2013

Enhancing Secrecy via Exploring Randomness in the Wireless Physical Layer

Rehan Talat
University of Massachusetts Amherst

ENHANCING SECRECY VIA EXPLORING RANDOMNESS IN THE WIRELESS PHYSICAL LAYER

A Thesis Presented

by

REHAN TALAT

Submitted to the Graduate School of the
University of Massachusetts Amherst in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL AND COMPUTER ENGINEERING

September 2013

Electrical and Computer Engineering

ENHANCING SECRECY VIA EXPLORING RANDOMNESS IN THE WIRELESS PHYSICAL LAYER

A Thesis Presented

by

REHAN TALAT

Approved as to style and content by:

____

Dennis L. Goeckel, Chair

____

Robert W. Jackson, Member

____

Hossein Pishro-Nik, Member

____

C. V. Hollot, Department Chair
Electrical and Computer Engineering

ABSTRACT

ENHANCING SECRECY VIA EXPLORING RANDOMNESS IN THE WIRELESS PHYSICAL LAYER

SEPTEMBER 2013

REHAN TALAT

B.S., GIK INSTITUTE OF ENGINEERING SCIENCES AND TECHNOLOGY

M.S.E.C.E., UNIVERSITY OF MASSACHUSETTS AMHERST

Directed by: Professor Dennis L. Goeckel

In order to establish a secure connections in the wireless environment, cryptographic methods may require an exchange of a key or secret. Fortunately, the environment provides randomness due to multi-path fading that can be exploited by physical-layer security algorithms to help establish this shared secret. However, in some cases, multi-path fading might be absent or negligible; therefore, we look for artificial ways to increase randomness. In this thesis, we explore antenna radiation variation by altering the phase between two antennas as a means of creating artificial fading. We construct a model of the antenna gain variation by analyzing the radiation pattern and run Monte-Carlo simulations to compare our approach to a base case with only multi-path fading. We then empirically collect data in order to confirm our analysis. Finally, we incorporate this model in a prominent security algorithm to demonstrate the improvements in security possible through such an approach.

TABLE OF CONTENTS

Page

CHAPTER

LIST OF TABLES

Table **Page**

LIST OF FIGURES

Figure **Page**

CHAPTER 1

INTRODUCTION

In wireless communication systems, information is sent through the air; hence any device listening at the right frequency can record the broadcasted signal and potentially decode it for malicious purposes. Therefore, it is important that information is made secure so that only legitimate receivers can discern it. For this reason, cryptographic algorithms have been refined over the years to establish secure connections and render the signal captured useless to illegitimate nodes or adversaries.

While legitimate nodes can use a secure connection to share secret information, they may need to exchange secrets in the first place in order to establish this connection. This secret may be in the form of a key [14], a frequency hopping sequence [3], etc. For a brief moment while they exchange the secret, they need to maintain secret, reliable communication on an insecure channel, and, depending on the wireless channel, this can incur a very high communication cost. However, randomness in the channel can be used to improve this rate and to establish a secure connection. In this way, randomness in the wireless environment is often essential for secrecy and security.

This work explores enhancing the randomness in the wireless environment that can be used to create secrecy and thus enhance security. Specifically, we propose a physical layer technique that can provide randomness when natural randomness subsides without incurring a high cost.

1.1 Motivation

Key-based cryptographic methods require that the key is either previously agreed upon or is exchanged at the time of initiating conversation. The former is relatively easy to implement in the case of wired networks since the mobility of network elements is not an issue and the topology is fixed. The secret key has to be established once and can be used over again. Mobile nodes often communicate wirelessly and therefore, they have to transmit in the public insecure channel for a short time in order to establish a secure connection. They wander around and thus the network topology (e.g. neighbors and obstacles) is constantly changing.

In earlier works, key establishment has been approached with information-theoretic and computational security solutions. For example, [7] makes use of friendly-jamming to establish a secret key without dependence on the channel characteristics. Because of the probabilistic nature of wireless communications, even the computational security approaches make use of the randomness in the physical channel. In [3], Strasser et al. suggest the use of uncoordinated frequency hopping to establish a key for secure communication.

However, more extensive work has been done in the area of information-theoretic security which relies on the channel characteristics. The work in this area covers adaptation of existing protocols and methods to exploit the randomness in the channel; and uses secrecy rate as a base of evaluation. In [9], an oblivious transfer protocol based on the properties of the wireless physical channel is introduced. [4] measures the secrecy rate of using dirty-paper code in delivering confidential messages to multiple users using antenna diversity, whereas [6] evaluates the secrecy rate of slow-fading channels using channel state information.

The randomness in the channel is often used directly or indirectly in key generation and extraction techniques. In [5], the authors suggest taking RSS measurements to extract a secret key using the channel directly. [2] and [8] introduce the generation of dynamic secrets which constantly updates the system secrets. While these works focus on key generation, [10] and [11] focus on algorithms for exchanging keys, with [10] suggests a secret key exchange algorithm based on low-density parity-check codes using variations in the channel because of fading. On the other hand, [11] suggests a scheme called Physical-layer Enhanced Key Exchange method (PEK), which exchanges the key in the presence of an adversary by relying on the information loss at the adversary due to the randomness in the channel.

This work studies the effectiveness of randomness in establishing a secure communication in the wireless channel. Hence, it is important to consider the question of what will happen when the randomness goes away? In particular, multi-path fading is a major factor that causes randomness; however, its effect is reduced in stationary and less congested environments. From this motivation, we focus on antenna diversity as a means to generate randomness in the system and evaluate its usage. We explore the idea of generating artificial randomness through variation of the antenna pattern.

Our analysis is divided into two parts: the analytical section and the empirical section. In the first part, we analyze a linear two-element antenna array and its radiation pattern. In the second part, we make measurements to supplement our analytical work and study their impact on a prototypical security algorithm.

1.2 Background

For our research problem, we consider an oft-used jammer model. In this model, there are two allies (Alice and Bob) and one adversary, Eve. Alice and Bob want to communicate with each other; however, they must do so in the presence of an adversary, Eve. In particular, Eve acts as an eavesdropper and also has the ability to jam. If Eve is only listening, then she is termed “passive”. On the other hand, an active Eve has the additional ability to jam Bob while listening to Alice’s transmission.

If Eve is to be successful in her role as an adversary, she needs to be able to receive Alice's message directly or she needs to prevent Bob from receiving Alice's transmission. This is possible only if Eve is able to communicate at the same frequency as Alice and Bob. Moreover, Alice's signal which reaches Bob should have a high enough signal-to-noise ratio (SNR) so that Bob is able to successfully decode the message. The more successful Eve is in her efforts, the lower the secrecy rate will be and as a result, the system will incur a higher communication cost. In the analytical section, we analyze the probabilities of the events "Bob decodes Alice's message," denoted $P_{A \to B}$, and "Eve decodes Alice's message," denoted $P_{A \to E}$, to predict the likelihood of Alice's success (i.e, Eve's failure).

The radiation pattern generated by a phased array depends on the type of individual antenna elements and the number of antennas employed. We employ a two-element uniform linear array and, for the analysis work, each element is assumed to be an ideal isotropic antenna. This assumption is justified by the fact that dipole antennas can be used effectively as omni-directional antennas in a particular plane. The number of nulls in the generated pattern depends on the distance between the two elements and the phase difference of the source current in the two antennas. In our case, the underlying randomness is generated by the varying radiation pattern of the antennas being used by Bob and Alice. Although beam-forming can be achieved by deploying large antenna arrays and using complex algorithms, they incur a higher communication cost. On the contrary, we will demonstrate that we can artificially generate randomness using simple low-cost antennas.

For a fixed threshold, γ_a, the success is measured as the probability that the SNR of Alice's signal at Bob exceeds the threshold while Eve is unable to decode the same signal. We look into the case where the location of the friendly and adversary nodes are independent of each other.

The empirical section of our work contains measurements to corroborate our analysis. A dominant characteristic of the wireless channel is fading [1]. The channel response of the Alice-Bob channel and the Eve-Bob channel will be different from each other and there is a possibility that there is a deep fade in the Eve-Bob channel while Alice has a good channel to Bob. Generating randomness through antenna diversity can benefit in both cases where fading exists or does not exist. In order to see the effect of generating randomness on security of our method, we will incorporate this idea in the Dynamic Secrets algorithm introduced in [2].

1.3 Contribution

The current security and secrecy methods either have a high communication cost or require a pre-shared key. The amount of randomness required in many solutions leads us to believe that increasing randomness can improve these methods. Our main contribution in this research work is to study and analyze the different random phenomenon in such systems. We identify multi-path fading as the main source of randomness and then consider the worst-case scenario where it is less dominant. Therefore, we propose an artificial method for generating randomness by varying the phase of a two-element linear antenna array. We perform a thorough analysis of using antenna arrays by running Monte-Carlo simulations. And in the end, we empirically confirm the result of our simulations by collected measurements on a narrow-band channel. Moreover, we understand the limitations of our method and try to identify them as they come along.

In Chapter 2, we first lay the ground work for our theoretical analysis by presenting key concepts such as multi-path fading, and introduce the "Dynamic Secret [2]" security algorithm in more detail that relies on the randomness of the wireless channel. Moreover, we consider what happens if the multi-path fading, which produces the randomness, goes away. Thus, in Chapter 3, we present our idea of generating artificial randomness through antenna radiation variation and present Monte-Carlo simulation results to supplement our analysis. In Chapter 4, we test our idea by setting up a lab experiment and presenting its result. Furthermore, we assess these results by applying the solution to the Dynamic Secrets [2] algorithm in Chapter 5. Finally, we summarize our conclusions in the last chapter, Chapter 6.

CHAPTER 2

MULTI-PATH FADING

Multi-path fading is an important factor that contributes to the randomness of the wireless environment. In fact, for our analysis, we make an assumption that it is the only natural factor present in the system.

2.1 Multi-path Fading

The energy radiated by a transmitter is reflected, diffracted and scattered on its way toward the receiver. The same energy is incident on the receiver after taking multiple paths. There is an attenuation factor $\frac{\alpha_i(\theta,\phi,f)}{r}$ and time-delay τ_i associated with each path i of N paths, where (r, θ, ϕ) is the spherical coordinates of the point where the attenuation factor is calculated, and f is the carrier frequency. The variable $\frac{\alpha_i(\theta,\phi,f)}{r}$ depends on the product of the antenna patterns of transmit and receive antennas in the given direction[12] among other factors which can be taken as constant. The electrical field strength at the receiver[12] can be written as:

$$E(f, u) = \sum_{i=0}^{N-1} \frac{\alpha_i(\theta, \phi, f)}{r_i} e^{-j2\pi f \tau_i} \tag{2.1}$$

where u is the point at (r, θ, ϕ). The phases of different paths are assumed to be independent, and each has a uniform distribution in $[0, 2\pi]$. The electric field phasor in (2.1) can be expressed as a complex number $Z_r + jZ_i$ where Z_r and Z_i are real numbers. Because of the large number of paths present in the environment, the central limit theorem allows Z_i and Z_r to be modeled as independent and identically distributed (i.i.d.) Gaussian random variables, each with mean μ and variance σ^2. Let the magnitude of the received signal be a random variable R whose distribution we will derive subsequently.

The distribution that R takes depends on the mobility and environment of the receiver. For our analysis, let us assume the presence of a dominant path among the large number of paths between the transmitter and the receiver. This is true, for example, in scenarios where the transmitter and receiver are in direct line-of-sight (LOS). In this scenario, the power in all other reflected paths is less than the power in the dominant path. The electric field strength in (2.1) can be re-written as:

$$E(f,u) = \frac{\alpha_0(\theta,\phi,f)}{r_0} + \sum_{i=1}^{N-1} \frac{\alpha_i(\theta,\phi,f)}{r_i} e^{-j2\pi f \tau_i} \tag{2.2}$$

where the first term corresponds to the dominant path. In this scenario, Z_i and Z_r take a none-zero mean μ because of the dominant path and R takes a Rician distribution [16] with parameters K and σ^2. The parameter K is called the Rician K-factor and is the ratio of the power in the dominated path to the power in the reflected paths:

$$K = \frac{E\left[|\frac{\alpha_0(\theta,\phi,f)}{r_0}|^2\right]}{E\left[\sum\limits_{i=1}^{N-1} |\frac{\alpha_i(\theta,\phi,f)}{r_i}|^2\right]} \tag{2.3}$$

This type of fading is called Rician fading [13] and the probability distribution of R (for $r \geq 0$) is defined as:

$$f_R(r) = \frac{r}{\sigma^2} e^{\frac{-(r^2+|\frac{\alpha_0(\theta,\phi,f)}{r_0}|^2)}{2\sigma^2}} I_0\left(\frac{r\frac{\alpha_0(\theta,\phi,f)}{r_0}}{\sigma^2}\right) \tag{2.4}$$

where $I_0()$ is the 0th order modified Bessel function of the first kind and σ^2 is the variance.

For the special case when $K = 0$ i.e. there is no dominant path and all paths have comparable power, then Z_i and Z_r are i.i.d. Gaussian random variables with zero mean ($\mu = 0$). Therefore, the distribution for R reduces from a Rician distribution to a Rayleigh distribution [16]:

$$f_R(r) = \frac{r}{\sigma^2} e^{-r^2/2\sigma^2} \tag{2.5}$$

This type of fading is called Rayleigh fading [13]. Moreover, the square of the magnitude of the received signal, $|R|^2$, can be modeled as the convenient exponential distribution [12]:

$$f_{|}R|^2(r) = \frac{1}{2\sigma^2} e^{\frac{-r}{2\sigma^2}} \tag{2.6}$$

Let's now consider a channel between two nodes P and Q, denoted by PQ, that undergoes multi-path fading. Node P transmits a message, x_P to Node Q through the channel PQ. The message received at Node Q, y_Q, will be:

$$y_Q = h_{PQ} x_P + n_Q \tag{2.7}$$

where h_{PQ} is the fading coefficient, and n_Q is the noise at Q. In this Equation, h_{PQ} is a random variable which takes a distribution depending on the type of fading in the environment such as Rayleigh or Rician fading. We will now use the concepts presented thus far to introduce our system model and draw assumptions on which we have based our analysis.

2.2 System Model

The first chapter introduced a system that consists of three nodes i.e. Alice, Bob and Eve; which we will use in our analysis. Alice and Bob are allies who wish to communicate with each other. For ease of reference, we have designated Alice as the transmitter and Bob as the receiver. Secure communication techniques are aided if Alice and Bob can create a short shared key with each other before they begin transmission [11]. Moreover, this key exchange can take place on-demand over the air and hence possibly in the presence of an adversary. Therefore, it is essential that this exchange takes place secretly even if that results in a high communication cost.

Our Alice-Eve-Bob system results in three physical wireless channels i.e. Alice-Bob, Bob-Eve, and Alice-Eve. The three channels are independent of each other [12] and hence, can be represented by independent channel responses. Due to reciprocity, the A-B channel response is the same as the B-A channel response i.e. h_{AB} and h_{BA} are equivalent. Since each channel is independent of the others, it is possible to have a good Alice-Bob channel and a bad Alice-Eve channel at the same time. This scenario leads to information loss at Eve, which enables Alice and Bob to communicate secretly. Hence, it is important that such instances occur as frequently as possible, as they will improve the secrecy rate and lower communication costs.

A secret message is successfully exchanged between Alice and Bob if Bob can decode Alice's message and at the same time, Eve fails to do so. In the presence of noise, a node can decode a message if the signal-to-noise ratio of the received signal is greater than a certain threshold, γ. This noise can be due to external factors such as interference or internal factors such as thermal noise of the hardware. We assume that the noise present in the system is additive white gaussian noise (AWGN) with constant one-sided power spectral density, N_0.

For now, let's assume that Alice, Bob and Eve are using single omni-directional antennas i.e. antennas that radiate equal power in all directions. We will refer to this system as the base case, against which we will compare the scheme that we will introduce in the next chapter.

Let's expand on Equation (2.7) to incorporate the base case that we just introduced. We will begin by doing an analysis of the Alice-Bob channel. We assume that Alice is transmitting a signal with power $P_A = E[|x_p|^2]$. Since Alice is using an omni-directional antenna, it's gain toward Bob will be 1. Now, let $h_{A \to B}$ be the random variable that represents the fading coefficient for the channel between Alice and Bob. Therefore, the total power received by Bob will be $P_A*1*|h_{A\to B}|^2$. After taking into account the noise present in the system, we can write the received power at Bob from Alice, $RcvdPx_{A\to B}$, as:

$$RcvdPx_{A\to B} = \frac{P_{A\to B}|h_{A\to B}|^2}{r_{AB}^{\alpha}} \tag{2.8}$$

where r_{AB} is the the distance between Alice and Bob, and α is the path-loss exponent. Correspondingly, we can write the SNR as:

$$SNR_{A\to B} = \frac{P_{A\to B}|h_{A\to B}|^2/r_{AB}^{\alpha}}{N_0} \tag{2.9}$$

Before we analyze the Alice-Eve and Eve-Bob channel, we need to consider assumptions about Eve. We assume Eve can potentially jam Bob at the same frequency on top of having the capability to listen to Alice's communication. In other words, she has the capability to receive and transmit at any frequency. Hence, Alice and Bob cannot choose such a frequency that Eve is not able to listen to their conversation. Moreover, she is not initiating a man-in-the-middle attack nor is she too close to the source such that no security measure can be effective. She has unlimited energy, but a fixed transmission power i.e. she can transmit at a certain frequency for an indefinite amount of time up to a maximum transmission level. We next characterize Eve into two distinct profiles for our analysis.

2.2.1 Passive Eve

Eve is passive when it only has the ability to eavesdrop on Alice-Bob's conversation. If we assume $h_{A\to E}$ to be the fading coefficient of Alice-Eve's channel then similar to our analysis for (2.7), we write down the received power at Eve from Alice, $RcvdPx_{A\to E}$, as:

$$RcvdPx_{A\to E} = \frac{P_{A\to E}|h_{A\to E}|^2}{r_{AE}^{\alpha}} \tag{2.10}$$

where r_{AE} is the the distance between Alice and Eve, and α is the path-loss exponent. Correspondingly, we can write the SNR as:

$$SNR_{A\to E} = \frac{P_{A\to E}|h_{A\to E}|^2/r_{AE}^{\alpha}}{N_0} \tag{2.11}$$

2.2.2 Active Eve

Active Eve has the ability, in addition to eavesdropping, to jam communication. We make an assumption that Eve jams by generating noise at Alice's transmission frequency to attempt to make the legitimate signal indistinguishable at Bob. She does not jam by partially altering the message or re-transmitting the complete message. If we denote $P_{E\to B}$ as the power transmitted by Eve, $h_{E\to B}$ to be the fading coefficient of Eve-Bob's channel, and assume that Eve is also radiating energy uniformly in all directions; then by extending (2.8), we have:

$$RcvdPx_{A\to B} = \frac{P_{A\to B}|h_{A\to B}|^2}{r_{AB}^{\alpha}} + \frac{P_{E\to B}|h_{E\to B}|^2}{r_{EB}^{\alpha}} \tag{2.12}$$

where r_{EB} is the the distance between Eve and Bob, and α is the path-loss exponent. Correspondingly, we can write the SNR as:

$$SNR_{A\to B} = \frac{P_{A\to B}|h_{A\to B}|^2/r_{AB}^{\alpha}}{P_{E\to B}|h_{E\to B}|^2/r_{EB}^{\alpha} + N_0} \tag{2.13}$$

Since Eve is also listening, (2.10) and (2.11) hold true to calculate the power received at Eve.

In this section, we have presented a thorough examination of the system. Now, we would like to expand on this system by discussing a few secrecy algorithms that rely on multi-path fading.

2.3 Secrecy and Multi-path fading

As discussed in Section 1.1, randomness in the environment plays a vital role in establishing secrecy. Therefore, multi-path fading is very important in the wireless channel. Let us take a look at two secrecy algorithms, Dynamic Secrets [2] and Physical-layer Enhanced Key (PEK) exchange method [11], in light of multi-path fading. Both these algorithms make use of the Alice-Bob-Eve system model.

In [11], the author presents the PEK exchange algorithm that allows Alice and Bob to secretly exchange a key in order to establish a secure connection. Alice makes use of uncoordinated frequency hopping, within a range of agreed upon frequencies, to send out short messages. This makes it difficult for Eve to track which frequency is being used for communication. Moreover, it makes use of co-operative jamming whereby Alice employs a secondary antenna to jam Eve.

In [2], the author presents “Dynamic Secrets” as a method to maintain secrecy of a system by dynamically updating the system key. Alice and Bob agree on a secret key, which they periodically update by exchanging messages over the air. Adversaries like Eve can gain knowledge of the system key at a given instance; however, since the key is being constantly updated, she can not maintain knowledge of the key unless she is privy to the conversation between Alice and Bob.

The two algorithms described above rely on packets received at Bob that are lost at Eve. Randomness caused by multi-path fading increases the likelihood for this event to happen. Let’s consider Rayleigh fading. When the K-factor is small, multi-path fading is prevalent since there is no single path dominating all the other paths. But as the Rician K-factor gets bigger, a dominant path gets stronger and stronger. Thus, energy from all the other multi-paths become insignificant. In other words, the fading due to multi-path blends into the AWGN channel and the channel becomes deterministic. In such cases, the efficiency of these security algorithm reduces as it becomes more difficult to establish a secure connection and the communication cost can become prohibitive.

Therefore, in such instances, it is very useful for us if we can artificially generate randomness in the system. In the next chapter, we will show a way to vary antenna radiation as a method to artificially introduce randomness into the system. When the Rician K-factor is large, this artificial randomness can help security algorithms to establish and maintain secrecy at a lower communication cost.

