PHYSICAL LAYER ENCRYPTION USING FIXED AND RECONFIGURABLE ANTENNAS

BY

MICHAEL P. DALY

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, 2012

Urbana, Illinois

Doctoral Committee:

Professor Jennifer Bernhard, Chair
Professor Andreas Cangellaris
Professor Steven Franke
Professor Douglas Jones

ABSTRACT

Traditionally, antenna systems have been designed to achieve reliable wireless communication, while the problem of securing that communication from eavesdropping was left to mathematical cryptography. Recent research into physical layer encryption shows that jointly designing for reliability and secrecy at the physical layer may be a better solution. Physical layer encryption involves techniques that ensure a signal is information-theoretically secure, meaning that an eavesdropper with infinite time and computational resources will not be able to decode a message. Such techniques include purposely broadcasting artificial noise, transmitting direction-dependent signals, and opportunistic communications. This work addresses different methods for broadcasting artificial noise using fixed arrays, including tradeoffs with power usage and computational complexity. In addition, a method of producing direction-dependent distortion using reconfigurable arrays is also shown. These two methods are combined and shown to be more secure and power-efficient than either in isolation. An analysis of secrecy rates through mutual information makes it possible to compare the performance of all the various secure communication techniques. Simulations with various wireless channels as well as an experimental test using a fixed and reconfigurable array are presented.

ACKNOWLEDGMENTS

First, I thank my advisor Jennifer Bernhard for her mentorship and thoughtful guidance, shaping a green and unsure undergraduate into a self-confident Doctor of Philosophy. It's been quite a journey.

I would also like to thank the other members of my committee: Andreas Cangellaris, Steven Franke, and Douglas Jones for their guidance and insight.

I thank my parents for giving me their smart genes and for providing a loving and nurturing home in which I could reach my full potential. I cannot think of anything better.

Thank you Mary for excelling at your job.

Finally I thank my loving wife, business partner, and occasional research collaborator Erica for her support over these college years. Much of this thesis was inspired by our long walks down Green Street discussing wireless communications among other deep thoughts.

I would like to acknowledge the generous support of the NDSEG and SMART fellowships that funded the work of this dissertation.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Cryptographic vs. Information Theoretic Security

The broadcast nature of the wireless channel poses an inherent challenge for secure communications. Traditionally, the problem of security has been handled through cryptographic techniques, and was separate from the problem of reliable communication. The cryptographic methods that ensure security today fall into two categories: asymmetric and symmetric [1]. Symmetric encryption requires identical keys to be held by the sender and receiver, and when this condition is met, it is an efficient and simple way to transmit secure information. In the 1940s, Shannon proved that if the key length is greater than or equal to the message length, known as a one-time pad encryption, then it is theoretically impossible for an enemy to decode the message without the key [2]. Shannon termed this "perfect secrecy."

The impracticality of this method is that the key must be securely shared beforehand between the two parties and the key length is equal to the message length. Thus, the nature of the message would have to be known at the time of sharing the keys, so instead the actual message should simply be exchanged in that secure environment. Because of the need to be able to communicate securely without the luxury of a private secure channel to exchange keys, asymmetric encryption, also known as public-key cryptography, was developed with a key-exchange framework by Diffie and Hellman in 1976 followed by a practical implementation by Rivest, Shamir, and Adelman in 1978 [3, 4]. The public-key method works as follows. Assume the transmitter known as Alice would like to send a secure message to a receiver known as Bob without an eavesdropper, Eve, decoding that message. First, Bob generates a public key and private key and broadcasts his public key over a public channel. Alice uses Bob's public key to encode her message and transmits the encoded message. Only Bob can decode the message with his private key, which he did not transmit at all.

Communications today uses a combination of asymmetric encryption to handle key exchange and symmetric encryption to efficiently encrypt and decrypt parts of messages with a secure key [1]. However, public-key cryptography is not information theoretically secure like Shannon's one-time pad. The public and private keys are mathematically related, but there is no efficient way of computing the private key from the public key because it involves factoring the product of two large prime numbers. However, if Eve has infinite computational resources, determining the private key is possible. Information theoretic security implies that even with infinite computational resources, Eve still does not have enough information to break the encryption. More practical encryption techniques that are information theoretically secure have been developed and are described in the next section.

1.2 Information Theoretic Security

Research into information theoretic security began with the wiretap channel model proposed by Wyner [5]. Wyner showed that secure communication could occur when Eve had a probabilistically worse channel to Alice than did Bob. Secrecy arose from exploiting the theoretical rate at which Bob and Eve could decode messages based on their channels, rather than a key-based encryption scheme. Work in [6] generalized the analysis to two channels of which Eve's is not necessarily a degraded version of Bob's channel, and defined secrecy rate as the difference in channel capacities between Alice and Bob and Alice and Eve. If this difference is negative, meaning Eve has a better channel to Alice than does Bob, the secrecy rate is zero. Secrecy capacity is the supremum of all achievable secrecy rates [7]. Later work showed that secure communication could occur even when Eve's channel was statistically better than Bob's channel, but the rate of this communication may be too slow to be practical for sending data and only good for symmetric key exchanges [8]. The initial work on secrecy rates assumed additive white Gaussian noise (AWGN) channels, but subsequent analysis on fading channels also demonstrated secure communication is possible even when Eve has a better signal-to-noise ratio (SNR) on average [9, 10]. Current information theoretic security research falls into one of two branches: secret key agreement and keyless secure communications [7].

1.2.1 Secret Key Agreement

Secret key agreement involves ways that Alice and Bob can generate a common key for symmetric encryption while only publicly communicating and not using public-key cryptography. One method proposed is to use the common channel between Alice and Bob to construct a key. If reciprocity of the channel is assumed, then Alice and Bob should be able to sense the same channel magnitude and phase between them, which can be used to mathematically generate a key or transmit information at a low rate [11]. Using multiple-input multiple-output (MIMO) antenna arrays allows more than one channel estimate at a time, increasing the key complexity and security [12]. Experimental results with four-element arrays indicate that a high number of key bits can be generated with each channel observation [13].

1.2.2 Keyless Secure Communications

Work in keyless communications that is secured using the physical layer has progressed much, especially in recent years, since Wyner's initial 1975 paper. Secrecy capacity bounds have been derived for multiple antennas at the transmitter, receiver, and with collaborating eavesdroppers [14, 15, 16, 17, 18]. These bounds are derived with the unrealistic assumption that the transmitter knows its channel to Eve, and it was shown that the secrecy rate can be substantially less than this bound if only the statistics of Eve's channels are assumed [17].

Recent research on keyless secure communications involves developing implementable schemes to achieve secrecy capacity. In [19], the authors showed there exists an achievable secrecy rate for an AWGN main channel and an arbitrarily better (on average) Rayleigh fading eavesdropper channel by using Gaussian random codes, artificial noise injection, and power bursting. Artificial noise injection also was proposed in [16, 17] for security when using MIMO antennas in the presence of collaborating eavesdroppers. Practical artificial noise implementations using fixed arrays recently have been proposed

[20, 21, 22], with MIMO secrecy capacity for the AWGN channel derived in [23] and minimum guaranteed secrecy capacity for a fading channel found in [24]. Optimum power allocation between the signal power and artificial noise power was derived in [25] and later adjusted in [26] to account for imperfect channel state information (CSI). A very different optimal power allocation was found in [27], which assumed ordinary finite alphabet modulation schemes instead of a Gaussian alphabet.

Injecting artificial noise is not the only method of actively securing a transmission. Instead, the transmitted constellation can be created by a fixed or reconfigurable array in such a way that it becomes distorted in directions other than Bob's direction. Using a technique called near-field direct antenna modulation (NFDAM), a parasitic array is used to synthesize a quadrature amplitude modulation (QAM), which is transmitted undistorted in the desired direction but distorted in other directions [28, 29, 30]. This distortion makes the signal more difficult to decode in the presence of noise. This approach is similar to a direction-dependent signaling of [31], in which phase-shift keying is transmitted by rapid switching between transmit antennas within an array. By switching antennas instead of changing the phase of the transmitted signal, the phase shift varies based on the transmit direction. In a very similar fashion, [32] uses a two-element array with switched discrete phase shifts. Another spatially dependent signaling technique uses a spreading sequence to randomly shift the phase center of an array to generate a direction-dependent signal [33], while a technique in [34] uses a multi-feed Cassegrain antenna in which the sum beam passes an undistorted constellation but the difference beams transmit distorted versions.

These techniques are similar to another direction-dependent signaling technique called directional modulation (DM). DM can be used with any basic modulation, such as quadrature phase-shift keying (QPSK) or QAM, to produce a constellation that is undistorted to a desired receiver while distorted in most other directions, making the signal more difficult to decode by eavesdroppers. This requires a transmit array, but the receiver may have only a single element. In [35, 36], DM is used by a phased array to achieve low bit error rates (BERs) communicating with the desired receiver while enforcing higher BERs in other line-of-sight (LOS) directions by distorting the transmitted constellation. The same DM technique also was demonstrated in [37] with an array of reconfigurable antenna elements. Simulated and experimental results of DM using a phased array are presented in the appendix. These techniques are consolidated into a single reconfigurable array signal distortion technique presented here.

1.3 Dissertation Overview

All of the scenarios in this dissertation comparing the secrecy of various encryption methods assume that the desired receiver and eavesdroppers all have a single element and a constant channel. This also implies that no eavesdroppers may move around to find a less distorted message signal. The transmitter is not aware of the location of the eavesdroppers, but the eavesdropper is always assumed to know its channel to the transmitter.

Chapter 2 discusses physical layer security through artificial noise using fixed arrays. Existing artificial noise algorithms will be contrasted with two new proposed algorithms that generate artificial noise with lower computational demands. One of the new algorithms uses additive artificial noise (AAN) similar to the current algorithms in the literature, while the other uses multiplicative artificial noise (MAN), which is mathematically different and has tradeoffs relative to AAN. The metrics of secrecy capacity and mutual information (MI) for assessing the security of each algorithm are discussed in detail. Finally, all artificial noise algorithms are compared on a simulated Rayleigh fading channel for different power allocations between signal and interference power.

Chapter 3 explains another method for generating artificial noise through switching a reconfigurable array transmitter, called reconfigurable multiplicative noise (RMN). Tradeoffs of power usage, algorithm complexity, and training complexity are discussed. Also discussed are methods for choosing the element configurations to maximize secrecy rate and minimize transmit power.

Chapter 4 details the channel models that are used for performance simulations of the fixed and reconfigurable array algorithms. The statistical model used is a modified Saleh-Valenzuela channel [38]. In addition, ray tracing models from urban, indoor, and rural landscapes also are tested. Eavesdroppers are assumed spread throughout the volume in order to assess the likelihood of an eavesdropper decoding a secure message if it is mobile. Simulation results for the Saleh-Valenzuela and ray-tracing channels for fixed and reconfigurable array transmitters are given, and the tradeoffs of using isotropic versus directional transmit elements are assessed. Finally, the effect of imperfect channel estimation on secrecy is analyzed.

Chapter 5 presents a line-of-sight (LOS) experiment using a four-element array as either a reconfigurable or fixed array transmitter. QPSK modulation is transmitted and decoded by a single element receiver positioned at various angles from the transmitter to simulate either Bob at some desired transmit angle or Eve at all other angles. The results show the ability of Eve to decode the signal for various angles and methods of artificial noise generation.

Chapter 6 combines the two main physical encryption methods of AAN and RMN for the same transmitter. Simulation results over an urban channel model are presented. These show that combining AAN and RMN provides increased secrecy than either method alone, and is more power efficient.

Finally, Chapter 7 gives conclusions and ideas for future work.

1.4 Notation

For all mathematical expressions, a lower-case non-bolded variable (a) is a scalar, a lower-case bold variable ($\mathbf{a}$) is a vector, and an upper-case variable (A) is a matrix. The complex conjugates of a scalar a and vector $\mathbf{a}$ are a^* and $\mathbf{a}^*$, respectively. The operator $^\top$ denotes the vector or matrix transpose, and $\{\cdot\}^H$ is the Hermitian (conjugate transpose) operator. $||\mathbf{a}||$ is the vector norm of $\mathbf{a}$. $\Re(\cdot)$ and $\Im(\cdot)$ denote the real and imaginary parts of a complex number.

$\mathcal{CN}(\mu, \sigma^2)$ denotes a complex Gaussian random variable with zero mean real and imaginary parts that are independent Gaussian random variables each with variance $\sigma^2/2$ and with means of $\Re\{\mu\}$ and $\Im\{\mu\}$, respectively. $\log(\cdot)$ is the natural logarithm and $\log_2$ is the base 2 logarithm.

Probability density functions (PDFs) (which are continuous function) are written $f(\cdot)$ and discrete probability mass functions (PMFs) are written $p(\cdot)$. $I(X;Y)$ is the mutual information between X and Y.

CHAPTER 2

SECRECY WITH FIXED ARRAYS

Even though [6] found there was no rate at which secure communication was possible if Eve's channel were statistically better than Bob's channel, this does not mean there is nothing that could be done to give Bob's channel an artificial advantage. A method proposed in 2005 involves broadcasting additive artificial noise (AAN) in the nullspace of Bob's channel, degrading to various degrees all channels other than Bob's [20]. It is relatively easy to analyze this method of artificial noise because it is additive, and a secrecy capacity can be readily determined given a channel for Bob and Eve. The mathematical detail and secrecy capacity analysis of current AAN generation are given in Section 2.1. However, the current method suffers from the limitations of high computational overhead and lack of peak power control. Improvements on the artificial noise algorithm that resolve these issues are given in Section 2.2.

Another means of generating artificial noise has the effect of multiplying the desired signal by a random variable rather than adding a random variable to it. Hence, this is termed multiplicative artificial noise (MAN) generation. The salient points of MAN are that Bob receives an undisturbed signal in the same manner as with AAN due to channel inversion, and that it is simple to compute. However, adhering to a maximum transmit power limit is more complicated than with AAN. Also, there is no closed form expression for secrecy capacity. These issues are discussed in Section 2.3.

It will be shown in Section 2.3 that MAN has no closed form secrecy capacity, and in Chapter 3 the same problem will arise for signal distortion by reconfigurable arrays. Thus, a means of comparing these different methods of secrecy is desired. Section 2.4 discusses how mutual information (MI) is calculated and can give a secrecy rate (but not capacity) for any secrecy technique given channels for Bob and Eve. Finally, Section 2.5 compares the secrecy performance of AAN and MAN with respect to power allocation between the signal and artificial noise. In this section, only simulations using Rayleigh fading channels will be used, but more advanced channel models will be given in Chapter 4 and experimental data given in Chapter 5.

2.1 Additive Artificial Noise Generation (AAN)

2.1.1 Implementation

Negi and Goel [24] describe two methods for artificial noise placement: using multiple antennas and using multiple amplifying relays. This work is concerned with the former method. Let the signals received at time k by Bob and Eve be respectively given by

$$\begin{aligned} z_k &= \mathbf{h}^\top \mathbf{x}_k + n_k & (2.1) \\ y_k &= \mathbf{g}^\top \mathbf{x}_k + e_k & (2.2) \end{aligned}$$

This analysis is concerned only with single antenna receivers for Bob and Eve, so the received symbols for Bob and Eve, z_k and y_k, are scalar. The AWGN received at Bob and Eve respectively are given by n_k and e_k, with noise variances σ_n^2 and σ_k^2. The transmitted signal from Alice is $\mathbf{x}_k$ and $\mathbf{h}$ and $\mathbf{g}$ are the channels to Bob and Eve and are vectors because Alice might have multiple antennas. Assume $\mathbf{g}$ and $\mathbf{h}$ are slow fading, so we may treat them as constant in this analysis.

The transmitter computes $\mathbf{x}_k$ as the sum of a message signal $\mathbf{s}_k$ and an artificial noise signal $\mathbf{w}_k$:

$$\mathbf{x}_k = \mathbf{s}_k + \mathbf{w}_k \tag{2.3}$$

The message signal weights include transmit beamforming:

$$\mathbf{s}_k = \frac{\mathbf{h}^*}{||\mathbf{h}||} m_k \tag{2.4}$$

where m_k is the actual message symbol at time k that is beamformed using the channel conjugate $\mathbf{h}^*$. In this analysis, we assume Alice has an error-free estimate of the channel to Bob. The artificial noise $\mathbf{w}_k$ is chosen so it will be in the nullspace of Bob:

$$\mathbf{h}^\top \mathbf{w}_k = 0 \tag{2.5}$$

The artificial noise seen by Eve is given by $\mathbf{g}^\top \mathbf{w}_k$. This quantity is unknown to Alice because Eve's channel is assumed unknown to Alice and Bob. Alice then randomly changes $\mathbf{w}_k$ for each symbol k at the symbol rate so the artificial noise seen by Eve is not constant and thus Eve cannot simply filter it by subtracting a constant number from her received signal. It can be noted that Alice may change artificial noise at a rate less than the symbol rate. If the rate of change of noise symbols is zero, meaning constant artificial noise, transmitted constellations will be distorted in different directions but in the same way each time. This provides a modicum of secrecy and is the method known as directional modulation described in the Appendix. As the noise symbol rate of change is increased up to the symbol rate, secrecy increases.

Another way of interpreting AAN is that the message signal is sent on a fixed beam in the direction of Bob's channel, while another beam with a null in the direction of Bob is randomly varied, causing interference to all other receivers. This is illustrated in Figure 2.1 in which the solid beam conveys the message information from Alice to Bob while another beam shown in dashes is randomly varied at the symbol rate, and in this case two symbols are shown.

Generating $\mathbf{w}_k$ can be done in one of two ways. The first way is to compute a noise vector in Bob's nullspace each time. Let $\mathbf{v}_k$ be a vector of complex Gaussian random variables with zero mean and variance σ_v^2, which should be equal or near to Bob's channel power:

$$\sigma_v^2 = ||\mathbf{h}||^2 \tag{2.6}$$

Then let:

$$W_k = [\mathbf{v}_k, \mathbf{h}^*] \tag{2.7}$$

$$\boldsymbol{\omega}_k = W_k (W_k^H W_k)^{-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{2.8}$$

$$\mathbf{w}_k = \frac{\boldsymbol{\omega}_k}{||\boldsymbol{\omega}_k||} \tag{2.9}$$

Equation (2.8) ensures that the noise is orthogonal to Bob because it is a solution to:

$$W_k^H \boldsymbol{\omega}_k = \begin{bmatrix} \mathbf{v}_k^H \\ \mathbf{h}^\top \end{bmatrix} \boldsymbol{\omega}_k = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{2.10}$$

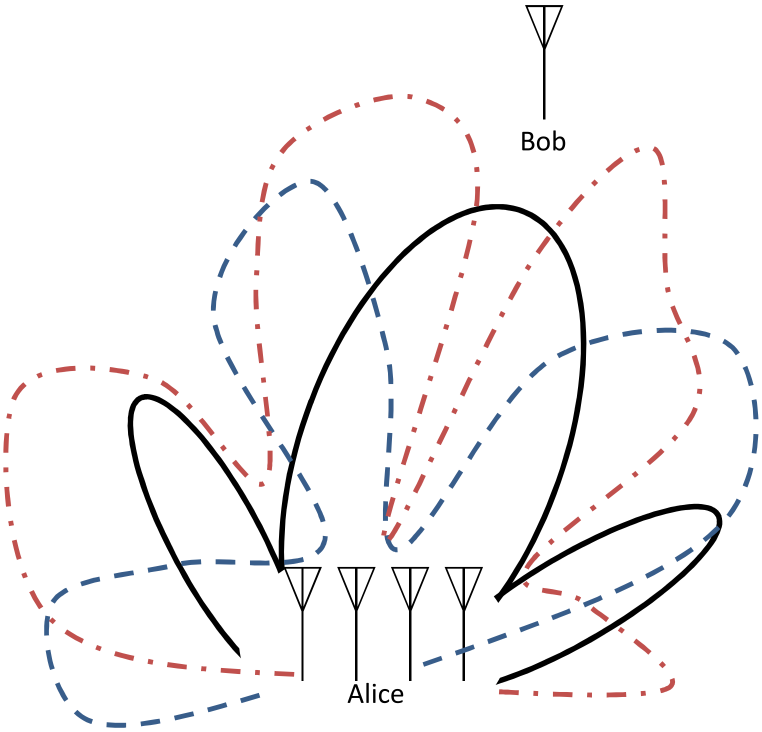


Figure 2.1: AAN example illustrating the signal beamforming (solid, black) and the patterns created by the random artificial noise weights (dashed, in color). The artificial noise patterns must have a null in the direction of Bob's channel.

This gives two equations:

$$\mathbf{v}_k^H \boldsymbol{\omega}_k = 1 \tag{2.11}$$

and

$$\mathbf{h}^\top \boldsymbol{\omega}_k = 0 \tag{2.12}$$

Equation (2.11) enforces that the norm of the noise weight vector $\boldsymbol{\omega}_k$ is one, and Equation (2.12) enforces no noise in the desired receiver's channel. Solving for $\boldsymbol{\omega}_k$ is straightforward from Equation (2.10):

$$W_k(W_k^H W_k)^{-1} W_k^H \boldsymbol{\omega}_k = W_k(W_k^H W_k)^{-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{2.13}$$

$$\boldsymbol{\omega}_k = W_k(W_k^H W_k)^{-1} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{2.14}$$

This method requires a matrix inversion from Equation (2.8) at the symbol rate. Even if the channel is constant over many symbols, the random interference $\mathbf{v}_k$ must be varied at the symbol rate, making the generation of artificial noise with this scheme computationally demanding.

The second method for generating $\mathbf{w}_k$ involves computing a singular value decomposition (SVD) to obtain an orthonormal basis for the nullspace of Bob's channel. The SVD of Bob's channel $\mathbf{h}$ is given by:

$$\mathbf{h} = U\Sigma V^H \tag{2.15}$$

Since $\mathbf{h}$ is an Nx1 vector for the N elements of Alice, V is a 1x1 matrix since it represents the eigenvectors of a single number ($\mathbf{h}^H\mathbf{h}$) and U is an NxN matrix whose columns are the eigenvectors of $\mathbf{h}\mathbf{h}^H$. The eigenvalues corresponding to the columns in U are contained in Σ, and therefore using linear combinations of the second through last columns of U yields solutions in the nullspace of $\mathbf{h}$. If B is the orthonormal basis of $\mathbf{h}$ that is composed of the second through last columns of U, then expressed mathematically, taking linear combinations of this orthonormal basis satisfies:

$$\mathbf{h}^\top B\mathbf{v}_k = 0 \tag{2.16}$$

Therefore, once an SVD is computed and assuming the channel does not change, all that need be done is to take linear combinations of the nullspace vectors, weighted by a randomly changing vector $\mathbf{v}_k$ in Equation (2.16).

Whether the artificial noise pattern is calculated through a matrix inversion or after an SVD, either method entails nontrivial computational complexity. For N transmit elements, the computational complexity for matrix inversion is $\mathcal{O}(N^3)$ while the complexity of an SVD of a vector is $\mathcal{O}(N^2)$. While the SVD has the advantage here for lower complexity and because it need only be performed at the channel fading rate instead of the symbol rate, both methods are nontrivial to implement in dedicated hardware. The desire for simpler algorithms for generating artificial noise is part of the motivation for the algorithms presented in Sections 2.2 and 2.3.

2.1.2 Secrecy Capacity Analysis

Because the total signal from Alice is a summation of the message signal and the artificial noise, the secrecy capacity analysis is straightforward. Assume the transmit power scaling is P_T. The transmit power is divided between the message signal power and the artificial noise power, and this will be denoted by the variable α taking a value between 0 and 1. Assume the message signal $\mathbf{x}_k$ is normalized to have unity average power, and Equation (2.9) already enforces the artificial noise weights to have unity power. The total signal transmitted by Alice with transmit power proportioned between signal and artificial noise is given by:

$$\sqrt{P_T}\mathbf{w}_{tot,k} = \sqrt{\alpha P_T}\mathbf{s}_k + \sqrt{(1-\alpha)P_T}\mathbf{w}_k \tag{2.17}$$

The average total transmit power is always P_T. This is proven by:

$$\begin{gathered} P_{total} = \left\| \sqrt{\alpha P_T}\mathbf{s} + \sqrt{(1-\alpha)P_T}\mathbf{w} \right\|^2 = \\ P_T \sum_{n=1}^{N} \left(\left(\sqrt{\alpha}\Re(s_n) + \sqrt{1-\alpha}\Re(w_n) \right)^2 + \left(\sqrt{\alpha}\Im(s_n) + \sqrt{1-\alpha}\Im(w_n) \right)^2 \right) \end{gathered} \tag{2.18}$$

The time subscripts k are omitted from $\mathbf{s}$ and $\mathbf{w}$.

$$\begin{gathered} P_{total} = P_T \sum_{n=1}^{N} \left(\alpha(\Re(s_n)^2 + \Im(s_n)^2) + (1-\alpha)(\Re(w_n)^2 + \Im(w_n)^2) \right) + \\ P_T \sum_{n=1}^{N} \left(2\sqrt{\alpha(1-\alpha)}(\Re(s_n)\Re(w_n) + \Im(s_n)\Im(w_n)) \right) \end{gathered} \tag{2.19}$$

$$\begin{gathered} P_{total} = P_T \left(\alpha \left\| \mathbf{s} \right\|^2 + (1-\alpha) \left\| \mathbf{w} \right\|^2 \right) + \\ P_T \left(2\sqrt{\alpha(1-\alpha)} \sum_{n=1}^{N} (\Re(s_n)\Re(w_n) + \Im(s_n)\Im(w_n)) \right) \end{gathered} \tag{2.20}$$

Since $\mathbf{s}$ and $\mathbf{w}$ are normalized so $\left\| \mathbf{s} \right\|^2 = 1$ and $\left\| \mathbf{w} \right\|^2 = 1$, P_{total} equals:

$$P_{total} = P_T \left(\alpha + (1-\alpha) + 2\sqrt{\alpha(1-\alpha)} \sum_{n=1}^{N} (\Re(s_n)\Re(w_n) + \Im(s_n)\Im(w_n)) \right) \tag{2.21}$$

$$P_{total} = P_T \left(1 + 2\sqrt{\alpha(1-\alpha)} \sum_{n=1}^{N} \left(\Re(s_n)\Re(w_n) + \Im(s_n)\Im(w_n)\right)\right) \tag{2.22}$$

Equations (2.4) and (2.5) imply that:

$$\mathbf{s}^H \mathbf{w} = 0 \tag{2.23}$$

Thus, the real part of Equation (2.23) is zero:

$$\sum_{n=1}^{N} \left((\Re(s_n) - j\Im(s_n))(\Re(w_n) + j\Im(w_n))\right) = 0 \tag{2.24}$$

where $j = \sqrt{-1}$.

$$\sum_{n=1}^{N} \left(\Re(s_n)\Re(w_n) + \Im(s_n)\Im(w_n)\right) = 0 \tag{2.25}$$

Equation (2.25) proves that the summation of Equation (2.22) is zero, and therefore $P_{total} = P_T$.

Substituting this transmitted signal in (2.17) into (2.1), the received signal at Bob is given by:

$$z_k = \sqrt{\alpha P_T}\mathbf{h}^\top \mathbf{s}_k + \sqrt{(1-\alpha)P_T}\mathbf{h}^\top \mathbf{w}_k + n_k \tag{2.26}$$

$$z_k = \sqrt{\alpha P_T}\mathbf{h}^\top \mathbf{s}_k + n_k \tag{2.27}$$

Eve receives the message signal but also artificial noise to some degree depending on her channel:

$$y_k = \sqrt{\alpha P_T}\mathbf{g}^\top \mathbf{s}_k + \sqrt{(1-\alpha)P_T}\mathbf{g}^\top \mathbf{w}_k + e_k \tag{2.28}$$

Since the artificial noise is independent of the message signal and the AWGN, simple expressions for the signal to interference plus noise ratio (SINR) for Bob and Eve can be created and used to calculate the secrecy capacity.

$$\mathrm{SINR}_{\mathrm{Bob}} = \frac{\alpha P_T \mathrm{E}[|\mathbf{h}^\top \mathbf{s}_k|^2]}{\sigma_n^2} \tag{2.29}$$

where $\mathrm{E}[\cdot]$ denotes the expectation. From Equation (2.4) and assuming the average symbol power is $\mathrm{E}[|m_k|^2]$, Bob's SINR can be written:

$$\mathrm{SINR}_{\mathrm{Bob}} = \frac{\alpha P_T ||\mathbf{h}||^2 \mathrm{E}[|m_k|^2]}{\sigma_n^2} \tag{2.30}$$

Eve's SINR given her channel $\mathbf{g}$ can be similarly computed from Equation (2.28):

$$\begin{aligned} \mathrm{SINR}_{\mathrm{Eve}} &= \frac{\alpha P_T \mathrm{E}[|\mathbf{g}^\top \mathbf{s}_k|^2]}{(1-\alpha)P_T \mathrm{E}[|\mathbf{g}^\top \mathbf{w}_k|^2] + \sigma_e^2} && (2.31) \\ \mathrm{SINR}_{\mathrm{Eve}} &= \frac{\alpha P_T \left|\mathbf{g}^\top \frac{\mathbf{h}^*}{||\mathbf{h}||}\right|^2 \mathrm{E}[|m_k|^2]}{(1-\alpha)P_T \mathrm{E}[|\mathbf{g}^\top \mathbf{w}_k|^2] + \sigma_e^2} && (2.32) \end{aligned}$$

The secrecy rate, given Bob's and Eve's channels $\mathbf{h}$ and $\mathbf{g}$, is a function of α and is given by [22]

$$R_{\mathrm{sec}}(\alpha) = \log_2(1 + \mathrm{SINR}_{\mathrm{Bob}}) - \log_2(1 + \mathrm{SINR}_{\mathrm{Eve}}) \tag{2.33}$$

The secrecy capacity is the best rate over all possible power allocations:

$$C_{\mathrm{sec}} = \arg\max_{\alpha} \left(R_{\mathrm{sec}}(\alpha)\right) \tag{2.34}$$

From comparing Equations (2.30) and (2.32), Bob is likely to have a higher SINR than Eve even if Eve has a stronger channel. First, transmit beamforming will maximize the signal power through Bob's channel for a given amount of power allocated to transmitting the signal, while Eve's signal power will be scaled by $\mathbf{g}^\top \frac{\mathbf{h}^*}{|\mathbf{h}|}$, which may or may not be large depending on how similar Eve's channel is to Bob's and the path loss of Eve's channel. Second, Bob's SINR is not impacted by the artificial noise because it is orthogonal to Bob's channel. The artificial noise term in Eve's SINR is $\mathrm{E}[|\mathbf{g}^\top \mathbf{w}_k|^2]$, which is an expectation because the noise is random. The received artificial noise will increase if Eve's channel is strong because $\mathbf{g}$ will be larger, which increases both the signal and artificial noise terms. This limits an increase in Eve's SINR. Simulations later in this chapter will show how the power allocation between signal and artificial noise impacts secrecy rates.

