometry was chosen based on a requirement for multiple radiation patterns from our DOA method. This direction finding algorithm is also detailed here, consisting of a modified version of MUSIC to support multiple sources from a single RF input. We share full-wave simulation results for the gain patterns and DOA performance in an additive white Gaussian noise (AWGN) channel.

CHAPTER 3

CHARACTERIZATION AND ANALYSIS OF A HEMISPIRAL PROTOTYPE

An early hemispiral proof-of-concept was made by hand and introduced in [42]. The current prototype, shown in Figure 3.1, is printed in copper C18150 by Stratasys Direct, Inc. It avoids the previous dielectric structure and enjoys higher realized gain, especially on patterns with input phasing away from 180°. Several fabrication flaws include uneven gaps between the two spiral arms (requiring suboptimal two-wire spacing to avoid shorts), a reduced outer radius, and a distorted outer profile. These all impact the resulting radiation in various ways, most notably reducing the realized gain by up to 1-2 dB depending on input phase and introducing pattern asymmetry, but updates were made to the simulation model to reflect the imperfections where possible. The results from this prototype are discussed in Sections 3.1 and 3.2.

3.1 Measurements

Figure 3.2 is a simplified block diagram of the general data collection setup for DOA estimation, though some measurements discussed in this section

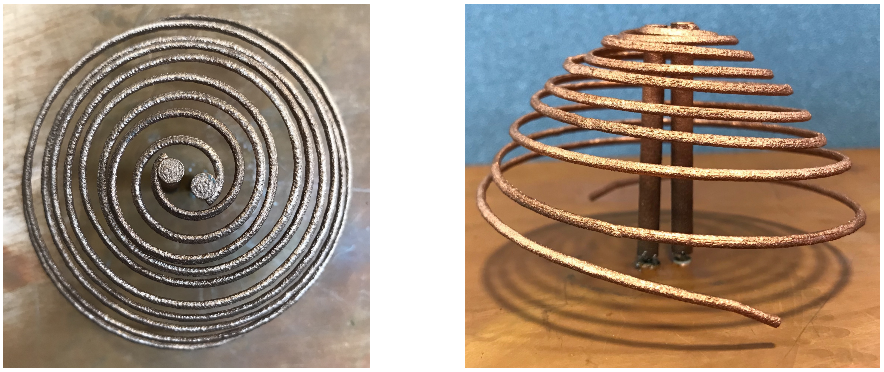


Figure 3.1: Hemispiral prototype with matching section

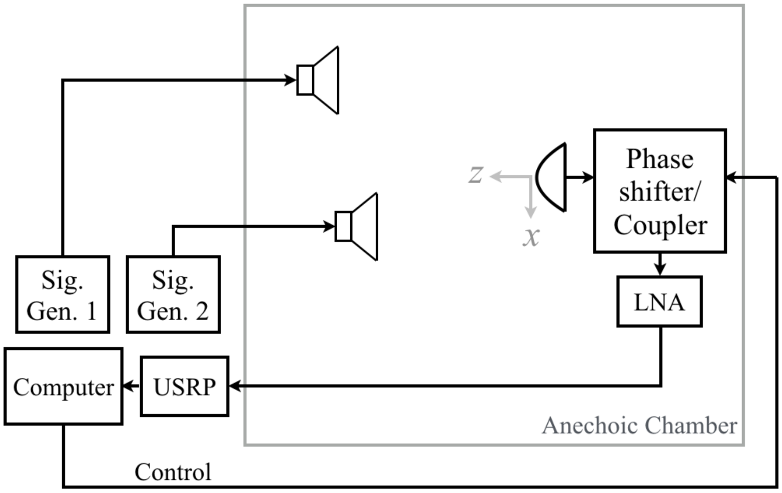
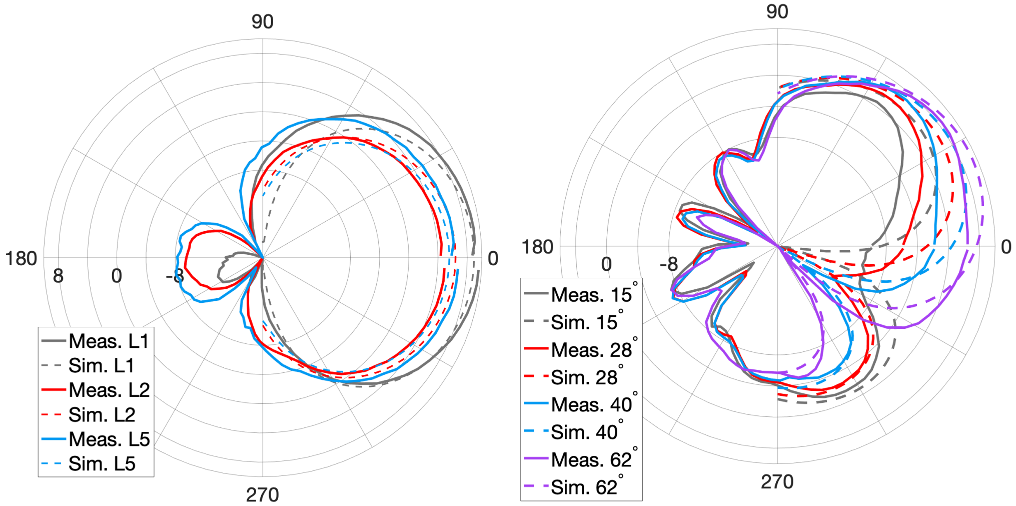


Figure 3.2: Example setup for DOA estimation data collection

require variations of this configuration. The diagram is a top-view, where the y-axis points to the chamber ceiling and the origin is referenced to the phase center of the hemispiral, the receiving antenna in this case. Radiation patterns were measured in the xz-plane, so for this demonstration direction estimation is limited to one plane. A system capable of accurately taking measurements in the entire upper hemisphere of the antenna would remove the limitation.

In all DOA data collection configurations, the hemispiral was the receiving antenna and dual-feed RHCP standard gain horns were the transmitting antennas. The receiver path included a USRP N210/DBSRX2 front end.

The hemispiral's gain patterns are shown in Figure 3.3. Under normal operation with 180° of phase between the arms, the top plot includes measured data (solid lines) for L1, L2, and L5 (black, red, and blue respectively), which are 9.6, 4.9, and 6.8 dB at maximum. The dashed lines represent data from HFSS simulations. There is a slight tilt in the measured data due to error in the manual xz alignment between the hemispiral and the horn. The most significant sources of error would come from the actual versus specified gain of the "known" calibration antenna at these frequencies. Figure 3.3 also includes several examples out of the ten total patterns used for direction estimation, labeled by their input phasing. These measurements constitute a calibration step for MUSIC. We used an analog phase shifter on one of the two coupler outputs, so a source of error for the null location is introduced by the difference between the expected and actual input phase, the latter of



(a) (b)

Figure 3.3: RHCP gain (dB) in the xz-plane for (a) the differential pattern at all bands and (b) other pattern modes by input phase at L1

which may fluctuate with temperature and even slight control voltage error. Additionally, the attenuation in the phase shifter path varies with control voltage, and the compensation in the coupler's other leg was chosen as an average over phase steps, causing an imbalance that varies with each pattern. In practice, eliminating the phase shifter is straightforward once the desired patterns are chosen. One possibility is to use RF switches to change line lengths on the coupler corresponding to the discrete set of desired phases.

The measured antenna VSWR for the common-mode input (worst case) is shown in Figure 3.4 over the frequency range between L5 and L1, with the actual GPS carriers marked. Civil GPS signals inhabit about 2 MHz centered around L1, L2 (L2C), and about 20 MHz at L5. Military codes are allocated 24 MHz at L1 and L2 [6]. This element is evidently well-matched over the entire range and not just at the GPS bands. Future work may include extending the measurements beyond the bordering GPS frequencies and possibly to other applications.

The MUSIC spectrums for xz-plane sources placed at various angles relative to the hemispiral are shown in Figure 3.5. During the calibration step, the turntable used to measure the radiation patterns has a tolerance of roughly 3°, so this is expected to be the limiting factor of our direction estimation accuracy. Section 3.2 discusses and quantifies how the estimation

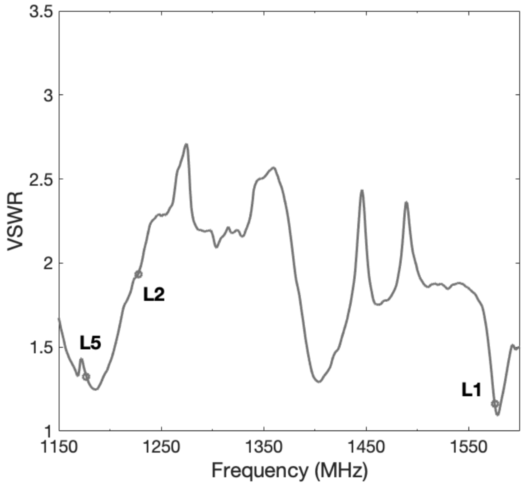
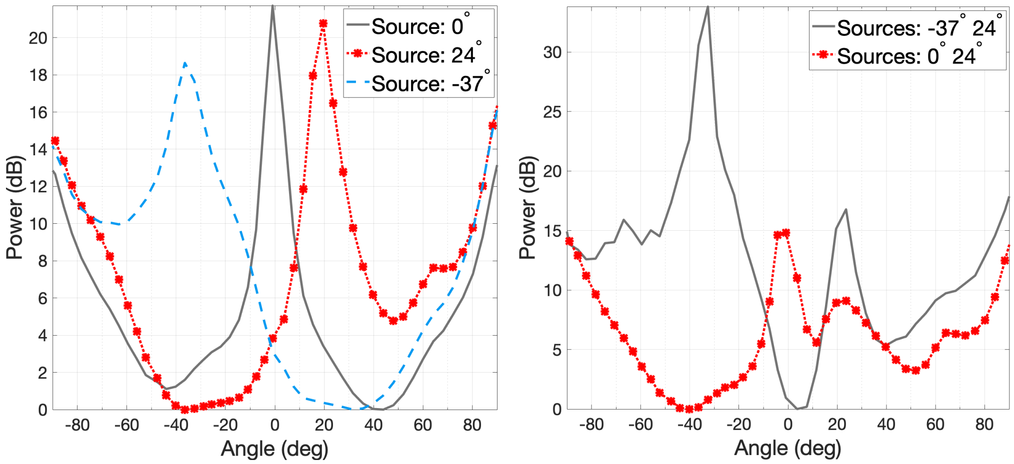


Figure 3.4: Measured common-mode VSWR: 1.16 (L1), 1.93 (L2), 1.32 (L5)



(a)

(b)

Figure 3.5: Example MUSIC spectrums from data collected at L1, processed with all 10 patterns: single source detection (a) does not require phase alignment, while the steps outlined in Chapter 2 are used with multiple sources (b)

error varies with other factors, like SNR and the patterns used. Using reference gain horn antennas in the anechoic chamber guarantees a fairly high SNR, but much lower SNR environments are studied in Section 3.2. These spectrums are constructed using all ten measured patterns, although fewer can be used at the expense of accuracy and confidence in the form of spectrum power. The impact of reducing patterns is also addressed in Section 3.2.

3.2 Further analysis

To quantify the system's limits, we used the measured pattern data to predict DOA performance in various simulation environments. The most pressing concern for GPS is the robustness of this system when signals of interest have low SNR, as is the case with satellite reception. As a rough benchmark, our algorithm could expect post-correlation SNR levels around 20 dB or more, depending on the receiver's integration time [6]. We found that above 26 dB of SNR, just two patterns are needed to produce results within 1° of accuracy after factoring in the tolerance of 3° noted in Section 3.1. Below 26 dB, it was observed that increasing the number of patterns yields higher estimation accuracy, with calibration-limited performance down to 12 dB when using up to eight patterns. However, not all additional patterns improve the estimate by the same amount. To be perfect substitutes for the mode vectors described in Section 2.3, the matrix $\mathbf{A}$ must be full column rank, which is not necessarily the case for an arbitrary set of patterns. The Pearson correlation coefficient, a measure of linear dependence, may be used for evaluation [43]. Its calculation for a pair of variables X and Y over T samples with mean μ and standard deviation σ is defined as [43]

$$\rho(X,Y) = \frac{1}{T-1}\sum_{i=1}^{T}\left(\frac{X_i-\mu_X}{\sigma_X}\right)\left(\frac{Y_i-\mu_Y}{\sigma_Y}\right) \tag{3.1}$$

where $\rho = 1$ indicates perfect correlation. We thus calculated a ρ-matrix of pairwise coefficients between all the patterns. For each pair of patterns, DOA estimation was performed for a sweep of incoming signals across ϑ, with error averaged over increasing noise levels. The median over ϑ is shown in Figure 3.6, against increasing correlation coefficients on the x-axis. While the error does trend higher for more correlated patterns, the relationship is obviously not perfect. Using only two patterns potentially leads to ambiguities at certain angles that may result in high error, especially in the presence of significant noise. Additionally, the correlation metric can only measure linear independence, so higher-order effects are not captured.

We also quantified system performance using incoming sources across all ϑ in the xz-plane, again averaging over a range of noise levels at each step. The hemispiral's expected wide FOV was confirmed with as few as three

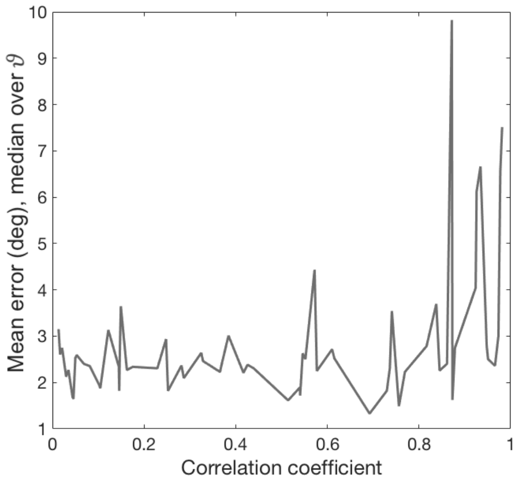


Figure 3.6: DOA error versus ρ over sources from $\vartheta = -60°$ to $60°$, averaged over SNR from 3 dB to 30 dB; patterns normalized to unity

patterns, shown in Figure 3.7 for several example pattern combinations with at least one low-correlation pair. The dashed line represents the calibration tolerance of the turntable.

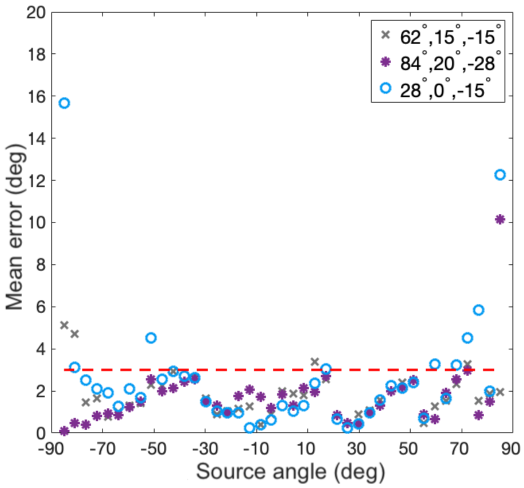


Figure 3.7: DOA error versus incoming source angle using several 3-pattern sets (denoted by input phase), averaged over SNR from 3 dB to 30 dB

Finally, we assessed the system's performance with respect to incoming signals with a potential frequency offset. For this experiment, we placed two incoming sources at $\vartheta = -35°$ and $70°$ in the xz-plane. With one source kept at L1, the second source was swept in frequency over the range of possible Doppler shifts for GPS. The results are reported in Figure 3.8, again with the calibration tolerance shown.

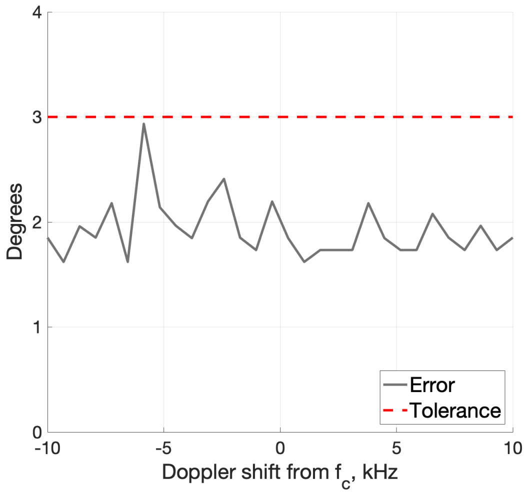


Figure 3.8: DOA error versus frequency offset between incoming sources at $-35°$ and $70°$ in xz with $f_c = 1.57542$ GHz, SNR $= 18$ dB; processed using all patterns

3.3 Summary

Measurement results for a prototype of the hemispiral antenna are presented in this chapter. In addition to collecting gain patterns for the different operation modes, we evaluate the prototype for DOA performance with our modified MUSIC algorithm. Further studies are done to test the limits of this method, including direction finding with multiple sources and in the presence of Doppler shifts in frequency. The DOA estimation accuracy over one plane of the upper hemisphere is also evaluated, with generally acceptable results over a wide range in the antenna's FOV.

CHAPTER 4

THEORY OF SECURE ANTENNA POLARIZATION MODULATION

Data interception from eavesdroppers is a major threat targeting the open nature of wireless broadcast networks. To mitigate the risk from this type of attack, we propose a new approach for data transmission that we term secure antenna polarization modulation, or SAPM. Dual-polarized antennas are used to create data distortion with an element of randomness at all transmission angles except the intended ones, and beamforming/beamsteering may be used to boost gain. As a first step in characterization, we derive and simulate performance using one intended receiver and line-of-sight (LOS) propagation in additive white Gaussian noise (AWGN) channels. The goal of this chapter is to establish a theoretical framework for SAPM in an idealized channel and create a baseline for expectations.

In Section 4.1, we provide an overall summary of SAPM compared to other systems with respect to security and other important features. Section 4.2 gives a technical overview and a high-level functional description of the method. Array equations and the spatial distortion model are discussed in Section 4.3. We derive the detection error probability for all parties, intended or otherwise, in Section 4.4. Simulation results are also shared to help validate the theory. The secrecy capacity of SAPM systems is the subject of Section 4.5, which includes comparisons to other methods for physical layer security. Sections 4.6 and 4.7 discuss further considerations for the technique, including energy concerns and spectral efficiency.

4.1 Comparison of techniques

Before diving into the technical details of SAPM, some expectations should be set regarding its performance versus other secure systems, including those implemented at the upper OSI layers. Several benchmarks and features are chosen for this high-level comparison, with an explanation of each following the summary in Table 4.1. In the table, green indicates good performance or presence of the feature, yellow is reduced performance, and red corresponds to poor performance or no availability. "N/A" indicates that the specific feature is not relevant for the technique.

Table 4.1: Summary of the expected performance of several techniques that may be used to increase wireless security

Feature	Encryption	BFN with I/Q Mod.	DM	BFN with PolSK	SAPM
Random data distortion	🟥	🟥	🟩	🟥	🟩
Keyless decoding	🟥	🟩	🟩	🟩	🟩
Secrecy rates	🟩	🟥	🟨	🟨	🟩
Power efficiency	🟨	🟩	🟥	🟩	🟨
Spectral efficiency	🟥	🟨	🟥	🟩	🟩
Agnostic to receiver location	🟩	🟥	🟥	🟥	🟥
Single transmit antenna	🟩	🟥	🟥	🟥	🟥
Multipath performance	N/A	🟩	🟥	🟨	🟨

- *Random data distortion* - correct bits are received in targeted transmitter look angles while pseudo-random bits are sent everywhere else, amounting to an information beamwidth; Sections 4.3.2 and 4.4
- *Keyless decoding* - no secret key needs to be shared between legitimate users
- *Secrecy rates* - the difference between the mutual information received by a legitimate user in the channel versus an eavesdropper; Section 4.5
- *Power efficiency* - system-level efficiency that includes both RF and DC input power; Section 4.6
- *Spectral efficiency* - measured in bits per symbol or transmission rate per 1 Hz bandwidth; Section 4.7
- *Agnostic to receiver location* - no information required about the relative angles that contain desired receivers
- *Single transmit antenna* - only have one transmit antenna required, instead of an array

- *Multipath performance* - robustness in fading channels, where multiple paths exist between transmitters and receivers; Section 7.2.1

Most of these characteristics are analyzed further in the following sections, as indicated in the list. It is worth noting that encryption provides a solution when system constraints are very different from those favoring the physical layer security methods in all but the first column. Namely, encryption would be used when the system can accommodate keys and authentication and would trade off secrecy for other factors, such as getting information about legitimate receivers' arrival angles. We include encryption in this list as a reference due to its established use, but SAPM performance will be directly benchmarked against other physical layer security methods unless considering system efficiency. For particularly flexible problem spaces that simply desire the highest levels of security, encryption may be combined with a solution implemented at the physical layer.

4.2 Background and functional description

Similar to PolSK, SAPM uses wave SOP to transmit the message as opposed to absolute amplitude, frequency, and/or phase. However, unlike PolSK, SAPM modulation is done with simultaneously radiated polarization patterns in different states. It is important to note that this does *not* require twice the number of antennas—in fact, SAPM may be fully implemented on an existing PolSK system with beamforming capabilities. In other words, SAPM transmitters utilize a single array of dual-polarized antennas with conventional array frontend control (attenuators/phase shifters or a fully digital BFN). Dual-polarized antennas, also required by PolSK, are generally sensitive to all polarizations at broadside, with the crossed dipole serving as a popular example [23], [44]. Over far field angles away from broadside, the nominal received or transmitted polarization degrades due to increasing cross-polarized components, resulting in PolSK's deterministic spatial distortion [27]. SAPM enjoys this effect in addition to its own pseudorandom distortion. To avoid ambiguity, a technical overview of polarization is provided in Section 4.2.1, along with definitions of relevant terms. We then describe the high-level functionality of an SAPM system in Section 4.2.2.

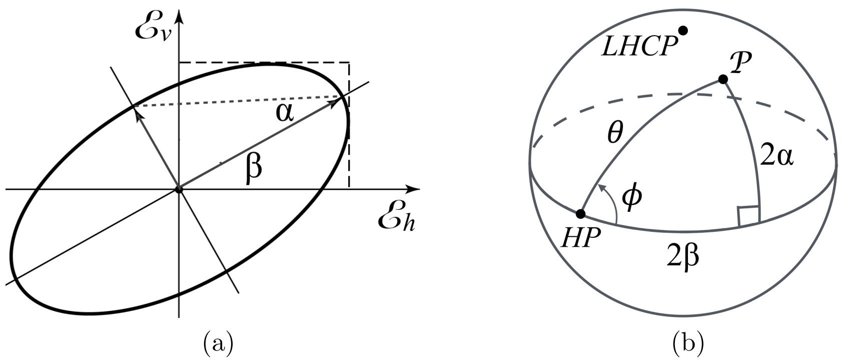


Figure 4.1: Polarization ellipse and Poincaré sphere, adapted from [23], [46]

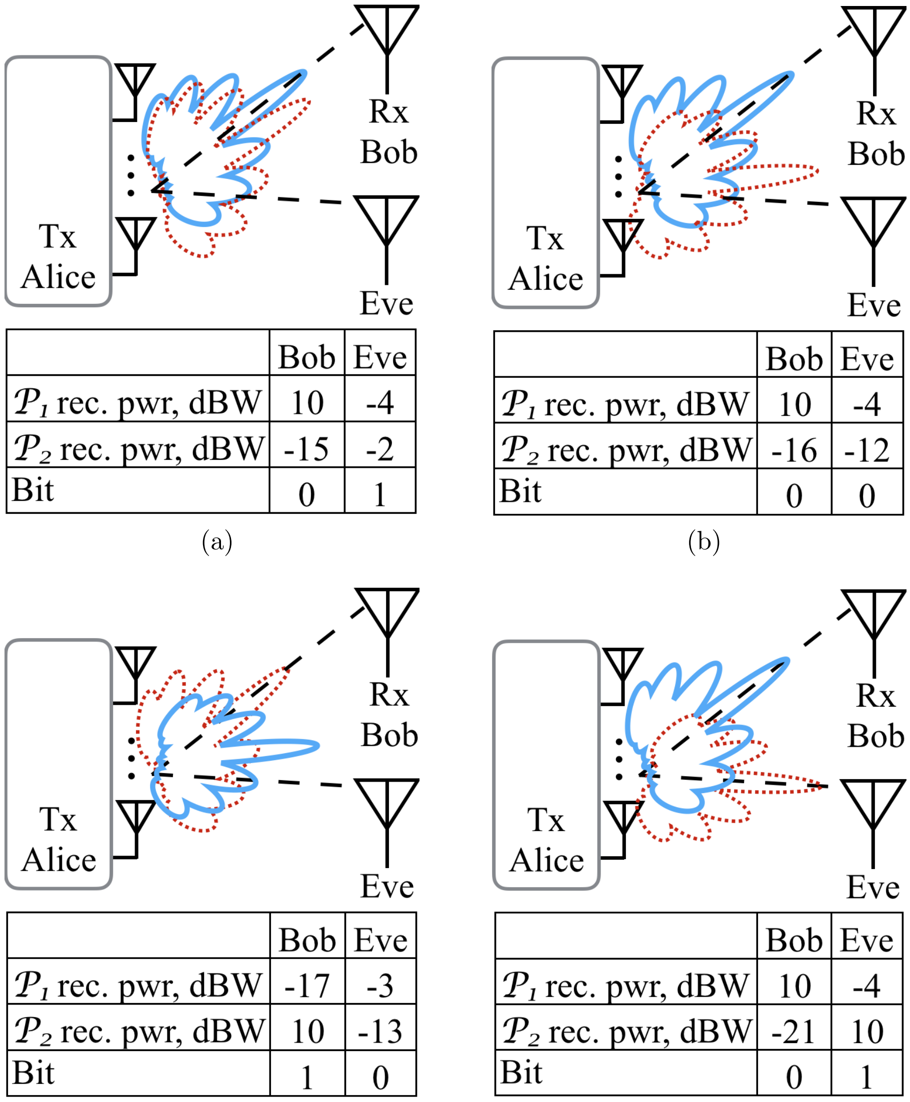
4.2.1 Representation of polarization state

The SOP of an electromagnetic wave may be expressed as the ratio of two orthogonal field components [45], [46]. The convention is to use $\mathcal{P} = \mathcal{E}_v/\mathcal{E}_h$, where $\mathcal{E}_v$ and $\mathcal{E}_h$ are complex vertical and horizontal electric field phasors in the plane of polarization; see Figure 4.1(a) [23]. In polar form, $\mathcal{P} = [\tan(\theta/2)]\, e^{j\phi}$, with magnitude equal to the fields' amplitude ratio and phase equal to their relative phase difference. Pure SOPs for equal energy signals may be entirely specified by the angles $[\theta, \phi]$. Then $\mathcal{P}$ lies on the surface of a Poincaré sphere in the coordinate system defined by three of the four Stokes parameters [45].

The Poincaré sphere is a geometric interpretation of the SOP and a convenient modulation surface. It is shown in Figure 4.1(b), where latitude 2α and longitude 2β are related to $[\theta, \phi]$, as well as to the ellipticity and tilt of the ellipse in Figure 4.1(a) [46]. For the purposes of this work, we opt to use θ as the inclination angle from the north pole and ϕ as the azimuthal angle to save processing steps. Their mapping to $[2\alpha, 2\beta]$ is given in [46]. The SOPs in our case are simply points on the surface of a rotated Poincaré sphere. Throughout the paper, coordinates on this sphere (representing SAPM symbols) are denoted $[\theta, \phi]$. When spherical coordinates actually refer to physical directions in space relative to some origin, they will instead be denoted $[\vartheta, \varphi]$.

4.2.2 High-level operation

Basic SAPM operation may be illustrated with a simplified binary case using two SOPs, $\mathcal{P}_1$ and $\mathcal{P}_2$, but the extension to higher order modulation



	Bob	Eve
$\mathcal{P}_1$ rec. pwr, dBW	10	-4
$\mathcal{P}_2$ rec. pwr, dBW	-15	-2
Bit	0	1

(a)

	Bob	Eve
$\mathcal{P}_1$ rec. pwr, dBW	10	-4
$\mathcal{P}_2$ rec. pwr, dBW	-16	-12
Bit	0	0

(b)

	Bob	Eve
$\mathcal{P}_1$ rec. pwr, dBW	-17	-3
$\mathcal{P}_2$ rec. pwr, dBW	10	-13
Bit	1	0

(c)

	Bob	Eve
$\mathcal{P}_1$ rec. pwr, dBW	10	-4
$\mathcal{P}_2$ rec. pwr, dBW	-21	10
Bit	0	1

(d)

Figure 4.2: Notional example of SAPM data transmission during four time steps (a)–(d), each during a different symbol period; over the total transmission time, Bob detects "...0010..." but Eve detects "...1001..."

is straightforward. Figure 4.2 illustrates SAPM communication between a transmitter, Alice, and a desired receiver, Bob. An eavesdropper, Eve, is also shown, but we assume that any direction without Bob may contain Eve. Array geometries, radiation patterns, and received power levels are approximations and examples used to aid the explanation.

The four diagrams illustrate the steady-state radiation patterns at four different symbol periods, with $\mathcal{P}_1$ as the blue solid line and $\mathcal{P}_2$ as the red dashed line. The primary SOP (intended bit) at each time step has its boresight pointed at Bob, while a secondary SOP is simultaneously radiated with one of its nulls pointed at Bob. For this *binary* case, it is intuitive that if the secondary SOP is orthogonal to the primary, it will coincide with the SOP representing the other bit since optimal error performance means that the symbols will be antipodal on the Poincaré sphere. On the other hand, the decision of what state to assign to the secondary involves a tradeoff between secrecy and Bob's error performance, which is an interesting path for future work. Going forward in this study, the secondary SOP is always kept orthogonal to the primary, so for modulation orders beyond two, the secondary will often not correspond to one of the other symbols.

The tables at every step list the received power in each polarization and the detected bits for Bob and Eve, which are obviously different: Bob's stream is "…0010…" while Eve observes "…1001…". As intended receivers move, Alice may beam- or null-steer accordingly [23], [47]. In this example, only peaks and nulls are pointed at Bob, but any combined pattern that satisfies Bob's error rate requirements would suffice. While the number of null patterns available is limited by the array geometry, i.e., a four-element linear array generally has three null patterns, more options with arbitrary pattern combinations may exist with the same array as long as Bob receives power above (below) some threshold in the primary (secondary) SOP. More options per symbol corresponds to less predictable spatial distortion and better security, but finding patterns that fulfill these thresholds requires knowledge of specific channel/receiver characteristics, such as noise figure and cross-polarization discrimination (XPD). To keep the analysis straightforward, we opt for the conservative requirement that each primary (secondary) pattern must have its maximum (null) directed to Bob. Then for each of $\mathcal{P}_m,\ m = 1,\ldots,M$ symbols in M-ary SAPM, there will be $l = 1,\ldots,L$ pattern combinations available to be chosen pseudorandomly at each symbol step.

4.3 Radiation and distortion

With basic functionality summarized, we now detail the methodology to synthesize SAPM patterns in Section 4.3.1. These equations provide insight for SAPM's directional spatial distortion, discussed in 4.3.2.

4.3.1 Array theory for SAPM

We start with an arbitrarily-spaced array of N dual-polarized elements in the xy-plane for a general case of two-dimensional beamsteering over the upper hemisphere. Expanding on basic array theory from [23], the radiation pattern is given in Equation (4.1), where field components are referenced to vertical ($\mathcal{E}_v$) and horizontal ($\mathcal{E}_h$) polarizations *locally* at the receiver, corresponding to far field components $-\mathcal{E}_\vartheta$ and $\mathcal{E}_\varphi$.

$$\begin{aligned}\begin{bmatrix}\mathcal{E}_v(m,\vartheta,\varphi)\\ \mathcal{E}_h(m,\vartheta,\varphi)\end{bmatrix} &= \begin{bmatrix} s_{vv}^{(1,\ldots,N)}, & s_{vh}^{(1,\ldots,N)}\\ s_{hv}^{(1,\ldots,N)}, & s_{hh}^{(1,\ldots,N)}\end{bmatrix}\\ &\quad\times\left[a_v^{(1,\ldots,N)}[m],\ a_h^{(1,\ldots,N)}[m]\right]^T\\ &\quad+\left[\hat{n}_v,\hat{n}_h\right]^T \end{aligned} \tag{4.1}$$

where $m=1,\ldots,M$, $\{\varphi \mid -\pi\le\varphi\le\pi\}$, $\{\vartheta \mid 0\le\vartheta\le\pi\}$, and

$$s_{vv}^{(n)} = f_{vv}^{(n)}(\vartheta,\varphi)e^{j\mathbf{k}\cdot\mathbf{r}_n} \tag{4.2}$$

$$\mathbf{k}\cdot\mathbf{r}_n = \frac{2\pi}{\lambda}\left(x_n\sin\vartheta\cos\varphi + y_n\sin\vartheta\sin\varphi\right) \tag{4.3}$$

The function $f_{vv}^{(n)}(\vartheta,\varphi)$ is the co-polarized arbitrary element radiation pattern for the n^{th} antenna at $[x_n, y_n]$, and λ is the wavelength at the carrier frequency. The spatial distributions $s_{vh}^{(n)}$, $s_{hv}^{(n)}$, $s_{hh}^{(n)}$ are similarly defined as (4.2), with their corresponding $f_{vh}^{(n)}, f_{hv}^{(n)}, f_{hh}^{(n)}$ patterns. These represent the complex transfer functions from the excitation terms to the field terms—i.e., $s_{vh}^{(n)}$ takes the horizontally polarized excitation a_h to the vertical field component $\mathcal{E}_v$ for the n^{th} element. The noise vector consists of zero-mean, circularly symmetric Gaussian distributions with power spectral density $N_0/2$. The set of symbols for Bob is represented by primary SOPs $\mathcal{P}_m=[\theta_m,\phi_m]$, so the secondary SOPs are the set $\mathcal{P}'_m=[\theta'_m,\phi'_m]$.

