SECURE COMMUNICATIONS IN FILTER BANK MULTICARRIER SPREAD SPECTRUM SYSTEMS

by

Arslan Javaid Majid

A dissertation submitted to the faculty of
The University of Utah
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

Department of Electrical and Computer Engineering

The University of Utah

August 2017

The University of Utah Graduate School

STATEMENT OF DISSERTATION APPROVAL

The dissertation of **Arslan Javaid Majid**
has been approved by the following supervisory committee members:

Behrouz Farhang ,	Chair(s)	**22 Nov 2016** Date Approved
Neal Patwari ,	Member	**22 Nov 2016** Date Approved
Rong Rong Chen ,	Member	**22 Nov 2016** Date Approved
Sneha Kasera ,	Member	**21 Mar 2017** Date Approved
Hussein Moradi ,	Member	_____ Date Approved

by **Gianluca Lazzi** , Chair/Dean of
the Department/College/School of **Electrical and Computer Engineering**
and by **David B. Kieda** , Dean of The Graduate School.

ABSTRACT

A fundamental characteristic of wireless communications is in their broadcast nature, which allows accessibility of information without placing restrictions on a user's location. However, the ease of accessibility also makes it vulnerable to eavesdropping. This dissertation considers the security issues of spread spectrum systems and in this context, a secure information transmission system compromised of two main parts is presented. The first component makes use of the principle of reciprocity in frequency-selective wireless channels to derive a pair of keys for two legitimate parties. The proposed key generation algorithm allows for two asynchronous transceivers to derive a pair of similar keys. Moreover, a unique augmentation - called *strongest path cancellation* (SPC) - is applied to the keys and has been validated through simulation and real-world measurements to significantly boost the security level of the design. In the second part of the secure information transmission system, the concept of artificial noise is introduced to multicarrier spread spectrum systems. The keys generated in the first part of the protocol are used as spreading code sequences for the spread spectrum system. Artificial noise is added to further enhance the security of the communication setup. Two different attacks on the proposed security system are evaluated. First, a passive adversary following the same steps as the legitimate users to detect confidential information is considered. The second attack studies a more sophisticated adversary with significant blind detection capabilities.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

NOTATION AND SYMBOLS

$\Re[x]$	Real value of x
$\Im[x]$	Imaginary value of x
$\mathbf{x}$, $\mathbf{X}$	Vector and matrix
$\|\|\mathbf{x}\|\|$	Euclidean norm of vector $\mathbf{x}$
$\|\|\mathbf{x}\|\|_\infty$	Infinity norm of vector $\mathbf{x}$
$\langle \mathbf{x}, \mathbf{y} \rangle$	Inner product of $\mathbf{x}$ and $\mathbf{y}$
$*$	Convolution operator
$n \bmod M$	n modulo M
$x(t)$	Continuous-time signal
$x[n]$	Discrete-time signal
$j = \sqrt{-1}$	Unit imaginary number
$\{\cdot\}^{\mathrm{T}}$	Matrix Transpose
$\{\cdot\}^{\mathrm{H}}$	Matrix Hermitian
A, B, E	Subscripts for Alice, Bob, and Eve

ACKNOWLEDGEMENTS

First and foremost, I would like to thank God for giving me the health, opportunity, and prosperity that I needed to complete the necessary objectives of my Ph.D.

Growing up, I had no idea what I wanted to do and getting a Ph.D. in electrical engineering was certainly not where I thought I would have ended up. In retrospect, my journey thus far could have ended in many different routes and it is unclear to me why and how this route came to be. Nevertheless, I am very thankful for this unforgettable experience.

I have many people to thank for helping me accomplish this work. None of this would have been possible without the "push" from my advisor, Dr. Behrouz Farhang. I am very glad that he helped me see the benefits in obtaining a Ph.D. Without his advice, I don't even know if I would have even started a master's degree, let alone a Ph.D. It is rare to see a professor in any university, let alone a top university, give their students more time, more help, and more support than Dr. Farhang has given. From listening to my ideas to understanding and helping with my shortcomings, I am greatly indebted to him for his contributions to my professional and personal life.

I would also like to thank Idaho National Laboratory for their support of this research. I don't know what this dissertation would be without their support. In particular, I would like to express my gratitude towards Dr. Hussein Moradi, who has always offered his time, support, advice, and mentoring to me along the various stages of my professional development.

I am also thankful to the University of Utah for the opportunities that it has given to me. Through the university, I have had the privilege of experiencing a top-notch education in the comfort of my home city. It has also been an utmost privilege to learn from the excellent faculty in the Department of Electrical and Computer Engineering. In particular, the field of Wireless Communications and Signal Processing has some of the best faculty at this university. I am especially thankful to Dr. Cynthia Furse, who gave me my first

job as an NSF outreach student at the University of Utah. Some of the most memorable times I've spent here were during the years that I worked for Dr. Furse. She is among the nicest, most understanding, and helpful faculty at the University of Utah. I would like to thank my first adviser, Dr. Mike Scarpulla, for his time and dedication in teaching me the very confusing topic of semiconductor physics. I gratefully acknowledge the members of my Ph.D. committee, who have been instrumental in helping me obtain the necessary knowledge and intuition in this work, particularly through their own research related to this work.

Last, but not least, I would like to express gratitude towards all members of my family for their unconditional love and support. My parents, Javaid and Samia Majid, who sacrificed everything they knew to come to this country so that their offspring can have the opportunities that they could never have. Thanks to the sacrifice of my parents, I developed the passion and energy to finish this work. I will be forever grateful to my parents for everything they have done for me. I am also thankful for the support, encouragement, and help that my best friend and brother, Sufhan Majid, gave to me. No one could ask for a better brother. Finally, I would like to thank my wife, Mehreen Majid, who has stuck with me through the most difficult part of my life with unwavering love and support. Whenever I need a lift or a smile, she is there for me. Thank you all.

CHAPTER 1

INTRODUCTION

The broadcast nature of wireless communications has made it possible to access information at unprecedented levels without restricting the user's location. However, this open communications environment also makes the medium more susceptible to malicious adversaries. In this dissertation, we consider the security issues involved in spread spectrum (SS) wireless communication systems. Such systems are used in applications which require resilience to harsh environments, resistance to channel fading through frequency diversity, low probability of detection (LPD), and low probability of interception (LPI). However, as with any wireless communication system, due to the broadcast nature of the communication, a passive eavesdropper (Eve) within the range of broadcast can obtain the transmitted signal between a pair of legitimate users (Alice and Bob) and, given a sufficient number of signal samples, may be able to identify the spreading sequence and recover the transmitted information.

An interesting avenue of research in the field of wireless security makes use of the time-varying and random nature of the wireless channel. Depending on the application, the wireless channel is either seen as a hindrance - particularly to broadcast communication devices whose primary goal is maximizing data throughput - or as an intriguing source of information suitable for many unique applications. Of particular interest to us in this dissertation is the application of wireless channels to wireless security.

This chapter serves as an introduction for the dissertation by educating the reader on the necessary background material required for understanding this work. We start with fundamentals on physical-layer security and give an overview of the different avenues of research within this field. The proposed security solution in this dissertation makes use of the reciprocal wireless channel and therefore, we devote a section of this chapter to it. The application for the proposed solution is for spread spectrum systems and therefore, we

devote a section to these types of systems. Next, as is common with most of the research in this field, we describe a model for the adversary. Following the adversary model, we highlight the contributions of this dissertation and end the chapter by giving an outline of this dissertation.

1.1 Fundamentals of Physical-Layer Security

In this section, a brief overview of physical-layer security is given. The discussion starts with Shannon's model of perfect secrecy, which is found to be a fairly restrictive solution. Next, this model is extended into three different areas into which wireless security has branched off. For the curious reader interested in this subject matter, we recommend the works in [1–3] where the following discussion is more elaborated upon.

1.1.1 Shannon's Perfect Secrecy

The foundation of information-theoretic security was laid out by Shannon in his classical work [4]. This work concluded that perfect secrecy is achievable when the size of the secret key is at least as large as the secret message. To help give a detailed explanation of the findings here, refer to Shannon's model of secrecy in Fig. 1.1. The goal here is to have Alice communicate a message error-free to Bob while a passive eavesdropper listens and acquires no information about the secret message.

In Fig. 1.1, Alice *encrypts* the confidential message $\mathcal{M}$ with a key $\mathcal{K}$ to form a codeword $\mathcal{X}$. The key $\mathcal{K}$ is known only to Alice and Bob and the encryption and decryption algorithms are known to Eve. Once the message is obtained by Bob, he *decrypts* it with $\mathcal{K}$ to get $\mathcal{M}$. The key, codeword, and message are now treated as random variables so that information theory can be applied.

The entropy of the message is given by $\mathbb{H}(\mathcal{M})$ and the *equivocation-rate* is defined as $\mathbb{H}(\mathcal{M}|\mathcal{X})$. Definitions of entropy, conditional entropy, and mutual information for any given random variables x and y are respectively given as

$$\mathbb{H}(X) = \sum_{x\in\mathcal{X}} p(x)\log_2 p(x) \tag{1.1}$$

$$\mathbb{H}(X|Y) = \sum_{x\in\mathcal{X},y\in\mathcal{Y}} p(x,y)\log_2 \frac{p(x)}{p(x,y)} \tag{1.2}$$

$$\mathbb{I}(X;Y) = \mathbb{H}(X) - \mathbb{H}(X|Y) \tag{1.3}$$

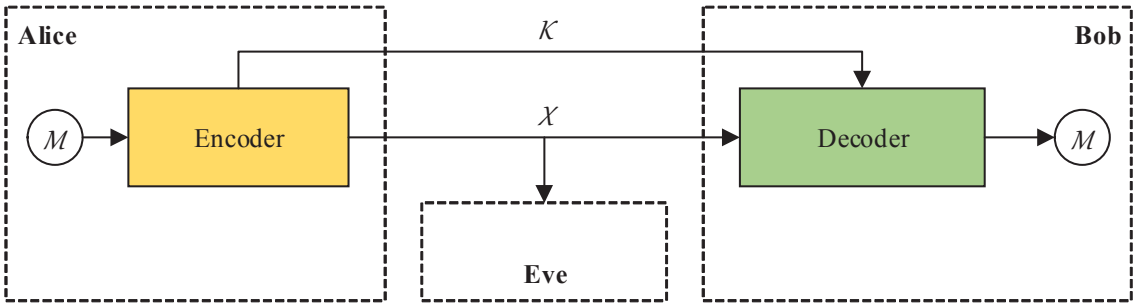

Figure 1.1. Shannon secrecy model

where $p(x)$ is the probability distribution of X and $p(x, y)$ is joint distribution of X and Y.

The *equivocation-rate* $\mathbb{H}(\mathcal{M}|\mathcal{X})$ describes Eve's uncertainty in $\mathcal{M}$ reduced by knowledge of codeword $\mathcal{X}$. A coding scheme achieves *perfect secrecy* if knowledge of $\mathcal{X}$ does not reduce uncertainty of message $\mathcal{M}$ - i.e., when the equivocation-rate is equal to the entropy of the message, so that

$$\mathbb{H}(\mathcal{M}|\mathcal{X}) = \mathbb{H}(\mathcal{M}) \tag{1.4}$$

which is equivalent to the information leaked to Eve being zero

$$\mathbb{I}(\mathcal{M}; \mathcal{X}) = 0 \tag{1.5}$$

In other words, perfect secrecy states that given the codeword $\mathcal{X}$, nothing will be revealed about the confidential message $\mathcal{M}$ by codeword $\mathcal{X}$. This result provides a quantitative measure of security that is based on three strict assumptions -

- *Computationally unbounded adversary* - The model does not define any computational constraint on Eve. Perfect secrecy essentially implies Eve has no way to guess the message $\mathcal{M}$ given $\mathcal{X}$.

- *Key exchange* - The only advantage that Alice and Bob have over the adversary in Shannon's model is in the key $\mathcal{K}$ that they share. The key is independent of the message $\mathcal{M}$. It must somehow be obtained by Alice and Bob through some procedure whilst remaining unknown to Eve.

- *Noiseless communication* - The two receivers of Bob and Eve both obtain the same transmitted codeword $\mathcal{X}$ without any error.

A scheme which is known to obtain this form of secrecy is the one-time pad. The one-time pad solution requires that the entropy of the key must be at least as large as the entropy of the message - i.e., for every message bit, it is necessary to use at least 1 secret bit or more.

The results of [4] is considered a ground-breaking achievement in the field of security. However, the result here is generally considered to be a pessimistic one since it requires a significant (if not impossible to achieve) key-distribtion algorithm that can generate the keys needed to achieve perfect secrecy. In the next set of sections, we show how relaxing the assumptions in Shannon's perfect secrecy model can allow for varying degrees of success in allowing two legitimate parties to communicate securely over the presence of a passive eavesdropper.

1.1.2 Cryptographic Solutions

The most ubiquitous solution for security in wireless networks relies on cryptography-based schemes that heavily utilize the application layer to provide security to the legitimate parties. Cryptographic protocols relax Shannon's assumption of a *computationally unbounded adversary*.

The system model remains largely the same as Shannon's original model and is shown in Fig. 1.2. Communication is still assumed to be error-free for all nodes. The most significant change here is that the key - known in these methods as a *session key* - is much shorter than the message length [5]. The session key is called as such to indicate that it is periodically generated using one of the many public key cryptography (PKC) protocols, which include the well-known Diffie-Hellman [6] key exchange and the Rivest-Shamir-Adleman (RSA) cryptosystem [7]. In PKC, session keys are generated through the help of *trapdoor one-way functions* - mathematical functions which are computationally difficult to compute without a special code - the code being provided to the legitimate users by a certificate authority. PKC-based methods require a lower bound assumption on the computational power of the adversary. Additionally, they are computationally expensive - hindering the application in mobile devices with limited battery power. Despite these shortcomings, cryptography-based solutions have proven to be very effective in security applications as of today due to 1) the straightforwardness of the techniques, particularly compared

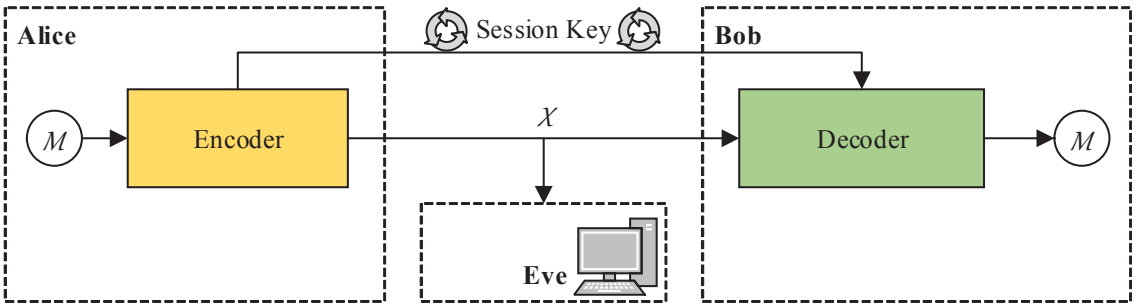

Figure 1.2. Cryptography model

to physical-layer-based counterparts and 2) the computational bounds of computers that have been mostly limited relative to the technology of today's cryptographic techniques.