2.1.3 Line-of-sight Performance of AAN

A simple method of assessing the secrecy of AAN is in the line-of-sight (LOS) channel between the transmit array and a desired receiver or eavesdropper. The transmit array is assumed to be four isotropic elements that are spaced half a wavelength apart. The desired receiver is at broadside, while eavesdroppers are assumed at other azimuthal angles around broadside. The transmit power is set so that the SNR at the desired receiver is 30 dB, meaning that the noise received by eavesdroppers will be dominated by the artificial noise of the transmitter. If the eavesdroppers and desired receiver all have the same channel strength, and the only difference in channels comes from the phases between the transmit elements and the receivers, then the SINR at all eavesdroppers and the desired receiver is shown in Figure 2.2.

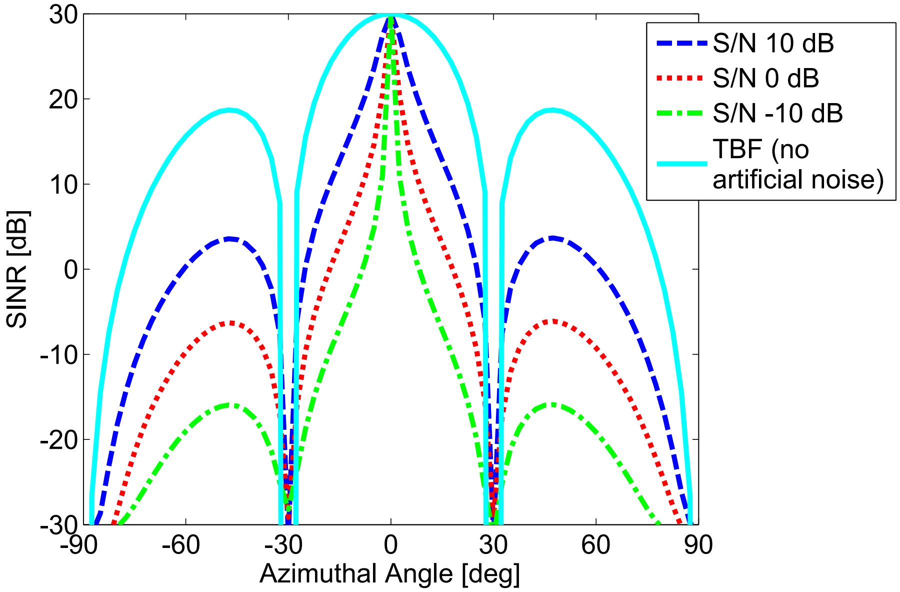


Figure 2.2: The effective SINR to an eavesdropper with a LOS channel (no reflections) to the desired receiver when the four-element transmit array is communicating to broadside. The transmitter power is set so the SNR at the desired receiver is 30 dB and artificial noise power varies from -10 dB to 10 dB relative to the signal power, or no artificial noise at all in the case of transmit beamforming.

The transmitter may send no artificial noise, which is the transmit beamforming case also shown in Figure 2.2. In this case, the receive SINR at the eavesdroppers is governed by the array factor. When more transmit power is added to create artificial noise, all directions around broadside suffer SINR degradation, even within the main lobe. This narrow region of high SINR around the desired receiver suggests that generating artificial noise also will degrade the SINR of eavesdroppers in scattering channels. This will be shown to be the case in Chapter 4.

2.2 Peak-power Limited AAN

The artificial noise method in Section 2.1 suffers from complexity issues in generating noise in the nullspace of the desired receiver. Furthermore, because the artificial noise is random, there are instances in which one of the transmitter weights is very large. The total power used is constant at each symbol due to the scaling in Equations (2.4) and (2.9), but there is nothing limiting individual element power. A high peak to average power ratio can be inefficient and demands a high dynamic range on power amplifiers. One solution to limit the peak element power is to simply reject randomly generated solutions that have one or more elements above the limit. This requires recalculating weights which must be done at the symbol rate, and may prove computationally costly if matrix inversions also are executed at the symbol rate. Another method of AAN element generation described in this section allows for peak but not average power constraints, and generates weights with linear complexity.

Let $w_{k,n}$ be the artificial noise weight at time k for element n of Alice. The total transmitted signal at time k and element n of Alice is $x_{k,n} = s_{k,n} + w_{k,n}$. Again assuming the transmitter Alice has N elements, the constraints to satisfy are:

1. $|\sqrt{\alpha} s_{k,n} + \sqrt{(1-\alpha)} w_{k,n}|^2 < P_{max}$ for all n from 1 to N (element maximum power constraint) .

2. $\mathbf{h}^\top \mathbf{w}_k = 0$ (artificial noise in nullspace of Bob).

The algorithm for generating artificial noise weights $w_{k,n}$ goes as follows:

1. $w_{k,1} \sim \mathcal{CN}(0, \sigma_1^2)$.

2. $w_{k,n} \sim \mathcal{CN}\left(-\frac{1}{h_n} \sum_{m=1}^{n-1} (h_m w_{k,m}), \sigma_n^2\right)$ for $n = 2$ to $n = N - 1$.

3. $w_{k,N} = -\frac{1}{h_N}\sum_{m=1}^{N-1}(h_m w_{k,m})$.

This algorithm generates a random weight drawn from a zero mean complex Gaussian distribution for one of the elements of Alice. Then all of the other random weights except one are generated in some order drawn from complex Gaussian distributions, except that the mean of the distribution is continually adjusted to keep the sum of the product of weights and Bob's channel close to zero, which is Constraint 2. Last, Constraint 2 is satisfied by the choice of the final weight in Step 3. The elements can be chosen in any order, but it seems most logical to choose them from lowest to highest $|h_n|$ so the last element is scaled down the most by the $\frac{1}{h_N}$ term, avoiding a high individual element power that might violate the first constraint.

The algorithm will not satisfy Constraint 1 if any sum of element beamforming and random weights exceeds the element maximum power constraint. This will happen with some probability that can be controlled based on the choice of σ_n^2. This variance will change as the weights are generated according to the following formula:

$$\sigma_n^2 = \frac{\frac{P_{max}}{3(1-\alpha)} - \frac{\alpha|h_n^2|}{(1-\alpha)||\mathbf{h}||^2} - \left|\frac{1}{h_n}\sum_{m=1}^{n-1}(h_m w_{k,m})\right|^2}{-\log(1-P_{success})} \tag{2.35}$$

where $P_{success}$ is a lower bound on the probability that all of the weights will be within the element maximum power constraint. This bound is set by the transmitter before transmission and is a tradeoff between how often a failure (and repeat of the algorithm for one symbol time) is tolerated and how many different values the artificial noise may take.

The variance in Equation (2.35) will be large when $P_{success}$ approaches zero, due to the denominator approaching zero. When $P_{success}$ approaches one, the denominator approaches $+\infty$ so the variance decreases toward zero. This makes sense because if the randomly generated zero mean noise never should surpass the element power constraints, it should be made very small.

The numerator in Equation (2.35) must be positive or else the variance will be negative. The first term of the numerator always will be positive while the second and third always will be negative. If the variance is calculated as negative in the algorithm, it is simply set to zero, resulting in the interference weight $w_{k,n}$ set to zero if it is for the first element or set to the average of the complex Gaussian in Step 2 of the algorithm for elements 2 to $N-1$.

The proof that (2.35) limits the probability of error is as follows. Let:

$$P_{success} = P\left(\left|\sqrt{\alpha}s_{k,n} + \sqrt{1-\alpha}w_{k,n}\right|^2 < P_{max}\right) \tag{2.36}$$

$$P_{success} = P\left(\left|\sqrt{\alpha}s_{k,n} + \sqrt{1-\alpha}\left(\mathcal{CN}\left(-\frac{1}{h_n}\sum_{m=1}^{n-1}(h_m w_{k,m}), \sigma_n^2\right)\right)\right|^2 < P_{max}\right) \tag{2.37}$$

$$P_{success} = P\left(\left|\sqrt{\alpha}s_{k,n} + \sqrt{1-\alpha}\left(-\frac{1}{h_n}\sum_{m=1}^{n-1}(h_m w_{k,m}) + \mathcal{CN}\left(0, \sigma_n^2\right)\right)\right|^2 < P_{max}\right) \tag{2.38}$$

Applying the Cauchy-Schwarz inequality,

$$\begin{gathered}\left|\sqrt{\alpha}s_{k,n} + \sqrt{1-\alpha}\left(-\frac{1}{h_n}\sum_{m=1}^{n-1}(h_m w_{k,m}) + \mathcal{CN}\left(0, \sigma_n^2\right)\right)\right|^2 \leq \\ 3\left(\left|\sqrt{\alpha}s_{k,n}\right|^2 + \left|\sqrt{1-\alpha}\left(-\frac{1}{h_n}\sum_{m=1}^{n-1}(h_m w_{k,m})\right)\right|^2 + \left|\sqrt{1-\alpha}\mathcal{CN}\left(0, \sigma_n^2\right)\right|^2\right)\end{gathered} \tag{2.39}$$

Thus,

$$\begin{gathered}P\left(\left|\sqrt{\alpha}s_{k,n} + \sqrt{1-\alpha}\left(-\frac{1}{h_n}\sum_{m=1}^{n-1}(h_m w_{k,m}) + \mathcal{CN}\left(0, \sigma_n^2\right)\right)\right|^2 < P_{max}\right) \geq \\ P\left(3\left(\left|\sqrt{\alpha}s_{k,n}\right|^2 + \left|\sqrt{1-\alpha}\left(-\frac{1}{h_n}\sum_{m=1}^{n-1}(h_m w_{k,m})\right)\right|^2 + \left|\sqrt{1-\alpha}\mathcal{CN}\left(0, \sigma_n^2\right)\right|^2\right) < P_{max}\right)\end{gathered} \tag{2.40}$$

Substituting Equation (2.40) into Equation (2.38):

$$P_{success} \geq P\left(3\left(\left|\sqrt{\alpha}s_{k,n}\right|^2 + \left|\sqrt{1-\alpha}\left(-\frac{1}{h_n}\sum_{m=1}^{n-1}(h_m w_{k,m})\right)\right|^2 + \left|\sqrt{1-\alpha}\mathcal{CN}\left(0, \sigma_n^2\right)\right|^2\right) < P_{max}\right) \tag{2.41}$$

$$P_{success} \geq P\left(\left|\sqrt{1-\alpha}\mathcal{CN}\left(0,\sigma_n^2\right)\right|^2 < \frac{P_{max}}{3} - \left|\sqrt{\alpha}s_{k,n}\right|^2 - \left|\sqrt{1-\alpha}\left(-\frac{1}{h_n}\sum_{m=1}^{n-1}(h_m w_{k,m})\right)\right|^2\right) \tag{2.42}$$

$$P_{success} \geq P\left(\left|\mathcal{CN}\left(0,\sigma_n^2\right)\right|^2 < \frac{P_{max}}{3(1-\alpha)} - \frac{\alpha}{1-\alpha}\frac{|h_n|^2}{||\mathbf{h}||^2} - \left|-\frac{1}{h_n}\sum_{m=1}^{n-1}(h_m w_{k,m})\right|^2\right) \tag{2.43}$$

Since $\left|\mathcal{CN}\left(0,\sigma_n^2\right)\right|^2$ is an exponential random variable with mean σ_n^2, the expression to the right of the $\geq$ in Equation (2.43) can be written as the cumulative distribution function (CDF) of an exponential random variable:

$$P_{success} \geq 1 - \exp\left(-\frac{\frac{P_{max}}{3(1-\alpha)} - \frac{\alpha}{1-\alpha}\frac{|h_n|^2}{||\mathbf{h}||^2} - \left|-\frac{1}{h_n}\sum_{m=1}^{n-1}(h_m w_{k,m})\right|^2}{\sigma_n^2}\right) \tag{2.44}$$

Setting σ_n^2 to the expression in (2.35) makes both sides of Equation (2.44) equal, meaning that using this variance in the algorithm will have a success rate greater than or equal to $P_{success}$. For example, if the desired success probability is Q, then substitution into Equation (2.44) yields:

$$P_{success} \geq 1 - \exp\left(-\frac{\frac{P_{max}}{3(1-\alpha)} - \frac{\alpha}{1-\alpha}\frac{|h_n|^2}{||\mathbf{h}||^2} - \left|-\frac{1}{h_n}\sum_{m=1}^{n-1}(h_m w_{k,m})\right|^2}{\frac{\frac{P_{max}}{3(1-\alpha)} - \frac{\alpha|h_n^2|}{(1-\alpha)||\mathbf{h}||^2} - \left|\frac{1}{h_n}\sum_{m=1}^{n-1}(h_m w_{k,m})\right|^2}{-\log(1-Q)}}\right) \tag{2.45}$$

$$\begin{aligned} P_{success} &\geq 1 - \exp\left(\log(1-Q)\right) && (2.46)\\ P_{success} &\geq 1-(1-Q) && (2.47)\\ P_{success} &\geq Q && (2.48) \end{aligned}$$

The fraction of times an element exceeded the element power constraint as a function of the user-specified probability of failure $(1 - P_{success})$ is shown in Figure 2.3. Four million trials were run on different Rayleigh fading channels for each probability of failure. A four-element array was simulated with maximum element power limit set to one and the beamforming weights were normalized to have unit power. The fraction of power allocated to artificial noise (α) was set anywhere from 1% to 99%. The user-specified bound on the failure rate proves to be a loose upper bound since the actual failure rate is an order of magnitude lower.

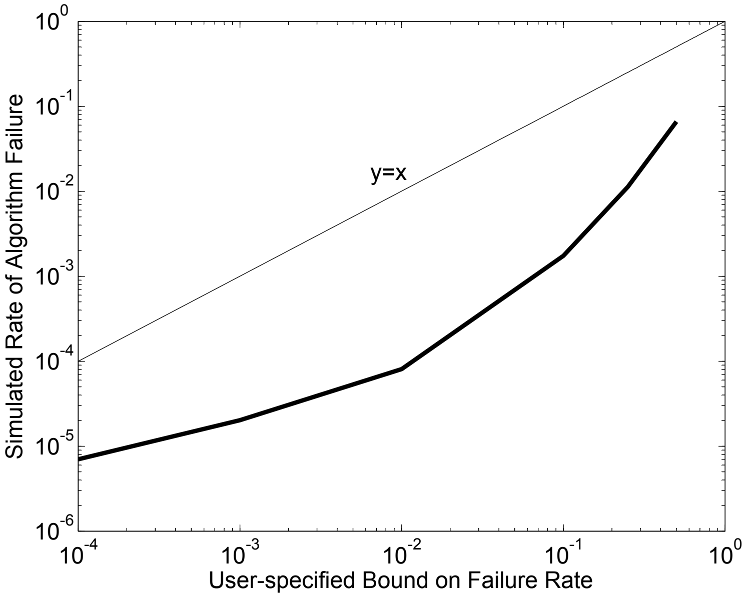


Figure 2.3: Fraction of time the peak power-limited AAN algorithm failed in simulation as a function of the user-specified bound on probability of failure. Weight generation failed at a rate less than the user-specified maximum failure rate.

One important note about the peak power-limited AAN algorithm is that the noise weights are no longer independent complex Gaussian random variables since the means and variances of the subsequent noise weights depend on the previous ones. The weights are still initially generated from an initial random Gaussian and are independent across time. Since the received artificial noise at an eavesdropper cannot be assumed to be white Gaussian noise, the mutual information (MI) between the transmitter and the eavesdropper is calculated by generating a large number of constellation points and calculating the mutual information using that constellation and the method explained in Section 2.4.2. This calculation assumes the number of possible constellation points at the eavesdropper is finite, but because there are still infinite ways the interference can add up and thus infinite constellation points, this calculation is an upper bound of the actual MI between the transmitter and eavesdropper.

2.3 Multiplicative Artificial Noise Generation (MAN)

Section 2.2 presented a method of generating AAN with the number of steps equal to the number of transmitting elements. This was intended to simplify the computational burden that came from projecting artificial noise onto the nullspace of the desired channel. This section describes another method to generate artificial noise that falls into the desired receiver's nullspace, called multiplicative artificial noise (MAN). Like the algorithm in Section 2.2, it is easy to compute; however, it differs mathematically from AAN in that the signal and artificial noise terms are not a summation but rather a product. This complicates secrecy capacity analysis and necessitates the alternative secrecy analysis in Section 2.4. Secrecy performance compared to AAN will be given in Section 2.5.

Given Alice's channel to Bob $\mathbf{h}$, Alice computes the weights for MAN as follows:

$$\mathbf{x}_k = \frac{\alpha\mathbf{h}^* + \alpha(1-\alpha)\mathbf{w}_k}{\alpha\left\|\mathbf{h}\right\|^2 + (1-\alpha)\mathbf{h}^\top\mathbf{w}_k} m_k \tag{2.49}$$

where m_k is the message symbol. Each $w_{k,n}$ in the vector $\mathbf{w_k}$ is a complex Gaussian random variable with zero mean and a variance that gives the random vectors about the same power as the beamforming part of (2.49). The method used here is to set $w_{k,n} \sim \mathcal{CN}\,(0, ||\mathbf{h}||^2/N)$.

The weights accomplish channel inversion so when sent through Bob's channel, the result is an undistorted message signal:

$$\mathbf{h}^\top\mathbf{x}_k + n_k = m_k + n_k \tag{2.50}$$

The variable α takes on a value from zero to one depending on the power dedicated to artificial noise. This is similar to the power distribution in AAN but not exactly the same. For example, when $\alpha = 1$, the weights reduce to:

$$\mathbf{x}_k = \frac{\mathbf{h}^*}{\left\|\mathbf{h}\right\|^2} m_k \tag{2.51}$$

which is simply transmit beamforming. But as α approaches zero, all weights approach zero rather than increasing the artificial noise part. This is due to the $\alpha(1-\alpha)$ term in front of the artificial noise part. Because of this, Equation (2.49) is the formulation for power-limited MAN.

If the weights were formulated as

$$\mathbf{x}_k = \frac{\alpha \mathbf{h}^* + (1-\alpha)\mathbf{w}_k}{\alpha \left\|\mathbf{h}\right\|^2 + (1-\alpha)\mathbf{h}^\top \mathbf{w}_k} m_k \tag{2.52}$$

then for α close to zero, the transmitted signal becomes a random number multiplied by the message signal. Take the extreme case of $\alpha = 0$ for the weights in (2.52). The weights now are:

$$\mathbf{x}_k = \frac{\mathbf{w}_k}{\mathbf{h}^\top \mathbf{w}_k} m_k \tag{2.53}$$

Bob still receives $\mathbf{h}^\top \mathbf{x}_k + n_k = m_k + n_k$. An eavesdropper with a channel $\mathbf{g}_k$ receives:

$$\mathbf{g}^\top \mathbf{x}_k + e_k = \frac{\mathbf{g}^\top \mathbf{w}_k}{\mathbf{h}^\top \mathbf{w}_k} m_k + e_k \tag{2.54}$$

The complex scaling of m_k in Equation (2.54) randomly varies from symbol to symbol causing multiplicative random noise. Section 2.5 shows that generating weights from the expression in (2.52) increases the secrecy at a high transmit power cost. Thus, Equation (2.52) is the formulation for power-unlimited MAN.

Because MAN transmits a message m_k multiplied by a random complex number instead of a message signal added to an interference signal, a closed form expression for SINR and thus a simple secrecy rate formula is not possible. In fact, this situation is analogous to a wireless fading channel in which a signal is multiplied by a time-varying random variable. In the case of a signal that is sent from Alice to Eve in which neither may know the CSI, determining an expression for channel capacity remains an open problem for most cases [39]. Instead of comparing rates using a closed form expression, the signal constellations seen by Bob and Eve can be used, with a few assumptions, to compute the mutual information (MI) between Alice and Bob, and Alice and Eve. This method for computing the MI is the same as the method described in Section 2.2 for peak power-limited AAN. Section 2.4 explains how MI is calculated from received constellations and how it will serve as a metric for the remaining simulations and experimental data.

2.4 Mutual Information Analysis of Signals

2.4.1 Mutual Information Definitions

The mutual information (MI) between X and Y is the reduction of uncertainty of X given the knowledge of Y [40]. We can designate Y as the received signal and X as the message transmitted. Given perfect reception of Y, the MI is equal to the number of bits in X because there is no uncertainty at the receiver about X when Y is received. More commonly, MI is given as bits per unit time, and the discrete time MI in bits per channel use will be used here.

MI is equivalent to the rate of communication because, for a given communication scheme, it equals the rate at which information bits are sent from Alice to Bob. All channels presented here are assumed to be discrete memoryless channels, meaning outputs only depend on the inputs at the current time. The information capacity, C, of a discrete memoryless channel is related to MI by [40]:

$$C = \max_{p(X)} I(X;Y) \tag{2.55}$$

where $p(X)$ is the probability distribution of the input, and the capacity is taken from the maximum MI taken over all possible input distributions.

For the scenarios considered in this work, the input distribution X will be discrete, such as QPSK or 16 QAM. The output distribution Y will be continuous due to the effects of AWGN and artificial noise. If we assume the transmitter maps an input x_k to a received signal $g(x_k)$ that includes the effect of the channel, and AWGN is represented in discrete time by n_k, then let $y_k = g(x_k) + n_k$ be the received signal. This assumes a constant channel over time and that the transmitter maps the inputs in the same way each time. This is not the case when the transmitter is implementing artificial noise or changing antenna configurations as is done in Chapter 3, but is true for transmit beamforming. Calculating MI for artificial noise or reconfigurable antenna secrecy will be addressed later. We will omit the time dependence, so $y = g(x) + n$. Let the AWGN be zero mean with variance N_0 and let the PMF of the input be $p(x)$, the output PDF be $f(y)$, and the joint PDF be denoted by $f(x, y)$. The MI between X and Y is given by:

$$I(X;Y) = \sum_x \int_y f(x, y) \log_2 \frac{f(x, y)}{p(x)f(y)} dy. \tag{2.56}$$

We assume each symbol has an equal probability of being chosen to be transmitted, $p(x) = \frac{1}{M}$ for an M-sized alphabet. From the law of total probability:

$$f(y) = \sum_{i=1}^{M} p(x_i) f(y|x_i). \tag{2.57}$$

Since $y = g(x) + n$, $y|x$ is a complex Gaussian random variable with mean equal to $g(x)$ and variance equal to the noise variance N_0,

$$f(y|x) = \frac{1}{\pi N_0} e^{-\frac{|y-g(x)|^2}{N_0}}. \tag{2.58}$$

Finally, by the definition of conditional probability,

$$f(x, y) = p(x) f(y|x). \tag{2.59}$$

Combining these results and given an M-ary modulation and fixed transmit array, the MI between the transmitted and received messages is given by:

$$I(X;Y) = \sum_{i=1}^{M} \left[\int_{\mathbb{C}} \frac{1}{M\pi N_0} e^{-\frac{|y-g(x_i)|^2}{N_0}} \log_2 \left(\frac{M e^{-\frac{|y-g(x_i)|^2}{N_0}}}{\sum_{l=1}^{M} e^{-\frac{|y-g(x_l)|^2}{N_0}}} \right) dy \right] \tag{2.60}$$

where the integral of y occurs over the complex plane.

2.4.2 Methods of Calculating Mutual Information

Given a discrete input distribution and a constellation mapping $g(x)$ at the receiver in the presence of AWGN, Equation (2.60) is one method of calculating the MI between the transmitter and receiver, and thus the rate at which error-free communication is possible. The integrand of (2.60) will have peaks at the locations of the noiseless received constellation points in the complex plane. This makes numerical integration of (2.60) difficult because the integrand has a high dynamic range of values over which to integrate.

Another method discussed in [41] involves computing the MI of the input and output *bits* rather than symbols. This has two advantages. First, it is numerically simpler because it involves a one-dimensional integral of a real-valued function rather than an integral over the complex plane. Second, it takes into account the bit mapping to symbols, while the symbolic MI assumes an optimal mapping. It will be shown that for some constellations, even a Gray coding mapping (in which adjacent symbols differ by only one bit [39]) yields a lower MI when calculated bit-wise relative to symbol-wise MI. Gray coding is not optimal because the probability of bit errors is not equal for each bit of the symbol.

Assuming all message bits are equally likely to be one or zero, the MI is calculated by:

$$I(A;B) = \frac{1}{2} \sum_{B \in \{0,1\}} \int_{-\infty}^{\infty} p(a|b) \log_2 \left(\frac{2p(a|b)}{p(a|b=0) + p(a|b=1)} \right) da \qquad (2.61)$$

where B are the transmitted bits (zero and one), A are the log-likelihood ratios of the received bits after symbol decoding, and $p(a|b)$ is the PDF of the log-likelihood ratio of a received bit given b was sent. The log-likelihood ratio of a received bit is given by:

$$L(\hat{b}) = \ln \left(\frac{p(\hat{b}=1|\mathbf{y})}{p(\hat{b}=0|\mathbf{y})} \right) \qquad (2.62)$$

where ln is the natural logarithm, $\mathbf{y}$ is a vector of received symbols, and $\hat{b}$ is the estimate of the current bit. Since we are not assuming coded symbols, the current bit only depends on the current received symbol y, so we can write:

$$L(\hat{b}) = \frac{p(\hat{b}=1|y)}{p(\hat{b}=0|y)} \qquad (2.63)$$

The probability that $\hat{b}$ is a one or zero based on the received symbol y is given by [42]:

$$p(\hat{b}|y) = \sum_{x \in \tilde{B}} \frac{1}{\pi N_0} e^{-\frac{|y-g(x)|^2}{N_0}} \qquad (2.64)$$

where $\tilde{B}$ is the set of transmit symbols that have $\hat{b}$. For example, if $\hat{b} = 0$ and 16 QAM were used and the first bit of the symbol were in question, then

$\tilde{B}$ might equal $\{1+0j, 0-1j, \ldots, -1+2j\}$ if those symbols correspond to the bits $\{0000, 0001, \ldots, 0111\}$ since 16 QAM has four bits per symbol.

Additionally, the received symbol y is a random variable that is composed of an AWGN variable $w \sim \mathcal{CN}(0, N_0)$ added to the transmitted symbol. This transmitted symbol s comes from the set of all possible symbols (denoted S) with equal probability, so $y = s + w$, $s \in S$. But if s is conditioned on bit b sent, then $s \in \tilde{S}$, where $\tilde{S}$ is the half of the total symbols that have the corresponding bit equal to b.

$L(\hat{b}|b)$ is computed from the received symbols y in the presence of noise using (2.63) and (2.64). A Monte Carlo simulation generates many bits from which log-likelihood ratios are computed and compiled into a PDF by taking a histogram, which is then used in (2.61) to find the MI.

The final step that relates the bit MI in (2.61) to the symbol MI in (2.56) is to scale the bit MI by the bits per symbol in an M-ary modulation:

$$I(X;Y) = \log_2(M) I(A;B) \tag{2.65}$$

If the input distribution is independent of time and uniformly distributed, the resulting MI as a function of SNR is shown in Figure 2.4 for various standard modulations. These MIs were calculated using both Equation (2.56) that uses the received symbols and Equation (2.61) that uses the received bits. The symbol results agree with the independent and uniformly distributed capacities found in [43].

Generally, the bit-wise MI is very close to the symbol-wise MI. A major exception is 32 QAM, which has noticeably lower MI when calculated from the received bit log-likelihoods. This is because there is no method of Gray coding a 32 QAM constellation. Other higher order modulations such as 64 QAM also suffer lower MI from the bit calculation even though that constellation is Gray coded. This is because even though adjacent constellation symbols map to bits that differ by only one bit, the probability that each of the four bits will be in error is not uniform over all symbols. Because of this non-uniformity, even a Gray code mapping is slightly suboptimal, given a 64 QAM modulation is used. But for practical performance considerations, it is better to use the bit-wise calculation of MI since it gives a tighter upper bound on achievable communicate rates when transmitting a Gray coded constellation.

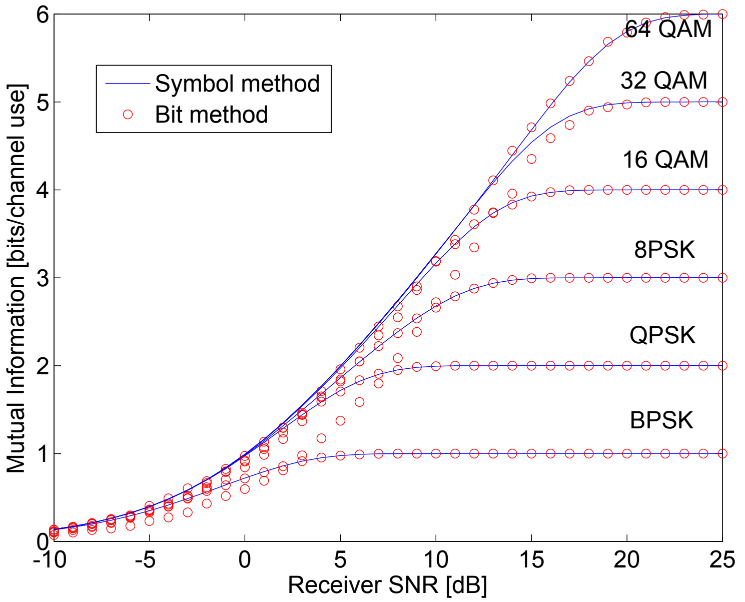


Figure 2.4: MI of various modulation schemes calculated from received symbols and from received Gray coded bits (all Gray coded except 32 QAM).

2.4.3 Relationship between Secrecy Rate and Practical Security

Before analyzing various physical layer encryption schemes from the standpoint of MI, this section explains how the difference in MI between Bob and Eve contributes to security. Even if there is a positive secrecy capacity, meaning the difference between Bob and Eve's MI is greater than zero, it is not clear how to best exploit secrecy capacity. The design of codes for secrecy is still in its infancy [44]. Instead of using a special code, one practical method is to transmit using a code rate that is greater than the MI of Eve's channel while less than that of Bob's channel. The rate is defined as the number of message bits per channel use. For example, if the transmitted modulation scheme is 16 QAM, which has 16 symbols and thus four bits per symbol, and the rate of the code used is 0.9, then $4 \times 0.9 = 3.6$ message bits are sent per each symbol transmitted.