Array excitations, approximated as constant over a symbol period, are derived here for main beam directions $[\vartheta_0,\varphi_0]$ and $[\vartheta'_0,\varphi'_0]$ in the two SOPs. For total input power P_{RF}, antenna input impedance Z_A, and fraction of power γ in the secondary state, the general form for the excitations are

$$a_v^{(n)}[m] = A_v e^{j(\chi_v + \psi'_v)} \tag{4.4}$$

$$a_h^{(n)}[m] = A_h e^{j(\chi_h + \psi'_h)} \tag{4.5}$$

where

$$\begin{aligned}
A_v &= \Bigg\{ \left(\frac{2Z_A P_t}{N}\right) \bigg[(1-\gamma)\sin^2\left(\frac{\theta_m}{2}\right) + \gamma \sin^2\left(\frac{\theta'_m}{2}\right) \\
&\quad + \sqrt{\gamma(1-\gamma)} \cos\left(\frac{\theta_m}{2} - \frac{\theta'_m}{2}\right) \cos\left(\psi_v - \psi'_v\right)\bigg] \Bigg\}^{1/2} \\
\chi_v &= \operatorname{atan2}\Bigg[\sqrt{1-\gamma}\sin\left(\frac{\theta_m}{2}\right)\sin\left(\psi_v - \psi'_v\right), \\
&\quad \sqrt{\gamma}\sin\left(\frac{\theta'_m}{2}\right) + \sqrt{1-\gamma}\sin\left(\frac{\theta_m}{2}\right)\cos\left(\psi_v - \psi'_v\right)\Bigg] \\
A_h &= \Bigg\{ \left(\frac{2Z_A P_t}{N}\right) \bigg[(1-\gamma)\cos^2\left(\frac{\theta_m}{2}\right) + \gamma \cos^2\left(\frac{\theta'_m}{2}\right) \\
&\quad + \sqrt{\gamma(1-\gamma)} \cos\left(\frac{\theta_m}{2} - \frac{\theta'_m}{2}\right) \cos\left(\psi_h - \psi'_h\right)\bigg] \Bigg\}^{1/2} \\
\chi_h &= \operatorname{atan2}\Bigg[\sqrt{1-\gamma}\cos\left(\frac{\theta_m}{2}\right)\sin\left(\psi_h - \psi'_h\right), \\
&\quad \sqrt{\gamma}\cos\left(\frac{\theta'_m}{2}\right) + \sqrt{1-\gamma}\cos\left(\frac{\theta_m}{2}\right)\cos\left(\psi_h - \psi'_h\right)\Bigg]
\end{aligned}$$

For the n^{th} element,

$$\psi_v = \phi_m - \frac{2\pi}{\lambda}\left(x_n \sin\vartheta_0 \cos\varphi_0 + y_n \sin\vartheta_0 \sin\varphi_0\right) \tag{4.6}$$

$$\psi_h = -\frac{2\pi}{\lambda}\left(x_n \sin\vartheta_0 \cos\varphi_0 + y_n \sin\vartheta_0 \sin\varphi_0\right) \tag{4.7}$$

$$\psi'_v = \phi'_m - \frac{2\pi}{\lambda}\left(x_n \sin\vartheta'_0 \cos\varphi'_0 + y_n \sin\vartheta'_0 \sin\varphi'_0\right) \tag{4.8}$$

$$\psi'_h = -\frac{2\pi}{\lambda}\left(x_n \sin\vartheta'_0 \cos\varphi'_0 + y_n \sin\vartheta'_0 \sin\varphi'_0\right) \tag{4.9}$$

As a check, we may allow γ to approach zero in (4.4) and (4.5). The excitations are then identical to those for PolSK.

To simplify the analysis, we adapt these equations for an equally-spaced linear array along the y-axis and consider performance over angles φ in azimuth, at $\vartheta = 90°$. The terms starting with x_n may be eliminated from Equation (4.3) and Equations (4.6)-(4.9), and for each of m symbols, there are $L = N - 1$ combined pattern options for SAPM. While Alice uses the array to produce $L \times M$ distinct, directive patterns, Bob does not need to know anything about the l parameter and may use a single antenna that is sensitive to the set $\mathcal{P}_m$. It is most convenient to use one or more dual-polarized antennas, which usually provide orthogonally-polarized signals on two channels.

4.3.2 Constellation distortion

It is seen from the equations in Section 4.3.1 that the radiated polarization pattern is altered by the SAPM excitation vector in a different way than in conventional PolSK. The orthogonal polarization changes the spatial characteristics of the SOP with the introduction of the prime terms in Equations (4.4)-(4.9). In this section, we further illuminate the impact.

In general, the range of transmission angles that do not contain Bob are all potential locations for Eve. Several assumptions about receiver capabilities are stated below:

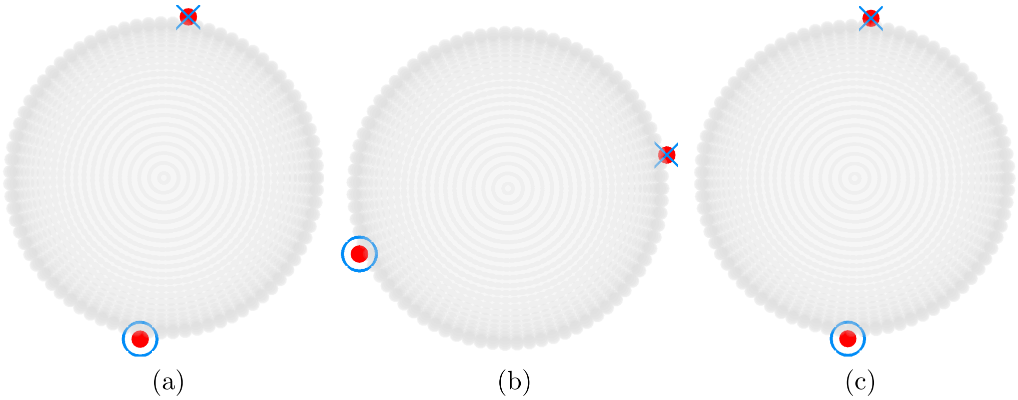
- All parties have the required hardware (dual-polarized antennas, receivers, etc.)
- The modulation order M is known
- All parties have the ability to dynamically calibrate and estimate signal constellations

The last assumption means that receivers may use some method to find the nominal constellation intelligently, which we will discuss later in the section. Additionally, if the estimated symbols have high absolute correlation with the intended symbols, Eve may glean useful information.

PolSK

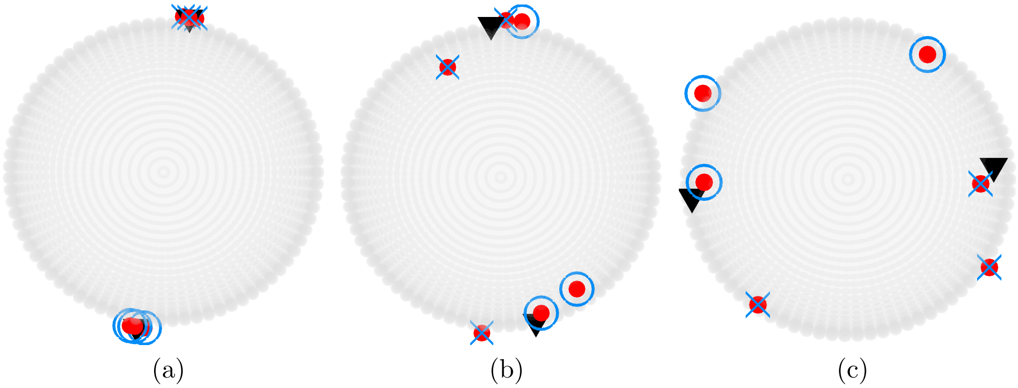
For any transmitting antenna, some amount of cross-polarization is radiated and the nominal SOP varies over look angle [26], [27]. As noted, this increases the security of PolSK by essentially creating polarization mismatch at angles away from broadside. Since this variation in SOP is due to the channel transfer function, Equations (4.2) and (4.3), the constellation distortion is deterministic. During demodulation, we estimate θ_m and ϕ_m, which are nonlinear functions of the received $\mathcal{E}_v/\mathcal{E}_h$; see Section 4.2.1. Figure 4.3(a) is a plot of the noiseless portion of the demodulated signal (red dots) for Bob at azimuth $\varphi = 0^\circ$ relative to Alice at origin. In this case, $M = 2$, so there are two red dots overlaid with two different blue shapes ("$\times$" or "$\circ$") to show which transmitted symbol produced each received one.

PolSK's constellation warping with angle may be described as nonlinear mapping functions $\mathbf{g}_m = [g_m^\theta(\varphi), g_m^\phi(\varphi)]^T$ that take the transmitted symbol, $\mathcal{P}_m$, to the noiseless portion of the demodulated signal. These functions vary with antenna parameters and are generally different for each nominal transmitted SOP [26], [27]. As the authors of [30] observe, this mapping causes the received constellation points to shift across the Poincaré surface as receivers move in φ. In Figures 4.3(b) and 4.3(c), two examples of this shift are shown for receivers located at $\varphi = -28^\circ$ and $\varphi = 44^\circ$, respectively. In general, over all spatial angles in the transmitter's field of view, the received symbols shift smoothly across the sphere and almost always remain sufficiently separated. Eavesdroppers may simply calibrate their reference angle in Stokes space to receive the correct bits—in fact, any receiver, including Bob, should be using calibration techniques to at least account for polarization mismatch between the transmit and receive antennas. It is also evident from Figure 4.3(c) that the shift can be very minimal at certain look angles; in this case, $\varphi = 44^\circ$ consists of a radiation sidelobe. When noise is included in the analysis, the dots become smears of points distributed over the spherical surface. Then the correction step would need to include an averaging of demodulated points to estimate the nominal received constellation.



(a) (b) (c)

Figure 4.3: Binary PolSK: Demodulated received signals (red dots) without noise for a receiver at (a) $\varphi = 0°$ (Bob), (b) $\varphi = -28°$ (Eve 1), and (c) $\varphi = 44°$ (Eve 2) relative to Alice; overlaid with the corresponding transmitted symbol (blue "×", "○")



(a) (b) (c)

Figure 4.4: Binary SAPM with $L = 3$: Demodulated received signals (red dots) without noise and their mean centers of mass (black "▼") for a receiver at (a) $\varphi = 0°$ (Bob), (b) $\varphi = -28°$ (Eve 1), and (c) $\varphi = 44°$ (Eve 2) relative to Alice; overlaid with the corresponding transmitted symbol (blue "×", "○")

SAPM

For SAPM, the mapping changes with choices made regarding the secondary pattern. For each of the M symbols, we may form a subset of excitations based on these selections that correspond to mapping functions $[\mathbf{g}_{m,1}, \ldots \mathbf{g}_{m,L}]$, for a total of L members in each subset. Over azimuth, the demodulated signal plus noise is

$$\mathbf{w}(\varphi) = \begin{bmatrix} g^{\theta}_{m,l}(\varphi) \\ g^{\phi}_{m,l}(\varphi) \end{bmatrix} + \begin{bmatrix} \hat{n}_{\theta} \\ \hat{n}_{\phi} \end{bmatrix}$$

$$m = 1, \ldots, M, \quad l = 1, \ldots, L \tag{4.10}$$

where $[\hat{n}_{\theta}, \hat{n}_{\phi}]^T = \hat{\mathbf{n}}$ is no longer Gaussian.

In Figures 4.4(b) and 4.4(c), we again show with red dots the noiseless portion of the received symbol $[g^{\theta}_{m,l}(\varphi), g^{\phi}_{m,l}(\varphi)]^T$ for eavesdroppers located at $-28°$ and $44°$, respectively, when Bob is at 0°. Since Eve has knowledge of M, she may aggregate demodulated points over time to calibrate out polarization mismatch and the shift from the intended $\mathcal{P}_m$. To this end, k-means++ clustering was used to approximate the nominal constellation by finding the average centers of mass $\mathbf{b}_m$ (black "▼") for all incoming signals demodulated using an optimal Stokes receiver for PolSK [24], [48]. Following the same steps, Bob ($\varphi = 0°$) would instead see the constellation shown in Figure 4.4(a), where the cluster centers overlap very closely with the received symbols. The plots are again overlaid with the two different blue shapes ("×" or "○") for the corresponding transmitted symbol. Although the received set for Bob is demodulated correctly (all "×"s or "○"s cluster together, as expected), this is not the case for the Eves.

Unless otherwise stated, we keep power ratio γ at 1/2 and only consider the null patterns as possibilities for the secondary, which limits L to $N - 1$ (4.3.1). In general, the sets L will be bigger because more than one power ratio may be used and other pattern combinations should be considered, as discussed in 4.2.2. It should be noted that approximating the nominal constellation and calibrating out polarization mismatch must be done for all polarization-modulated methods, including PolSK, and suitable procedures beyond k-means++ may be used, as long as this step is kept consistent between Eve and Bob.

4.3.3 Simulation model

Both the transmitting and receiving SAPM antennas play critical roles in system performance, as discussed in [26], and further analysis of these effects will be the topic of a separate investigation. The radiation patterns used

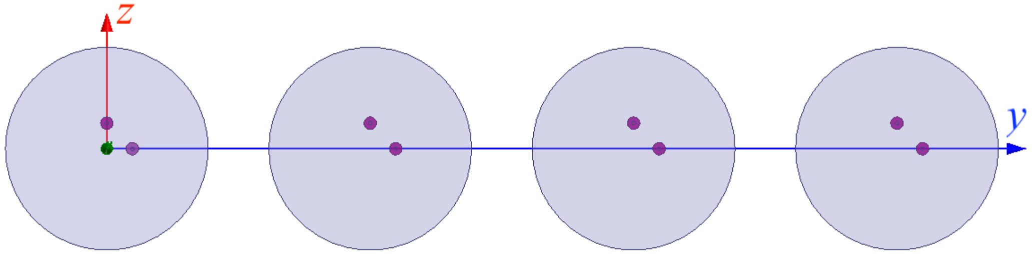


Figure 4.5: Linear array of dual-polarized circular microstrip patch antennas with half-wavelength spacing at 2.4 GHz; broadside at $\vartheta = 90°, \varphi = 0°$

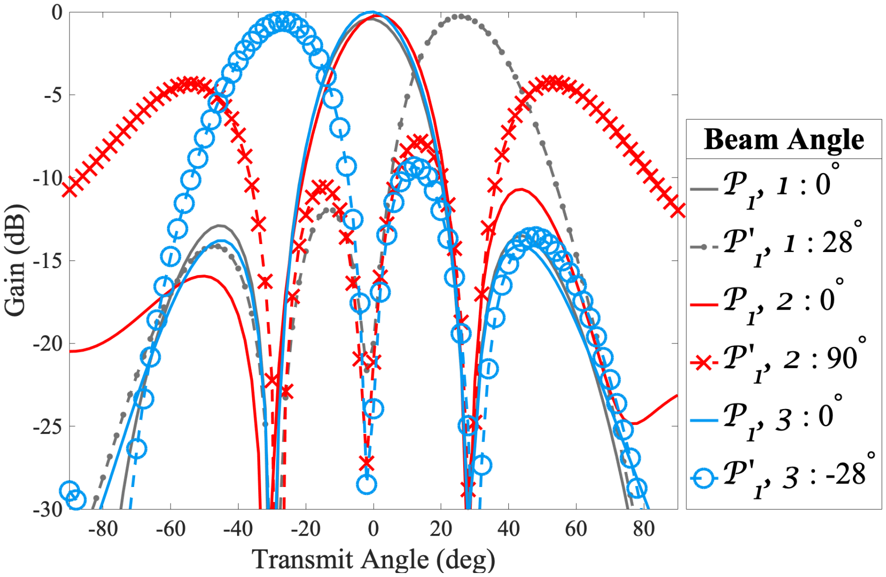


Figure 4.6: Set of $l = [1, 2, 3]$ options for one symbol $\mathcal{P}_1, l$ with simultaneous secondary SOP $\mathcal{P}'{}_1, l$; intended boresight angle reported for each pattern; Bob located at $\varphi = 0°$

in this chapter are from full-wave HFSS simulations of a four-element linear array in free space, shown in Figure 4.5. Each element is a circular dual-polarized microstrip patch designed to be resonant at S band. Figure 4.6 shows a subset of the gain patterns available from this array, plotted over the xy-plane when the primary $[\theta_m, \phi_m] = [90°, -90°]$, or right-hand circular polarization. The power coefficient γ is kept at 0.5 for all scenarios.

4.4 Error probability

System performance may be quantified by the probability of errors during detection, where the range of transmission angles with low error probability forms an *information beam*. To increase security, this beam should be as narrow as possible around Bob. For conventional methods, where error probability is a function of SNR, the information beam has the same shape as the power pattern. In those cases, the only ways to reduce the width of the beam are to decrease SNR in the transmission or increase array gain (size), neither of which is usually desirable. For SAPM, we show in this section that the information beam is reduced without either requirement.

First, we derive a lower bound for symbol error probability in 4.4.1 and 4.4.2. These are verified against simulations using a full-wave field solver in 4.4.3 to compare SAPM information beamwidths to those of traditional systems.

4.4.1 Post-demodulation probability density function

Due to its reliance on only relative phase and amplitude, SAPM, like PolSK, should be considered a noncoherent technique because demodulation may be accomplished without estimating absolute carrier phase. Detection is done at each symbol period as opposed to differential phase-shift keying (DPSK), another noncoherent method that requires two consecutive periods per symbol [49]. Since SAPM is identical to PolSK for communication to Bob, we use a modified Stokes receiver for convenience [24]. As there is no single optimal bit-mapping strategy for PolSK (with a few exceptions, such as gray-coding for the 8-cube constellation), the conversion from symbol error probability to the bit level may be calculated numerically based on application-specific optimization constraints [24].

Demodulation brings the signal centered at the carrier or intermediate frequency down to baseband in order to produce estimates for $\mathcal{P}_m$. Given the intended transmission parameters, the probability density function (PDF) of the demodulator output $\mathbf{w}$ is $p_{\mathbf{w}} = p_{\Theta,\Phi}$, adapted from [24], [50]:

$$\begin{aligned} p_{\Theta,\Phi}(\theta,\phi \mid \mathcal{P}_m, l, \varphi) = \frac{\sin\theta}{4\pi}&\left[1 + \frac{E_s}{2N_0}(1+U)\right] \\ &\times \exp\left[-\frac{E_s}{2N_0}(1-U)\right] \end{aligned} \tag{4.11}$$

where E_s is the total energy per symbol and

$$\begin{aligned} U &= \sin\left[g^{\theta}_{m,l}(\varphi)\right]\sin\theta\cos\left[\phi - g^{\phi}_{m,l}(\varphi)\right] \\ &\quad + \cos\left[g^{\phi}_{m,l}(\varphi)\right]\cos\theta \\ m &= 1,\ldots,M, \quad l = 1,\ldots,L \end{aligned}$$

The detector that follows demodulation determines which of the M messages was sent. Going forward, we assume equiprobable symbol transmission, so optimal detection is based on the maximum-likelihood (ML) criterion [49].

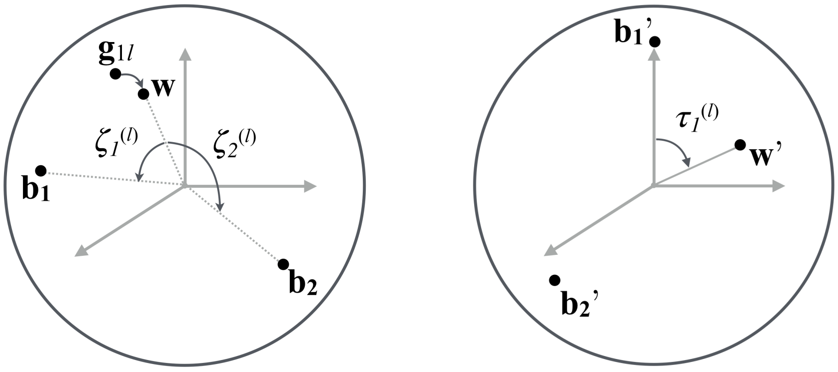
4.4.2 Derivation of error bound

For M-ary SAPM, the average symbol error probability at φ is defined as

$$P_M\left[E(\varphi)\right] = \frac{1}{M}\sum_{m=1}^{M}\iint\limits_{D_m}\left[1 - p_{\Theta,\Phi}(\theta,\phi \mid \mathcal{P}_m,\varphi)\right]d\theta d\phi \tag{4.12}$$

where E is the set of error events and D_m defines the boundary of the decision region around each symbol. For any receiver, Equation (4.12) may be solved exactly once the D_m are defined, but finding the optimal regions is usually not a straightforward task for higher M [24]. To make the analysis agnostic to the definition of D_m, we derive a lower bound on uncoded symbol error probability based on great-circle distances, or central angles on the unit sphere, which comes from the Fisher distribution approximation to Equation (4.11) [50].

We start with an intended transmission of $\mathcal{P}_1$ using the l^{th} excitation for binary SAPM, which will later be generalized to $M > 2$. At some φ, the demodulated signal plus noise is $\mathbf{w} = \mathbf{g}_{1l} + \hat{\mathbf{n}}$. A receiver in this location has estimated the constellation to be $[\mathbf{b}_1, \mathbf{b}_2]$, which correspond to $[\mathcal{P}_1, \mathcal{P}_2]$, shown in Figure 4.7(a). There is an error if $\mathbf{w}$ is closer to $\mathbf{b}_2$ than $\mathbf{b}_1$. Equation



(a) (b)

Figure 4.7: Demodulated constellation for a receiver at an arbitrary (ϑ, φ), two symbols shown

(4.13) summarizes this event E, given $\mathcal{P}_1$ and excitation l, in terms of central angles ζ. We drop the φ notation, since it is understood that the analysis is for an arbitrary angle in azimuth.

$$\begin{aligned} P_2(E \mid \mathcal{P}_1, l) &= P\left(E_{21}^{(l)}\right) \\ &= P\left(\|\mathbf{w} - \mathbf{b}_2\| < \|\mathbf{w} - \mathbf{b}_1\| \mid \mathcal{P}_1, l\right) \\ &= P\left(\zeta_2^{(l)} < \zeta_1^{(l)}\right) \end{aligned} \tag{4.13}$$

To calculate $\zeta_1^{(l)}$ more easily, we may rotate all locations on the sphere such that $\mathbf{b}_1$ is at the north pole, Figure 4.7(b). Then $\zeta_1^{(l)}$ reduces to $\tau_1^{(l)}$, the inclination angle of the rotated $\mathbf{w}$'. The same step is done for $\zeta_2^{(l)}$.

Equation (4.13) may be written as the probability that $\mathbf{w}$ falls in the region of $[\theta, \phi]$ where the difference of $\tau_2^{(l)}$ and $\tau_1^{(l)}$ is less than zero:

$$\begin{aligned} P\left(\zeta_2^{(l)} < \zeta_1^{(l)}\right) &= P\left(\tau_2^{(l)} < \tau_1^{(l)}\right) \\ &= P\left(\mathbf{w}(\theta, \phi) \mid \tau_2^{(l)}(\theta, \phi) - \tau_1^{(l)}(\theta, \phi) < 0\right) \\ &= \int\limits_{\tilde{\phi}} \int\limits_{\tilde{\theta}} p_{\Theta,\Phi}(\theta, \phi \mid \mathcal{P}_1, l) d\theta d\phi \end{aligned} \tag{4.14}$$

where

$$\{\tilde{\theta}, \tilde{\phi}\} = \left\{[\theta, \phi] \mid \tau_2^{(l)}(\theta, \phi) - \tau_1^{(l)}(\theta, \phi) < 0\right\}$$

Over $L(1)$ total excitations for $\mathcal{P}_1$, assuming each option is equiprobable, the error probability for this symbol is then

$$P\left(E_{21}\right) = \frac{1}{L(1)} \sum_{l=1}^{L(1)} P\left(E_{21}^{(l)}\right) \tag{4.15}$$

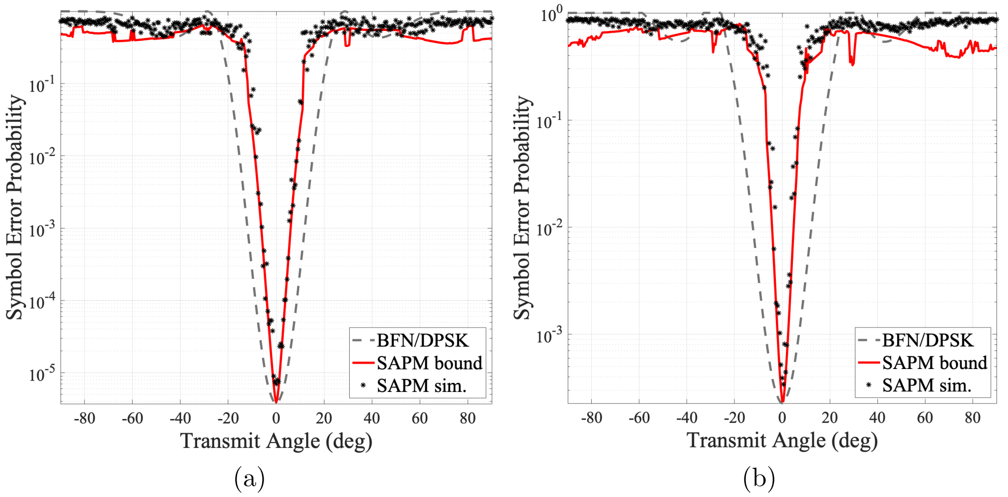
To generalize the results to constellations of M symbols, we use the lower bound of the Boole-Fréchet inequality for logical disjunction [51]. For each of L configurations of a transmitted $\mathcal{P}_m$, there are $M-1$ other $\mathcal{P}_k, k \neq m$ results that are errors if they are detected instead. The bound is the maximum of the set:

$$\begin{aligned} P_M(E) &\geq \max\left[P\left(E_{km}^{(l)}\right)\right] \\ &\geq \max\Bigg[P\left(E_{\substack{1\\m}}^{(1)}\right), \ldots, P\left(E_{\substack{k_{M-1}\\m}}^{(1)}\right), \\ &\qquad P\left(E_{\substack{1\\m}}^{(L)}\right), \ldots, P\left(E_{\substack{k_{M-1}\\m}}^{(L)}\right)\Bigg] \end{aligned} \tag{4.16}$$

$$m = 1, \ldots, M \qquad k \neq m$$

4.4.3 Simulation results

In Figure 4.8, we plot the error bounds derived here (red solid lines) for 4-ary and 8-ary modulation across $\{\varphi \mid -90^\circ \leq \varphi \leq 90^\circ\}$, at SAPM energy per bit to noise (E_b/N_0) of 14 dB for Bob. Alice transmits to Bob at $\varphi = 0^\circ$, and aside from a small margin around Bob, all other angles are considered fair game for Eve. Simulation results (black dots) with receivers at every half-degree step are overlaid on the plots, where 4 million bits are transmitted in each case. We use a minimum distance detector, a reasonable approximation to the ML detector for our SNR range [50]. Along the same axis, we also plot the theoretical symbol error probability for a conventional beamformer transmitting DPSK (gray dashed lines), as a comparison to another noncoherent technique [49].



(a)

(b)

Figure 4.8: Simulated and theoretical (a) 4-SAPM and (b) 8-SAPM uncoded error probability over azimuth, with increasingly narrow information beamwidth compared to beamforming; average SAPM $E_b/N_0 = 14$ dB for Bob at $\varphi = 0°$; E_b/N_0 at other angles for both methods may be found from Figure C.1 in Appendix C

For DPSK, the evaluation of symbol error probability involves numerical integration for $M > 4$; see Equation (4.17) from [49]. Its form is identical to PSK with an extra factor of 1/2 times per-symbol SNR E_s/N_0, since the noise variance is twice as high due to a signal projection during noncoherent demodulation [49].

$$P_{M,DPSK}(E) = 1 - \int_{-\pi/M}^{\pi/M} p_\Theta(\theta)d\theta \tag{4.17}$$

$$\begin{aligned} p_\Theta(\theta) &= \frac{1}{2\pi}e^{C(\theta)} \int_0^\infty v \ \exp\left[-\frac{\left(v - \sqrt{E_s/N_0}\cos\theta\right)^2}{2}\right] dv \\ &= \frac{1}{2\pi}e^{C(\theta)} \int_{(\sqrt{E_s/N_0}\cos\theta)}^\infty e^{-a^2/2}\left[a + \sqrt{E_s/N_0}\cos\theta\right] da \\ &= \frac{1}{2\pi}\left\{e^{-E_s/2N_0} + \sqrt{\frac{-2\pi E_s}{N_0}}e^{C(\theta)}\cos\theta \ Q\left(\sqrt{\frac{E_s}{N_0}}\cos\theta\right)\right\} \end{aligned} \tag{4.18}$$

where

$$C(\theta) = -\frac{E_s \sin^2\theta}{2N_0}$$

To fairly assess performance over the Eve angles, error ratios are made equal in Bob's direction by reducing (4-ary case) or increasing (8-ary case) the total power in the DPSK transmission. This adjustment allows us to compare the information beamwidth, and, in general, a system would not transmit more power than necessary to achieve a certain target error rate at the intended receiver.

The simulation results agree well with the theoretical SAPM bounds. It is also quite evident that SAPM has a significantly smaller range of angles over which errors are low enough for reception. For a symbol error ratio of 0.001, the 4-SAPM information beamwidth is about 12° versus 24° for 4-DPSK. The effect gets more pronounced as modulation order increases: at the same error level, the 8-SAPM beamwidth is about 4° versus about 14° for 8-DPSK.

4.5 Secrecy capacity and security

Given that SAPM has been developed as a technique to provide increased system security, it is important to measure this increase and compare it to other secure tactics. Section 4.4 addresses this from an implementation viewpoint, using errors over time as a benchmark at a given transmission rate. In this section, we provide a way to determine that transmission rate and quantify the theoretical secrecy capacity of a given channel.

For a general discrete memoryless channel (DMC) with inputs $\widehat{\mathcal{P}} = \mathcal{P}_1, \ldots, \mathcal{P}_M$ and outputs $\mathbf{B} = \mathbf{b}_1, \ldots, \mathbf{b}_K$, the mutual information $I(\mathcal{P}_m; \mathbf{b}_i)$ is defined as the information about event $\mathcal{P}_m$ provided by the occurrence of $\mathbf{b}_i$ [49]. Then $I(\widehat{\mathcal{P}}; \mathbf{B})$ is the average mutual information over the entire sets. Mutual information represents a rate of communication, and, in our calculations, it has units of bits per channel use (bpcu).

The secrecy rate is defined as the difference between Bob's and Eve's mutual information, and the maximum rate over all possible input distributions is the secrecy capacity [52]. When the rate is positive, the system has the potential for secure communications [53]. For this investigation, we take the same view as [54] and analyze the secrecy rate itself independent of coding. The most straightforward means of leveraging a positive secrecy rate for system security is to transmit at a code rate greater than the capacity supported by Eve's channel and less than that of Bob's channel [54]. In the following derivations, we make use of two different models for Eve's knowledge, resulting in a typical secrecy rate as well as a secrecy lower bound. In both cases, we assume that receivers are static over a single symbol period.