2.4 Measuring Success: Defining a metric

We will now define a metric that we will use throughout our analyis to compare the base case with a test case. As mentioned earlier, a secret message is sent successfully from Alice to Bob if Bob decodes the message and Eve does not. Since, we made an assumption that Bob and Alice are independently located at a fixed distance around Alice, therefore, we can also assume that the event whether Bob decodes Alice's message is independent of the event that Eve decodes Alice's message. So the probability of success can be defined as:

$$\begin{aligned} P_{succ} &= \text{P(“Bob decodes” AND “Eve does not decode”)} \\ &= \text{P(Bob decodes)} * \text{P(Eve does not decode)} \\ &= \text{P(SNR of Alice's signal at Bob} > \gamma_b) * \text{P(SNR of Alice's signal at Eve} < \gamma_e) \end{aligned} \tag{2.14}$$

where γ_b and γ_e is the minimum SNR required to decode a message successfully at Bob and Eve, respectively. We can now extend our analysis in Section 2.2 to evaluate the probability of success. We deduce the probability of success for Passive Eve base case as follows:

$$\begin{aligned} P_{succ} &= P(\tfrac{P_A|h_{A\to B}|^2}{N_0} > \gamma_b)P(\tfrac{P_A|h_{A\to E}|^2}{N_0} < \gamma_e) \\ &= P(\tfrac{P_A|h_{A\to B}|^2}{N_0} > \gamma_b)[1 - P(\tfrac{P_A|h_{A\to E|^2}}{N_0} > \gamma_e)], \end{aligned} \tag{2.15}$$

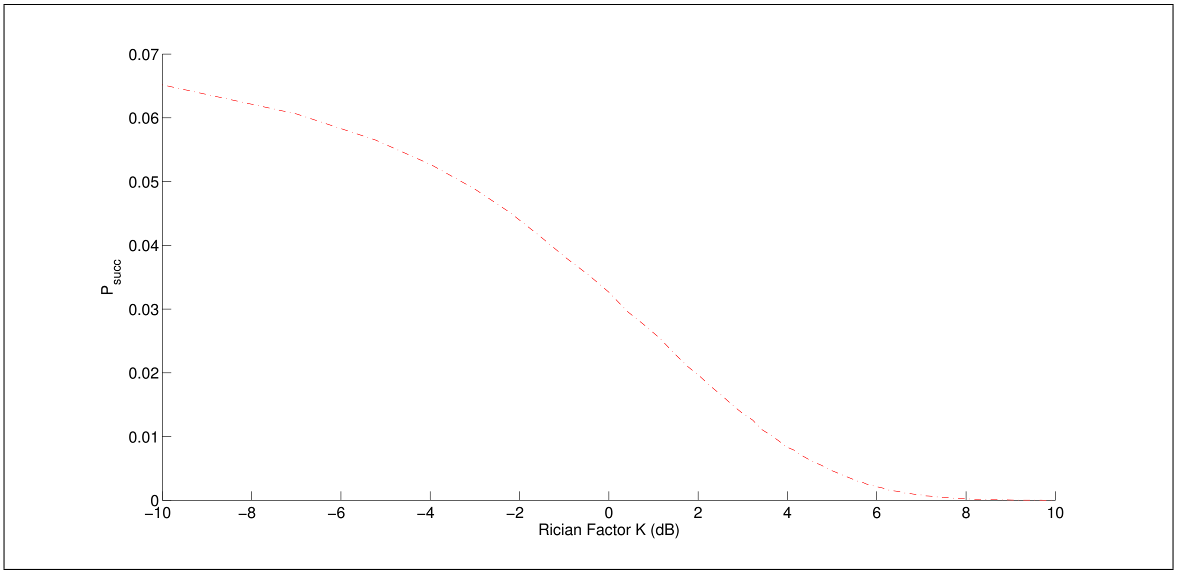
When the channel exhibits Rayleigh fading, $|h_{P \to Q}|$ takes an exponential distribution. Hence, this expression can be further evaluated as:

$$P_{succ} = \left(e^{-\gamma_b N_0/2\sigma^2 P_A}\right)\left(1 - e^{-\gamma_e N_0/2\sigma^2 P_A}\right) \tag{2.16}$$

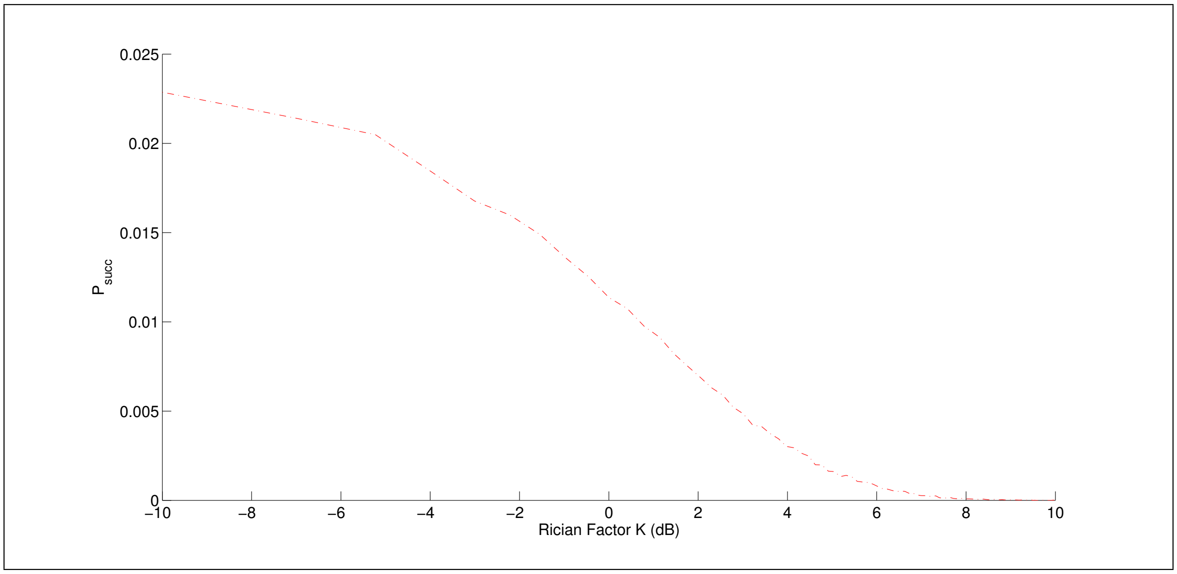
Similarly, we deduce the probability of success for Active Eve base case as follows:

$$P_{succ} = P(\frac{P_A|h_{A\to B}|^2}{P_E|h_{E\to B}|^2/r_{EB}^2 + N_0} > \gamma_b)[1 - P(\frac{P_A|h_{A\to E}|^2}{N_0} > \gamma_e)] \tag{2.17}$$

We will run Monte-Carlo simulations to see how P_{succ} varies with increasing Rician K-factor for Passive and Active Eve. We assume that total power transmitted by Alice, P_A, is fixed at 10 units. Moreover, when Eve is jamming we assume that the total power transmitted by Eve, P_E, is also fixed at 10 units. We assume that the noise power density in the system is constant i.e. $N_0 = 1$. The decode threshold for Bob, γ_b is fixed at 5 dB, and we assume that Eve's decode threshold is fixed at $(\gamma_e = 1dB)$. The results of the simulations for Passive and Active Eve are plotted in Figure 2.1 and we observe that as the K-factor increases, i.e. multi-path fading goes away, the probability of success reduces to zero.



(a) Passive Eve



(b) Active Eve

Figure 2.1: Probability of Success vs Rician K-factor. Bob's threshold to decode a message, γ_b, is fixed at 5 dB. Eve's threshold to decode a message, γ_e, is fixed at 1 dB. We observe that as the channel changes from Rayleigh fading (K-factor = 0) to an additive white Gaussian noise (AWGN), the probability of success decreases to zero as fading goes away.

CHAPTER 3

ANTENNA DIVERSITY AND RANDOMNESS

Antennas play an important role in any wireless communication system. They convert the energy from an electric current into electro-magnetic radiation and vice versa. The radiation fields, which is one way to characterize antennas, is divided into three regions: reactive near field, radiating near field (formerly Fresnel) and radiating far field (formerly Fraunhofer). The “radiation pattern” of an antenna is the gain as a function of angle of its radiating far field. The boundary between the radiating near and far field is generally accepted as approximately equal to $(2L^2)/\lambda$ from the source of radiation, where L is the length of the largest dimension of the antenna, and λ is the wavelength of the source. For example, for an antenna of length 7.1 inches, and operating at 400 MHz, the boundary is approximately a distance of 3.5 inches from the antenna. Figure 3.1 shows the radiation pattern of a half-wave dipole antenna.

The radiation pattern is a three dimensional plot since the antenna radiates in all directions. In most cases, the two-dimensional azimuthal and elevation plane plots provide sufficient information to understand the complete pattern. The radiation pattern consists of lobes of energy (simplistically named as main, side, front and back lobes) and nulls, where energy is not present. The antenna is unable to transmit, or in reciprocity is unable to receive, in directions where the nulls occur. In reality, the radiation pattern is not neatly defined into lobes as there are numerous other factors in play; however, the directivity remains the same.

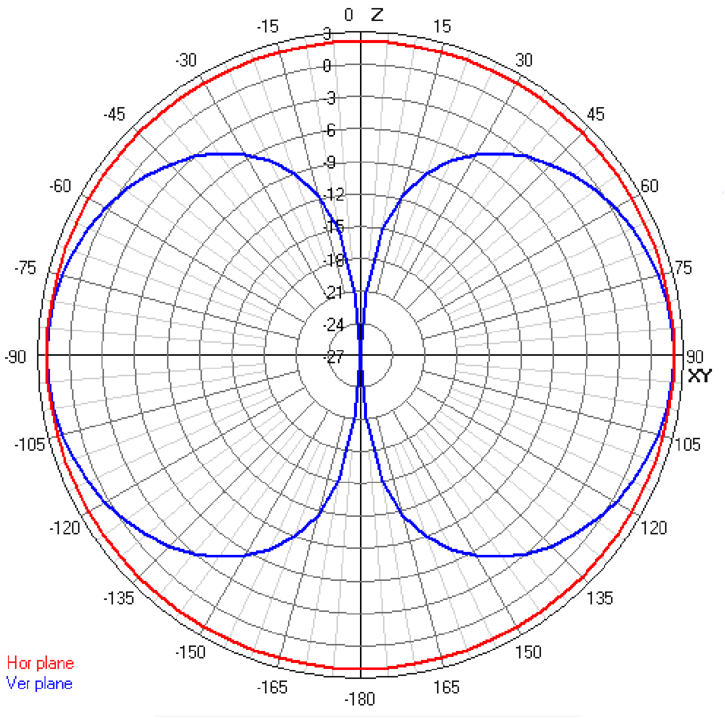


Figure 3.1: Radiation pattern of a dipole antenna that has two lobes and two nulls. The red plot shows the azimuthal plane radiation and and blue plot shows the elevation plane radiation.

In our work, we use the antenna's radiation pattern to generate randomness in the system. Referring back to Figure 3.1, let's consider a point at the 90° angle mark of the figure. Denote the gain of the antenna at that point by X. If we are able to vary the radiation pattern of the antenna, this will consequently vary the value of X. This can be achieved in a number of ways including but not limiting to changing the dimensions of the antenna, and rotating the antenna on its axis. If we normalize the gain of the antenna, the value of X will vary from 0 to 1 where the distribution of values depend on the radiation pattern. In the case of an isotropic antenna, which radiates equally in all directions, the value of X will remain constant. However, isotropic antennas do not exist in practical situations and each antenna has some sort of directivity associated with it. Nonetheless, isotropic antennas are used as the basis of making comparison between several antennas and it is the one that we will be using in our work.

In this chapter, Section 3.1 provides an explanation of the characteristics of an antenna array. In Section 3.2, we analyze these characteristics with reference to the transmitter-receiver system. Section 3.3 extends the system model presented in Section 2.2 to incorporate antenna arrays. And then, we present Monte-Carlo simulations that we ran on the extended model in Section 3.5

3.1 Antenna Arrays

Single element antennas are replaced by antenna arrays in a lot of applications where the radiation pattern of single elements does not meet the directivity or performance requirements. The array is constructed by placing the single elements in a one or two dimensional arrangement. The same input is fed to all elements but with varying linear or non-linear phase difference to achieve the required radiation pattern. The Array factor is an important characteristic which depends only on the elements' geometrical configuration. The radiation pattern of the array is given by:

$$\text{Array Radiation Pattern} = \text{Array Factor} * \text{Element Radiation Pattern} \tag{3.1}$$

In our system, we use a two element array separated by a distance d and having a phase difference of α. The distance d can be expressed in terms of the radiating electromagnetic wave's wavelength as $n\lambda$. For our analysis, we are using isotropic antenna elements that radiate equally in every direction. Hence, when normalized, it will have a gain of 1 in every direction. In our case, the array radiation pattern is equal to the array factor AF; therefore, it can be expressed as:

$$AF(\theta) = \cos\left(\frac{kd\cos(\theta) + \alpha}{2}\right) \tag{3.2}$$

where $k = \frac{2\pi}{\lambda}$, $d = n\lambda$, and θ is the angle of incidence.

Equation (3.2) represents the normalized field pattern, however, we will use the normalized power pattern which represents a plot of the square of the amplitude of the electric or magnetic field in angular space. Hence, the power pattern can be represented as follows:

$$G(\theta) = \cos^2\left(\frac{2\pi n \cos(\theta) + \alpha}{2}\right) \tag{3.3}$$

The frequency of the electromagnetic wave determines n whereas α depends on the phase difference of the currents fed into the antennas. If we vary these constants, we can in turn vary the radiation pattern of the antenna array. Since we want to generate a varying radiation pattern, it is difficult to achieve it by constantly altering the physical dimensions or by changing the frequency. Therefore, we achieve a varying radiation field by altering the phase difference only. Figure 3.2 illustrates the radiation pattern for a two-element isotropic array.

3.2 Analysis

In this section, we derive the probability distribution for a varying antenna pattern of a two-element linear phase array. We assume that the transmitter is stationary and the locations of the receiver nodes are varying. For ease of reference, we will do the analysis with reference to the system model introduced in Section 2.2 whereby Alice is the transmitter node, Bob is the receiver node and Eve is the adversary.

Let θ_b denote the angle of Bob from Alice and θ_e denote the location of Eve from Alice. It is assumed

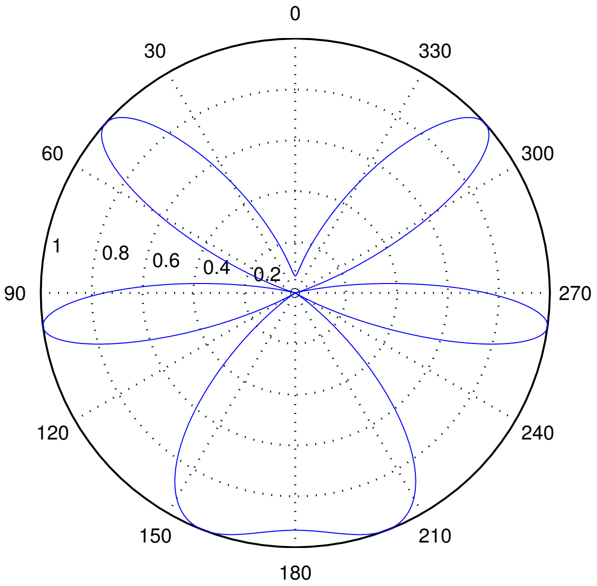


Figure 3.2: Polar Plot: Power radiation pattern of an antenna array with two isotropic elements ($d = 1.25\lambda$, $\alpha = \pi/3$).

that Bob's and Eve's location are independent of each other, and Bob and Alice are not aware of Eve's location. However, the two nodes are at the same distance from Alice. In other words, we can consider that Eve or Bob are on the circumference of a unit circle with Alice in the center. Moreover, we assume that Bob and Eve can take any location around Alice with equal probability. This means that θ_b and θ_e are i.i.d. uniform random variables in the range $[-\pi, \pi)$.

$$\theta_b \sim U[-\pi, \pi) \tag{3.4}$$

$$\theta_e \sim U[-\pi, \pi) \tag{3.5}$$

Let G_b denote the antenna gain at Alice in Bob's direction and G_e denote the antenna gain at Alice in Eve's direction. Since G_b and G_e are functions of θ_b and θ_e, respectively, they are also i.i.d. random variables in the range $[0, 1]$. In order to find the probability density function of G_x (in this subsection, from here onward G_x will refer to both G_b and G_e unless specified), we will first find $P(G_x < g)$ i.e. the cumulative distribution function (cdf).

We will proceed through extending the use of the antenna array shown in Figure 3.2. The elements in the array are separated by a distance 1.25λ and have a phase difference of $\pi/3$ radians. Hence, the gain G from (3.3) is:

$$G(\theta) = \cos^2\left(\frac{2.5\pi\cos(\theta) + \frac{\pi}{3}}{2}\right)$$

Figure 3.3 shows the same radiation pattern in a cartesian plot rather than a polar plot. This plot is more convenient to find the range of θ, $\Delta\theta$s, to evaluate $P(G_x < g)$. For example, let's say we would like to evaluate $P(G_x < g)$ for $g = 0.5$. From Figure 3.3, we see that there are five sub-ranges of θ that satisfy this condition:

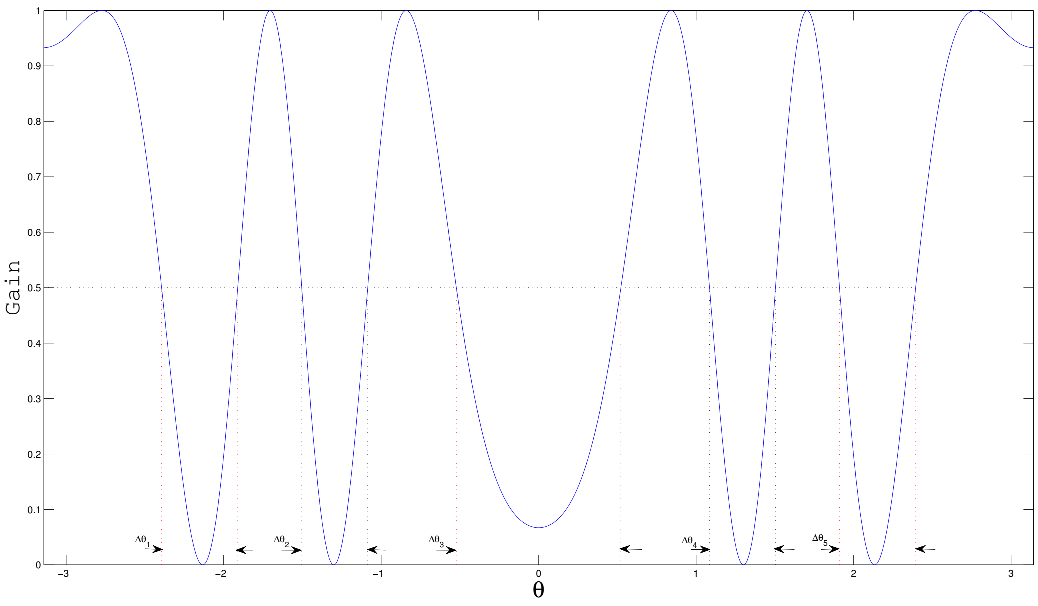


Figure 3.3: Cartesian Plot: Power Radiation Pattern of two-element isotropic antennas ($d = 1.25\lambda$, $\alpha = \pi/3$).

$$\begin{aligned} \Delta\theta_1 :&\quad -2.394 < \theta < -1.9106 \\ \Delta\theta_2 :&\quad -1.5040 < \theta < -1.0852 \\ \Delta\theta_3 :&\quad -0.5222 < \theta < 0.5222 \\ \Delta\theta_4 :&\quad 1.0852 < \theta < 1.5040 \\ \Delta\theta_5 :&\quad 1.9106 < \theta < 2.394 \end{aligned} \tag{3.6}$$

Using information from (3.4), we calculate the probabilities:

$$\begin{aligned} P(\Delta\theta_1) =&\quad \tfrac{1}{2\pi}(-1.9106 - (-2.394)) = 0.0769 \\ P(\Delta\theta_2) =&\quad \tfrac{1}{2\pi}(-1.0852 - (-1.5040)) = 0.0667 \\ P(\Delta\theta_3) =&\quad \tfrac{1}{2\pi}(0.5222 - (-0.5222)) = 0.1662 \\ P(\Delta\theta_4) =&\quad \tfrac{1}{2\pi}(1.5040 - 1.0852) = 0.0667 \\ P(\Delta\theta_5) =&\quad \tfrac{1}{2\pi}(2.394 - 1.9106)) = 0.0769 \end{aligned}$$

Hence,

$$P(G_x < 0.5) = \sum_{i=1}^{n} P(\Delta\theta_i) = 0.4534 \tag{3.7}$$

In this way, we can generate the cdf for G_x for a given n and α. Writing it down in a closed form solution, we have the following expression:

$$P(G < g) = \begin{cases} 1, & \text{for } g \geq G_{max} \\ \sum_{i=1}^{m} P(\Delta\theta_i), & \text{for } G_{min} < g < G_{max} \\ 0, & \text{for } g \leq G_{min} \end{cases} \tag{3.8}$$

where, since θ follows a uniform distribution and using the symmetry in the radiation pattern, $P(\Delta\theta_i)$ is defined as:

$$P(\theta_i^{(s)} < \theta < \theta_i^{(e)}) = \frac{1}{\pi}(\theta_{m_1} - \theta_{m_2})$$

and m is the number of intervals of θ in $[0, \pi)$ for which $G_x < g$. $\theta_i^{(s)}$ and $\theta_i^{(e)}$ are start and end values, respectively, of those m intervals.

3.3 Extending the System Model

We introduced the communication model for analyzing the base case in Section 2.2. Now, we will extend the same model to introduce the test case by including the suggested varying-phase antenna array. The assumptions we make for Alice, Bob and Eve also hold true for the test case. The only difference is that since we will be using varying-phase antenna array instead of omni-directional antennas at some nodes, the power radiated by that node will not be the same in every direction.