Thus, if Bob has an MI greater than 3.6 bits and Eve has an MI less than 3.6 bits due to a worse channel or the addition of artificial noise, then practical coding schemes will be able to be demodulated by Bob, while Eve will have a very low probability of decoding any packets. An example simulation illustrating this result for a code in use today is shown in Figure 2.5. This figure shows the MI of many different receivers and their corresponding BER when demodulating a 16 QAM modulation with a rate 0.9 code. The code used is an LDPC inner code and a BCH outer code (to avoid error floors), following the framework used by the digital video broadcasting satellite (DVB-S2) system [45]. Because the code is nearly capacity-achieving, the receivers that had MIs as low as about 3.6 bits were able to demodulate all of the simulated packets with zero bit errors in the presence of AWGN. However, as soon as the MI drops below 3.6 bits, the BER grows very quickly to 0.5 or blind guessing.

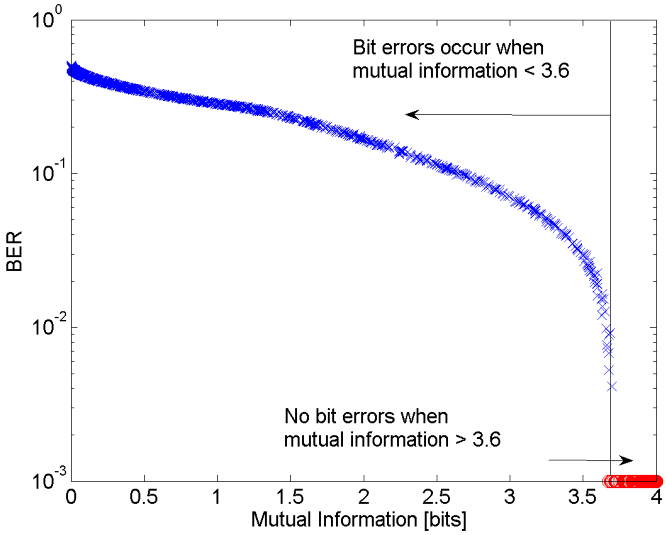


Figure 2.5: The relationship of MI between a transmitter sending 16 QAM and various receivers, and the actual BER of those receivers when using a rate 0.9 code (implying 3.6 information bits per channel use).

In practice, there are usually fixed coding rates to choose from rather than a variable rate, so transmitting at the highest rate possible for Bob to reliably receive the message will ensure that the highest number of eavesdroppers will be thwarted by physical layer encryption alone.

2.5 Fixed Array Secrecy Comparison

The secrecy rates and transmit power usage of AAN from Section 2.1, peak power-limited AAN from Section 2.2, power-limited MAN from Section 2.3, and power-unlimited MAN from Equation (2.52) are compared in this section. Alice is a four-element transmitter and Bob and Eve are single-element receivers. Weights for various power allocations from all power in transmit beamforming ($\alpha = 0.9$) to almost all power in the artificial noise component ($\alpha = 0.1$) were calculated, and simulations were carried out on 100 Rayleigh fading channel realizations for Bob and Eve. It is assumed that the channel is constant over the time period analyzed. The secrecy rate was calculated from the difference in MI. The MI was calculated from the received constellation noise variance method described in the previous section.

Figure 2.6 shows the average secrecy rate of each encryption method as a function of signal and noise power allocation. All four methods have the same secrecy rate when $\alpha = 1$ because all converge to transmit beamforming. In general in these Rayleigh fading channels in which Bob and Eve have about equal SNRs, a power allocation that devotes about the same power to artificial noise as to the signal performs best in terms of secrecy rate for all four methods.

Much of the difference in secrecy rates among the four methods can be explained by the average transmit power used by each method, which is shown in Figure 2.7. The power used was allowed to vary between methods while the only criterion was that the same-strength signal must be transmitted to Bob. Because each method produces artificial noise in a slightly different way, the total transmit power varied. The peak transmit powers are shown in Figure 2.8. A high transmit power occurs when a random set of artificial noise weights is large in magnitude.

As mentioned in Section 2.3, the power-unlimited MAN weights tend to have large peak powers when α is small in Equation (2.52) and most of the power is devoted to artificial noise. This method can generate weights especially high in amplitude because the denominator in (2.52) can become very small when α is small and $\mathbf{h}^\top \mathbf{w}$ also is small, but the numerator may not be small. This differs from the power-limited MAN formula for weights in (2.49) in which it is very likely that the numerator also will be small when the denominator is small.

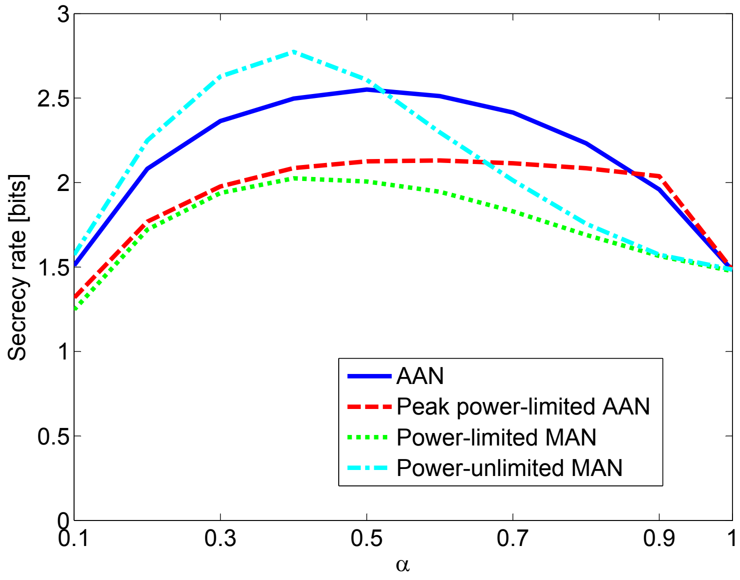


Figure 2.6: Secrecy rates for the four fixed array encryption algorithms averaged over 100 channel realizations and for various allocations of power between pure beamforming ($\alpha = 1$) and almost entirely artificial noise ($\alpha = 0.1$).

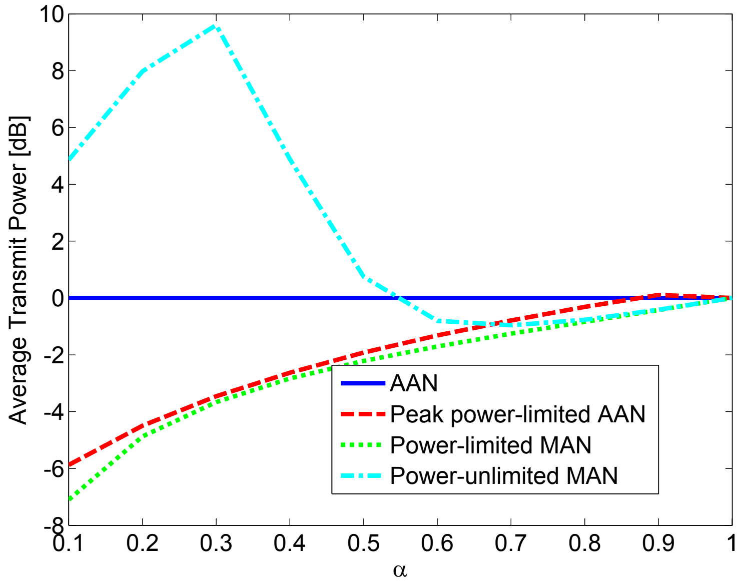


Figure 2.7: Average transmit power of the four fixed array encryption algorithms for 100 channel realizations, relative to AAN average transmit power.

Figures 2.6, 2.7, and 2.8 show there is a tradeoff between secrecy rate and peak and average transmit power among these four methods. Where the

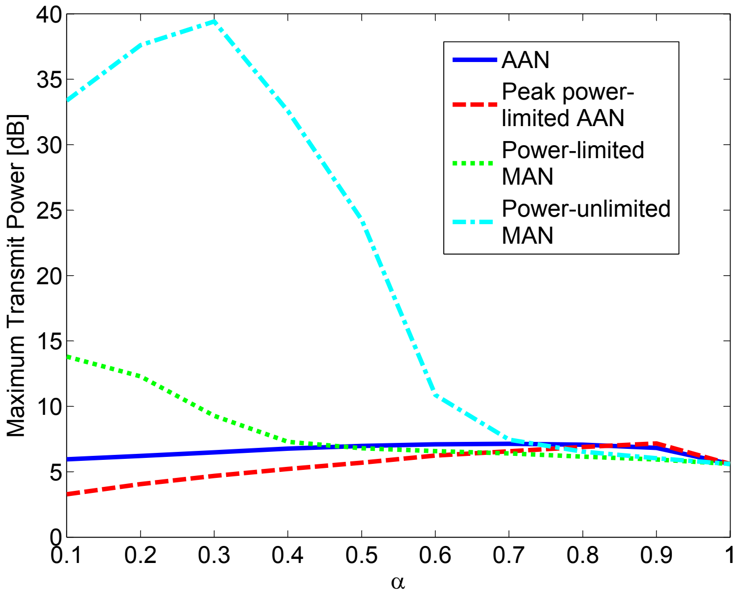


Figure 2.8: Maximum transmit power of each of the four fixed array encryption algorithms versus beamforming and artificial noise power allocation.

power-limited MAN transmit power becomes lower than the AAN transmit power, its secrecy rate also becomes lower than AAN. Peak power-limited AAN and power-limited MAN methods had lower secrecy rates and transmit powers in general. Another simulation was carried out to test the performance when all methods had the same average transmit power. Again, the condition of the identical transmitted signal to Bob was enforced, and powers were adjusted to match that of AAN by adjusting the noise powers of the other three methods independently of their transmitted signal power. The results are shown in Figure 2.9.

In this case, the simulation did not repeat the transmit beamforming case when $\alpha = 1$ because all four methods converge and have the same average power and secrecy rate that already is shown in Figure 2.7. When average transmit power is the same, no method has a secrecy advantage. Both AAN methods have lower peak powers than the MAN methods.

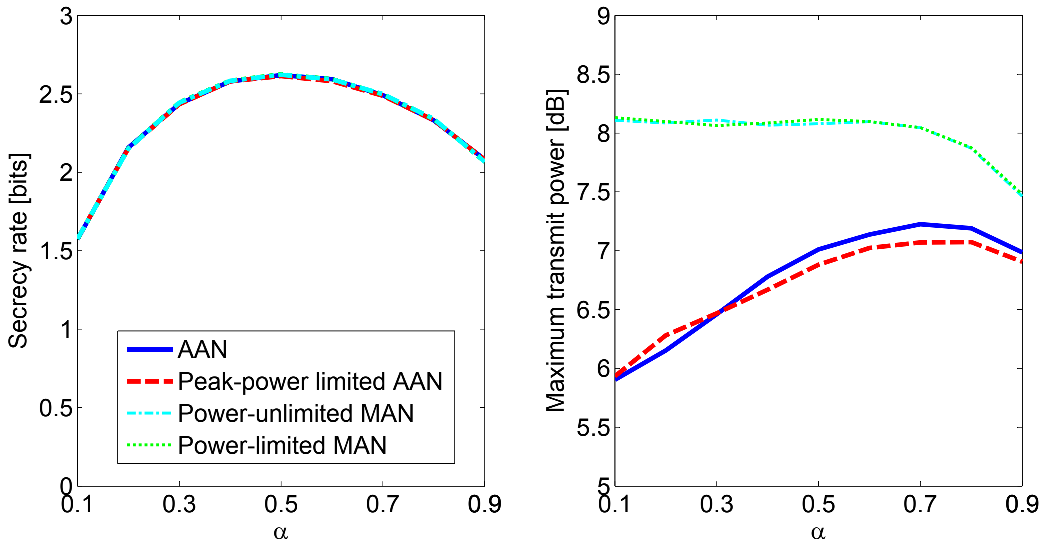


Figure 2.9: Left: secrecy rate for the four fixed array encryption algorithms when the artificial noise component of each is adjusted so all methods have the same average power. Right: maximum transmit power of each algorithm when all four have identical average power, as power allocation is varied between pure noise and pure beamforming.

2.6 Conclusion

In this chapter, four physical layer encryption schemes for fixed transmit arrays have been described. The original AAN scheme from [20] has high secrecy rates in simulations of Rayleigh fading channels, but it has no method for controlling its peak power level and can be computationally intensive to implement. The peak-power limited AAN method does not require matrix inversion to generate its weights, and allows for peak but not average power control. It performs as well as normal AAN for the same average transmit power in Rayleigh fading channel simulations. The power-limited MAN method is much simpler than either AAN method for weight generation, but has a higher peak power for the same average transmit power. The power-unlimited MAN method can have extremely high peak powers, and both MAN methods have high peak powers when most of the transmit power is allocated to artificial noise generation.

In the remainder of this work, the security of the artificial noise methods will be compared in simulated indoor, outdoor, and urban channel environments. AAN also will be implemented experimentally. Before that, Chapter

3 discusses the reconfigurable multiplicative noise (RMN) method that distorts transmitted signals to Eve using an array of reconfigurable elements.

CHAPTER 3

SECRECY WITH RECONFIGURABLE ARRAYS

The method presented in this chapter achieves its security benefit differently from the artificial noise in Chapter 2 in that it foils eavesdroppers by distorting the transmitted signal rather than adding noise to it. By randomly selecting antenna configurations in the transmitting array at the symbol rate, a random phase and amplitude multiplies the transmitted symbol. In effect, the multiplicative randomness seen by eavesdroppers due to switching is mathematically similar to the multiplicative randomness induced by the fixed array MAN algorithm. This method of distorting the signal with reconfigurable elements is termed reconfigurable multiplicative noise (RMN).

This multiplicative randomness is compensated by appropriate element weights so the desired receiver does not experience any random variation and instead receives one unchanging constellation. Section 3.1 reviews idealized and real radiation patterns of reconfigurable elements that will be used in tests of this secrecy algorithm. Then Section 3.2 goes into mathematical detail on the algorithm used for RMN. Section 3.3 discusses the difference compared to Chapter 2 in calculating the secrecy rate. Finally, Section 3.4 briefly discusses reconfigurable pattern selection and whether there is a better way to select patterns than to choose all with equal probability.

3.1 Idealized and Actual Reconfigurable Antenna Patterns

Reconfigurable antennas are able to change some combination of their operating frequency or bandwidth, their polarization, or their radiation pattern [46]. This work focuses solely on pattern reconfigurable antennas, which come in two varieties: beam-steerable and null-steerable. In order to determine which of the two is more desirable from a security perspective, a canonical beam-steering antenna and a canonical null-steering antenna are tested via simulation. The radiation patterns for one configuration of each are shown in Figure 3.1. Both have average gains that are normalized to one and are assumed to have one dominant polarization. The other three configurations have beams or nulls centered at 90°, 180°, and 270°, so either element can cover all 360° in azimuth in a simulated environment.

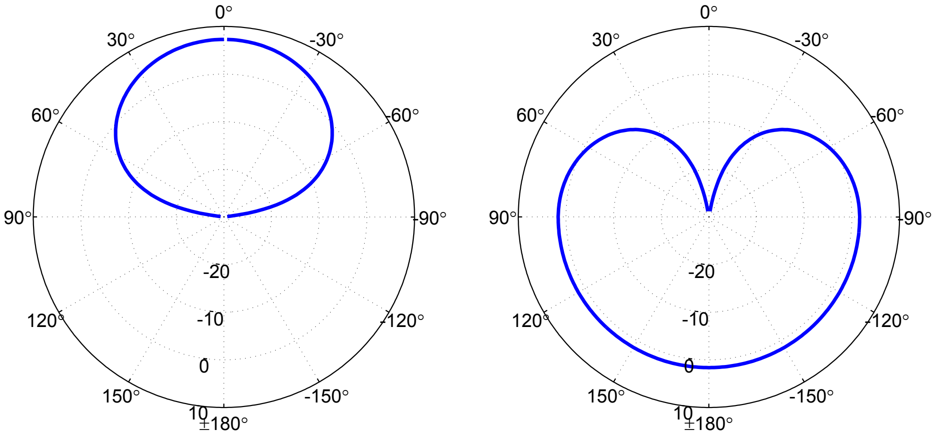


Figure 3.1: One of four possible radiation patterns for an ideal beam-reconfigurable antenna (left) and ideal null-reconfigurable antenna (right). The other three configurations have beams or nulls centered at 90°, 180°, and 270°.

In addition to ideal patterns, three actual radiation pattern reconfigurable antennas are used in simulations (as well as one in the experiment in Chapter 5). The patterns of all configurations for the dominant polarization are shown in Figure 3.2. To be able to determine which type of pattern performs best, rather than total performance that includes other factors such as efficiency and impedance match, all patterns are normalized so their gains are one. Also, these antennas are designed for different operating frequencies, but in simulations, all are assumed to operate at the same frequency so the channel environment is the same and the relative security can be compared.

The first antenna in Figure 3.2 is the reconfigurable microstrip parasitic array (RMPA) [47]. This antenna has three pattern configurations. The second antenna is the broadside to endfire reconfigurable antenna (BERA) [48], which switches between two patterns. These two antennas are beam-steering reconfigurable antennas. The final antenna is called the reconfigurable null-steering antenna (RNSA) [49]. In simulation and experiment, all antennas

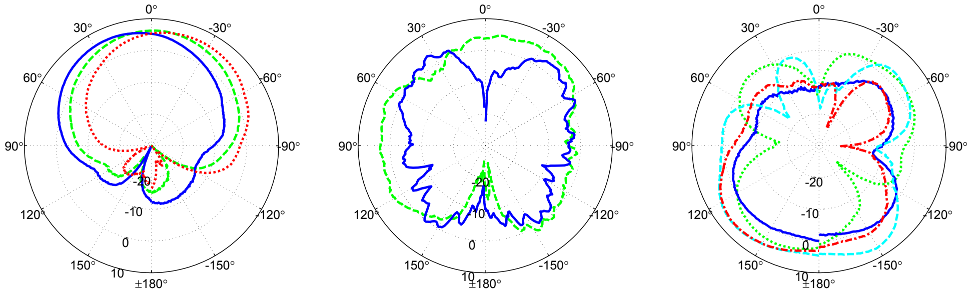


Figure 3.2: Normalized radiation patterns of all switching configurations for three reconfigurable antennas: RMPA (left), BERA (center), RNSA (right). Only the dominant polarization is shown.

will be arrayed and positioned so their patterns shown in Figure 3.2 are in the azimuthal plane.

3.2 Reconfigurable Multiplicative Noise (RMN)

This section explains how the reconfigurable transmit array (Alice) uses pattern reconfigurability to increase security when transmitting to the desired receiver (Bob) in the presence of an eavesdropper (Eve), both of whom are fixed single element receivers. We assume Alice has learned the channels from each of her elements to Bob in each of the elements' states of reconfiguration. If channel reciprocity is assumed, then Bob need not know the channel but simply send out a training signal for Alice to use, and then Eve will not be able to learn her channels to Alice prior to the beginning of the message. However, if channel reciprocity is not assumed, for example due to differences in the RF chains on transmit and receive, then through the channel training between Alice and Bob, Eve can learn her channels to Alice. We assume the latter scenario for all simulations and experiments.

For each symbol sent, Alice chooses random states of configurations for its elements. To keep a constant response to Bob and be power efficient, Alice applies element weights in the manner:

$$w_n(k) = \frac{h^*_{ABn} E^*_{ABn}(k)}{\sum_n |h_{ABn}|^2 |E^*_{ABn}(k)|^2} m(k) \tag{3.1}$$

where h_{ABn} is the channel from the n^{th} element of Alice to Bob, $E_{ABn}(k)$ is the effective pattern from the n^{th} element of Alice to Bob at symbol time k, and $m(k)$ is the symbol sent at time k. The effective pattern is defined as the contribution of the radiation pattern in all directions of departure of significance between Alice and the receiver. Just as the channel might have multiple paths that contribute to the channel tap, the contribution of the radiation pattern might be from multiple directions of departure. This weighting scheme is simply transmit beamforming given the reconfiguration at time k.

Bob receives:

$$r_B(k) = \sum_n h_{ABn} E_{ABn}(k) w_n(k) + n(k) = m(k) + n(k) \tag{3.2}$$

Eve receives:

$$\begin{aligned} r_E(k) &= \sum_n h_{AEn} E_{AEn}(k) w_n(k) + e(k) && (3.3) \\ r_E(k) &= \frac{\sum_n h_{AEn} h^*_{ABn} E_{AEn}(k) E^*_{ABn}(k)}{\sum_n |h_{ABn}|^2 |E_{ABn}(k)|^2} m(k) + e(k) && (3.4) \end{aligned}$$

where $n(k)$ and $e(k)$ are AWGN at time k at Bob and Eve, respectively.

Thus, Eve has a multiplicative random channel that changes at the symbol rate, due to the time dependence of the element patterns in the numerator and denominator of Equation (3.4), which multiplies the message signal $m(k)$. Like the MAN transmit scheme in Chapter 2, it is not possible to compute a closed-form expression for capacity, but a bit-wise method can be used to compute the MI of the RMN transmit technique. The method is not entirely the same as that used in fixed arrays in Chapter 2 due to a different assumption about the nature of the noise. The details of computing bit-wise and symbol-wise MI are given in Section 3.3.

Unlike fixed array secrecy methods, RMN provides some added secrecy even if Alice has only a single element. When $N = 1$, Eve receives:

$$\begin{aligned} r_E(k) &= m(k) \frac{h_{AE} h^*_{AB} E_{AE}(k) E^*_{AB}(k)}{|h_{AB}|^2 |E_{AB}(k)|^2} + e(k) && (3.5) \\ r_E(k) &= m(k) \frac{h_{AE}}{h_{AB}} \frac{E_{AE}(k)}{E_{AB}(k)} + e(k) && (3.6) \end{aligned}$$

Even with a single transmit element, Alice converts Eve's AWGN channel into a multiplicative random channel by randomly reconfiguring at the symbol rate.

3.3 RMN Secrecy Rate Calculation

Similar to the multiplicative forms of noise generated with fixed arrays, the secrecy rate of RMN has no closed-form expression. Calculating the difference in MI from the constellations of Bob and Eve can be done using either the constellation symbols only, as is explained later in this section, or using the bit-wise method explained in Section 2.4.2, with a slight modification. Without AWGN, there are a limited number of unique constellation points that Eve receives, unlike artificial noise techniques that always generate new random points. Therefore, it is assumed that Eve knows how each of the received symbols maps to bits and the sole element of uncertainty is AWGN. It is not necessary to calculate additional noise based on constellation point variance around a mean, and the bit-wise method in Section 2.4.2 is employed using only AWGN to calculate the MI between Alice and Bob or Eve.

One example of constellations transmitted by RMN is shown in Figure 3.3. These constellations were received in the experiment in Chapter 5. The transmitting array was a two-element array in which each element could configure two ways, and the modulation scheme was QPSK. The left constellation in Figure 3.3 seen by Bob has virtually a normal QPSK constellation, aside from a few errors in phase shifters that will be discussed in Chapter 5. The constellation on the right seen by an eavesdropper has 16 distinct points due to the 2^2 array configurations times the four-symbol constellation.

The formulas for symbol-wise integration to find MI are derived. Although bit-wise MI calculations are used in this work because of their greater numerical stability, symbol-wise integration should yield the same MI. Given an M-ary modulation with a reconfigurable transmit array in which each antenna can reconfigure its radiation pattern in C discrete states, there are N^C different total array patterns that can be produced for an N element array. If y is the received symbol and x is the transmitted symbol, then the distribution of y given x is slightly more complex than the fixed array case

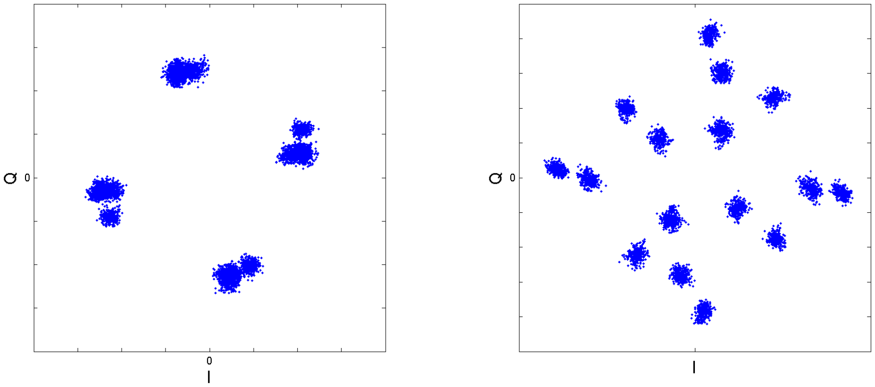


Figure 3.3: Received constellations from the RMN transmission at Alice (left) and an eavesdropper (right).

in Equation (2.57) and is given by:

$$f(y|x) = \sum_{k=1}^{C^N} p(c_k) f(y|x, c_k), \tag{3.7}$$

where c_k denotes the k^{th} array configuration. Assume the array reconfigures in each configuration with uniform probability. Then $p(c_k) = \frac{1}{C^N}$. Because the transmitted symbol location is known to all receivers and the only uncertainty is AWGN,

$$f(y|x) = \sum_{k=1}^{C^N} \frac{1}{C^N \pi N_0} e^{-\frac{|y-g(x,c_k)|^2}{N_0}}, \tag{3.8}$$

where $g(x, c_k)$ maps transmitted symbol x to the received constellation when the transmit array configuration is c_k and N_0 is the AWGN power. The MI between the transmit array and a receiver becomes:

$$\begin{aligned} I(X;Y) = \sum_{i=1}^{M} \int_{\mathbb{C}} \sum_{k=1}^{C^N} & \left\{ \frac{1}{C^N M \pi N_0} e^{-\frac{|y-g(x_i,c_k)|^2}{N_0}} \right\} \\ & \log_2 \left(\frac{M \sum_{q=1}^{C^N} e^{-\frac{|y-g(x_i,c_q)|^2}{N_0}}}{\sum_{l=1}^{M} \sum_{p=1}^{C^N} e^{-\frac{|y-g(x_l,c_p)|^2}{N_0}}} \right) dy \end{aligned} \tag{3.9}$$

3.4 Radiation Pattern Selection

We have assumed that Alice changes randomly to one of the N^C pattern configurations that an N element array with reconfigurable elements that configure C different ways can produce. It has been assumed that each of these configurations is chosen with equal probability. This method will be tested in simulation and is used in the experimental test. Another method is to bias the patterns toward those with better channels to Bob. Because the channels already are known to Alice, she can limit configurations only to those whose patterns are strongly in the direction of Bob's channel.

If Alice only configures to the single best pattern, this simply becomes transmit beamforming. A compromise between transmit beamforming and equiprobable patterns is to bias toward stronger patterns proportional to the channel strength. For example, let $N = 1$ and $C = 2$, meaning Alice is a single element that only configures its pattern in two ways. If the first configuration has twice the SNR to Bob as the second, then Alice will choose the first configuration on average twice as much. This weighted pattern selection scheme is tested via simulation in Chapter 4.

3.5 Conclusion

RMN is another physical layer encryption technique that can be used by itself or combined with artificial noise generation. The latter is demonstrated in Chapter 6. Its security benefit relies on the distorted received constellation by Eve to be more difficult to decode in the presence of AWGN than a normal constellation. Because of this, RMN can be defeated if Eve has a sufficiently strong channel. However, because the transmitter does not generate artificial noise, RMN can be more power efficient than AAN or MAN, but this depends on the antenna radiation patterns. Simulations in Chapter 4 and an experiment in Chapter 5 compare these tradeoffs between RMN and artificial noise encryption.

CHAPTER 4

WIRELESS CHANNEL MODELS

Chapter 4 begins with an explanation of the modified Saleh-Valenzuela channel model, which is a statistical model similar to a Rayleigh fading channel but also takes into account individual antenna patterns and angles of arrival and departure. This is important because different antenna patterns can be tried with this model, and secrecy of each type of reconfigurable antenna can be compared. This performance comparison is given in Section 4.2.

Next, Section 4.3 presents channels generated from a ray-tracing program called Wireless Insite® [50]. Models from actual indoor, urban, and rural landscapes are used to generate channels between a transmit array and receivers spaced throughout the volume of the environment. Channels are found assuming all rays arrive in a time interval to contribute to a single channel tap. The performance of each reconfigurable antenna as well as a fixed array of omnidirectional elements is given in Section 4.4.

Section 4.5 assesses whether using directional antennas offers increased secrecy when using AAN, which can use either fixed or reconfigurable transmit elements. Finally, Section 4.6 analyzes the robustness of AAN and RMN in the face of imperfect channel state information.

4.1 Modified Saleh-Valenzuela Channel

As opposed to an analytical model such as the Raleigh fading channel model that was used to evaluate fixed antenna algorithms in Chapter 2, physical models characterize the channel on the basis of electromagnetic wave propagation [51]. Unlike analytical models, these models take into account antenna patterns and directions of arrival and departure. This allows for comparisons of performance between different pattern-reconfigurable antennas.

The category of physical models can further be subdivided into deterministic models, geometry-based stochastic models, and non-geometric stochastic models [51]. Deterministic models are completely specified by data computed from a measurement or simulation such as ray tracing. This type of model will be used in simulations in Section 4.3. Geometry-based stochastic models compute channels from random geometric arrangements, while non-geometric stochastic models do not use a specific geometry but rather describe parameters such as direction of arrival and propagation delay based on probability density functions.

A well-known non-geometric stochastic model is the Saleh-Valenzuela channel [38]. This model does not take into account antenna pattern but does describe multipath components with an exponentially decaying probability distribution. It groups multipath components arriving at the receiver into clusters that arrive in a Poisson process. The time between the first and last clusters is governed by an exponential decay. Let τ be the time after the first arriving cluster of multipath components and γ be the decay constant. Then only components that arrive when $\exp(-\tau/\gamma)$ is greater than some threshold will be considered in the model. Similarly, within each arriving cluster, the individual multipath components' arrival times are also a Poisson process that is governed by a second decay constant. These individual components arrive sometime after the arrival cluster time, which is the arrival time of the first multipath component of that cluster, and no components arrive once the decay has gone below some threshold.

An extension to the Saleh-Valenzuela model to include antenna patterns and angles of arrival and departure is proposed in [52]. This is termed the Saleh-Valenzuela model with angle of arrival (AOA) / angle of departure (AOD), or SVA model for brevity. Each cluster's AOA and AOD is determined by some probability distribution, and in the case of this work is uniformly distributed over all azimuthal angles. The individual multipath components' AOAs and AODs are Laplacian distributed around the mean AOAs and AODs. The antenna radiation patterns are incorporated by multiplying the pattern value at the AODs for the transmit antennas. The single receive antennas are assumed to be omnidirectional, and all channel modeling is assumed to take place in a single plane rather than three dimensions.