We begin with the typical operation model, which continues to use the same assumptions as Section 4.4. Constellation estimation is again done with a clustering algorithm over a set number of bits for all receivers, including Bob. Given our input alphabet of $\widehat{\mathcal{P}}$ at the transmitter and observations $\mathbf{w}$ after the demodulator, the detector output is $\mathbf{B}$. From [49], the average mutual information (again, with implied φ-dependence) is

$$I(\widehat{\mathcal{P}};\mathbf{B}) = \sum_{m=1}^{M}\sum_{i=1}^{M} P(\mathbf{b}_i|\mathcal{P}_m)P(\mathcal{P}_m)\log_2\frac{P(\mathbf{b}_i|\mathcal{P}_m)}{P(\mathbf{b}_i)} \tag{4.19}$$

$$P(\mathbf{b}_i|\mathcal{P}_m) = \sum_{l=1}^{L} P(l)P(\mathbf{b}_i|\mathcal{P}_m, l) \tag{4.20}$$

The probability that $\mathbf{b}_i$ is the outcome when $\mathcal{P}_m$ is transmitted with the l^{th} excitation equals the intersection of events $J_{i,k}$, each of which denote the occurrence that $\mathbf{w}$ is closer to $\mathbf{b}_i$ than any other member of $\mathbf{B}$. The derivation for $P(\mathbf{b}_i|\mathcal{P}_m, l)$ is similar to the steps from Equation (4.15):

$$P(\mathbf{b}_i|\mathcal{P}_m, l) = P\left(\bigcap_{\substack{k=1\\k\neq i}}^{M} J_{i,k}\right) \tag{4.21}$$

$$P(J_{i,k}) = P\left(\zeta_i^{(l)} < \zeta_k^{(l)}\right) = \int\limits_{\tilde{\phi}}\int\limits_{\tilde{\theta}} p_{\Theta,\Phi}(\theta,\phi \mid \mathcal{P}_m, l)\, d\theta d\phi \tag{4.22}$$

where

$$\{\tilde{\theta},\tilde{\phi}\} = \left\{[\theta,\phi] \mid \tau_i^{(l)}(\theta,\phi) - \tau_k^{(l)}(\theta,\phi) < 0\right\}$$

The bound on the intersection is the minimum of $\left[P(J_{i,k_1}),\ldots,P(J_{i,k_{M-1}})\right]$ [51]. Then this defines an upper bound on Eve's mutual information for the nominal model.

For the second model, we make the assumption that all Eves know exactly how the received SOP from each excitation maps to the true message. In other words, $\mathbf{g}_{m,l}(\varphi)$ must be known for all m, l, and φ. It is an even more pessimistic view than assuming that a secret key is known to adversaries because SAPM never needs to broadcast or share $\mathbf{g}_{m,l}(\varphi)$ with Bob. In fact, in addition to l selection being pseudorandom at each symbol step, Alice may alter any or all subsets within $\mathbf{g}_{m,l}(\varphi)$ at any time without affecting Bob. In any case, we still address this scenario to serve as a secrecy rate floor, or an overall lower bound, for SAPM under the worst-case assumptions. We may now use a continuous output channel model instead of the DMC, so the mutual information is defined as

$$\begin{aligned} I(\widehat{\mathcal{P}};\mathbf{W}) = \frac{1}{M}\sum_{m=1}^{M}\int_{\theta}\int_{\phi}\sum_{l=1}^{L}\frac{1}{L}p_{\Theta,\Phi}(\theta,\phi|\mathcal{P}_m,l) \\ \times \log_2\left[\frac{M\sum_{n=1}^{L}p_{\Theta,\Phi}(\theta,\phi|\mathcal{P}_m,n)}{\sum_{r=1}^{M}\sum_{u=1}^{L}p_{\Theta,\Phi}(\theta,\phi|\mathcal{P}_r,u)}\right]d\theta d\phi \end{aligned} \tag{4.23}$$

where $\mathbf{W} = \mathbf{w}_1,\ldots,\mathbf{w}_m$ continuous Gaussian distributions for each corresponding member of $\widehat{\mathcal{P}}$.

There are two different regions over transmitter look angle that are most susceptible to eavesdroppers: the angles close to Bob and the power peaks around the radiation sidelobes. We define two different ways to calculate the mutual information in Eve's channel based on either region of risk.

The range close to Bob occupies a portion of the main beam, so the limits are set by the first-null beamwidth ($FNBW$), about $\pm 25°$, minus a region of $\pm 4°$ around Bob [23]. Over this range, the *mean* mutual information is used for Eve, representing an average risk over the main beam. The region around Bob may be adjusted depending on frontend implementation; for the testing discussed in Chapter 6, the 6-bit phase shifters on the BFN have a nominal overall error of $\pm 5°$ [55]. This translates to a maximum boresight angle tolerance of $\pm 3.5°$ over the range of reasonable beamsteering in the front hemisphere. Therefore, the region that may include Bob is this angular tolerance with some margin to account for tracking errors and other factors. This definition also allows convenient comparisons to the secrecy rates in [54]. As the range that may include Bob is reduced, the secrecy rates for all methods studied here would approach 0, with the implication that Eve may get closer and closer to Bob's location. Of course, at the limit where Eve and Bob occupy the same look angle, all the physical layer solutions that we have considered so far would be ineffective from a security standpoint, including beamforming. This scenario is outside the scope of our investigation, but, in general, systems may choose to incorporate encryption or channel key generation along with a base physical layer solution.

The regions for potential sidelobes span the rest of the azimuthal plane in front of the transmitter, or ±90°, minus the main beam range. The *maximum* mutual information is used for Eve over these limits, representing the highest risk at a sidelobe.

Figure 4.9 shows the main lobe secrecy rates discussed in this section plotted alongside the theoretical rates for two other 4-ary modulation methods. This time, beamforming is done using PolSK, but DPSK is used with DM instead of PSK, as in [22], to be consistent with the other noncoherent techniques. In general, the radiated power density is higher in the main beam than in the sidelobes, so data security in this region may be weighted with higher importance for many applications. Figure 4.10 shows the secrecy rates at the sidelobes. In both cases, SAPM is seen to outperform the other methods for the typical case (red line with "x") above E_b/N_0 of about 5 dB (main beam) and 15 dB (sidelobes). For the worst-case model (solid red line), SAPM performance is slightly better or roughly the same as PolSK in the main beam, and better than DM below about 12 dB E_b/N_0. The sidelobe performance of PolSK around $E_b/N_0 = 10$ dB is best, but some of the reasons for that can be understood from the analysis in Section 4.6. In later characterization (see Section 5.2.3) when we reduce the fraction of power in the secondary SOP, SAPM is seen to outperform PolSK across the entire range of E_b/N_0, even for its worst-case model.

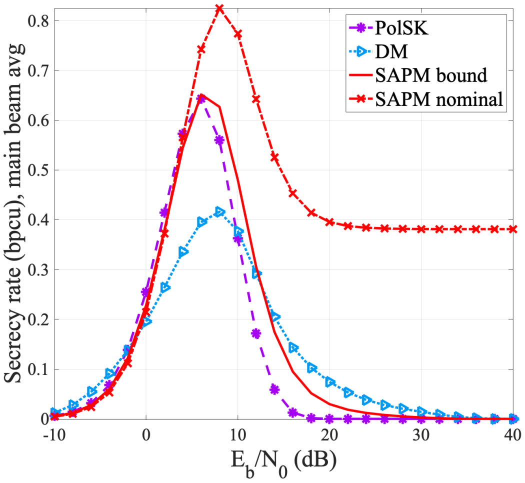


Figure 4.9: Average risk in the main lobe: 4-SAPM secrecy rates compared to other methods, calculated using the mean Eve mutual information across $\{\varphi \mid -25° \leq \varphi \leq -4° \bigcup 4° \leq \varphi \leq 25°\}$; 1/2 of P_{RF} in secondary SOP

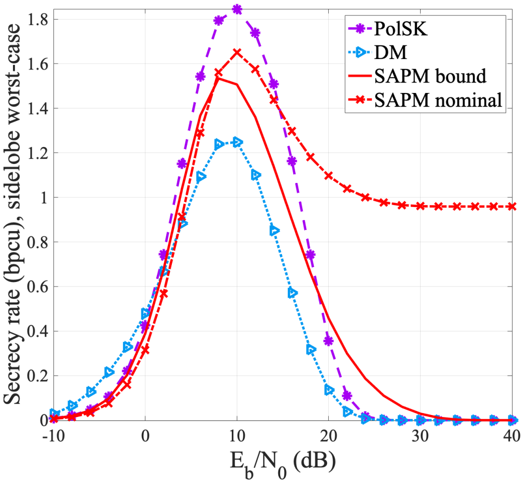


Figure 4.10: Risk at a sidelobe: 4-SAPM secrecy rates compared to other methods, calculated using the maximum Eve mutual information across $\{\varphi \mid -90° \leq \varphi \leq -30° \bigcup 30° \leq \varphi \leq 90°\}$; 1/2 of P_{RF} in secondary SOP

Figure 4.11 is a plot of the minimum E_b/N_0 required for Eve to correctly demodulate the intended symbol versus increasing communication rate. The code rate is assumed to be unity. For the typical SAPM case, if two bits can be successfully transmitted per symbol, it is evident that Eve may not be able to demodulate correctly no matter how low the noise floor.

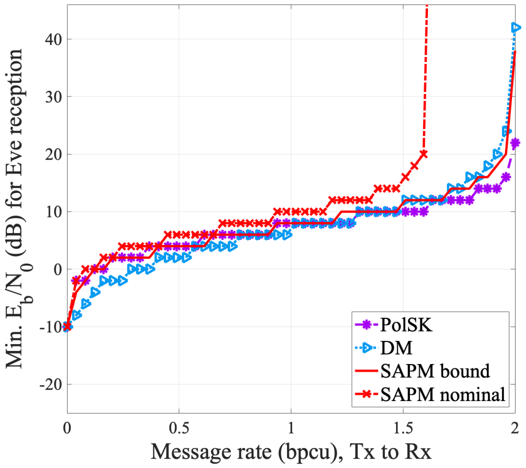


Figure 4.11: Required SNR per bit for Eve to correctly receive 4-ary modulated signals based on mean Eve mutual information in the main beam; 1/2 of P_{RF} in secondary SOP

4.6 System energy tradeoffs

Energy use and system efficiency are always relevant concerns when weighing added security against the power overhead required. In the context of our investigation, we define efficiency at the system level as

$$\eta = \frac{P_{out}}{P_{in}} = \frac{P_{out}}{[P_{RF} + P_{DC}]} \tag{4.24}$$

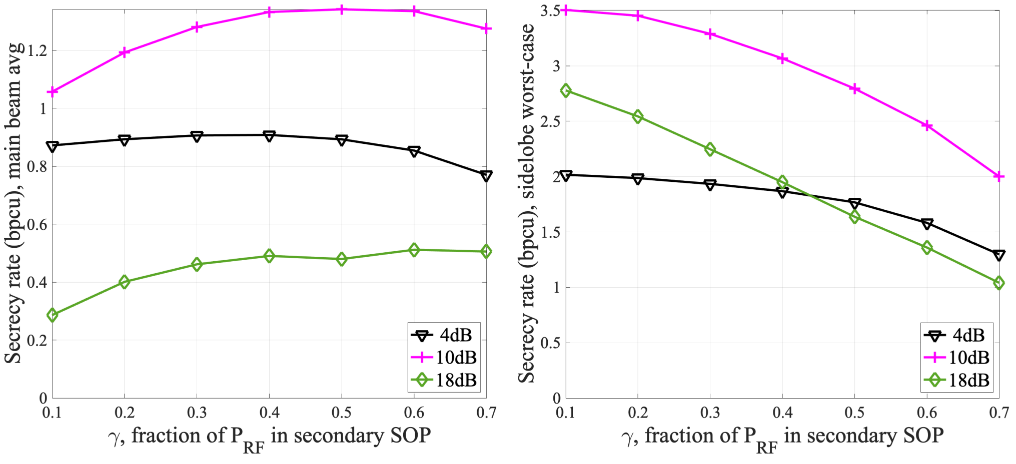
where P_{RF} and P_{DC} are RF and DC power inputs at the transmitter, respectively, and P_{out} is RF power received. Factors influencing η include modulation scheme, processor requirements, antenna/array gain, impedance/polarization match, and other channel considerations.

A significant flaw of DM is the reduction in the degrees of freedom to provide directive power, as the array's phase shifters are used for data modulation rather than beamforming as traditionally defined [22]. P_{RF} must be higher to achieve the equivalent receiver SNR as a conventional BFN, since transmit antenna gain would be lower. In general, artificial noise-based methods have lower efficiency due to the increased P_{RF} required for the useless data sent everywhere and the increased P_{DC} overhead for noise generation [3]. The most efficient method is pure beamforming, but from the analysis so far, it is often subject to lower security levels than SAPM.

4.6.1 Secondary polarization power allocation

It is intuitive that SAPM sits somewhere between beamforming and DM/artificial noise from the standpoint of efficiency, with a large dependency on the amount of transmitted RF power devoted to the secondary simultaneous polarization. The transmitting SAPM array may be designed using the same steps as a BFN for PolSK, but the power budget should target antenna gain levels that account for the loss in the secondary.

In Figure 4.12, we plot secrecy rates over increasing RF power in the secondary SOP (the coefficient γ) for three different received E_b/N_0 levels at Bob. We adopt the worst-case model from Section 4.5 as a conservative secrecy lower bound for SAPM. Again, the two plots represent the main beam, i.e., the angles around Bob, and the angles where radiation sidelobes occur. The same ranges are used for calculating the maximum Eve information at



(a) (b)

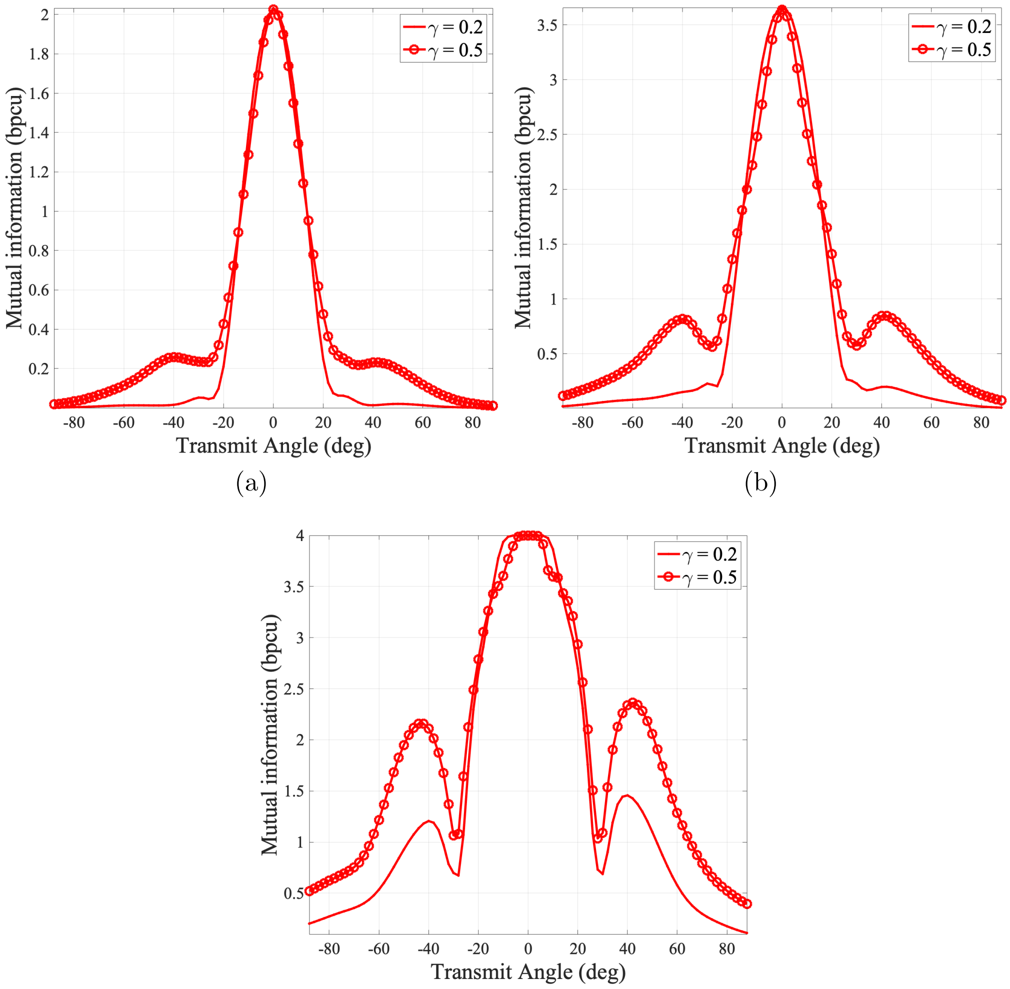
Figure 4.12: SAPM secrecy rates versus the amount of power allocated to the secondary SOP (a) over the main beam and (b) at the sidelobes; E_b/N_0 at Bob = 4, 10, and 18 dB; $M = 16$; calculated using SAPM secrecy lower bound

a sidelobe, $\{\varphi \mid -90^\circ \leq \varphi \leq -30^\circ \bigcup 30^\circ \leq \varphi \leq 90^\circ\}$, and the mean Eve information over the main beam, $\{\varphi \mid -25^\circ \leq \varphi \leq -4^\circ \bigcup 4^\circ \leq \varphi \leq 25^\circ\}$.

There is a tradeoff in risk between the main beam and sidelobe regions as the secondary SOP power is increased. While secrecy rates tend to peak around $\gamma = 0.4 - 0.6$ for the main beam, the sidelobe rates are always decreasing with γ. The first observation, Figure 4.12(a), is explained by the narrowing of the information beam explored in Section 4.4.3, which becomes more prominent as γ is increased. However, the received power near the radiation nulls also increases, so this begins to decrease the mean secrecy rate again after $\gamma >\ 0.5$.

The decreasing secrecy rates observed in Figure 4.12(b) for all three per-bit SNR levels is due to the inevitably increased power received at the sidelobe regions with increasing γ. Figure 4.13 may help with visualizing these trends; it shows the SAPM mutual information across transmitter look angle for the patch array for the same three Bob E_b/N_0 levels. While a higher γ produces a narrower main beam around Bob, it is clear in all three plots that the mutual information levels around the nulls and the sidelobes are also increased. Increasing information for Eve in these locations obviously lowers secrecy rates and counteracts the narrowing effect on the main beam.

Despite this sidelobe power increase, the received SOPs will not be correct,



(a)

(b)

(c)

Figure 4.13: SAPM mutual information at $\gamma = 0.2$ and 0.5 across look angle for the patch array at (a) $E_b/N_0 = 4$ dB, (b) $E_b/N_0 = 10$ dB, and (c) $E_b/N_0 = 18$ dB; $M = 16$; calculated using SAPM secrecy lower bound

nor will they remain consistent with each intended symbol; see Section 4.3.2. However, due to the use of the worst-case model, where Eve knows the mapping functions $\mathbf{g}_{m,l}(\varphi)$, the assumption is that Eve knows the correspondence between the true symbol and the demodulated signal even if it is closer to another nominal symbol location. Whether this view is too pessimistic is discussed in Section 4.4.3, but the aim is to provide a lower bound for SAPM secrecy rates.

Applications may choose γ based on how they specifically weigh the perceived risk in either region. For the remainder of this chapter, we continue to use $\gamma = 0.5$, but in Chapter 5, performance using different levels of secondary power is explored.

4.6.2 Energy comparison

It is reasonable to question the theoretical efficiency of SAPM versus other secure methods, including cryptography-based techniques. There are two important points that must be understood in the following analysis, however—comparing physical layer solutions to upper layer strategies seems to indicate that one or the other must be chosen. In reality, physical and upper layer methods may be combined, which is included in our analysis in the form of security-oriented beamforming and encryption. The second point is that the comparison is strictly based on efficiency and not necessarily apples-to-apples because these systems offer varying levels of actual security. They may also incur other costs that would not be accounted or controlled for, such as the hardware requirements for many physical layer solutions and the secondary key-sharing channels and coordination required by cryptography.

With these caveats in mind, we proceed to simulate data transmission in an idealized control environment using several secure methods. The inherent assumptions in the simulation are:

- Communication is LOS in an AWGN channel
- Overhead for modulation, demodulation, and RF frontend is not included (common to all methods)
- Encryption and decryption energies, E_{enc} and E_{dec}, include energy used per bit and overhead (divided by total bits)

- Both transmitters and receivers are perfectly impedance and polarization matched to their corresponding antennas
- Receiver antennas are omnidirectional, $G_{Rx} = 0$ dB
- All methods require an algorithm to determine array excitations; energy consumption strictly for this processing is not included

Several of these assumptions may seem too idealized, but they are necessary approximations for a practical comparison in simulation. More in-depth studies removing one or more of these assumptions may be conducted in the future to produce a more accurate picture.

For now, we select security-oriented beamforming (alone and combined with two types of encryption methods), DM, and SAPM as points of comparison. The RF energy transmitted per symbol is calculated by approximating the average power over the symbol period T_s as constant and using the Friis transmission equation [23]:

$$E_{Tx} = P_{RF} T_s \tag{4.25}$$

$$P_{RF} = \frac{(4\pi R)^2 P_{out}}{g_{Rx} g_{Tx} \lambda^2} \tag{4.26}$$

where $g_{Rx(Tx)}$ is the linear receive (transmit) antenna gain, R is the range or distance between the transmitter and receiver, and λ is the free-space wavelength.

The total energy for each method is

$$E_{\text{BFN}} = E_{Tx} N_s \tag{4.27}$$

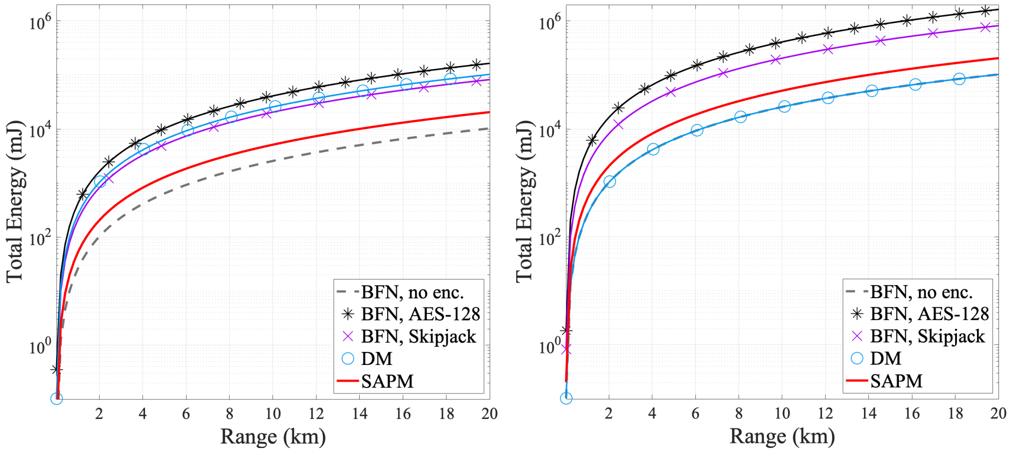
$$E_{\text{BFN,enc}} = E_{enc} N_{b,enc} + E_{dec} N_{b,enc} + E_{key} N_{b,key} + E_{Tx} N_{s,enc} \tag{4.28}$$

$$E_{\text{DM}} = g_{Tx} \left[E_{Tx} N_s \right] \tag{4.29}$$

$$E_{\text{SAPM}} = \frac{1}{1-\gamma} \left[E_{Tx} N_s \right] \tag{4.30}$$

where N_s is the total number of symbols transmitted representing raw message bits, $N_{b,enc}$ is the total number of bits after encryption, $N_{s,enc}$ is the total number of symbols after encryption, E_{key} is the energy per bit to generate the key, and $N_{b,key}$ is the length of the key.

In Figure 4.14, we plot the energy usage versus range in kilometers for a single transmitter/single receiver system using each of the methods. One



(a) (b)

Figure 4.14: Energy consumption versus transmission range for a transmitter with (a) 10 dB of antenna gain and (b) 0 dB of antenna gain sending one message byte: $M = 2$, received SNR $= 5$ dB, bandwidth $= 10$ MHz

byte of plaintext data is transmitted with binary modulation, with other system specifications reported below the figure. The two encryption strategies selected are the widely-used Advanced Encryption Standard (AES) with a 128 bit key and Skipjack [56]. The former is a block cipher popular among government and civil applications, and the latter is a lightweight algorithm developed to target more limited devices. All encryption-related consumption data is derived from and calculated using [56], [57].

Again, the portion of power in the secondary SOP, γ, is kept at 0.5 for this simulation. As this decreases, the energy usage unsurprisingly approaches that of the BFN without encryption. In this idealized case, it appears that the additional energy required for encryption does outweigh the doubling of transmitted power for SAPM. However, these results vary with the amount of data transmitted and the encryption key size, number of rounds, etc. [56]. While Figure 4.14(a) uses 10 dB for transmit array gain, slightly lower than the gain of the array in Figure 4.5, Figure 4.14(b) removes the transmit array gain to show consumption without any benefit of directional transmitted power.

4.7 Noise floor and spectral efficiency

The level of noise power in the environment affects SAPM performance in two distinct ways [58]. First, the secrecy rates offered by SAPM are comparatively higher at higher per-bit SNR, as seen in Figures 4.10 and 4.9. This is evident from the difference in Bob and Eve's mutual information regardless of M (modulation order). Improved secrecy with higher SNR is important because eavesdropping risk is intuitively greatest in low-noise environments, and there is a tradeoff between transmitted power and secrecy in traditional systems. This tradeoff is seen to be more forgiving for SAPM, especially considering the nominal use case in Figure 4.9.

The second effect manifests if system designers choose to maximize spectral efficiency. With increasing SNR, higher orders of modulation can be used while still hitting error rate thresholds at Bob. Increasing modulation order significantly improves the level of security provided by SAPM by further narrowing the information beamwidth.

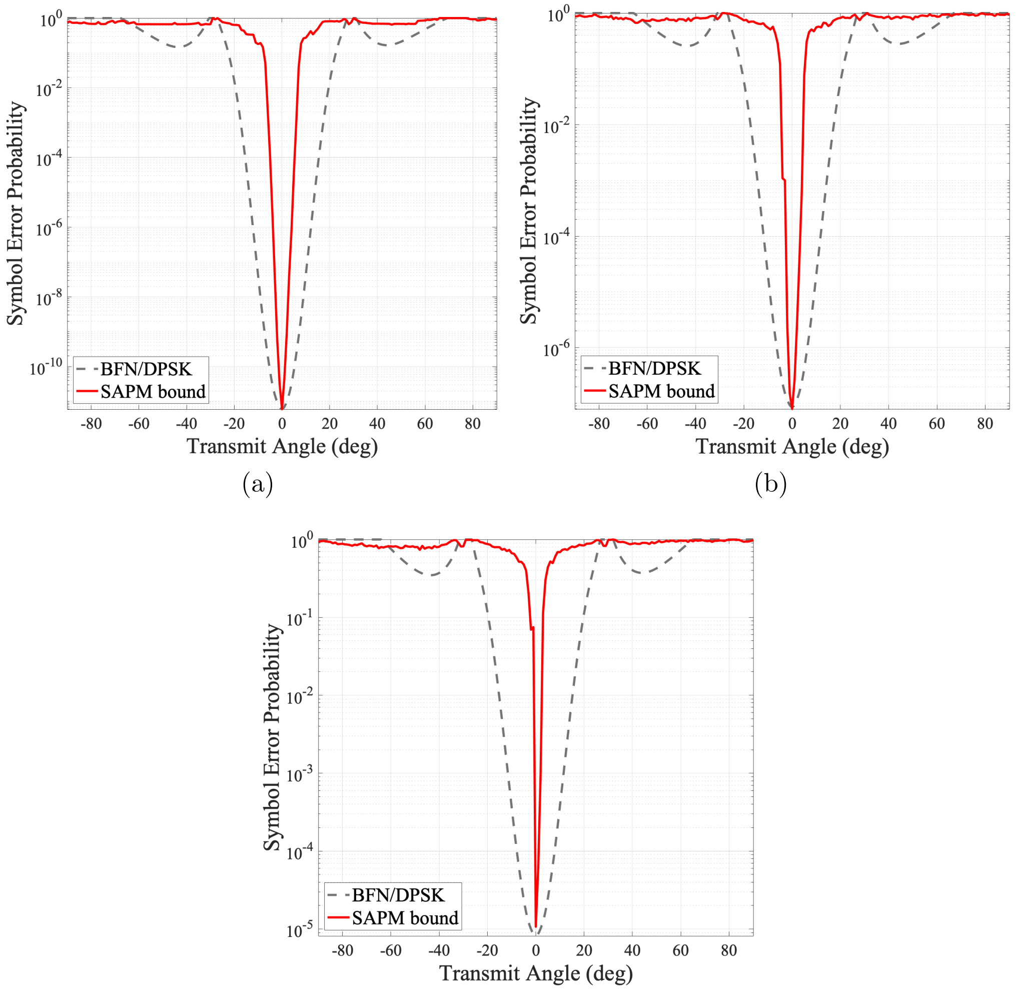
In Figure 4.15, we plot the error bounds derived based on the theory from Section 4.4 for 8-SAPM, 16-SAPM, and 32-SAPM across azimuth using the same array and simulation geometry described in Section 4.3.3. Again, overlaid on the plots are theoretical uncoded symbol error probabilities for a conventional BFN using the same physical array and setup, transmitting DPSK with corresponding M [49].

Tables 4.2 and 4.3 summarize the information beamwidths for error requirements of 10^{-2} and 10^{-3} at various received per-bit SNR levels. Where the error probabilities are too high for the requirement ($M = 16$ at $E_b/N_0 = 12$ dB), the widths are marked "N/A".

Table 4.2: Symbol error rate = 10^{-2} information beamwidths for the same array using beamforming with DPSK versus SAPM

	$M = 4$		$M = 16$	
E_b/N_0, dB	BFN, °	SAPM, °	BFN, °	SAPM, °
12	24.2	14.8	N/A	N/A
18	38.6	20.0	29.6	7.5
28	50.9	20.7	45.8	7.5

With higher M, it is evident that SAPM information beamwidths are



(a) (b)

(c)

Figure 4.15: Symbol error probability over azimuth for SAPM compared to beamforming at (a) $M = 8$, (b) $M = 16$, and (c) $M = 32$; average SAPM $E_b/N_0 = 20$ dB for Bob at $\varphi = 0°$; E_b/N_0 at other angles for both methods may be found from Figure C.1 in Appendix C

Table 4.3: Symbol error rate $= 10^{-3}$ information beamwidths for the same array using beamforming with DPSK versus SAPM

	$M = 4$		$M = 16$	
E_b/N_0, dB	BFN, °	SAPM, °	BFN, °	SAPM, °
12	13.0	6.1	N/A	N/A
18	33.9	17.1	22.0	5.7
28	49.1	20.7	42.9	7.5

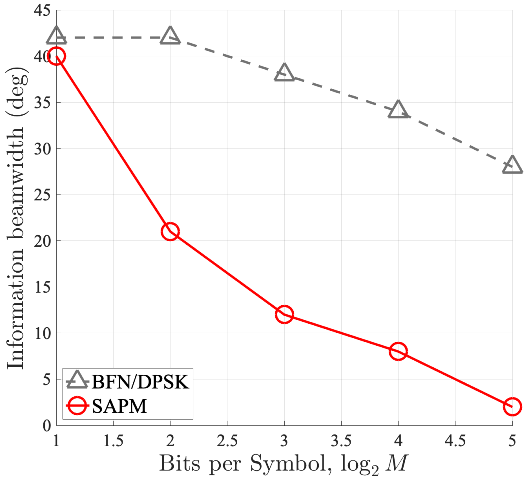


Figure 4.16: Information beamwidths with increasing modulation order for SAPM compared to beamforming, at an uncoded symbol error rate of 10^{-2}; average SAPM $E_b/N_0 = 20$ dB for Bob at $\varphi = 0°$; E_b/N_0 at other angles for both methods may be found from Figure C.1 in Appendix C

increasingly narrower when compared to traditional beamforming. Figures 4.16 and 4.17 report the widths for both methods versus the number of bits transmitted per symbol, or $\log_2 M$, at uncoded error rates of 0.01 and 0.001. The performance margin, in terms of the difference between BFN and SAPM beamwidths, is always positive and increases dramatically beyond binary modulation. At the upper end of the range reported, beamwidth narrowing appears to slow for SAPM because it is actually getting close to our sampling resolution of 1 degree.

The error probability, and therefore the SNR and XPD, required at Bob serves as the spectral efficiency ceiling. For example, if the minimum uncoded symbol error probability is 10^{-6}, we can see from Figure 4.15(c) that we cannot use 32-SAPM.

Our current work only considers equipower symbols, corresponding to a single spherical shell in Stokes space. In low-noise environments, we may further increase the order of modulation by transmitting at discrete total power levels, evaluated as the sum of power in both orthogonal received signals. These may be visualized as multiple Poincaré spheres enclosing each other like Russian nesting dolls, with noise mapped to the radial direction dictating their proximity. Absolute phase information may also be used in addition to absolute power, essentially creating a fourth dimension for modulation. The resulting scheme would be treated as a combination of

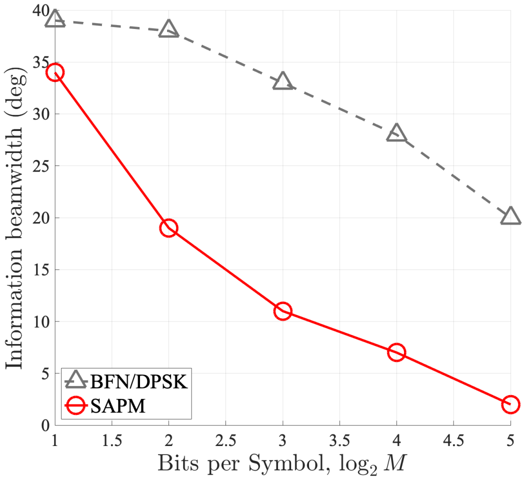


Figure 4.17: Information beamwidths with increasing modulation order for SAPM compared to beamforming, at an uncoded symbol error rate of 10^{-3}; average SAPM $E_b/N_0 = 20$ dB for Bob at $\varphi = 0°$; E_b/N_0 at other angles for both methods may be found from Figure C.1 in Appendix C

QAM and PolSK for applications with sufficiently high SNR, and may be the topic of future investigations.