3.3.1 Passive Eve

In this scenario, both Bob and Eve are the listening nodes whereas Alice is the only transmitting node. Therefore, we deploy a varying-phase antenna array at Alice whereas Bob and Eve will be using single omni-directional antenna. We represent the gain of Alice's antenna array in the direction of Bob and Eve as $Y_{A \to B}$ and $Y_{A \to E}$, respectively. Since the total power transmitted by Alice is the same for Bob and Eve, we can denote it by P_A. Therefore:

$$P_{A \to B} = P_{A \to E} = P_A$$

Since $h_{A \to B}$ is the fading coefficient of the Alice-Bob channel, Bob is at unit distance from Alice, $r_{AB} = 1$, and N_0 is the noise power spectral density; we can write the SNR of the signal received at Bob as:

$$SNR_{A \to B} = \frac{P_A |h_{A \to B}|^2 Y_{A \to B}}{N_0} \tag{3.9}$$

Similarly, $h_{A \to E}$ is the fading coefficient of the Alice-Eve channel, Eve is at unit distance from Alice, $r_{AE} = 1$, and N_0 is the noise power spectral density; we can write the SNR of the signal received at Eve as:

$$SNR_{A \to E} = \frac{P_A |h_{A \to E}|^2 Y_{A \to E}}{N_0} \tag{3.10}$$

3.3.2 Active Eve

Recall that, in this scenario, both Bob and Eve are still the listening nodes, however, along with Alice, Eve is also attempting to jam the communication at Bob. In this test case, we deploy two antenna arrays, one used by Alice and one used by Bob. It is also important to note that, although Eve is trying to jam Bob, we assume Alice is not affected by these jamming efforts. Analogous to the definition of $Y_{A \to B}$ and $Y_{A \to E}$, let us represent the gain of Bob's antenna array in the direction of Alice and Eve as $Y_{B \to A}$ and $Y_{B \to E}$, respectively. Let the total power being transmitted by Eve be denoted as P_E. Since the total power transmitted by Alice is the same for Bob and Eve, we can denote it by P_A. Since $h_{A \to B}$ and $h_{E \to B}$ are the fading coefficients of the Alice-Bob and Eve-Bob channels, respectively, Eve and Bob are at a unit distance from Alice ($r_{AB}, r_{AE} = 1$), and while N_0 is the noise power spectral density; we can write the SNR of the signal received at Bob as:

$$SNR_{A\to B} = \frac{P_A|h_{A\to B}|^2 Y_{A\to B} Y_{B\to A}}{P_E|h_{E\to B}|^2 Y_{B\to E}/r_{EB}^2 + N_0}, \tag{3.11}$$

where r_{EB} is the distance between nodes Bob and Eve and the path-loss exponent is 2. Similarly, $h_{A\to E}$ is the fading coefficient of the Alice-Eve channel, Eve is at unit distance from Alice ($r_{AE} = 1$) and N_0 is the noise power spectral density; we can write the SNR of the signal received at Eve as:

$$SNR_{A\to E} = \frac{P_A|h_{A\to E}|^2 Y_{A\to E}}{N_0} \tag{3.12}$$

3.4 Measuring Success: Defining a metric

In Section 2.4, we introduced a metric to measure the success of the base case. Now, we will extend that metric for the test case. To reiterate, a secret message is sent successfully from Alice to Bob if Bob decodes the message and Eve does not. Hence, the probability of success can be extended for the test case of Passive and Active Eve. For Passive Eve, we can write P_{succ} as follows:

$$\begin{aligned} P_{succ} &= P(\tfrac{P_A|h_{A\to B}|^2 Y_{A\to B}}{N_0} > \gamma_b) P(\tfrac{P_A|h_{A\to E}|^2 Y_{A\to E}}{N_0} < \gamma_e) \\ &= P(\tfrac{P_A|h_{A\to B}|^2 Y_{A\to B}}{N_0} > \gamma_b)[1 - P(\tfrac{P_A|h_{A\to E}|^2 Y_{A\to E}}{N_0} > \gamma_e)]. \end{aligned} \tag{3.13}$$

Similarly, for Active Eve as follows:

$$P_{succ} = P(\frac{P_A|h_{A\to B}|^2 Y_{A\to B} Y_{B\to A}}{P_E|h_{E\to B}|^2 Y_{B\to E}/r_{EB}^2 + N_0} > \gamma_b)[1 - P(\frac{P_A|h_{A\to E}|^2 Y_{A\to E}}{N_0} > \gamma_e)] \tag{3.14}$$

3.5 Monte-Carlo Simulations

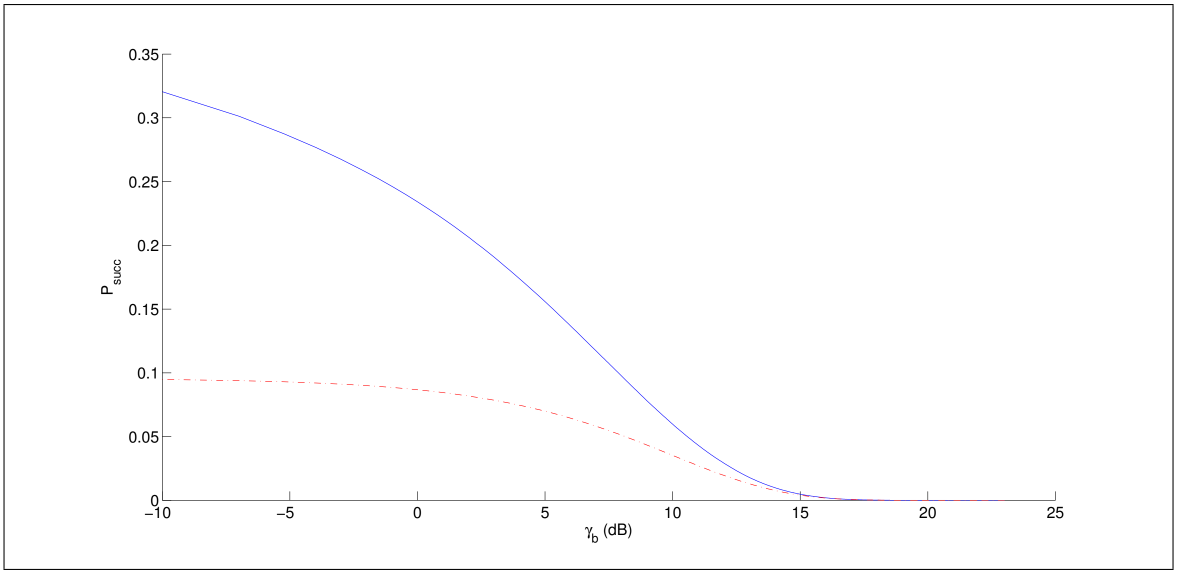
We will present results of running Monte-Carlo simulations for Rician (K-factor = 5 dB) and Rayleigh fading (K-factor = 0 dB) environments. The two antennas at

Alice's varying-phase antenna array are separated by n wavelengths and have a phase difference of α. We assume that total power transmitted by Alice, P_A, is fixed at 10 units. Moreover, when Eve is jamming we assume that the total power transmitted by Eve, P_E, is also fixed at 10 units. We assume that the noise power density in the system is constant i.e. $N_o = 1$. While the decode threshold for Bob, γ_b can vary from -10 dB to 25 dB, we assume that Eve's decode threshold is fixed at ($\gamma_e = 1dB$).

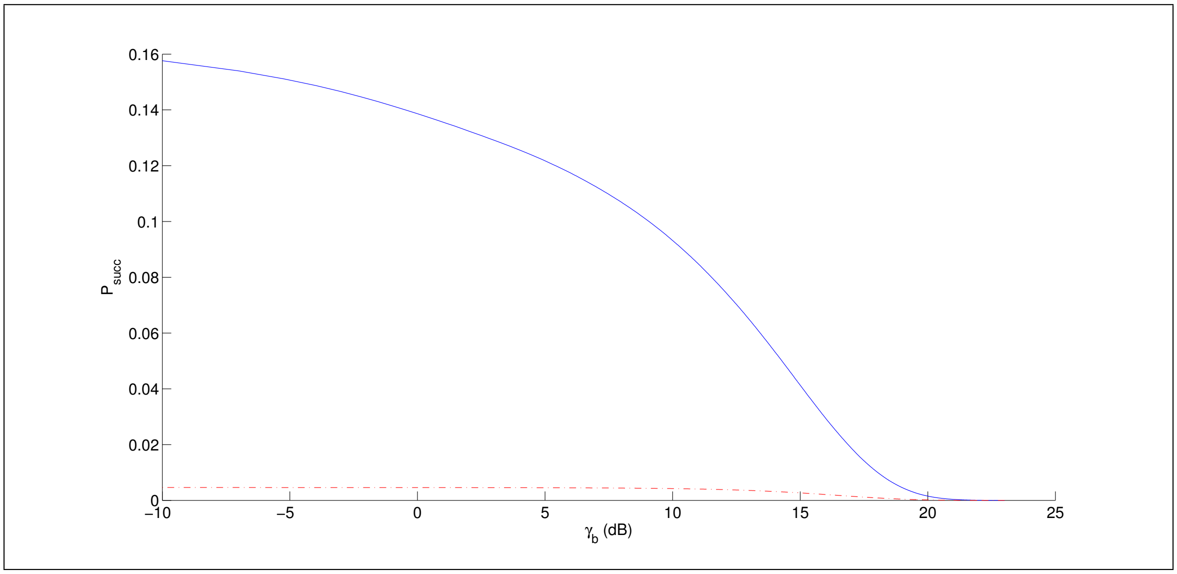
The following sections show simulation results for Passive and Active Eve. Recall that in Passive Eve test case scenario, Alice only uses an antenna array whereas in Active Eve test case scenario, both Alice and Bob use the antenna arrays. We observe that in Passive Eve simulations, the test case always shows more success than the base case. In the Active Eve simulations, the base case is more successful when multi-path fading is dominant in the channel (lower K-factor). But, as multi-path fading becomes less dominant, and the slowly goes away, the test case is more successful than the base case. We attribute this to presence of another antenna array at Bob.

3.5.1 Passive Eve

1. Varying SNR at fixed K, α and n:



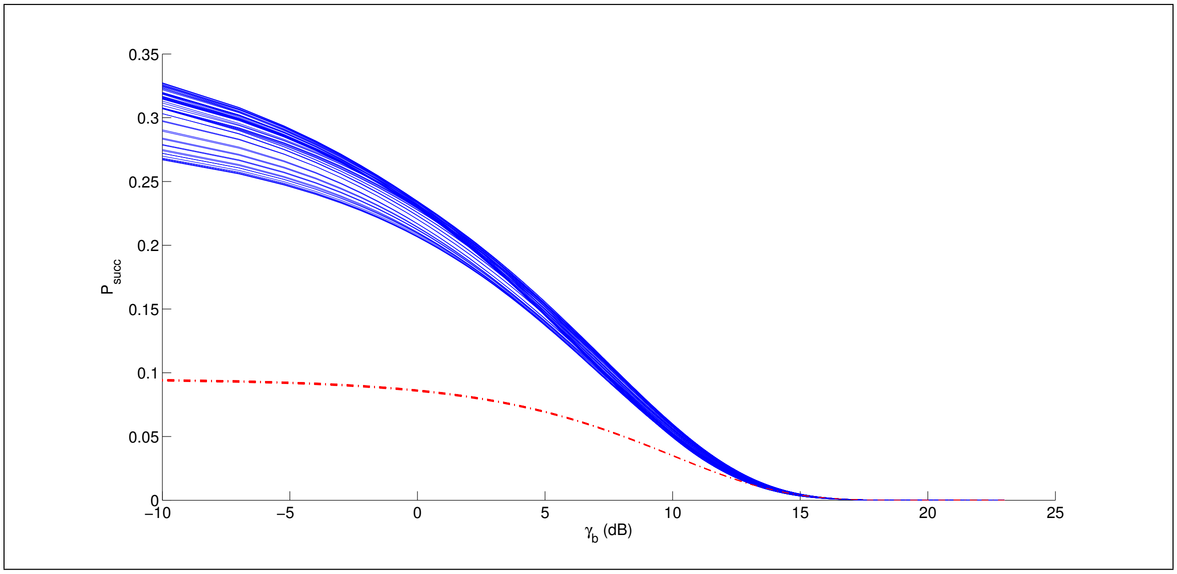
(a) Rician K-factor = 0 dB (Rayleigh Fading)



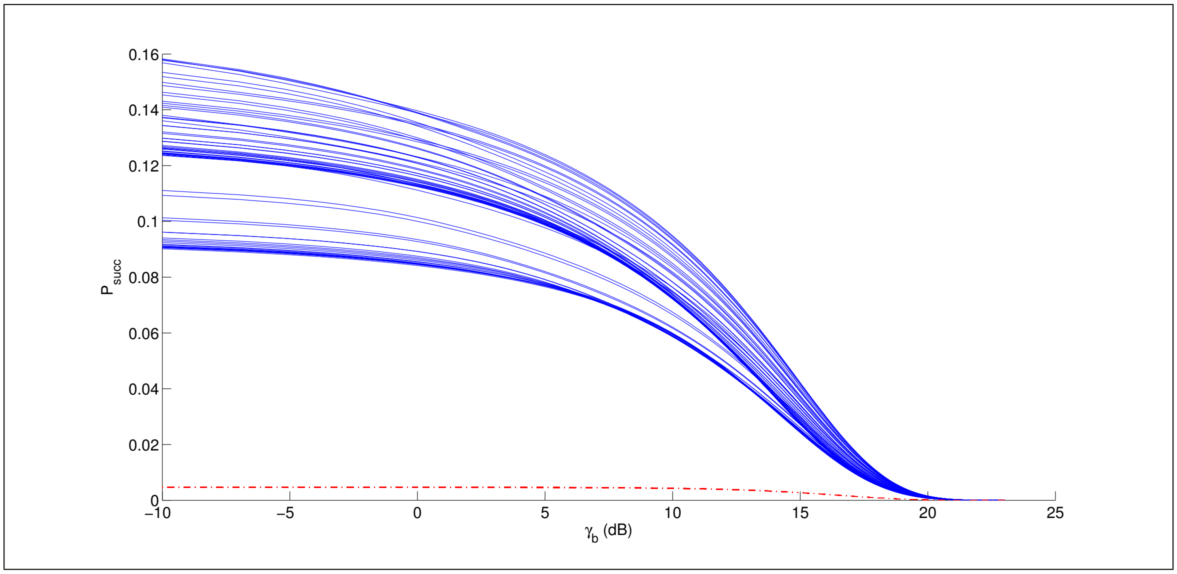
(b) Rician K-factor = 5 dB

Figure 3.4: Probability of Success vs Bob's threshold to decode a message for a fixed K, $\alpha = \pi/2$ rad and $n = 3.3$. Eve's threshold to decode a message, γ_e, is fixed at 1 dB. In these plots, the blue curve corresponds to the test case and the red curve corresponds to the base case. We observe that for the two channel conditions, one with Rayleigh fading and other with high K-factor, the test case is performing better than the base case for fixed α and n.

2. Varying SNR and α at fixed K and n:



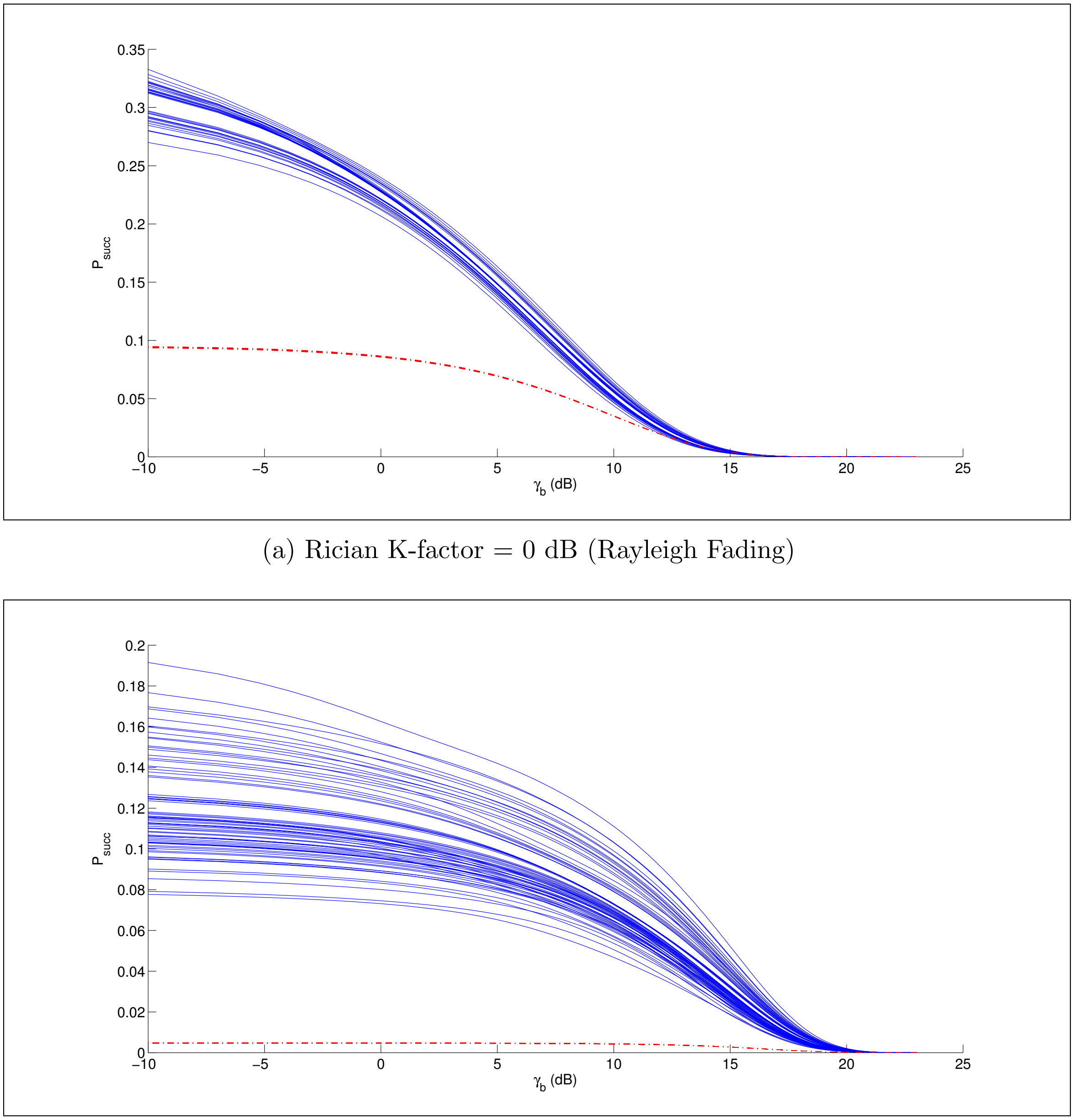
(a) Rician K-factor = 0 dB (Rayleigh Fading)



(b) Rician K-factor = 5 dB

Figure 3.5: Probability of Success vs Bob's threshold to decode a message for a fixed K, and $n = 3.3$. The phase difference, α is varied from $-\pi$ to π to generate separate plots and then superimposed on a single axis. Eve's threshold to decode a message, γ_e, is fixed at 1 dB. In these plots, the blue curve corresponds to the test case and the red curve corresponds to the base case. We observe that for the two channel conditions, one with Rayleigh fading and other with high K-factor, the test case is performing better than the base case for fixed n and varying α.

3. Varying SNR and n at fixed K and α:

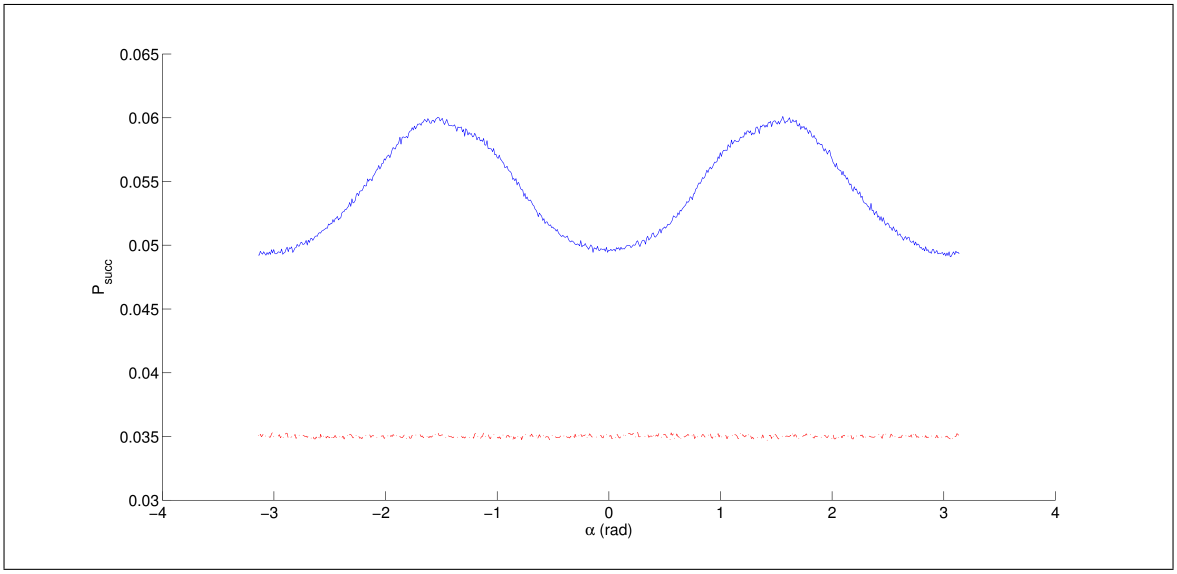


(a) Rician K-factor = 0 dB (Rayleigh Fading)

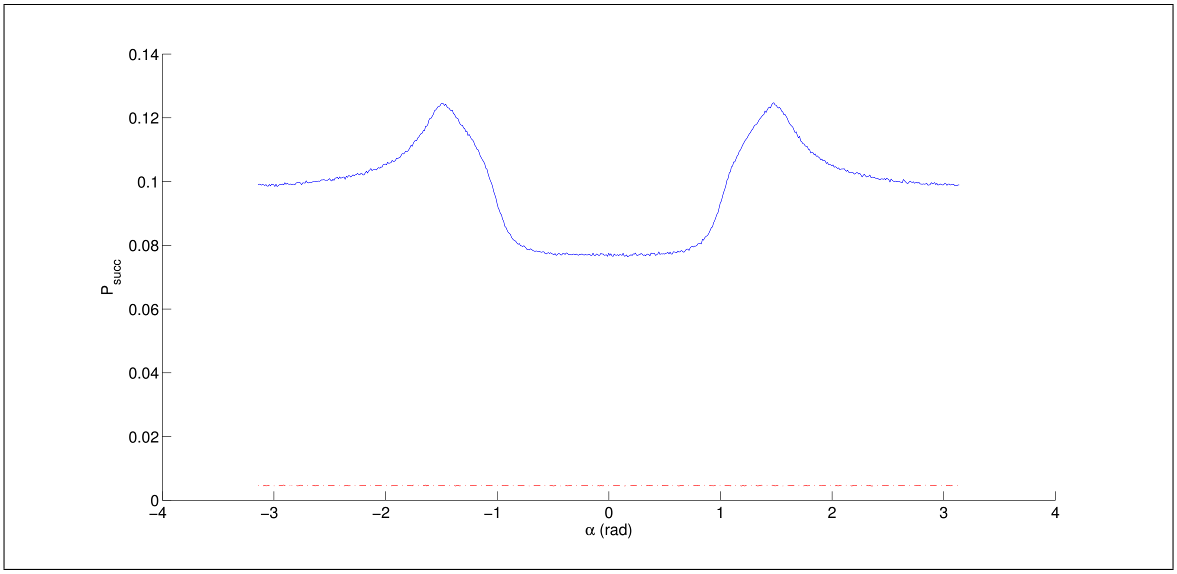
(b) Rician K-factor = 5 dB

Figure 3.6: Probability of Success vs Bob's threshold to decode a message for a fixed K, and $\alpha = \pi/2$. The separation of elements in the antenna array, n is varied from 0.5 to 4 wavelengths to generate separate plots and then superimposed on a single axis. Eve's threshold to decode a message, γ_e, is fixed at 1 dB. In these plots, the blue curve corresponds to the test case and the red curve corresponds to the base case. We observe that for the two channel conditions, one with Rayleigh fading and other with high K-factor, the test case is performing better than the base case for fixed α and varying n.