4.2 SVA Channel Performance

Simulated SVA channels were used to assess whether there is a performance gain from favoring radiation pattern configurations with higher SNRs to the desired receiver, as specified in Section 3.4. The three measured patterns and two idealized patterns in Section 3.1 were tested. For each type of antenna, a four-element transmitter was used and channels were simulated to a single desired receiver and a single eavesdropper, both using omnidirectional antennas. The RMN algorithm was used to secure a 16 QAM transmitted signal, and the MI to each receiver was calculated. The transmit power was scaled so the desired receiver had an MI of 3.7 bits. Fifty antenna configurations were used with the RMN algorithm calculated two ways: either the 50 configurations were taken from all of the possible ways the four-element transmit array could reconfigure with equal probability, or configurations were selected with a bias that was linearly proportional to the relative SNR the combined array pattern gave to the desired receiver.

The results are given in Table 4.1. For all five different antennas, choosing antenna patterns biased by how well they pointed to the desired receiver resulted in lower required transmit power relative to an unbiased selection of antenna patterns, as is expected. Average power was reduced by less than 1 dB for most cases. The reduction in randomness did not negatively affect the secrecy. In all five cases, the average MI to the eavesdropper was lower when pattern choice was not uniformly random. This is because the reduction in transmit power made up for the cases in which the same antenna configurations might have been chosen multiple times. Choosing the same antenna configuration increases the MI to Eve, but the lowered transmit power makes up for the increase, resulting in a slight total decrease in average MI to Eve and therefore an increase in the secrecy rate.

4.3 Ray Tracing Channel Models

In this section, the fixed and reconfigurable antenna physical layer encryption methods are compared for their security in simulated channel environments.

Table 4.1: Average MI to Eve and average additional power for uniformly chosen patterns over patterns weighted by desired receiver SNR.

Antenna type	**Eve MI (uniformly chosen)**	**Eve MI (pattern biased)**	**Additional power**
RMPA	1.7	1.7	0.2 dB
BERA	1.4	1.4	0.3 dB
RNSA	1.3	1.3	0.4 dB
Ideal beam	0.7	0.6	1.1 dB
Ideal null	1.2	1.1	0.3 dB

The channels are generated from models of indoor, outdoor urban, and outdoor rural environments used in Wireless Insite® ray tracing analysis software [50]. As shown in Figures 4.1, 4.2, 4.3, 4.4, and 4.5, the transmitter is a four-element linear array with half-wavelength spacing placed in the center of the environments. Examples of the strongest paths from one of the transmit antennas to a receiver are shown in each figure. The operating frequency was chosen to be 1.9 GHz. The channel was calculated using ray tracing and taking the strongest 10 paths to comprise the channel tap from an element of the transmitter to one of the receivers. All receivers are vertically polarized dipoles with gains of one, and are spaced many wavelengths apart from each other. The transmitters use either a vertically polarized dipole pattern in the case of fixed array transmission, or one of the reconfigurable antenna patterns, and the channels incorporating all of these patterns in all configurations were computed.

The transmitters all used 16 QAM modulation, and it is assumed the data rate is low enough that narrowband channel assumptions are valid. After one of the receivers in the volume was designed as the desired receiver, the transmitter was assumed to have perfect channel information and scaled its transmit power so the MI between Alice and Bob was 3.7 bits, or equivalently, Bob always had an SNR of 12.9 dB. All receivers suffer from the same amount of environmental additive white Gaussian noise. All the other receivers are designated as eavesdroppers, and their received signals were analyzed while the transmitter sent a simulated transmission to Bob. Any eavesdropper having an MI to Alice greater than 3.7 bits was decided as decoding the message while those with lower MIs were said not to have decoded the message. The metric presented in the tables that follow is the percentage of eavesdroppers

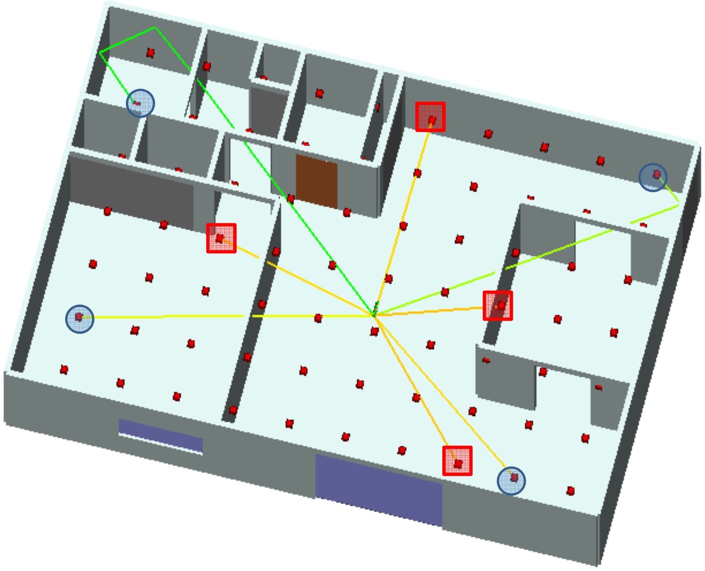


Figure 4.1: Apartment indoor channel environment generated by Wireless Insite® with transmit array in center as green boxes and potential desired receivers or eavesdroppers spaced throughout volume as red boxes. The four low SNR desired receivers are highlighted with blue circles and the four medium SNR desired receivers are highlighted with red squares.

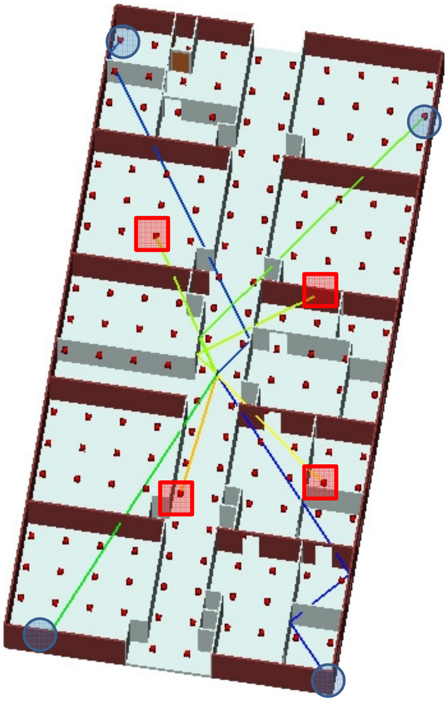


Figure 4.2: Office indoor channel environment.

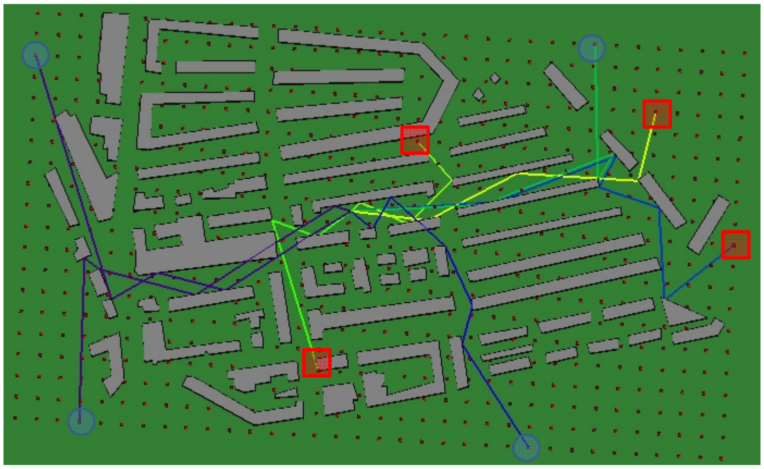


Figure 4.3: Urban channel environment modeled from part of Bern, Switzerland.

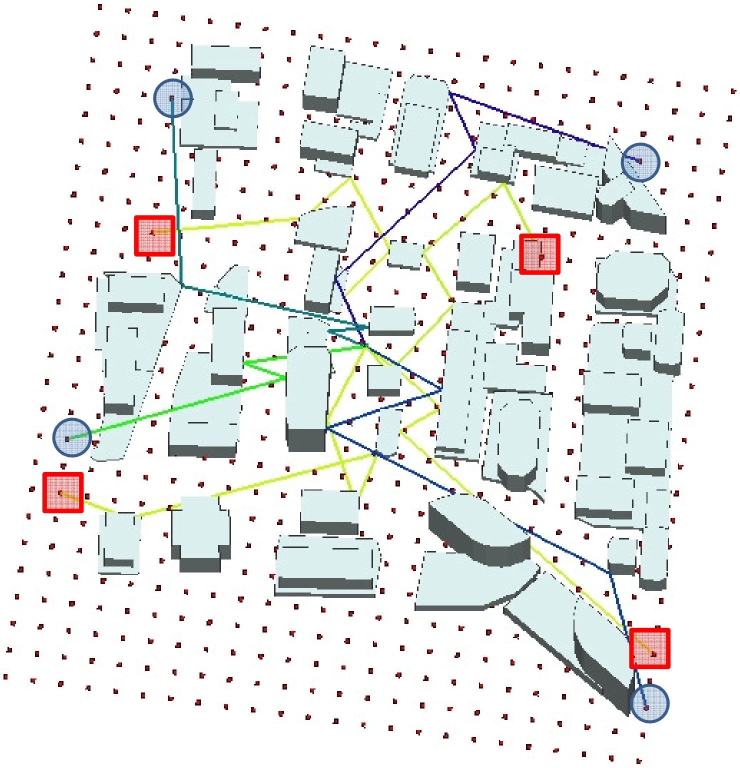


Figure 4.4: Urban channel environment modeled from part of Rosslyn, Va.

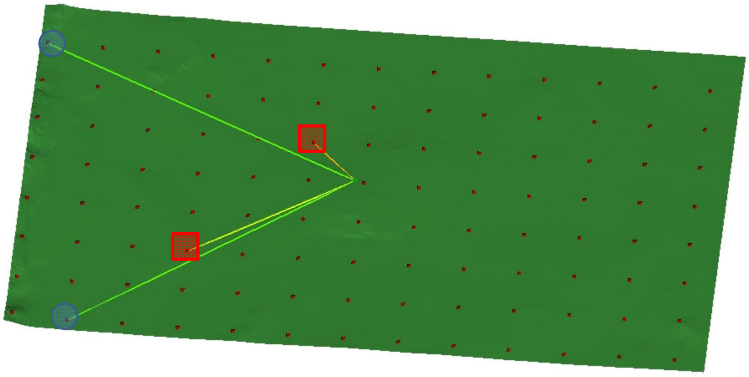


Figure 4.5: Rural channel environment from plains outside of Boulder, Co.

in a volume who were able to decode the message. This parameter is important because it gives an indication of how well a single eavesdropper could decode a message given freedom to move around in a volume. Also given is the transmit power for each scheme, relative to the power required for the fixed dipole array to transmit with an MI of 3.7 bits when using transmit beamforming.

All five reconfigurable antennas are simulated transmitting with the RMN encryption scheme. Patterns are chosen randomly with a bias to those with high SNRs to the desired receiver. A fixed dipole array transmitting with AAN also is simulated. The α parameter is set at either 1/11, 1/2, or 10/11, which corresponds to a noise power that is 10 dB greater than the signal power, equal to the signal power, and 10 dB less than the signal power, respectively. Also tested with the fixed array was the MAN scheme with α equal to 1/2. The transmit beamforming (TBF) array also used dipole elements (that are omnidirectional in the azimuthal plane), which is why some reconfigurable antennas with directional patterns occasionally had lower power usage. Section 4.5 directly compares TBF and AAN using either isotropic elements or beam-steering directional elements pointed toward the desired receiver.

The desired receivers in each simulated environment were chosen as part of a low or medium SNR group. Four receivers were chosen from each environment (except the rural environment in which two were chosen) to be the desired receivers, but of course not at the same time. The four receivers in the low SNR group were chosen from the lowest 10% of all receivers, as measured by the strength of the channels to the transmitters. The four were also spread out approximately 90° apart from each other, so the reconfigurable antennas whose radiation patterns tended to be maximum in one direction would not have an advantage or disadvantage. The same criteria were used to choose the four desired receivers in the medium SNR group, except they were chosen from those receivers whose channels were in the middle 10% by SNR.

4.4 Urban, Indoor, and Rural Channel Performance

Tables 4.2 and 4.3 present the results of the two indoor environments (an apartment and an office) shown in Figures 4.1 and 4.2. In the apartment environment, transmit beamforming alone is enough to thwart about one-third of the eavesdroppers when the desired receiver has one of the lowest channels relative to the rest of the eavesdroppers, and almost 90% of the eavesdroppers are thwarted when the desired receiver has a channel better than about half of the eavesdroppers. Performance is worse in both cases in the office environment. Clearly, transmit beamforming alone is not very reliable in ensuring physical layer encryption in these environments, especially if an eavesdropper can move around and find a stronger channel.

The performance of AAN is highly dependent on the artificial noise power. When the artificial noise is only 10% of the signal power ($\alpha = 10/11$), the percentage of eavesdroppers in the apartment environment with an MI greater than the desired receiver decreased from 66% to 15%. The same dramatic improvement is apparent in the office environment. In highly adverse transmit situations, adding small amounts of artificial noise results in dramatic improvements in secrecy. However, the noise power must greatly increase in order to deny all eavesdroppers a greater MI and thus have a positive secrecy rate in all cases. Even using the same noise power as the signal power left some eavesdroppers with a higher MI, and only when the noise power was made 10 times the signal power were there no eavesdroppers in either environment with a higher MI. This was true for both the desired receivers with moderate SNRs and those with low SNRs.

The other fixed antenna scheme, MAN, tended to have high transmit power no matter the α that was assigned. Only $\alpha = 1/2$ is reported here. The reason transmit power tended to be high was that some randomly generated

Table 4.2: Percentage of eavesdroppers able to decode message and relative average power use for fixed and reconfigurable antenna transmitters in apartment indoor environment.

Encryption scheme	**Low SNR receivers**	**Medium SNR receivers**
Transmit beamforming	65.9% 0 dB	10.9% 0 dB
AAN ($\alpha = 1/11$)	0% 10.4 dB	0% 10.4 dB
AAN ($\alpha = 1/2$)	1.1% 3.0 dB	0.4% 3.0 dB
AAN ($\alpha = 10/11$)	15.2% 0.4 dB	3.6% 0.4 dB
MAN ($\alpha = 1/2$)	0% 14.9 dB	0% 15.8 dB
RMN (BERA)	17.4% −2.4 dB	1.8% −0.8 dB
RMN (RMPA)	18.8% −0.1 dB	6.5% 4.2 dB
RMN (RNSA)	5.1% 0.1 dB	2.2% 0.9 dB
RMN (Ideal beam)	2.2% −0.7 dB	0% −0.6 dB
RMN (Ideal null)	5.4% −0.3 dB	1.4% −0.1 dB

noise vectors caused the denominator in Equation (2.49) to become very small, causing large values for the MAN weights. In practice, if these random weights exceed some power threshold, they may be discarded and new weights generated. Because the average MAN power was even higher than the AAN power with noise 10 dB higher than signal power, the MAN encryption scheme also was able to prevent reception by all eavesdroppers in both indoor environments.

The performance of the RMN algorithm varied somewhat based on the reconfigurable antenna used. Most antennas resulted in average transmit powers near that of transmit beamforming, and some, especially the ideal beam-steering antenna, resulted in transmit powers less than that of transmit beamforming. The ideal beam-steering array can achieve a lower power than that used by transmit beamforming with omnidirectional antennas because

Table 4.3: Percentage of eavesdroppers able to decode message and relative average power use for fixed and reconfigurable antenna transmitters in office indoor environment.

Encryption scheme	**Low SNR receivers**	**Medium SNR receivers**
Transmit beamforming	83.2% 0 dB	24.7% 0 dB
AAN ($\alpha = 1/11$)	0% 10.4 dB	0% 10.4 dB
AAN ($\alpha = 1/2$)	1.8% 3.0 dB	0.6% 3.0 dB
AAN ($\alpha = 10/11$)	29.3% 0.4 dB	10.1% 0.4 dB
MAN ($\alpha = 1/2$)	0% 14.8 dB	0% 15.3 dB
RMN (BERA)	32.3% −0.5 dB	5.4% 0.4 dB
RMN (RMPA)	33.8% 0.2 dB	8.4% 6.2 dB
RMN (RNSA)	15.3% 0.9 dB	1.3% 2.7 dB
RMN (Ideal beam)	5.5% 0.3 dB	0.5% −0.1 dB
RMN (Ideal null)	21.1% 0.0 dB	3.5% 0.0 dB

its directional antennas more often are pointed toward the desired receiver. If this were comparing the average power of RMN with beam-steering antennas to the power of transmit beamforming with beam-steering antennas that are fixed pointed toward the desired receiver, the transmit beamforming power would always be less. As mentioned earlier, the average gain of all antenna patterns was normalized to one, so only the radiation pattern shape – and not antenna efficiency – could be a factor influencing secrecy performance. The patterns were normalized in the azimuthal plane only because the pattern-reconfigurable antennas were only measured in one cut-plane rather than three-dimensional radiation patterns. Thus, a full three-dimensional model with radiation patterns is a topic for future work.

In some cases, notably the RMPA antenna when communicating to the medium SNR group, transmit power was significantly higher than the other

RMN cases. This is because the RMPA's pattern is limited in its directional coverage, even with reconfiguring. Even though the receivers were chosen from four different directions, it is likely that one of the desired receivers was located in a direction close to nulls for all of the RMPA antennas, resulting in increased transmit power to achieve the required MI to that receiver.

Performance of AAN, MAN, and RMN in the two urban environments, Rosslyn, Va, and Bern, Switzerland, is shown in Tables 4.4 and 4.5. It is more difficult in these environments to transmit securely to both the low SNR and medium SNR receivers, as evidenced by the fact that about 95% of eavesdroppers in both environments have a better MI than the low SNR desired receiver when transmit beamforming is used. The urban environments are more challenging because there is a wider range of SNRs between the channels of highest and lowest receiver. For example, in the case of the Bern environment, the difference between the highest and lowest channel SNRs (not including antenna patterns) is 128 dB, while the difference between highest and lowest SNR is 33 dB in the apartment environment.

As with the indoor channel case, adding a small amount of noise with AAN initially produces great returns. Adding artificial noise with power -10 dB of the signal power reduced the number of eavesdroppers with a higher MI by 25% in the case of the low SNR receivers in the Bern channel and by 67% in the Rosslyn channel. However, the artificial noise power additionally required to achieve a positive secrecy rate between the desired receiver and all eavesdroppers is considerably higher. Even when using AAN with noise 10 dB higher than the signal power, some eavesdroppers had a higher MI. In one case when transmitting MAN to the medium SNR desired receivers, all eavesdroppers were forced to have a lower MI. In this case, the MAN transmit scheme required 21.6 dB more power than transmit beamforming, illustrating how much power must be expended by any physical layer encryption scheme for total security.

The RMN encryption schemes that use real-world antenna patterns tend to be highly variable in the required amount of transmit power and the secrecy provided. For example, when transmitting to low SNR receivers in the BERN environment, the RMPA antennas required on average 17.6 dB more power than transmit beamforming while the RNSA antennas required 3.0 dB less. Both transmit arrays achieved approximately the same level of secrecy. This can be explained by the limited paths in urban environments.

Table 4.4: Percentage of eavesdroppers able to decode message and relative average power use for fixed and reconfigurable antenna transmitters in Bern urban environment.

Encryption scheme	**Low SNR receivers**	**Medium SNR receivers**
Transmit beamforming	95.5% 0 dB	41.1% 0 dB
AAN ($\alpha = 1/11$)	5.0% 10.4 dB	1.9% 10.4 dB
AAN ($\alpha = 1/2$)	32.6% 3.0 dB	5.8% 3.0 dB
AAN ($\alpha = 10/11$)	71.2% 0.4 dB	19.5% 0.4 dB
MAN ($\alpha = 1/2$)	2.8% 14.6 dB	0.4% 15.7 dB
RMN (BERA)	84.8% 11.8 dB	23.2% −1.0 dB
RMN (RMPA)	84.9% 17.6 dB	36.8% 10.7 dB
RMN (RNSA)	83.5% −3.0 dB	19.0% 1.3 dB
RMN (Ideal beam)	62.6% −2.6 dB	17.1% −0.6 dB
RMN (Ideal null)	89.8% −0.2 dB	24.4% 0.0 dB

As compared to the indoor environment in which rays could pass through walls with attenuation, the simulated channels in the urban environments assumed rays passing through buildings would be attenuated much more than those rays taking an entirely outdoor path bouncing off of buildings, so the rays going indoors were neglected. Because of this, the transmit arrays placed on a narrow street in between tall buildings had limited angles of departure to the desired receivers, even though the desired receivers may have been located in different directions. The real-world patterns had angles at which no configurations radiated significant power, and this resulted in great power differences between the antenna types.

The ideal beam and null antenna arrays had less dramatic power differences because they were designed to have four configurations, one for each 90° sector. The beam-steering array generally had the lowest average transmit

Table 4.5: Percentage of eavesdroppers able to decode message and relative average power use for fixed and reconfigurable antenna transmitters in Rosslyn urban environment.

Encryption scheme	**Low SNR receivers**	**Medium SNR receivers**
Transmit beamforming	94.5% 0 dB	40.9% 0 dB
AAN ($\alpha = 1/11$)	0.5% 10.4 dB	0.1% 10.4 dB
AAN ($\alpha = 1/2$)	6.8% 3.0 dB	0.7% 3.0 dB
AAN ($\alpha = 10/11$)	30.9% 0.4 dB	14.7% 0.4 dB
MAN ($\alpha = 1/2$)	0.2% 20.1 dB	0% 21.4 dB
RMN (BERA)	84.4% −0.4 dB	26.0% 1.2 dB
RMN (RMPA)	74.3% 13.6 dB	19.5% 0.4 dB
RMN (RNSA)	80.8% −3.3 dB	20.3% 3.0 dB
RMN (Ideal beam)	58.4% 0.4 dB	12.0% 1.3 dB
RMN (Ideal null)	82.2% 0.2 dB	21.8% 0.3 dB

power of any transmit array and foiled more eavesdroppers than any other encryption scheme using similar power levels. This is consistent with the beam-steering array's performance in the indoor channel environments.

The final environment simulated was a rural landscape with no buildings shown in Figure 4.5, and the results are given in Table 4.6. The rural channel had very few possible paths from transmitter to receiver except a direct LOS path and a path with a single ground bounce. Because of this, the most directive antennas tended to greatly outperform the omnidirectional antennas from a power efficiency perspective. The ideal beam-steering transmit array used almost 10 dB less power than the omnidirectional fixed array employing AAN with high artificial noise, and the beam-steering array still was able to foil more eavesdroppers in the case of medium SNR desired receivers.

Table 4.6: Percentage of eavesdroppers able to decode message and relative average power use for fixed and reconfigurable antenna transmitters in rural environment.

Encryption scheme	**Low SNR receivers**	**Medium SNR receivers**
Transmit beamforming	84.7% 0 dB	26.4% 0 dB
AAN ($\alpha = 1/11$)	6.9% 10.4 dB	2.8% 10.4 dB
AAN ($\alpha = 1/2$)	34.7% 3.0 dB	5.6% 3.0 dB
AAN ($\alpha = 10/11$)	70.8% 0.4 dB	15.3% 0.4 dB
MAN ($\alpha = 1/2$)	5.6% 14.4 dB	0% 17.5 dB
RMN (BERA)	43.1% 1.5 dB	11.1% 0.6 dB
RMN (RMPA)	20.8% 22.8 dB	4.2% 16.3 dB
RMN (RNSA)	55.6% −3.0 dB	13.9% −2.8 dB
RMN (Ideal beam)	18.1% 1.4 dB	1.4% 1.3 dB
RMN (Ideal null)	55.6% 0.3 dB	9.7% 0.3 dB

4.5 Directional vs. Isotropic Transmit Antennas

While the RMN encryption scheme requires antennas that can change their radiation patterns, and therefore cannot be isotropic, the AAN scheme allows for either directional or isotropic antennas. The four possible patterns of an ideal beam-steering antenna that was used in previous RMN simulations in this chapter are shown in Figure 4.6 and are compared to four isotropic antenna elements. Simulations using AAN were run in one indoor wireless environment (Figure 4.1) and one outdoor urban environment (Figure 4.4).

Figure 4.7 shows the additional percent of eavesdroppers that were prevented from reception when directional transmit antennas are used instead of isotropic. Directional antennas have a major impact when there is no artificial noise transmitted. Anywhere from about 5% to almost 40% of the total eavesdroppers were able to decode the packets when the transmitter had

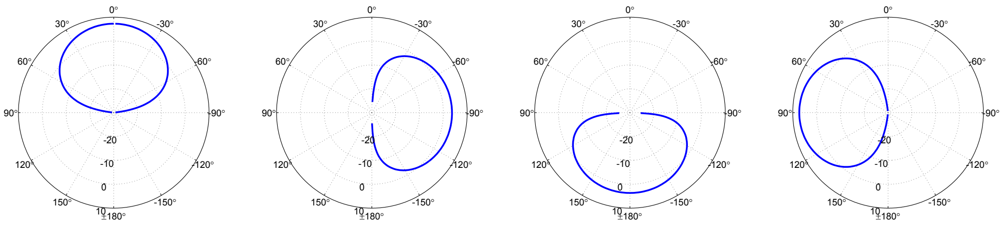


Figure 4.6: The four possible radiation patterns for an ideal beam-reconfigurable antenna element in the azimuthal plane (vertical polarization only). Average gain is normalized to 0 dBi.

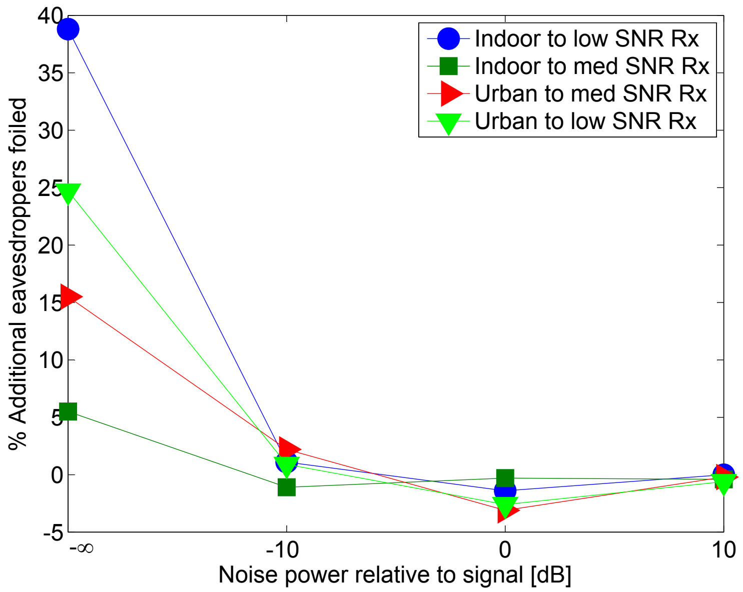


Figure 4.7: The percent of additional eavesdroppers that are not able to decode the signal when the transmit elements have the directive patterns shown in Figure 4.6 instead of isotropic.

isotropic antennas while not being able to decode when the transmitter used directional antennas. However, the benefit diminished with levels of artificial noise comparable to the signal power or higher. There were even instances when an isotropic transmit array allowed fewer eavesdroppers to decode the signal than did the reconfigurable array. This occurred because the reconfigurable array elements have four fixed patterns from which to choose. In some instances, the best configuration to the desired receiver also strengthens the channels of eavesdroppers even more than if the antenna elements were isotropic and all beamforming was done digitally.

4.6 Performance under Noisy Channel Estimates

A continuing assumption for all simulations so far is that the channel estimate has been error-free. In practical scenarios, there is always noise in the estimate of the channel at the transmitter or receiver. An incorrect channel estimate by the transmitter can severely impact secrecy performance because the artificial noise transmitted will no longer be in the nullspace of the desired receiver. Work in [26] attempts to mitigate this consequence of imperfect channel state information (CSI) by proposing several algorithms in which Alice and Bob communicate to better their estimates of the channel. This results in Alice allocating vanishingly small power to artificial noise when CSI uncertainty is high, but even a little artificial noise made dramatic improvements in the secrecy rate. This agrees with the simulation results shown in Tables 4.2, 4.3, 4.4, 4.5, and 4.6, where the addition of some artificial noise and a slight increase in transmit power resulted in far fewer eavesdroppers able to decode the message versus transmit beamforming. Further work on imperfect CSI algorithms in [53] proposed algorithms that could mitigate moderate CSI estimation errors, if the statistics of the estimation errors were assumed known.

In this section, Alice's estimate of the channel is corrupted by AWGN of some power level relative to the channel from Alice to Bob. The indoor office environment from Figure 4.2 is used for simulations, and the desired receivers are the four with medium SNRs relative to eavesdropper SNRs. Figure 4.8 shows the effective SINR of one of the desired receivers under imperfect channel estimates from various encryption schemes. The effective SINRs are plotted as a function of the noise in the channel estimate, expressed as a ratio of the noise power ($\sigma^2_{\Delta \mathrm{h}}$) to the channel strength for the four-element fixed array channel (σ^2_{h}). Artificial noise with powers of -10 dB, 0 dB, and 10 dB, relative to signal power, were analyzed. The RMN case that was analyzed used a four-element array of ideal beam-reconfigurable antennas. Because this requires channel estimates for each antenna configuration, these estimates also were corrupted with the same noise power levels as for the fixed array. Also analyzed was the AAN encryption scheme with equal signal and artificial noise power combined with the RMN scheme. This AANRMN algorithm is explained in detail in Chapter 6.

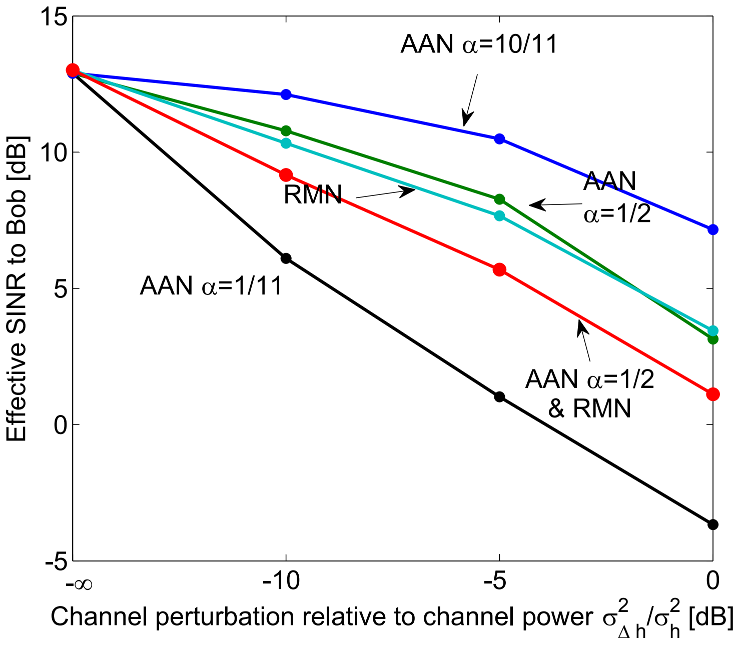


Figure 4.8: The average effective SINR of *one of the four* medium SNR desired receivers with noise in the channel estimates. The ratio of noise in the channel estimate to the channel strength ($\sigma^2_{\Delta\mathrm{h}}/\sigma^2_{\mathrm{h}}$) goes from 0 (no noise) to 1 (0 dB). RMN encryption with beam-steering antennas and AAN with low artificial noise ($\alpha = 10/11$), equal noise ($\alpha = 1/2$), and high artificial noise ($\alpha = 1/11$) are simulated. Also simulated is combined AANRMN with equal signal and artificial noise power.