Given the success and advancements of this field, we note that the solutions presented in this dissertation are not to be look at strictly as replacements to cryptography-based methods. Rather, the physical-layer security methods discussed in this dissertation serve as a means of enhancing current wireless security. More specifically, in this dissertation, we look to enhance security of wireless communication based on spread spectrum technology.

1.1.3 Physical-Layer Key Generation

Another set of solutions to the wireless security problem are *physical-layer key generation* methods. A good set of surveys in this area can be found in [2, 8–10]. Here, the assumption from Shannon's perfect secrecy model where the adversary has no bounds on computational power is kept intact. Instead, researchers look to solve the *key exchange* problem in Shannon's perfect model. The main concept here is to generate a *secret key* between Alice and Bob by making use of the following properties of the wireless fading channel:

- Channel reciprocity - The wireless channel between any two tranceivers using the same wireless link experiences the same fading properties (gains, phase shifts, and multipath delays).

- Channel randomness - Channel fading across time and frequency benefits from randomness due to Doppler spread and multipath delay spread, respectively.

- Channel independence over space - An adversary located more than a few wavelengths away from the legitimate users experiences another random and uncorre-

lated channel [11].

The utilization of the key itself is up to the designer and can be used either as a one-time pad - effectively providing perfect secrecy - or a session key as part of a cryptographic solution. Figure 1.3 shows the following steps described in [12] that physical-layer key generation methods obey : 1) randomness sharing, 2) information reconciliation, 3) privacy amplification, and 4) secure communication.

As depicted in Figure 1.3, in *randomness sharing*, the legitimate parties probe the reciprocal wireless channel between them. The 'randomness' here refers to the channel state information (CSI) and is referred to in Fig. 1.3 as X and X' for Alice and Bob, respectively. In *information reconciliation*, the two nodes communicate with one another to reconcile the differences, or non-reciprocities, between their channel measurements. This step is crucial in obtaining keys that agree completely with one another at a high percent. *Privacy amplification* is a process that maps the reconciled channel measurements to a key whose maximum size depends on the randomness of the measurements. Any information which was leaked through information reconciliation is removed. At the end of this step, Alice and Bob respectively have the keys K and K'. The goal here is to develop a protocol in which the keys are at least as large as the *secret-key capacity* of the channel [1]. The secret-key capacity quantitatively defines the amount of randomness that can be extracted from the channel in the form of a key. Finally, in *secure communication*, the parties transmit messages using the key - either as a one-time pad to provide perfect secrecy or as a key for standard encryption algorithms.

1.1.4 Secure Information Transmission

Shannon's perfect secrecy model assumes that Bob and Eve retrieve exactly the same message as the one that was transmitted. However, most practical communication systems have some degree of additive noise seen at a receiver. In this section, we discuss a particular subclass of Shannon's perfect secrecy model in which noise is added to Alice's transmitted sequence.

One of the earliest attempts to relax Shannon's assumption on *noiseless communication* was made by Wyner in his seminal report on the *degraded wire-tap channel* (DWTC) [13]. As the name implies, this model considers an eavesdropper who *wiretaps* the link between

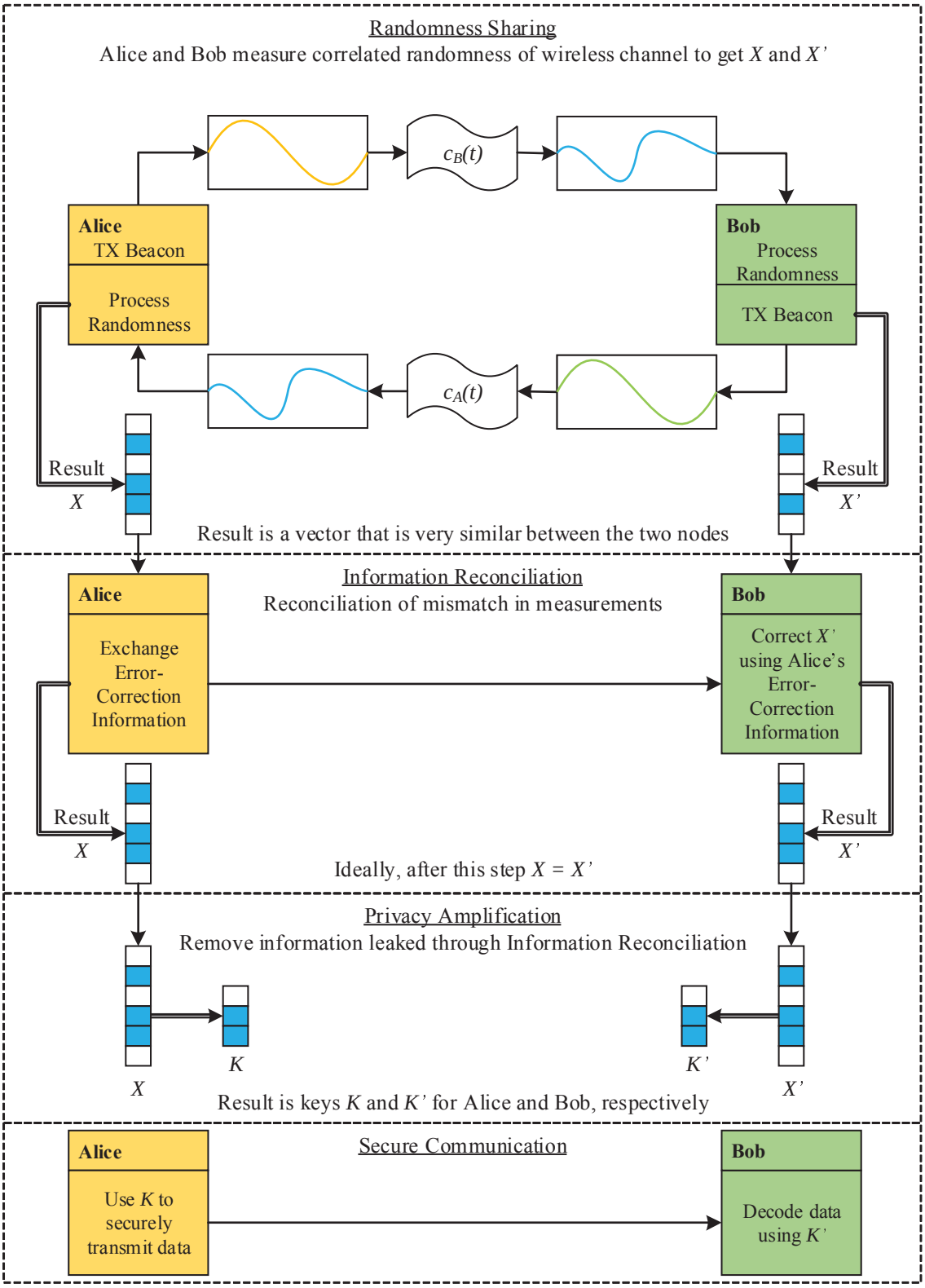

Figure 1.3. Flowchart describing outline of the general physical-layer key generation model.

the legitimate parties, experiencing noise from the receiver channel *and* the eavesdropper channel. Hence, the eavesdropper sees a *degraded* version of the signal obtained by Bob. It was shown in this report that secrecy could be achieved in the DWTC model even without a secret key due simply to the fact that the eavesdropper's received signal is degraded compared to the Bob's. The report introduced the notion of *secrecy capacity* - defined as the maximum rate at which a transmitter can reliably communicate a confidential message to the intended receiver without an eavesdropper being able to decode it.

The DWTC studied by Wyner in [13] was later extended to the Gaussian WTC [14]. The secrecy capacity found for the Gaussian WTC is a simpler, and therefore more appealing, characterization compared to [13]. For the Gaussian WTC, the secrecy capacity was given by

$$C_s = \frac{1}{2}\log_2\left(1+\frac{P}{\sigma_\eta^2}\right) - \frac{1}{2}\log_2\left(1+\frac{P}{\sigma_\epsilon^2}\right) \tag{1.6}$$

where P/σ_η^2 and P/σ_ϵ^2 are the respective signal-to-noise ratio (SNR) at the receivers of Bob and Eve.

The secrecy capacity definition in (1.6) is simply the difference in capacity of the main link and the wiretap link. Two main assumptions of these models should be noted at this point. First, the secrecy capacity characterization discussed so far only guarantees secrecy if the channel state information (CSI) of both the Alice-Bob and Alice-Eve links are *perfectly* known to Alice. This is often referred to as the Full-CSI case. For practical situations in which such knowledge is unavailable, the secrecy capacity cannot be calculated and thus perfect secrecy is not guaranteed. Furthermore, in situations where the secrecy capacity is undefined due to lack of Full-CSI knowledge, encoding schemes that are used to ensure perfect secrecy cannot be used. Second, it should also be noted that so far, this characterization requires Eve to be at a disadvantage compared to Bob - i.e., secrecy does not exist if Eve's SNR is greater than Bob's SNR. Due in part to the stringent assumptions required in these early models, research in this area remained largely stagnant until very recently when the reciprocal wireless channel was introduced into Wyner's model.

The secrecy capacity of wireless channels was analyzed in [12]. In this definition of secrecy capacity, flat-fading was introduced into the expression in (1.6) as follows

$$C_s = \log_2\left(1+\frac{|h_\mathrm{B}|^2 P}{\sigma_\eta^2}\right) - \log_2\left(1+\frac{|h_\mathrm{E}|^2 P}{\sigma_\epsilon^2}\right) \tag{1.7}$$

Note that the factor of $\frac{1}{2}$ is removed in (1.7). This is attributed to the use of complex-valued signaling instead of real-valued signals use to obtain (1.6). Fig. 1.4 illustrates the model of secure information transmission systems used in [12], a derivative of the original Wyner DWTC.

In [12], it was shown that fading can play an important role in securing wireless communications without a key. The fluctuation in the receivers' SNR values induced by fading can be used to transmit confidential information at opportunistic times when the eavesdropper's instantaneous SNR falls below that of the legitimate receiver.

In practical situations where the eavesdropper's CSI is unknown to Alice, outage-based characterizations have been adopted. To this end, Barros and Rodrigues in [15] introduced the outage probability of secrecy - defined as the probability that the instantaneous secrecy capacity in (1.6) is less than the target secrecy rate R_s, i.e.,

$$\mathcal{P}_{\text{out}}(R_s) = \mathcal{P}(C_s < R_s) \tag{1.8}$$

Another definition, which we have found to be more practical, for the probability of secrecy outage was given in [16]. The alternative definition of probability of secrecy outage is given by

$$\mathcal{P}_{\text{out}}(R_s) = \mathcal{P}(R_{\text{T}} - C_{\text{E}} < R_s) \tag{1.9}$$

where R_{T} is the rate of the transmitted codeword and C_{E} is the capacity of the eavesdropper's link, expressed as $C_{\text{E}} = \log_2\left(1 + \frac{|h_{\text{E}}|^2 P}{\sigma_e^2}\right)$. We also express C_{B} similarly.

The difference between the two outage-based characterizations is the following. In (1.8), it is implied that Alice chooses an encoding strategy to work optimally for the perfectly known instantaneous realization of the CSI between herself and Bob. On the other hand, in (1.9), a target rate is chosen by Alice based on some limited information about the channel between Alice and Bob. In this way, the target rate may be chosen smaller than the main link channel capacity in order to meet a certain reliability constraint. Hence, using (1.9), it is possible to ensure a certain level of reliability in the main link's channel and therefore, a secrecy outage occurs when the capacity of Eve's channel is within a margin of R_s of the target rate.

Works related to the secrecy capacity have recently been extended to different types of channels [17–20] as well. Moreover, practical techniques for secure information transmis-

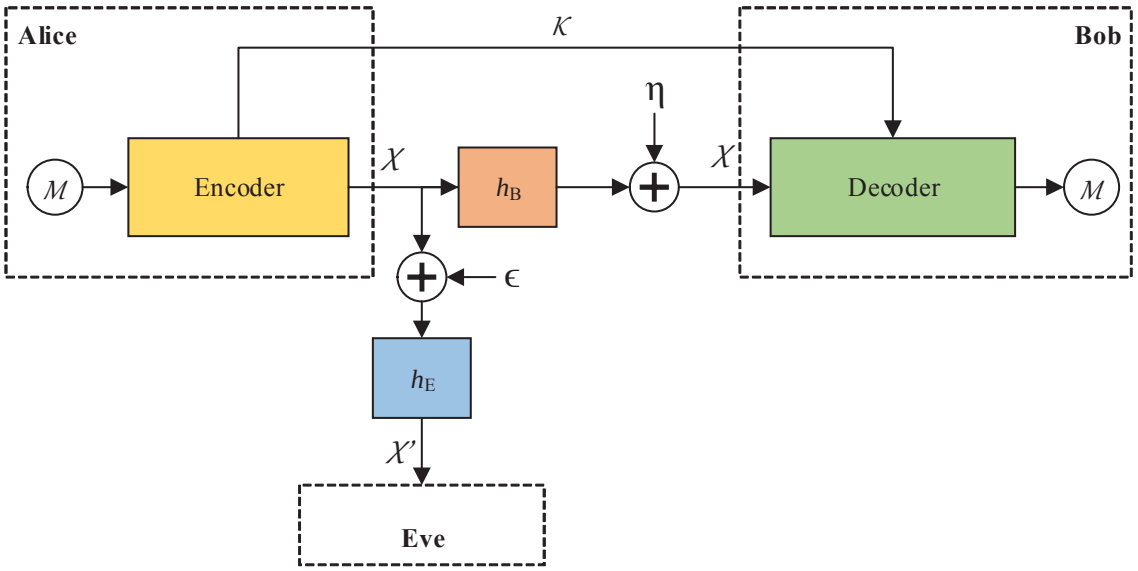

Figure 1.4. Secure information transmission model - note that we use h_B and h_E to represent the channels between Alice to Bob and Alice to Eve, respectively.

sion systems that make use of the fading channel were also presented in [21–23]. Arguably, the first scheme that proposed such a concept was [21]. Here, the the confidential message was encoded using the inverse phase of the CSI between Alice-Bob. When the signal is transmitted, the CSI between Alice-Bob acts as a decryptor, allowing Bob to retrieve the message. At the same time, the phase of the eavesdropper's channel, being different from the receiver's channel, prevented Eve from decoding the confidential information. The work in [22] extended this idea to multiple-input multiple-output (MIMO) communication systems.