4. Varying α at fixed K, n and SNR:



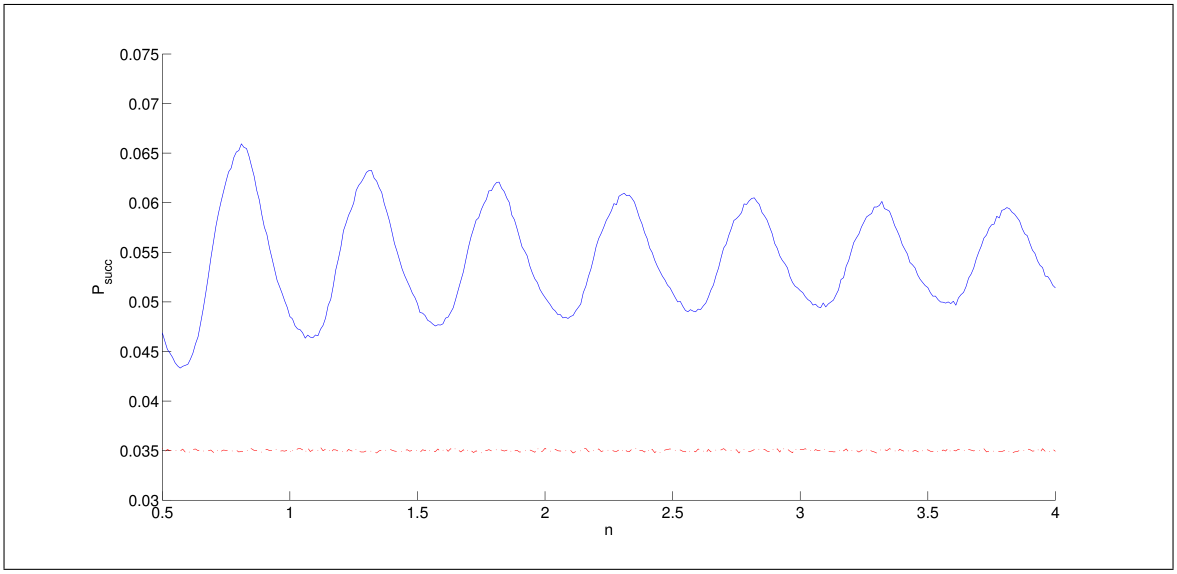
(a) Rician K-factor = 0 dB (Rayleigh fading) and $\gamma_b = 10$ dB.



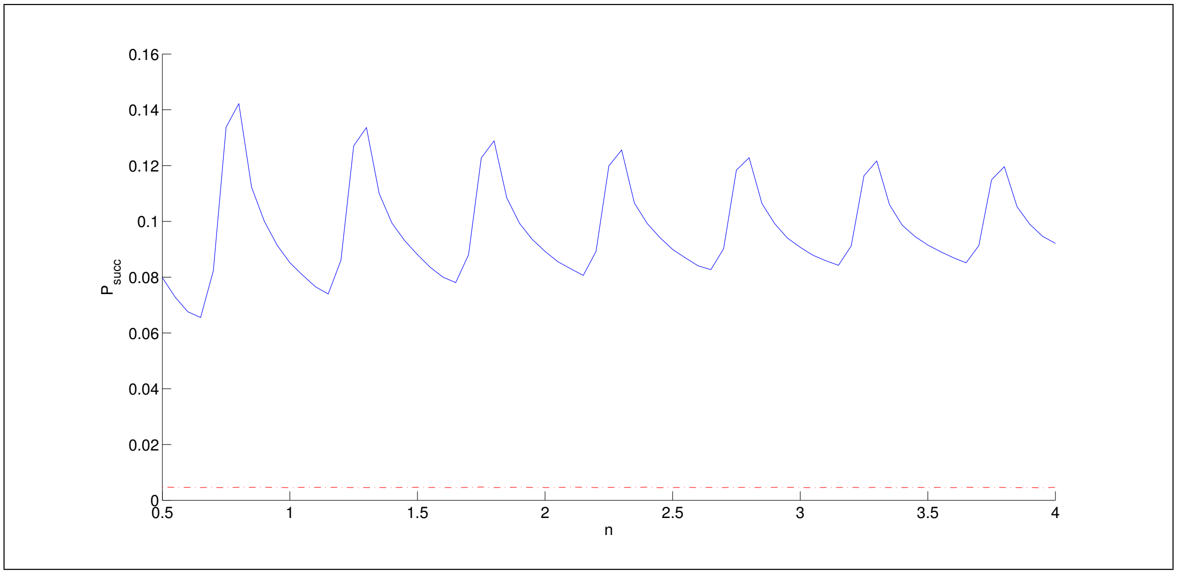
(b) Rician K-factor = 5 dB and $\gamma_b = 5$ dB.

Figure 3.7: Probability of Success vs phase difference in an antenna array for a fixed K, $n = 3.3$, and γ_b. Eve's threshold to decode a message, γ_e, is fixed at 1 dB. In these plots, the blue curve corresponds to the test case and the red curve corresponds to the base case. We observe that for the two channel conditions, one with Rayleigh fading and other with high K-factor, the test case is performing better than the base case for fixed n and γ_b.

5. Varying n at fixed K, α and SNR:



(a) Rician K-factor = 0 dB (Rayleigh fading) and γ_b = 10 dB.



(b) Rician K-factor = 5 dB and γ_b = 5 dB.

Figure 3.8: Probability of Success vs separation of elements in the antenna array for a fixed K, $\alpha = \pi/2$, and γ_b. Eve's threshold to decode a message, γ_e, is fixed at 1 dB. In these plots, the blue curve corresponds to the test case and the red curve corresponds to the base case. We observe that for the two channel conditions, one with Rayleigh fading and other with high K-factor, the test case is performing better than the base case for fixed α and γ_b.

6. Varying K at fixed n, α and SNR:

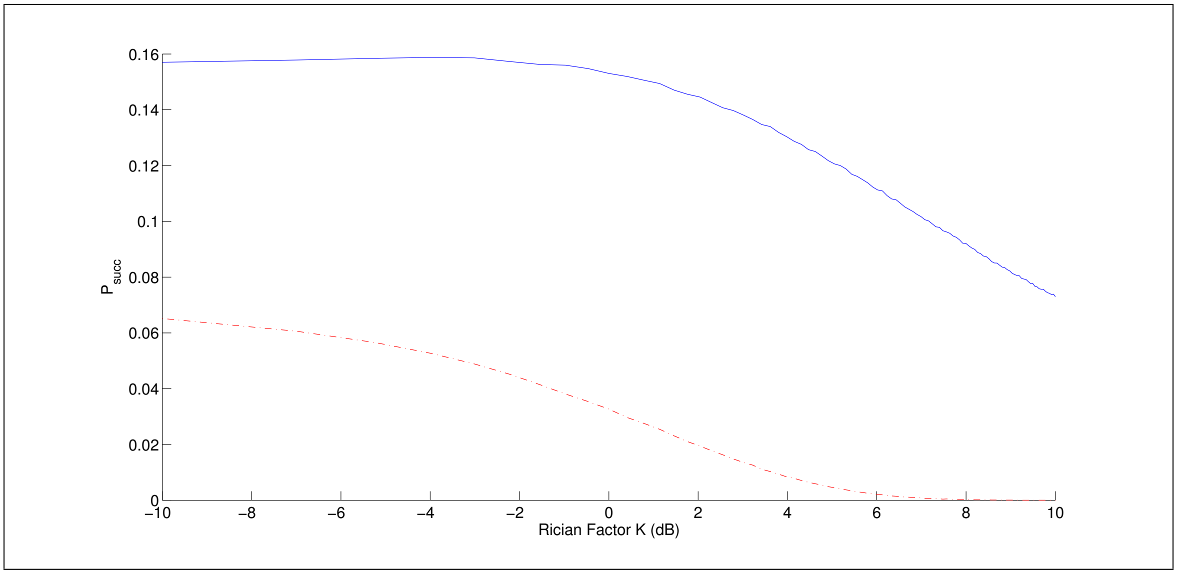
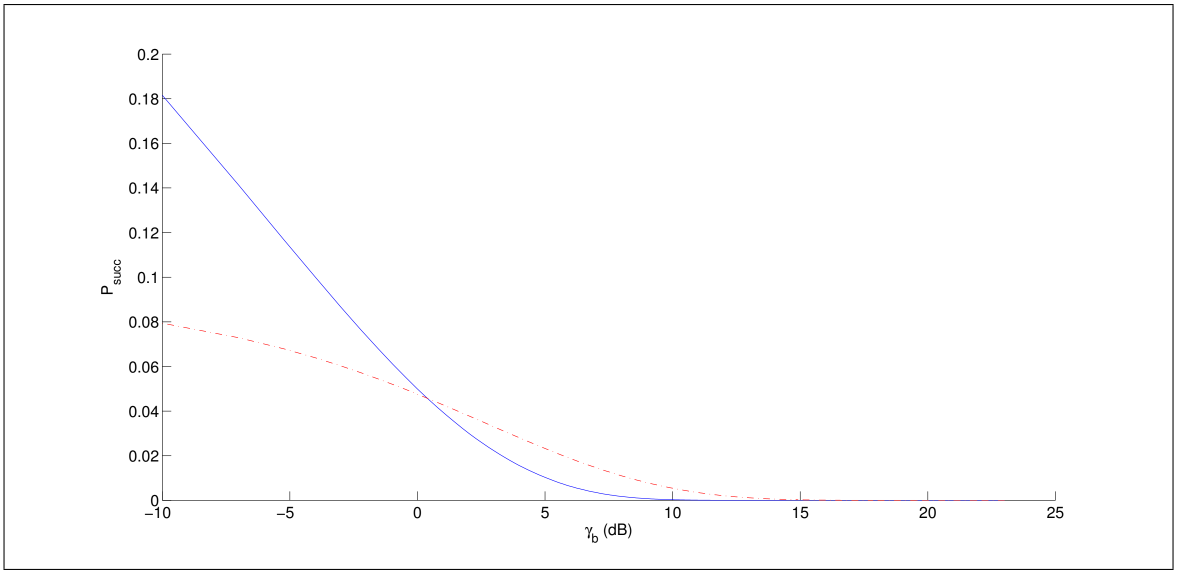


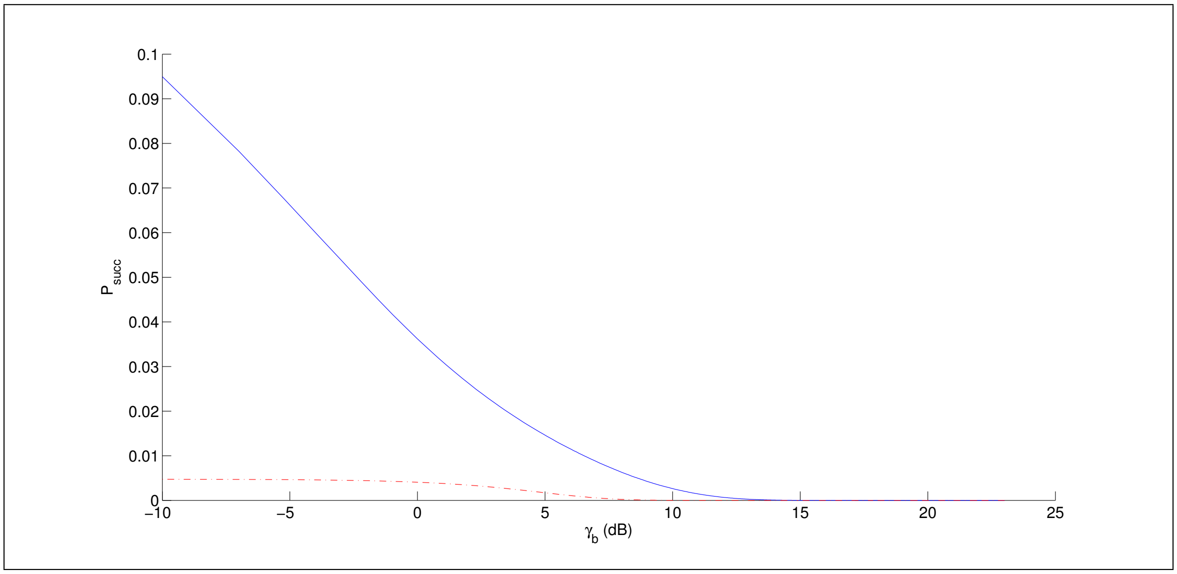
Figure 3.9: Probability of Success vs Rician K-factor for a fixed $n = 3.3$, and $\alpha = \pi/2$. Bob's threshold to decode a message, γ_b, is fixed at 5 dB. Eve's threshold to decode a message, γ_e, is fixed at 1 dB. In these plots, the blue curve corresponds to the test case and the red curve corresponds to the base case. We observe that when Eve is passive, the test case has a higher P_{succ} compared to the base case. At higher Rician K-factor, the fading channel becomes a noisy one and the base case completely fails whereas the test case still provides an advantage.

3.5.2 ActiveEve

1. Varying SNR at fixed K, α and n:



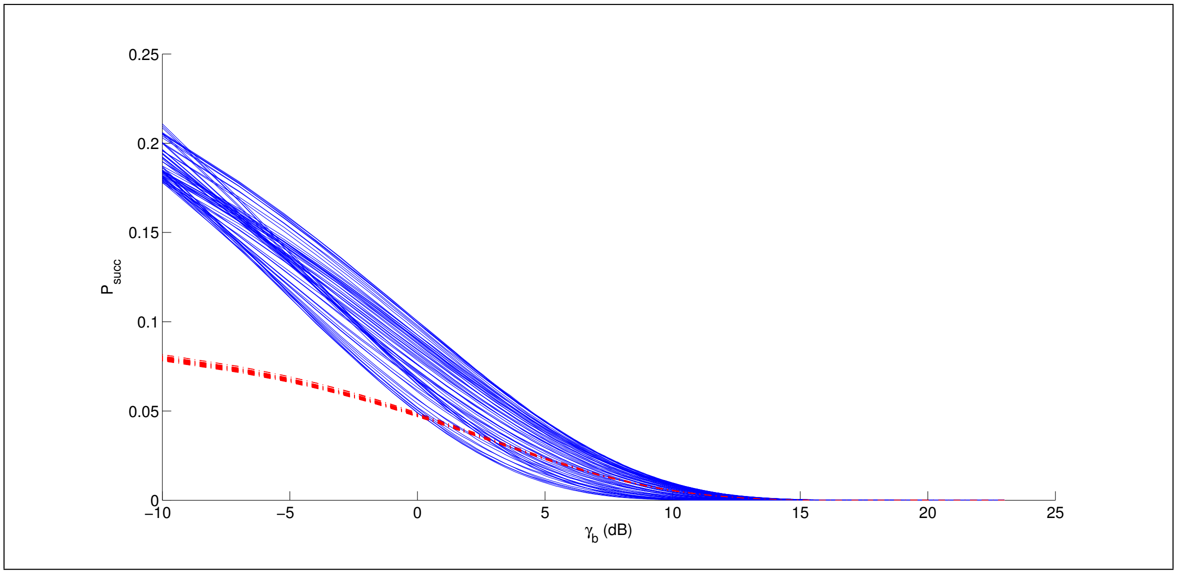
(a) Rician K-factor = 0 dB (Rayleigh fading)



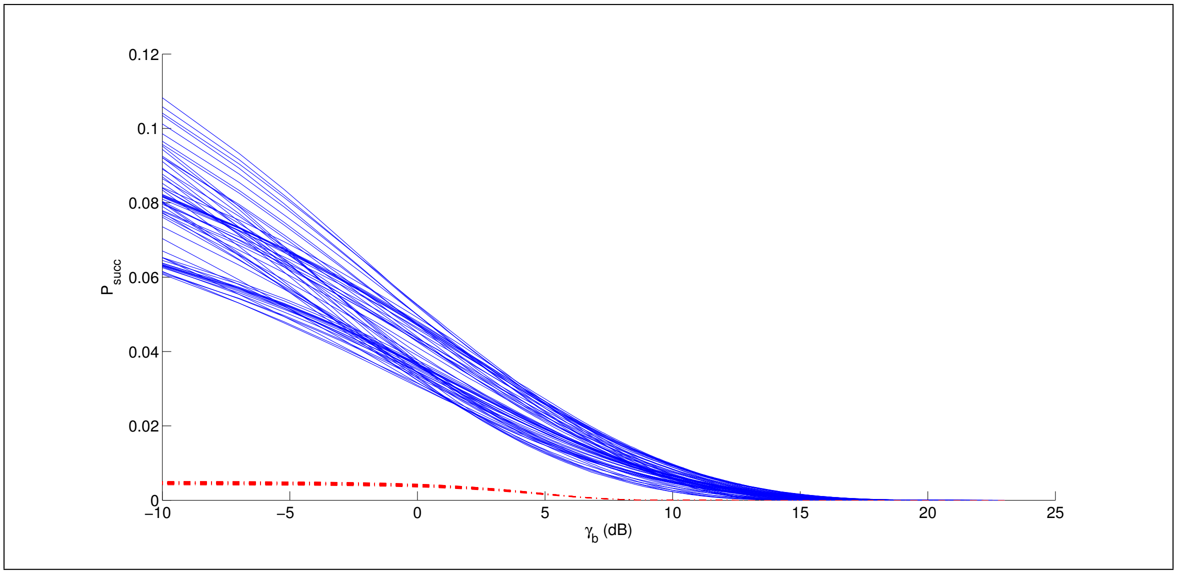
(b) Rician K-factor = 5 dB

Figure 3.10: Probability of Success vs Bob's threshold to decode a message for a fixed K, $\alpha = \pi/2$ rad and $n = 3.3$. Eve's threshold to decode a message, γ_e, is fixed at 1 dB. In these plots, the blue curve corresponds to the test case and the red curve corresponds to the base case. We observe that for the high K-factor, the test case has higher success than the base case. However, for Rayleigh fading channel, base case has more success than test case as γ_b increases.

2. Varying SNR and α at fixed K and n:



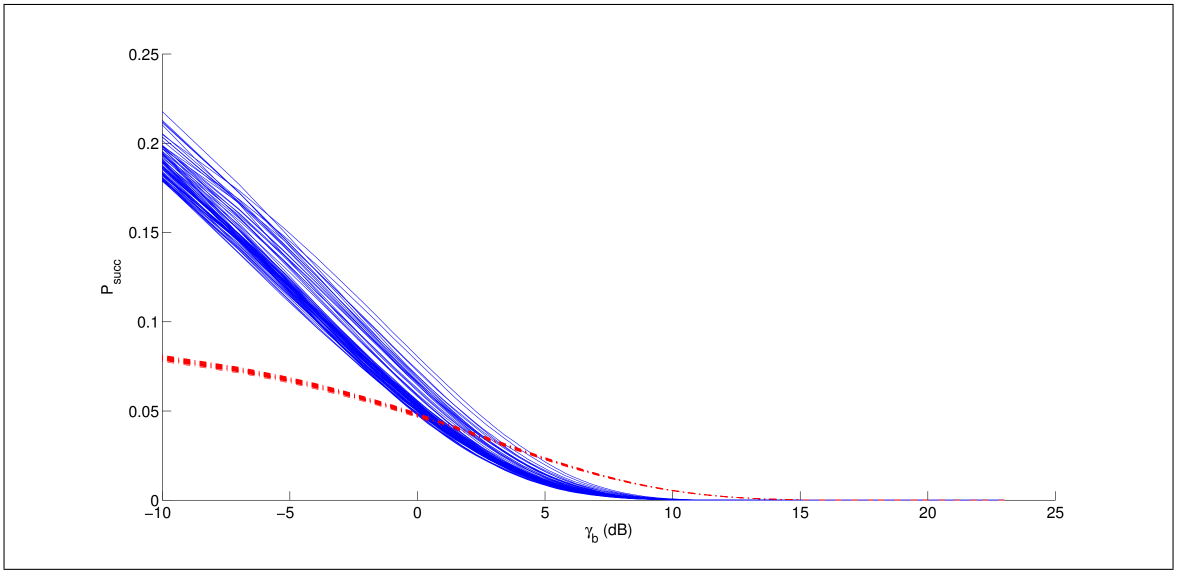
(a) Rician K-factor = 0 dB (Rayleigh fading)



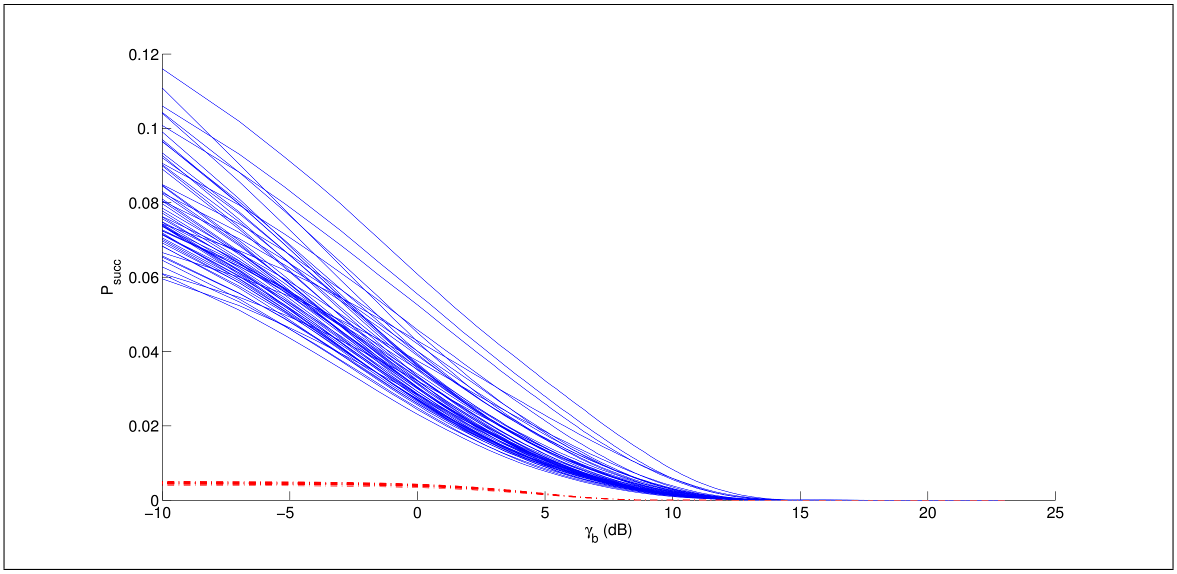
(b) Rician K-factor = 5 dB

Figure 3.11: Probability of Success vs Bob's threshold to decode a message for a fixed K, and $n = 3.3$. The phase difference, α is varied from $-\pi$ to π to generate separate plots and then superimposed on a single axis. Eve's threshold to decode a message, γ_e, is fixed at 1 dB. In these plots, the blue curve corresponds to the test case and the red curve corresponds to the base case. We observe that for the high K-factor, the test case has higher success than the base case. However, for Rayleigh fading channel, base case has more success than test case as γ_b increases.