One hundred simulations of noisy channel estimates and subsequent transmission to the desired receiver were carried out. Both AAN and RMN suffer in SINR performance when their channel estimates become noisy. This decrease in SINR at the desired receiver can be crucial if the SINR goes below the minimum threshold for a given code rate, and thus Bob no longer can decode the message. As expected, more artificial noise power at the transmitter causes a lower received SINR because some of that artificial noise is now sent through Bob's channel. In the case in Figure 4.8 in which the artificial noise power is 10 dB greater than the signal power ($\alpha = 1/11$), even a little noise in the CSI estimate with one-tenth the power of the channel to Bob dramatically reduced the SINR to Bob by about 7 dB. The combined AAN-RMN algorithm suffers from the effects of noise more than either individual algorithm because the erroneous channel estimate causes both artificial noise to be transmitted to Bob (AAN's problem) and Alice's transmit antennas to no longer beamform perfectly (RMN's problem).

The RMN encryption scheme was then compared to the AAN scheme with equal artificial noise power to signal power ($\alpha = 1/2$) over all four desired receivers. The resulting effective SINRs are shown in Figure 4.9. The SINRs were slightly less degraded by noise when using the RMN scheme versus AAN. This is because RMN is biased to use the stronger channels more often, meaning it leverages its directive antennas to be pointing more often in the direction of the desired receiver. Even though the average channel power to the desired receiver of the beam-steering antennas over all configurations is approximately the same as the omnidirectional antenna power, RMN uses its better channels more often and therefore the noise has a slightly smaller impact on the channel estimate.

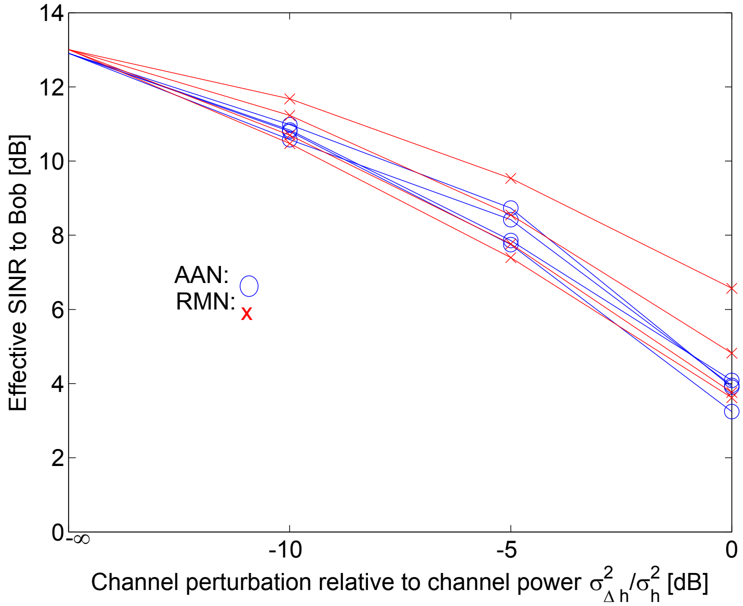


Figure 4.9: The average effective SINR of *all four* medium SNR desired receivers with noise in the channel estimates. The ratio of noise in the channel estimate to the channel strength ($\sigma^2_{\Delta\mathrm{h}}/\sigma^2_{\mathrm{h}}$) goes from 0 (no noise) to 1 (0 dB). RMN encryption with beam-steering antennas, AAN with equal noise to signal power ($\alpha = 1/2$), and the two algorithms combined are simulated.

This slight advantage for RMN in effective SINR results in significantly increased security. The MI between Alice and each Eve for all trials and all desired receivers was calculated for the two schemes. The percentage of eavesdroppers having an MI greater than 3.7 bits, the threshold used in the previous simulations in this chapter, did not change with increasing CSI estimation errors. This is because Bob's channel does not determine how well the average eavesdropper receives the signal, so a slight change in Bob's channel neither increases nor decreases the performance of the eavesdroppers. In this particular case, the percentage of eavesdroppers with MIs greater than 3.7 bits ranged from 0% to 0.7%, and there was no trend with increasing channel estimation error, nor were there significant differences between RMN and AAN transmission.

However, the difference in secrecy performance is evident when comparing how often there is a positive secrecy rate. Because Bob's MI will be affected by the decreased SINR, it makes sense to compare how many eavesdroppers have an MI greater than Bob's MI rather than greater than the fixed 3.7 bits benchmark. When an eavesdropper has a higher MI than Bob, there is no rate at which secure communication is possible. Bob's MI will be less than 3.7 bits when his effective SINR goes lower than 12.9 dB. Figure 4.10 shows the average number of eavesdroppers that had MIs greater than Bob's MI as a function of channel estimation error. As the channel estimation error becomes significant, there are about twice as many eavesdroppers that have a higher MI than Bob from the AAN encryption than from the RMN encryption.

The combined AANRMN scheme allows fewer eavesdroppers to gain a higher MI than Bob's MI despite the fact that Bob's MI is degraded by imperfect CSI using the AANRMN scheme more than either AAN or RMN alone. It is shown in Chapter 6 that AANRMN provides more secrecy than either encryption scheme on its own, and therefore the eavesdroppers have lower MIs to start. Therefore Bob can tolerate a lower MI than with AAN or RMN alone and still have a positive secrecy rate compared to most eavesdroppers.

AAN and RMN encryption performed surprisingly similarly considering they transmit artificial noise in entirely different ways. Slight errors in the channel estimate to Bob significantly lowered Bob's receive SINR. This can be mitigated using AAN encryption because the amount of artificial noise power transmitted can be controlled, but lowering the artificial noise allows more eavesdroppers to decode the confidential message. While some work already has been done to determine the optimal artificial noise power level under imperfect channel estimates and under certain assumptions, a more general power allocation for AAN and a derivation of the power allocation

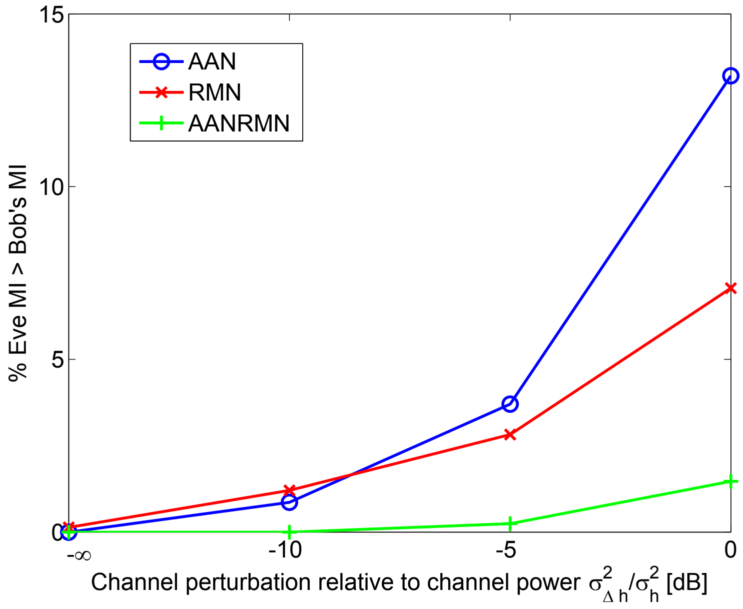


Figure 4.10: The percentage of eavesdroppers who are able to decode a signal intended for one of the four medium SNR receivers in the office channel. Either AAN or RMN encryption is used with noisy channel estimates that range from zero noise to noise power of the estimate equal to the channel power.

for RMN are topics for future work.

4.7 Conclusion

Several conclusions can be drawn from the simulations in this chapter. First, it is better to select patterns for RMN encryption with a bias toward those that direct more radiation toward the desired receiver. Although this may reduce the randomness that prevents eavesdroppers from easily decoding constellations they receive, it is compensated by the fact that those eavesdroppers now receive a signal with lower average power, and therefore AWGN also thwarts their attempts to decode the message.

Second, in all simulated wireless channel environments, it was seemingly possible to communicate with a randomly selected receiver while preventing all other eavesdroppers in the volume from receiving the same or better MI using physical layer encryption alone. Of course, this assumes all receivers were alike, and the eavesdroppers had no special advantages such as directional antennas or the ability to collaborate. The surest way to achieve a positive secrecy rate between the desired receiver and any eavesdropper was to increase artificial noise power, which was demonstrated in the AAN and MAN techniques' results. The required noise power for all positive secrecy rates was very high, often more than 20 dB higher than the power to simply transmit to the desired receiver without any physical layer encryption.

Third, RMN encryption is a viable alternative to artificial noise methods because it can achieve comparable rates of secrecy while often requiring much less transmit power. The best type of pattern reconfigurable antenna as judged by fractions of eavesdroppers foiled and power efficiency was the ideal beam-steering antenna. The real-world pattern antenna performance was highly variable because there were transmit angles at which no pattern configuration had a high intensity. Thus, an important design goal when using RMN with pattern reconfigurable antennas is to assure good pattern coverage over the entire set of possible transmit angles for at least one of the radiation pattern reconfigurations. The ideal beam-steering array outperformed the ideal null-steering antenna in almost every scenario. Thus, the other design principle is that it is better to use a beam-reconfigurable antenna than a null-reconfigurable antenna for this type of physical layer encryption. This makes intuitive sense because in the limit as the beam reconfigurable antenna becomes more and more directive, as long as it can still point to the desired receiver, the power levels to all other eavesdroppers can be further reduced. In the extreme case, a highly directive beam assures virtually all other eavesdroppers have a lower MI, solely because their channels are different from that of the desired receiver.

Chapter 5 experimentally compares transmit beamforming, AAN, and RMN using a BERA transmitting array in a purely LOS environment. Chapter 6 shows the simulated performance when combining AAN and RMN into a single encryption scheme.

CHAPTER 5

FIXED AND RECONFIGURABLE ARRAY SECRECY TEST

An experimental test of AAN and RMN techniques is presented in this chapter. A four-element array of reconfigurable BERA elements is used as the transmitter. If wired with radio-frequency microelectromechanical switches (RF MEMS), each element can either configure to a broadside or endfire radiation pattern, but elements are hardwired for proof of concept with two of the four in broadside mode and the other two in endfire mode. For AAN transmission, two elements are chosen that are broadside mode, while RMN is implemented by using two of the four elements to simulate two elements that change between endfire and broadside. A desired receiver is located in a LOS channel from the transmit array, and eavesdroppers are located in other directions also with LOS channels of approximately the same signal strength. A more detailed experimental setup is given in Section 5.1 and secrecy results are given in 5.2.

5.1 Experimental Setup

The transmit array is a four-element linear array of broadside to endfire reconfigurable antennas (BERA) [48]. They are spaced one-half wavelength apart at their operating frequency of 6.9 GHz. The first and third elements are hardwired to broadside mode and the second and fourth elements are hardwired to endfire mode. The dominant polarization is horizontal ($\hat{\mathrm{y}}$), shown in Figure 5.1. The array is located inside an anechoic chamber, and the receiving standard gain horn is used as both the desired antenna and eavesdropper. The array rotates in the xy (azimuthal) plane as well, and thus the desired receiver and eavesdroppers are level with the transmit array in this plane. The measured active element patterns of all elements at the operating frequency and dominant polarization are shown in Figure 5.2.

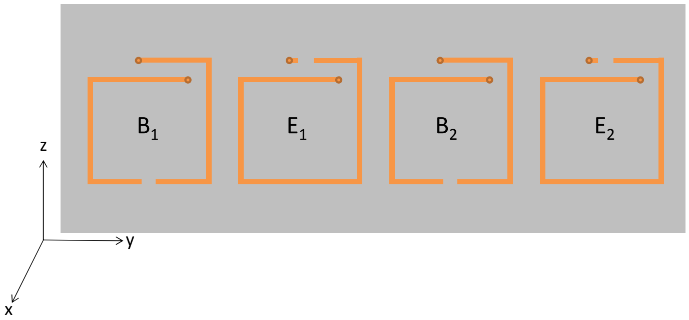


Figure 5.1: Transmit array dominant polarization is horizontal (ŷ) and eavesdroppers and desired receiver are level with the transmit array in the azimuthal (xy) plane.

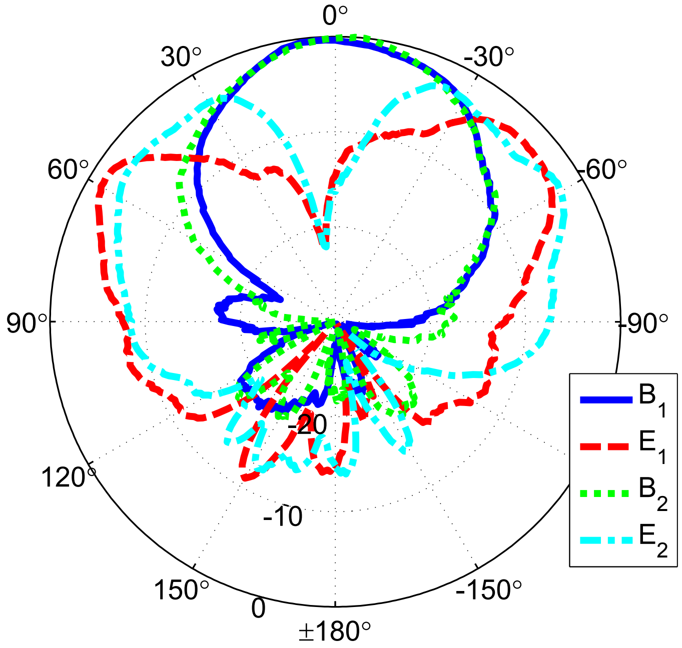


Figure 5.2: Active element patterns of all four transmit elements configured in either broadside or endfire mode.

5.1.1 Transmit Beamforming Experimental Setup

Three different transmit methods are evaluated: simple transmit beamforming, AAN, and RMN. The transmit beamforming experimental setup is shown in Figure 5.3. Only elements B$_1$ and B$_2$ are used, and the other two elements are prevented from radiating by configuring the phase shifters behind them into high isolation states. The signal transmitted is QPSK modulated at 200 kbps. The reason for the low bit rate and the reason that a higher order modulation is not used is the phase shifters provide the modulation rather than it being generated in baseband, due to hardware constraints. The phase shifters are 5 bit digital phase shifters with 360° of phase that are controlled by a computer. The computer cannot switch the phase shifters faster than 100,000 times per second due to limits on the operating system. A higher order modulation is not possible because the signal must be constant in amplitude because of control only of the phase. The signal generator shown in Figure 5.3 generates a 6.9 GHz CW signal, which then becomes modulated QPSK by the phase shifters before entering the antenna elements.

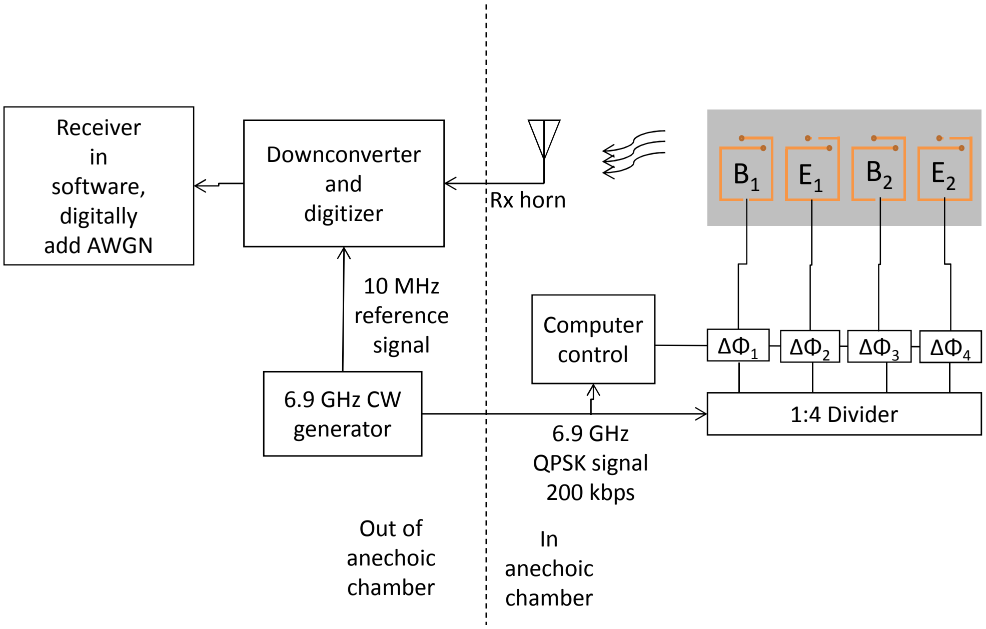


Figure 5.3: Experimental setup for transmitting RMN and transmit beamforming. The latter only uses elements B_1 and B_2.

The desired receiver is arbitrarily designated to be 40° from the transmit array broadside. The total radiation pattern of the two broadside elements when both phase shifters provide 0° phase and when the two-element array is steered to the desired receiver is shown in Figure 5.4. The pattern maximum when steered to 40° is closer to 30° due to phase quantization error as well as variations in the insertion loss of the phase shifters. The insertion loss was noticed to vary over 3 dB when the phase shifters were configured to various modes. Also, the phase error of the digital phase shifters was as high as 20°, meaning that a phase shifter directed to 180° may only provide 160° of phase. It was decided not to correct for these errors because they would similarly affect AAN and RMN transmissions and be difficult to correct in those two schemes.

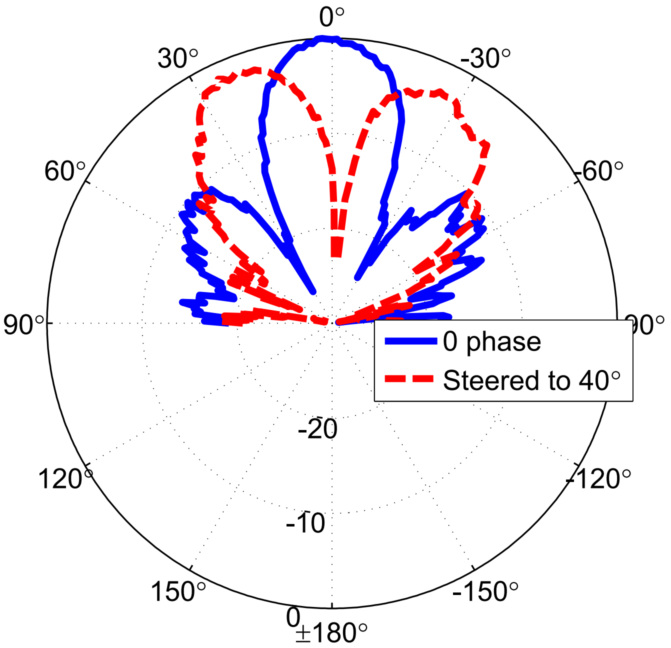


Figure 5.4: Total radiation pattern of elements B_1 and B_2 when steered toward broadside and toward 40°. The pattern maximum is closer to 30° due to amplitude variations in the phase shifters as well as phase quantization error.

Once the transmitted signal was received by the standard gain horn acting as the desired receiver or an eavesdropper, depending on the rotation of the transmit array to 40° for the desired receiver or another angle for an eavesdropper, it was downconverted and digitized. The receiver is locked to the 6.9 GHz frequency by a reference signal from the signal generator so a phase-lock loop is not necessary. A method of synchronizing the symbol rate is necessary, however, because the symbol rate is generated by a computer connected to the phase shifters and not locked to the receiver. The method implemented was to oversample the signal by a factor of four and use a delay lock loop to continually adjust the best sampling point.

5.1.2 Reconfigurable Multiplicative Noise Transmission Experimental Setup

Figure 5.3 also depicts the experimental setup for RMN transmission. In contrast to the transmit beamforming setup, RMN uses all four elements but only two at a time. One element from B_1 and E_1 and one from B_2 and E_2 is chosen randomly. The other two elements are turned off by their phase shifters. This mimics the effect of using two elements that are reconfigurable between broadside and endfire, with the only difference being a phase offset from switching between the adjacent hard-wired broadside and endfire elements.

Phase shifts of the two transmitting elements are chosen to give the same amplitude signal in the desired direction, and the proper phase according to the current QPSK symbol. For the desired transmit angle of 40°, the corresponding phase shifts are given in Table 5.1.

Table 5.1: Phase shifts necessary to give a zero phase response toward the desired receiver with all four RMN element combinations, and the measured normalized amplitude and phase response.

Elt. combo.	1st elt. phase	2nd elt. phase	Amplitude	Phase
B_1 B_2	−142°	17°	0.5 dB	10°
B_1 E_2	−76°	−60°	0.2 dB	−5°
E_1 B_2	−155°	−2°	0.2 dB	−2°
E_1 E_2	−111°	−58°	−0.8 dB	−2°

At the symbol rate, one of the four element combinations from Table 5.1 is randomly chosen with equal probability. The phase shifters corresponding to those elements are set to the phases in Table 5.1 added to the phase of the current QPSK symbol, quantized to the nearest 5.625° because 5 bit phase shifters are used.

5.1.3 Additive Artificial Noise Transmission Experimental Setup

The experimental setup for AAN differs slightly from both transmit beamforming and RMN, and is shown in Figure 5.5. Like transmit beamforming, only the two broadside elements are used. Each element receives the combined output of two different phase shifters, where one phase shifter ($\Delta\Phi_{\text{sig}}$)

serves to direct the beam to the desired receiver and produce the QPSK symbol, while the other phase shifter ($\Delta\Phi_{\text{int}}$) produces the artificial noise that falls in the nullspace of the channel to the desired receiver.

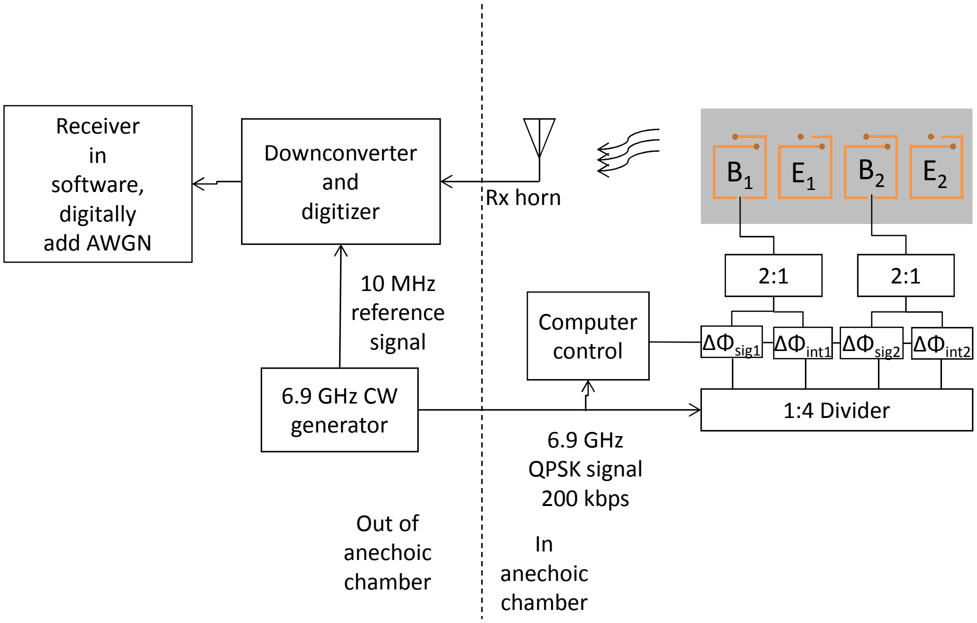


Figure 5.5: Experimental setup for AAN transmission. The two broadside elements transmit. Phase shifters $\Delta\Phi_{\text{sig1}}$ and $\Delta\Phi_{\text{sig2}}$ beamform to the desired receiver and produce the QPSK symbols, while $\Delta\Phi_{\text{int1}}$ and $\Delta\Phi_{\text{int2}}$ produce artificial noise in the nullspace of the desired receiver's channel.

The equations governing the phase shifts at each symbol time are as follows. Like in the other two experimental cases, the desired receiver is the standard gain horn 40° from the transmit array broadside. Let the channels from elements B_1 and B_2 to the desired receiver be given by h_{B_1} and h_{B_2}. The signal phase shifters are set to beamform to the desired receiver and add the phase of the current message symbol $m[k]$:

$$\Delta\Phi_{\text{sig1}}[k] = -\angle \text{h}_{\text{B}_1} + \angle m[k] \tag{5.1}$$

$$\Delta\Phi_{\text{sig2}}[k] = -\angle \text{h}_{\text{B}_2} + \angle m[k] \tag{5.2}$$

The measured channel amplitudes are within 0.2 dB of each other, which is crucial for generating the artificial noise part of AAN because there is only phase control of the transmitting elements. The constraint on the artificial noise is that it must add to zero at the desired receiver. This is equivalent to randomly steering a beam at the symbol rate that always has a null in the direction of the desired receiver. The first of the two interference phase shifters is free to take any value $\Delta\Phi_{\text{int1}}$

$$\Delta\Phi_{\text{int1}} = 2\pi r \tag{5.3}$$

where r is a uniform random variable between zero and one. For no interference in the desired direction, the second phase shifter must satisfy:

$$\exp\left(j\left(\text{h}_{\text{B}_1} + \Delta\Phi_{\text{int1}}\right)\right) + \exp\left(j\left(\text{h}_{\text{B}_2} + \Delta\Phi_{\text{int2}}\right)\right) = 0 \tag{5.4}$$

because channels from both elements to the desired receiver are equal in amplitude. Equation (5.4) is satisfied when the second phase shifter is set to:

$$\Delta\Phi_{\text{int2}} = \Delta\Phi_{\text{int1}} + \angle\text{h}_{\text{B}_1} - \angle\text{h}_{\text{B}_2} + \pi \tag{5.5}$$

Due to amplitude variations in the phase shifters, phase errors between the set phase shift and the actual produced phase shift, and phase quantization, the artificial noise is not exactly zero in the desired direction. But results in Section 5.2 show the artificial noise at the desired receiver is low relative to the signal power.

5.2 Fixed and Reconfigurable Array Performance

5.2.1 Received Constellations

This section describes the results of the transmission of data using either ordinary transmit beamforming, AAN, or RMN. The message transmitted by all three methods is a pseudo-random binary sequence (PN15). The desired receiver was chosen to be 40° from array broadside, and the eavesdropper locations to be measured were chosen to be 0° (broadside), 20°, 30°, 50°, and 60°. Depending on the type of interference (AAN, RMN, or none), the eavesdroppers will receive constellations that are distorted in different ways, while the desired receiver should receive an ordinary QPSK constellation regardless of the security method. Measured received constellations without any added noise in postprocessing are shown in Figures 5.6, 5.7, and 5.8.

The received constellations from transmit beamforming shown in Figure

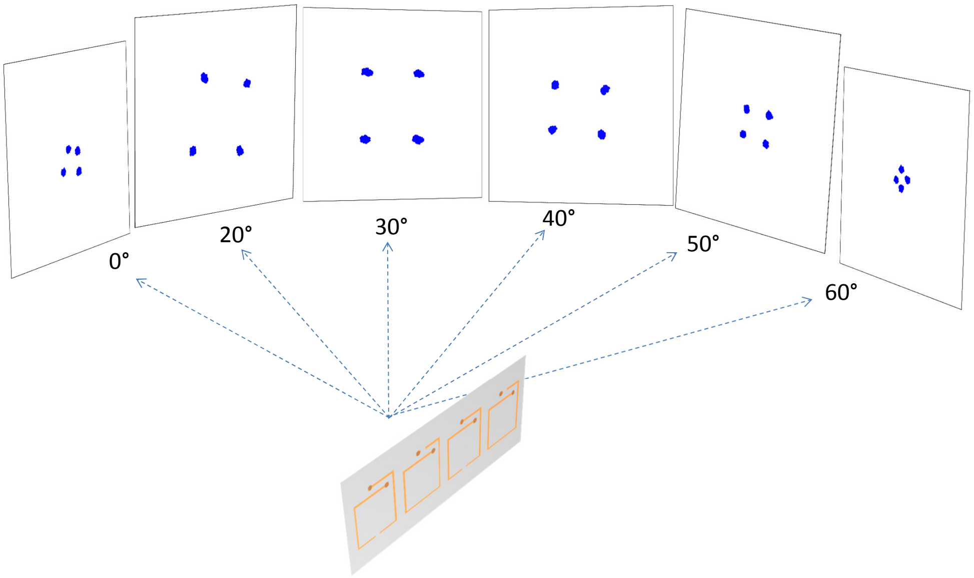


Figure 5.6: Measured constellations at the desired receiver (40°) and all eavesdroppers. The constellation at 30° is slightly larger in amplitude than the desired receiver's constellation due to errors in the phase shifters that distort the radiation pattern, as shown in Figure 5.4. Postprocessing noise not added.

5.6 are simply scaled in amplitude and rotated due to the radiation pattern from the transmit array and the differences in path phase when the transmit array is rotated. The constellation amplitudes correspond to the measured radiation pattern in Figure 5.4. Due to phase shifter errors, the pattern maximum was closer to 30° than to the desired receiver at 40°. Transmit beamforming adds no physical layer encryption, and eavesdroppers only may be thwarted by mathematical cryptographic methods or by a sufficiently low SNR.