4.8 Summary

This chapter is an introduction to SAPM and its basic operation. It includes a brief review of wave polarization fundamentals and the Poincaré sphere representation. We propose paths to higher-order modulation using SAPM and discuss potential hardware architecture. SAPM performance is analyzed at a theoretical level and compared to other modulation methods, and it is found to be superior under a number of metrics, including secrecy and error rate.

CHAPTER 5

ANTENNAS FOR POLARIZATION MODULATED TECHNIQUES

Current polarization-based wireless systems almost always utilize vertical and horizontal dipoles as a means of generating or receiving multiple polarization states. However, choosing a different antenna design may benefit the system in a number of ways. Strictly speaking, the orthogonal dipoles fall within the category of dual-polarized antennas, which are sensitive to a continuum of polarizations depending on their feed configurations. These antennas usually allow polarization-diverse systems to cut their antenna element count by a factor of two, which is more significant when the system uses arrays.

In this chapter, we analyze the polarization-related performance exhibited by different types of dual-polarized antennas. Section 5.1 discusses benchmarks that are relevant for any polarization modulated method, including SAPM and PolSK. Representative geometries from the chosen dual-polarized antenna categories are evaluated within these metrics at 2.4 GHz. Section 5.2 uses these antennas in simulations of SAPM operation to compare their performance with respect to secrecy rates and information beamwidths. To our knowledge, this is the first time that the significance of antenna geometry and design has been discussed with respect to polarization modulated techniques. All results and data presented in this chapter are from full-wave simulations done in HFSS, so coupling effects are accounted for in the case of arrays.

5.1 Antenna elements and radiated polarization

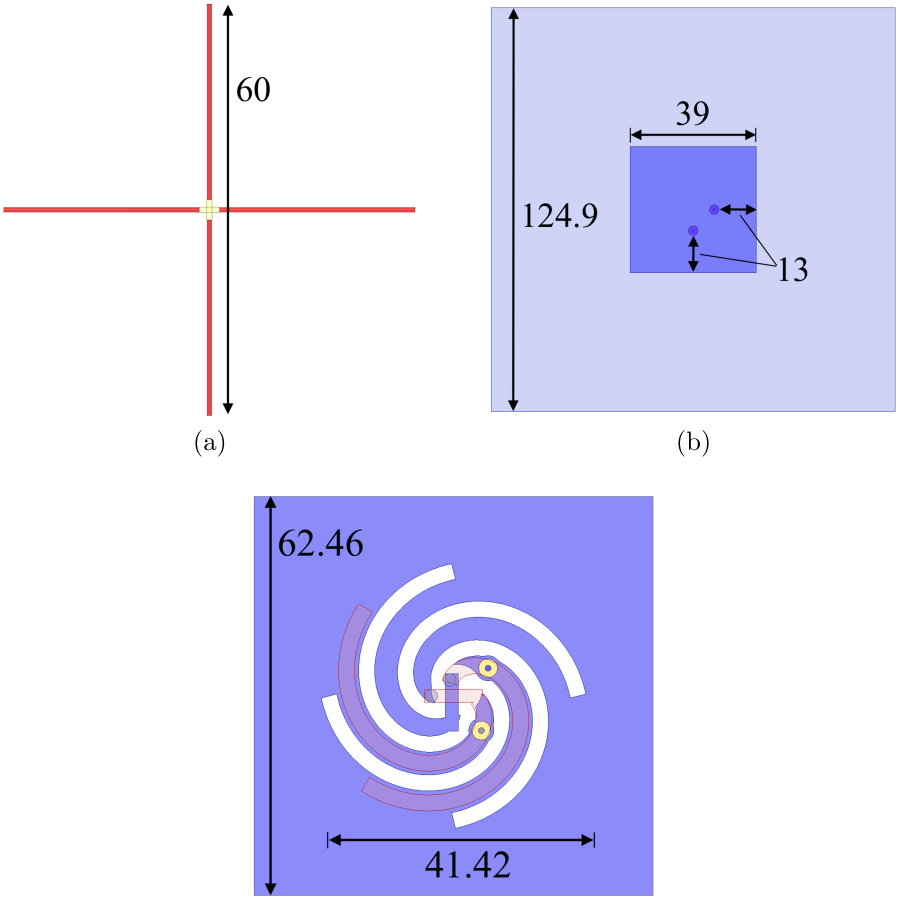
Research on the wireless adaptation of PolSK is at a fairly early stage, even though it has a long history in optics, so the antenna requirements are not well-documented for this scheme. In this section, we consider benchmarks to evaluate the performance of a given antenna in any wireless system that leverages multiple polarizations for communication. For the practical implementations of SAPM and PolSK, it is important to understand how these metrics will limit the overall system's performance.

As noted, it is most practical to use one or more dual-polarized antennas. These can be grouped into three categories: collocated orthogonal antennas, antennas that are fed at two or more locations to excite different modes, and single antennas based on periodic structures. We choose one from each category to study in this chapter: a crossed dipole, a four-arm Archimedean spiral, and a dual-fed microstrip patch. All elements are sized and optimized for a design frequency of 2.4 GHz.

The crossed dipole antenna is the most ubiquitous one in PolSK literature. Strictly speaking, it is actually two dipoles with a shared phase center, each with its own feed. A model of the crossed dipole used in this study is shown in Figure 5.1(a), although its full extent (0.48λ) is truncated for visibility in the picture.

The second antenna, a rectangular microstrip patch, usually radiates a linearly polarized (LP) electric field in the direction of its feed axis [23]. When another feed is incorporated on the perpendicular axis, an LP mode is excited in that direction as well. The relative phase and amplitude between the feeds may be altered to radiate fields in any nominal SOP. In general, its length along the feed axis should be half the effective wavelength [23]. Since we have orthogonal feed axes, the design was optimized for impedance match and gain with parametrics, resulting in the feed locations and outer square dimensions shown in Figure 5.1(b). A 3.175 mm Rogers Duroid 5880 substrate was selected during design based on its low loss (dissipation factor of 9E-4) and thickness to prevent warping. The ground plane is a full wavelength in extent and is only partially shown.

The last dual-polarized antenna, a four-arm spiral, is generally the most space-efficient design because it is based on angular dimensions instead of lengths. Most dual-polarized spiral designs found in the literature today still draw very heavily on the seminal works in this area [59]. We use a cavity-backed, equivalent slot version of this antenna for ease of feeding, which is shown in Figure 5.1(c) [60]. Despite its nominal left-hand oriented turns, the extra arms support more modes that allow this antenna to radiate other SOPs. For example, both LHCP and RHCP may be excited with equal-amplitude ±90° of phase on the two feeds. The opposite mode radiates



(a) (b)

(c)

Figure 5.1: Geometries of the three representative dual-polarized antennas used in the analysis with dimensions given in mm; all elements are parallel to the yz-plane with broadside at $\vartheta = 90°, \varphi = 0°$

because the waves travel almost in-phase for most of the spiral (due to the feed locations) and only radiate after they reflect from the ends of the arms, at which point they are right-handed [59]. Again, the precise feed locations and dimensions were set via impedance match and gain optimization in HFSS parametrics.

5.1.1 Poincaré spread

We first consider the distribution of demodulated data around their nominal constellation points on the surface of the Poincaré sphere. While this distribution is a function of the noise on the received signals, it also varies

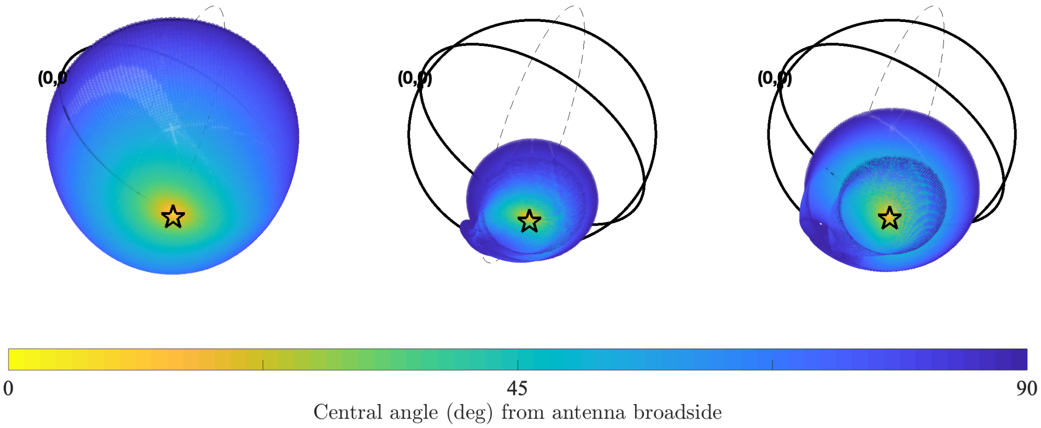


Figure 5.2: Poincaré sphere visualization for far-field radiation using (l-r) the crossed dipole, four-arm spiral, and square patch; nominal transmitted SOP (star) $\mathcal{P} = 1\angle{-90^\circ}$

deterministically over look angle with the properties of the antenna. For clarity, we will only consider the effects of the transmitting antenna, assuming an ideally matched receiving antenna, but in general both will impact performance. Since most antennas are reciprocal, transmit and receive patterns are the same and the analysis can be extended to include receiving antennas by the angle of arrival in the far field.

The mathematics associated with the Poincaré sphere in the Stokes coordinate system were presented in Chapter 4. As shown in Figure 4.1b, we define the north pole of the sphere at 90° latitude as left-hand circular polarization (LHCP) and the south pole as RHCP. The equator consists of LP at various tilt angles, from horizontal at 0° longitude to vertical at 180° longitude. Latitudes between 0° and 90° that are not on the equator or the poles represent left-hand elliptical polarizations (LHEP), while those between 0° and -90° are RHEP [46].

To help visualize polarization state over transmit angle for the models in Figure 5.1, simulation results from HFSS are shown in Figure 5.2 for antenna excitations corresponding to RHCP, or $\mathcal{P} = 1\angle{-90^\circ}$, for the three test antennas. The SOP is sampled at far-field receiver locations over the entire frontal hemisphere of all antennas, and no noise is added. The color map in Figure 5.2 linearly corresponds to the angular distance from the sample point to antenna broadside.

We can map in Stokes space the true transmitted SOP for all far-field look

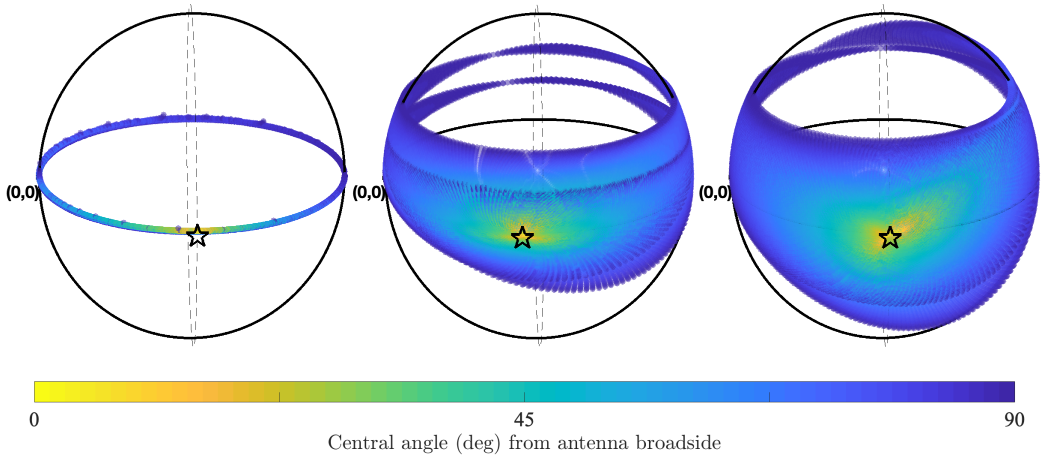


Figure 5.3: Poincaré sphere visualization for far-field radiation using (l-r) the crossed dipole, four-arm spiral, and square patch; nominal transmitted SOP (star) $\mathcal{P} = 1\angle 0°$

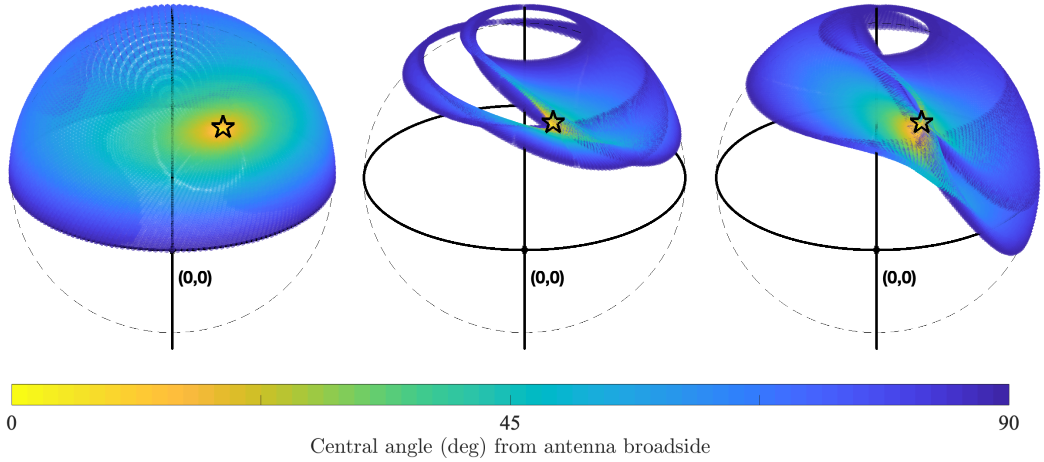


Figure 5.4: Poincaré sphere visualization for far-field radiation using (l-r) the crossed dipole, four-arm spiral, and square patch; nominal transmitted SOP (star) $\mathcal{P} = 0.4\angle 68°$

angles in physical space for any set of excitations to understand the variation. Figures 5.3 and 5.4 show the results for nominal transmitted SOPs of 45° tilted LP and LHEP, respectively.

The spheres are rotated to give a better view of the red regions (closest to broadside and the correct polarization), and the latitude/longitude of $(0, 0)$ is marked to clarify the orientation. The equator and the 0° and 180° longitude lines are solid, and the ±90° longitude lines are dashed.

These figures provide evidence that the intended polarization state is only accurate at broadside. However, it is clear that the polarization state "spreads" differently in each column, corresponding to each antenna, and the shape of this spread depends on the intended state. Looking at Figure 5.2, it is obvious that the SOPs received around the crossed dipole have much greater variation because more surface area is covered on the Poincaré sphere. The cluster around the correct SOP (RHCP at the south pole) is much tighter for the four-arm spiral over all look angles, even at angles in-plane with the antenna (90° from broadside, or dark blue). However, applications are generally not interested in performance in this range—for a skyward-facing antenna, these would be the angles close to the horizon, where radiated power is very low anyway.

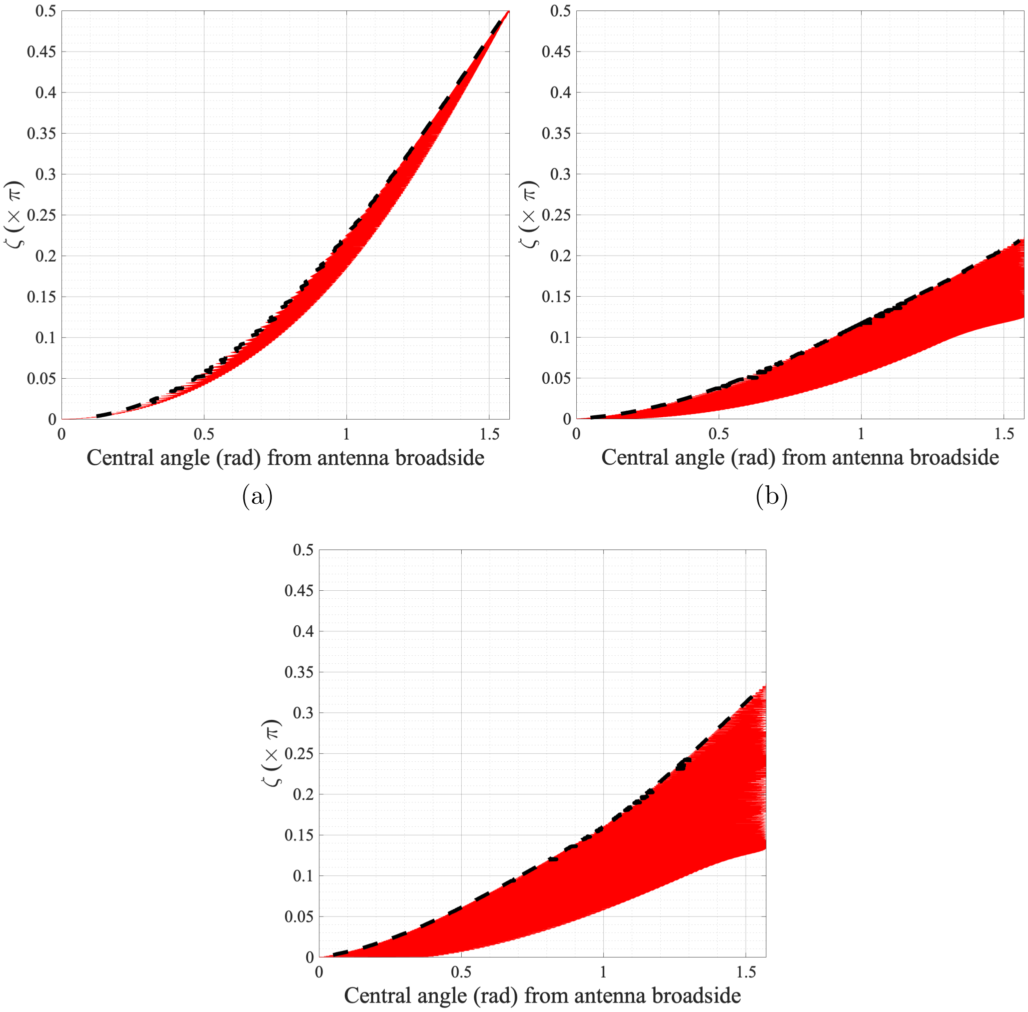
We define a metric, the Poincaré spread, to characterize SOP characteristics in Stokes space over a domain in physical space that may be arbitrarily set. That domain can be bounded by an upper limit and a lower limit, both central angles in physical space defining great-circles centered at broadside. Over the transmission angles that fall into this domain, the behavior in Stokes space at each point may be defined by the arclength ζ from its SOP (a location on the Poincaré surface) to the nominal SOP at broadside. For this study, the sphere's radius is always one and radian central angle is equal to arclength. We take the linear slope of the maximum ζ envelope between the two limit angles as an indication of how closely SOPs cluster around the correct state as one travels away from the target transmission angle:

$$\text{Poincaré spread} = \frac{\max\{\zeta_{hi}\} - \max\{\zeta_{lo}\}}{\angle hi - \angle lo} \tag{5.1}$$

In Equation (5.1), the transmission angle limits $\angle hi, \angle lo$ are in radians, and maximum ζ corresponds to worst error in received SOP. If there is no distortion in polarization with look angle, the Poincaré spread would be zero. High levels of distortion with look angle would result in spread values closer to one. In general, $\angle lo$ could be set to zero, encompassing an entire region around the receiver.

Figure 5.5 plots the Stokes space arclengths for received polarizations over all far-field angles in the front hemisphere of the three test antennas, where each ζ is plotted in red and the black dashed line is a fitted envelope of the maximum arclengths.

Table 5.1 includes results for the Poincaré spread calculated from simulations using the three antennas of interest, at the SOPs of RHCP, 45° LP, and



(a) (b) (c)

Figure 5.5: ζ, arclengths in Stokes space between received SOP and the nominal SOP $\mathcal{P} = 1\angle{-90^\circ}$ (at antenna broadside), across angles in the front hemisphere for the (a) crossed dipole, (b) four-arm spiral, and (c) square patch; Poincaré spread is the slope of the black dashed line between two chosen limit points on the x-axis

LHEP. These are generally in line with the observations from the Poincaré sphere visualizations, which indicate that the crossed dipole tends to have greater SOP variations with angle. However, from Figure 5.3, it is difficult to tell whether the dipole's cluster around the nominal SOP is tighter than the others—visually, it appears this might be the case. From the spread calculation, we find that it does drift away from the correct answer more quickly, even if the SOPs tend to stay linear.

Table 5.1: Poincaré spread using 5°/40° for lower/upper look angles for the antennas from Figure 5.1; three nominal transmitted SOPs $\mathcal{P} = 1\angle{-90^\circ}$ (RHCP), $\mathcal{P} = 1\angle 0^\circ$ (LP, 45° tilt), and $\mathcal{P} = 0.4\angle 68^\circ$(LHEP)

	Dipole	Spiral	Patch
RHCP	0.18	0.10	0.15
LP, 45° tilt	0.25	0.17	0.23
LHEP	0.24	0.14	0.10

We generally desire the Poincaré spread to be as low as possible, because higher variation with look angle in the range of interest could mean that calibration bits must be sent with higher frequency. As SOPs drift from their nominal locations in Stokes space, receivers must constantly correct for this bias to avoid receiving bits in error. A tighter cluster of points around the correct Stokes location also means that higher modulation orders may be considered for the application, as this will introduce more valid nominal symbol locations on the sphere. This effect will be seen in Section 3.3b, where the dipole's expected error probabilities are higher than those of the other antennas, even when controlling for received power. A large spread in Stokes space generally complicates efforts to achieve an acceptable error rate for all polarization-modulated methods.

5.1.2 Error vector magnitude

The data from Section 5.1.1 illustrates the deterministic polarization distortion discussed in Section 4.3.2 of Chapter 4. Based on the results so far, it is clear that even a single antenna may have significant directionality when it comes to radiated SOP. In general, a PolSK receiver can tolerate some level of imperfection before demodulation results in errors. The natural question

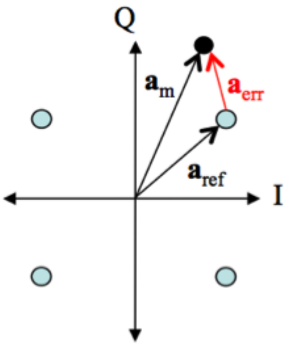


Figure 5.6: Illustration of error vector magnitude (EVM) calculation using the IQ-plane [61]

of how to determine the domain of operation for each of our test antennas, or the antenna field of view (FOV), is addressed in this section.

To quantify the level of imperfection, we select the error vector magnitude (EVM) because it carries relevant information regarding the nature of the signal's deviation from its ideal symbol location. The EVM is the difference between a sample's transmitted constellation location and the actual one demodulated by the receiver. Equation (5.2) is the RMS EVM over K total collected points. It is the mathematical definition commonly used in the industry for conventional I/Q demodulation and will be used to explain the concept [61].

$$EVM_{\text{RMS,IQ}} = \sqrt{\frac{\sum_{k=1}^{K} |\mathbf{a}_{ref,k} - \mathbf{a}_{Rx,k}|^2}{\sum_{k=1}^{K} |\mathbf{a}_{ref,k}|^2}} \tag{5.2}$$

Vector $\mathbf{a}_{ref}$ is where the ideal symbol location is relative to the origin, and $\mathbf{a}_{Rx}$ is the actual received location after demodulation. The error vector $\mathbf{a}_{err}$ is $\mathbf{a}_{ref} - \mathbf{a}_{Rx}$, and referencing it to the ideal $\mathbf{a}_{ref}$ produces the EVM. Figure 5.6 conveys this in graphical form.

We have already noted that for our spherical modulation surface, the error vector is ζ, an arclength or a central angle in the case of our unity-radius sphere. The spherical distance of interest is between the nominal SOP, $\mathcal{P}_{ref}$ and the SOP at the k^{th} receiver. The adaptation of RMS EVM to Stokes space is

$$\text{EVM}_{\text{RMS},\zeta} = \sqrt{\frac{\sum_{k=1}^{K} \left[\zeta\left(\mathcal{P}_{ref,k}, \mathcal{P}_{Rx,k}\right)\right]^2}{K\pi^2}} \tag{5.3}$$

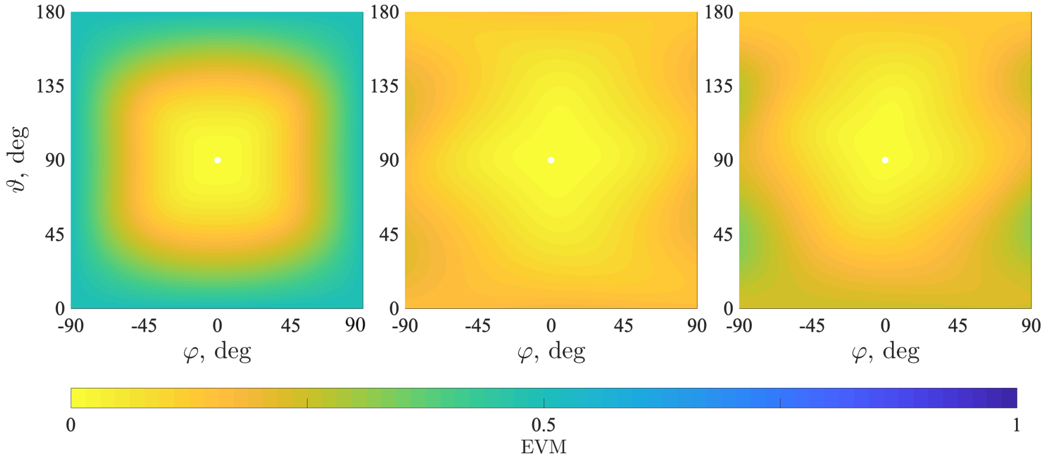


Figure 5.7: EVM over the entire front hemisphere for (l-r) the crossed dipole, four-arm spiral, and square patch; nominal transmitted SOP $\mathcal{P} = 1\angle{-90^\circ}$

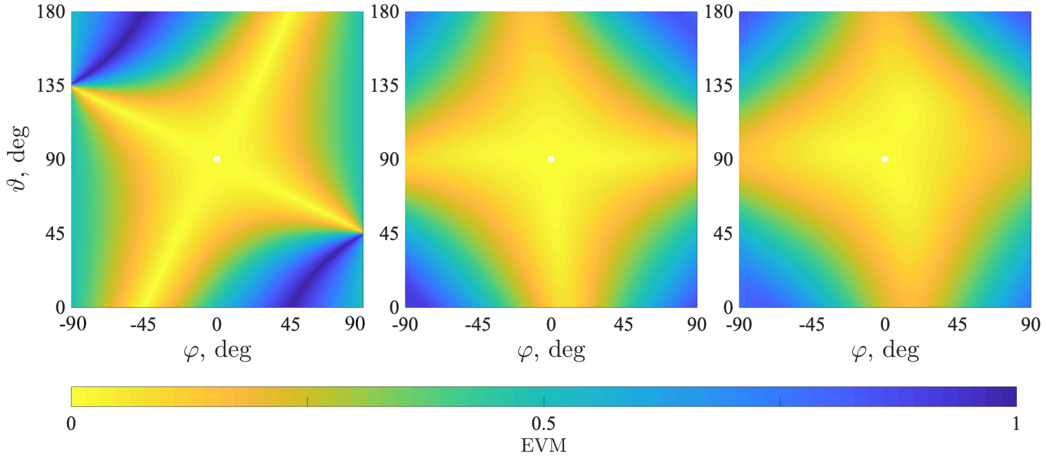


Figure 5.8: EVM over the entire front hemisphere for (l-r) the crossed dipole, four-arm spiral, and square patch; nominal transmitted SOP $\mathcal{P} = 1\angle 0^\circ$

where the range of $\text{EVM}_{\text{RMS},\zeta}$ is between 0 and 1. Figures 5.7–5.9 include plots of EVM over transmission angle evaluated for the antennas from Figure 5.1, when configured respectively in RHCP, 45° LP, and LHEP. We do not include noise in these simulations, so K is simply 1 and the error magnitude is solely due to polarization distortion over transmission angle in the frontal hemisphere of the antenna. The vertical axis represents the angle off $\hat{z}$ (ϑ) and the horizontal axis spans azimuth (φ).

The color map has yellow representing the correct state, or EVM $= 0$, and dark blue as the maximum EVM, or the orthogonal polarization. Table 5.2

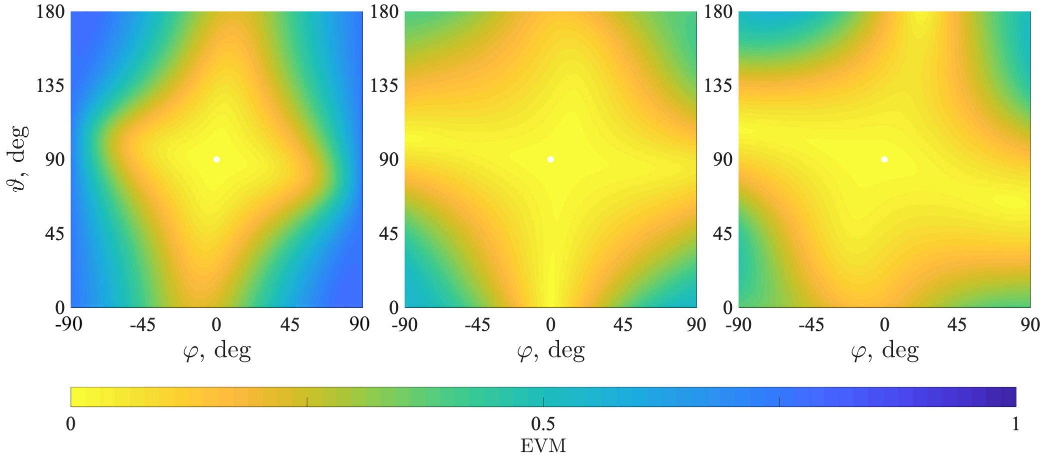


Figure 5.9: EVM over the entire front hemisphere for (l-r) the crossed dipole, four-arm spiral, and square patch; nominal transmitted SOP $\mathcal{P} = 0.4\angle 68°$

shows the mean EVM over all steradians for each of these configurations. While the averaging is done over (ϑ, φ), the EVM is calculated in Stokes space. These numbers are somewhat inflated by the fact that near the plane of the antenna, the SOP is potentially very far from the intended state and, in some cases, close to the orthogonal state.

For each polarization simulated, even LP, the average error is lower for the spiral and the patch. These results are summarized in Table 5.2.