3. Varying SNR and n at fixed K and α:



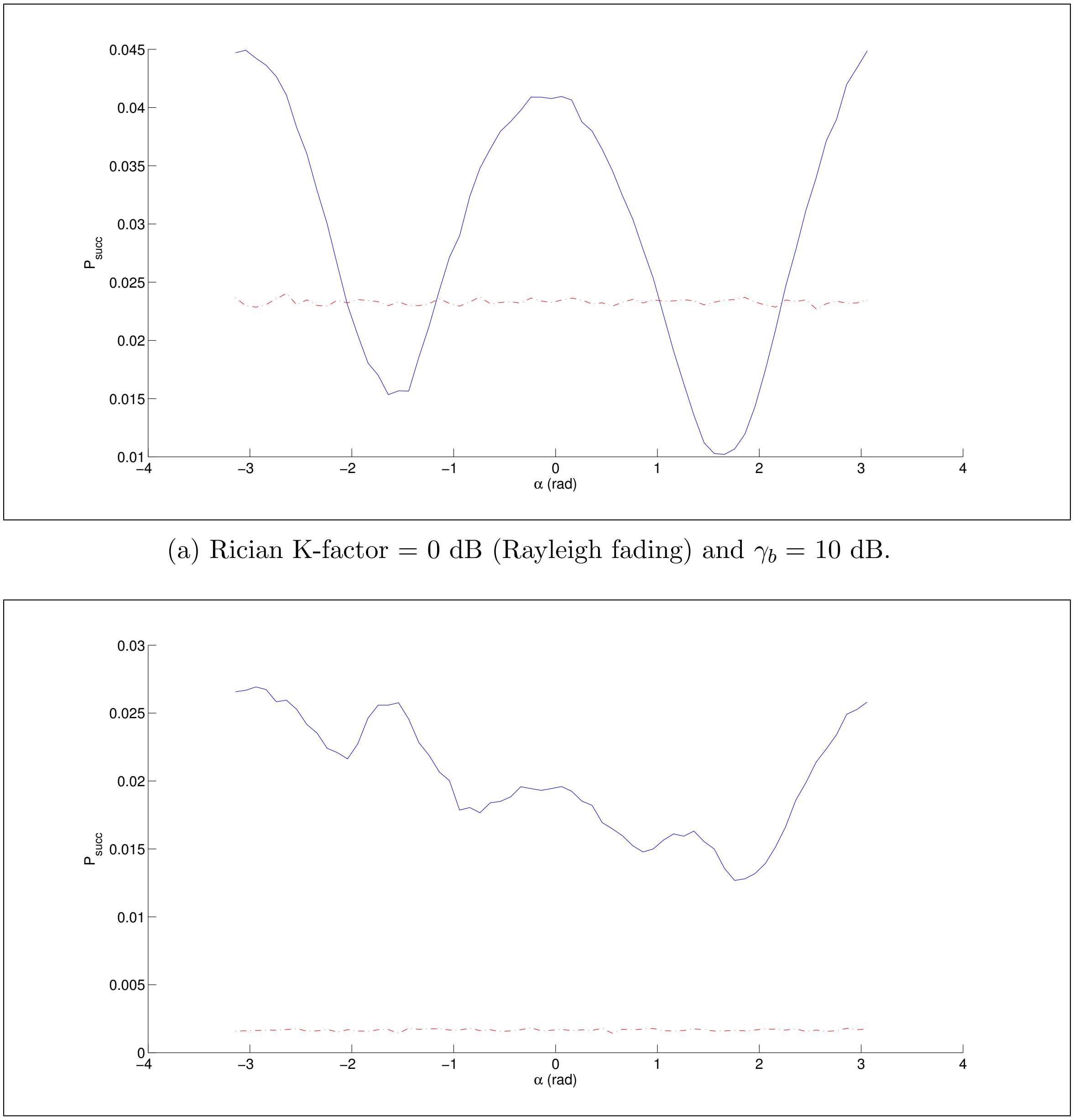
(a) Rician K-factor = 0 dB (Rayleigh fading)



(b) Rician K-factor = 5 dB

Figure 3.12: Probability of Success vs Bob's threshold to decode a message for a fixed K, and $\alpha = \pi/2$. The separation of elements in the antenna array, n is varied from 0.5 to 4 wavelengths to generate separate plots and then superimposed on a single axis. Eve's threshold to decode a message, γ_e, is fixed at 1 dB. In these plots, the blue curve corresponds to the test case and the red curve corresponds to the base case. We observe that for the high K-factor, the test case has higher success than the base case. However, for Rayleigh fading channel, base case has more success than test case as γ_b increases.

4. Varying α at fixed K, n and SNR:

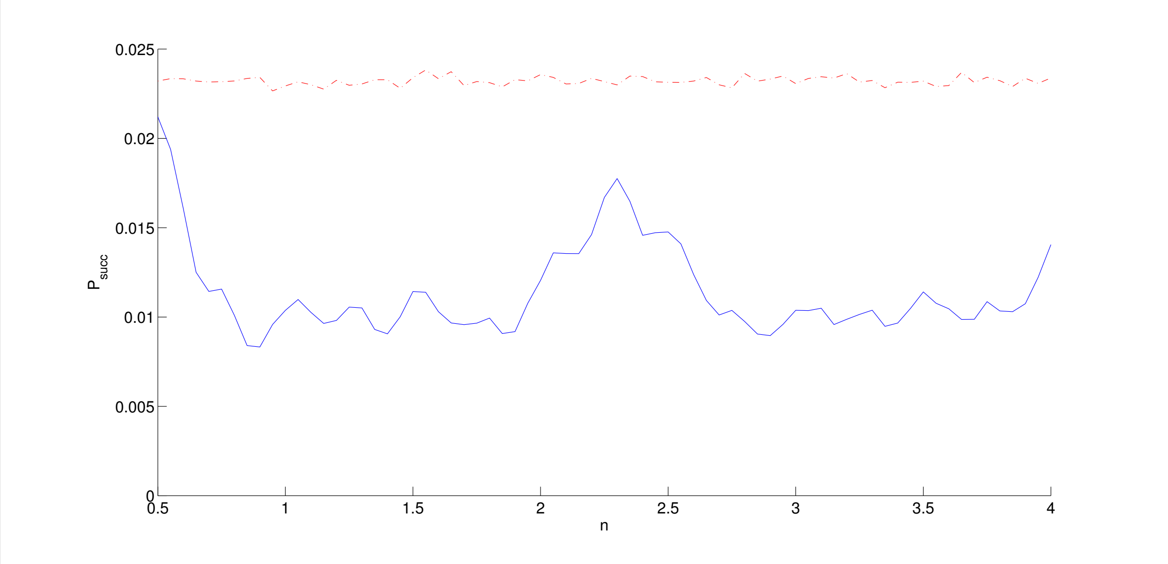


(a) Rician K-factor = 0 dB (Rayleigh fading) and $\gamma_b = 10$ dB.

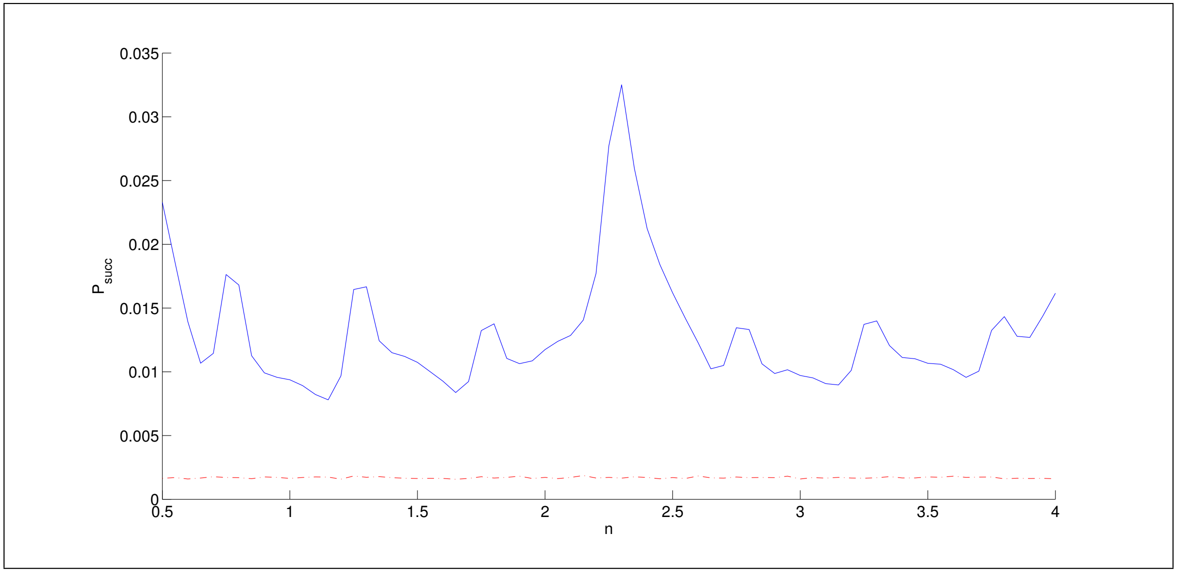
(b) Rician K-factor = 5 dB and $\gamma_b = 5$ dB.

Figure 3.13: Probability of Success vs phase difference in an antenna array for a fixed K, $n = 3.3$, and γ_b. Eve's threshold to decode a message, γ_e, is fixed at 1 dB. In these plots, the blue curve corresponds to the test case and the red curve corresponds to the base case. We observe that for the high K-factor, the test case has higher success than the base case. However, for Rayleigh fading channel, base case has more success than test case at some α ranges.

5. Varying n at fixed K, α and SNR:



(a) Rician K-factor = 0 dB (Rayleigh fading) and $\gamma_b = 10$ dB.



(b) Rician K-factor = 5 dB and $\gamma_b = 5$ dB.

Figure 3.14: Probability of Success vs separation of elements in the antenna array for a fixed K, $\alpha = \pi/2$, and γ_b. Eve's threshold to decode a message, γ_e, is fixed at 1 dB. In these plots, the blue curve corresponds to the test case and the red curve corresponds to the base case. We observe that for the high K-factor, the test case has higher success than the base case. However, for Rayleigh fading channel, base case has higher success than the test case.

6. Varying K at fixed n, α and SNR:

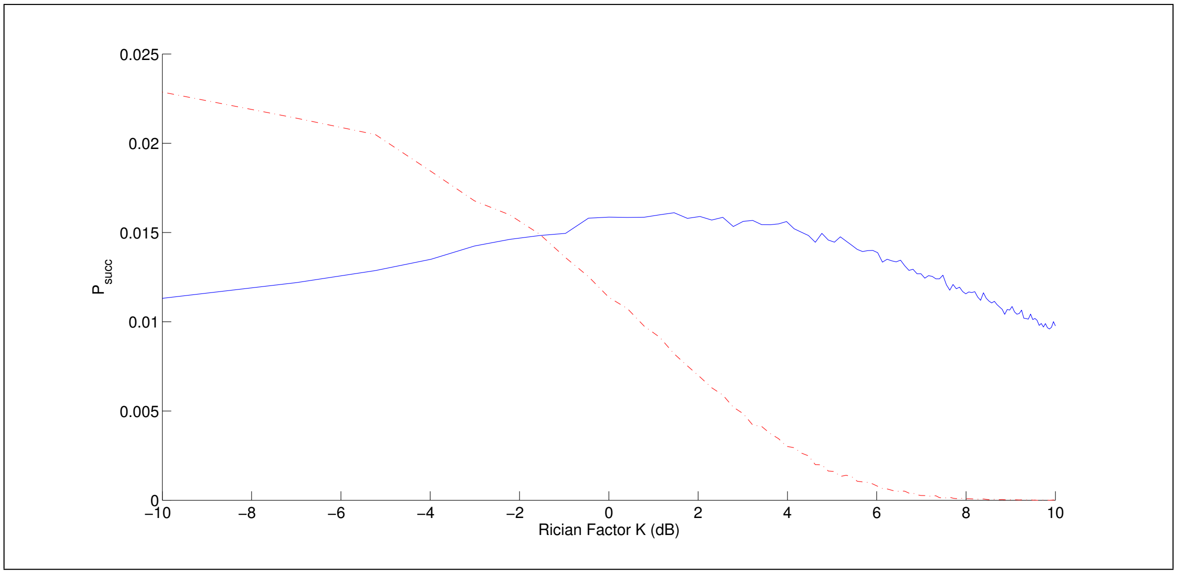


Figure 3.15: Probability of Success vs Rician K-factor for a fixed $n = 3.3$, and $\alpha = \pi/2$. Bob's threshold to decode a message, γ_b, is fixed at 5 dB. Eve's threshold to decode a message, γ_e, is fixed at 1 dB. In these plots, the blue curve corresponds to the test case and the red curve corresponds to the base case. We observe that when the K-factor is lower, the base case has more success than test case. However, as the K-factor increases and the channel becomes noisy, the base case is less successful than the test case.

CHAPTER 4
MEASUREMENTS

Indoor experiments were set up to supplement the analytical work. The measurements were conducted at two different locations: a laboratory and a classroom. These two locations provided an environment with minimal interference from moving objects e.g. a student walking through the environment. The laboratory provided a more congested environment compared to the classroom, as it is furnished with benches, cabinets, other lab equipment and the entrances to smaller rooms. The classroom is large and relatively empty with chairs stacked against one of the walls. Furthermore, the lab instruments being used for the experiments were automated in order to minimize corruption in data collection caused by human interference in the environment.

The goal is to measure the variation in the received signal strength when a varying-phase antenna array is used instead of a single antenna. Therefore, we ran two iterations of the same experiment; one using a single antenna system (Figure 4.1), and one using a two-element linear antenna array (Figure 4.2). We generate a single tone at 2.527 GHz using the signal generator and transmit it in the air using one of the two antenna systems. At the receiver, the signal is received by a single omni-directional antenna. All antennas employed were off-the-shelf TP-Link's 2.4GHz 8dBi Indoor Desktop Omni-directional Antennas that are readily available on the market. In order to prevent interference with the wide-band wifi signal, a slightly different frequency was chosen than 2.4 GHz.

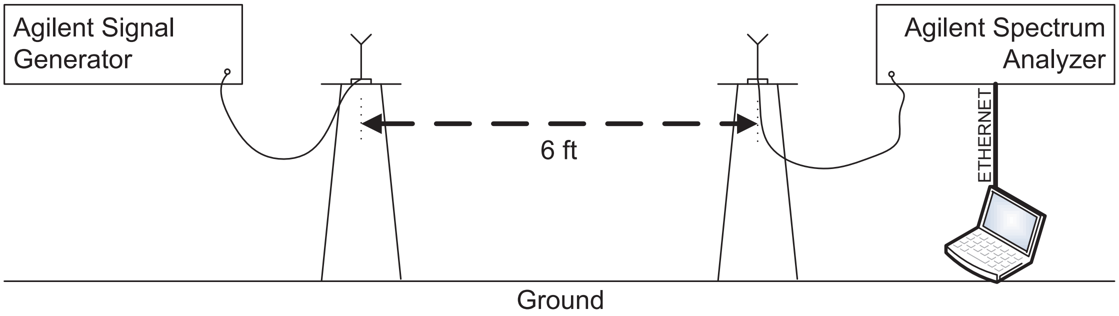


Figure 4.1: The configuration of the instruments to take measurements for the base case. A single antenna system was used in the base case.

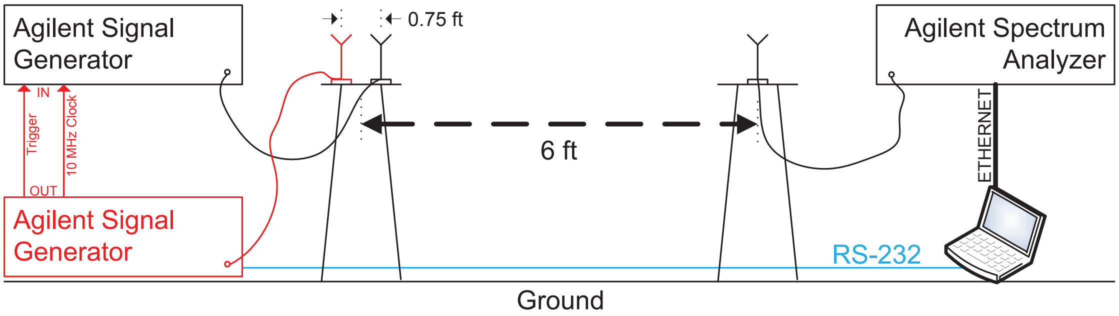


Figure 4.2: The configuration of the instruments to take measurements for the test case. A two-element linear antenna system was used in the test case. Compared to the base case, an extra signal generator was used and its clock was locked with the first generator.

Table 4.1: A summary of the different parameters configured while taking measurements.

No.	Parameter	Value
1.	Transmit Frequency	2.527 GHz
2.	Separation between antenna elements of the array	9 in
3.	Length of the antenna elements of the array	11.5 in
4.	Far field region of the antenna array	57 in
5.	Distance between transmitter and receiver in all cases	72 in
6.	Power of each antenna element (Test Case)	10 dBm
7.	Power of single omni-directional antenna (Base Case)	13 dBm
8.	Resolution bandwidth configured at spectrum analyzer	10 kHz

At the transmitter, Agilent E44xx Series signal generators were employed as they were readily available in the lab. One signal generator is sufficient for the single antenna case, but, in order to create a varying phase difference while using a phased array, another signal generator was required. In the later case, the two signal generators were phase locked and used the same clock reference. This was done by using the 10 MHz reference signal port and trigger port that are standard on such generators. The "10 MHz out" port of the first generator was connected to the "10 MHz" in port of the second generator. Similarly, the "trigger out" of the first generator was connected to the "trigger in" of the second generator using a standard coax cable. At the receiver, the antenna is connected to an Agilent Spectrum Analyzer. Since the signal generated is a single narrow-band tone, the resolution bandwidth of the spectrum analyzer is set to 10 kHz.

While using the phased array, certain physical parameters were kept constant during each measurement. The antenna separation of the phased array was fixed at 9 inches which corresponds to ($n =$)1.93 wavelengths. The longest dimension of the phased array was the antenna's length at 11.5 inches; hence, the far field radius ($2L^2/\lambda$) was calculated to be around 57 inches. Hence, the transmitter and receiver were placed 72 inches apart with an unobstructed line-of-sight (LOS) path.

This distance ensured that the receiver lied in the far field of the transmitter. We ensured that a LOS path was present to reduce the effects of multi-path fading in our measurements and, per Chapter 2, test the case of most interest. Moreover, the antenna systems were placed on stools of the same size to prevent reflections caused by proximity to the ground that might have otherwise increased the effect of multi-path fading. For the phased array, the amplitude of the signal at each antenna was fixed at 10 dBm. While running the case with the single antenna system, the amplitude was doubled (13 dBm) to account the added gain of using two antennas. Moreover, while comparing both systems, it was ensured that the single antenna was placed at the mid-point of the two-antenna system. Table 4.1 provides a summary of this configuration.

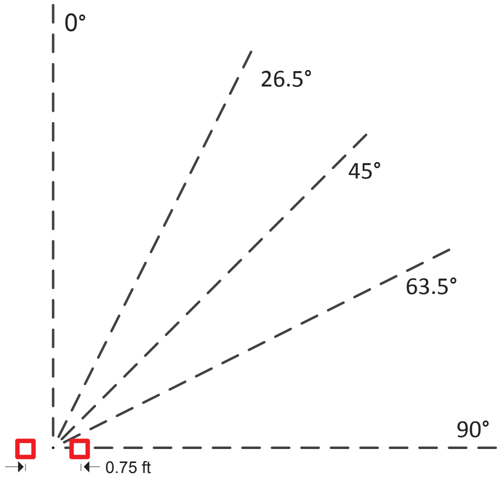


Figure 4.3: This figure show the five positions (1-5) of the receiver with respect to the transmitter (red) where data was collected for the both cases.

The process of generating a random phase at the transmitter and collecting data samples at the receiver was automated to prevent human error. Moreover, it ensured that no extra reflections were added while taking measurements. Five data sets for each case at each location were collected by placing the receiver at 0°, 26.5°, 45°, 63.5° and 90° (positions $1 - 5$ as shown in Figure 4.3) of the deployed antenna system. The perpendicular bisector of the imaginary line joining the two transmit antennas in the azimuth plane was taken as the reference axis. At each position, 5000 samples were collected over a duration of 30 minutes. A scripting language, python, was used for this purpose. Appendix A provides the python code used for this setup. Moreover, python was also used for generating a random phase from $(-\pi, \pi)$ and applying it to one of the generators while using the two-antenna system. Appendix A also contains the python code used for this process. Moreover, in this case, the randomly varying phase difference was applied independently of the data collection process.

Figure (4.4) shows two plots on together. The one on top shows the signal strength of the received signal of both antenna systems, whereas the second plot is the phased-array antenna system data at the same position in the form of a histogram to show the variation of the RSSI. The blue signal represents the samples collected from a two-antenna phased array system while the red signal represents a single antenna system at the transmitter. Similarly, Figures (4.5) to (4.8) show measurement results of positions 2-5 inside the laboratory. To make it easier to draw a comparison, all figures have the same set of axes.

From this data, it is evident that the two-antenna array with varying phase provides more variation in the signal strength compared to the single antenna system. Moreover, the variation in the received signal strength across different locations is not the same. For example, the standard deviation of the signal strength with the varying phase antenna array system at position 4 is 6.45 dB whereas at position 1 it is 4.45 dB. For the single antenna system, it is 0.15 dB at position 4 and 0.21 dB at position 1.