When the array transmits AAN as shown in Figure 5.7, the constellations other than that of the desired receiver have interference in the form of random deviations from the transmitted four QPSK constellation points. Because the artificial noise is created by phase shifters instead of weights with full amplitude and phase control, these deviations from the actual constellation points are constant in amplitude and therefore form rings around the points. Obviously, this is less secure than full amplitude and phase controlled interference that would fill in the area around the constellations, but there is ambiguity in the areas in which these rings intersect. This further

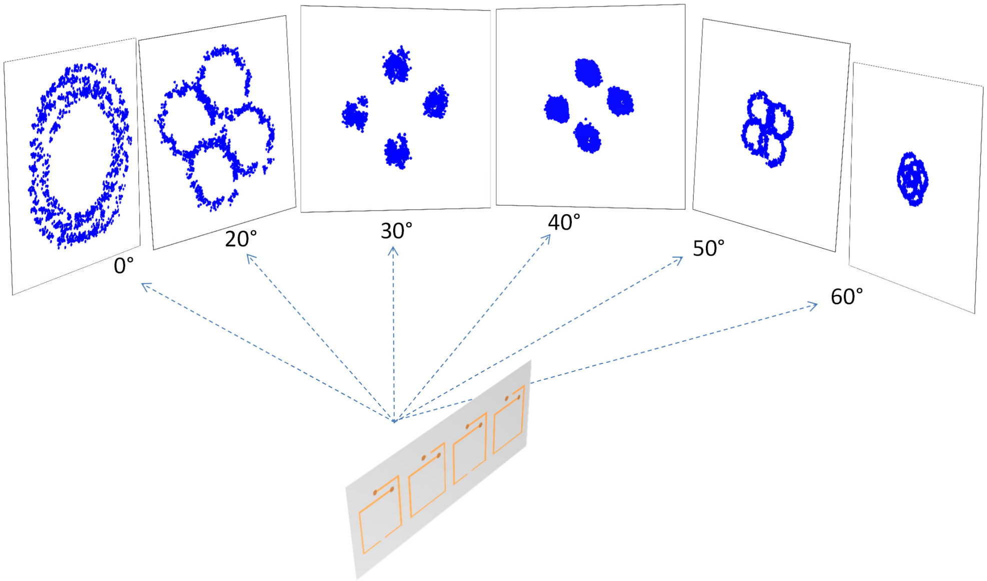


Figure 5.7: Measured constellations when AAN is used to transmit the data. The artificial noise distortion is limited to a nearly constant magnitude circle around the constellation points because interference is implemented with phase control only. Postprocessing noise not added.

complicates the eavesdroppers' task of decoding the received signals in the presence of AWGN.

The received constellations before added AWGN that are created by a RMN scheme are shown in Figure 5.8. The pairs of broadside, endfire, or mixed broadside and endfire element patterns all have the same amplitude to the desired receiver when phases are chosen according to Table 5.1. This is evident by the single QPSK constellation to 40°. In other directions there are as many as 16 distinct constellation points seen by the eavesdroppers, due to the four QPSK points multiplied by the four different array pattern configurations. The increased number of points are clustered closer together and therefore are more easily confused in the presence of AWGN.

5.2.2 Secrecy Rates

Gaussian noise is added in postprocessing to mimic channels of various SNRs. From these channels, secrecy can be compared between transmit beamforming and no encryption scheme and using AAN or RMN encryption. Because the received constellations at the desired receiver are all undistorted, the MI

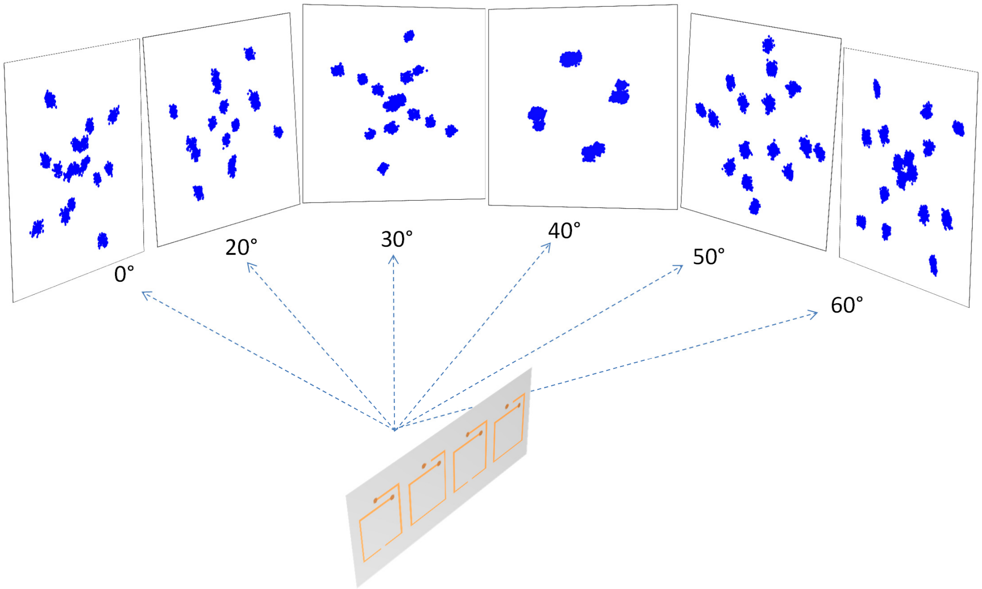


Figure 5.8: Measured constellations when RMN is used to transmit the data. Eavesdroppers receive 16 constellation points because the four QPSK symbols are multiplied by the four different array pattern configurations. Postprocessing noise not added.

as a function of SNR should be the same regardless of the transmit scheme. The MI is calculated according to Section 2.4.2 on the measured data with added AWGN, and the resulting MIs are shown in Figure 5.9, verifying that they are very similar. The assumption that the eavesdroppers know the bit assignments of constellation points is more valid with the AAN transmitted in this experiment than if the AAN had phase and amplitude control. It is discernible simply from looking at the constellations distorted by AAN in Figure 5.7 to which symbol most of the constellation points belong, though ambiguities arise in the areas where two rings of interference intersect.

Because the constellations received by the eavesdroppers are very different depending on the transmit method, MI as a function of Bob's SNR varies. A more meaningful way to analyze the secrecy performance is shown in Figure 5.10. It shows the minimum SNR required by each eavesdropper to successfully decode a signal when the communication rate from Alice to Bob is given on the horizontal axis. In the case of transmit beamforming (TBF), a scaled and rotated version of the same QPSK constellation is sent to all eavesdroppers. As a function of SNR, scaling and rotating a QPSK constellation does

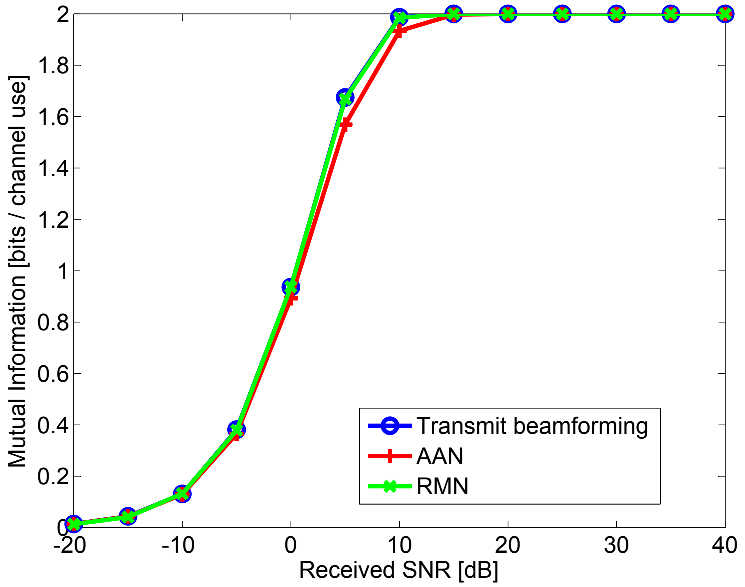


Figure 5.9: MI vs. desired receiver SNR at the desired receiver when AWGN is added in postprocessing. Because all constellations should have no distortion or artificial noise, the MI is the same for all methods.

not lower the MI, and consequentially all received TBF constellations require the same minimum SNR for a given rate. The constellations produced by AAN and RMN are distorted in other ways that will lower the MI for a given SNR. Thus, eavesdroppers require a higher SNR to compensate for this distortion.

In general, AAN seems to slightly outperform RMN from Figure 5.10. Specific comparisons showing the secrecy rate between the desired receiver and a single eavesdropper are shown in Figures 5.11 through 5.15. The secrecy rate, which is the difference in MI between Bob and Eve, is shown as a function of Bob's SNR. The secrecy rate is equal to zero if Bob's MI is lower than Eve's MI. When Bob has a very low SNR, Eve also will have a very low SNR because the channels in this experiment are all LOS and similar in strength. The MI of any signal at Bob or Eve is close to zero, and therefore the secrecy rate is close to zero. Similarly, when Bob has a very high SNR, any Eve also will have a high SNR, and the MI between Alice and Bob or Eve will both be close to two bits, leading to a nearly zero secrecy rate again.

Assuming the eavesdroppers have similarly strong channels to Alice as Bob's channel to Alice, Alice and Bob should communicate with a moderate

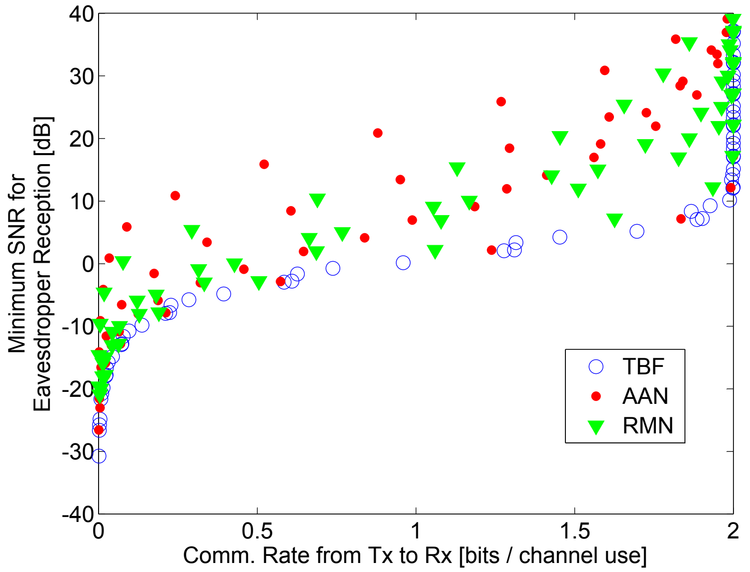


Figure 5.10: The minimum SNR for each eavesdropper to be able to decode the message as a function of the communication rate between Alice and Bob. Eavesdroppers receiving AAN and RMN require a higher SNR than TBF for the same rate because their constellations are distorted and thus harder to decode in the presence of noise.

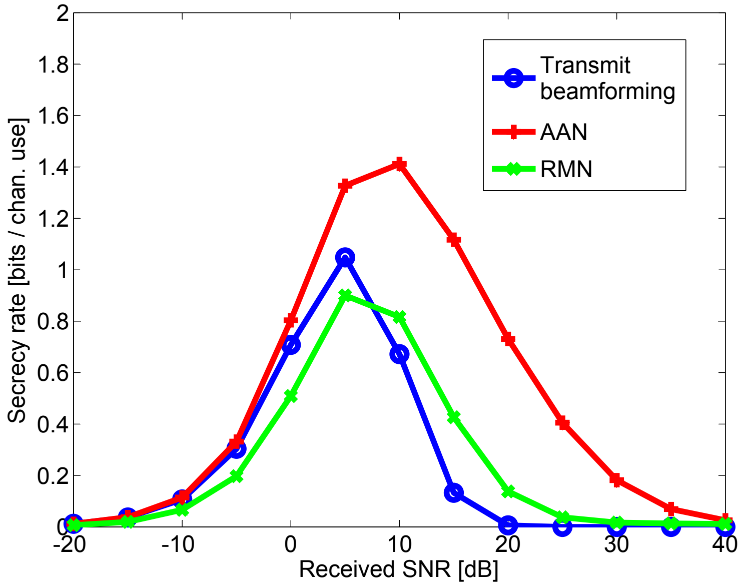


Figure 5.11: The secrecy rate (difference in MI) between the desired receiver and the eavesdropper at 0° for all three methods, as a function of Bob's SNR.

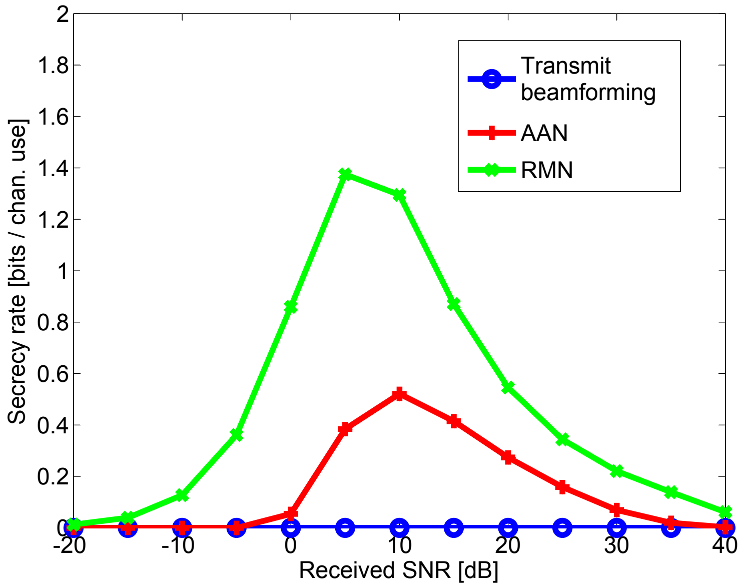


Figure 5.12: The secrecy rate (difference in MI) between the desired receiver and the eavesdropper at 20° for all three methods, as a function of Bob's SNR.

SNR in order to maximize their secrecy capacity. Figures 5.11 through 5.15 indicate that Alice should adjust her power so Bob has an SNR between 0 dB and 10 dB to maximize the secrecy rate. Even transmit beamforming offers some secrecy capacity gains in this SNR regime due to Alice's ability to direct her radiation. It is in the 0 dB to 10 dB SNR regime that the MI quickly climbs from nearly zero to nearly the maximum for both ordinary constellations and constellations distorted by RMN or AAN. Equivalently, Figure 5.10 shows that communicating with a rate from 1 to 2 bits per channel use allows the largest spread, up to about 25 dB, between the minimum SNR required by Bob to decode the message and the minimum required by an eavesdropper receiving AAN or RMN.

In three of the figures in 5.11 through 5.15, AAN achieves the highest secrecy capacity, and in the other two, RMN is the best. Whether RMN or AAN are more secure toward a specific eavesdropper is a function of the transmitted constellation. From Figures 5.7 and 5.8, the eavesdroppers for which AAN yields a higher secrecy capacity tend to receive a more clustered together constellation from AAN than RMN. When RMN yields a higher secrecy capacity, the opposite is true.

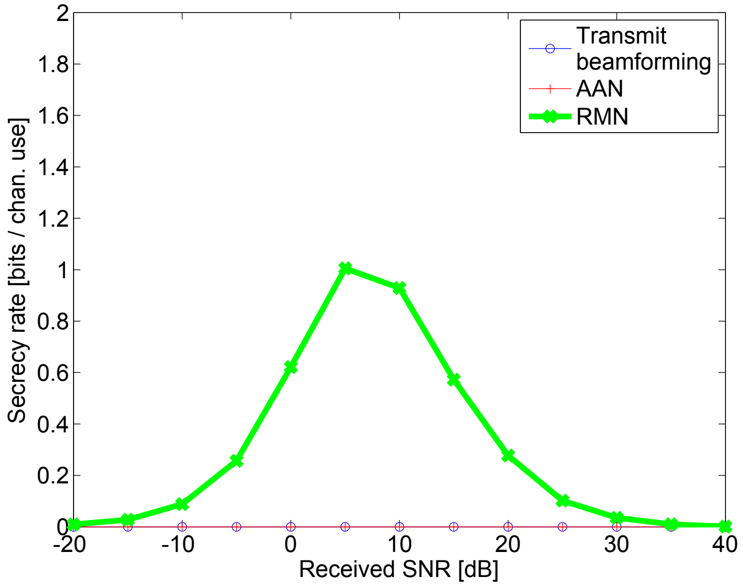


Figure 5.13: The secrecy rate (difference in MI) between the desired receiver and the eavesdropper at 30° for all three methods, as a function of Bob's SNR.

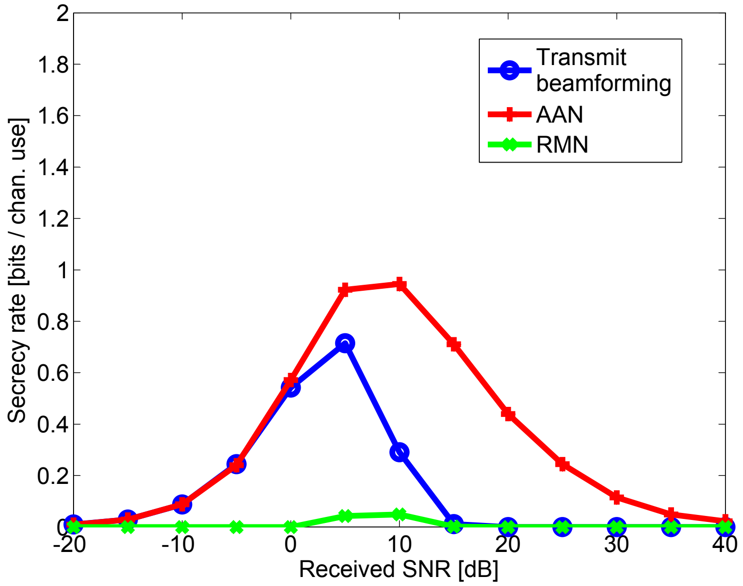


Figure 5.14: The secrecy rate (difference in MI) between the desired receiver and the eavesdropper at 50° for all three methods, as a function of Bob's SNR.

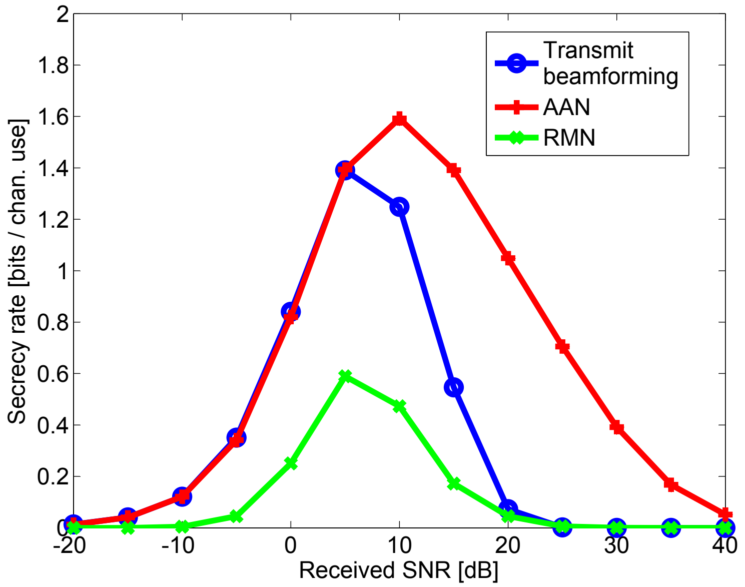


Figure 5.15: The secrecy rate (difference in MI) between the desired receiver and the eavesdropper at 60° for all three methods, as a function of Bob's SNR.

5.3 Power Efficiency

Because of the limitations of using phase shifters instead of full amplitude and phase control of weights, this experiment is not a good indicator of the relative power efficiency of RMN and AAN in comparison to transmit beamforming. This is why all secrecy rate results were presented as a function of SNR rather than using the received power. The transmit power going into the phase shifters was the same for transmit beamforming, AAN, and RMN. The power received at the desired receiver was 0.3 dB lower when transmitting AAN than transmit beamforming. Adding artificial noise should not change the signal in the desired transmit direction, which is why these two received powers are very close. The received power when using RMN was 2.5 dB higher than transmit beamforming. This is due to the use of different pairs of elements rather than only using the two broadside elements, as well as different calculated phase shifts that direct the beam toward the desired receiver. As mentioned earlier, due to errors in the actual phase shifts, the main beam for transmit beamforming and AAN is closer to 30° rather than the desired receiver at 40°. RMN may appear more power efficient, but with ideal phase shifters and perfect measurement of the antenna radiation patterns, transmit beamforming would be as power efficient as RMN. AAN would ideally be half as power efficient because two of the four phase shifters were used for artificial noise. But because these phase shifters were turned off during transmit beamforming and RMN, the power going into them was wasted. This is why AAN and transmit beamforming yielded the same received power to the desired receiver with the same input power.

5.4 Conclusion

Even with the limited capabilities of the experimental setup, AAN and RMN showed increased secrecy versus protecting unwanted reception by transmit beamforming alone. When viewed in the context of eavesdropper SNR in Figure 5.10, both RMN and AAN were more difficult for any eavesdroppers to decode for a given SNR. This suggests a combination of the two methods might perform even better than either alone. This is explored in Chapter 6.

CHAPTER 6

COMBINED RMN AND AAN ENCRYPTION

The two main physical encryption techniques described here, AAN and RMN, are complementary. AAN involves forming a constant fixed beam to the desired receiver while randomly steering another beam that has a null to the desired receiver. RMN involves maintaining constant power to the desired receiver while randomly altering its antenna patterns among a finite number of states. Thus, the communication to the desired receiver is accomplished in the same way by both methods while the randomness in the channels seen by eavesdroppers is accomplished by different means. An array of reconfigurable elements can accomplish both AAN and RMN at the same time. Methods and simulation results are given in this chapter.

6.1 Simulation Setup

The transmit array is a four-element array of beam-steering reconfigurable elements shown in Figure 4.7. Two channel environments are tested: the indoor apartment environment shown in Figure 4.1 and the urban Rosslyn environment shown in Figure 4.4. The power allocation between signal and artificial noise power for AAN was varied in the same way as in Chapter 4. Simulations were run with α equal to 1/11, 1/2, and 10/11, which corresponds to power ratios between artificial noise and signal of 10 dB, 0 dB, and -10 dB, respectively. The same four low SNR and four medium SNR receivers for each environment were used as the desired receivers.

For each symbol transmitted, random antenna radiation patterns were chosen by the method specified for RMN in Section 3.2. Then, with the channel to the desired receiver determined by the choice of antenna patterns, AAN is generated by the method given in Section 2.1. For each antenna pattern configuration, 1,000 artificial noise symbols are generated and the overall artificial noise power is determined by the averaging method discussed in Section 2.5. This artificial noise power is added to the AWGN power, which always is equal to one for all simulations. The final MI between the transmitter and an eavesdropper is then calculated using this new noise power in Equation (2.61).

The performance of this combined AANRMN scheme was compared to transmit beamforming (TBF), AAN, and RMN. The transmit arrays for TBF, AAN, and RMN also used the beam-steering element patterns shown in Figure 4.7. For TBF and AAN, these antenna patterns were steered in the best possible manner toward the desired receiver.

6.2 Simulation Results

The results of simulations for both channel environments are shown in Figures 6.1 and 6.2. The percentage of eavesdroppers able to decode the message is again defined as the percentage of eavesdroppers that had MIs greater than the MI to the desired receiver, for which the transmit power was adjusted so this MI was 3.7 bits. The average transmit power in decibels is relative to the transmit power of the fixed array when implementing ordinary transmit beamforming.

The percent of eavesdroppers decoding the packets from TBF and AAN transmitters falls on the same curves as a function of artificial noise. Initially, the marginal benefits of adding artificial noise are great, as the percent of eavesdroppers decoding falls dramatically between TBF, which has no artificial noise, and AAN with artificial noise with only -10 dB of the signal power. As more artificial noise is added, the number of eavesdroppers able to decode becomes close to zero in all cases, although a lot of noise power is required.

The RMN encryption scheme tended to be less secure for the same transmit power than AAN in most cases, although it offered more security in the case of the indoor channel to the medium SNR receivers. The reason it was less power efficient in the urban channel was that transmission through walls was not allowed in the ray tracing calculation, so it was more important to adjust the reconfigurable elements to their optimal beamsteering as steering them away from the optimal directions required much higher compensatory

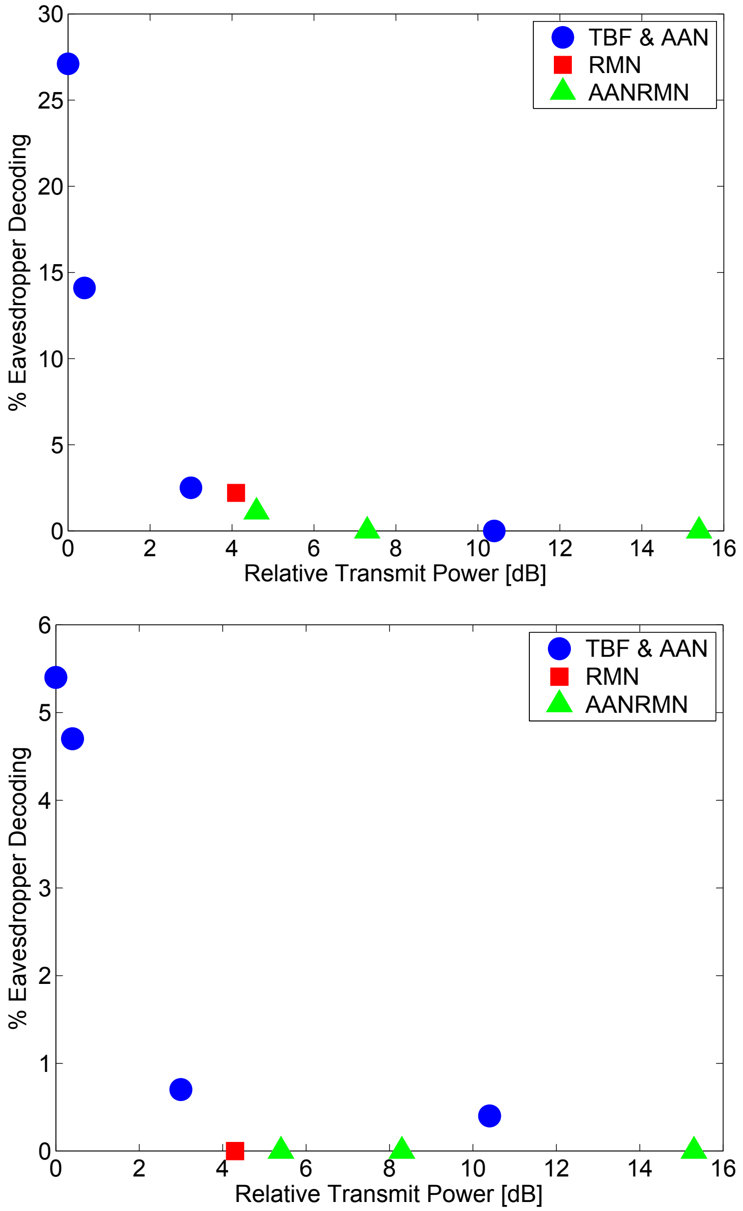


Figure 6.1: Comparison of the secrecy vs. transmit power tradeoff for various encryption schemes: AAN, RMN, and combined AANRMN. All transmitters use the ideal beam-steering antenna elements of Figure 4.6 (with AAN and TBF patterns fixed and steered to the desired receiver). Simulations are of the indoor environment to low SNR desired receivers (top) and medium SNR desired receivers (bottom).

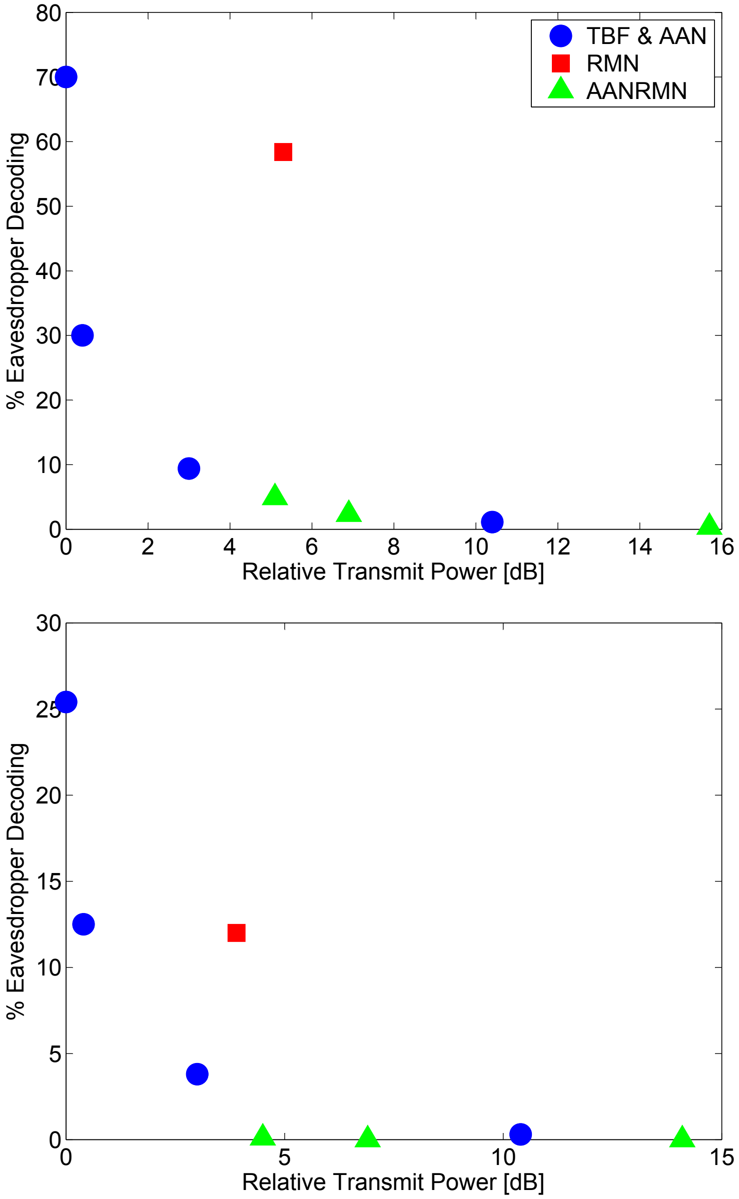


Figure 6.2: Comparison of the secrecy vs. transmit power tradeoff for various encryption schemes for the outdoor urban channel for low SNR desired receivers (top) and medium SNR receivers (bottom).

transmit power. Similarly in the low SNR indoor case, fixing the antenna patterns in the optimal direction and generating artificial noise was the more power-efficient scheme. Only when the SNRs to the desired receivers were medium relative to the SNRs of potential eavesdroppers did it make sense to distort the signal by reconfiguring antenna patterns.

In the AANRMN cases, with enough artificial noise, none of the eavesdroppers were able to decode the packets. This is significant because some eavesdroppers had SNRs 25 dB greater than Bob's receive SNR in the indoor environment and over 100 dB greater in the outdoor environment, even with the transmitter array optimally desired toward Bob. It did not take nearly this much artificial noise to cause the eavesdroppers to have worse channels because the transmitted artificial noise and signal are sent through the same strong channel to Eve.