Most popular amongst the class of secure information transmission systems is the study of multiple-input multiple-output (MIMO) channel models. The concept for the MIMO channel is that Alice has an advantage over the adversary in the form of available number of transmit antennas. Perhaps the most influential piece of work in this area is that of Goel et. al.[24, 25]. Here, it was shown that the advantage of having multiple transmit antennas allows for Alice to generate *artificial noise*. The produced artificial noise lies in the null-space of the Alice-Bob channel. At the legitimate receiver, the artificial noise is removed by the channel while the adversary's channel is degraded by this noise. The main result of this paper showed the existence of a secrecy scheme in which it is possible

to achieve a non-zero secrecy capacity even when Eve has a better channel than Bob and when Alice does not know the Alice-Eve CSI. The artificial noise transmission strategy is discussed in more detail in a later chapter in this dissertation. We will see that this strategy can be useful, not only for MIMO systems, but for spread spectrum technology as well.

1.2 The Wireless Channel

The primary focus of this dissertation is the study of physical-layer security enhanced by the utilization of the wireless channel. This section provides a sufficient background on wireless channels to educate the reader on forthcoming discussions in this work. For a more thorough overview of this subject, the interested reader is referred to [26–28], from where the overview in this section is mostly summarized.

In wireless communication applications, a transmitter sends a message to the intended receiver using electromagnetic (EM) waves generated using radio frequency (RF) equipment and broadcast through the transmitter's antenna. A high-level view of such a communication system is shown in Fig. 1.5. Once sent, the emitted EM waves propagate in all directions (assuming a standard omnidirectional transmit antenna). Hence, the signal does not reach the receiving antenna directly. Instead, the radio waves seen by the receiver are composed of many copies of the transmitted signal with different gains, delays, and phase-shifts. These *multipath* components constructively and destructively combine at the receiver to cause fading and distortion of the transmitted information. Oftentimes in the literature, fading is categorized in two main forms - large-scale and small-scale fading. As implied by the name, large-scale fading applies to large-scale networks in which fading is caused by the natural surroundings around the network. As an example, mountainous terrains exhibit different large-scale fading characteristics compared to urban areas. Moreover, within urban areas, communication networks surrounded with big buildings have different fading traits compared to residential areas and so on. The work in this dissertation will be predominantly associated with small-scale fading effects.

Small-scale fading is characterized by the combination of gains and delay shifts of the many multipath components arriving at the receiver. The multipath channel can be considered as having a "bandwidth", which is typically referred to as the *coherence bandwidth*. The coherence bandwidth is inversely proportional to the multipath *delay spread*,

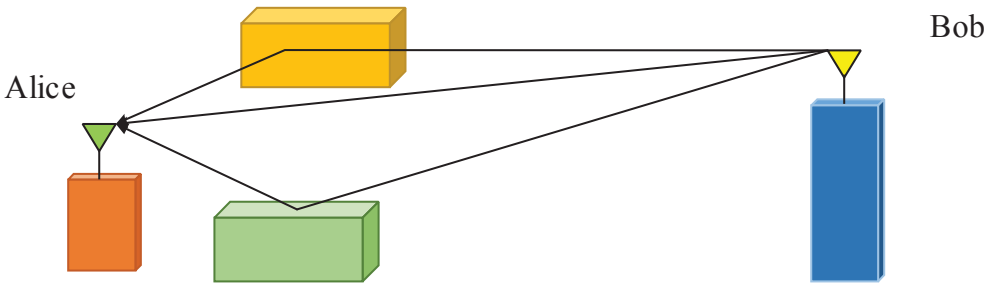

Figure 1.5. Wireless channel multipath propagation, black arrows show scattering

which describes the dispersion characteristics of the gains and time shifts of the multipath components of the channel. The multipath propagation between a pair of nodes is unique to that node-pair and depends on the surrounding objects responsible for the reflecting, scattering, and/or diffracting of the emitted EM waves. A slight location shift (on the order of a few wavelengths) by either the transmitter or receiver is sufficient enough to result in completely different fading characteristics (see Fig. 1.6). Furthermore, motion of the objects surrounding the nodes also induces changes in multipath propagation. Hence, the motion of the nodes (or motion surrounding the nodes) strongly influences small-scale fading. In fact, this type of motion induces a shift in received-signal's frequency - a phenomenon which is commonly called the Doppler shift. Related to the Doppler shift is the *coherence time*, which quantifies how static the channel is.

In general, there are four main types of small-scale fading experienced by a radio channels depending on the transmitted signal's time period and bandwidth relative to the coherence time and bandwidth of the channel. These four characterizations are shown in Fig. 1.7. When transmitting a narrowband signal - i.e., the bandwidth of the signal is much smaller than that of the channel - the fading across the signal's bandwidth will be largely correlated (i.e., flat) across the band. On the other hand, for frequency selective channels, the transmit signal bandwidth is large relative to the coherence bandwidth and thus the channel amplitude varies across the frequency domain. Slow and fast fading channels refer to the time-varying nature of the channel relative to the transmitted symbol period.

The type of small-scale fading considered in this dissertation is the frequency selective, block-fading channel model. The block-fading aspect here refers to the assumption that the channel is static over a "block" duration, after which time the channel may change. More-

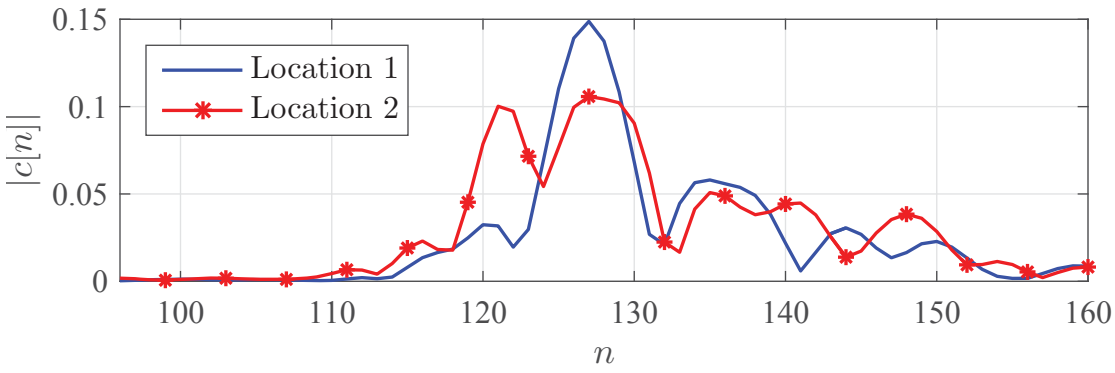

Figure 1.6. Example channel estimate from our experiment to show how a slight change in receiver position introduces different small-scale fading effects. In this example, a channel estimate was taken at location 1 and then the receiver node was moved by $\sim$ 1 meter (roughly 3 wavelengths) to location 2 where the second channel estimate was obtained.

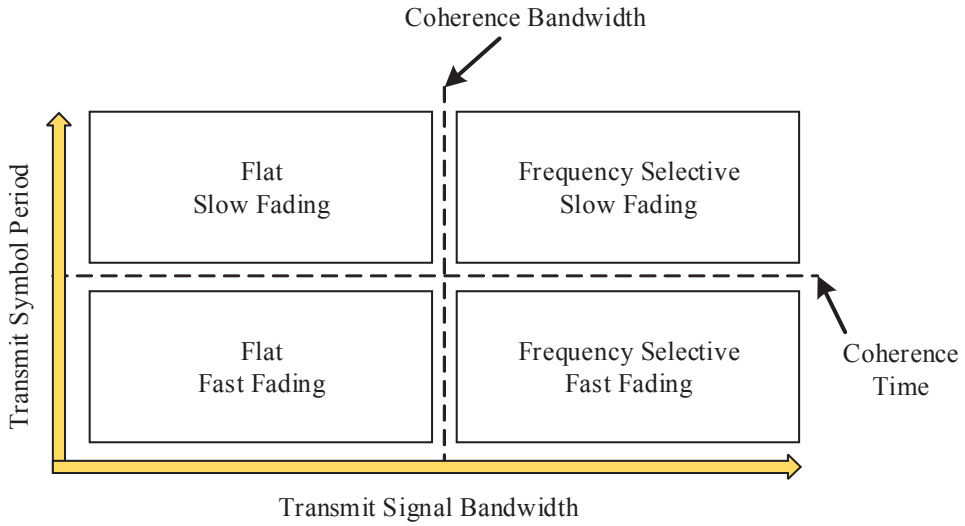

Figure 1.7. Illustration of different types of fading experienced by a signal as a function of transmit signal bandwidth and transmit symbol period. The boundary lines for coherence time and coherence bandwidth should be interpreted as soft boundaries.

over, the transmit sequence has a wide bandwidth relative to the coherence bandwidth and therefore, the channel is considered as frequency selective. These types of channels are often modeled as linear, time varying filters. The time-varying nature is caused by motion in the environment whereas the filtering nature of the channel is an artifact of the complex gains and time shifts of the multipath propagation. Due to the block-fading model assumption, the channel is assumed to be time invariant over a block duration and

therefore, we may simply represent the channel impulse response as

$$c(nT_s) = \sum_{i \in \mathcal{M}} \alpha_i p(nT_s - \tau_i) \tag{1.10}$$

where $\mathcal{M} = \{0, 1, \ldots, M-1\}$ and M is the number of multipath components. The sampling period is denoted by T_s. The parameters α_i and τ_i are the complex gain and delay associated with the i^{th} path and $p(t)$ is the combined responses of the transmit and receive filters. In this dissertation, we call $p(t)$ the *probing pulse*, because of obvious reasons that will become clear as we proceed.

In most real environments, any two different multipath components within the channel impulse response are uncorrelated with one another. In other words α_1 and α_2 are uncorrelated since the two gains are caused by different scatters. In the literature, this type of channel model is considered as having uncorrelated scattering (US) [27]. Furthermore, we call multipaths *resolvable* if the time difference between any two multipath delays is larger than the inverse bandwidth of the probing pulse. In a later section, we will discuss the simulation model that we use for the channel impulse response in (1.10).

In this dissertation, we are largely interested in the physical-layer security application of the wireless channel. Due to the *channel reciprocity* property, we use (1.10) to represent the reciprocal channel between two pairs of legitimate users (Alice and Bob). For any other user located more than a few wavelengths away from the legitimate parties (i.e., Eve), the channel is represented by

$$c'(t) = \sum_{i \in \mathcal{M}'} \alpha'_i p(t - \tau'_i). \tag{1.11}$$

Considering *channel independence over space*, the channel parameters in (1.10) and (1.11) are assumed to be independent of each other.

1.3 Multicarrier Spread Spectrum

In this section, we provide a brief background on multicarrier spread spectrum (MC-SS) technology since the secure information transmission system proposed in this dissertation is built around MC-SS-based systems. However, we should point out that the proposed secure communication idea can also be trivially adopted into competing SS systems such as direct-sequence SS (DS-SS), frequency-hopping SS (FH-SS), etc. Having said that, the extension of our design to other SS approaches is deemed outside the scope

of this dissertation. The following literature on MC-SS systems is recommended for the interested reader [29–31].

MC-SS, like its DS-SS and FH-SS counterparts, is merely a subclass of SS systems. The basic concept of SS communication systems is to *spread* a relatively narrow band transmit signal across a wide bandwidth. The spreading procedures allows for SS systems to achieve a *processing gain* - defined as the ratio of signal-to-noise ratio after and before despreading. The manner in which spreading is accomplished differs between SS technologies. For example, the main difference between DS-SS and MC-SS is that in DS-SS, the spreading is applied in the time domain while in MC-SS, the frequency domain is used.

There are many applications for which SS is useful. Examples are - anti-jamming, low probability of detection (LPD), low probability of interception (LPI), multiple-access, resilience to frequency selective channel fading, etc. [30]. MC-SS systems in particular have been shown to be resilient to partial and narrowband interference [31–33].

A block diagram of the transmitter for the MC-SS system is shown in Fig. 1.8. Here, the illustration shows that a data symbol is multiplied by the set of spreading gain sequences - $\{\gamma_0, \gamma_1, \ldots \gamma_{N-1}\}$. Following the multicarrier modulator block, each data symbol is spread across multiple subbands in the frequency domain. The subbands are sufficiently narrow band, and since fading on each narrow band subcarrier can be considered to be relatively flat, a simple one-tap equalizer can be utilized, thereby significantly reducing complexity of the design.

1.3.1 Filter Bank Multicarrier Spread Spectrum

A particular form of MC-SS, developed by our research group is called filter bank MC-SS (FB-MC-SS); see [29, 34–36] for more detail. Fig. 1.9 shows a simple diagram of the transmitter-receiver pair for the FB-MC-SS system.

In FB-MC-SS, the transmit signal is generated as

$$x(t) = \sum_{n} \sum_{k=0}^{N-1} \gamma_k s[n] h_k(t - nT) \tag{1.12}$$

where $s[n]$ is the n-th transmitted symbol, $h_k(t)$ are a set of non-overlapping filters, T is symbol interval, and γ_k are a set of spreading gains. The filters $h_k(t)$ all originate from the same prototype filter $h(t)$ and thus, are expressed as

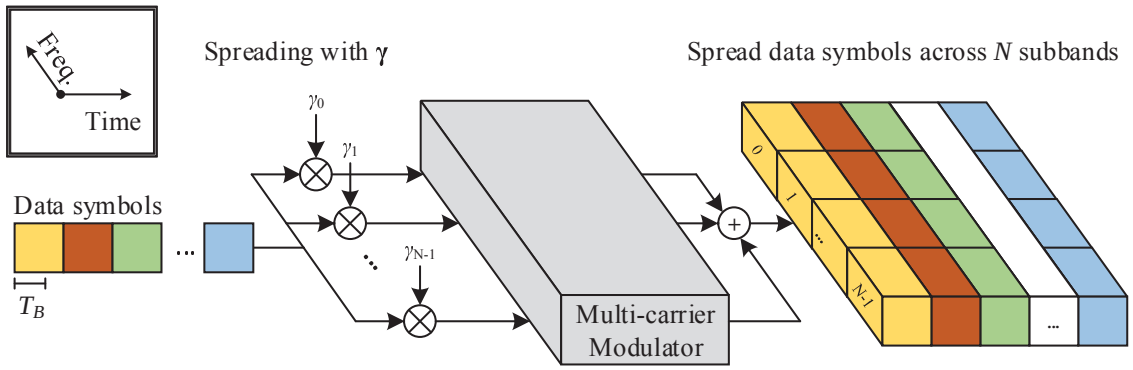

Figure 1.8. MC-SS transmitter diagram

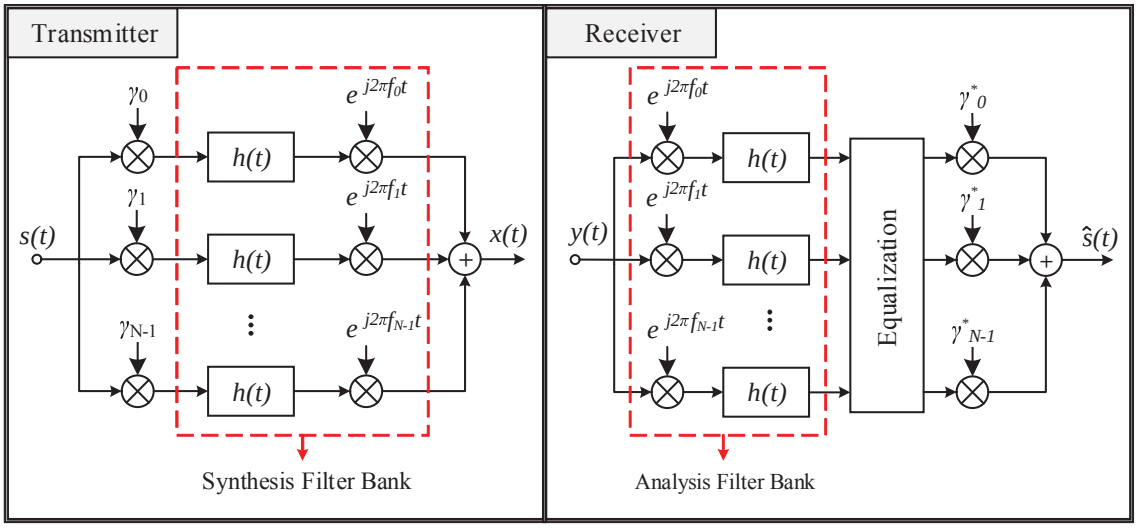

Figure 1.9. Simplified block diagram of FB-MC-SS transmitter and receiver

$$h_k(t) = h(t)e^{j2\pi f_k t} \tag{1.13}$$

where f_k are the centers of the subcarrier bands. In FB-MC-SS, as introduced in [34], $f_k = 4\pi/T$ and $h(t)$ is a square-root raised-cosine filter with the roll-off factor $\alpha = 1$. With these choices, the set of filters $h_k(t)$ are mutually exclusive in their pass/transition bands. Moreover, the *processing gain* achieved in this spread spectrum system is found to be $2N$, where N is the number of active bands, [34].