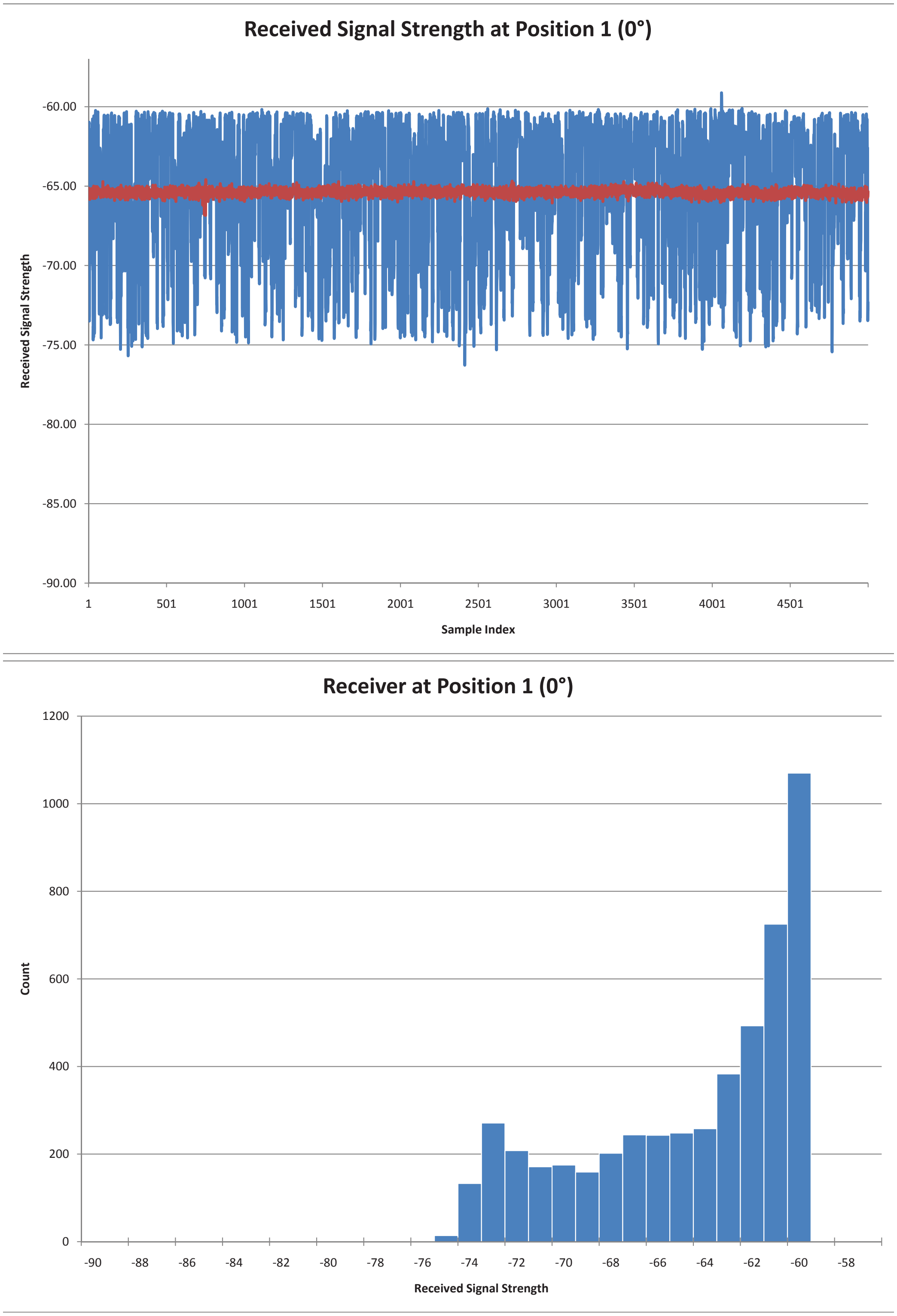


Figure 4.4: Received Signal at Position 1 (0°) of the Laboratory. **Top:** Blue represents RSSI measurements using two-antenna phased array while red represents the RSSI measurements using a single antenna. **Bottom:** Histogram showing variation of the data samples collected for two-antenna phased array system

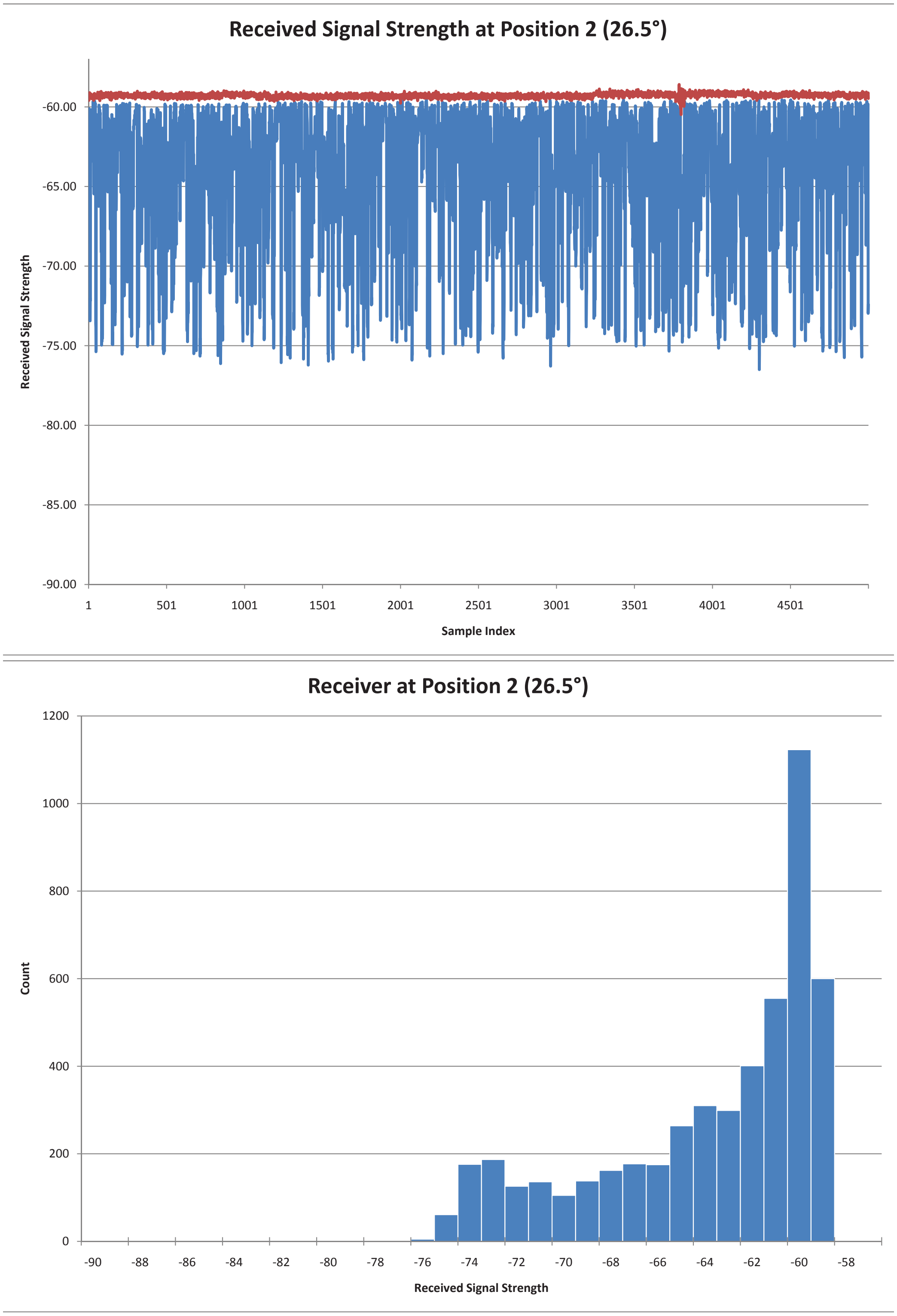


Figure 4.5: Received Signal at Position 2 (26.5°) of the Laboratory. **Top:** Blue represents RSSI measurements using two-antenna phased array while red represents the RSSI measurements using a single antenna. **Bottom:** Histogram showing variation of the data samples collected for two-antenna phased array system

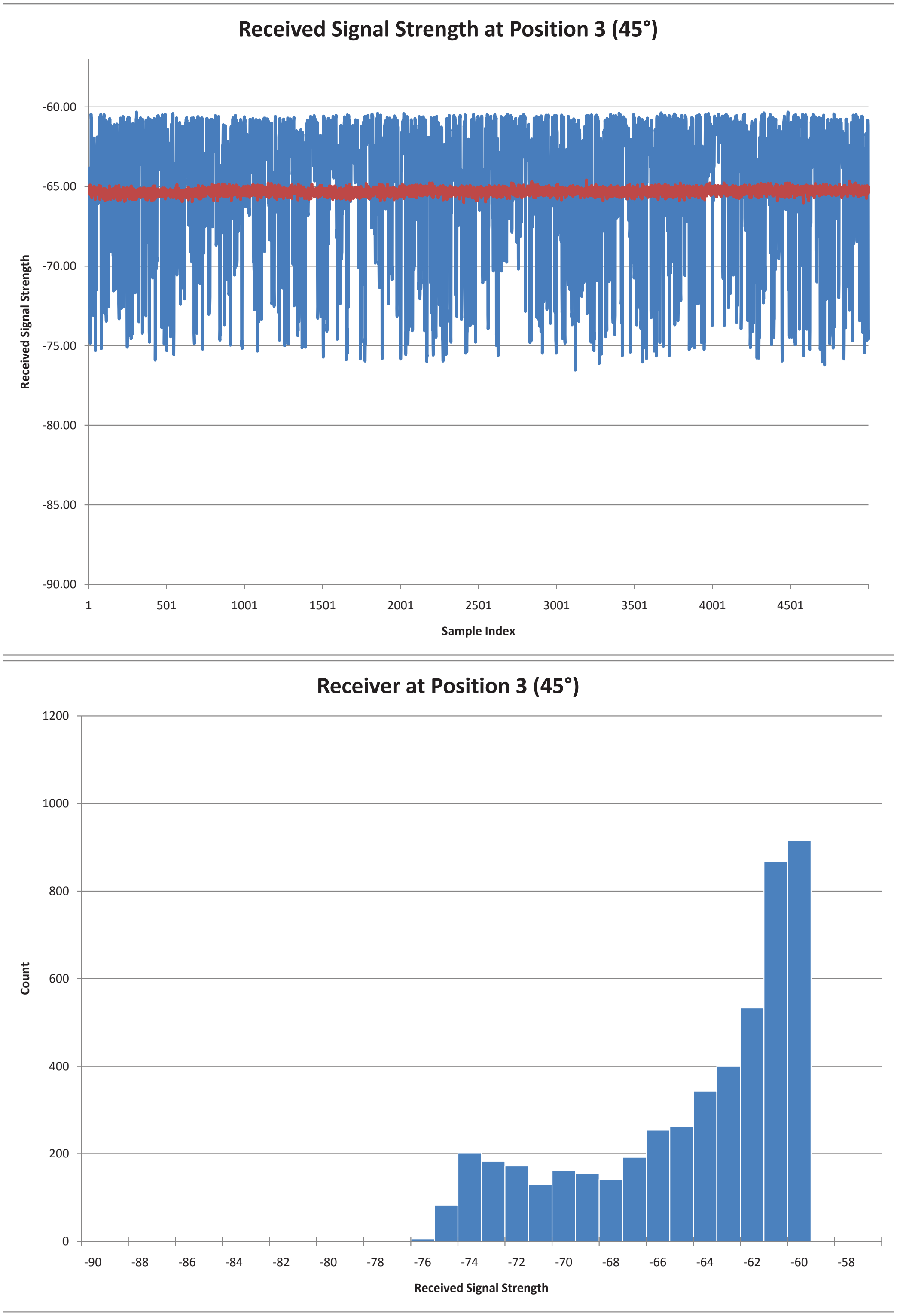


Figure 4.6: Received Signal at Position 3 (45°) of the Laboratory. **Top:** Blue represents RSSI measurements using two-antenna phased array while red represents the RSSI measurements using a single antenna. **Bottom:** Histogram showing variation of the data samples collected for two-antenna phased array system

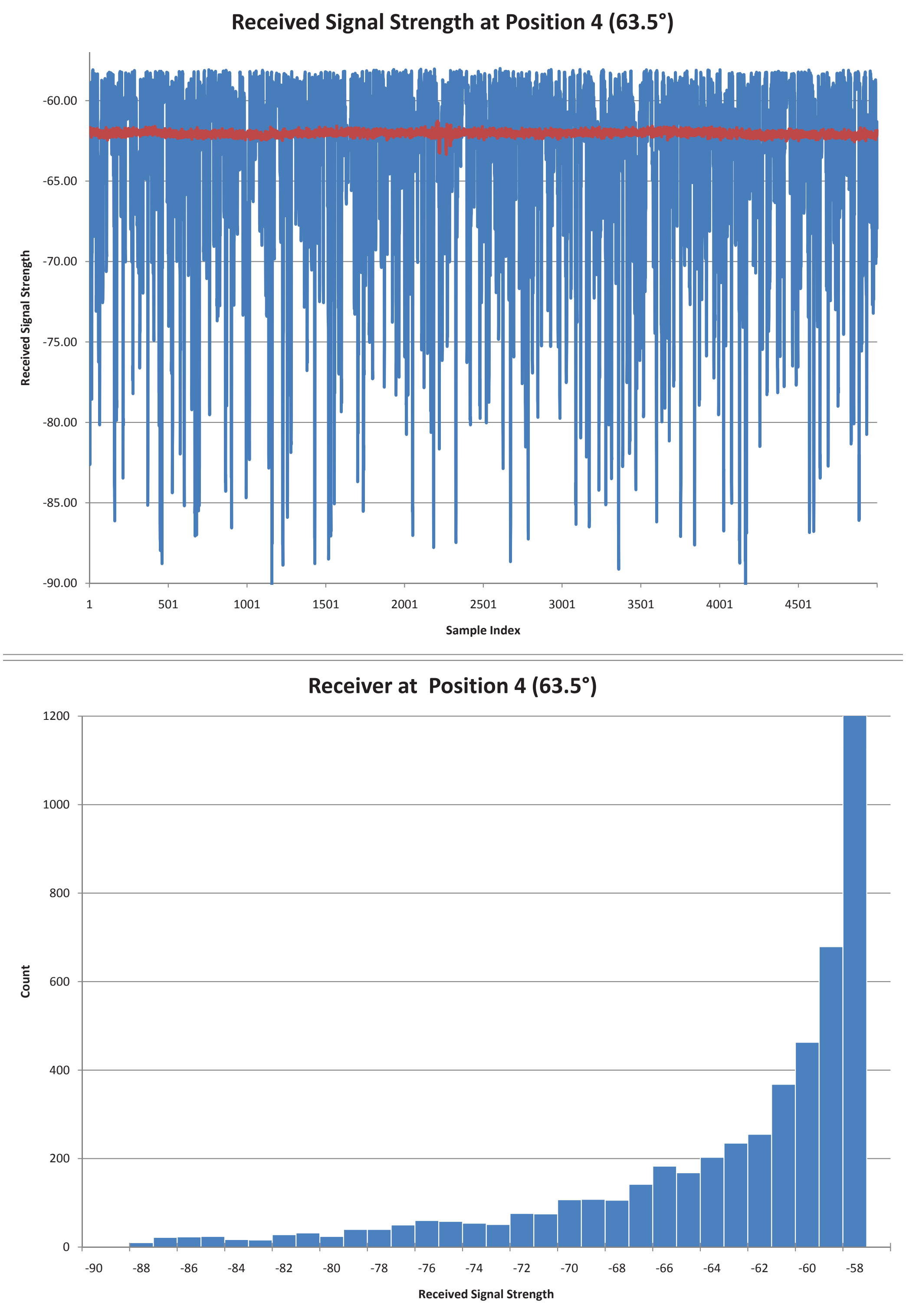


Figure 4.7: Received Signal at Position 4 (63.5°) of the Laboratory. **Top:** Blue represents RSSI measurements using two-antenna phased array while red represents the RSSI measurements using a single antenna. **Bottom:** Histogram showing variation of the data samples collected for two-antenna phased array system

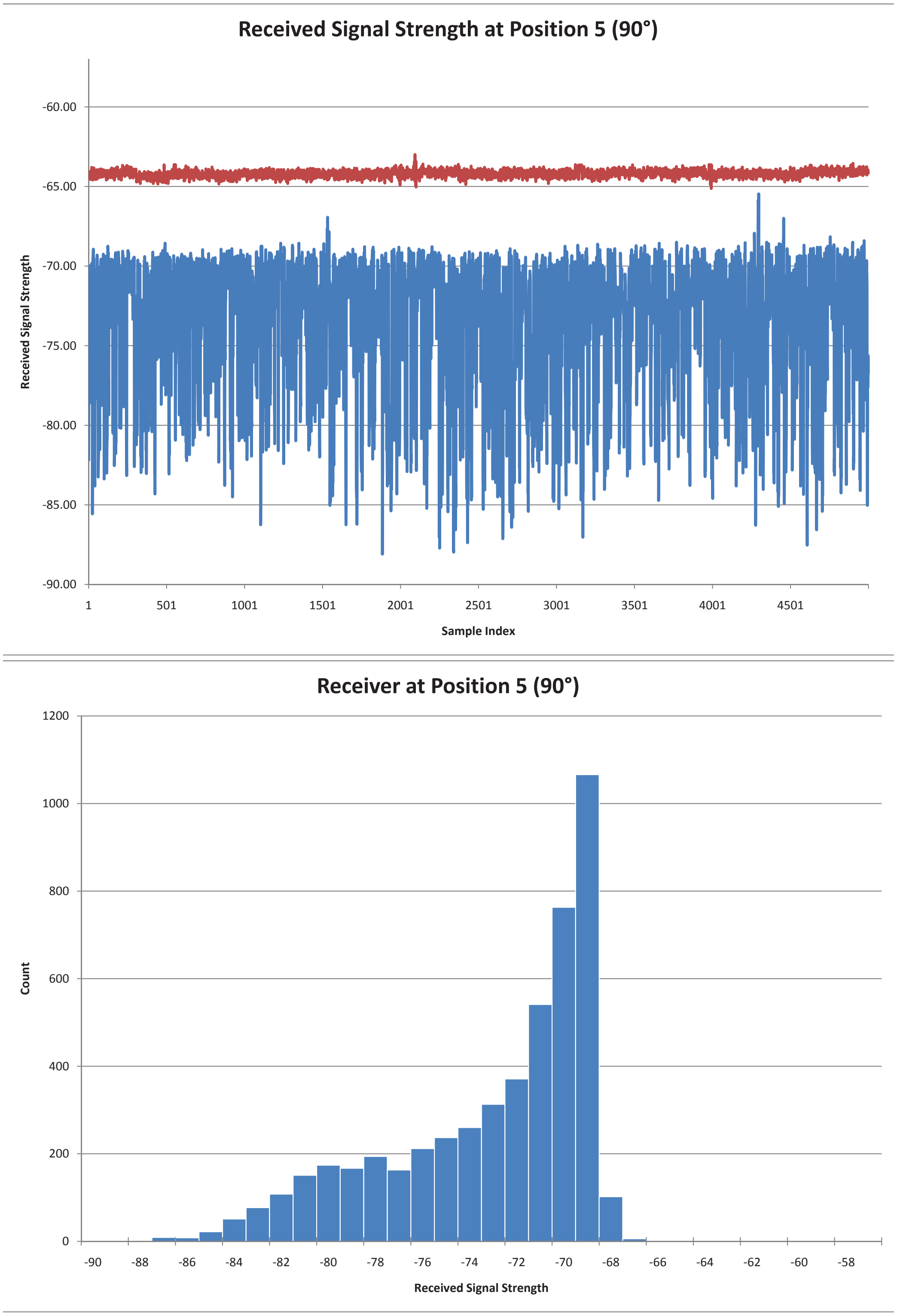


Figure 4.8: Received Signal at Position 5(90°) of the Laboratory. **Top:** Blue represents RSSI measurements using two-antenna phased array while red represents the RSSI measurements using a single antenna. **Bottom:** Histogram showing variation of the data samples collected for two-antenna phased array system

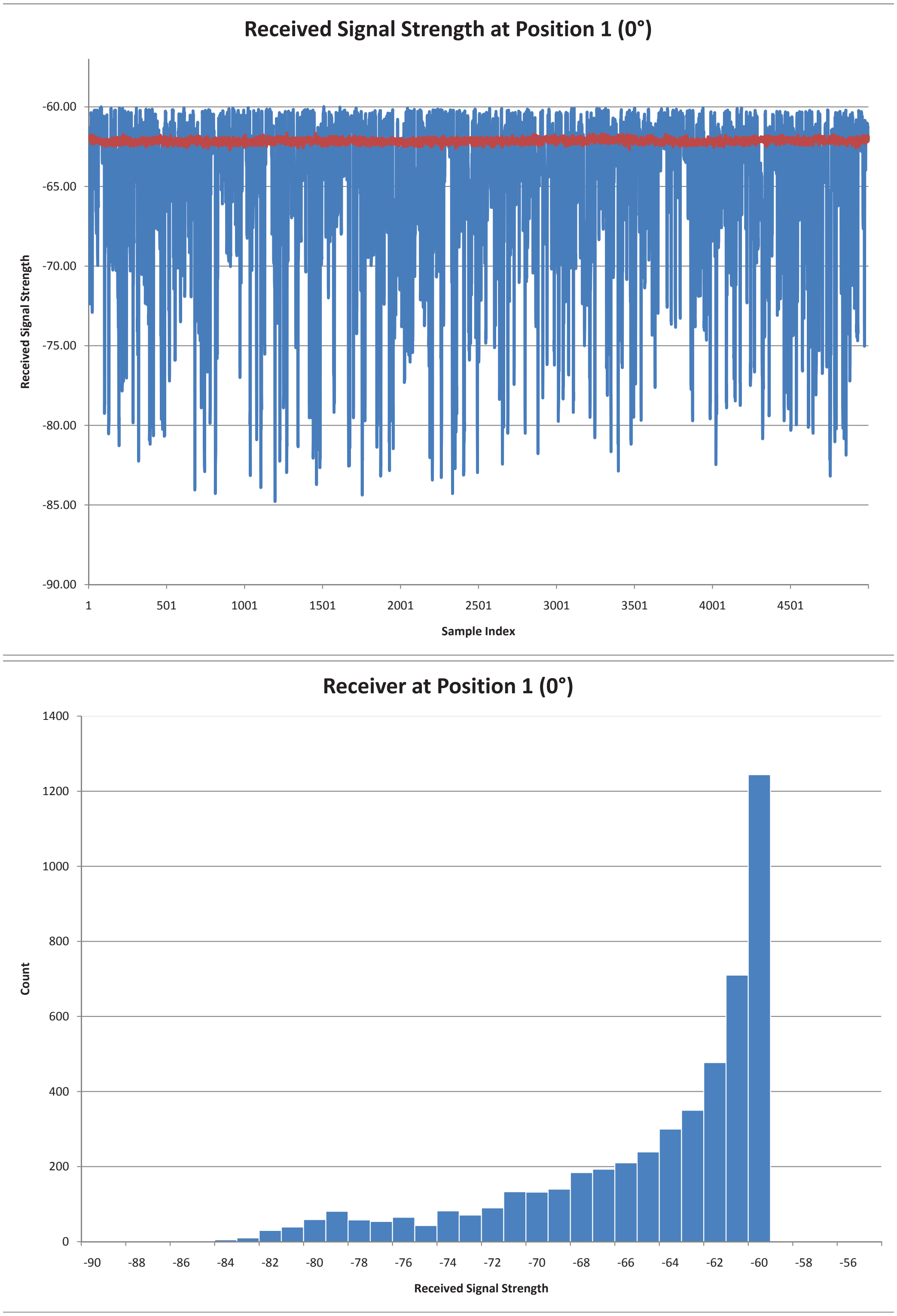
For the laboratory environment, we “roughly” estimated the Rician factor and found it to be at least 11 dB i.e. the LOS signal was always the dominant path of the static Rician multi-path fading environment. The signal strength was directly measured with the line-of-sight intact. Then, an obstacle with RF absorbing properties is placed in the middle of the transmitter and receiver to break the line-of-sight, and the received signal strength is noted. The Rician K-factor is thus calculated using these two values.

$$\text{K-factor} = \frac{E[\text{Power of the dominant LOS path}]}{E[\text{Power of all other reflected paths}]}$$

The experiment was repeated in the less congested environment of a large classroom. Figures (4.9) to (4.13) show the result of these measurements. Similar to the previous data set, it shows two plots where the first plot shows the comparison between the two-antenna array (blue) and the single antenna (red) whereas the second plot shows the variation of the two-antenna array data-set. For this data-set, we see that the standard deviation of the two-antenna system is 2.27 dB at position 4 whereas it is 5.65 at position 1. On the other hand, for the single antenna system, the standard deviation is 0.16 dB and 0.14 dB at position 4 and position 1, respectively.