The effect of using reconfigurable antennas in the transmit array as opposed to fixed antennas can also be seen in Figures 6.1 and 6.2. AAN alone is able to reduce the amount of eavesdroppers receiving to about 1% or less in all environments and receiver sets. However, AANRMN achieves the same secrecy at lower transmit power. From the figures, AANRMN achieves this level of eavesdropper reception with about 5 dB less transmit power. This is because some of the distortion of the signal is caused by pattern reconfiguration rather than artificial noise transmission.

6.3 Conclusion

The data in Figures 6.1 and 6.2 show it is advantageous to combine additive artificial noise with multiplicative noise induced by changing antenna element patterns. The combined noise causes much lower MIs between the transmitter and eavesdroppers than using either method alone, and both methods can be used at the same time without any additional calculation than what is required for both methods separately. In addition, the required transmit power for a given fraction of eavesdroppers thwarted was almost always less than either AAN or RMN alone.

CHAPTER 7

CONCLUSION

7.1 Summary

Additive artificial noise (AAN) has been experimentally tested and its performance has been compared to other schemes using mutual information (MI). An entirely different physical-layer encryption scheme called reconfigurable multiplicative noise (RMN) that uses pattern-reconfigurable antennas has been described. The two encryption schemes were then combined and the secrecy and power efficiencies of all schemes were compared in indoor and outdoor wireless channel simulations.

When adjusted for SNR, both AAN and RMN resulted in lower MI for all eavesdroppers than using transmit beamforming (TBF) in the experimental conditions described in Chapter 5. AAN has the advantages of using fixed antennas and was slightly more secure overall due to transmitting artificial noise. However, broadcasting artificial noise could be harmful if there are friendly receivers in the area who also would be swamped by the noise. If there are multiple friendly receivers, the AAN transmitter should keep track of all of their channels and a more complicated calculation must be done in order to broadcast noise only in the common nullspace of all friendly receivers' channels.

RMN can be more power efficient because it does not spend transmit power on artificial noise, but it requires pattern-reconfigurable antennas and its security performance cannot be incrementally adjusted by adding or subtracting artificial noise. Additionally, RMN's power efficiency is contingent on how well the antenna patterns point in the direction of the desired receiver. If the antenna patterns are steered away from the desired receiver, then more transmit power is needed in order to keep the same receive SNR.

In simulations, AAN and RMN combined (AANRMN) was able to prevent all eavesdroppers in indoor and outdoor environments from decoding a message, even though some eavesdroppers had significantly better channels to the transmitter than the desired receiver's channel to the transmitter. This means if the transmitter sends a message that is coded very near the capacity of its channel to the desired receiver, it is highly unlikely that any eavesdropper could decode a message because it would be impossible for the eavesdropper to decode packets sent at a rate higher than its channel capacity. All techniques are before any mathematical encryption and thus do not incur the key-sharing overheads that lower the data rate.

7.2 Impact of Current Work

This work advances the state of the art in physical-layer encryption in several ways:

- The AAN method proposed several years ago achieves the secrecy capacity bound derived in [16] for multiple transmit elements and single element eavesdroppers and desired receiver. But previously, there existed no method to constrain peak power when transmitting AAN. This work proposed modifications to AAN to constrain peak power with a user-specified probabilistic rate of success. Because random Gaussian noise is part of the transmitter weights, there is always some chance that the total transmit power will exceed a peak power bound, in which case the transmitter simply discards those weights and recalculates new ones.

- The AAN method in the literature is also computationally intensive, as it requires either repeated matrix inversions of the channel or a singular value decomposition of the channel matrix. A new method for fixed transmit elements called multiplicative artificial noise (MAN) was proposed and shown to perform comparably to AAN in simulated channels.

- Similar to MAN but using reconfigurable transmit elements, the reconfigurable multiplicative noise (RMN) encryption uses the same computationally easy channel inversion calculation rather than a full channel matrix inversion. RMN adds increased secrecy because each transmit element also randomly changes its radiation pattern at the symbol rate. This was shown in experiment and simulations to perform slightly worse than AAN overall. RMN's benefit over AAN, besides computational simplicity, is that it was shown in simulations to be more robust to errors in the channel estimate to the desired receiver.

- Combining AAN and RMN into a single transmit encryption technique (called AANRMN) allowed a high level of secrecy while using less transmit power and thus lowering the noise floor for other friendly receivers in the vicinity of the transmitter. In simulations and when using enough artificial noise power, AANRMN was able to force all eavesdroppers to a lower mutual information than the desired receiver, even though the locations of eavesdroppers were unknown to the transmitter and some eavesdroppers had much stronger channels than the desired receiver due to their proximity to the transmitter.

- A method for comparing encryption techniques using mutual information was devised. Previous work ([28, 29, 30]) with spatially varying signals assumed any constellation in which at least one point was sufficiently distorted would be undecodable, but this is incorrect. While [16] derives the secrecy rate for AAN, many other techniques such as MAN and RMN have no possible closed-form expression for the secrecy rate. But the mutual information between the transmit array and all receivers can be calculated from the received constellation regardless of the technique. Hence, any physical-layer encryption technique can be evaluated in this manner, although it may require averaging over receivers and eavesdroppers with many different channel realizations.

- Simplified forms of AAN and RMN are generated experimentally for the first time and their relative secrecy rates compared. AAN was slightly more secure than RMN in this scenario, and both were more secure than transmit beamforming.

7.3 Future Work

Before the benefits of RMN or combined AANRMN can be realized, pattern-reconfigurable antennas must be designed that are more easily fabricated. Current designs that have switches connected to the radiating elements use bias networks that must be electromagnetically isolated lest they also radiate. Because of the difficulty of fabrication, antennas hardwired to one radiation pattern were used in the experiment in the work done here. In order to become widely adopted, pattern-reconfigurable antennas should be designed that are easier to mass-produce and have a large tolerance for fabrication error, while not being too complex or expensive so that a phased-array becomes a better option. One option is to use electrically steerable passive array radiators (ESPARs) as the radiating elements, since these have a longer history of being reliably produced. However, the inter-element coupling of ESPARs may be harder to control and large inter-element is spacing required.

One important tradeoff of any artificial noise scheme is between secrecy and an increased noise floor for the entire wireless network. If many transmitters are radiating artificial noise, the result will be that the noise floor is raised for all receivers, whether they are eavesdroppers or attempting to communicate with another party entirely. Spread-spectrum networks suffer a similar problem. Because transmitted signals are spread over the entire bandwidth, they add to the noise floor of all receivers. However, spread-spectrum offers similar secrecy in that it is difficult to decode a spread-spectrum signal without knowledge of the spreading sequence. The secrecy and noise power of AAN should be compared to spread-spectrum signaling methods. It is also possible to combine the spread-spectrum signaling with artificial noise. This work used QPSK or 16 QAM modulation as the signaling type but a spread-spectrum signal could have carried the message, and artificial noise could be added without changing the algorithms described here.

Finally, this work has been concerned with eavesdroppers and desired receivers using a single antenna element. Theoretical bounds have been derived in [17] for collaborating eavesdroppers or those with multiple antennas, but implementable encryption techniques that take multiple receive antennas into account have not yet been developed. In fact, when using multiple receive antennas for the desired receiver and eavesdropper, it was shown that the secrecy rate of AAN is significantly lower than the secrecy capacity bound derived in [17]. Future methods could look to relax the constraint that no amount of artificial noise should be transmitted to the desired receiver. If the desired receiver has multiple antennas, then it may be able to filter out some amount of artificial noise. Thus, new physical-layer encryption techniques should be developed for multiple receive and eavesdropper antenna elements.

APPENDIX A

DIRECTIONAL MODULATION

This appendix presents a physical layer encryption method called directional modulation (DM) that is a subset of additive artificial noise (AAN). Sections A.1 and A.2 are adapted from [35] and Section A.3 is adapted from [36]. DM is similar to AAN because the transmitted signal constellation is distorted to any eavesdropper with a different channel than the desired receiver, while the desired receiver sees a normal constellation. However, while AAN sends a new randomly generated constellation point each symbol time to an eavesdropper, DM switches between a fixed number of constellation points. The secrecy comes from the fact that a subset of these constellation points tend to be very close together, making it difficult for an eavesdropper to distinguish among them in the presence of external noise. The calculation of array weights for DM uses a genetic algorithm instead of the closed-form expressions used in AAN for putting noise in the nullspace of the desired receiver. This calculation is explained first, followed by simulated and measured results.

A.1 Array Weight Calculation via a Genetic Algorithm

Figure A.1 shows a simplified block diagram of a traditional phased array and an array using DM. In the traditional array, the digital modulation is produced in baseband, mixed with the carrier frequency, and sent out through progressively phased elements. In the case of DM, the phase shifters actually create the modulation by changing phase of a single tone. The amplitude or phase shifts constituting a digital modulation are created by the phase shifters, rather than a baseband block, which is why the signal is directional and appears distorted in undesired directions.

An efficient optimization algorithm for DM to determine the phase shifts

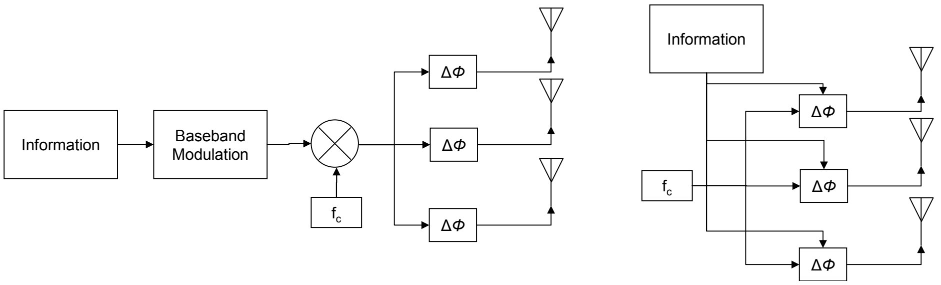


Figure A.1: Traditional array transmitter (left) and DM transmitter (right).

necessary to implement a digital modulation is presented. A GA was chosen for this application because GAs have been used numerous times for array pattern synthesis, including nulling [54] and sidelobe reduction [55, 56]. The optimization cost function presented in Section A.1.2 is not convex, and there exists no method to obtain a globally optimal solution. A GA can give a good solution quickly, albeit saying nothing about optimality. In this section, we assemble basic beamforming equations in a format that allows direct use by GAs. This formulation also helps provide a clear linkage between radiation pattern synthesis and digital symbol synthesis. From [57], we can express the radiation pattern of an arbitrarily-spaced three-dimensional array of N elements at time t as

$$E(\theta, \phi, t) = \sum_{n=1}^{N} f_n(\theta, \phi) e^{j\mathbf{k}\cdot\mathbf{r}_n} s_n(t) \tag{A.1}$$

where $f_n(\theta, \phi)$ is the active element pattern of element n, and

$$\mathbf{k} \cdot \mathbf{r}_n = \frac{2\pi}{\lambda} \left(x_n \sin(\theta) \cos(\phi) + y_n \sin(\theta) \sin(\phi) + z_n \cos(\theta) \right) \tag{A.2}$$

where (x_n, y_n, z_n) is the location of element n and λ is the wavelength at the carrier frequency. The term $s_n(t)$ is the excitation of element n at time t; it is a continuous wave (CW) signal phase-shifted appropriately for each element and whose phase changes at the symbol rate. How the active element patterns are found is described next.

A.1.1 Active Element Patterns

The antenna array measured for all calculations in this appendix is a four-element linear array of microstrip patches, shown in Figure A.2. The operating frequency is 7 GHz, and all elements are spaced one-half of a wavelength apart. At the operating frequency, the return loss of all elements is greater than 12 dB. All patterns are taken in the azimuthal plane (xy) and E-plane ($\hat{z}$) polarization is used with the plane of the array in the yz plane.

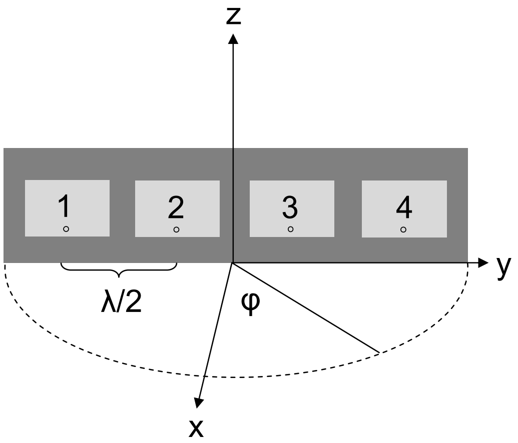


Figure A.2: Four-element linear patch array transmitting at 7 GHz.

The active element pattern (or scan element pattern) is the radiation pattern of a single element when it is located in an array [58, 59]. It is different from the isolated element pattern due to mutual coupling between array elements and surface wave loss, and it is necessary to include these effects so that digital modulation magnitudes and phases are precise. One can measure the active element pattern of an element by terminating all other array elements in 50 Ω. Because Maxwell's equations are linear, the total radiation pattern of the array is the superposition of the active element patterns [57]. This is confirmed in Figure A.3, in which the radiation pattern when all elements are uniformly driven is compared to the summation of the four active element patterns, for azimuthal angles (ϕ) from $-90°$ to $+90°$ corresponding to the half plane in front of the array. As expected, there is good agreement, meaning that the active element patterns can be used for precise calculations.

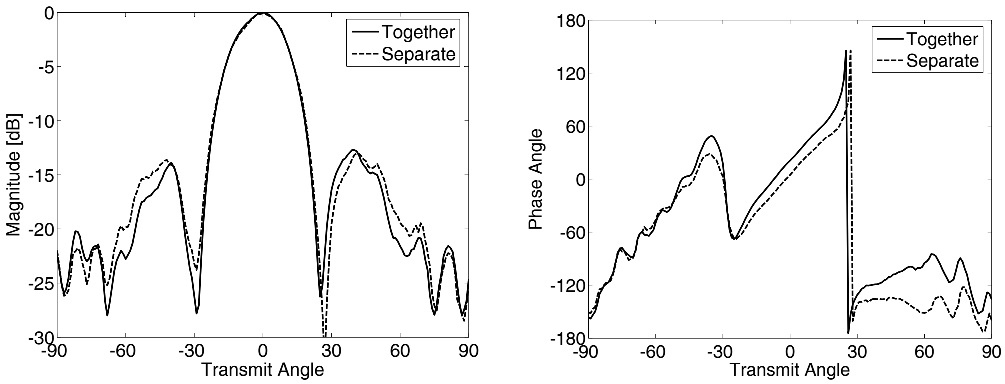


Figure A.3: Normalized magnitude and phase of the measured radiation pattern when all elements are driven (together) and the pattern predicted by the summation of the active element patterns (separate).

A.1.2 GA Optimization for BER

The independent variables in the optimization are the phase shifts at each of the four elements, denoted as γ_i for the i^{th} element. Thus, the excitations are forced have magnitude equal to one by

$$s_i(t) = \exp\left(j\gamma_i(t)\right) \tag{A.3}$$

In the GA, members of the population are sets of four phase angles γ, one for each element. The population size was set to four, with children formed from random crossover of the two best members.

Let L be the set of directions in which low BER is desired, H be the set of directions in which high BER is desired, w_i and w_j be weights chosen based on the importance of the BER in certain directions, and (θ_i, ϕ_i) and (θ_j, ϕ_j) represent transmit directions. The cost function is given as follows:

$$\text{Cost} = \sum_{i \in L} w_i \cdot \text{BER}(\theta_i, \phi_i) - \sum_{j \in H} w_j \cdot \text{BER}(\theta_j, \phi_j) \tag{A.4}$$

The BER is a function of the noise power (assumed to be equal in all directions) and the received constellation, assuming both the desired receivers and eavesdroppers have perfect knowledge of the channel and thus also knowledge of the received constellation diagrams.

How BER is calculated is described next. DM creates arbitrary four-point (4-ary) constellations rather than square QPSK constellations. Because the

BERs of these constellations must be repeatedly calculated as part of the GA, it is desirable to have a closed-form expression of BER. While methods have been found to determine closed-form expressions for arbitrary constellations [60, 61, 62], these methods are complicated and instead a simple bound similar to the nearest-neighbor approximation [39] is used. The nearest-neighbor approximation states that the probability of symbol error can be approximated by the distance of the two closest constellation points

$$P_{\text{error}} = Q\left(\frac{d/2}{\sqrt{N_0/2}}\right) \tag{A.5}$$

where d is the Euclidean distance between the two closest constellation points, $N_0/2$ is the noise power spectral density, and $Q(x)$ is the complementary Gaussian error function. More precisely, d for the constellation transmitted in direction k is computed as:

$$\min_{i,j,i\neq j} |E(\theta_k, \phi_k, t)_i - E(\theta_k, \phi_k, t)_j| \tag{A.6}$$

where $E(\theta_k, \phi_k, t)_i$ is the transmitted radiation pattern in direction k for the constellation symbol i. This assumes there is only one closest point or one nearest neighbor to each point, which is a valid assumption for the 4-ary constellations considered here. Next, the bound can be made more precise by considering the probability of symbol error of each constellation point separately. Let d_i be the minimum Euclidean distance from point i to any other point in that constellation. Assuming all four constellation points are equally likely, the probability of symbol error is given by

$$P_{\text{error}} = \frac{1}{4}\sum_{i=1}^{4} Q\left(\frac{d_i/2}{\sqrt{N_0/2}}\right) \tag{A.7}$$

Finally, by Gray coding, we can approximate the probability of bit error as half the probability of symbol error for a 4-ary constellation [39]. The final expression for a lower bound on BER is given by

$$P_b(\text{error}) = \frac{1}{8}\sum_{i=1}^{4} Q\left(\frac{d_i/2}{\sqrt{N_0/2}}\right) \tag{A.8}$$

This expression was used in the GA to evaluate the cost function in Equation

(A.4). It will be shown in Sections A.2.1 and A.2.2 that this bound closely predicts the simulated BERs.

A.2 Phased Array DM Simulations

Simulations based on the measured element patterns and the phase shifts from the GA are given next. It is shown that DM can achieve a low BER in a narrow beamwidth toward a desired receiver and still enforce a high BER in other directions.

A.2.1 Secure Communication to Broadside

The GA was used to find phase shifts that give a low BER in a 10° beamwidth around broadside and a high BER to all other angles in the half-plane from $-90°$ to $+90°$. The resulting BERs given by the lower bound in Equation (A.8) and by simulation are shown in Figure A.4. In simulations, up to 2×10^8 random bits were transmitted per angle (1° increments) and white Gaussian noise was added to the signal. There is good agreement with the lower bound in (A.8) and simulation.

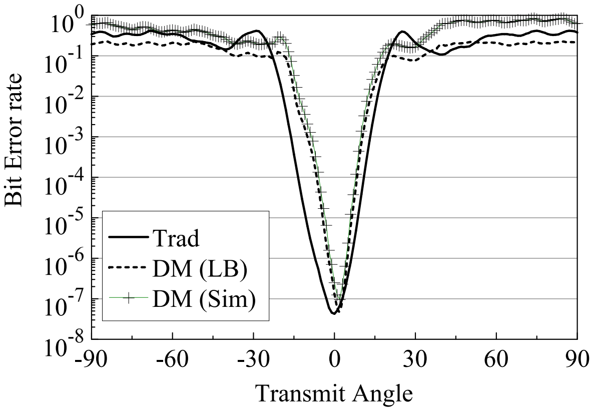


Figure A.4: BER when desired receiver is at broadside for the traditional array (Trad.), the DM array lower bound (LB), and DM simulated BER (sim).

Also shown in Figure A.4 is the BER from a traditional array transmitter phased to broadside. This BER is a function of amplitude of the radiation pattern. The expression for the probability of bit error for a QPSK modulation is given by [63]:

$$P_b(\text{error}) = Q\left(\sqrt{\frac{E_b}{N_0/2}}\right) \tag{A.9}$$

The energy per bit in QPSK, E_b, is equal to half the symbol energy, E_s. E_s is found by taking the square magnitude of the radiation pattern in the direction of interest. The largest magnitude radiation pattern at broadside is produced by the traditional transmitter when all four elements are in phase. This creates a much lower BER at broadside for the traditional array than for the DM array. In order to fairly compare the BER levels in the sidelobe regions, the power of the traditional array was reduced until the BER was the same at broadside as the DM array, while the noise power is kept the same for both transmitters. This means the traditional array achieves the same low BER toward the desired receiver as the DM array, without spending more power than necessary, which would increase sidelobe power as well as mainlobe power. In this manner, the security in the undesired directions can be compared while the arrays have the same performance in the desired direction. The broadside radiation pattern of the traditional transmitter is shown in Figure A.5, along with radiation patterns created by the four sets of phases of the DM transmitter.

The traditional array and the DM array have the same order of magnitude of BER in the directions away from broadside, but the DM array has a narrower beamwidth in which the BER becomes very low. Thus, at some angles such as ±10°, the BER of the DM array is several orders of magnitude higher than the BER of the traditional transmitter. While a uniformly fed array has the narrowest possible pattern beamwidth, the DM transmitter has a narrower BER beamwidth because it has greater capability to alter constellations.

The spatial variability of DM is evident when comparing received constellations at $-50°$. Both arrays achieve about the same high BER (0.2) in this direction. But the signal magnitude of the traditional array in this direction is clearly lower than several of the DM constellation point magnitudes by as much as 13 dB, as can be seen in Figure A.5. Yet, even with this larger signal power, the DM array still manages to keep the BER high. The reason for this can be seen from Figure A.6. The two DM points that have large

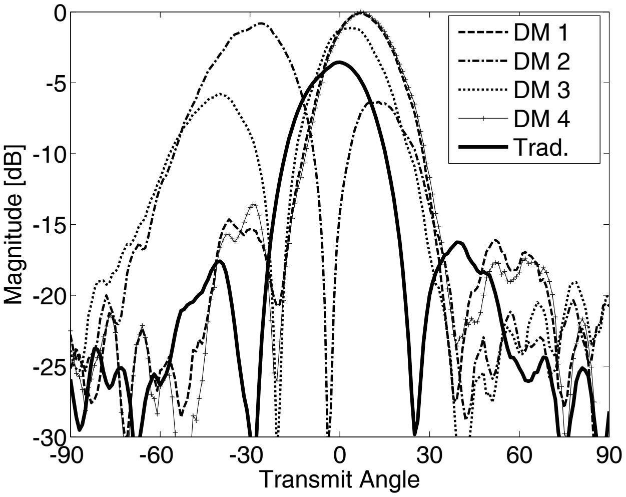


Figure A.5: Normalized radiation patterns when phased to give low BER toward broadside and high BER everywhere else. DM 1 through DM 4 are the radiation patterns when the four different DM constellation points are sent. Also shown is the relative magnitude of the radiation pattern of the traditional array (all elements in-phase) to achieve the same BER toward broadside.

magnitudes also are very close together in phase, while the other two points have very small magnitudes. Thus, it is difficult for a receiver to distinguish between either pair of points in the presence of noise. The traditional array is able to achieve a low signal magnitude in this direction, but the constellation is still separated as much as possible given that amplitude, providing an opportunity for undesired eavesdropping.

A.2.2 Secure Communication to $-45°$

DM also has advantages over a traditional array when steered away from broadside. Figure A.7 shows the radiation patterns for both transmitters when the desired receiver is at $-45°$ from broadside. The traditional array faces the effects of broadening of the mainlobe and higher sidelobe levels when it is steered away from broadside.

These effects manifest themselves in the BER of the traditional transmitter, shown in Figure A.8. Compared to the DM array, the traditional array has a wider BER beamwidth around the desired direction and the sidelobes cause regions of lower BER in undesired directions. The DM BER has the

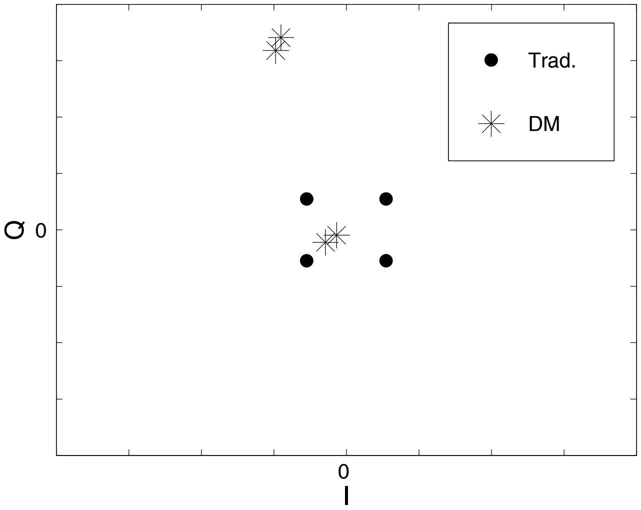


Figure A.6: Constellation diagrams at $-50°$ from broadside for the traditional array and the DM array. While the magnitude of the traditional array's constellation is decreased, it is still able to be decoded, while the DM constellation is, in essence, scrambled.

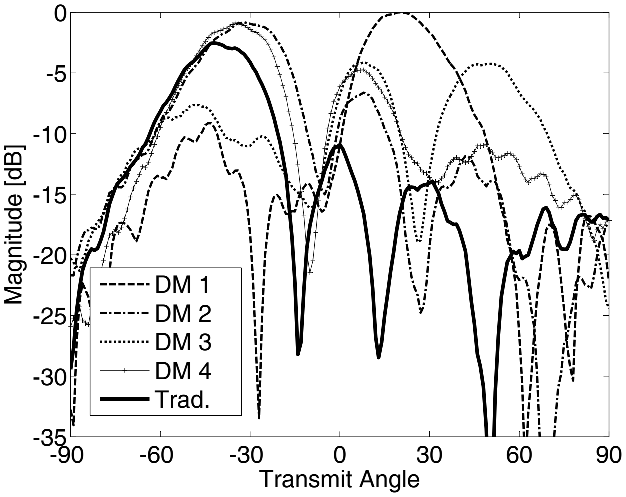


Figure A.7: Normalized radiation patterns when phased to give low BER toward $-45°$ and high BER everywhere else. DM 1 through DM 4 are the resulting radiation patterns when the four different DM constellation points are sent. Also shown is the relative magnitude of the radiation pattern of the traditional array (phased to $-45°$) to achieve the same BER toward $-45°$.

same narrow beamwidth over which lower BER is transmitted as in Figure A.4. It also smooths out sidelobes, displaying a relatively constant high BER in the undesired transmission directions.

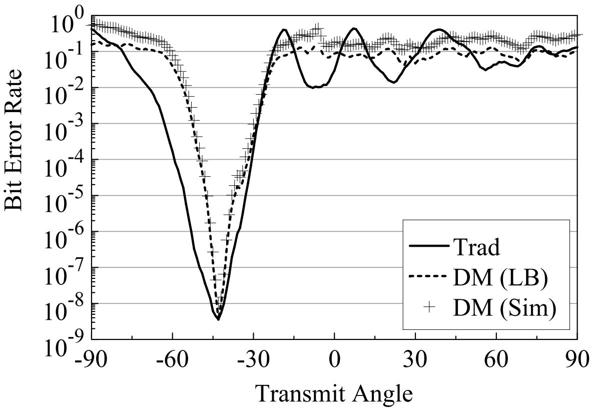


Figure A.8: BER when desired receiver is at −45° shown for traditional array (Trad.), the lower bound of the DM array (LB) and DM simulated BER (Sim).

A.3 Experimental Results

To measure the performance of DM versus baseband modulation, three experiments are conducted for each transmitter where a desired receiver is located in a LOS channel at broadside, −30°, and +20°, relative to the transmit array. Eavesdropping receivers may be located in any other direction besides that of the desired receiver, and their locations are not known to the transmitter. The transmit array is the microstrip patch antenna array described in Section A.1.1. The receive antenna is a standard gain horn oriented to receive the dominant polarization of the microstrip patch array.

A.3.1 Traditional Baseband Array Setup

The experimental procedure of the traditional phased array transmitter will be explained first. A block diagram of the entire arrangement is shown in Figure A.9. The first step for the traditional phased array is to calculate the necessary phase shifts to steer toward the three receiver directions. The calculated phase shifts are stored in a computer located inside an anechoic chamber along with the transmit and receive antennas, and four five-bit Miteq digital phase shifters [64]. The phase shifters are actually six-bit, but the number of analog outputs from the computer limits the amount of control bits to five. The phase shifts were calculated assuming isotropic element patterns. Thus, some beamforming error is introduced because the microstrip patch patterns are not entirely constant over the angles of interest, while other error is due to the quantization of the phase shifts. Still, the measured patterns when phased to the three desired directions all have mainlobes of approximately the same magnitude, shown in Figure A.10. Since the mainlobes steered off of broadside are not significantly lower than the mainlobe when all phase shifters are set to 0°, this suggests the phasing is close to ideal. One other source of error is the presence of a computer inside the anechoic chamber, which slightly distorts the patterns, causing one of the sidelobes in the broadside pattern in Figure A.10 to be about 5 dB higher than the other.

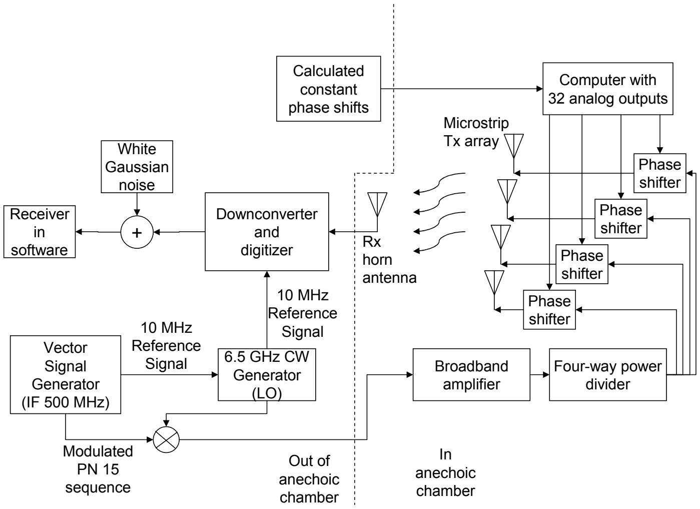


Figure A.9: Experimental configuration of the traditional phased array transmitter and receiver.

The baseband digital modulation is generated by an Agilent E4438C vector signal generator. A pseudorandom binary sequence (PN15) is sent by the traditional and DM transmitters [65]. These information bits are used to create Gray-coded QPSK modulation with a bit rate of 200 kbps that is passed through a root-raised-cosine filter. The vector signal generator upconverts the modulation to an intermediate frequency (IF) of 500 MHz, and it is then externally mixed to 7 GHz. The RF signal is amplified by a broadband amplifier with 21 dB gain and then passes through a four-way power divider before passing through the phase shifters and finally, the antenna array.