At the receiver, the data symbols $s[n]$ are recovered by linearly combining the the outputs of an analysis filter bank in which the subcarrier filters are matched to $h_k(t)$, for $k = 0, 1, \cdots, N-1$.

The advantage of the FB-MC-SS technique over other MC-SS-based waveforms is that

the use of non-overlapping filters do not leak across to other subbands. Hence, partial or narroband interference is limited only to the affected subcarriers. In [29], experimental evidence of the FB-MC-SS system outperforming the DS-SS system in an interference environment was shown.

1.3.2 Security in Spread Spectrum

As of today, the security in SS has been limited mostly to their spreading sequence. It is often simply stated that a SS message signal transmitted by Alice cannot be recovered without the right spreading code. However, very little has been said on true security of the SS systems and most security solutions in the implementations of SS are limited. In fact, surveys in [37] and [38] confirm that research in this area is open.

Real-world implementations of SS systems, e.g., IS-95 and IS-2000 standards [39], have used long-periodic psuedo-noise (PN) sequences in combination with a mask for physical-layer security. The mask is shared between the mobile and base station, while the long-code PN sequence is defined by a 42-bit linear feedback shift register with a *publicly* known characteristic polynomial. Despite the long period of the PN sequence, it has been shown that an adversary with reasonable computational resources can implement a brute force attack in as little as 2.2 seconds [37]. Li et al. [40] showed that an adversary with knowledge of the characteristic polynomial need only intercept 42 continuous long-code PN sequence bits to regenerate the entire long-code sequence. A solution proposed in [40] uses a combination of cryptography and physical-layer techniques to aid in scrambling the long PN sequence. However, the security of this method is reliant on the assumption of a computationally bounded adversary and is limited by secrecy of the encryption session key, assumed to be known *a-priori* in [40] between Alice and Bob.

1.4 Adversary Model

For the remainder of this dissertation, we will use the following model to characterize the adversary in our secure communication setup. We assume Eve is a passive eavesdropper and she can estimate the channel between herself and the legitimate parties. Eve performs the same steps as Alice and Bob in order to obtain her own key to detect the communicated data transmitted by Alice. Eve can be near the legitimate users (i.e., in our

experiments, her antenna is placed 1/3 meter away from Bob), but she cannot be in the *exact* same location as Alice or Bob. Eve does not transmit channel probes and our current security solution does not authenticate the nodes. Eve does not jam the parties during channel probing, nor does she modify the transmitted messages before they are received by a legitimate party. Moreover, it is assumed a sufficiently clean channel is available between Alice and Bob so that they can obtain reciprocal estimates.

1.5 Dissertation Contributions

This dissertation describes the development of a wireless security solution for SS systems, though the focus is kept on MC-SS for the simplicity it offers. A side contribution of this dissertation which has resulted in an evolution of the implementation of the FB-MC-SS system in [34] was reported in [35] and [41] - the latter of which was awarded a *Best Demonstration Award* in 2012's IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN).

The main contribution of this dissertation is in the design of a robust secure information transmission solution for spread spectrum communication. The system has two main parts. First, we use the reciprocal wireless channel to derive a pair of keys shared between two legitimate users. Next, the key is used as an integral part of our proposed secure information system.

The key generation algorithm that we propose allows for two asynchronous users to obtain a key using the estimated channel impulse response (CIR). A significant problem for keys generated using CIR estimates - for which we have identified and contributed a solution to - is the time and phase misalignment between Alice and Bob's obtained CIRs. Related to this matter, we also contribute an augmentation - called strongest path cancellation (SPC) - to the key generation protocol.

For the second part of the secure communication system, we introduce the concept of artificial noise to spread spectrum systems. For this system, a unique artificial noise power allocation strategy is proposed which ensures a level of high reliability for the main link. Finally, we study a blind-detection attack on the secure information transmission system and such attacks, when limited to the use of the second order moments of the received signal, can be avoided.

A preliminary version of this system resulted in [42] and was awarded a travel grant by the MILCOM conference in 2015. An update to this paper - entitled *Fault Tolerant Key Generation and Secure Spread Spectrum Communication* - has been submitted to IEEE Wireless Transactions and is pending review.

1.6 Structure of Dissertation

The organization of this dissertation largely follows the block diagram of the proposed secure information transmission system shown in Fig. 1.10. For the first step, Alice transmits a beacon signal to Bob who detects and transmits a beacon back to Alice. This step is called channel probing and the implementation details of this protocol are highlighted in Chapter 2. Following channel probing, the topic of channel estimation, key generation, and other postprocessing steps are also discussed in Chapter 2.

Chapter 3 expands on time and phase synchronization and includes a study comparing and contrasting different approaches that can be used to solve the problem. Furthermore, the augmentation of *Strongest Path Cancellation* naturally follows in this section. The combination of Chapters 2 and 3 completes the key generation portion of the dissertation - i.e., the first two blocks in Fig 1.10. In Chapter 4, the last block in Fig 1.10 is described. In this step, Alice encodes confidential information symbols using her spreading codes (key) and adds artificial noise prior to transmission. Bob applies his own spreading sequence to the received data for detection of the information symbols and to remove artificial noise. Finally, concluding remarks are given in Chapter 5 along with possible future research activities.

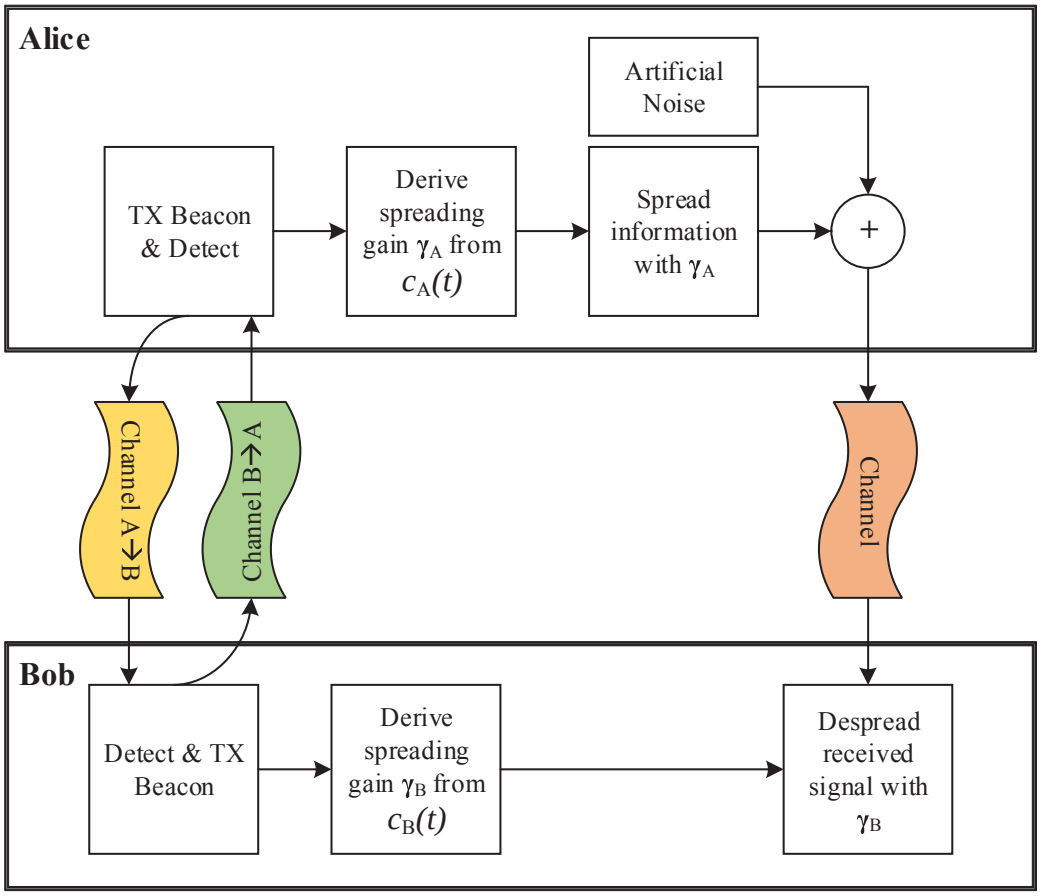

Figure 1.10. Block diagram of secure information transmission system.

CHAPTER 2

SECURE KEY GENERATION

In this chapter, we detail the first set of steps that will allow for two parties to engage in reciprocal channel-based key exchange. This chapter will include a discussion about channel probing, a thorough description of our channel estimator, as well as a channel gain and delay estimator. Details about the simulation and experiment channel model are also given. This chapter, as well as the entire dissertation, uses the terms spreading code vector, key, spreading gains, and spread sequence interchangeably.

2.1 Related Work

In this dissertation, we will discuss the use of the properties of the wireless channel in order to enhance the security level of the spreading gains in spread spectrum systems. Application of the wireless channel in security applications is not new. In fact, there have been many papers that discuss use of the salient features of the wireless channel to enhance security in a wireless communication network. A good set of surveys in this area are [2, 8–10]. There are papers that discuss *physical-layer key generation*, *secure information transmission*, and those that discuss the aspect of theoretical security based on the bounds of secrecy capacity.

In physical-layer key generation, researchers use the wireless channel to obtain a secret key (see Fig. 1.3). In this line of work, research has focused on extracting a secret key that must 1) be highly similar between Alice and Bob, 2) have high entropy, and 3) have a high key generation rate. The secret key rate is highly dependent on the variations of the channel as well as the degrees of freedom available in the estimate channel.

To increase variations in the channel, the concept of specialized electronically steerable antennas to create artificial channel fading was introduced in [43]. This was later reinvestigated in [44] from an information-theoretic standpoint. In short, special care must be taken with these devices to ensure that the artificial fading induced by these antennas cannot be

learned by the adversary.

Other methods to enhance the key generation rate in physical-layer key generation techniques have been discussed as well. For example, user-mobility has been proposed to enhance key generation rate [45]. In [46], it was shown through experimentation that the received signal strength (RSS) from the multiple antennas available to MIMO radios increases the degrees of freedom in a given estimate of the channel. In turn, this was shown to increase key generation rate. Similar to the idea of using MIMO transceivers, the work of Premnanth et al. [47–49] discusses the concept of increasing secret key generation rates by using a MIMO-like system. A MIMO-like system, as opposed to a MIMO system, is one in which multi-antenna capability comes from a collaboration of nodes each using a single antenna, rather than from a single node equipped with multiple antennas. In this collaborative system, one of Alice's multiple set of nodes transmits a probe to Bob's MIMO-like set of nodes. All of Bob's nodes record the measurement from one of Alice's nodes. The process is repeated across all of Alice's nodes. Once all of Alice's nodes have had their turn, Bob repeats the procedure so that Alice's nodes can obtain a reciprocal estimate of the channel. Challenges - which are addressed in [47–49] - of such MIMO-like systems arise from the significant amount of time required by each set of users to probe the channel that connects the two parties.

Another effort to enhance key generation rates was made by Wilson et al. [50], who derives the mutual information of the wideband channel case. The authors of [50] show that extracting keys from the multiple independent multipath components of the channel - as opposed to using just the RSS - can significantly boost the key generation rate. Another interesting discussion in this report is the connection between bandwidth and secret-key rate. Although the bandwidths analyzed in the report mostly apply to ultra-wideband (UWB) radios, it was shown that increasing the bandwidth past a given point - depending on the delay spread of the channel - provides diminishing returns. Theoretical maximum key lengths of up to 150 bits at 30 dB for NLOS UWB type channels were shown to be achievable in [50].

The secret key rate that was found in [50] was derived in the context of UWB channels. Another approach was taken in [51] which considers channels of much narrower bandwidth compared to UWB channels. The challenge of such ”non-UWB” channels is that the

bandwidth may not be sufficient enough to resolve the individual multipaths components of the channel. In [51], Ye et al. derive an *upper bound* to the maximum key length that can be extracted by Alice and Bob from i.i.d observations of the channel. When multipaths are not resolvable due to bandwidth constraints, the maximum achievable key rate is less than the derived upper bound.

The theoretically derived expressions for the key rates in [50] and [51] only consider randomness of the complex gains of multipath fading channel. Following this assumption, both reports propose that the upper bound of the achievable key rate can be obtained when a statistical model of each individual multipath components is available. In this context, the power delay profile of a given channel model can be plugged into the equations in [50] and [51] to find an upper bound for achievable key rates in UWB and non-UWB channels, respectively. One important piece of information about the wireless channel that we believe can possibly increase achievable key rates are the time-delays of the channel. Through intuition from our experiments, we've found that the time-delays of each of the individual multipath components of the channel can possibly contribute to increasing the randomness of the keys derived from multipath fading channels. However, the derivations of this result are not within the scope of this dissertation because in this dissertation, we are interested in developing a secure information transmission solution for SS systems rather than a physical-layer key generation system.