There are some observations that we can draw from the two sets of measurements. Firstly, the two-antenna phase array provides more radiation variation in comparison to the single antenna system. The standard deviation, calculated by joining the two data sets, of the varying phase two-antenna system is 5.38 dB whereas the standard deviation of the single antenna system is 1.78 dB (It is important to note here that this is calculated by combining all 50,000 samples. That is why we are seeing a 1.78 dB standard deviation rather than 0.2 dB standard deviation that we had observed earlier.). Secondly, this variation in signal strength is not attributed to position/angle of incidence. The standard deviation of the variation of the antenna array at Position 4 of the laboratory (6.45 dB) is not the same as the standard deviation at Position 4 of the classroom(2.27 dB). Thirdly, it is possible that a certain position in a location may generate results deviating from the norm (e.g. Position 5 of the classroom). This can be attributed to a strong reflector in the vicinity or other geometrical properties of the environment.

Lastly, we can draw an assumption regarding the efficiency of varying phase two-antenna arrays over single antenna systems using these results. The environment in which we took our measurements has a very high Rician factor, which suggests that the environment is nearly an AWGN channel. In other words, it presents a worst-case scenario where multi-path fading plays a minor role in creating randomness in the channel. Thus, our results show that even in a static and less dynamic environment, we are able to generate artificial randomness.


Received Signal Strength at Position 1 (0°)

Receiver at Position 1 (0°)

Figure 4.9: Received Signal at Position 1 (0°) of the Classroom. **Top:** Blue represents RSSI measurements using two-antenna phased array while red represents the RSSI measurements using a single antenna. **Bottom:** Histogram showing variation of the data samples collected for two-antenna phased array system

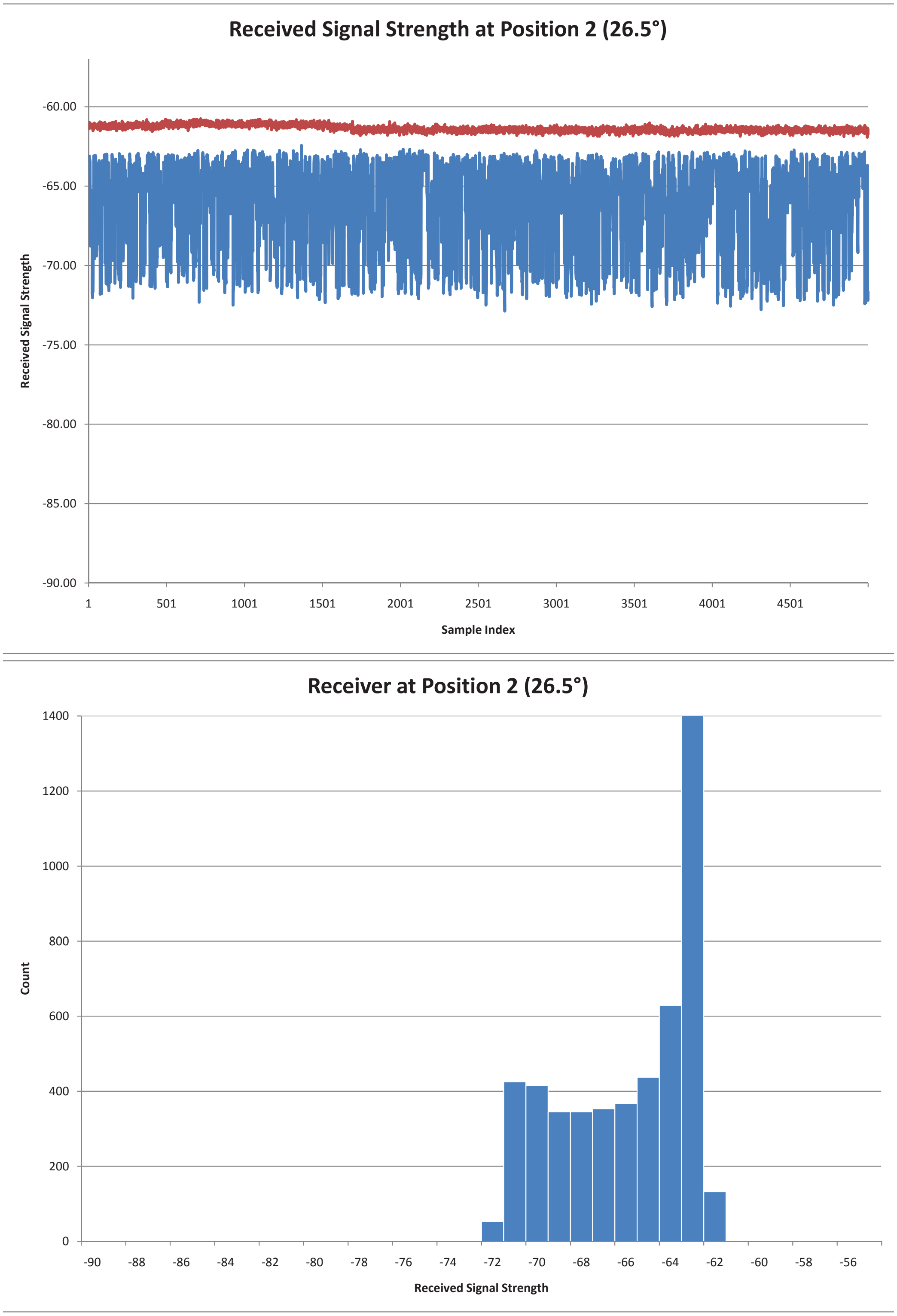


Figure 4.10: Received Signal at Position 2 (26.5°) of the Classroom. **Top:** Blue represents RSSI measurements using two-antenna phased array while red represents the RSSI measurements using a single antenna. **Bottom:** Histogram showing variation of the data samples collected for two-antenna phased array system

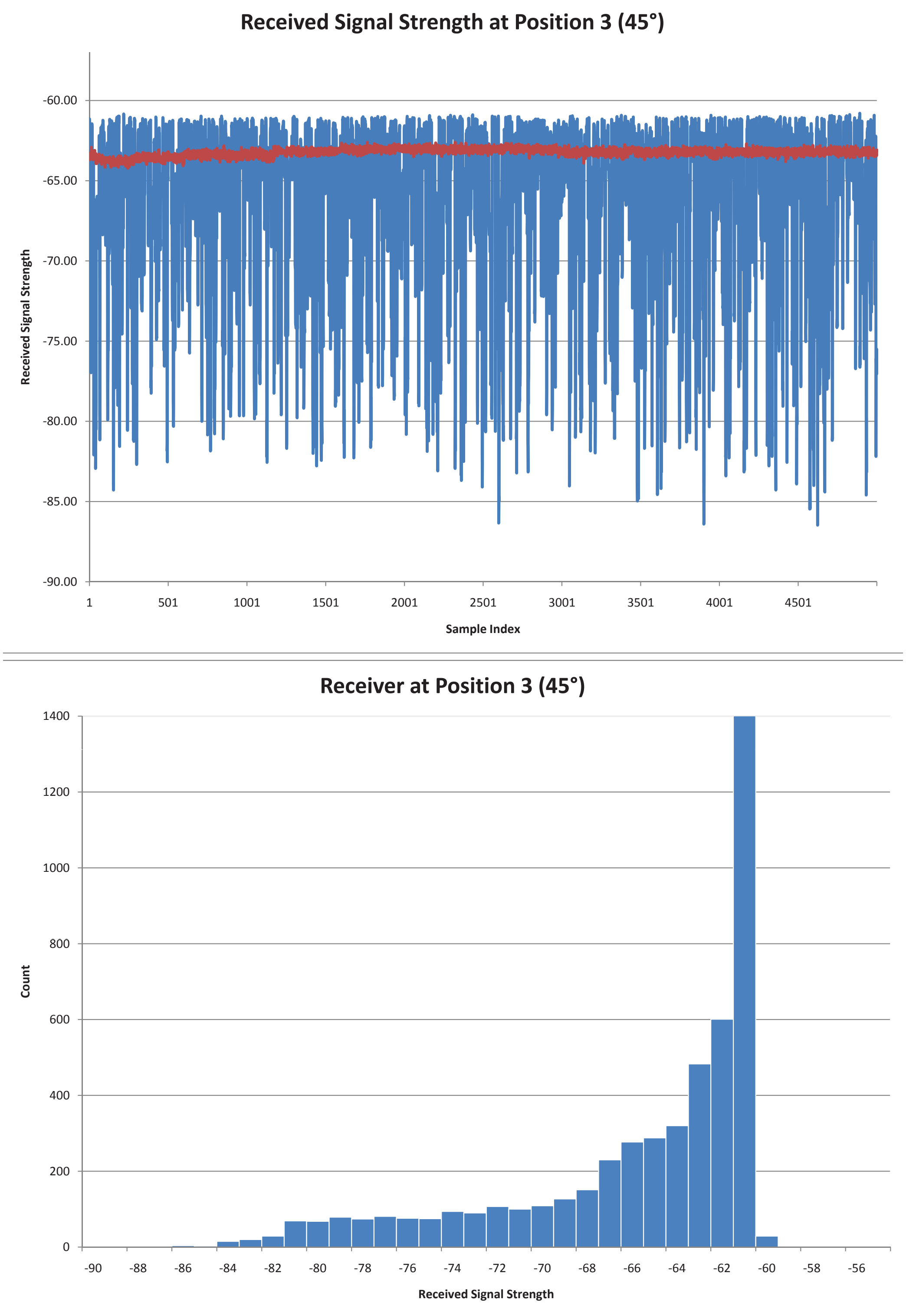
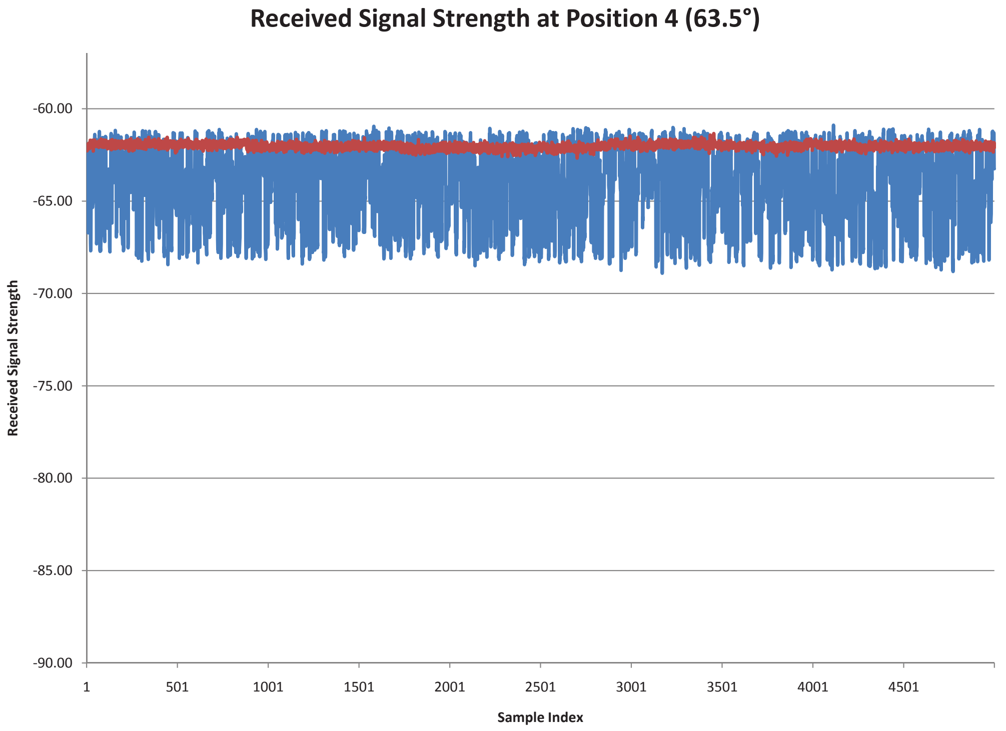


Figure 4.11: Received Signal at Position 3 (45°) of the Classroom. **Top:** Blue represents RSSI measurements using two-antenna phased array while red represents the RSSI measurements using a single antenna. **Bottom:** Histogram showing variation of the data samples collected for two-antenna phased array system



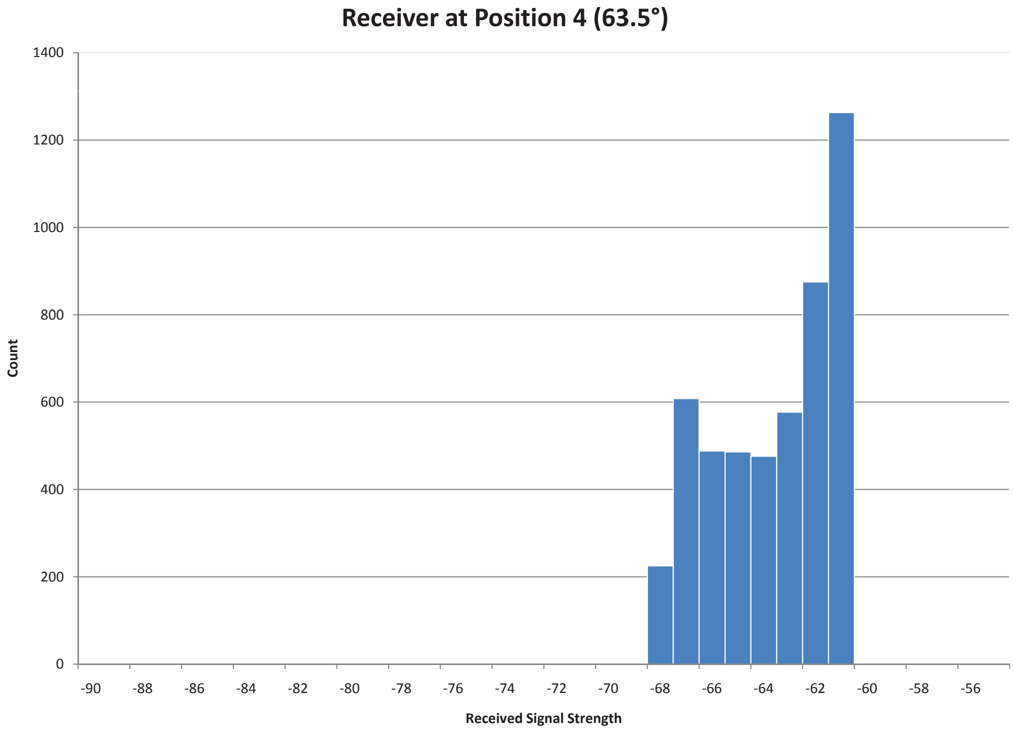


Figure 4.12: Received Signal at Position 4 (63.5°) of the Classroom. **Top:** Blue represents RSSI measurements using two-antenna phased array while red represents the RSSI measurements using a single antenna. **Bottom:** Histogram showing variation of the data samples collected for two-antenna phased array system

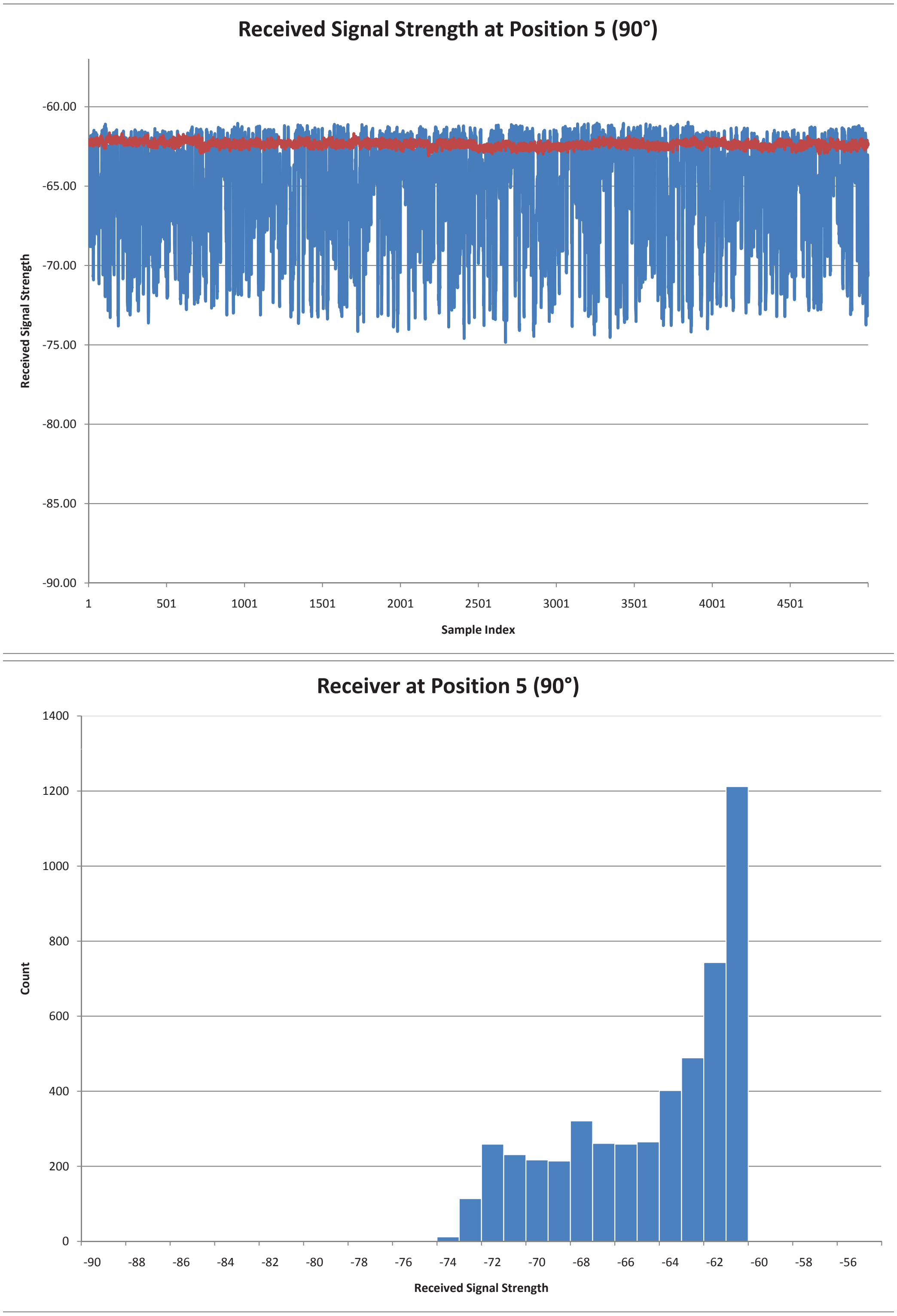


Figure 4.13: Received Signal at Position 5 (90°) of the Classroom. **Top:** Blue represents RSSI measurements using two-antenna phased array while red represents the RSSI measurements using a single antenna. **Bottom:** Histogram showing variation of the data samples collected for two-antenna phased array system

CHAPTER 5

IMPROVEMENT OF DYNAMIC SECRETS

In Section 2.3, we reviewed the “Dynamic Secrets” [2] algorithm. Recall that the algorithm relies on information loss due to randomness in the environment. We will quantify the performance of that algorithm by implementing it for the base case and test case presented in the previous chapter. It is important to note that the original algorithm was designed for link-layer transmissions whereas we will be measuring its performance at the physical layer. Therefore, we adapted the idea accordingly but, in essence, it is the same idea as presented in [2]. We want to find out the expected cost, $E[X]$ of establishing a shared secret key using the dynamic secrets algorithm. Although we look at expected cost, note that it is possible to use other performance metrics, and the following procedure can be used to evaluate those metrics [15].

Figure 5.1 shows the markov state diagram that we will use to analyze this algorithm. We begin by assuming that initially the connection is insecure. Alice and Bob do not share a system secret. They need to exchange messages in order to establish

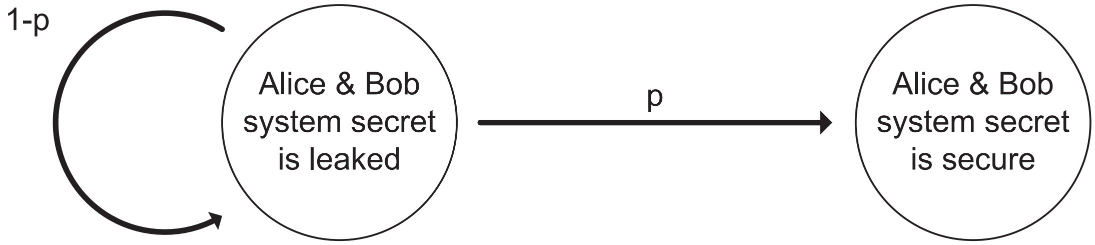

1-p
Alice & Bob system secret is leaked
p
Alice & Bob system secret is secure

Figure 5.1: Markov state diagram showing the possible states to investigate the number of trials it will take before the system secret is secure. This happens while Eve loses information when she is unable to decode, and while Bob is successful in decoding Alice’s message.

a shared secret. The dynamic algorithm suggests that with each transmission, Alice and Bob generate a system secret irrelevant of whether Eve is unable to decode the message or not. This system secret is "dynamically" updated as Bob decodes more of Alice's messages. Therefore, even though if Eve is initially able to eavesdrop on the communication, and is aware of the algorithm, it will eventually lose track of the system secret when it fails to decode a message because of packet loss caused by randomness in the environment. Referring back to Figure 5.1, the final state "Alice & Bob system secret is secure" is analogous to the case when Bob is able to decode while Eve is not able to decode Alice's message. Therefore, the probability "p" is actually the same as P_{succ} that we defined in Section 3.4. Hence, the probability of staying in the initial state is $(1 - P_{succ})$ while the probability of transitioning to the final state is (P_{succ}). Let the cost incurred with each transition be fixed and denote it by τ.