After reception by a standard gain horn, root-raised-cosine bandpass filtering, downconversion to baseband, and digital sampling are accomplished by an Agilent E4440A spectrum analyzer. Artificial AWGN noise is added

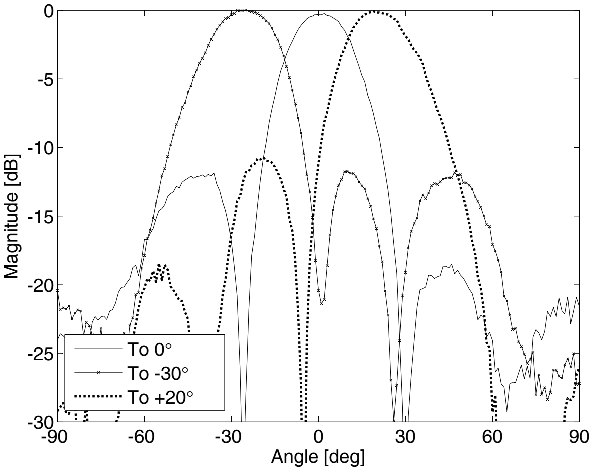


Figure A.10: Normalized measured patterns when the transmit array is steered to broadside, −30° from broadside, and +20° from broadside.

to achieve a desired SNR. This noise is complex because the filter has been bandpass filtered and downconverted to baseband. The signal plus noise is demodulated in Matlab [66]. A 10 MHz reference signal between the local oscillator (LO) and the spectrum analyzer makes a phase lock loop (PLL) unnecessary.

A.3.2 Directional Modulation Array Setup

The arrangement of the DM transmitter, shown in Figure A.11, differs from the traditional transmitter because the modulation is now synthesized in the RF portion. The signal sent into the phase shifters is a sinusoid at the array operating frequency. The signal leaving the phase shifters is modulated due to the fast, repeated changes of the phase shifters, and these modulated signals are not simply delayed copies of each other. Rather, the signals leaving the phase shifters are modulated such that they combine in the far-field to create the desired 4-ary modulation only in the desired direction [35].

Instead of calculating a single set of phase shifts, a set is calculated for each digital symbol (in this case, four). This requires knowledge of the active element patterns, which are measured beforehand. The GA from Section A.1.2 calculates the four sets of phase shifts based on the active element patterns. The cost function has been altered to:

$$\text{Cost} = \frac{\text{BER(desired direction)}}{\min(\text{BER(undesired directions)})} \tag{A.10}$$

because then weights on the BER for each direction do not have to be assigned, as they did in (A.4), eliminating one source of uncertainty about the design.

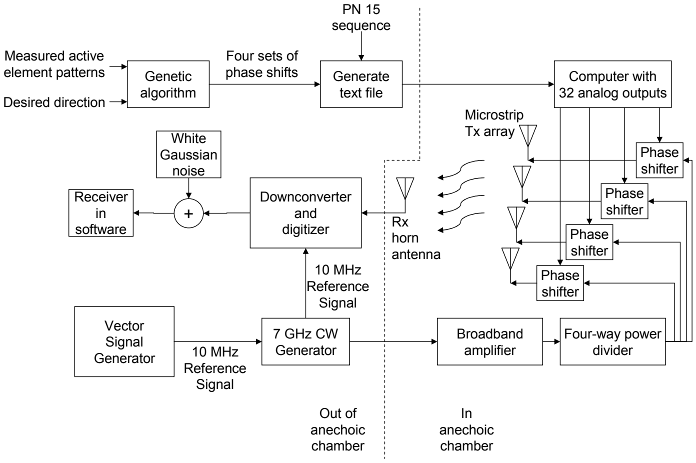


Figure A.11: Experimental configuration of the traditional phased array transmitter and receiver.

There is a “don’t care” region of 5° on either side of the desired direction that is not part of the “undesired directions” in Equation (A.10) because it is a transition region from low to high BERs. The solutions from the GA are also restricted to those that are possible to be produced by the quantized five-bit phase shifters. In order to increase accuracy, the actual phase shifts of the phase shifters were measured and used in the GA. For example, switching the most significant bit in one of the phase shifters produces a 175.3° shift instead of 180°. As a final step in the GA, the sets of phase shifts were assigned to the four symbols based on Gray coding. Table A.1 shows the set of phase shifts used for communication toward broadside.

After the phase shifts are calculated, they are used to construct a text file that governs the real-time switching of the phase shifters. For each symbol consisting of two bits of the pseudorandom binary sequence, control voltages are recorded to produce the corresponding phase shifts for that symbol. Two periods of the binary sequence (32767 symbols) are loaded into a computer containing analog control voltages for the five bits of each phase shifter. The

Table A.1: Set of phase shifts for DM to produce four symbols when the desired receiver is at broadside from the transmit array.

Symbol	Elem. 1	Elem. 2	Elem. 3	Elem. 4
“00”	−143°	−146°	−145°	86°
“01”	−79°	−91°	−74°	−77°
“10”	96°	94°	121°	102°
“11”	42°	−44°	−44°	78°

computer repeatedly reads through the entire sequence changing the phase shift control bits at a rate of 100k Symbols/sec, yielding a bit rate of 200 kbps.

The receiver for DM is nearly the same as the receiver for traditional QPSK modulation. A normal bandpass filter is used instead of a root-raised-cosine filter, because no pulse shaping is done on transmit. The transmitted CW signal still shares a common reference with the downconverter in the receiver, so a phase lock loop is not needed. However, the symbol timing in the DM transmitter is now regulated by the computer controlling the phase shifters, which does not share a common reference with the receiver's sampling clock. Therefore, the received signal is oversampled by a factor of four above the symbol rate and a delay lock loop is implemented to determine the best sampling points.

The bit rate is limited by the speed of the computer producing the analog outputs, since it must produce outputs for twenty control bits each time two bits are transmitted. The switching speed of the phase shifters is actually much faster, on the order of nanoseconds [64]. The transient effects of switching a phase shifter are shown in Figure A.12. Here, a single phase shifter is connected between a signal generator operating at 7 GHz and the receiver by a wire. The most significant bit (0° to 180°) is repeatedly changed at a rate of 100 kHz. The receiver then downconverts the signal and creates complex baseband samples. Ten periods of switching (100 μs) are shown in Figure A.12. It takes about half of the symbol period for the phase shifter to transition, and therefore oversampling by a factor of four guarantees that at least one sample should occur when the transmitted symbol has reached steady state. The discontinuous parts of the curves are likely due to a disallowed bias voltage. When the bias voltage transitions between 0 V and −5 V, there is a point around −2.5 V where both the 0° and 180° modes in the phase shifter are off. This point in the middle of the two bias voltages is what we call the disallowed bias voltage. At this point, the phase shifter's insertion loss increases by about 20 dB, suppressing the signal.

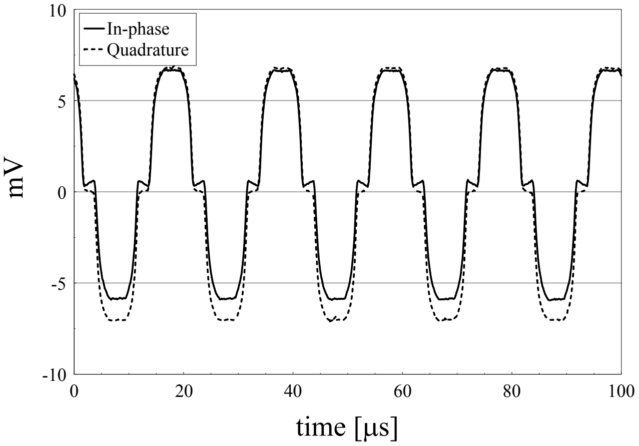


Figure A.12: Measured downconverted output of a phase shifter fed with a 7 GHz CW signal and switched between 0° to 180° at a rate of 100 kHz.

A.3.3 BER Measurement Results from DM and QPSK Signals

In the anechoic chamber, the antenna array for both transmitters was rotated from $-50°$ to $+50°$ while the receiver horn antenna was stationary, to simulate receivers at these directions. Between 1.9×10^6 and 2.0×10^6 bits were sent at each direction in 10° increments and AWGN was added with a noise power of -52 dBm over the frequencies of interest to achieve an SNR of 12 dB in the desired direction. In comparison, the received signals have received power less than -40 dBm. The input power for both transmitters was -7.5 dBm, split equally to each antenna.

Figure A.13(a) shows the BERs of a desired receiver at broadside and other eavesdropping receivers from $-50°$ to $+50°$. Also shown are predicted BER curves based on measured radiation patterns. The predicted BER for the DM transmitter is a lower bound calculated from the GA using the active element patterns [35]. The predicted BER for the traditional transmitter is calculated using the measured pattern data from Figure A.10. The relation between the radiation pattern power and BER for QPSK is given in [35]. The predicted BER for the traditional transmitter agrees well with the measured BER, and the measured BER of the DM transmitter is always slightly above its calculated lower bound. The close agreement between BERs estimated from radiation patterns and the BERs measured from transmitting a digital modulation is important because it means performance can be accurately assessed when designing a DM transmitter (for example, using the GA in [35], given measured or simulated radiation patterns).

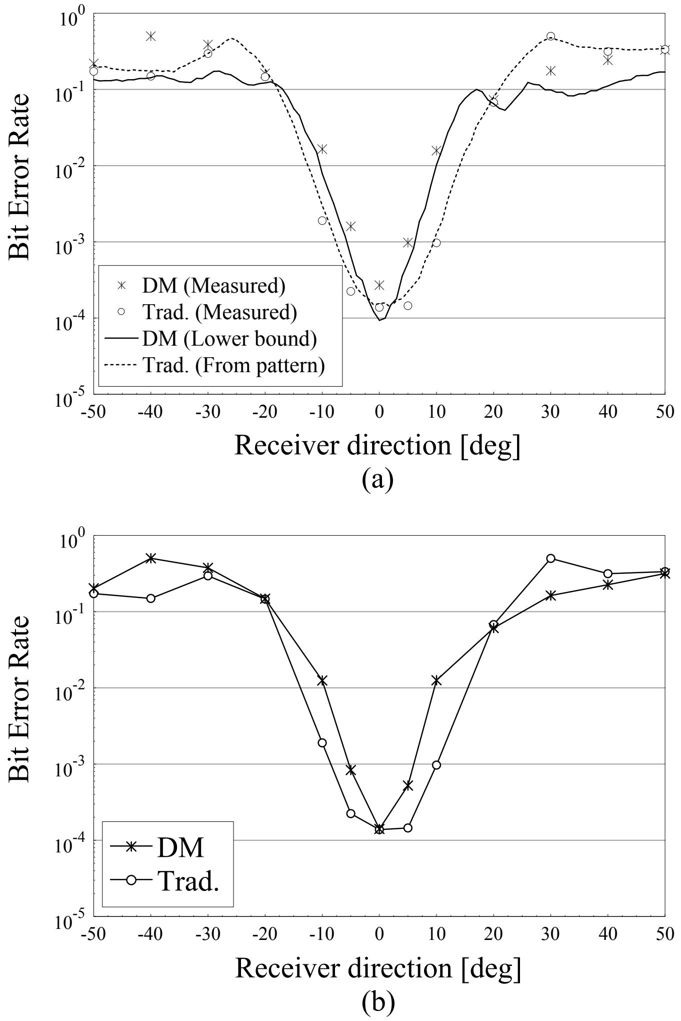


Figure A.13: (a): Measured BERs when both transmitters are directed to broadside. Also shown is the predicted BER of the traditional transmitter based on the measured radiation pattern and the predicted lower bound of the BER of DM based on the measured active element patterns. (b): The noise power in the DM case is decreased by 0.6 dB so that both transmitters achieve the same BER toward the desired receiver at broadside.

One important feature in Figure A.13(a) is that the BER of the traditional transmitter in the desired direction is less than the BER of the DM transmitter. This is to be expected because the phased array maximizes the power in the broadside direction as its sole priority. On the other hand, the DM transmitter trades some of the power transmitted in the desired direction for a narrower region of low BERs and high BERs in all other directions. This also is evident in Figure A.13(a) in the 20° region around broadside where the BER of an eavesdropper is sometimes an order of magnitude lower if the traditional array is transmitting compared to the DM array.

However, in order to fairly compare the narrowness of the BER regions, the BER in the direction of the desired receiver should be equal for both the DM and traditional transmitters. In the case of the desired receiver at broadside, this is accomplished by raising the signal-to-noise ratio (SNR) of the DM transmitter 0.6 dB (by lowering the added noise power after signal reception), which lowers the BER in all directions. This new BER curve is shown in Figure A.13(b) along with the same measured BERs of the traditional array from Figure A.13(a). The DM transmitter is able to transmit a low BER in a narrower region than the traditional transmitter, confirming the results first calculated in [35].

The reason the DM transmitter produces a narrower low BER region can be found from the received power and the received constellations. Figure A.14 shows the average received symbol power calculated from the radiation pattern of the traditional transmitter and the active element patterns of the DM transmitter. This received symbol power was used to calculate the predicted BER curves in Figure A.13(a). Because all constellation points have the same magnitude in the traditional array with QPSK, the average symbol power equals the instantaneous symbol power. On the other hand, the DM array creates arbitrary constellations with different power for different symbols, so average symbol power is used to compare the two methods.

Toward the desired receiver at broadside, the two transmitters send about the same power (after increasing the DM transmitter power by 0.6 dB). But off broadside, the DM array tends to send more power than the traditional array. Yet, the measured BERs are either lower for the DM array or about the same as the traditional array. The reason for this can be gleaned from the received constellation. For example, the first 200 received constellation points that would be seen by an eavesdropper at +50° when the DM and traditional transmitters are intending to transmit to 0° is shown in Figure

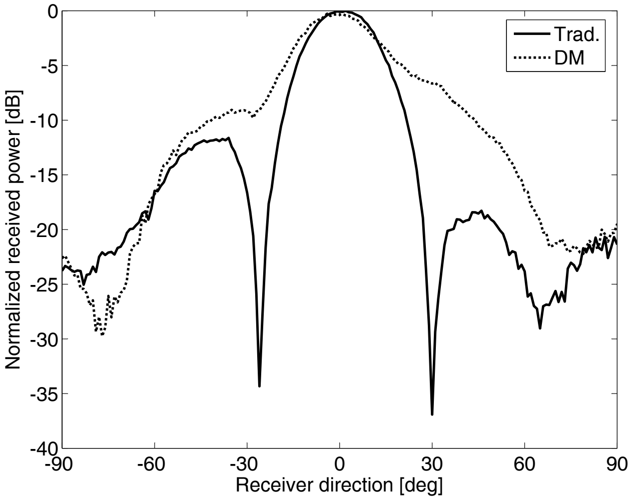


Figure A.14: Average received symbol power by both transmitters when directed toward broadside.

A.15. From Figure A.14, the symbol power calculated from radiation patterns is 7.7 dB higher at +50° for the DM array than the traditional array. The BER measured at +50° was approximately the same for both transmitters (0.20 for the traditional array and 0.16 for the DM array). The reason the DM array achieves this same high BER toward the eavesdropper while transmitting at a higher power level is evident from the constellation diagram. Three of the constellation points are grouped close together, even though they are far from the origin. This indicates three signals with higher power that look approximately the same, and thus are difficult to demodulate correctly. The traditional baseband constellations are the same shape regardless of where the receiver is located, so the only way to increase BER and reduce the chance of demodulation by an eavesdropper is to reduce the power of each symbol, or equivalently reduce the sidelobe level in the radiation pattern.

Figures A.16 and A.17(a) show the predicted and measured BER when the desired receiver is at −30° and +20°, respectively. These figures have the same characteristics as Figure A.13(a). The low BER region is narrower for the DM transmitter than the traditional transmitter, while the BERs are approximately equal between the two transmitters in the sidelobe region. In the case when the desired receiver is at −30°, both transmitters produce the same BER at −30° with equal input power, because the traditional array's maximum of the radiation pattern occurs at −26° rather than −30°.

In the case when the desired receiver is at +20° from array broadside,

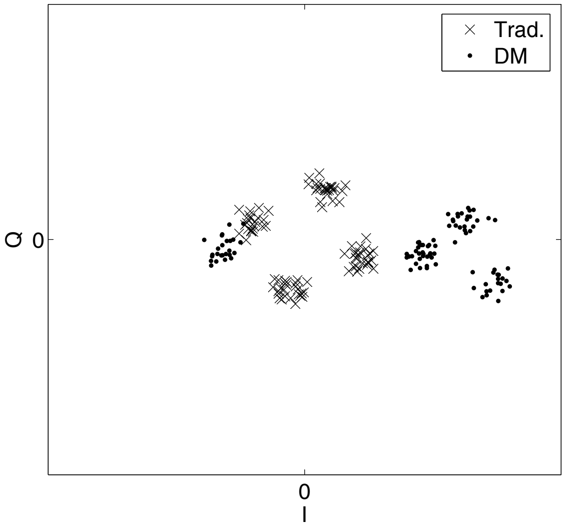


Figure A.15: Received constellations from both transmitters by an eavesdropping receiver at +50° when both transmitters directed toward broadside.

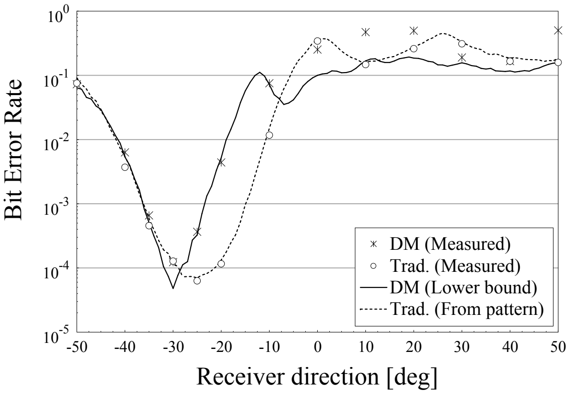
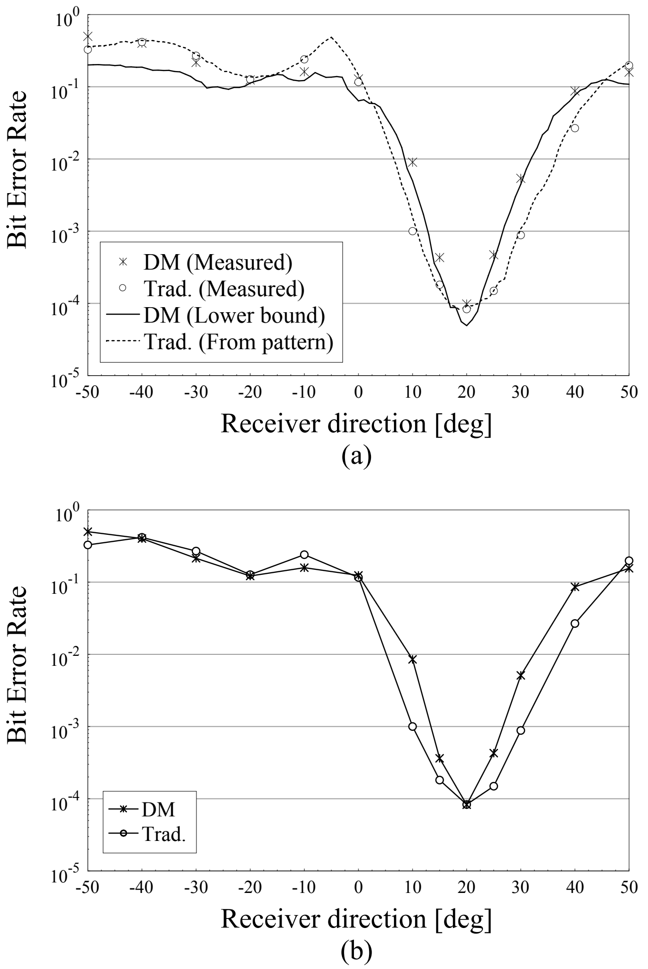


Figure A.16: Measured BERs when both transmitters are directed to −30°. Also shown is the predicted BER of the traditional transmitter based on the measured radiation pattern and the predicted lower bound of the BER of DM based on the measured active element patterns.

the DM transmitter produced the same BER as the traditional transmitter toward +20° when the SNR of the DM transmitter was increased by 0.1 dB, shown in Figure A.17(b). The region of low BER once again is narrower for the DM transmitter.

This section has presented the first experimental demonstration of directional modulation by transmitting data in real time. The measurements indicate that a DM transmitter manipulates a direction-dependent signal so that it is harder to decode in more undesired directions. In addition, the



(a)

(b)

Figure A.17: (a): Measured BERs when both transmitters are directed to +20°. Also shown is the predicted BER of the traditional transmitter based on the measured radiation pattern and the predicted lower bound of the BER of DM based on the measured active element patterns. (b): The noise power in the DM case is decreased by 0.1 dB so that both transmitters achieve the same BER toward the desired receiver at broadside.

DM array sends a signal that will be decoded by the desired receiver with the same low BER (with some small increase in transmit power possibly necessary) with no additional work needed by the receiver.

REFERENCES

[1] E. A. Jorswieck, A. Wolf, and S. Gerbracht, “Secrecy on the physical layer in wireless networks,” *Trends in Telecommunications Technologies*, pp. 413–435, 2010.

[2] C. E. Shannon, “Communication theory of secrecy systems,” *Bell Sys. Tech. Journ.*, vol. 28, no. 4, pp. 656–715, 1949.

[3] W. Diffie and M. E. Hellman, “New directions in cryptography,” *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[4] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[5] A. D. Wyner, “The wire-tap channel,” *Bell Sys. Tech. Journ.*, vol. 54, pp. 1355–1387, 1975.

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

[7] A. Mukherjee, S. A. Fakoorian, J. Huang, and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,” *CoRR*, vol. abs/1011.3754, 2010.

[8] U. M. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Trans. Info. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[9] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “An opportunistic physical-layer approach to secure wireless communications,” in *Proc. 44th Allerton Conf. on Communication Control and Computing*, 2006.

[10] P. K. Gopala, L. Lai, and H. E. Gamal, “On the secrecy capacity of fading channels,” *IEEE Trans. Info. Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[11] H. Koorapaty, A. A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Comm. Letters*, vol. 4, no. 2, pp. 52–55, 2000.

[12] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Trans. Mobile Computing*, vol. 10, no. 2, pp. 205–215, 2011.

[13] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Trans. Info. Forensics and Security*, vol. 5, no. 3, pp. 381–392, 2010.

[14] F. Oggier and B. Hassibi, "The MIMO wiretap channel," in *3rd Intl. Symp. ISCCSP*, 2008, pp. 213–218.

[15] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Info. Theory*, vol. 55, no. 6, pp. 2547–2553, 2009.

[16] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[17] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas - part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[18] J. Li and A. Petropulu, "Transmitter optimization for achieving secrecy capacity in Gaussian MIMO wiretap channels," *Arxiv preprint arXiv:0909.2622*, 2009.

[19] Z. Li, R. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in *IEEE Int. Symp. Inf. Theory, 2007*, Jun. 2007, pp. 1296–1300.

[20] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Vehicular Tech. Conf.*, vol. 62, no. 3, 2005, pp. 1906–1910.

[21] X. Li, J. Hwu, and E. P. Ratazzi, "Array redundancy and diversity for wireless transmissions with low probability of interception," in *2006 ICASSP*, vol. 4, 2006.

[22] O. Al-Rabadi and G. Pedersen, "Directional space-time modulation: A novel approach for secured wireless communication," in *IEEE Intl. Conf. Comm.*, 2012.

[23] R. Negi and S. Goel, "Secret communication in presence of colluding eavesdroppers," in *2005 MILCOM*, 2005, pp. 1501–1506.

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

[25] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation," *IEEE Trans. Vehicular Tech.*, vol. 59, no. 8, pp. 3831–3842, 2010.

[26] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Proc.*, vol. 59, no. 1, pp. 351–361, 2011.

[27] S. Bashar, Z. Ding, and C. Xiao, "On the secrecy rate of multi-antenna wiretap channel under finite-alphabet input," *IEEE Comm. Letters*, no. 99, pp. 1–3, 2011.

[28] A. Babakhani, D. B. Rutledge, and A. Hajimiri, "A near-field modulation technique using antenna reflector switching," in *IEEE Int. Solid State Circuits Conf.*, Feb. 2008, pp. 188–189.

[29] A. Babakhani, D. B. Rutledge, and A. Hajimiri, "Transmitter architectures based on near-field direct antenna modulation," *IEEE Journ. Solid-State Circuits*, vol. 43, no. 12, pp. 2674–2692, Dec. 2008.

[30] A. Chang, A. Babakhani, and A. Hajimiri, "Near-field direct antenna modulation (NFDAM) transmitter at 2.4 GHz," in *IEEE Antennas Propag. Soc. Int. Symp.*, 2009.

[31] E. J. Baghdady, "Directional signal modulation by means of switched spaced antennas," *IEEE Trans. Comm.*, vol. 38, pp. 399–403, Apr. 1990.

[32] H. Shi and A. Tennant, "Direction dependent antenna modulation using a two element array," in *Proc. 5th European Conf. on Ants. and Propag. (EUCAP)*, Apr. 2011, pp. 812–815.

[33] T. Hong, M.-Z. Song, and Y. Liu, "RF directional modulation technique using a switched antenna array for physical layer secure communication applications," *Progress in Electromagnetics Research*, vol. 116, pp. 363–379, 2011.

[34] T. Hong, M.-Z. Song, and Y. Liu, "Directional sensitive modulation signal transmitted by monopulse Cassegrain antenna for physical layer secure communication," *Progress in Electromagnetics Research M*, vol. 17, pp. 167–181, 2011.

[35] M. P. Daly and J. T. Bernhard, "Directional modulation technique for phased arrays," *IEEE Trans. Antennas Propag.*, vol. 57, pp. 2633–2640, Sep. 2009.

[36] M. P. Daly, E. L. Daly, and J. T. Bernhard, “Demonstration of directional modulation using a phased array,” *IEEE Trans. Antennas Propag.*, vol. 58, pp. 1545–1550, May 2010.

[37] M. P. Daly and J. T. Bernhard, “Beamsteering in pattern reconfigurable arrays using directional modulation,” *IEEE Trans. Antennas Propag.*, vol. 58, pp. 2259–2265, Jul. 2010.

[38] A. Saleh and R. Valenzuela, “A statistical model for indoor multipath propagation,” *IEEE Journ. Selected Areas in Comm.*, vol. 5, no. 2, pp. 128–137, 1987.

[39] A. Goldsmith, *Wireless Communications*, 1st ed. New York, NY: Cambridge University Press, 2005.

[40] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, N. J.: John Wiley & Sons, Inc., 2006.

[41] S. T. Brink, “Convergence behavior of iteratively decoded parallel concatenated codes,” *IEEE Trans. Comm.*, vol. 49, no. 10, pp. 1727–1737, 2001.

[42] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication.* Cambridge: Cambridge University Press, 2005.

[43] M. Tuchler, “Turbo equalization,” Ph.D. dissertation, Munich University of Technology, 2004.

[44] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering.* Cambridge Univ. Press, 2011.

[45] Digital Video Broadcasting, ETSI EN 302 307, V1.2.1, April 2009.

[46] J. T. Bernhard, *Reconfigurable Antennas.* Morgan & Claypool Publishers, 2007.

[47] S. Zhang, G. H. Huff, J. Feng, and J. T. Bernhard, “A pattern reconfigurable microstrip parasitic array,” *IEEE Trans. Antennas Propag.*, vol. 52, no. 10, pp. 2773–2776, 2004.

[48] G. H. Huff and J. T. Bernhard, “Integration of packaged RF MEMS switches with radiation pattern reconfigurable square spiral microstrip antennas,” *IEEE Trans. Antennas Propag.*, vol. 54, pp. 464–469, Feb. 2006.

[49] S. Yong and J. T. Bernhard, “Design of a pattern null reconfigurable antenna,” in *IEEE Intl. Symp. Phased Array Systems and Technology (ARRAY)*, 2010, pp. 376–380.

[50] Wireless Insite 2.3, Remcom. [Online]. Available: www.remcom.com

[51] P. Almers et al., "Survey of channel and radio propagation models for wireless MIMO systems," *EURASIP Journal on Wireless Communications and Networking*, vol. 2007, no. 1, pp. 56–56, 2007.

[52] J. W. Wallace and M. A. Jensen, "Modeling the indoor MIMO wireless channel," *IEEE Trans. Antennas Propag.*, vol. 50, no. 5, pp. 591–599, 2002.

[53] X. Yang and A. L. Swindlehurst, "On the use of artificial interference for secrecy with imperfect CSI," in *2011 IEEE 12th Intl. Workshop on Signal Proc. Advances in Wireless Comm.*, June 2011, pp. 476–480.

[54] R. L. Haupt, "Phase-only adaptive nulling with a genetic algorithm," *IEEE Trans. Antennas Propag.*, vol. 45, pp. 1009–1015, June 1997.

[55] R. L. Haupt, "Thinned arrays using genetic algorithms," *IEEE Trans. Antennas Propag.*, vol. 42, pp. 993–999, June 1994.

[56] K. K. Yan and Y. Lu, "Sidelobe reduction in array-pattern synthesis using genetic algorithm," *IEEE Trans. Antennas Propag.*, vol. 45, pp. 1117–1122, June 1997.

[57] R. J. Mailloux, *Electronically Scanned Arrays*, 1st ed. San Rafael, CA: Morgan & Claypool Publishers, 2007.

[58] D. M. Pozar, "The active element pattern," *IEEE Trans. Antennas Propag.*, vol. 42, pp. 1176–1178, Aug. 1994.

[59] R. C. Hansen, "Comments on 'The active element pattern'," *IEEE Trans. Antennas Propag.*, vol. 43, p. 634, June 1995.

[60] J. W. Craig, "A new, simple and exact result for calculating the probability of error for two-dimensional signal constellations," in *Proc. IEEE MILCOM'91*, 1991, pp. 571–575.

[61] L. Szczecinski, C. Gonzalez, and S. Aissa, "Exact expression for the BER of rectangular QAM with arbitrary constellation mapping," *IEEE Trans. Communications*, vol. 54, pp. 389–392, March 2006.

[62] L. Szczecinski, S. Aissa, C. Gonzalez, and M. Bacic, "Exact evaluation of BER for arbitrary modulation and signaling in AWGN channel," in *Proc. IEEE GLOBECOM 2005*, 2005, pp. 1234–1238.

[63] J. G. Proakis, *Digital Communications*, 4th ed. Boston, MA: McGraw-Hill, 2001.

[64] "Digital phase shifters," MITEQ, Inc. [Online]. Available: http://amps.miteq.com/datasheets/MITEQ-DPS.PDF.

[65] B. P. Lathi, *Modern Digital and Analog Communication Systems*, 3rd ed. New York: Oxford University Press, 1998.

[66] MATLAB version 7.0.4.365 (R14) Service Pack 2, Natick, MA: The Mathworks, Inc, 2005.