Table 5.2: Mean EVM over all transmission angles in the front hemisphere for the antennas from Figure 5.1 and three nominal transmitted SOPs $\mathcal{P} = 1\angle{-90°}$ (RHCP), $\mathcal{P} = 1\angle 0°$ (LP,45° tilt), and $\mathcal{P} = 0.4\angle 68°$(LHEP)

	Dipole	Spiral	Patch
RHCP	0.29	0.10	0.14
LP, 45° tilt	0.30	0.26	0.26
LHEP	0.36	0.16	0.16

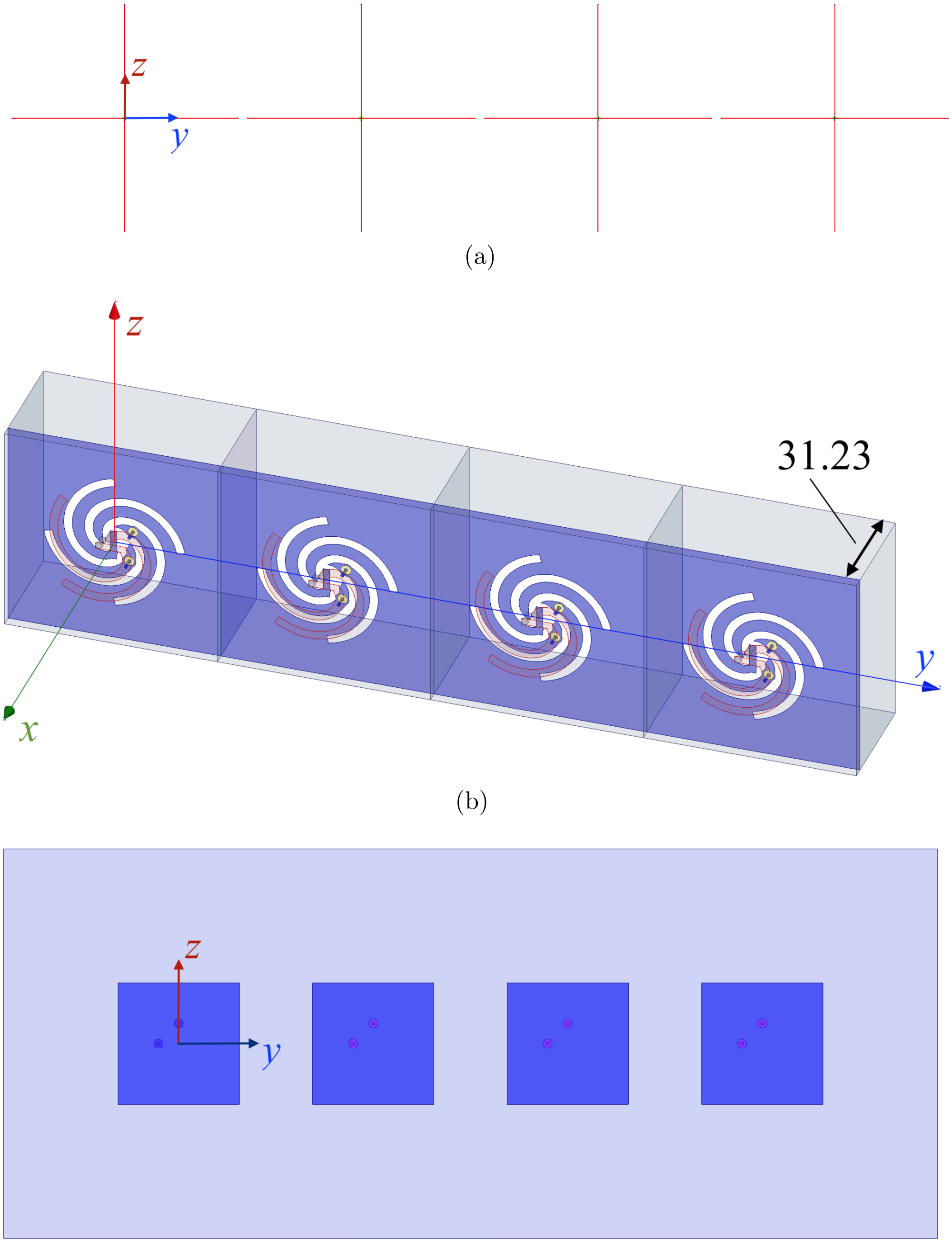
In general, to calculate the FOV from the EVM data, a maximum EVM may be set at the threshold where the intended receiver detects an incorrect symbol, similarly to how error probabilities are used in Chapter 4. The FOV is then the set of transmission angles $[\vartheta, \varphi]$ that fall into the domain bordered by the maximum EVM. However, it is important to remember that this section only treats the EVM at the antenna level, i.e., how the antenna characteristics affect the radiation relative to broadside, which is our reference. At the system level, analysis similar to Section 4.4 must be done over SNR to determine the true received EVMs.

In this study of isolated antenna impact, it can be seen from Figure 5.9 that for certain SOPs and elements, a region of low EVM may extend all the way to the plane of the antenna at certain perpendicular cuts. It is also interesting to observe the narrower low-EVM regions of the crossed dipole, which may indicate better security, at least for the single-element transmitter. However, FOV is traditionally evaluated based on received SNR (effectively radiated power when controlling the channel). In that context, the dipole is the *least* directive, with the lowest gain and the most broad FOV. Later in the chapter, in Section 5.2, we account for both effects to see the resulting impact to system performance.

5.1.3 Cross-polarization discrimination

EVM is useful for RF design as a performance benchmark, but it is worthwhile to explore the wave characteristics that affect the error vector and how isolated element behavior translates to arrays. A shift in the demodulated SOP in Stokes space from the nominal point may be thought of as a decrease in the power of the co-polarization (the nominal SOP) and an increase in the cross-polarization (its antipodal SOP). A traditional metric for polarization purity in antenna design is the cross-polarization discrimination, or XPD. This is defined as “magnitude of the relative power of the cross-polarized pattern with respect to the co-polarized pattern at a given angle” [62]. In this section, we compare the XPD of each of the test antennas alone and in a linear $\lambda/2$-spaced array to show the impact of the antenna element on the total array’s performance. The array geometries, with broadside at $\varphi = 0°$, are shown in Figure 5.10, and their radiation patterns are plotted in Figure 5.11.

Figures 5.12 to 5.14 report the XPD over transmission angle for the crossed dipole, four-arm spiral, and square patch. Overlaid with each plot is the array XPD using the respective elements. It should be noted that these are simulated with excitations for a nominal transmitted SOP of RHCP at broadside, and the shapes/levels of XPD will vary for other polarizations.



(a)

(b)

(c)

Figure 5.10: Four element $\lambda/2$-spaced arrays of the antenna elements from Figure 5.1: (a) crossed dipoles, (b) four-arm Archimedean spirals, and (c) square microstrip patches; dimensions given in mm

Visually, the trend from these plots indicates that the dipole (alone) yields a slightly narrower region of very high XPD at broadside, while the spiral (alone) has lower XPD at its peak but slopes down much more gently, never

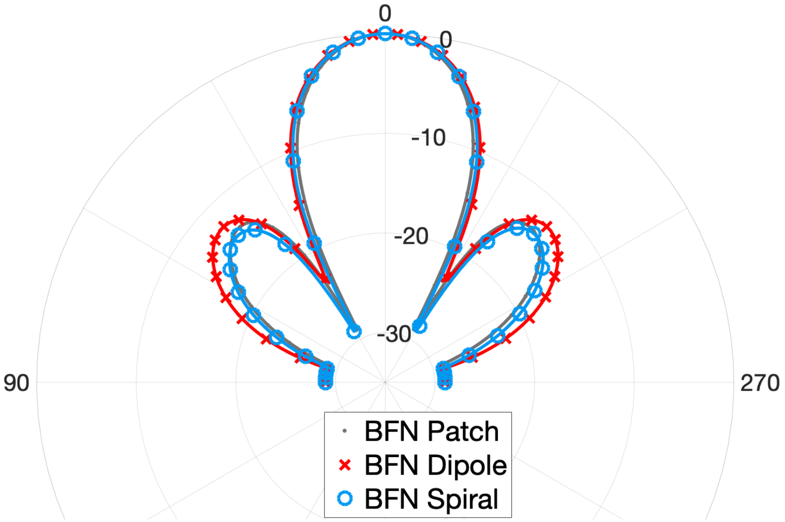


Figure 5.11: Normalized RHCP gain, dB, for the linear $\lambda/2$-spaced arrays from Figure 5.10; input excitations correspond to boresight angle $\varphi = 0°$

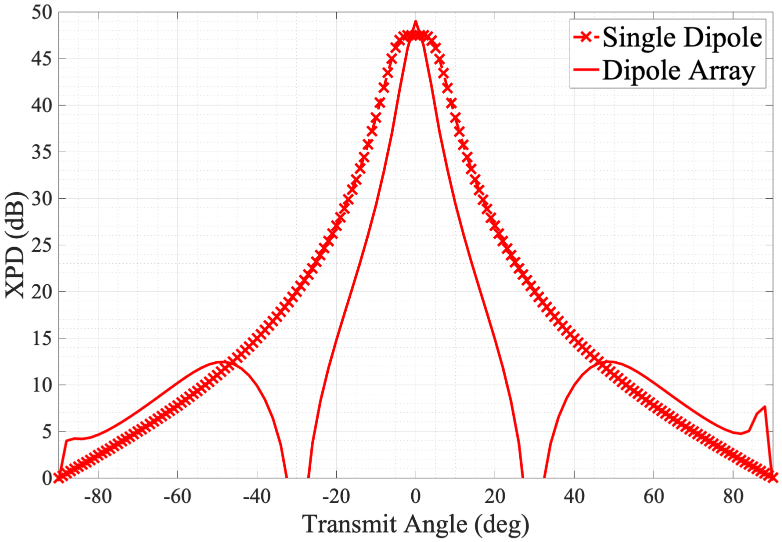


Figure 5.12: Cross-polarization discrimination over the front hemisphere for the crossed dipole, single element and array of N=4; co-polarization $\mathcal{P} = 1\angle{-90°}$ (RHCP); cross-polarization $\mathcal{P} = 1\angle 90°$(LHCP)

dipping below 10 dB even at the horizon. The patch has performance somewhere between these two extremes. This confirms our FOV observations from Section 5.1.2.

For the arrays, the XPD difference in level and shape become much more pronounced because element-to-element coupling produces higher-order effects. The crossed dipole array XPD generally looks like the single-element case with a narrower main region and nulls where deep array nulls should

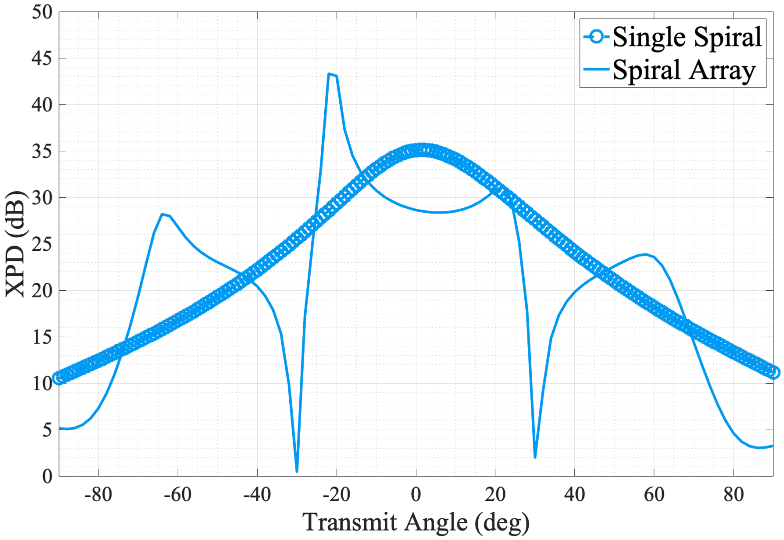


Figure 5.13: Cross-polarization discrimination over the front hemisphere for the four-arm spiral, single element and array of N=4; co-polarization $\mathcal{P} = 1\angle{-90^\circ}$ (RHCP); cross-polarization $\mathcal{P} = 1\angle 90^\circ$(LHCP)

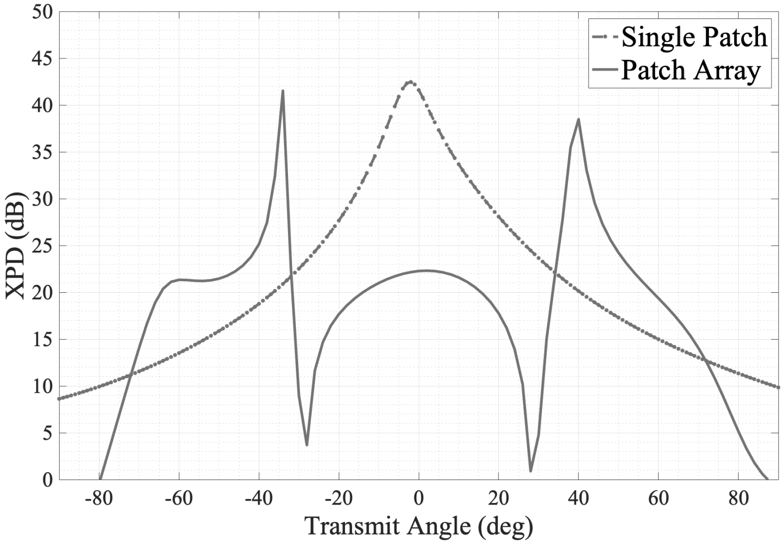


Figure 5.14: Cross-polarization discrimination over the front hemisphere for the square patch, single element and array of N=4; co-polarization $\mathcal{P} = 1\angle{-90^\circ}$ (RHCP); cross-polarization $\mathcal{P} = 1\angle 90^\circ$(LHCP)

be. This is reminiscent of the element radiation pattern to array radiation pattern relationship, but only because the cross-polarized components are so low compared to the co-polarized wave. When we observe the spiral array XPD, we can see higher XPD corresponding to where sidelobes exist in the power patterns. There is an interesting dip at broadside and then an off-center peak, both due to a misalignment in the peaks/nulls between the co- and cross-polarized components. The most different case is the patch array, where the cross-polarized components are clearly low away from broadside, but in the main lobe, XPD is much worse than for the single patch. This is in line with previous authors' observations of the relatively high cross-polarized radiation from microstrip patch antenna arrays, where the coupling effects between neighboring elements tend to be more complicated [23].

It is important to note that XPD carries no information about absolute power or the radiated pattern. Each data point is a power ratio, but the co- and cross-polarized patterns may change independently for a given antenna, and high XPD can very well coincide with low power to combine for a less pronounced effect on security. We document ranges of XPD that may in theory form a FOV in Table 5.3, but practical implementation requires a transmitter FOV that also accounts for power and radiation patterns. The analysis in this section is meant to highlight the underlying wave behavior of our EVM-defined FOV, which needs to be considered along with power for polarization-modulated techniques.

Table 5.3: Range of transmitter look angles (deg) where XPD < 15 dB; single antennas (Figure 5.1) and N=4, $\lambda/2$-spaced linear arrays; nominal $\mathcal{P} = 1\angle{-90^\circ}$ (RHCP)

	Dipole	Spiral	Patch
Single element	80	141	114
Array	40	60	48

5.2 Antenna elements and SAPM impact

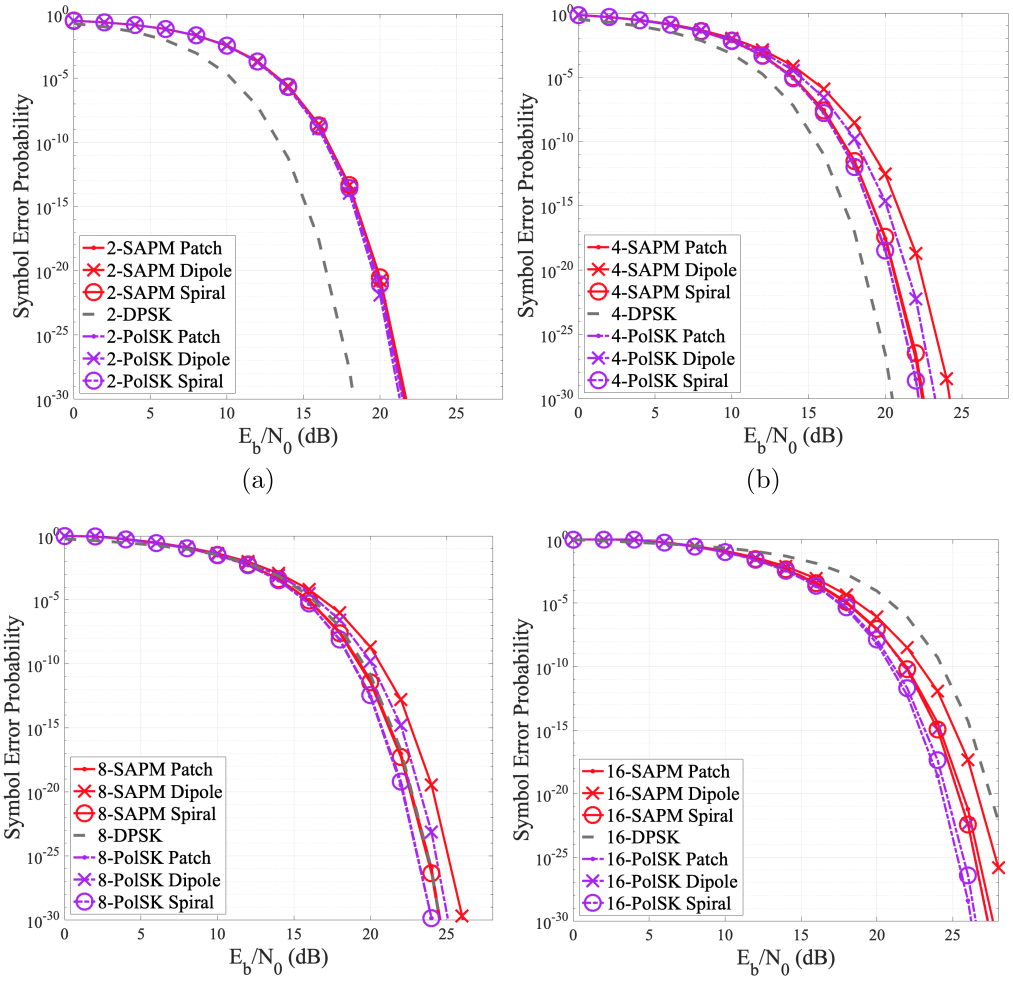
The analysis in Section 5.1 may be used to evaluate antennas for any variant of polarization modulation, including SAPM and PolSK. Now we turn our focus to antenna characteristics that specifically impact SAPM in a different way than conventional methods. In general, for I/Q modulation, the variable that affects performance as measured by error probability is E_s/N_0, or per symbol SNR. Converting E_s/N_0 to per bit SNR, or E_b/N_0, and treating that as the independent variable, we may directly compare error probabilities across modulation methods regardless of order M. This effectively removes the antennas in the path because they are accounted for in the signal energy levels. Any polarization mismatches in these systems are simply power reduction factors similar to impedance mismatches: to be optimized in construction and implementation, but to be ignored in the theoretical analysis.

The situation is more complicated for polarization modulated techniques. Error performance is still affected by SNR, which would shrink or enlarge the radius of the Poincaré sphere and disperse the symbols on its surface in a distribution around the nominal constellation, but now there is also a warping of the nominal constellation on the sphere's surface. This effect is due to cross-polarized wave components that increase away from antenna broadside, as discussed in Section 5.1.2, depolarization from multipath [27], or radiated cross-polarized components, discussed in 5.1.3. These factors are all antenna-dependent, so there is a level of approximation in any analysis where the discussion in Section 5.1 is ignored.

5.2.1 Error probabilities at Bob

SAPM has to consider all of the factors discussed so far in addition to the secondary SOP characteristics when they are superposed with the primary SOP. Since radiation patterns are always a function of antennas and arrays/BFNs (if applicable), there is an additional link between an SAPM system and its RF hardware.

To illustrate our point, Figure 5.15 includes plots of symbol error probability versus E_b/N_0 for these three types of methods at various M. Obviously, the conventional DPSK system is agnostic to antenna type because we control E_b/N_0 at each data point. However, SAPM and PolSK are quite obviously affected by antenna choice as M increases and nominal symbol locations get closer together on the sphere, as predicted by the analysis in Section 5.1.1. The improved XPD of the dipole element at broadside (Bob) observed in



(a) (b)

(c) (d)

Figure 5.15: Symbol error probabilities over E_b/N_0 at Bob ($\varphi = 0°$) for the different types of antenna arrays from Figure 5.10

Section 5.1.3 is actually evident in binary PolSK and SAPM, but the resulting decreased error probability is quite small compared to the orders of magnitude in the differences at the higher modulation orders. In the following sections, we investigate how these effects translate to system-level SAPM performance.

5.2.2 Information beamwidth versus antenna type

The information beamwidth, as defined in Section 4.4, serves as an indication of security in the main beam at a specified error rate. In that section, when determining this metric for one type of antenna array, we were careful to equalize the error at Bob by adjusting received SNR levels for the beamformer (nominal E_b/N_0 is always reported for SAPM reception at Bob). This type of adjustment is done when comparing information beamwidths to control for decreasing beamwidth with increasing Bob error, a trivial and misleading effect. We assume transmitted P_{RF} may be changed to achieve the required error rate at the receiver.

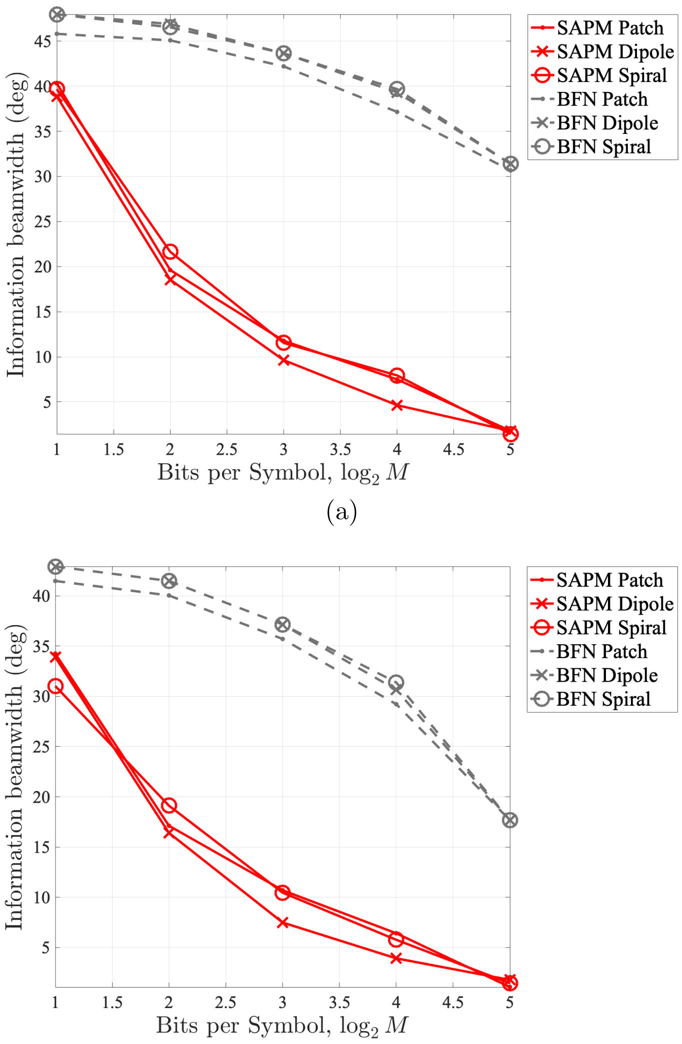
In this section, we additionally equalize error probabilities for each array type, with the SAPM patch array error at Bob serving as the reference. Figure 5.16 shows the beamwidths over increasing spectral efficiency for SAPM compared to conventional beamforming.

It is evident that, regardless of antenna design, the gap between SAPM and DPSK is quite large and increases with modulation order until it is essentially resolution-limited at 5 bits per symbol, or $M = 32$. For SAPM, the beamwidths are generally smaller for the crossed dipoles, which seems counterintuitive until the analyses from Sections 5.1.2 and 5.1.3 are considered. The EVM- and XPD-related performance for the crossed dipole helps explain, in part, why it produces a narrower region of correct data around Bob. Another important effect for SAPM information beamwidth is the shape of the secondary SOP nulls, which are affected not only by antenna geometry and XPD, but also by the accuracy of null placement, i.e., tolerance in the frontend components. In this study, the patterns are from HFSS, so the array excitations are ideal, but phase and amplitude biases and their impact on SAPM may be an interesting path for future work.

For the BFN, the trend is as expected. DPSK error rates and therefore information beamwidths are strictly determined by the varying levels of total received power *over look angle.* Since the patch array has a slightly narrower main (radiation) beam and higher gain than the others, when Bob E_b/N_0 is adjusted to equate error probability, the patch yields a slightly narrower information beam.

5.2.3 Secrecy rate versus antenna type

Sidelobe levels are not considered when evaluating information beamwidth—only the main lobe (usually directed at Bob) is analyzed at a given error



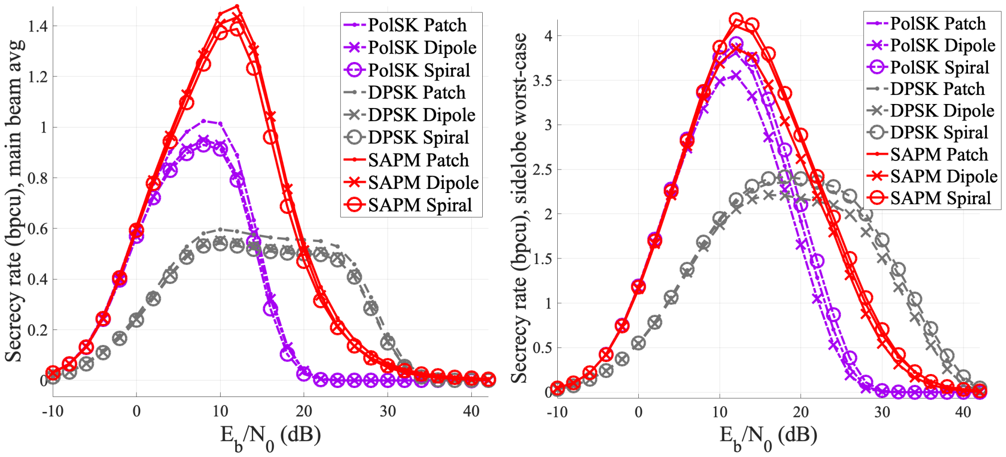
(a)

(b)

Figure 5.16: Information beamwidths for Bob at 0° with increasing modulation order for SAPM compared to beamforming with DPSK, at an uncoded symbol error rate of (a) 10^{-6} and (b) 10^{-12}; average SAPM $E_b/N_0 = 28$ dB at Bob for the patch array (reference); E_b/N_0 at other angles for both methods may be found from Figure 5.15

rate. Thus, other metrics, such as secrecy rate, should also be included when making tradeoffs for system design.

Following the approach in Section 4.5 to calculate mutual information and secrecy rates, we now consider the impact of the antenna element. In an effort to be conservative with assumptions, the analysis in this section will only consider the most pessimistic case described in Section 4.5 (Eve has more a priori information than Bob). The same angular ranges are used for



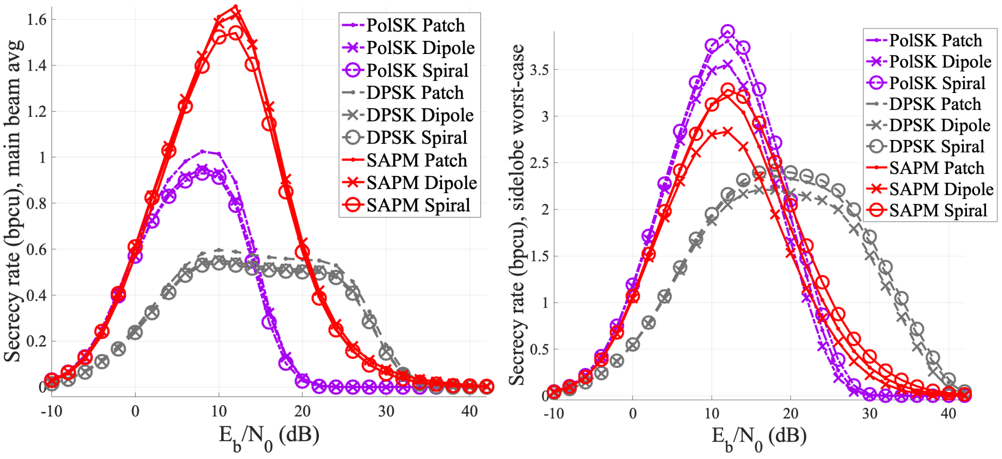
(a) (b)

Figure 5.17: Secrecy rates over E_b/N_0 for Eve: (a) average risk in the main beam and (b) maximum risk at a sidelobe for different types of antennas in a linear $\lambda/2$-spaced array; $M = 32$; calculated using SAPM secrecy lower bound; 1/5 of P_{RF} in secondary SOP

calculating the maximum Eve information at a sidelobe and the mean Eve information over the main beam. Specifically, with Bob situated at $\varphi = 0°$, $\{\varphi \mid -90° \leq \varphi \leq -30° \bigcup 30° \leq \varphi \leq 90°\}$ constitute the Eve angles for the sidelobe range, and the main beam Eve angles are $\{\varphi \mid -25° \leq \varphi \leq -4° \bigcup 4° \leq \varphi \leq 25°\}$. Secrecy rates versus E_b/N_0 over these two regions of risk are displayed in Figure 5.17, for SAPM compared to beamforming with PolSK and DPSK using our test antennas.

It is observed for the three antennas that SAPM has better secrecy performance than the other methods (both main beam and sidelobes). Building on the analysis from Section 5.1.3, the elements with the lowest individual gain, the dipoles, have the highest sidelobes. This translates to the dipole array achieving the worst secrecy rates when compared to the other antennas for all transmission schemes in Figure 5.17b. Rates for the spiral and the patch are very similar, as can be expected from their comparable patterns in Figure 5.11.

There is a tradeoff between performance in the two regions of risk, discussed in Section 4.6. In general, increasing the amount of power in the secondary SOP improves secrecy in the main beam (to an extent) at the cost of lowering secrecy in the sidelobes. Figure 5.18 illustrates this tradeoff when we increase the power devoted to the secondary to half the total power.



(a) (b)

Figure 5.18: Secrecy rates over E_b/N_0 for Eve: (a) average risk in the main beam and (b) maximum risk at a sidelobe for different types of antennas in a linear $\lambda/2$-spaced array; $M = 32$; calculated using SAPM secrecy lower bound; 1/2 of P_{RF} in secondary SOP

It is clear that while secrecy rates are higher in the main beam for SAPM, compared to when just 1/5 of total power is dedicated to the secondary, the secrecy rates in the sidelobe regions are lower than PolSK. When considering a per-bit SNR range from about 12 dB to 18 dB, there is a more pronounced difference (between 0.5 and 1 bit per channel use) in the rates for SAPM between the dipole and the spiral. This may seem like a small increment, but it can nevertheless impact the "safe" transmission rate for which Bob can demodulate correctly and Eve cannot. It also underlines the point that the antennas chosen will matter from this perspective.

5.3 Summary

In this chapter, we investigated antenna design guidelines for techniques that employ polarization modulation. We found suitable metrics to evaluate radiated polarization characteristics and the impact on overall system performance. These metrics were illustrated using simulation results from several representative dual-polarized antennas. The first metric, the Poincaré spread, is a gauge of distortion in Stokes space given a physical angular range of interest around the transmitter. Antennas with higher spread will be more limited in the ability to use higher modulation orders even if Bob's received signal meets the required SNR levels. On the other hand, the FOV is a good way to relate antenna characteristics to error performance over physical space. In this analysis, we chose to use EVM as an example because it provides more information for RF design, but one can easily use bit or symbol error probability, as done in Chapter 4. If just one antenna is used as a transmitter, this would define the system's valid angular range for receivers. If multiple antennas are used in an array, the FOV of a single antenna operates like an envelope for the array FOV, neglecting higher-order effects. This characteristic comes from the single-element radiation pattern as related to the total pattern of its array [23]. The proposed metrics may be used to design any general multi-polarization system.

We also examined antenna design impact specifically on SAPM performance with regard to security. While error rates in a fixed direction are not directly antenna-dependent because system gain is accounted for in received SNR, this is not the case for SAPM due to depolarization effects. To some extent, the same may be said for PolSK. Truly significant antenna-dependent behavior is seen when evaluating error over spatial angles. The existence of the secondary SOP and cross-polarized waves changes the SAPM information beamwidth expectations between antenna types, with up to 12° of difference at binary modulation. The antenna-dependency for BFNs is much more straightforward because it is power pattern-dependent and mostly consistent with modulation order. To account for secure performance in all regions around Alice, not just those close to Bob, one may consider secrecy rates. We observed that the halfwave dipoles, usually considered low-to-moderate gain antennas, achieved better secrecy in the main beam at angles close to Bob, but the Archimedean spirals had marginally better secrecy in the sidelobes. Both of these effects are highly dependent on the power division between the primary and secondary SOPs, and the same trends with antenna type are seen for BFNs using PolSK and DPSK.

CHAPTER 6

SAPM PROTOTYPE AND PROOF-OF-CONCEPT

Since SAPM security performance compares favorably to other methods from theoretical calculations and simulations, the natural next step is to demonstrate its viability with a prototype. In this chapter, we describe the efforts to produce this proof-of-concept and analyze the resulting measurement data. First, fabrication details are shared in Section 6.1. The equipment used and the setup of the anechoic chamber are described and shown in Section 6.2. An important step in using any beamforming application is the calibration of the BFN itself, which is especially important for SAPM and is outlined in Section 6.3. Finally, measurements are shared in Section 6.4, along with a discussion of the results.

6.1 Array fabrication

The square microstrip patch array from Figure 5.10(c) was chosen based on performance in simulations from Chapter 5, where its characteristics over most categories tended to be either better than or on par with the others. Details on the design justifications for the element may be found in Section 5.1. Another favorable consideration for choosing the patch is the ease of manufacturing for this type of antenna; we were able to use a single process and mill the design using a Quick Circuit Model 5000 machine. In general, imperfections in the fabrication process, such as tolerances in the x-,y-, and z-dimensions of milling, are only expected to impact the input match of the patches. In other words, these effects, along with error in path attenuation and reflection coefficient measurements, would decrease the accuracy of the absolute measured gain of the prototype but should not detract from its purpose of validating SAPM. Figure 6.1 is a photograph of the final product.