We map the markov process to a linear system via the signal flow graph [15] to analyze the expected cost of transitioning from the initial state to the final state. It is possible to evaluate the expected cost by other simpler methods. However, the Signal Flow Graph is a useful method to draw other conclusions than the expected cost such as moment generating functions and finding probability bounds. This method transforms the markov process into a transfer function. Figure 5.2 shows the signal flow graph for this markov state diagram where $H(s)$ is the reduced form transfer function between the two states.

$$H(s) = \frac{P_{succ}e^{s\tau}}{1 - (1 - P_{succ})e^{s\tau}} \tag{5.1}$$

We can find the expected cost, $E[X]$ through the first moment generating function of $H(s)$ at $s = 0$, which is $H'(s)|_{s=0}$.

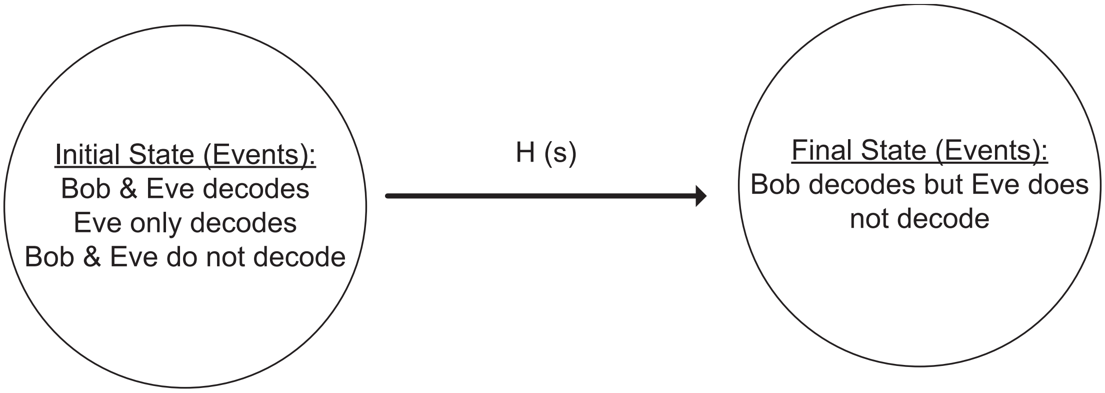
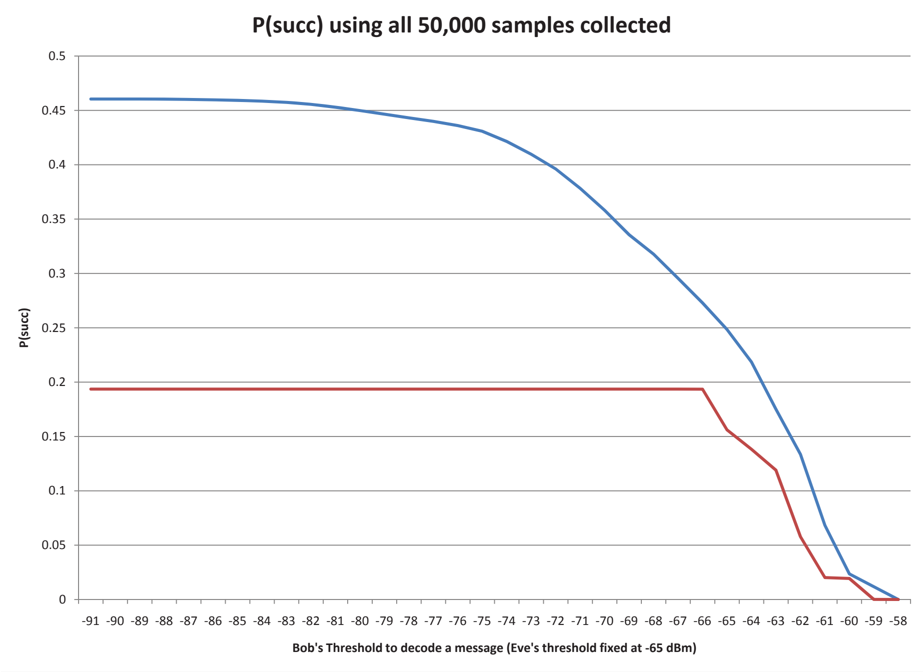


Figure 5.2: This Figure shows the signal flow graph of the Markov state diagram shown in Figure 5.1. Note that in the signal flow graph form, we can represent the transition between one state to the other as a transfer function. Moreover, the graph shows the list of events that are part of each node.

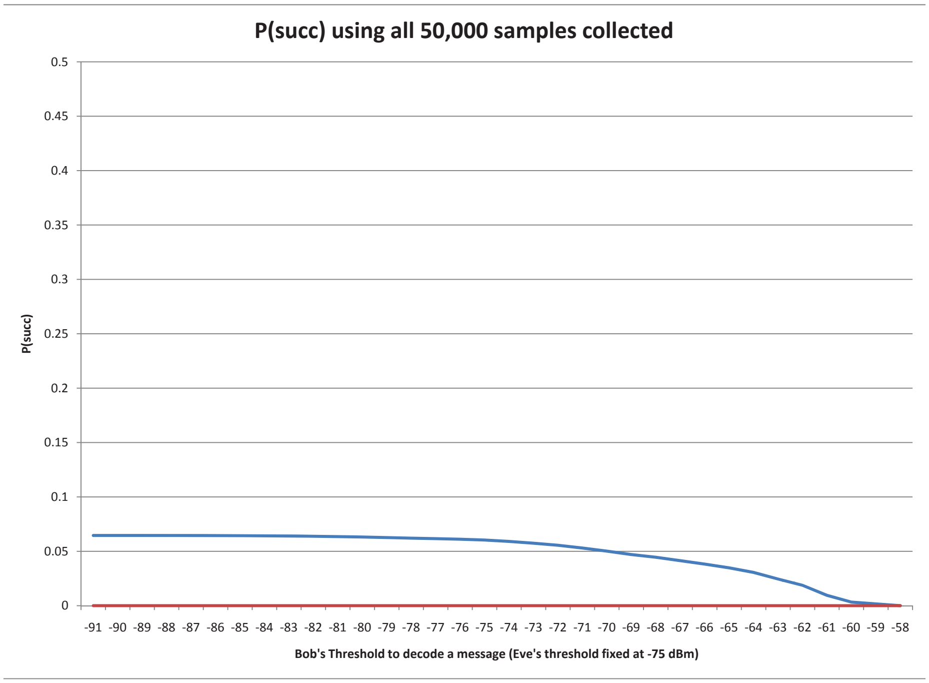
$$\begin{aligned}
E[X] &= H'(s)|_{s=0} \\
&= \tfrac{d}{ds}\left(\tfrac{P_{succ}e^{s\tau}}{1-(1-P_{succ})e^{s\tau}}\right)|_{s=0} \\
&= \tfrac{d}{ds}\left(\tfrac{P_{succ}e^{s\tau}}{1-(1-P_{succ})e^{s\tau}}\right)|_{s=0} \\
&= \tfrac{(1-(1-P_{succ})e^{s\tau})(\tau P_{succ}e^{s\tau})-(-\tau(1-P_{succ})e^{s\tau})(P_{succ}e^{s\tau})}{(1-(1-P_{succ})e^{s\tau})^2}|_{s=0} \\
&= \tfrac{\tau P_{succ}}{P_{succ}^2} \\
&= \tfrac{\tau}{P_{succ}}
\end{aligned} \tag{5.2}$$

From (5.2), we can see that the expected cost totally depends on P_{succ} for this system. We calculate P_{succ} from measurement data collected in the previous chapter, and assume that the cost of each transition is 10 units, $\tau = 10$. We fix Eve's threshold to decode a message and sweep Bob's threshold to decode a message to plot P_{succ} and expected cost, $E[X]$. Figure 5.3 shows the calculated P_{succ} using this information. Correspondingly, Figure 5.4 shows the expected cost.

From the plots, we can see that when we are using a two-element antenna array, the cost to establish a secret key is lower compared to that of using a single antenna. Moreover, it is important to note that Eve's threshold is first set to -65 dBm (if we assume noise to be -75 dBm, $\gamma_e = 10$ dB)which means that it is a weak Eve. In other words, she is only able to decode Alice's message if the signal strength is strong. If we

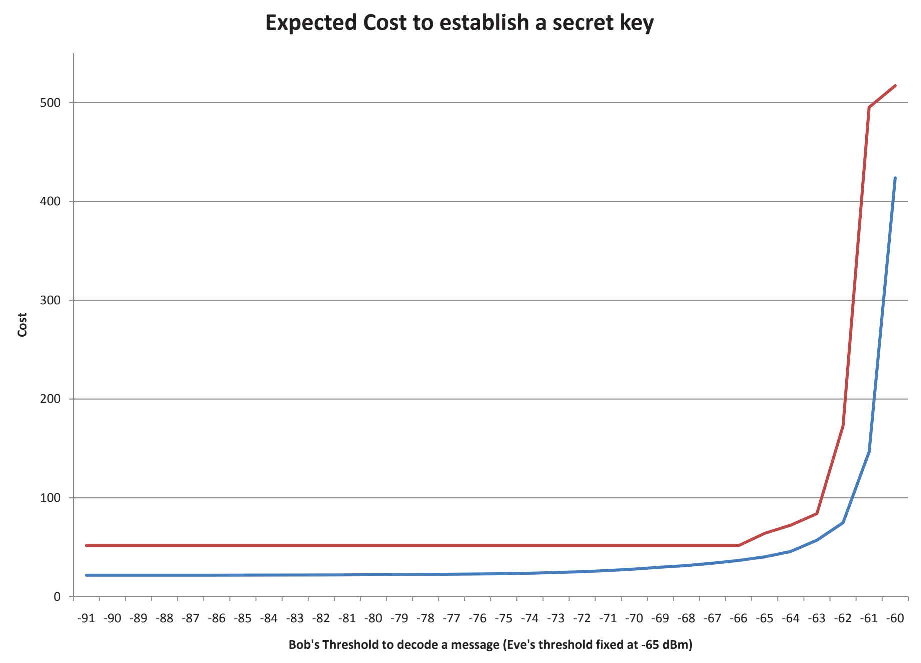


(a) P_{succ} vs Bob's decode threshold when Eve's decode threshold is -65 dBm (Strong Eve)

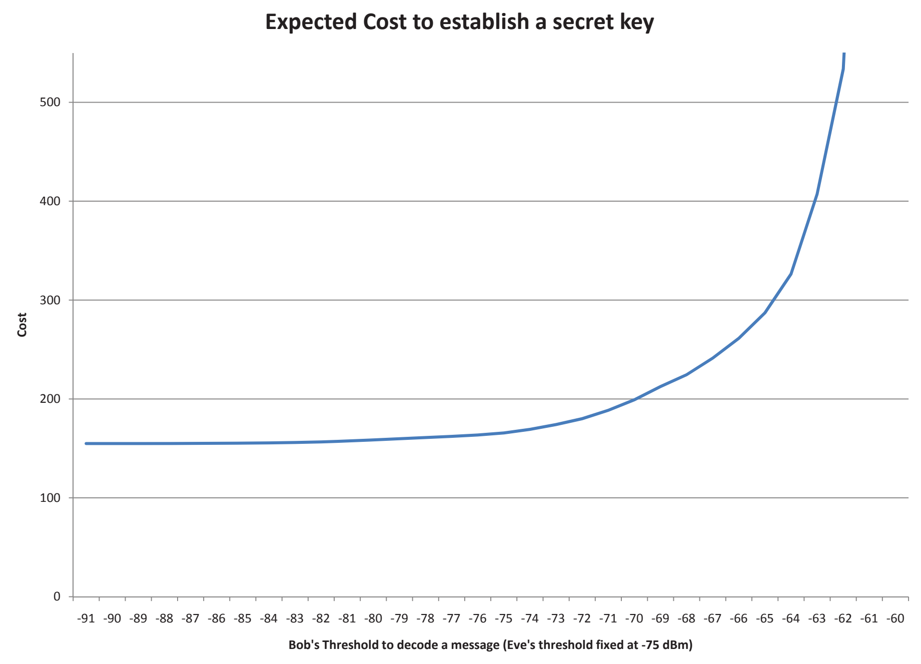


(b) P_{succ} vs Bob's decode threshold when Eve's decode threshold is -75 dBm (Strong Eve)

Figure 5.3: Compared to the single antenna system (red), the antenna array system (blue) is still able to perform when Eve is stronger.



(a) Expected Cost vs Bob's decode threshold when Eve's decode threshold is -65 dBm (Weak Eve)



(b) Expected Cost vs Bob's decode threshold when Eve's decode threshold is -75 dBm (Strong Eve)

Figure 5.4: The expected cost for the antenna array system (blue) rises when Eve becomes stronger but it is still able to operate. Whereas, the single antenna system (red)'s cost is ∞ since P_{succ} is 0.

lower Eve's threshold to -75 dBm (if we assume noise to be -75 dBm, $\gamma_e = 0$ dB), and hence, have a stronger Eve, we observe that the single omni-directional antenna will not be successful at all while the two-element antenna array will still be able to operate.

This result can be compared with the Monte-Carlo simulation data for Passive Eve presented in Section 3.5.1. It is important to realize that the two results can not be compared in absolute terms because of the number of assumptions made while running the simulations. However, we observe similar trend in both the simulation and empirical data. Similar to the simulation results, we see that test case performs better than the base case. Since the K-factor is high, the variation due to multi-path fading alone is very small. This is evident from the red plots presented in the previous chapter. Our method provides greater variation and hence, the probability of success is higher. Moreover, we see that as Eve is stronger, the probability of Alice succeeding in the base case drops to 0 whereas Alice in the test case is still able to exceed with low probability.

CHAPTER 6
CONCLUSION

In the wireless channel, randomness is often required to establish security and/or secrecy. This randomness is generated by multi-path fading in the environment. However, in static and less congested scenarios, randomness can go away as the multi-path fading is not present. In such scenarios, we can get this randomness back by generating artificial randomness through antenna radiation variation. As an example, let us recall the Passive Eve model where Alice wants to communicate with Bob and Eve has the ability to listen to that conversation. We have defined P_{succ} as the probability of the event when Bob can decode Alice's message but Eve can not. The analysis on "Dynamic Secrets" show that at a high Rician K-factor of 10 dB, without our antenna radiation variation, the P_{succ} is 0 whereas when we employ our method; the probability of success, P_{succ}, is approximately 0.075.

The conclusion that we draw from our results is significant, as it enhances secrecy in worst-case scenario, but at the same time certain limitations apply to them. The most important consideration is regarding the capabilities of the eavesdropper, Eve. In our calculations, we assume Bob and Eve to be at the same distance. It is possible to assume a more pessimistic case where Eve is closer to Alice. This will certainly reduce P_{succ}, as it is similar to the case in Chapter 5 where we reduce Eve's decoding threshold from -65 dBm to -75 dBm to indicate a stronger Eve. However, at the same time, P_{succ} of the linear antenna array will still improve relative to the single antenna case. Also note that as Eve gets closer to Alice, within a certain distance it is possible that, even with our method, we may not be able to force Eve to miss any messages.

While in the case of passive Eve it may be sufficient to use our method at Alice's side only, that may not be the case when Eve is active. Since Eve is trying to jam Bob in a static Eve-Bob channel, we must then also use our method at Bob. However, this places certain limitations as the receiver design can be much more complex than a transmitter.

APPENDIX

AUTOMATION OF LAB INSTRUMENTS

Lab instruments such as signal generators and spectrum analyzers provide multiple options for automation. The most common languages that they use are SCPI (Standard Commands for Programmable Instrumetnts) and TCL (Tool Command Language). Hence, we can send commands to the instrument using telnet over ethernet or via RS-232 and GPIB interfaces. Scripting languages such as python provide a means to send a sequence of messages to the instrument and receive its response.

In our setup, we also use python to send SCPI commands to the instruments. There are two scripts that run indpendently of each other. The first script, chooses a random phase between $-\pi$ and π and applies it to one of the signal generator. The other signal generator is always at the same phase reference, thus, this generates a random phase. The python script is presented below:

```
#Python script to apply random phase to one of the two signal generators.
import SCPI
import sys
import string
import SIGGEN
import random
import math

# Open the connection to Serial Port of Signal Generator
sig=SIGGEN.SIGGEN()
sig.SerialClose()
sig.SerialOpen()

# Set Zero Phase Reference
sig.SerialWrite(’Phase:Reference’)
phase=0
sig.SerialWrite(’Phase:Adjust ’+str(phase)+’ rad’)
```

```
for i in range(0,10000):
       if (i%1==0):
              phase=random.uniform(-math.pi,math.pi) #Uniformly select a
                 rendom phase from -pi to pi
              sig.SerialWrite('Phase:Adjust '+str(phase)+' rad')
                 #Apply phase
```

The above script depends on a class SIGGEN which is not part of a standard library. This class helps to establish RS-232 connection between the computer and signal generator. It is re-produced below:

```
#Class to establish RS-232 connection with signal generator
import serial

class SIGGEN:
       def __init__(self):                #Constructor opens a serial port
              self.ser=serial.Serial(
                     port='COM13',
                     baudrate=9600,
                     parity=serial.PARITY_NONE,
                     stopbits=serial.STOPBITS_ONE,
                     bytesize=serial.EIGHTBITS
              )

       def SerialClose(self):
              self.ser.close()

       def SerialOpen(self):
              self.ser.open()

       def SerialWrite(self,msg):
              self.ser.write(msg + '\r\n')

       def GetValue(self):
              out = ''
              while self.ser.inWaiting() > 0:
                     out += self.ser.read(1)
              if out != '':
                     return out

       def out_print(self):
              out = ''
              while self.ser.inWaiting() > 0:
                     out += self.ser.read(1)
              if out != '':
                     print ">>" + out
```

The second script collects 5000 measurement samples from the spectrum analyzer. The following script was used:

```
#Python script to collect samples from the spectrum analyzer
import SCPI
import timeit
import time
import sys
import string
import SIGGEN

f = open('16June_K_factor_lab_no_absorber.txt','a') #Creating a local file
   to save collected samples
power = SCPI.SCPI("192.168.1.15")
FREQ="+2.52700000E+009"

for i in range(0,5000): #5000 iterations to collect 5000 samples
       power.sendCmd("FETCH:SAN?")
       x=power.getMeasurements()
       tempindex=string.index(x,FREQ)
       y=x[tempindex:(tempindex+33)]
       f.write(y+"\n")
f.close()
```

BIBLIOGRAPHY

[1] S. Popa, N. Draghiciu, and R. Reiz, “Fading Types in Wireless Communication Systems,” *Journal of Electrical and Electronics Engineering*, vol.1, no.1, pp.232-237, 2008.

[2] S. Xiao, W. Gong and D. Towsley, “From Uncertainty to Secrecy: A Dynamic Approach,” *Signals, Systems and Computers (ASILOMAR), 2010 Conference Record of the Forty Fourth Asilomar Conference on*, vol., no., pp.37-41, 7-10 Nov. 2010

[3] M. Strasser, C. Popper, S. Capkun, and M. Cagalj, “Jamming-resistant Key Establishment using Uncoordinated Frequency Hopping,” *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, vol. , no., pp. 64-78, 18-22 May 2008.

[4] R. Liu, and H.V. Poor, “ Multi-Antenna Gaussian Broadcast Channels with Confidential Mesages,” *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, vol., no., pp. 2202-2206, 6-11 July 2008.

[5] S.N. Premnath, S. Jana, J. Croft, P.L. Gowda, M.Clark, S.K.Kasera, N. Patwari, and S.V. Krishnamurthy, “Secret Key Extraction from Wireless Signal Strength in Real Environments,” *Mobile Computing, IEEE Transactions on*, vol.PP, no.99, pp.1.

[6] P.K. Gopala, L. Lai, and H. El Gamal, “On the Secrecy Capacity of Fading Channels,” *Information Theory, IEEE Transactions on*, vol.54, no.10, pp.4687-4698, Oct. 2008.

[7] S. Gollakota, and D. Katabi, “Physical Layer Wireless Security Made Fast and Channel Independent,” *INFOCOM, 2011 Proceedings IEEE*, vol., no., pp.1125-1133, 10-15 April 2011.

[8] S. Xiao, W. Gong, and D. Towsley, “Secure Wireless Communication with Dynamic Secrets,” *INFOCOM, 2010 Proceedings IEEE*, , vol., no., pp.1-9, 14-19 March 2010.

[9] Z. Hao, S. Zhong and Li E. Li, “Towards Wireless Security without Computational Assumptions An oblivious transfer protocol based on an unauthenticated wireless channel,” *INFOCOM, 2011 Proceedings IEEE*, vol., no., pp.2156-2164, 10-15 April 2011.

[10] M. Bloch, J. Barros, M.R.D. Rodrigues, and S.W. McLaughlin, “Wireless Information-Theoretic Security,” *Information Theory, IEEE Transactions on*, vol.54, no.6, pp.2515-2534, June 2008.

[11] C. Capar, M. Zafer, D. Goeckel, D. Towsley, and D. Agrawal, “Physical-Layer-Enhanced wireless secret key exchange,” *Annual Conference of the International Technology Alliance (ACITA)*, 2010.

[12] D. Tse and P. Viswanath, “Fundamentals of Wireless Communication,” *Cambridge University Press*, May 2005.

[13] S. S. Haykin and M. Moher, “Modern Wireless Communications,” *Pearson/Prentice Hall*, 2005.

[14] W. Diffie and M.E. Hellman, “New directions in cryptography,” *Information Theory, IEEE Transactions on* , vol.22, no.6, pp.644,654, Nov 1976.

[15] R. Howard, “Dynamic Probabilistic Systems,” *J. Wiley & Sons Inc*, 1971.

[16] A. Papoulis and S.U. Pillai, “Probability, random variables, and stochastic processes,” *Tata McGraw-Hill Education*, 2002.