Complementary to the research of [50] is the work of Liu et al. [52] which shows that key extraction based on the entire channel state information (CSI) achieves superior key rate performance than RSS-based methods that are most commonly used. It should be noted that although increased diversity in CSI estimates is useful in terms of the key generation rate, it is more complex to implement the CSI-based key generation techniques due to the fact that RSS information is readily available in standard radios.

Many works within the physical-layer key generation scope have reported implementations and issues therein of RSS-based key generation [49, 53–56]. RSS is a popular statistic of the radio channel because of its availability in most off-the-shelf wireless cards. It can easily be measured without any modification on a per frame basis. In one of the pioneering literature pieces on the implementation of RSS-based key generation, Mathur et al. [53] report two successful implementations of secret key sharing using off-the-shelf

802.11a devices. The two implementations make use of RSS and CIR information of the channel to achieve a key rate of approximately 1 bit per second. Premnath et al. [49] examine key generation using RSS information available in 802.11-based laptops. In [49], the authors examine key generation in different types of indoor environments where the environment are characterized by the variations in the channel. By building upon the work of [53], [49] proposes an environment-adaptive secret key generation technique which adapts according to RSS variation. Implementation of this architecture was validated in 802.11-based laptops. In a later piece by the same author, the key generation method discussed in [49] was used in evaluating secret key generation using Bluetooth radios [54].

The work of Croft et al. [55] was among the first to validate the practicality of high-rate RSS-based physical-layer key generation. Implemented on TelosB wireless sensors, key generation rates of up to 22 bits per second with approximately 4% probability of bit disagreement were reported using the proposed HRUBE key generation method. This paper was then extended to a method called ARUBE [56]. Here, rates of up to 40 bits per second with the same 4% probability of bit disagreement were obtained using TelosB wireless sensors. Implementation issues that are brought up in [55, 56] and solved accordingly are: 1) mismatch due to fractional timing offset between Alice and Bob, 2) trade-off of high key generation rate versus low probability of bit disagreement, and 3) temporal correlation in channel measurements. The issue of temporal correlation is discussed in other works as well [57–59], though with different solutions. In particular, the study in [58] has looked into the temporal correlation in UWB channels due to slow fading. In [58], a linear channel prediction algorithm was proposed to remove predictable estimations. Similarly, the proposed idea can be used as a decision mechanism through which Alice and Bob can decide when to probe the channel. A related study in [59] has looked into sampling the wideband channel at a percentage of the coherence time intervals and issues thereof. It was suggested in this report that often using 50% coherence time sampling may be insufficient to ensure randomness of the key in slow fading channels.

Another group's [60, 61] work in this area is in the validation of properties of the wireless channel for ultra-wideband measurements. Of particular interest in their work is that they are one of the few to consider the similarity between Bob and Eve's measured channel. One of their findings is that using the envelope of the channel measurements yields high

cross-correlation between Bob and Eve's channel vector - suggesting the possibility of successful passive attacks.

In summary of our discussion of *PHY-layer key generation*, we note that these sets of methods focus on obtaining pairs of keys which are identical to one another- e.g., the keys are by design *fault-intolerant*. This criterion requires for both nodes to either 1) engage in a lengthy period of measurements so that channel noise can be averaged out to a sufficiently low level or 2) repeat multiple iterations of *information reconciliation* to compensate for non-reciprocities in the channel measurements. This significantly slows the throughput of the key generation system. Additionally, many in the field do not consider the significant *communication cost* [62] of *information reconciliation*. This cost is due to the fact that the information passed between legitimate parties must be communicated error free which requires proper digital modulation that includes overhead due to synchronization, forward-error correction, channel training and equalization, MAC information, etc.

In the context of our work for SS security, we note that the processing gain of SS systems allows some tolerance of mismatch of spreading codes used by the two communicating parties. Thus, SS provides an interesting opportunity to implement a secret key-based communication system that is *fault tolerant* to a mismatch of the keys generated by Alice and Bob if the key is used as a set of spreading codes for SS.

2.2 Channel Probing

Suppose now that we have the following problem. Two sets of authenticated users (Alice and Bob) wish to communicate across a wideband channel securely with a multi-carrier spread spectrum (MC-SS) technique. To do so, the parties need to somehow set up identical, or near identical, spreading code vectors in the presence of a knowledgeable adversary (Eve) who knows the protocols through which the legitimate parties set up spreading codes. If Eve can somehow obtain the same spreading code that Alice and Bob are using, then we deem the security of this system to be compromised.

We make use of the reciprocal wireless channel to set up these spreading codes so that codes are highly correlated for two users on opposite ends of the same link while statistically uncorrelated for any adversary located in a different position from Alice and Bob.

The first step in this endeavor is referred to as channel probing. The concept itself is fairly simple - Alice transmits some beacon signal to Bob so that he can estimate the channel connecting the two users. Bob, upon hearing Alice's beacon, follows up by transmitting a beacon back to Alice for her own channel estimation purposes. The channel that is probed must be estimated at the same frequencies for both links. Thus, to avoid interfering with one another, they must resort to a time-division duplex (TDD) method.

The diagram in Fig. 2.1 shows this simple procedure. Ideally, the probe should be sampled at coherence time intervals, so that the same frequency-selective channel is not estimated over and over again. In practice, however, channel probing is not quite as simple. Real-world scenarios include cases in which Alice or Bob do not hear one another, synchronization between the two is off, the users need gain adjustment in their received signals, etc. Thus, special care must be taken in practical channel probing algorithms. Fig. 2.2 depicts a state machine of the channel probing that we have implemented. It is a more complex variant of the mechanism depicted in Fig. 2.1.

The channel probing protocol depicted in Fig. 2.2 starts with a crucial *Synchronization Stage* used to control the digital and analog gains depending on the received signal data. In this way, if two nodes are placed too close to one another, the gains are adjusted so that clipping of the received signal does not occur. The opposite situation is also configured so that when nodes are too far away from one another, gains are adjusted so that quantification noise does not significantly impact the received signal. The synchronization stage is completed when the two parties have obtained P packets. If at any point, should the two nodes timeout due to not receiving an acknowledge packet from the other node, the two nodes adjust their gains and restart the *Synchronization stage* all over again.

At the end of this stage, Alice and Bob both obtain the average power in their received data and use it to control the digital and analog gains. Note that the power is averaged over many packets to minimize errors due to channel noise. As long as there is little difference in the radio frequency (RF) hardware between the two nodes, the gains configured of Alice and Bob will be roughly the same. Note that the gains configured at the end of the *Synchronization Stage* are not reconfigured in the *Channel Probing Stage*. This is to make sure that either Alice or Bob do not reconfigure these parameters as it introduces a non-reciprocity in the channel estimates that is software-based.

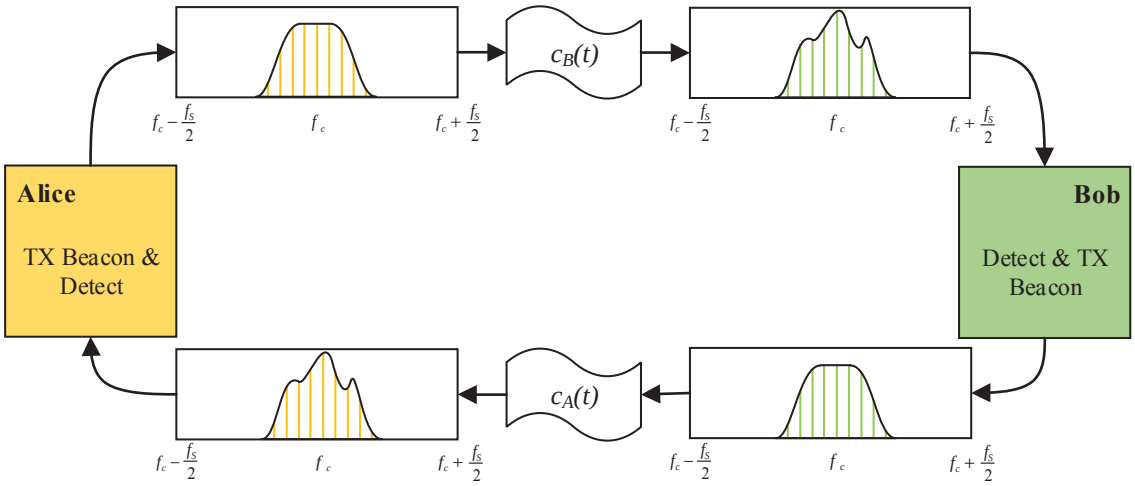

Figure 2.1. High-level description of the channel probing method.

In the *Channel Probing Stage*, Alice acts as the master and Bob as the slave. Each state starts a timer which will be used to dictate when a timeout has occurred. After the *Synchronization Stage* ends, Alice's transmits a beacon to Bob. If Bob acknowledges that the beacon has been received, he sends a beacon back to Alice and the timer is reset. Once Alice receives a beacon back from Bob, she resets her timer as well and the two nodes start again after a channel coherence time period. If at any point should either of the two nodes timeout, both nodes will remain silent and proceed back to the *Synchronization Stage* since the digital gains need to be updated.

Note that the channel coherence time period is itself a fuzzy quantity. It should ideally be known *a-priori*. However, the true nature of the channel is difficult to describe statistically as it depends on the environment in which the two nodes are communicating. If the two nodes are sitting in a static environment for example, the channel coherence time is indefinite and thus, the estimates of this static channel would generate the same key. In our implementation, we have set the probing system so that measurements are made once every second and that movement around one of the nodes ensures enough channel variation in time so that the same key is not generated over and over again. Note that the key generation discussed in this dissertation uses channel frequency selectivity as a source of obtaining randomness as opposed to time variation of the channel.

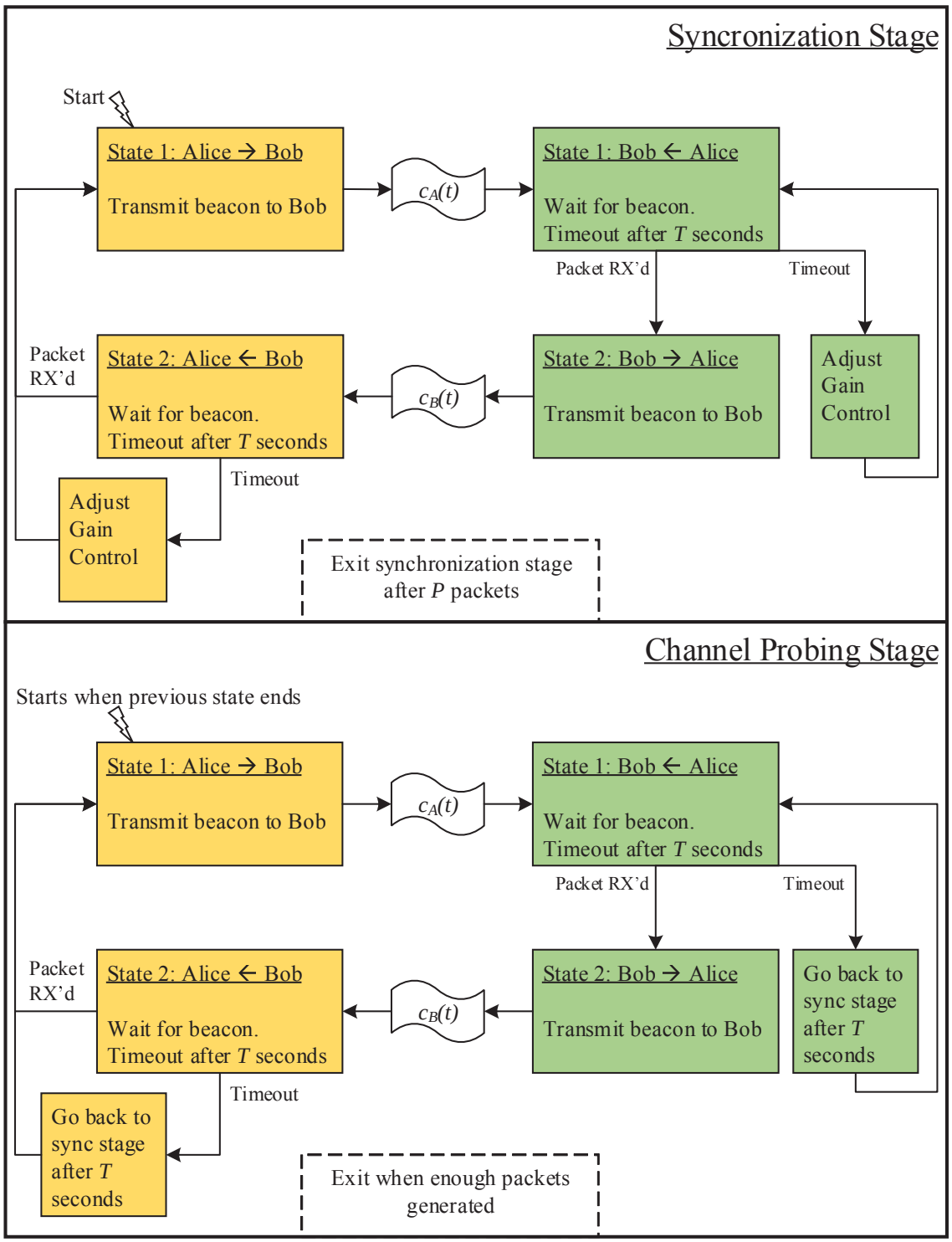

Figure 2.2. State machine of the implemented channel probing protocol.

2.3 Transmitter Design

The transmit sequence that we use is an N length Zadoff-Chu polyphase sequence [63, 64]. The sequence is formally defined for even values of N as

$$s[n \bmod N] = e^{(\frac{i\pi n^2}{N})}. \tag{2.1}$$

The Zadoff-Chu sequence has seen widespread use in LTE and UMTS systems [65] due mostly to its special signal processing properties, most notably that it is orthogonal to cyclic shifts. To show this, we define the $N \times N$ matrix

$$\mathbf{S} = \begin{bmatrix} s[0] & s[N-1] & s[N-2] & \dots & s[1] \\ s[1] & s[0] & s[N-1] & \dots & s[2] \\ s[2] & s[1] & s[0] & \dots & s[3] \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s[N-1] & s[N-2] & s[N-3] & \dots & s[0] \end{bmatrix} \tag{2.2}$$

and it can be shown that this is an orthogonal matrix - i.e.

$$\frac{1}{N}\mathbf{S}^{\mathrm{H}}\mathbf{S} = \frac{1}{N}\mathbf{S}\mathbf{S}^{\mathrm{H}} = I_N. \tag{2.3}$$

which shows that $s[n \bmod N]$ is orthogonal to cyclic shifts. We will find that this property is useful for channel estimation.