While the size of the ground plane is modeled accurately in simulations,

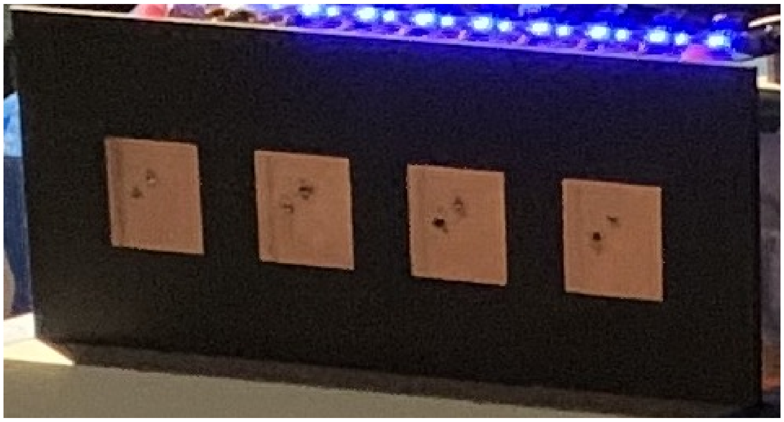


Figure 6.1: Fabricated microstrip array on a 3.175 mm-thick Duroid 5880 substrate, based on the design of Figure 5.10(c)

the metal equipment behind the array, shown in Section 6.2, is not included in HFSS and is expected to affect the patterns close to the plane of the array and decrease the front-to-back ratio [23]. Again, this should only minimally impact the high-level goal of these experiments. However, any errors in the calibration steps discussed in Section 6.3 are expected to affect radiation shapes and null-depths, which would be more critical to SAPM performance.

6.2 Anechoic chamber setup

Figure 6.2 is a block diagram of the equipment used inside and outside the anechoic chamber to take radiated gain patterns and symbol error rate measurements. Commands and data are sent over ethernet between this and a mechanical turntable (not shown), a Keysight PNA Network Analyzer (N5224B), and a Raspberry Pi 3 Model B+ single-board computer. The BFN is an analog 8-channel phase/amplitude controller (PAC-8S2 v1.0) from the Advanced Radar Research Center (ARRC) at the University of Oklahoma. The function of the Raspberry Pi is to control the 6-bit phase shifters (MAPS-010164) and 6-bit attenuators (HMC472ALP4E) on this board over SPI. A photograph of the test setup is shown in Figure 6.3, and Figure 6.4 shows a close-up view of the transmission path.

For patterns, calibration is required to account for the gain or loss along the path between the network analyzer output terminal and the device under test (DUT), as well as the receiving antenna gain and its path to the analyzer's

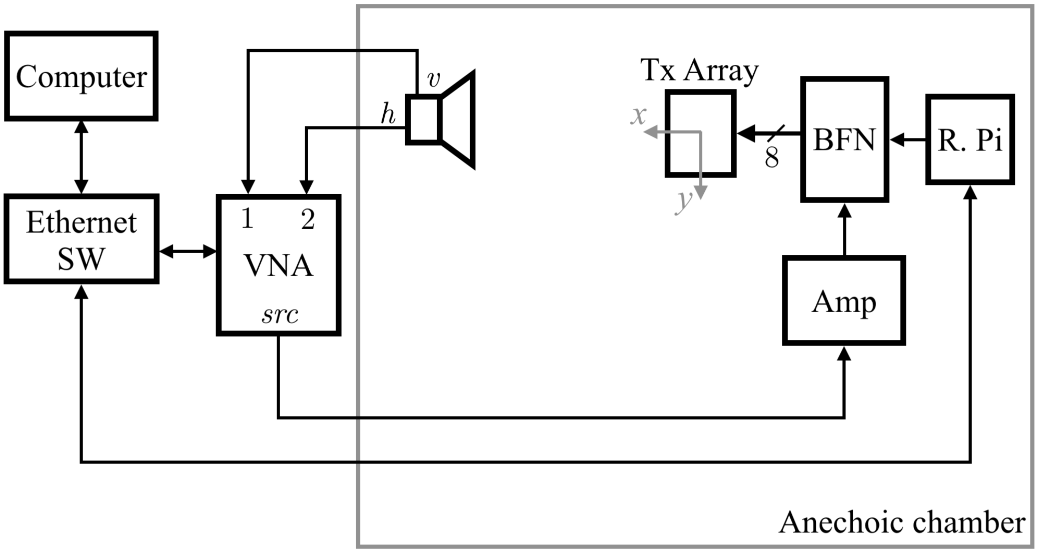


Figure 6.2: Block diagram of testing setup, including the ethernet switch ('SW'), vector network analyzer ('VNA'), patch antenna array ('Tx array'), beamforming network ('BFN'), amplifier ('Amp'), and Raspberry Pi ('R. Pi')

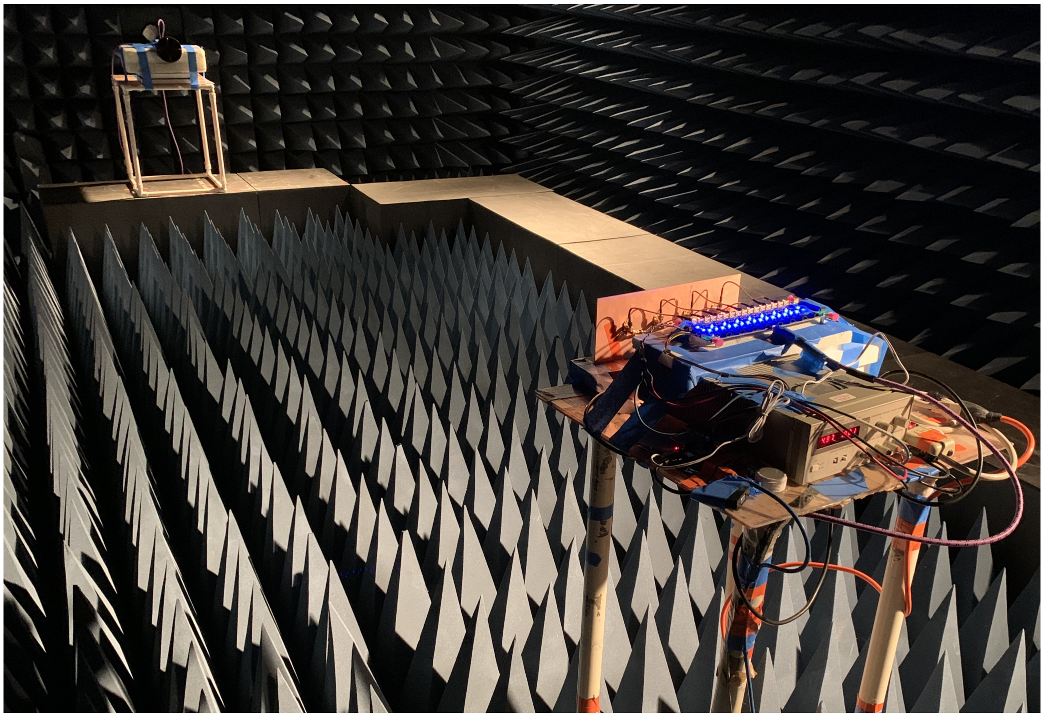


Figure 6.3: Chamber setup, with transmitting elements in the foreground on top of the turntable

inputs. This is not to be confused with the calibration of the BFN in Section 6.3. During the antenna calibration, a standard gain horn with known gain

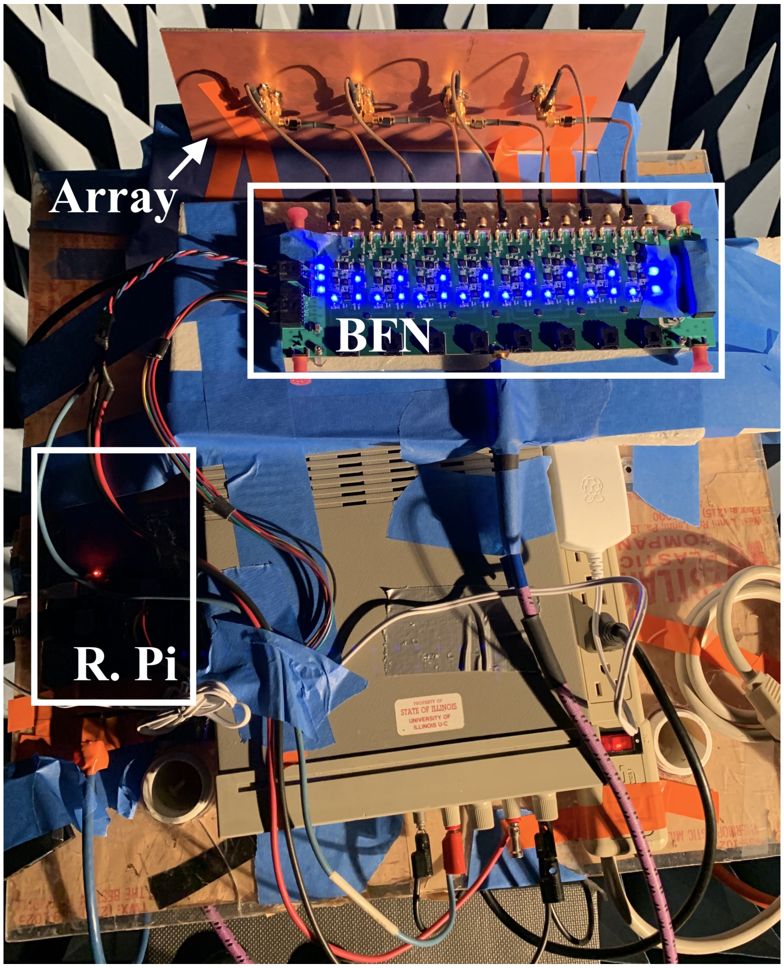


Figure 6.4: Transmitter module: the BFN (courtesy of the ARRC), antenna array, Raspberry Pi, and the DC power source

is swapped with the DUT (marked 'Tx Array' in the diagram). Ordinarily for antennas that are dominantly single-polarization, one S_{21} measurement across the bandwidth of interest is then taken with the gain horn transmitting via port 1 and the receive antenna on port 2. This serves as the calibration step. When the DUT's S_{21} is measured, its magnitude is squared (to calculate power gain) and normalized with the calibration $|S_{21}|^2$ to remove the effect of the gains/losses in the path aside from the DUT gain. The calculation of gain from received power ratios comes from the Friis transmission formula [23].

In our case, two separate calibration measurements are done for the v- and h-ports, one with the gain horn oriented to radiate a vertically polarized wave and again with a horizontally polarized wave. The measurement is a ratio of the received power at the v-port or the h-port referenced to the transmitted power from the internal source. The PNA includes physical jumper connections to decouple its internal RF source from the receivers at each test port. This configuration allows us to coherently measure the orthogonal v- and h-polarized wavefronts, and a third calibration step is required to account for any phase difference caused by the two separate paths to the analyzer.

The measured (and corrected) v and h signals are fed into the demodulator/detector to determine the received SOP. We can also measure the gain in an arbitrary polarization by projecting the measurement onto the appropriate unit-magnitude Jones vector [23], [45]:

$$\begin{aligned}\text{Gain}_\rho &= \frac{4\pi}{P_{\text{acc}}}\left(\frac{\left|r\left[\mathcal{E}_v, \mathcal{E}_h\right] \cdot \hat{\rho}\right|^2}{2\eta_0}\right) \\ &= \left|\sqrt{\text{Gain}_v}\angle\phi_{vh} \times \hat{\rho}_v + \sqrt{\text{Gain}_h} \times \hat{\rho}_h\right|^2 \end{aligned} \tag{6.1}$$

where P_{acc} is the power accepted by the antenna and η_0 is the free-space intrinsic impedance. The phase between the v and h signals, $\angle\phi_{vh}$, and the v, h gain terms are directly measured as described in this section. The Jones vector is defined as

$$\hat{\rho} = \begin{bmatrix} \hat{\rho}_v \\ \hat{\rho}_h \end{bmatrix} = \begin{bmatrix} \sin\left(\theta/2\right) e^{j\phi} \\ \cos\left(\theta/2\right) \end{bmatrix} \tag{6.2}$$

As always, $[\theta, \phi]$ are spherical coordinates in Stokes space that fully specify the desired polarization ρ.

6.3 Beamformer calibration steps

From Figure 6.4, it can be seen that each antenna port is fed via coaxial cables behind the ground plane, which are not phase-matched. As such, we must include these cables in our calibration of the BFN to account for their individual phase offsets in addition to the offsets from the board and part tolerance. It is not possible to know what excitations are fed to the antenna elements without a thorough and accurate calibration, but, luckily, it only has to be done once and the results are not impacted by the radiation environment. This step is not specific to SAPM and should be done for

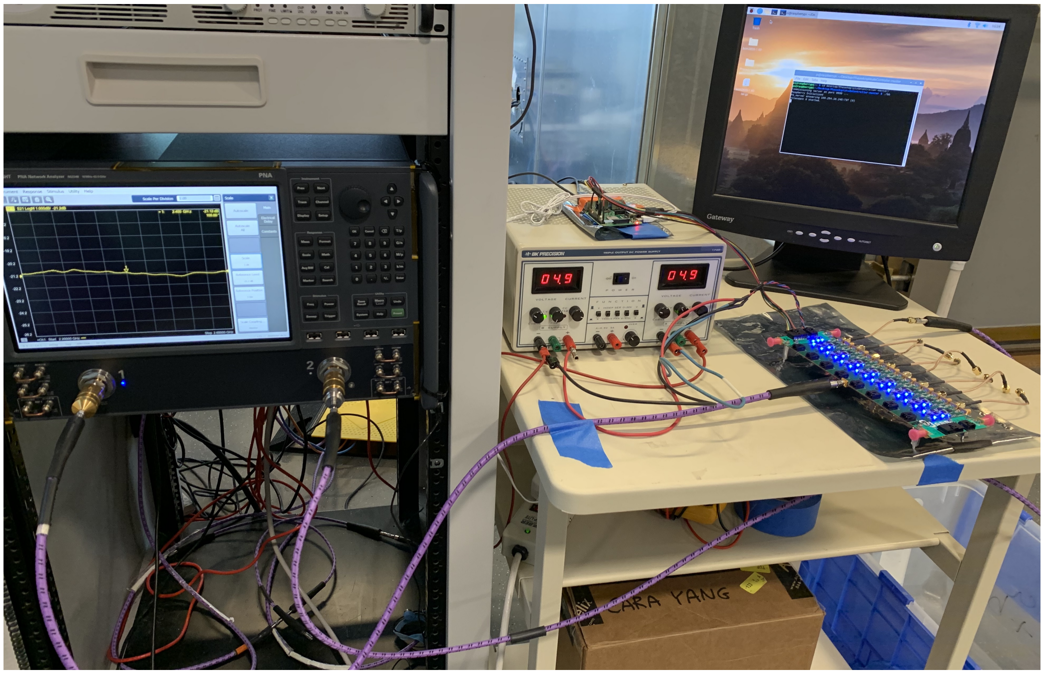


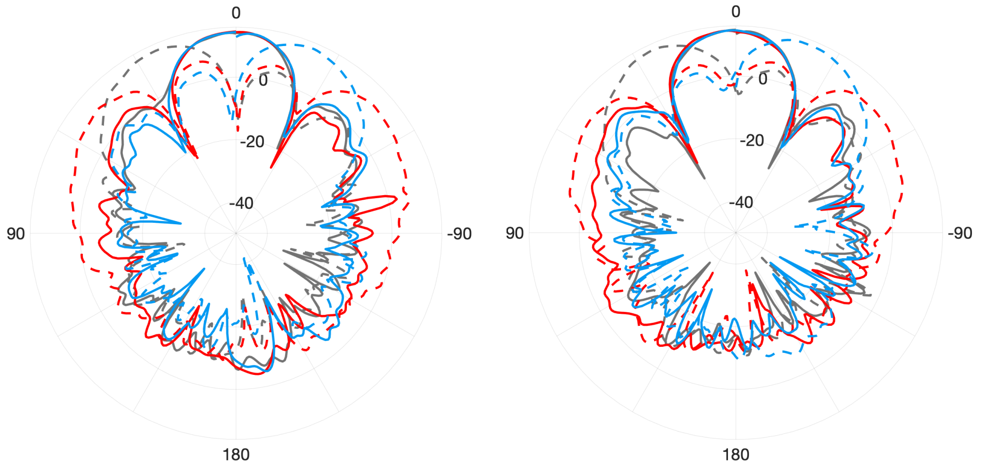
Figure 6.5: Calibration setup

any beamforming system. We include amplitudes in the calibration process, but unsurprisingly, the variation in attenuation is comparatively low. A photograph of the calibration setup is shown in Figure 6.5.

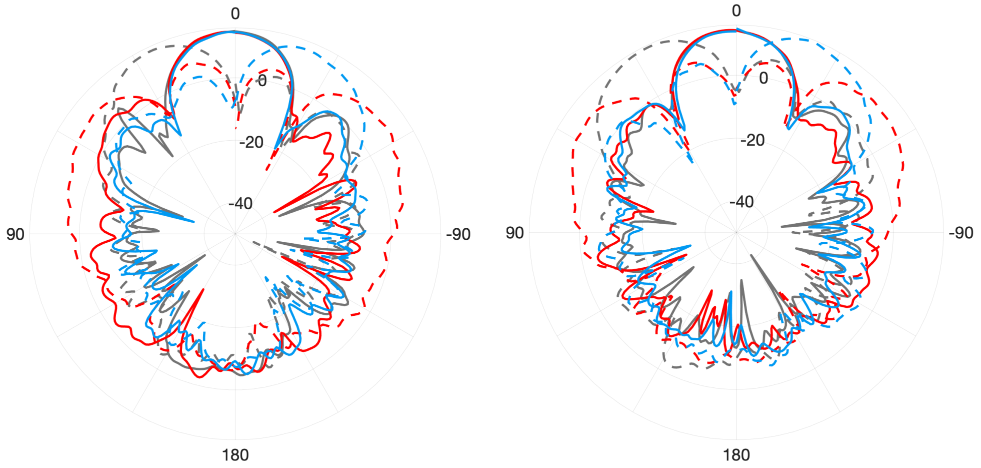
The measured S_{21} data from this setup, where port 1 is the RF input to the BFN and port 2 is individually connected to each cable, tells us the actual phase and attenuation of the path. These measurements were done at every phase setting ($0° - 360°$) for each 2 dB increment of available attenuation (0-32 dB). Any time different cables are used in the path, this calibration must be redone. It was observed that the output phase changes in steps when settings are incremented between 4° and 7°, which falls in line with the part specification of nominal ±1.5° for the least significant bit (5.6°), and ±5° overall [55].

6.4 Measurement results

For M=4, the gain patterns in dB are shown in Figure 6.6, which includes polar plots of all four symbols. In each plot, the gain in the primary SOP is plotted in solid lines and the gain in the secondary is dashed. Each symbol has three SAPM options (overlaid) since we have only opted to use null



(a) Symbol 1 (b) Symbol 2



(c) Symbol 3 (d) Symbol 4

Figure 6.6: Measured gain (dB) of the patch array configured for 4-SAPM at 2.4 GHz with $L = 3$ options for each symbol: solid lines denote primary SOP (current symbol), dashed lines denote simultaneous antipodal SOP with target main beam directions $[-28°, 28°, 90°]$; Bob at 0°; 1/2 of P_{RF} in secondary SOP

patterns for the secondary with our four-element array.

It is evident that not all secondary nulls have the same depth or are perfectly aligned, which would affect both the error rates at Bob and the shape of the information beamwidths. For symbols 2 and 3, it is clear that at least one of the nulls is shifted to the positive side of 0°, so we expect a smaller width and a similar shift in the information beam. For a given application, iterative steps to align the nulls may be necessary as an additional calibration step. Appendix D includes gain and polarization information for the other

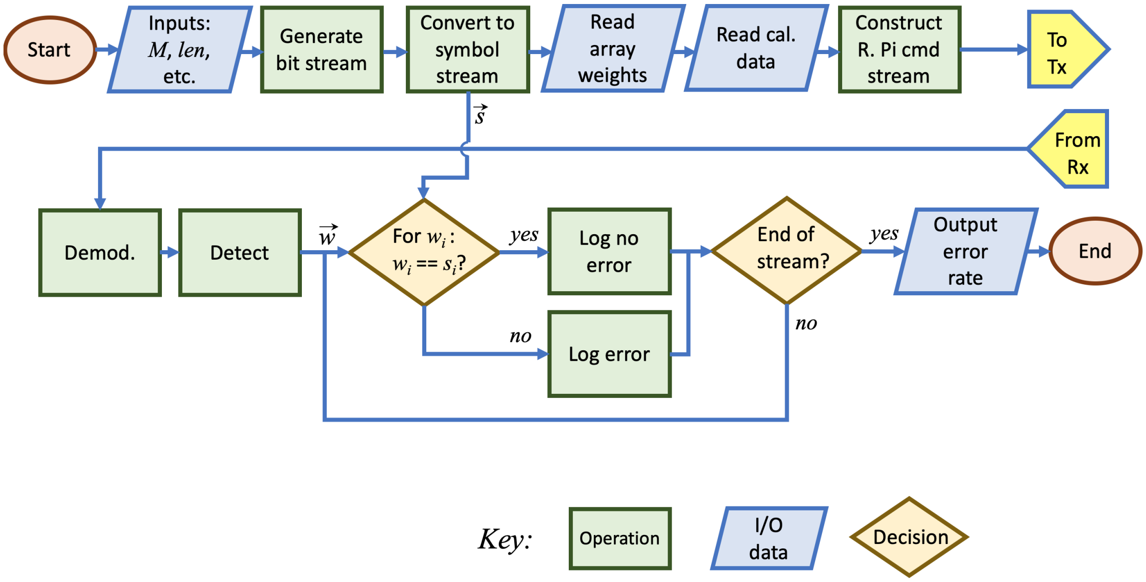
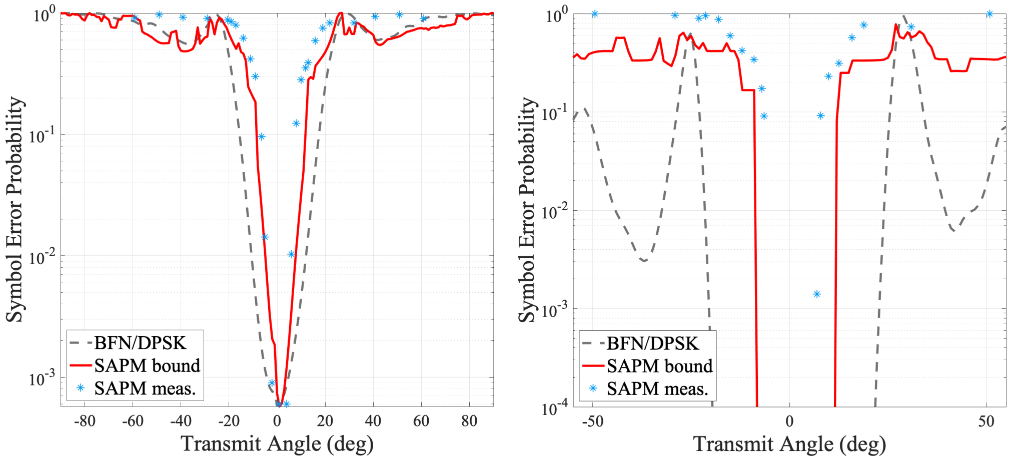


Figure 6.7: Flowchart for the M-ary SAPM processor: generation, transmission, receipt, and interpretation of data; symbol stream of length len

tested modulation orders.

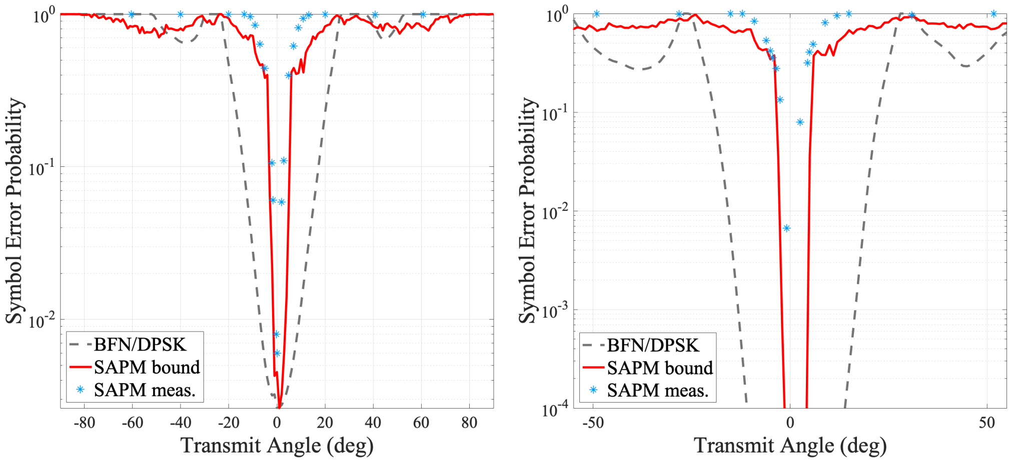
Measured symbol error rates are reported (blue "$*$"s) in Figures 6.8 and 6.9. The setup from Figure 6.3 is employed, with an intended receiver at $\varphi = 0°$. Whereas for pattern measurements, a single S_{21} sweep is taken at each look angle, for error rate measurements, a known list of symbols, represented by nominal SOPs, is transmitted as commands to the BFN. A simplified flowchart is provided in Figure 6.7 for a quick reference of the steps, where the demodulation/detection is done with a modified Stokes receiver as in Section 4.4's simulations. For this investigation, all data is processed asynchronously after the entire stream is transmitted and received. In a real-world application with an optimized processor, this flow may still be used with the stream length len set appropriately (possibly the word length or frame size).

The pseudorandom number generator for creating the bit stream follows the widely known Mersenne Twister algorithm [63]. The general rule of thumb for total number of symbols transmitted at a given angle is at least 10 times the expected number of symbols per symbol error, with a floor of 1,000 symbols. Due to time and resource limitations, it was not reasonable to transmit more than 50,000 symbols (100,000 or 200,000 bits for M=4 or



(a) (b)

Figure 6.8: Theoretical and measured 4-SAPM uncoded error probability over azimuth at average SAPM E_b/N_0 of (a) 12 dB and (b) 26 dB for Bob at $\varphi = 0^\circ$; E_b/N_0 at other angles for both methods may be found from Figure C.1 in Appendix C



(a) (b)

Figure 6.9: Theoretical and measured 16-SAPM uncoded error probability over azimuth at average SAPM E_b/N_0 of (a) 16 dB and (b) 23 dB for Bob at $\varphi = 0^\circ$; E_b/N_0 at other angles for both methods may be found from Figure C.1 in Appendix C

M=16, respectively) for each look angle. For clarity, the axis is restricted in range for the higher-SNR scenarios reported in Figures 6.8(b) and 6.9(b). Close to Bob, the results (zero errors) are obviously not reliable because of this limitation and are thus not reported.

In each figure, we again overlay the error probability bound derived in Section 4.4.2 with red solid lines and the theoretical beamformer DPSK error with gray dashed lines. It is evident from these plots that the SAPM bound is fairly tight when noise and secondary SOP levels are lower, but tends to underestimate error probability as these increase, i.e., away from Bob and especially at $M = 16$. This was seen to some degree in the higher-order modulation simulations from Section 4.4.3, and it is expected from the bounding method we chose [51]. In general, this result indicates that the analysis provides conservative estimates regarding the security improvement from SAPM. The difference between SAPM and BFN information beamwidths jumps significantly from $M = 4$ to $M = 16$, which confirms the trend from Chapter 4.

Figure 6.10 is a plot of measured 16-ary SAPM error rates when the intended receiver is at 30° relative to Alice. We slightly increase SNR at Bob to keep the measured error rates in the same range as Figure 6.9(a), which facilitates a rough comparison. All other variables and setup factors are kept the same, but the excitations at the array are altered to beam and null steer to Bob at the new location. Again, the observed match between theoretical and measurement data is quite close at angles around Bob. While the BFN information beamwidth has increased when steering to Bob at 30° from Bob at 0° (Figure 6.9(a)), the SAPM beamwidth is constant or even smaller. The antenna element radiation pattern acts like an envelope for total radiation as power is steered away from broadside, which means that the total gain decreases in the main beam and the sidelobes increase. This behavior impacts error rates for I/Q modulation methods much more than SAPM, as discussed in Chapter 5.

6.5 Summary

This chapter presents the results from measurements collected in an anechoic chamber using an array of dual-polarized square patches. The setup and calibration steps are summarized, with the more time-intensive procedures mostly related to the beamformer and its path. Luckily, these steps generally only need to be done once and do not require the system to be in-situ, as long as no extreme temperature fluctuations that may affect the individual parts

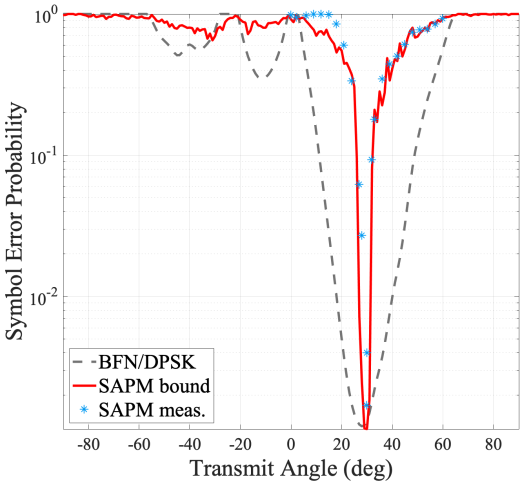


Figure 6.10: Theoretical and measured 16-SAPM uncoded error probability over azimuth at average SAPM E_b/N_0 of 18 dB for Bob at $\varphi = 30°$; E_b/N_0 at other angles for both methods may be found from Figure C.1 in Appendix C

are expected in the deployment environment. Gain patterns are provided for each symbol in 4-ary operation, with more patterns in Appendix D. No additional calibration and corrections are done after these measurements to adjust the null locations or align them with more accuracy, but this may certainly be an iterative process in a given application to improve error rates at Bob. In general, the error performance has been shown to be quite close to simulations and theory even without additional array excitation corrections. The most critical evidence has been presented, which is that for the same error rates at the intended receiver, we see a much narrower region of low error for SAPM when compared to regular beamforming. All other factors have been kept constant where possible, including all the hardware. The data and analysis from this chapter serves as a proof-of-concept for SAPM in an AWGN channel with a LOS signal component.

CHAPTER 7

CONCLUDING THOUGHTS

In this chapter, we summarize the original contributions of this work and discuss their potential impact on wireless network security. We also outline a few interesting directions for further analysis in the future.

7.1 Contributions

Greater challenges are associated with securing a wireless network as opposed to a wired system, but there is no denying that most modern communications schemes are shifting to or already using a wireless interface. Our work aims to address two significant threats to wireless security; namely, denial of service in the form of jamming and data interception in the form of eavesdropping.

Our first approach is developed from the view of a GPS receiver seeking a desired signal in the possible presence of jammers. Civilian GPS is an ideal problem space because it is an open, unsecured broadcast, and numerous sectors critical to our lives depend on uninterrupted GPS service. As a receiver-side solution to counter the risk of GPS interference, we presented the design of the hemispiral antenna combined with an algorithm to leverage its unique attributes. When compared to prior work, our design is smaller and/or cheaper than other single-antenna solutions capable of direction finding. In addition, our modified MUSIC algorithm is capable of identifying more than one source despite having only one RF input, which, to our knowledge, has not been shown by other authors.

Our second solution is for a system with a known target transmission angle but possible eavesdroppers in other directions, where we have design control over both transmitters and receivers. We introduced a novel technique in the realm of physical layer security: secure antenna polarization modulation, or SAPM. Similar to some families of prior approaches, SAPM scrambles data in all directions aside from the intended transmission angle. However, it improves upon the existing work by introducing straightforward beamforming capabilities in addition to data distortion and removing the coherence requirement of other antenna- or RF-based modulation methods. Compared to traditional PolSK, the directional distortion of SAPM has an inherent element of randomness that is not easy for eavesdroppers to calibrate out. Even under pessimistic assumptions that eavesdroppers have more information than what is transmitted and may account for the distortion, we showed that SAPM is usually still more secure than other methods. We derived a model for LOS performance in an AWGN channel and verified its accuracy with both simulations and measurements of a prototype. By establishing this theoretical framework for SAPM in an idealized environment, we have created a baseline for future work using more complex practical channels. In addition, we provided analysis on the impact of antenna design for polarization-based methods—SAPM or otherwise. Practical antenna considerations are generally left out of the prior work on this topic, but techniques like SAPM and PolSK are affected by antenna parameters in a way that is unique from traditional modulation. We strive to help bridge the gap in knowledge with respect to this topic.

7.2 Future work

In this section, we provide several avenues for continued research related to the ideas presented in this dissertation. The bulk of these proposals involve SAPM because it is an entirely new modulation scheme that requires further characterization beyond the scope of our investigation. For the hemispiral, the available paths for future work are more straightforward. While we have demonstrated 2D direction finding over one plane, the method supports 3D angle of arrival detection. The processing changes for 3D DOA include expanding the **A**-matrix to capture pattern variation over all (θ, ϕ) in the upper hemisphere. Other interesting avenues for further hemispiral characterization may involve performance comparisons against known antennas, design revisions with better manufacturability, and alternate methods of implementation.