A block diagram describing the transmitter is shown in Fig. 2.3. The transmit sequence is appended with multiple copies of itself to allow for signal averaging at the receiver for more precise channel estimation. In total, K repetitions of the transmit sequence form the beacon signal - i.e., $n = 0, 1, \dots NK-1$. It is then pulse-shaped with a square-root raised cosine filter $p_{\mathrm{T}}[n]$ with roll-off factor of $\frac{1}{2}$. The output at the end of this step can be written as

$$x(t) = \sum_n s[n \bmod N] p_{\mathrm{T}}[t - nT_b]. \tag{2.4}$$

where $T_b = T_s L$ is the time interval between beacon symbols and T_s is the sampling interval of the ADC. The output $x(t)$ in (2.4) is up-converted to the desired radio frequency (RF) band and transmitted.

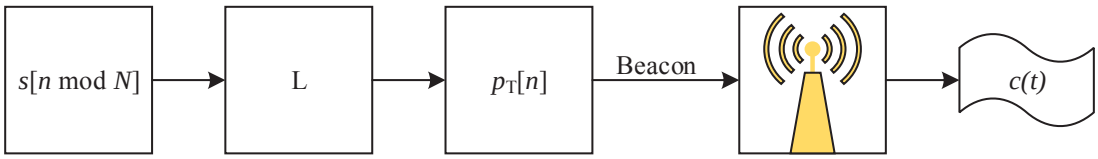

Figure 2.3. Block diagram of channel probing transmitter

2.4 Channel Estimation

The received signal samples, after demodulation to baseband, are filtered with $p_R(t)$ - a filter matched to $p_T(t)$. Ignoring channel noise for the time being, this results in a received signal that is periodic with NL and is equivalent to

$$y(t) = \sum_n s[n \bmod N] c(t - nT_b)\,. \tag{2.5}$$

The received data is sampled at discrete time intervals equally spaced at intervals of T_s. Next, by decimating a period of $y(t)$ by a factor of L, we obtain L signal vectors, each of length N. We denote these vectors by $\{\mathbf{y}_\ell | \ell = 0, 1, \cdots, L-1\}$. These relate to L decimated samples of the impulse response of the equivalent baseband channel, $c(t)$, according to the equations

$$\mathbf{y}_\ell = \mathbf{S}\mathbf{c}_\ell \tag{2.6}$$

where

$$\mathbf{y}_\ell = [y(\ell T_s) \;\; y(\ell T_s + T_b) \;\; \ldots \; y(\ell T_s + (M-1)T_b)]^{\mathrm{T}} \tag{2.7}$$

$$\mathbf{c}_\ell = [c(\ell T_s) \;\; c(\ell T_s + T_b) \;\; \ldots \; c(\ell T_s + (N-1)T_b)]^{\mathrm{T}}\,. \tag{2.8}$$

A least-squares estimate of the channel response following (2.6) can be obtained for $\mathbf{c}_\ell$ as follows

$$\mathbf{c}_\ell = \frac{\mathbf{S}^{\mathrm{H}}\mathbf{y}_\ell}{\mathbf{S}^{\mathrm{H}}\mathbf{S}} \tag{2.9}$$

$$= \frac{1}{N}\mathbf{S}^{\mathrm{H}}\mathbf{y}_\ell \tag{2.10}$$

where (2.10) follows from the fact that the transmit signal is orthogonal to cylic shifts (2.3).

Solutions to $\mathbf{c}_\ell$ (2.10) for $\ell = 0, 1, \cdots, L-1$, give a set of components of the channel impulse response which can be interleaved to construct a channel impulse response vector of length LN. This process which is performed by Alice, Bob, and Eve leads to the respective CIR estimates that we denote by $c_A[n]$, $c_B[n], c_E[n]$. This channel estimation technique is

advantageous in that it allows us to obtain the samples of CIR at a high resolution in time with a relatively low complexity, [66]. This, as will be found later, will become instrumental in development of an effective key generation algorithm.

2.4.1 Discussion of Channel Probing Parameters

The parameters associated with channel probing and estimation are L, N, and K which respectively represent the oversampling factor, the length of the transmit sequence, and the number of transmit sequences within a beacon. The discussion in this section details how these parameters were chosen for our experiment.

The oversampling factor L is determined by the bandwidth given to us in practice. In our case, following the implementation of the FB-MC-SS system in [35] to which the work in this dissertation applies, the total given bandwidth is 32.5 MHz with a sampling rate of $T_s^{-1} = 130$ MHz. Therefore, we use an oversampling factor of $L = 4$. Given that the probing pulse is derived from a root-raised cosine filter with a roll-off factor of $\frac{1}{2}$, the 32.5 MHz bandwidth of the transmitted signal corresponds to the 3 dB bandwidth.

Next, the factor N should be chosen such that the maximum length of the channel can be resolved by the transmit sequence. Otherwise, if the channel leaks across packets, the time averaging of multiple transmit sequences will incoherently average the signal resulting in significant channel estimation error. For our measurement campaign, we selected $N = 128$, though it was later found that all measured channels fit well within a temporal window corresponding to $N = 64$. Following channel estimation, the number of samples in the truncated CIR estimate is equal to $LN = 256$, which gives the CIR a duration of $\sim 2\mu s$.

Finally, the value of K should ideally be set according to the expected channel coherence time interval. A high value of K allows more time averaging in the received signal and therefore reduces the effects of channel noise. Increasing K will expand the beacon duration. If the beacon duration is such that the block fading model is no longer applicable, the time averaging process is not guaranteed to constructively average the received signal and therefore, increasing K too much can also add significant estimation error.

To determine a value of K, we need an expected value for the channel coherence time T_c as well as the *channel probing time duration* - defined as the time it takes for Alice to estimate

Bob's channel and vice versa, i.e., the time it takes for Alice to switch between transmitter and receiver. To determine K, the total duration of Alice's and Bob's beacons plus the channel probing time duration - denoted by T_p - should be set equal to the expected value of T_c. In our implementation of the channel probing system, we successfully managed to keep the channel probing time duration to a value $\sim$ 1 ms. The total time duration of the transmitted signals of Alice and Bob is equal to $(2 \cdot K \cdot LN) \times T_s$.

In our experiment, we set $K = 30$ and note that approximately 5 transmit sequences are used for packet detection. This gives a beacon duration of $\sim$ 0.12 ms which means that so long as the coherence time of the channel is greater than $T_p \approx$ 1.24 ms, the estimated CIR should be sufficient. It should be noted that this is approximately one order of magnitude smaller than expected values of coherence time intervals in indoor environments (typically a value in the order of 10 ms is used [59]). In retrospect, we note that the value of K could have been set higher so that better channel estimation could have been accomplished. However, a minor detail regarding our choice of K is as follows. The time-varying nature of the channel is not exactly abrupt and the channel coherence time is a soft value. The CIR may slowly vary from one estimate to another a coherence time period away. This slow variation of the channel may increase error from the block-averaging procedure. In short, setting K is not an exact science - a given K may work for one environment yet can be too high for the very same environment at different periods of the day due to fluctuation.

2.5 Channel Gain and Delay Estimation

Following channel estimation, the CIR path gains and delays are estimated for the purpose of time and phase alignment which is discussed in the following chapter.

To start, Alice and Bob interpolate their respective CIRs $c_{\mathrm{A}}[n]$ and $c_{\mathrm{B}}[n]$ by a factor of L_2. This further increases the time resolution of the available samples. The remaining steps are performed on these interpolated CIRs which we call $\tilde{c}_{\mathrm{A}}[n]$ and $\tilde{c}_{\mathrm{B}}[n]$ and assume to be a good approximation to the respective continuous time functions. In the subsequent discussions, we refer to the length of the interpolated CIRs $\tilde{c}_{\mathrm{A}}[n]$ and $\tilde{c}_{\mathrm{B}}[n]$ as N_c.

After interpolation, both nodes estimate the "path candidates" in their respective CIRs. Path candidates are considered to be a combination of estimated path gains and delays, which for Alice are respectively denoted by $\tilde{\alpha}_{i,\mathrm{A}}$ and $\tilde{k}_{i,\mathrm{A}}$, for $i = 0, 1, \cdots, M-1$, and are

similarly defined for Bob. These parameters are determined by taking the following steps. Here, we have removed the subscripts A and B for simplicity, but it should be understood that the presented steps are applied to both $\tilde{c}_{\mathrm{A}}[n]$ and $\tilde{c}_{\mathrm{B}}[n]$.

Step 0: Initialize $i = 0$ and $\tilde{c}_i[n] = \tilde{c}[n]$.

Step 1: Let

$$[\tilde{k}_i, \tilde{\alpha}_i] = \arg\min_{\tilde{k}_i, \tilde{\alpha}_i} ||\tilde{c}_i[n] - \tilde{\alpha}_i p[n - \tilde{k}_i]||^2. \tag{2.11}$$

Step 2: Remove path candidate i from the CIR by taking

$$\tilde{c}_{i+1}[n] = \tilde{c}_i[n] - \tilde{\alpha}_i p[n - \tilde{k}_i]\,. \tag{2.12}$$

Step 3: Increment i by one and repeat **Step 1** and **Step 2** until $i = M$.

The result of this step gives $(\tilde{\alpha}_{i,\mathrm{A}}, \tilde{k}_{i,\mathrm{A}})$, $(\tilde{\alpha}_{i,\mathrm{B}}, \tilde{k}_{i,\mathrm{B}})$, and $(\tilde{\alpha}_{i,\mathrm{E}}, \tilde{k}_{i,\mathrm{E}})$ for Alice, Bob, and Eve, respectively. It will be seen in the following chapter that this aids in the proper synchronization of the time and phase offsets between Alice and Bob's CIRs.

2.6 Key Generation

The channel gain and time delay estimates are used in time and phase synchronization. At this time, we will move forward as if synchronization has been properly executed according to the procedure in the subsequent chapter.

The final step in obtaining a spreading code sequence from the reciprocal wireless channel is outlined here. All parties follow the same procedure as Alice who first takes the DFT of the time and phase aligned channel estimate and stores it in $\mathbf{C}_{\mathrm{A}}$. Next, a key is constructed as

$$\left\{ \gamma_{\mathrm{A}} = \frac{\mathbf{C}_{\mathrm{A}}[\mathbf{m}]}{\|\mathbf{C}_{\mathrm{A}}[\mathbf{m}]\|} \;\middle|\; \mathbf{m} \in \left[\text{Passband of } \mathbf{C}_{\mathrm{A}}\right] \right\} \tag{2.13}$$

by Alice. Similarly, Bob and Eve respectively generate γ_{B} and γ_{E}.

At this point, we note that further processing can be applied to build an arguably more secure key. For instance, in one particular idea reported in [41], the key is generated according to the following steps.

1. The vector $\mathbf{m}^{\mathrm{s}}$ which is obtained by a random shuffling of the elements of $\mathbf{m}$ is generated

2. Define the phase vector $\Theta = \angle(\mathbf{C}_{\mathrm{A}}(\mathbf{m})) + \angle(\mathbf{C}_{\mathrm{A}}(\mathbf{m}^{\mathrm{s}}))$

3. Construct the following vector as the key

$$\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{s}} = e^{j\Theta} \tag{2.14}$$

This effectively gives a key that is the summation of the phase of the channel frequency response with a shuffled version of the same signal. This key has a nice property which further decorrelates Eve's key from the legitimate users'. In a later section, we will compare keys against one another when they are used as part of the secure information transmission system.

The key generation procedure discussed so far in this chapter is summarized in Fig. 2.4. Once obtained, these sequences are used as an integral part of the secure information transmission communication system.

2.7 Wireless Channel Models

To help in evaluating the various different ideas discussed in this dissertation, we use both simulation and experimental channel data. The simulated channels follow a standard approach that is prevalent in wireless communication research. The experimental data set was obtained through a measurement campaign in environments in which we expect the proposed design to work. The simulation model is given so that results can be numerically confirmed and evaluated while measurement data confirms the practicality of our proposed system. The details related to these two types of channels are discussed in this section.

2.7.1 Simulation Model

The wireless channel simulation model considered in this dissertation is relatively simple. It should be noted that there is a significant amount of research in the field of wireless channel modeling and that there are many channel models other than the one we use. For a more thorough description of wireless channel modeling, we recommend [28].

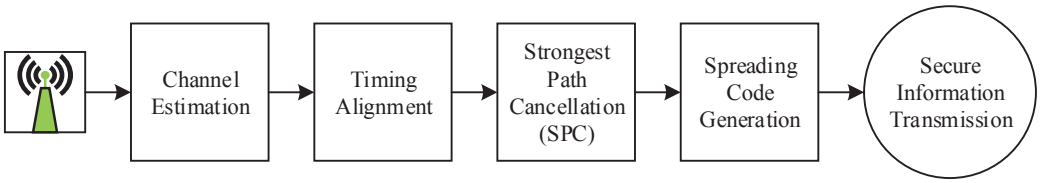

Figure 2.4. Block diagram of proposed key generation method in which spreading gains are generated from the channel impulse response. Note that the time alignment and strongest path cancellation blocks are discussed in the next chapter.

The model of the wireless channel that we will make use of follows a multipath Rayleigh fading channel model adopted by the IEEE 802.11 Working Group for software simulations [67]. A nice feature of this channel simulation model is that it only requires one parameter to be defined - the mean delay spread [27]. This is because the root mean square (rms) delay spread and the mean delay spread are the same for the exponentially distributed power delay profile. The discrete-time exponential channel model is defined as

$$A_c[k] = A_c[0]e^{-kT_s/\bar{T}_m} \tag{2.15}$$

where

$$A_c[0] = 1 - e^{-T_s/\bar{T}_m} \tag{2.16}$$

and $\bar{T}_m$ is the mean delay spread parameter.

Due to uncorrelated scattering, the tap gains - α_i - and delays - τ_i - of the channel expression in (1.10) are set in the following manner. The tap delays are uniformly sampled at intervals of LT_s. The complex-valued gain of each multipath component is Rayleigh faded. However, we do note that the first multipath component may at times follow a Rician distribution to simulate a line-of-sight (LOS) multipath wireless channel, in accordance with the IEEE 802.11 wirless channel report in [**?**].

2.7.2 Experimental Channel

In addition to a simulation model for the wireless channel, real-world results are also obtained to confirm satisfactory operation of the proposed system. We validate our methods with a transceiver based on the National Instruments (NI) platform. The transceiver consists of an NI FlexRIO FPGA Module (NI PXIe-7975R). This module is connected to an NI FlexRIO RF Transceiver (NI 5791R), which has a sampling rate of 130 MHz. The FPGA

and transceiver module are both connected to an NI real-time controller (NI PXIe-1082), which is used as a host PC and is programmed using NI LabVIEW Real-Time. The FlexRIO RF Transceiver is connected to a circulator (Model No. CS-0.900) that is fed to an RF amplifier (NI PXI-5691) and then to a single antenna. All three parties in our experiment (Alice, Bob, and Eve) use identical transceiver setups and Eve's transmitter is turned off. Experiments are run at a carrier frequency of 900 MHz.