7.2.1 SAPM performance in fading channels

The main focus of this work is the characterization of SAPM in AWGN channels, but in this section we outline the approach for analysis in multipath-induced fading channels. The dual-polarized channel transfer functions of interest are identical to PolSK; however, the SAPM excitation vectors defined in Section 4.3.1 would alter the received signals. We revise Equation (4.1) to account for distance from the transmitter, r:

$$\begin{bmatrix}\mathcal{E}_v(m,r,\vartheta,\varphi)\\ \mathcal{E}_h(m,r,\vartheta,\varphi)\end{bmatrix} = \mathbf{H}\begin{bmatrix}\vec{a}_v[m]^T\\ \vec{a}_h[m]^T\end{bmatrix} + \begin{bmatrix}\hat{n}_v\\ \hat{n}_h\end{bmatrix} \tag{7.1}$$

where the channel matrix $\mathbf{H}$ represents a summation of the complex transfer functions of all paths from the array to a receiver at $[r,\vartheta,\varphi]$. The excitation vectors $\vec{a}$ in either polarization are previously defined in Equations (4.4) and (4.5).

If there is a strong LOS component, we may choose a dual-polarized Rician fading channel with Rician factor K. Then $\mathbf{H}$ is defined from [25] as

$$\mathbf{H} = \sqrt{\frac{K}{1+K}}\bar{\mathbf{H}} + \sqrt{\frac{1}{1+K}}\hat{\mathbf{H}} \tag{7.2}$$

where $\bar{\mathbf{H}}$ represents the coherent wave components and $\hat{\mathbf{H}}$ is the noncoherent portion.

For an N-element array,

$$\bar{\mathbf{H}} = \begin{bmatrix}\vec{s}_{vv} & \vec{s}_{vh}\\ \vec{s}_{hv} & \vec{s}_{hh}\end{bmatrix} \tag{7.3}$$

where the length-N $\vec{s}$ vectors represent the co- and cross-polarized complex transfer functions from each of n antennas in the array, Equation (4.2). The noncoherent component, from [50], is calculated from the polarization correlation matrix $\mathbf{R}$:

$$\hat{\mathbf{H}}^H = \mathbf{R}^{1/2}\mathbf{H}_g^H \tag{7.4}$$

$$\mathbf{R} = \begin{bmatrix} 1 & \sqrt{\mu\chi}\sigma_t^* & \sqrt{\chi}\sigma_r^* & \sqrt{\mu}\delta_c * \\ \sqrt{\mu\chi}\sigma_t & \mu\chi & \sqrt{\mu}\chi\delta_x^* & \mu\sqrt{\chi}\sigma_r^* \\ \sqrt{\chi}\sigma_r & \sqrt{\mu}\chi\delta_x & \chi & \sqrt{\mu\chi}\sigma_t^* \\ \sqrt{\mu}\delta_c & \mu\sqrt{\chi}\sigma_r & \sqrt{\mu\chi}\sigma_t & \mu \end{bmatrix} \tag{7.5}$$

The matrix $\mathbf{R}$ is comprised of channel-specific parameters: μ, the co-polarization ratio, χ, the XPD, $\sigma_{t(r)}$, the transmit and receive correlation coefficients, and $\delta_{c(x)}$, the co- and cross-polarized correlation coefficients. These include, to a large extent, the effects of the transmit and receive antennas. Once $\mathbf{H}$ is determined, we may derive PDFs for $\mathcal{E}_{v,h}$ (and $\mathcal{E}_{\theta,\phi}$) in a fading channel from the received signal covariance matrix, which would follow the same form as [25], [50]. Based on the results from this work, a full characterization of SAPM performance in these practical environments is warranted and highly recommended before consideration for deployment.

7.2.2 Array design for SAPM

Our investigation of the impact of antenna design on polarization modulation naturally leads to the question of whether the design of the array might play a part in SAPM performance. The short answer is yes, because the radiation patterns available to the transmitter are directly dependent on the array geometry, the number of antenna elements, etc. At the most basic level, the total number of available null patterns will generally increase with array size. It is interesting to consider how much this would impact performance with regard to error and secrecy. It is also quite intuitive that with more patterns available, there are more degrees of freedom in the placement of beam maximums and nulls, and therefore greater ease in enabling multi-user support.

An additional array-related question has to do with the tolerance of the array feed components. While we showed that a certain degree of error in null placement is fine for SAPM operation, it is important to quantify how much error is allowed and what levels of degradation are expected. A possible way to study this is by sweeping the calibration measurements across some range to observe the effect on gain patterns and error rates.

7.2.3 Privacy in multi-user implementations and alternative configurations

There are open questions regarding the limitations of SAPM with respect to expanded applications. For example, the initial theory presented does not preclude multiple users in one signaling environment. An important topic for future work is the ceiling of total transmitters and receivers in a shared location on the same carrier. Analysis may reveal the parameters that define this ceiling. Any design tradeoffs in the implementation of multi-user systems ought to be established.

Time-domain multiplexing combined with higher order modulation is a way to share the spectrum with multiple users without compromising data bandwidth. Our work on SAPM performance with higher spectral efficiency suggests that increasing modulation order results in greater secrecy margin, but further investigation is required to determine its limits, especially for fading channels.

Finally, performance in areas with numerous transmitting devices may be studied. For some applications, it is desirable to hide the SAPM transmission completely. The use of polarization for information allows other features of the signal to intentionally resemble a different signature, such as GSM, thus masking the true SAPM transmissions. This may be implemented in all directions, including those of intended receivers. Yet another interesting area for further work involves evaluating the probability of detection for SAPM with characterization of its spectrum as compared to the mimicked protocol.

7.3 Conclusion

For applications where sensitive data is shared over wireless networks, there is always the possibility of service disruptions from jammers or an unauthorized recording of the broadcast. While the damage from jamming interference is generally obvious, eavesdroppers are difficult to detect but may nevertheless lead to catastrophic results, such as the breach of personal identifying data. Countermeasures to both types of attacks must be considered in modern wireless systems.

The novel solutions presented in this dissertation are viable methods to address these threats, for two different kinds of design spaces. We believe that our contributions can help bolster security for a wide range of applications, with potentially increasing impact as wireless communication systems continue to expand across the globe.

APPENDIX A

ALTERNATIVE DERIVATIONS FOR DEMODULATION OF POLARIZATION MODULATED METHODS

As noted in Chapter 4, SAPM, like PolSK, should be considered a noncoherent technique because demodulation may be accomplished without estimating absolute carrier phase. Since SAPM is identical to PolSK for intended communication, a general PolSK receiver may be used, as is done in the main body of the investigation [24]. In this appendix, we present an alternative way to derive the probability density functions (PDFs) in an AWGN channel for the two demodulated parameters Θ and Φ, the spherical coordinates of the received signal mapped to Stokes space.

A.1 Representation of incoming signals

At the transmitter, the message is represented by symbols $\mathbf{s}_m = [\bar{\theta}_m, \bar{\phi}_m]$ on the surface of a rotated Poincaré sphere, per Section 4.2.1. For PolSK, a receiver in an arbitrary direction (ϑ_0, φ_0) relative to the transmitter will be able to recover a symbol $\mathcal{P}_m = \mathbf{g}_m(\vartheta_0, \varphi_0)$ plus noise from the channel. For SAPM, the mapping functions over spatial angles form a set $[\mathbf{g}_{m,1}, \ldots \mathbf{g}_{m,L}]$ for each of the M symbols. We demodulate the signals to directly estimate θ_m and ϕ_m, as opposed to measuring the Cartesian Stokes parameters and then mapping these to spherical coordinates, as done in [24].

Without loss of generality, we assume that the dual-polarized receive antennas provide an incoming signal with vertical linear polarization (VP) in our reference coordinate system and another with horizontal (HP) at every symbol step. In cases where the antennas are sensitive to two different orthogonal polarizations, a simple rotation may be done in Stokes space. The sets of incoming signals plus noise are $[v_1, v_2 \ldots, v_M]$ and $[h_1, h_2 \ldots, h_M]$, where each member of the set is defined as

$$v_m(t,\vartheta,\varphi) = a_{v,m}(t,\vartheta,\varphi)\ p(t)\cos[\omega_c t + \phi_{v,m}(t,\vartheta,\varphi) + \phi_c] + n_v \tag{A.1}$$

$$h_m(t,\vartheta,\varphi) = a_{h,m}(t,\vartheta,\varphi)\ p(t)\cos[\omega_c t + \phi_{h,m}(t,\vartheta,\varphi) + \phi_c] + n_h \tag{A.2}$$

$$m = 1, 2, \ldots, M$$

The spatial angles $\vartheta \in (0,\pi), \varphi \in (0, 2\pi)$ are relative to the transmitter, ω_c is the radian carrier or intermediate frequency (IF), ϕ_c is the absolute carrier phase (unknown but common to both polarizations), and $n_{v[h]}$ represents zero-mean white Gaussian noise with power spectral density (PSD) $N_0/2$. For ease of notation, they are written in Equations (A.1)-(A.2) as continuous signals assuming that the ADC samples much higher than the Nyquist rate. The information-bearing components are the signals' relative amplitudes, $a_{v,m}/a_{h,m}$, and phase, $\phi_{v,m} - \phi_{h,m}$, where the time dependency may be dropped if these are approximately constant over a single symbol period T_s. The term $p(t)$ represents time-variation in the form of a pulse waveform that results from switching the array coefficients as part of the SAPM modulation mechanism. The waveform $p(t)$ is periodic with T_s, and to simplify the analysis, we assume the switching transients are many orders higher in frequency than the symbol rate and $p(t)$ is effectively a unit rectangular pulse with energy per symbol $E_p = T_s$. The total energy per symbol is then $E_s(\vartheta,\varphi) = E_p\left[a_{v,m}(\vartheta,\varphi)^2 + a_{n,m}(\vartheta,\varphi)^2\right]/2$ across a unit impedance. For an arbitrary receiver at (ϑ_0, φ_0), and the amplitudes are related by θ_m, where $\mathcal{P}_m = [\theta_m, \phi_m]$:

$$a_{v,m} = \sqrt{2\frac{E_s}{E_p}}\sin\left(\theta_m/2\right) \tag{A.3}$$

$$a_{h,m} = \sqrt{2\frac{E_s}{E_p}}\cos\left(\theta_m/2\right) \tag{A.4}$$

$$\tag{A.5}$$

We initially assume that the noise components are uncorrelated between the two channels. Demodulation brings the signal centered at the carrier or IF down to baseband in order to produce estimates for $\mathbf{s}_m$. A simplified functional block diagram is shown in Figure A.1 based on [49].

For both channels, the same basis functions are used to expand the signals.

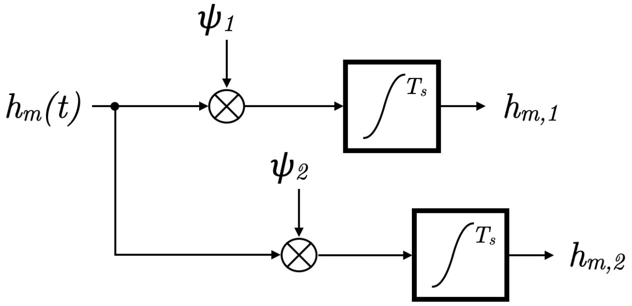


Figure A.1: General demodulator for any polarization modulated signal: only the horizontally polarized channel is shown (the vertically polarized channel is identical) [49]

These may be selected from the traditional two-dimensional amplitude-phase modulation basis functions, defined as [49]

$$\psi_1 = \sqrt{\frac{2}{E_p}} p(t) \cos(\omega_c t) \tag{A.6}$$

$$\psi_2 = -\sqrt{\frac{2}{E_p}} p(t) \sin(\omega_c t) \tag{A.7}$$

After the integrate-and-dump filters, the demodulator outputs, expressed in the complex domain, are

$$\begin{aligned}
\mathbf{v}_m &= a_{v,m}\sqrt{\frac{E_p}{2}} e^{j(\phi_{v,m}+\phi_c)} + \mathbf{n}_v \\
&= \sqrt{E_s} \sin(\theta_m/2) e^{j(\phi_{v,m}+\phi_c)} + \mathbf{n}_v \qquad \text{(A.8)} \\
\mathbf{h}_m &= a_{h,m}\sqrt{\frac{E_p}{2}} e^{j(\phi_{h,m}+\phi_c)} + \mathbf{n}_h \\
&= \sqrt{E_s} \cos(\theta_m/2) e^{j(\phi_{h,m}+\phi_c)} + \mathbf{n}_v \qquad \text{(A.9)}
\end{aligned}$$

The in-phase and quadrature components of the variables $\mathbf{v}_m$ and $\mathbf{h}_m$ each follow normal distributions $\mathcal{N}(\mu, \sigma^2)$:

$$v_{m,1} \sim \mathcal{N}\left(\sqrt{E_s}\sin(\theta_m/2)\cos(\phi_{v,m}+\phi_c), \frac{N_0}{2}\right) \tag{A.10}$$

$$v_{m,2} \sim \mathcal{N}\left(\sqrt{E_s}\sin(\theta_m/2)\sin(\phi_{v,m}+\phi_c), \frac{N_0}{2}\right) \tag{A.11}$$

$$h_{m,1} \sim \mathcal{N}\left(\sqrt{E_s}\cos(\theta_m/2)\cos(\phi_{h,m}+\phi_c), \frac{N_0}{2}\right) \tag{A.12}$$

$$h_{m,2} \sim \mathcal{N}\left(\sqrt{E_s}\cos(\theta_m/2)\sin(\phi_{h,m}+\phi_c), \frac{N_0}{2}\right) \tag{A.13}$$

Using the outputs from the demodulator, Section A.2 describes the steps to form Φ, a noisy estimate for $\phi_m = \phi_{v,m} - \phi_{h,m}$. Section A.3 describes the procedure for estimating θ_m from Θ, which may be done in parallel.

A.2 The probability density function of Φ

It will become clear from the derivations in this section that the common carrier phase, ϕ_c, will not impact the estimation of ϕ_m. To derive the marginal probability density function (PDF) f_Φ given ϕ_m, we project $\mathbf{v}_m$ onto $\mathbf{h}_m$ [49]:

$$\begin{aligned}\mathbf{v}_m\mathbf{h}_m^* = \frac{E_s}{2}\sin\theta_m e^{j(\phi_{v,m}-\phi_{h,m})} + \sqrt{E_s}\sin(\theta_m/2)e^{j(\phi_{v,m}-\phi_c)}\mathbf{n}_h^* \\ + \sqrt{E_s}\cos(\theta_m/2)e^{-j(\phi_{h,m}-\phi_c)}\mathbf{n}_v + \mathbf{n}_v\mathbf{n}_h^*\end{aligned} \tag{A.14}$$

The term $\mathbf{n}_v\mathbf{n}_h^*$ complicates the calculation of f_Φ, but we take the same approach as [49] and assume that for realistic SNR levels, this is dwarfed by the other two noise terms and may be neglected. Since the lowpass noise is a circular Gaussian process, the statistics of $\mathbf{n}_v$ and $\mathbf{n}_h$ are independent of the phase rotation terms $\cos(\theta_m/2)e^{-j(\phi_{h,m}-\phi_c)}$ and $\sin(\theta_m/2)e^{-j(\phi_{v,m}-\phi_c)}$, respectively [49]. Incorporating these simplifications, the complex projection becomes

$$\mathbf{v}_m\mathbf{h}_m^* = \frac{\sqrt{E_s}}{2}\sin\theta_m e^{j\phi_m} + \mathbf{n}_h^* + \mathbf{n}_v \tag{A.15}$$

The phase of this projection is calculated from converting the Cartesian components $Z_1 = \mathcal{R}\{\mathbf{v}_m\mathbf{h}_m^*\}$ and $Z_2 = \mathcal{I}\{\mathbf{v}_m\mathbf{h}_m^*\}$ to polar angle and magnitude, where the angle is Φ. Based on our initial assumptions, Z_1 and Z_2 follow normal distributions with mean $\mu_{Z_1} = \frac{1}{2}\sqrt{E_s}\sin\theta_m\cos\phi_m$,

$\mu_{Z_2} = \frac{1}{2}\sqrt{E_s}\sin\theta_m \sin\phi_m$, and equal variances $\sigma^2 = N_0$. The noise PSD is twice as high as that of coherent IQ demodulation due to the projection step. The joint PDF of Z_1, Z_2 may be converted to polar coordinates with steps outlined in [64] to determine the angle between Z_1 and Z_2, which is equivalent to Φ. The joint density function in polar coordinates given a transmitted symbol $\mathbf{s}_m$ is

$$\begin{aligned} f_{U,\Phi}(u, \phi \,|\mathbf{s}_m) = &\frac{u}{2\pi N_0} \\ &\times \exp\left\{\frac{-\left[u^2 + (E_s \sin^2\theta_m)/4 + rA_1\sqrt{E_s \sin^2\theta_m}\right]}{2N_0}\right\} \end{aligned} \tag{A.16}$$

where

$$\begin{aligned} A_1 &= \cos\phi_m \cos\phi + \sin\phi_m \sin\phi = \cos(\phi_m - \phi) \\ U &= \sqrt{Z_1^2 + Z_2^2},\ U \in (0, \infty) \\ \Phi &= \tan^{-1}\big(Z_2/Z_1\big),\ \Phi \in (-\pi, \pi) \end{aligned}$$

Integrating over the range of polar magnitude, we arrive at the marginal PDF of Φ:

$$\begin{aligned} f_\Phi(\phi \,|\mathbf{s}_m) &= \int_0^\infty f_{U,\Phi}(u, \phi \,|\mathbf{s}_m) du \\ &= \frac{1}{2\pi}\Bigg\{\exp\left(\frac{-E_s \sin^2\theta_m}{4N_0}\right) \\ &+ \sqrt{\pi\frac{E_s}{N_0}}\sin\theta_m A_1 \exp\left(\frac{-E_s \sin^2\theta_m A_2^2}{4N_0}\right) \\ &\times Q\left(-\sqrt{\frac{E_s}{2N_0}}\sin\theta_m A_1\right)\Bigg\} \end{aligned} \tag{A.17}$$

where

$$A_2 = \sin(\phi_m - \phi)$$

The Q-function in Equation (A.17) is defined as $Q(a) = \frac{1}{2}\mathrm{erfc}\left(a/\sqrt{2}\right)$ [49].

A.3 The probability density function of Θ

To find Θ, we take the arctangent of the ratio of the demodulator output magnitudes:

$$\Theta = 2 \times \tan^{-1}\left(\frac{|\mathbf{v}_m|}{|\mathbf{h}_m|}\right) \tag{A.18}$$

Based on the derivations in Section 4.4.1, both magnitude terms follow a Rice distribution:

$$|\mathbf{v}_m| \sim \text{Rice}\left(|\nu_v| = a_{v,m}\sqrt{E_p/2} = \sqrt{E_s}\sin(\theta_m/2), \sigma_v = \sqrt{N_0/2}\right) \tag{A.19}$$

$$|\mathbf{h}_m| \sim \text{Rice}\left(|\nu_h| = a_{h,m}\sqrt{E_p/2} = \sqrt{E_s}\cos(\theta_m/2), \sigma_h = \sqrt{N_0/2}\right) \tag{A.20}$$

If the ratio is treated as a single variable R, its PDF is given by [65]

$$\begin{aligned} f_R(r) = {} & \frac{2r(\sigma_v/\sigma_h)^2}{\left[r^2 + (\sigma_v/\sigma_h)^2\right]^2} \\ & \times \Big[(1 + B_1)I_0(B_2) + B_2 I_1(B_2)\Big] \exp\left(B_1 - \frac{\nu_v^2}{2\sigma_v^2} - \frac{\nu_h^2}{2\sigma_h^2}\right) \end{aligned} \tag{A.21}$$

where

$$B_1 = \frac{(r\nu_v/2\sigma_v^2)^2 + (\nu_h/2\sigma_h^2)^2}{(r/\sigma_v)^2) + (1/\sigma_h)^2}$$

$$B_2 = \frac{2r\,(\nu_v/2\sigma_v^2)\,(\nu_h/2\sigma_h^2)}{(r/\sigma_v)^2) + (1/\sigma_h)^2}$$

$I_n(a)$ is the n^{th}-order modified Bessel function of the first kind. Along with (A.19) and (A.20), the PDF f_R defines the behavior of the argument of the arctangent in Equation (A.18). The PDF of Θ follows in a straightforward manner:

$$f_\Theta(\theta\ |\mathbf{s}_m) = \frac{|\sec^2(\theta/2)|}{2} f_R(\tan(\theta/2)),\ \theta \in (0, \pi) \tag{A.22}$$

Equations (A.22) and (A.17) approximately match the results for general PolSK presented in [24],[50], with better alignment at higher SNR. It should be noted that the authors in [24] always reference the noiseless received vector to the north pole of the Poincaré sphere, so only f_Θ is a relevant point of comparison.

A.4 Optimal maximum-likelihood detector

Over each symbol interval, the detector outputs $\hat{m}$, an estimate of the message transmitted based on the (noisy) demodulated vector $\mathbf{w} = [\Theta, \Phi]$, which represents a distinct location on the surface of the rotated Poincaré sphere. An optimal detector is one that maximizes the probability of a correct decision, or, equivalently, minimizes the probability of an error. Going forward, we assume that all symbols are transmitted with equal probability ($P(\mathbf{s}_m) = 1/M$), so the ML criterion is optimum [49]. Equation (A.23) defines this decision rule at (ϑ_0, φ_0) given that $\mathbf{s}_m$ is transmitted. Its minimum distance approximation is given by Equation (A.24)) [49].

$$\hat{m} = \underset{1 \le m \le M}{\arg\max} \big[f_{\Theta,\Phi}(\mathbf{w} \mid \mathbf{s}_m) \big] \tag{A.23}$$

$$= \underset{1 \le m \le M}{\arg\min} \| \mathbf{w} - \mathcal{P}_m \| \tag{A.24}$$

The joint PDF $f_{\Theta,\Phi}$ is found from the product of Equations (A.17) and (A.22) because these distributions are statistically independent based on our initial assumptions. Figure A.2 is a plot of $f_{\Theta,\Phi}$ for a receiver at the intended direction (in this case, $[\vartheta = 90°, \varphi = 0°]$) when $\mathbf{s}_m = [90°, -90°]$. The joint cumulative distribution $F_{\Theta,\Phi}$ is the area under this 3-dimensional surface.

As described in [49], a minimum distance detector compares the Euclidean distances between $\mathbf{w}$ and all M symbol locations. In this case, it is more convenient to deal with orthodromic distances over the surface of a unit-radius sphere, where the term $\|\mathbf{w} - \mathcal{P}'_m\|$ becomes a central angle ζ:

$$\zeta(\mathbf{w}, \mathcal{P}'_m) = \cos^{-1} \big[\cos\Theta \cos\theta_m + \sin\Theta \sin\theta_m \cos|\phi_m - \Phi| \big] \tag{A.25}$$

In the corner case that $M = 2$ and the transmitter and receiver antennas are perfectly matched in polarization, simplified detection schemes may be used. The received signal set is equivalent to dual-channel on-off keying (OOK), and only average power measurements are required without the need to track relative phase between $\mathbf{v}$ and $\mathbf{h}$.

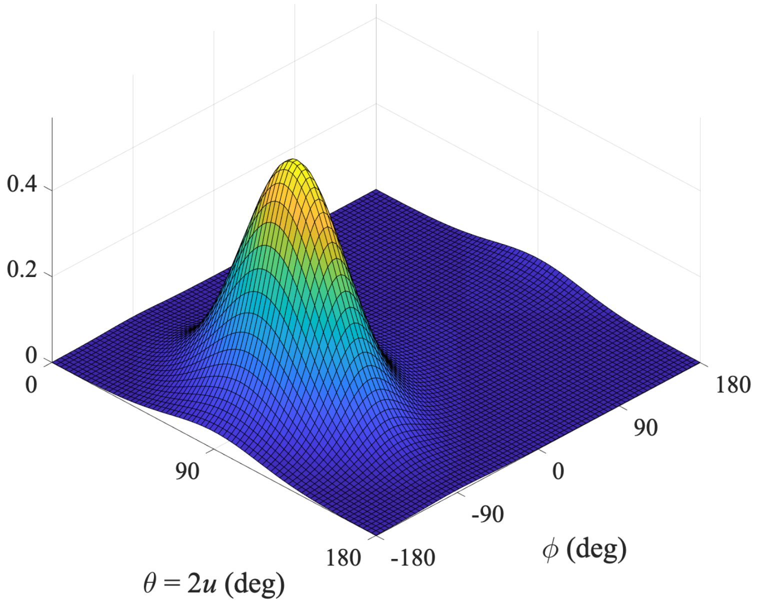


Figure A.2: The joint PDF $f_{\Theta,\Phi}(\theta, \phi)$ given $\mathbf{s}_m = [90°, -90°]$, SNR per symbol = 10 dB

A.5 Probability density functions for α, β

As an aside, it is possible to map the variables Φ, Υ to latitude and longitude on the unrotated Poincaré sphere based on the traditional definition in [46], but care must be taken because the mapping functions are not 1:1. As an academic exercise based on the mapping from Φ, Υ to 2α, 2β [46], we present Equation (A.26) for the joint PDF of $2A$ (latitude) and $2B$ (longitude), given a transmission of RHCP. The signum function arises to resolve the ambiguity in the inverse trigonometric relationships.

$$\begin{aligned} p_{2A,2B}(2\alpha, 2\beta | s_m = \text{RHCP}) = \frac{1}{4\pi^2} & \left[e^{-\psi_c/4} + \frac{\sqrt{\pi\psi_c}}{2} \left(\frac{-b}{\text{sgn}(2\beta)\sqrt{1+b^2}} \right) \right. \\ & \left. \times\, e^{-\psi_c/\left[4(1+b^2)\right]} \text{erfc} \left(\frac{\sqrt{\psi_c} b}{2\text{sgn}(2\beta)\sqrt{1+b^2}} \right) \right] \\ & \times \left\{ e^{-\psi_s} + \frac{\sqrt{\pi\psi_s}}{2} \left(\sqrt{1-a} + \sqrt{1+a} \right) \right. \\ & \left. \times\, e^{-\psi_s\left(1-\sqrt{1-a^2}\right)/2} \text{erfc} \left[\frac{-\sqrt{\psi_s}}{2} \left(\sqrt{1-a} + \sqrt{1+a} \right) \right] \right\} \end{aligned} \tag{A.26}$$

where

$$a = \cos 2\alpha \cos 2\beta \qquad b = \tan 2\alpha \csc 2\beta \tag{A.27}$$

Figure A.3 plots the joint PDF over $2\alpha, 2\beta$, with both incoming and post-limiter SNR levels of 10 dB. As expected, the latitude 2α has a maximum at $-90°$, but variation in longitude 2β is uniform since we are at a pole.

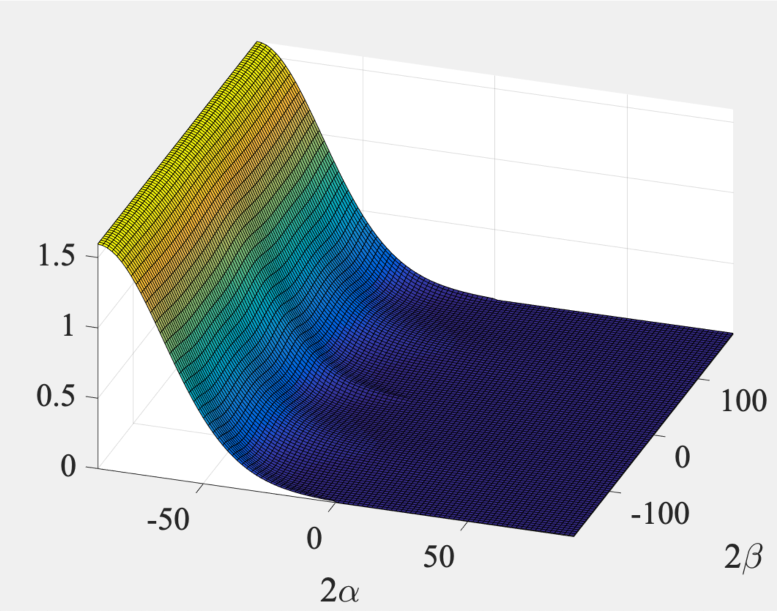


Figure A.3: The joint PDF $p_{2A,2B}(2\alpha, 2\beta)$ for s_m = RHCP ($2\alpha_m = -90°$, $2\beta_m$ = undefined)

APPENDIX B

SAPM HARDWARE ARCHITECTURE

For SAPM, the frontend may be implemented with fewer nonlinear components, such as mixers, in the signal path when compared to the traditional superheterodyne architecture. However, a beamforming network (BFN) is required, either digital or analog. In particular, the phase shifters and attenuators used in the BFN must be controlled at the symbol rate whereas conventional beamformers only need to operate these components at the beamsteering rate. Section B.1 discusses the transmitter frontend with examples of how to implement the required functionality for SAPM. Section B.2 presents several examples of possible receiver solutions, although any PolSK-capable receiver is acceptable.

B.1 Transmitter frontend

For conventional modulation techniques, the signal containing the message is generated at baseband and mixed up to the carrier frequency to be transmitted by the antennas. SAPM transmitters, however, accomplish the modulation by altering the complex weights on each antenna's feed in the array. A continuous wave signal at the carrier rate may be directly routed to each phase shifter and attenuator, which are controlled at the symbol rate. Figure B.1 is a simplified block diagram that illustrates this functionality (only one path of N is shown, where an N-element array would be used). The solid lines may be digital or analog, but their nominal frequency is the symbol rate $f_s = 1/T_s$. The dotted lines denote the RF path and operate at the carrier frequency, f_c. Only functional blocks are shown for clarity, so signal conditioning components like filters and matching elements are excluded.

The main benefit of this transmitter architecture is the reduction of nonlinear components in the signal path, which should significantly reduce the

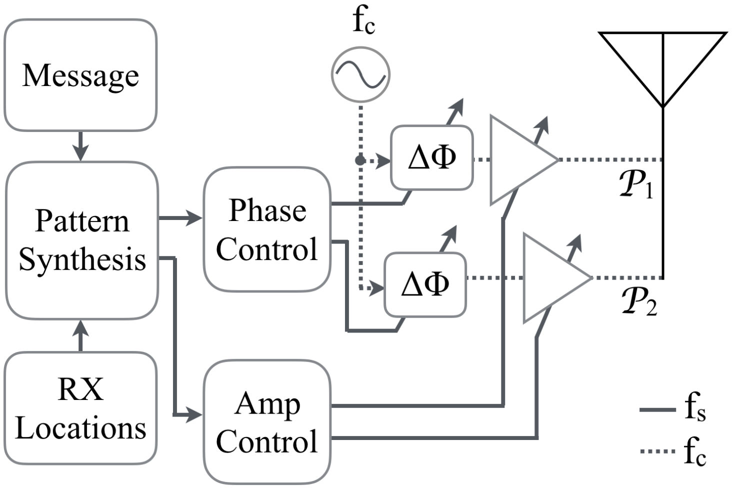


Figure B.1: Abstracted functional diagram of transmitter RF frontend

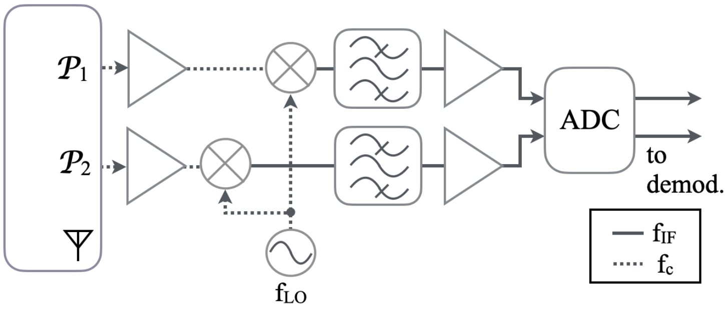
harmonics produced and help alleviate output filtering requirements. The remaining nonlinear feed components are almost always required with arrays, especially when beamsteering functionality exists.

B.2 Receiver frontend

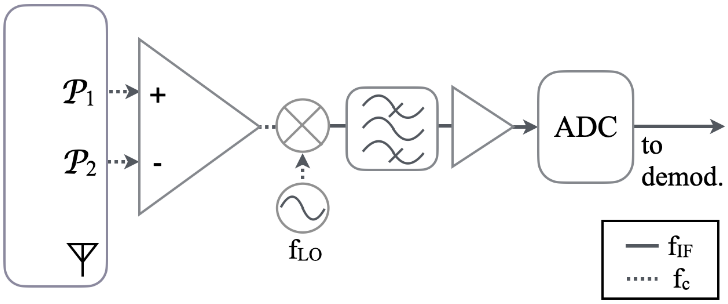
In general, SAPM is agnostic to receiver frontend architecture, as long as distinct paths exist for the reception of two orthogonally polarized signals. A single dual-polarized receive antenna may be used.

Two example receiver architectures are given in Figure B.2. To keep the explanation straightforward, we assume that the receiving antenna(s) is dual-polarized and outputs two orthogonal polarizations $\mathcal{P}_1$ and $\mathcal{P}_2$. If we keep the paths separate and use a dual-channel ADC as in Figure B.2a, the receiver frontend may be implemented with a conventional superheterodyne architecture (here we show one stage with a local oscillator at frequency f_{LO} to mix down to the intermediate frequency f_{IF}).