Time-division duplexing is used for channel probing. The duration of each transmitted packet, consisting of multiple repetitions of the ZC sequence, is 118$^-$s. A few extra ZC sequences are prepended to the packet for packet detection purposes. The time duration between the time it takes for Alice to measure Bob's channel and vice versa is ~ 1 ms.

Details of the experimental setup are illustrated in Fig. 2.5. In total, 6500 channel measurements are captured. Prior to obtaining each measurement, the environment around Alice is varied, either by moving Alice or having an experimenter move around the node to ensure variation between measurements. In Fig. 2.5, the dashed lines show how Alice's location was varied across the map while the nodes of Bob and Eve are kept between one of the two locations shown in the map. Data is collected from over-the-air measurements and subsequently used to generate keys offline.

2.8 Conclusion

This chapter has described some of the preliminaries of the secure information transmission system. In particular, the channel probing protocol used to obtain over-the-air measurement data was detailed. Additionally, we described methodologies of our channel estimation technique along with channel gain/delay estimation and key generation. The simulation and experimentation channel that we use throughout this dissertation were also detailed.

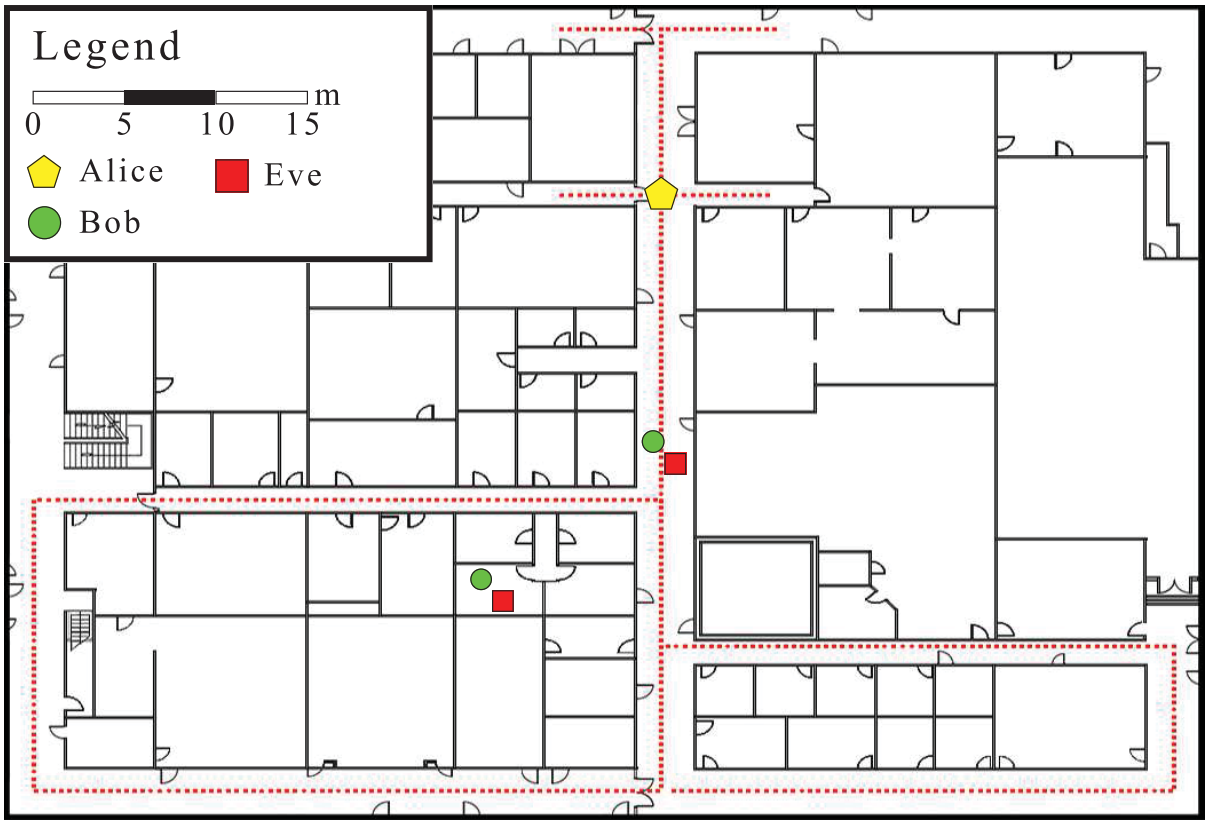

Figure 2.5. Experimental setup on the third floor of Merrill Engineering Building at the University of Utah. The position of Alice was varied across the dotted lines while Bob and Eve remained stationary in one of the two displayed locations. Eve was synchronized to Bob's clock, while Alice and Bob operated on asynchronous clocks. The antenna of Bob and Eve were placed approximately 1/3 meter apart.

CHAPTER 3

RECIPROCAL CHANNEL TIME/PHASE ALIGNMENT AND STRONGEST PATH CANCELLATION

The wireless channel is a viable candidate for security applications in wireless communications. This is due to the properties mentioned in Chapter 1 which can effectively allow a pair of legitimate users (Alice and Bob) to share a secret - the secret being a realization of the channel - that is statistically uncorrelated for a third party (Eve) located more than a few wavelengths away from the main users.

To exploit the wireless channel as a means for physical-layer security, two authenticated users go through a channel probing process. Here, Alice transmits a beacon packet to Bob, who upon hearing Alice, quickly transmits the same packet back to Bob (see Chapter 2 for a more detailed description of the beaconing and channel estimation process).

Although the wireless channel between a pair of users at identical frequency and time instants is reciprocal, bidirectional measurements of the channel are not. Among the non-reciprocites which can degrade the similarity of the estimated channel between a pair of users are:

- Additive channel noise.
- Interference arising from other active nodes within vicinity of the communicating parties.
- Differences in hardware which can contribute to carrier frequency, phase, and IQ offsets.
- Doppler shifts, which can contribute to a significant amount of disagreement between Alice and Bob's channel measurements if the channel probe time duration is

longer than the channel coherence time - i.e., the channel is fluctuating more quickly than the time it takes for Alice and Bob to probe the channel.

- Time misalignment arising from the TDD (time-division duplexing) nature of the channel beaconing protocol.

Given the above channel non-reciprocities, in this chapter, we will focus on the non-reciprocities that can be controlled through signal processing. To this end, we note that time and phase synchronization are the two most obvious non-reciprocities that can be controlled and hence, we devote this chapter to the discussion of time/phase alignment.

3.1 Background

The work discussed in this chapter addresses practical issues in physical-layer security applications which make use of the reciprocal radio channel. We consider the extraction of a key using measurements the channel impulse response (CIR) - thus randomness in the key comes from the frequency selectivity of the channel. When the reciprocal CIR is considered, we've found that timing and phase offsets can contribute to a significant source of error between Alice and Bob's channel measurements. The first part of this chapter will focus on time and phase alignment.

As a motivating example, we present Fig. 3.1 which shows one particular realization from our experimental data set following channel estimation. It is quite easy to see from this figure that despite the fact that the CIRs of Alice and Bob exhibit similar profiles, the timing offset between the two users contributes to a large amount of dissimilarity in the measurements.

It should be reemphasized that we do not assume Alice and Bob to be time or phase synchronized. A number of researchers - particularly those evaluating simulation results - assume there to be perfect synchronization between the nodes [50, 68]. Some researchers working on obtaining real-world measurements use a cable to synchronize the clocks of Alice and Bob [69, 70], while others use uni-directional measurements to approximate bi-directional measurements [60]. Furthermore, in many reports - e.g., [45, 71, 72] - it is unclear how exactly time and phase offsets are taken care of.

Contrary to these works, our solution adheres to the true nature of wireless communications - i.e., Alice and Bob are operating two asynchronous and disconnected transceiver

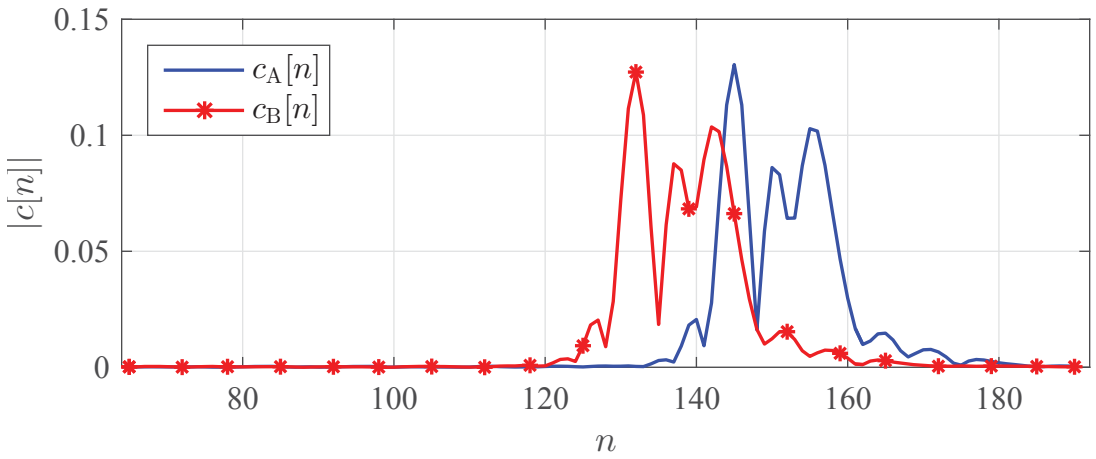

Figure 3.1. Example plot of the magnitude of the channel following the channel estimation step. Here, $c_A[n]$ and $c_B[n]$ represent the CIR estimate at Alice and Bob's node, respectively.

nodes located a reasonable distance away from one another. Little has been said in the literature about the synchronization problem addressed in this chapter. In fact, we've only been able to find the following research on this topic. Madiseh et al. in [73] discuss how synchronization errors can lead to diminishing key rates, but do not present a solution. In particular, it is interesting to see that there is a significant drop in mutual information between Alice and Bob's received signals even when the time misalignment between the two nodes is small. Croft et al. discuss the requirement of time and phase synchronizaton in CIR measurements in [74]. Here, they propose a solution in which the CIRs of Alice and Bob are time aligned according to the median value of the magnitude of the CIR. Phase synchronization is accomplished by zero-forcing the angle of the sum of the CIR to zero. In [51], an orthogonal greedy algorithm is utilized to seek the complex gain and time delay of the different multipath component of the channel. However, it is unclear how the authors handle the situation in which the time delays of one of the multipath components of the CIR differs between the two nodes.

In light of the current state of the art, we aim to give both a thorough review of the problem of timing and phase synchronization in reciprocal radio channel measurements as well as compare a set of solutions. Later, we will see that our augmentation of strongest-path cancellation (SPC) follows from these discussions.

3.2 Channel Time/Phase Alignment Model

Following the channel estimation step, Alice and Bob both have their own discrete sample estimates $c_{\mathrm{A}}[n]$ and $c_{\mathrm{B}}[n]$ which contain time and phase offsets with respect to one another. We can represent $c_{\mathrm{A}}[n]$ and $c_{\mathrm{B}}[n]$ in equation form as

$$c_{\mathrm{A}}[n] = c(nT_s - \mu_{\mathrm{A}})e^{j\phi_{\mathrm{A}}} + \eta_{\mathrm{A}}[n] \tag{3.1}$$

$$c_{\mathrm{B}}[n] = c(nT_s - \mu_{\mathrm{B}})e^{j\phi_{\mathrm{B}}} + \eta_{\mathrm{B}}[n] \tag{3.2}$$

where μ_{A} and μ_{B} are time delays, ϕ_{A} and ϕ_{B} are phase errors, and η_{A} and η_{B} are noise terms that arise from channel noise. The parameter $c(nT_s)$ represents the reciprocal wireless channel, discretely sampled at time spacings of T_s. In this chapter, we will consider the wireless channel to be well-modeled by the widely accepted frequency-selective wideband channel model [26]

$$c(nT_s) = \sum_{i \in \mathcal{M}} \alpha_i p(nT_s - \tau_i) \tag{3.3}$$

where $\mathcal{M} = \{0, 1, \ldots, M-1\}$ and M is the number of paths. The parameters α_i and τ_i are the complex gain and delay associated with the i^{th} path and $p(t)$ is the combined responses of the transmit and receive filters.

The parameters $(\mu_{\mathrm{A}}, \phi_{\mathrm{A}})$ and $(\mu_{\mathrm{B}}, \phi_{\mathrm{B}})$ are, in general, different between Alice and Bob and hence, if uncompensated for, can lead to a significant source of disagreement between the two legitimate parties. In this chapter, the following three phenomena associated with time and phase misalignment will be discussed - 1) integer time offset, 2) fractional time offset, and 3) phase offset. A greater part of the discussion in this chapter will be devoted to the integer time offset as our solution for adjusting the fractional time and phase offsets simply follows from synchronization of the integer timing offset.

3.3 Time/Phase Alignment

Two different types of approaches can be taken with regards to time alignment. The difference between these two approaches is that one set of methods assumes that a public, insecure channel is available for Alice and Bob to *feedback* synchronization messages and the other set of methods does not assume such a channel is available. Many physical-

layer key generation protocols in the literature assume the availability of such a channel [2, 8–10].

The trade-off in using a public channel versus not is that the use of such an outlet *will* allow for Alice and Bob to agree on a reference with a very high percentage. On the other hand, it incurs a significant energy cost on the network since sophisticated digital modulation techniques are required to ensure that data integrity is upheld. Additionally, using a public channel for feedback opens the door for the adversary to use/abuse such information to its advantage. Given the trade-offs, it makes sense to discuss our findings for both types of approaches.

The following steps are taken prior to making a timing decision. First, we take the CIR following the channel estimation step in Section 2.4 from (3.1) and (3.2) and proceed by shifting the CIR of each estimate according to its strongest path to a predefined location. Next, Alice and Bob interpolate their respective CIRs $c_{\mathrm{A}}[n]$ and $c_{\mathrm{B}}[n]$ by a factor of L_2, to further increase the time resolution of the available samples to them. The remaining steps are performed on these interpolated CIRs which we call $\tilde{c}_{\mathrm{A}}[n]$ and $\tilde{c}_{\mathrm{B}}[n]$ and assume to be good approximations of the respective continuous time functions. In the subsequent discussions, we refer to the length of the interpolated CIRs as N_c. Finally, path candidates in their respective CIRs are calculated using the techniques discussed in Section 2.5. Once path candidates $(\tilde{\alpha}_i, \tilde{k}_i)$ are calculated, the interpolated CIRs are time-shifted such that their largest path gain falls to the middle point of respective sequences. Note that this requires adjustment of the delay parameters $\tilde{k}_i$.

After this set of steps, the respective nodes need to process the path candidates, use them to make a timing decision, and proceed to apply that decision to the CIRs. A set of methods to accomplish these tasks are discussed in the following sections. Once the timing decision has been applied, the results are subsequently decimated L_2 fold to obtain a pair of channel estimates.