When using this technique for binary modulation, the ADC input channel may be collapsed into a single one if $\mathcal{P}_1$ and $\mathcal{P}_2$ are actually the two states used, shown in Figure B.2b. In this case, each symbol state simply depends on whether a signal is present on the dual lines from the antenna(s). If $\mathcal{P}_1$ and $\mathcal{P}_2$ are in-phase at the transmitter and the pattern switching mechanism is phase-locked to the carrier frequency, the output of the differential amplifier



(a) Any order modulation



(b) Order 2 modulation

Figure B.2: Two example functional diagrams of SAPM receiver architecture

at the receiver will be very similar to a BPSK signal, especially if a limiter is included in the path. Depending on carrier frequency, it may be prudent to move the down-conversion stage (mixer/LO/filter) before the differential amplifier, requiring two sets of RF components.

APPENDIX C

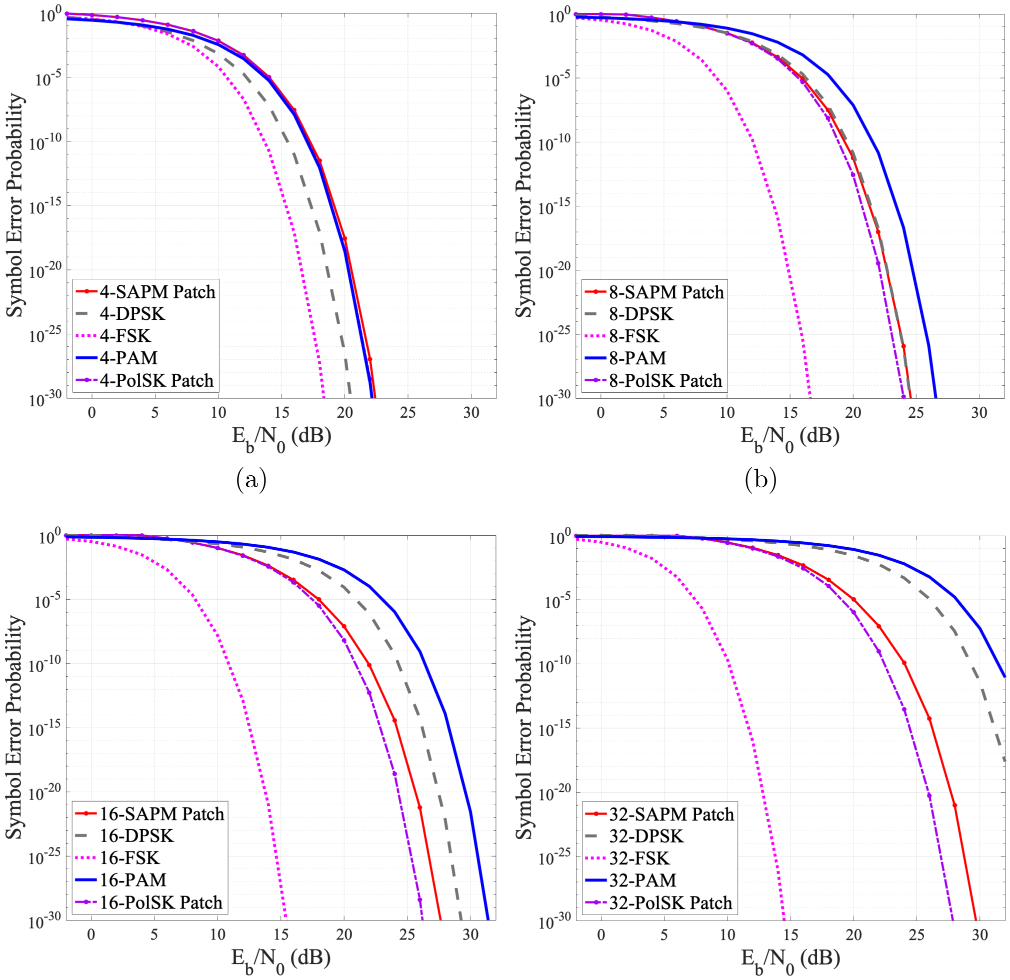
SAPM ERROR PERFORMANCE COMPARED TO OTHER MODULATION SCHEMES

In the course of this investigation, we generally relied on a beamformer using DPSK to compare against SAPM performance due to the fact that it is a well-known method that may provide a clear reference point. Additionally, like SAPM and PolSK, it may be demodulated noncoherently. However, extending the analysis to other methods, such as frequency-shift keying (FSK) and pulse-amplitude modulation (PAM), can also provide useful information. Figure C.1 includes the theoretical AWGN error probabilities for these modulation schemes over E_b/N_0 for $M = 4$, 8, 16, and 32 [49].

In the cases of PolSK and SAPM, the antenna design has a non-negligible impact that was explored in Chapter 5. In these figures, we limit the data to the simulated radiation of the square microstrip patch array. The nominal constellations transmitted to intentional receivers are identical between PolSK and SAPM, which clearly have an offset in error performance. The main factor for the difference is the increased XPD in the SAPM secondary polarization; see Chapter 5 for the complete analysis. For FSK, noncoherent demodulation is used, and it is evident that when possible, FSK is preferred from an error-minimizing perspective. Of course, FSK is very expensive when modulation order is high, due to the required bandwidth.

Figures C.2-C.4 summarize the expected error performance over azimuth for these methods. As in Chapter 4, error ratios are made equal in Bob's direction by adjusting the total power transmitted in each approach. The E_b/N_0 at Bob for SAPM is reported in the figure captions, but the corresponding E_b/N_0 for each method may be read off the plots in Figure C.1. This adjustment allows us to compare the information beamwidth, and, in general, a system would not transmit more power than necessary to achieve a certain target error rate at the intended receiver.

While it is true that for $M = 16$ and 32, FSK and PolSK begin to show slightly narrower information beamwidths as compared to DPSK and PAM,



(a) (b)

(c) (d)

Figure C.1: Theoretical symbol error probabilities over E_b/N_0 for an extended comparison of modulation schemes; simulations use the square patch array; DPSK, FSK, and PAM equations from [49]; PolSK from [50]; SAPM derived in Chapter 4

it is obvious that the narrowing effect is significantly more pronounced for SAPM.

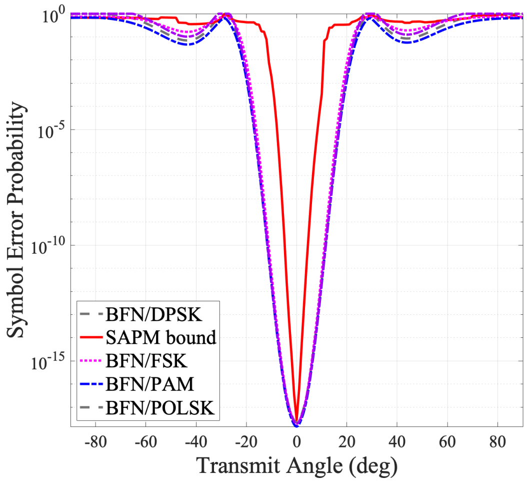


Figure C.2: Theoretical 4-SAPM uncoded error probability over azimuth compared to beamforming using other techniques; average SAPM $E_b/N_0 = 20$ dB for Bob at $\varphi = 0°$; corresponding E_b/N_0 for all methods may be found from Figure C.1; 1/2 of P_{RF} in secondary SOP

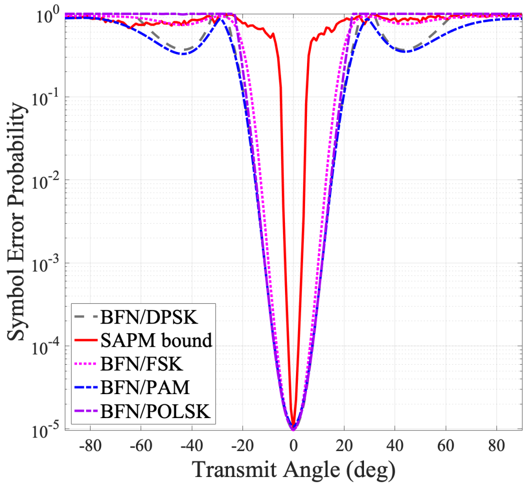


Figure C.3: Theoretical 16-SAPM uncoded error probability over azimuth compared to beamforming using other techniques; average SAPM $E_b/N_0 = 18$ dB for Bob at $\varphi = 0°$; corresponding E_b/N_0 for all methods may be found from Figure C.1; 1/2 of P_{RF} in secondary SOP

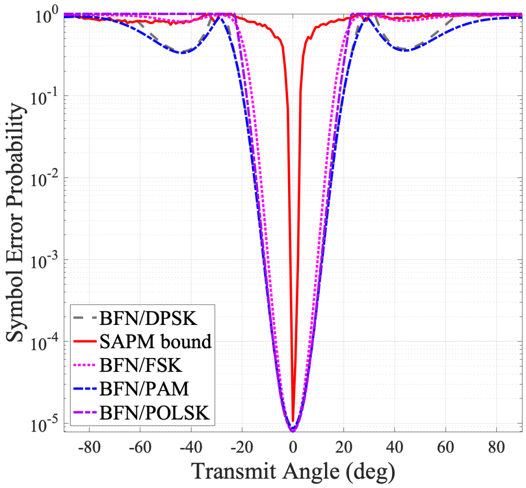


Figure C.4: Theoretical 32-SAPM uncoded error probability over azimuth compared to beamforming using other techniques; average SAPM $E_b/N_0 = 20$ dB for Bob at $\varphi = 0°$; corresponding E_b/N_0 for all methods may be found from Figure C.1; 1/2 of P_{RF} in secondary SOP

APPENDIX D

ADDITIONAL SAPM GAIN AND POLARIZATION INFORMATION

Much of the analysis in the main body of this dissertation is based on 4-SAPM and 16-SAPM, but we did simulations up to $M = 32$ and testing up to $M = 16$. In this appendix, we include details on the actual polarization states (SOPs) for each modulation order used. Tables D.1-D.5 are the nominal SOPs transmitted by Alice to the intended receiver Bob, in spherical coordinates $[\theta, \phi]$ on the surface of a rotated unit-radius Poincaré sphere in Stokes space. As a reminder, the polarization ratio $\mathcal{P}$ is $[\tan(\theta/2)]\, e^{j\phi}$ [46]. For this investigation, the north pole is thus horizontal linear polarization instead of RHCP (optics) or LHCP (microwave theory). The spherical constellation may be calculated a number of ways—we modified an algorithm based on minimizing Reisz s-energy to instead optimize based on the minimum central angle of the nearest neighboring point [66]. For certain special cases ($M = 4, 8$), we used the vertices of an inscribed regular polyhedron, although this may not necessarily produce the most optimal error performance [24].

We also include in Figures D.1-D.3 the gain patterns for binary and 8-SAPM, as a reference. The patterns for 4-SAPM are given in Chapter 6. No recalibration or tuning was done to adjust the null locations, although that may be desirable in actual deployment. In general, while the plots obviously represent gain in *different* SOPs, the pattern shapes themselves look very similar, and thus we limited the inclusion of these to $M = 8$.

Table D.1: Binary SAPM: nominal SOP represented by spherical coordinates $[\theta, \phi]$ for transmission to the intended receiver

Symbol (binary)	θ (deg)	ϕ (deg)
0	90.00	90.00
1	90.00	-90.00

Table D.2: 4-SAPM: nominal SOP represented by spherical coordinates $[\theta, \phi]$ for transmission to the intended receiver

Symbol (binary)	θ (deg)	ϕ (deg)
00	129.41	22.53
01	75.41	125.95
10	116.00	-129.20
11	34.78	-42.19

Table D.3: 8-SAPM: nominal SOP represented by spherical coordinates $[\theta, \phi]$ for transmission to the intended receiver

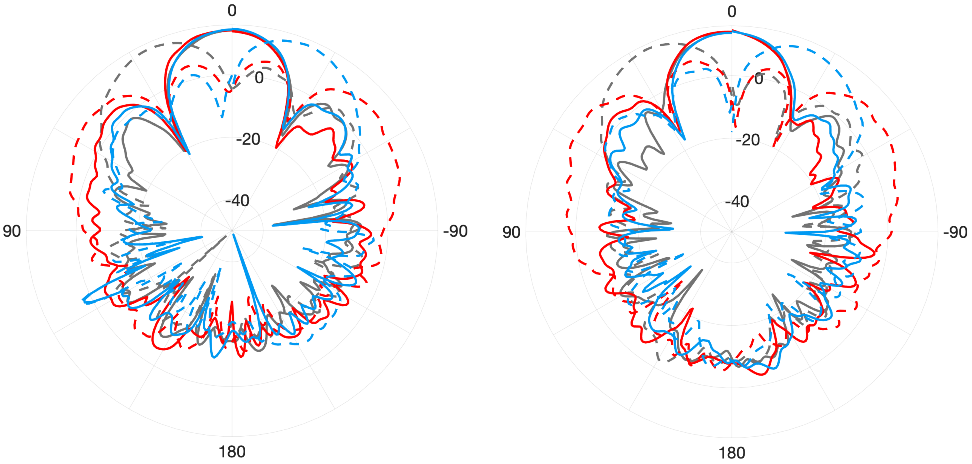
Symbol (binary)	θ (deg)	ϕ (deg)
000	54.74	45.00
001	54.74	135.00
010	54.74	-135.00
011	54.74	-45.00
100	125.26	-45.00
101	125.26	45.00
110	125.26	135.00
111	125.26	-135.00

Table D.4: 16-SAPM: nominal SOP represented by spherical coordinates $[\theta, \phi]$ for transmission to the intended receiver

Symbol (binary)	θ (deg)	ϕ (deg)
0000	66.33	-38.91
0001	98.98	161.60
0010	149.38	-94.99
0011	79.23	64.90
0100	18.87	-99.98
0101	153.10	136.82
0110	115.89	-147.22
0111	88.38	10.05
1000	49.75	122.43
1001	129.04	-23.34
1010	57.00	-169.17
1011	70.89	-111.80
1100	132.73	46.86
1101	101.47	-74.39
1110	35.59	28.93
1111	104.43	108.23

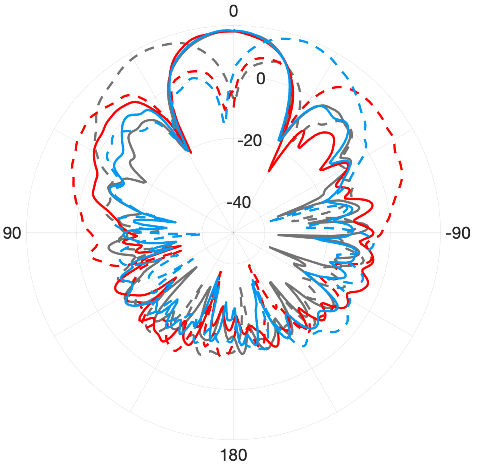
Table D.5: 32-SAPM: nominal SOP represented by spherical coordinates $[\theta, \phi]$ for transmission to the intended receiver

Symbol (binary)	θ (deg)	ϕ (deg)
00000	82.98	32.34
00001	36.97	-100.22
00010	114.50	176.97
00011	101.90	-74.34
00100	59.05	140.28
00101	32.97	179.99
00110	58.58	-141.57
00111	65.91	-69.53
01000	106.73	0.19
01001	41.06	24.85
01010	177.03	-145.02
01011	115.21	-114.67
01100	112.94	111.24
01101	61.11	62.85
01110	147.60	0.37
01111	3.01	30.85
10000	140.26	-151.07
10001	77.91	-107.26
10010	74.55	-179.72
10011	97.17	-147.03
10100	84.67	-36.83
10101	95.57	145.69
10110	141.15	-80.17
10111	76.57	103.61
11000	121.45	-39.22
11001	121.44	38.68
11010	69.72	-6.16
11011	37.30	99.98
11100	39.57	-36.51
11101	99.14	71.89
11110	140.47	142.87
11111	141.91	79.70

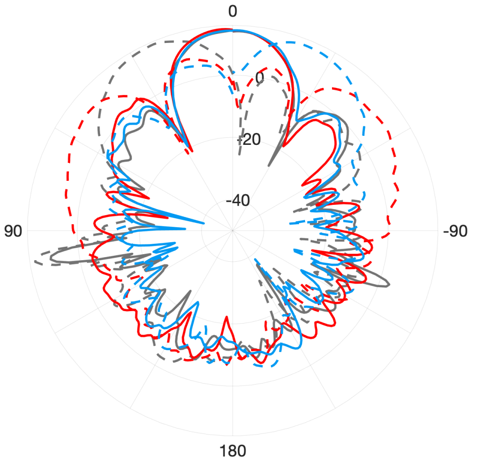


(a) Symbol 1 (b) Symbol 2

Figure D.1: Measured gain (dB) of the patch array configured for binary SAPM at 2.4 GHz with $L = 3$ options for each symbol; solid lines denote primary SOP (current symbol); dashed lines denote simultaneous antipodal SOP with target main beam directions $[-28^\circ, 28^\circ, 90^\circ]$; Bob at 0°; 1/2 of P_{RF} in secondary SOP

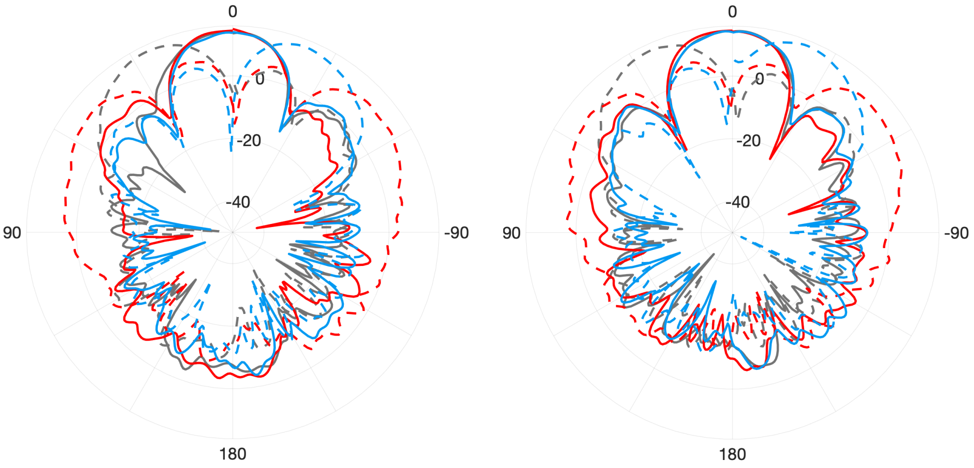


(a) Symbol 1 (b) Symbol 2

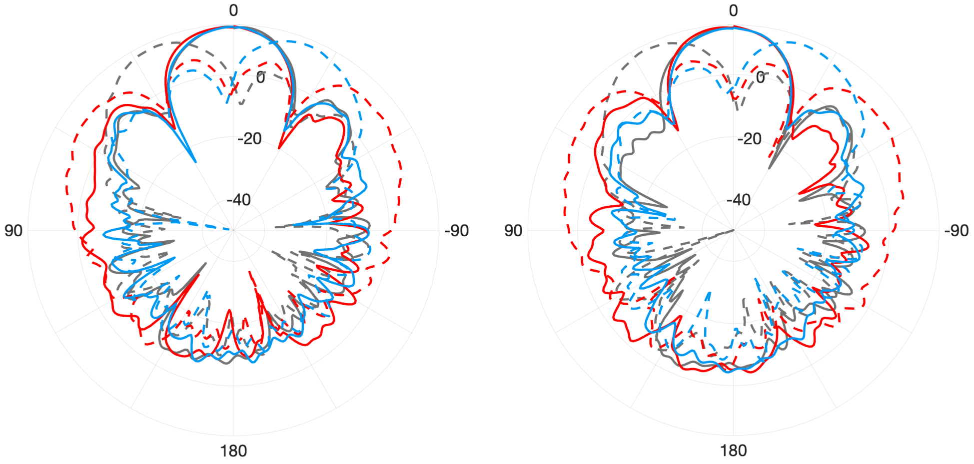


(c) Symbol 3 (d) Symbol 4

Figure D.2: Symbols 1-4: measured gain (dB) of the patch array configured for 8-SAPM at 2.4 GHz with $L = 3$ options for each symbol; solid lines denote primary SOP (current symbol); dashed lines denote simultaneous antipodal SOP with target main beam directions $[-28°, 28°, 90°]$; Bob at 0°; 1/2 of P_{RF} in secondary SOP



(a) Symbol 5 (b) Symbol 6



(c) Symbol 7 (d) Symbol 8

Figure D.3: Symbols 5-8: measured gain (dB) of the patch array configured for 8-SAPM at 2.4 GHz with $L = 3$ options for each symbol; solid lines denote primary SOP (current symbol); dashed lines denote simultaneous antipodal SOP with target main beam directions $[-28°, 28°, 90°]$; Bob at 0°; $1/2$ of P_{RF} in secondary SOP

REFERENCES

[1] "2017 Internet Crime Report," 2018, Federal Bureau of Investigation, Internet Crime Complaint Center. [Online]. Available: https://pdf.ic3.gov/2017_IC3Report.pdf

[2] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 4, pp. 42–56, 2009.

[3] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," in *Proc. IEEE*, vol. 104, no. 9, Sep. 2016, pp. 1727–1765.

[4] *Open Systems Interconnection-Basic Reference Model: Naming and Addressing*, ISO/IEC Std. 7498-1, 1994.

[5] Y. Shiu, S. Y. Chang, H. Wu, S. C. Huang, and H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[6] P. Misra and P. Enge, *Global Positioning System (GPS): Signals, Measurements and Performance*, 2nd ed. Lincoln, MA: Ganga-Jamuna Press, 2011.

[7] Dept. of Homeland Security, "Risks to U.S. critical infrastructure from global positioning system disruptions," The National Risk Estimate, Tech. Rep. IATF/HITRAC, Nov. 2012.

[8] S. Pullen and G. Gao, "GNSS jamming in the name of privacy: Potential threat to GPS aviation," Mar. 2012, *Inside GNSS*. [Online]. Available: http://insidegnss.com/auto/marapr12-Pullen.pdf

[9] G. Gibbons, "FCC fines operator of GPS jammer that affected Newark airport GBAS," Aug. 2013, *Inside GNSS*. [Online]. Available: http://www.insidegnss.com/node/3676

[10] "Satellite navigation ground based augmentation system (GBAS)," Apr. 2018, Federal Aviation Administration. [Online]. Available: https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/laas/

[11] I. J. Gupta, I. Weiss, and A. Morrison, "Desired features of adaptive antenna arrays for GNSS receivers," in *Proc. IEEE*, vol. 104, no. 6, June 2016, pp. 1195–1206.

[12] J. L. Volakis, A. O'Brien, and C.-C. Chen, "Small and adaptive antennas and arrays for GNSS applications," in *Proc. IEEE*, vol. 104, no. 6, June 2016, pp. 1221–1232.

[13] U. Rohde, J. Whitaker, and H. Zahnd, *Communications Receivers: Principles and Design*, 4th ed. New York, NY: McGraw-Hill Education, 2017.

[14] R. Schmidt, "Multiple emitter location and signal parameter estimation," *IEEE Trans. Antennas Propag.*, vol. 34, pp. 276–280, Mar. 1986.

[15] N. C. Karmakar, Ed., *Handbook of Smart Antennas for RFID Systems.* Hoboken, NJ: John Wiley and Sons, 2010.

[16] H. Paaso, A. Mammela, D. Patron, and K. R. Dandekar, "Modified MUSIC algorithm for DOA estimation using CRLH leaky-wave antennas," in *8th Int. Conf. Cognitive Radio Oriented Wireless Networks*, July 2013, pp. 166–171.

[17] R. Penno and K. Pasala, "Theory of angle estimation using a multiarm spiral antenna," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 37, no. 1, pp. 123–133, Jan. 2001.

[18] C. Y. Kataria, G. X. Gao, and J. T. Bernhard, "Design of a compact hemispiral GPS antenna with direction finding capabilities," *IEEE Trans. Antennas Propag.*, vol. 67, no. 5, pp. 2878–2885, May 2019.

[19] A. Mukherjee, S. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Feb. 2014.

[20] H. V. Poor, M. Goldenbaum, and W. Yang, "Fundamentals for IoT networks: Secure and low-latency communications," in *Proc. 20th Int. Conf. Distributed Comput. Netw.*, Bangalore, India, Jan. 2019, pp. 362–364.

[21] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[22] M. P. Daly and J. T. Bernhard, "Directional modulation technique for phased arrays," *IEEE Trans. Antennas Propag.*, vol. 57, no. 9, pp. 2633–2639, Sep. 2009.

[23] C. Balanis, *Antenna Theory: Analysis and Design.* Hoboken, NJ: John Wiley and Sons, 2016.

[24] S. Benedetto and P. T. Poggiolini, "Multilevel polarization shift keying: Optimum receiver structure and performance evaluation," *IEEE Trans. Commun.*, vol. 42, no. 2/3/4, pp. 1174–1186, Feb/Mar/Apr 1994.

[25] X. Wu, T. G. Pratt, and T. E. Fuja, "Polarization shift keying for wireless communication," *IEEE Trans. Wireless Commun.*, Aug. 2019, Early Access.

[26] C. Y. Kataria and J. T. Bernhard, "Antenna evaluation for increased security in polarization modulation," in *13th European Conf. Antennas Propag. (EuCAP)*, Krakow, PL, 2019.

[27] K. T. Wong and Y. I. Wu, "Spatial-polarizational correlation-coefficient function between receiving-antennas in radiowave communications – geometrically modeled, analytically derived, simple, closed-form, explicit formulas," *IEEE Trans. Commun.*, vol. 57, no. 12, pp. 3566–3570, Dec. 2009.

[28] Y. Ding and V. Fusco, "Polarization distortion as a means for securing wireless communication," in *8th European Conf. Antennas Propag. (EuCAP)*, The Hague, 2014.

[29] Z. Luo, H. Wang, and W. Lv, "Directional polarization modulation for secure transmission in dual-polarized satellite MIMO systems," in *8th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Yangzhou, China, 2016.

[30] Q. Zhang, Z. Yang, W. Wang, J. Ren, W. Huang, and N. Zhang, "A dual-polarized antennas based directional modulation scheme," in *26th Int. Conf. Telecommun. (ICT)*, Hanoi, Vietnam, 2019, pp. 468–473.

[31] X. Zhang, B. Zhang, and D. Guo, "Physical layer secure transmission based on fast dual polarization hopping in fixed satellite communication," *IEEE Access*, vol. 5, pp. 11 782–11 790, 2017.

[32] C. Y. Kataria, S. J. Franke, G. X. Gao, and J. T. Bernhard, "Theory of secure antenna polarization modulation for line-of-sight propagation," in review.

[33] Y. Zhao, D. Hu, Z. Liu, and Y. Zhao, "Calibrating the transmitter and receiver location errors for moving target localization in multistatic passive radar," *IEEE Access*, vol. 7, pp. 118 173–118 187, 2019.

[34] G. Lasser, J. Cazden, and D. Filipovic, "A spiral antenna for amplitude-only direction finding," in *Proc. IEEE Int. Symp. Antennas Propag.*, July 2017.

[35] L. J. Chu, “Physical limitations of omni-directional antennas,” *IEEE Trans. Antennas Propag.*, vol. 19, no. 12, pp. 1163–1175, 1948.

[36] J. J. Adams, S. C. Slimmer, T. F. Malkowski, E. B. Duoss, J. A. Lewis, and J. T. Bernhard, “Comparison of spherical antennas fabricated via conformal printing: Helix, meanderline, and hybrid designs,” *IEEE Antennas Wireless Propag. Lett.*, vol. 10, pp. 1425–1428, Dec. 2011.

[37] P. E. Mayes, “Frequency-independent antennas and broad-band derivatives thereof,” in *Proc. IEEE*, vol. 80, no. 1, Jan. 1992, pp. 103–112.

[38] *High Frequency Structure Simulation (HFSS)*, ANSYS, Inc. Std., Rev. 16.2, 2015.

[39] J. D. Krieger, W. F. Moulder, A. J. Chapman, C. Yang, and P.-F. Wolfe, “6-10 GHz circularly-polarized multistatic array for standoff microwave imaging,” in *Proc. IEEE Int. Symp. Antennas Propag.*, July 2018.

[40] W. J. Dally and J. W. Poulton, *Digital Systems Engineering*, 1st ed. Cambridge, UK: Cambridge University Press, 1998.

[41] C. Y. Kataria, J. T. Bernhard, and G. X. Gao, “A single hemispiral antenna for GNSS interference mitigation and direction estimation,” in *Proc. 30th Int. Tech. Meeting Satellite Division Inst. Navigation (ION GNSS+)*, Portland, OR, Sep. 2017, pp. 3453–3459.

[42] C. Y. Kataria, G. X. Gao, and J. T. Bernhard, “Design of a compact hemispiral antenna for increased GPS security,” in *Proc. Allerton Antennas Symp.*, Monticello, IL, Sep. 2017, pp. 75–79.

[43] G. Yule and M. Kendall, *An Introduction to the Theory of Statistics*, 14th ed. London, England: Charles Griffin, 1968.

[44] M. Mirmozafari, S. Karimkashi, and G. Zhang, “An overview of dual polarized isolated antennas,” in *Proc. IEEE Int. Symp. Antennas Propag.*, 2016, pp. 1893–1894.

[45] J. N. Damask, *Polarization Optics in Telecommunications.* New York, NY: Springer, 2005.

[46] G. A. Deschamps, “Techniques for handling elliptically polarized waves with special reference to antennas: Part II - geometrical representation of the polarization of a plane electromagnetic wave,” *Proc. IRE*, vol. 39, no. 5, pp. 540–544, May 1951.

[47] R. L. Haupt, “Phase-only adaptive nulling with a genetic algorithm,” *IEEE Trans. Antennas Propag.*, vol. 45, no. 6, pp. 1009–1015, June 1997.

[48] I. Dabbura, "K-means clustering: Algorithm, applications, evaluation methods, and drawbacks," Sep. 2018, Towards Data Science. [Online]. Available: https://towardsdatascience.com

[49] J. G. Proakis and M. Salehi, *Digital Communications*, 5th ed. New York, NY: McGraw-Hill Education, 2008.

[50] C. Guo, X. Wu, C. Feng, and Z. Zeng, "Spectrum sensing for cognitive radios based on directional statistics of polarization vectors," *IEEE J. Select. Areas Commun.*, vol. 31, no. 3, pp. 379–393, Mar. 2013.

[51] T. Hailperin, *Boole's Logic and Probability*, 2nd ed. Amsterdam, the Netherlands: Elsevier Science Publishers, 1986.

[52] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[53] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[54] M. P. Daly, "Physical layer encryption using fixed and reconfigurable antennas," Ph.D. dissertation, Dept. Elect. Comput. Eng., Univ. Illinois, Urbana-Champaign, May 2012.

[55] "MAPS-010164 data sheet," MACOM, Lowell, MA.

[56] J. Lee, K. Kapitanova, and S. H. Son, "The price of security in wireless sensor networks," *Comput. Networks: Int. J. Comput. Telecommun. Networking*, vol. 54, no. 17, pp. 2967–2978, Dec. 2010.

[57] D. H. Bui, D. Puschini, S. Bacles-Min, E. Beigne, and X. T. Tran, "AES datapath optimization strategies for low-power low-energy multisecurity-level Internet-of-Things applications," *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 25, no. 12, pp. 3281–3290, 2017.

[58] C. Y. Kataria, S. J. Franke, and J. T. Bernhard, "Signal-to-noise ratio considerations for secure antenna polarization modulation," in *14th European Conf. Antennas Propag. (EuCAP)*, Copenhagen, DK, 2020.

[59] S. Kuo and C. Liu, "Multiple polarization spiral antenna," U.S. Patent 3 562 756, Feb. 9, 1971.

[60] J. D. Dyson, "The equiangular spiral antenna," *IRE Trans. Antennas Propagat.*, pp. 181–187, Apr. 1959.

[61] M. D. McKinley, K. A. Remley, M. Myslinski, J. S. Kenney, D. Schreurs, and B. Nauwelaers, "EVM calculation for broadband modulated signals," in *64th ARFTG Conf. Dig.*, Orlando, FL, Dec. 2004, pp. 45–52.

[62] “Cross polar discrimination (XPD),” Mar. 2020, Halberd Bastion. [Online]. Available: https://halberdbastion.com/resources/academic/rf-parameters/cross-polar-discrimination-xpd

[63] M. Matsumoto and T. Nishimura, “Mersenne twister: A 623-dimensionally equidistributed uniform pseudo-random number generator,” *ACM Transactions on Modeling and Computer Simulation*, vol. 8, no. 1, pp. 3–30, Jan. 1998.

[64] S. Ross, *A First Course in Probability*, 9th ed. Boston, MA: Pearson Education, 2014.

[65] S. Okui, “Probability distributions for ratios of fading signal envelopes and their generalization,” *Electron. Commun. Japan*, vol. 64, no. 3, pp. 72–80, 1981.

[66] A. Semechko, “Particlesamplesphere,” July 2019, GitHub. [Online]. Available: https://github.com/mrezanejad/3DAOFSkeletons/blob/master/Libs/sampling%20sphere/ParticleSampleSphere.m