In upcoming discussions, we will take $(\tilde{\alpha}_{\mathrm{T}}, \tilde{k}_{\mathrm{T}})$ to be the path candidate which Alice and Bob use for time alignment and refer to this path candidate as the *selected time path candidate*. Note that the subscripts A and B have been removed in the selected timing point, but it should be understood that the steps presented in the following sections are applied to both $\tilde{c}_{\mathrm{A}}[n]$ and $\tilde{c}_{\mathrm{B}}[n]$ and that the subscripts may be reintroduced for emphasis.

Once a timing decision has been made - e.g., the selected time path candidate or time index has been found - the CIRs of Alice and Bob are circularly shifted so that the time indices $\tilde{k}_{\mathrm{T}}$ (or n_{T}) fall to a predefined location.

3.3.1 Time/Phase Alignment With Feedback

A block diagram is provided in Fig. 3.2 to help illustrate the concept of the time alignment methods which use a public feedback channel to aid in synchronization. Here, Alice acts as the leader and gives Bob information regarding her timing decision.

3.3.1.1 Mean Delay Reference

In this method, Alice time aligns according to her strongest path and then proceeds to calculate the relative time difference between her estimate of the mean delay parameters and the location of the strongest path. This information is fed back to Bob, who uses it to time align his own channel. To start, the mean delay parameter

$$\bar{k} = \left\lfloor \frac{\sum_i \tilde{k}_i |\tilde{\alpha}_i|^2}{\sum_i \tilde{k}_i} \right\rceil . \tag{3.4}$$

is calculated at both Alice's and Bob's nodes.

Next, Alice calculates the relative time difference between her estimate of the instantaneous mean delay and the location of her strongest path - which had been time aligned to the middle of the CIR. This results in a new delay parameter $k_{\mathrm{D}} = \frac{N_c}{2} - \bar{k}_{\mathrm{A}}$. Alice then transmits k_{D} to Bob. Note that this transmission does not need to be secure as this information has no value to Eve, whose channel has no similarity to Alice's or Bob's channel. Upon receiving k_{D}, Bob calculates the reference delay

$$k_{\mathrm{ref}} = \bar{k}_{\mathrm{B}} + k_{\mathrm{D}} \tag{3.5}$$

At this point, k_{ref} should be a time location in Bob's CIR near the strongest path of Alice's CIR. However, non-reciprocities in the CIR along with estimation error muddle the location of Alice's strongest path relative to Bob's. To handle this problem, we propose that Bob solves the equation

$$[\tilde{k}_{\mathrm{T,B}}, \tilde{\alpha}_{\mathrm{T,B}}] = \arg \min_{i \in [0, M-1]} ||p_i[n] - p[n - k_{\mathrm{ref}}]||^2 . \tag{3.6}$$

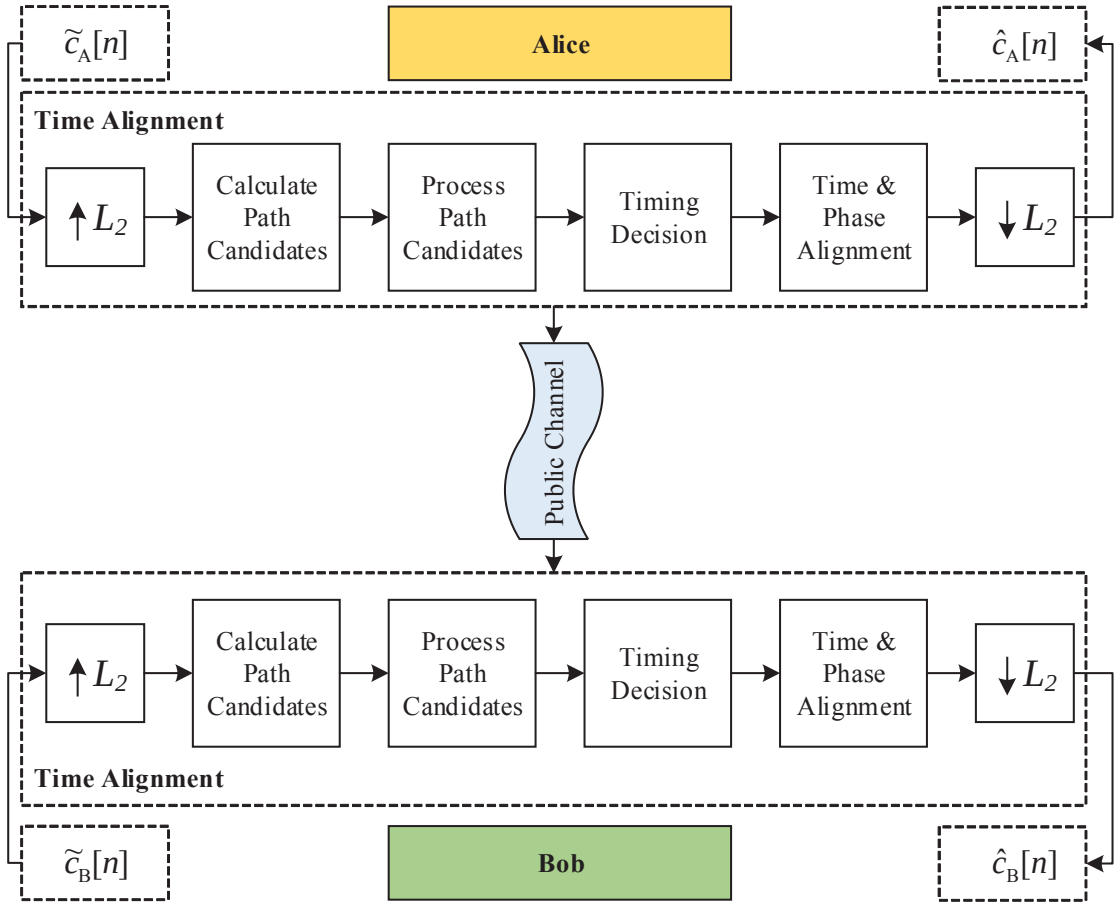

Figure 3.2. Block diagram of time synchronization with feedback

where $p_i[n] = \tilde{\alpha}_{i,\mathrm{B}} p[n - \tilde{k}_{i,\mathrm{B}}]$. Note that (3.6) searches for the path candidate of Bob's channel which maximally correlates to $p[n - k_{\mathrm{ref}}]$. The corresponding output $\tilde{k}_{i,\mathrm{B}}$ in (3.6) is then used as Bob's reference point and is thus time aligned to the middle of the respective sequence. This procedure finalizes the time alignment of $\tilde{c}_{\mathrm{A}}[n]$ and $\tilde{c}_{\mathrm{B}}[n]$.

3.3.2 Time/Phase Alignment Without Feedback

Fig. 3.3 shows a block diagram of the time alignment approach taken in this section. Note that Alice and Bob follow the exact same steps as one another and that they develop their own timing decision independent of one another. The methods discussed in this section are more prone to error than the previous section. However, this time/phase alignment approach does not require Alice and Bob to communicate across a public channel which is more advantageous from a design standpoint. It is noted here that interpolation

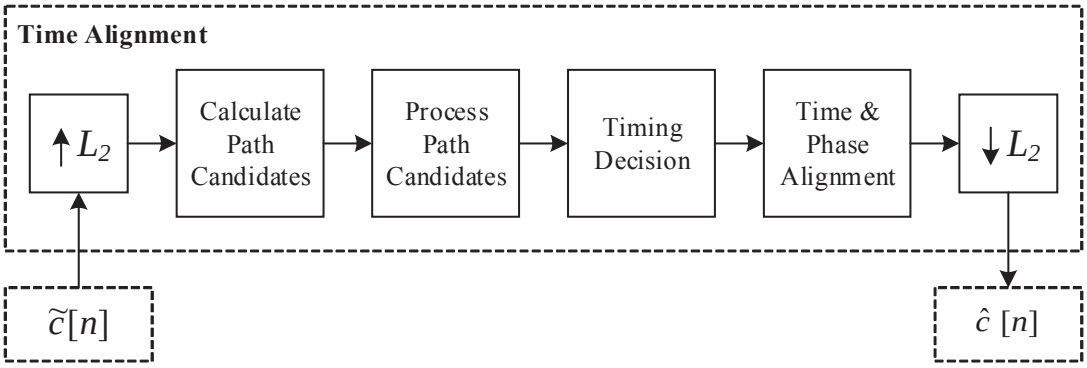

Figure 3.3. Block diagram of time synchronization without feedback

and path candidate calculation is assumed to be done prior to the steps taken in this section.

3.3.2.1 Fine Alignment

Fine alignment corresponds to time synchronization methods which choose one of the M path candidates $(\tilde{\alpha}_i, \tilde{k}_i)$ as the decision. A number of fine time alignment methods based on a thresholding approach are described in this section. The first path candidate (first in terms of temporal location) which passes a given threshold is taken to be the *selected path candidate*. In other words, the selected path candidate $(\tilde{\alpha}_{\mathrm{T}}, \tilde{k}_{\mathrm{T}})$ is the smallest $\tilde{k}_i$ which meets the condition $|\tilde{\alpha}_i| \geq \delta^{\mathrm{f}}$. The following procedures highlight different ways we obtain δ^{f}:

1. *Max-based Threshold* - In this approach, the first strongest path of the channel is determined as the time alignment point and δ^{f} is a value that is some percentage of the dominant path, i.e.,

$$\delta^{\mathrm{f}} = \beta_{\max} \cdot |\tilde{\alpha}_{\max}| \tag{3.7}$$

   where $\beta_{\max}$ is a percentage value between 0 and 1. Note that when $\beta_{\max} = 1$, this method simplifies to simply choosing the most dominant path.

2. *Percentile-based Threshold* - The parameter δ^{f} can also be based on the β_{perc} percentile of the channel gain. The β_{perc} percentile is the value below which $(100 \times \beta_{\mathrm{perc}})\%$ of the channel gain data are found. As an example, the median value of the channel gains - $\tilde{\alpha}_i$ for $i = 0, 1, \ldots, M-1$ - corresponds to the 50th percentile (i.e., $\beta_{\mathrm{perc}} = 0.5$).

Note that the median value of the channel was proposed as a time alignment point in [74].

The percentile can be computed by first sorting all M values of $|\tilde{\alpha}_i|$ in ascending order. The result of this sorting operation gives $\tilde{\alpha}^{\mathrm{s}}$, so that $|\tilde{\alpha}^{\mathrm{s}}_0| \leq |\tilde{\alpha}^{\mathrm{s}}_1| \leq \ldots |\tilde{\alpha}^{\mathrm{s}}_{M-1}|$. Next, the ordinal rank is found as

$$\iota = \lceil \beta_{\mathrm{perc}} M \rceil \tag{3.8}$$

and the following threshold δ^{f} is obtained from the ordinal rank as follows

$$\delta^{\mathrm{f}} = |\tilde{\alpha}^{\mathrm{s}}_{\iota}| \tag{3.9}$$

3.4 Strongest Path Cancellation

Once $\tilde{c}_{\mathrm{A}}[n]$ and $\tilde{c}_{\mathrm{B}}[n]$ are time aligned, they are circularly shifted so that the determined time alignment point will be located at the time index $n = 0$. The results are subsequently decimated L_2 fold to obtain a pair of channel estimates of length NL. Lastly, the channel estimates are phase aligned by introducing a phase shift to the elements of each CIR such that the path located at time index $n = 0$ has phase of zero. We call the final time and phase aligned CIRs $\hat{c}_{\mathrm{A}}[n]$ and $\hat{c}_{\mathrm{B}}[n]$.

Now that the timing and phase offsets have been resolved, let us consider the passive adversary, Eve, who follows the exact same synchronization steps as Alice for her own estimated CIR to obtain $\hat{c}_{\mathrm{E}}[n]$. At this stage, assume that the time and phase alignment method described in Section 3.3.1.1 - in which Bob time aligns according to the strongest path of Alice's estimated CIR - is used. Without getting into the detail, we note that by following Alice's time alignment steps, Eve can better synchronize with the legitimate users than she could by following Bob's alignment procedure.

For simplicity, we ignore the channel noise term and thus, note that the final CIR estimates for Alice and Eve can be expressed as

$$\hat{c}_{\mathrm{A}}[n] = |\tilde{\alpha}_{\mathrm{sp,A}}| p[nL_2] + \sum_{i \in \mathcal{M}_{\setminus \mathrm{sp}}} \tilde{\alpha}_{i,\mathrm{A}} p[nL_2 - \tilde{k}_{i,\mathrm{A}}] \tag{3.10}$$

$$\hat{c}_{\mathrm{E}}[n] = |\tilde{\alpha}_{\mathrm{sp,E}}| p[nL_2] + \sum_{i \in \mathcal{M}'_{\setminus \mathrm{sp}}} \tilde{\alpha}_{i,\mathrm{E}} p[nL_2 - \tilde{k}_{i,\mathrm{E}}] \tag{3.11}$$

where $\tilde{\alpha}_{\text{sp,A}}$ and $\tilde{\alpha}_{\text{sp,E}}$ are the gains of the strongest paths of Alice and Eve's channels respectively. Additionally, $\mathcal{M}_{\backslash \text{sp}}$ and $\mathcal{M}'_{\backslash \text{sp}}$ contains the set of all paths excluding the strongest path for Alice and Eve, respectively.

Next, we define the length NL CIR vectors $\hat{\mathbf{c}}_{\text{A}} = \{\hat{c}_{\text{A}}[n]\}$, $\hat{\mathbf{c}}_{\text{B}} = \{\hat{c}_{\text{B}}[n]\}$, and $\hat{\mathbf{c}}_{\text{E}} = \{\hat{c}_{\text{E}}[n]\}$. Also, we let $\mathbf{p} = \{p[n]\}$. Given (3.10) and (3.11), the partial correlation between Alice and Eve's CIR estimates can be expressed as

$$\varrho_{\text{AE}} = \frac{\hat{\mathbf{c}}_{\text{A}}^{\text{H}} \hat{\mathbf{c}}_{\text{E}}}{\|\hat{\mathbf{c}}_{\text{A}}\| \, \|\hat{\mathbf{c}}_{\text{E}}\|} \, . \tag{3.12}$$

Evaluation of (3.12) using (3.10) and (3.11) gives

$$\varrho_{\text{AE}} = \varrho_{\text{sp,AE}} + \varrho_{\backslash \text{sp,AE}} \tag{3.13}$$

where

$$\varrho_{\text{sp,AE}} = \frac{|\tilde{\alpha}_{\text{sp,A}}||\tilde{\alpha}_{\text{sp,E}}| \, \|\mathbf{p}\|^2}{\|\hat{\mathbf{c}}_{\text{A}}\| \, \|\hat{\mathbf{c}}_{\text{B}}\|} \tag{3.14}$$

is a positive and relatively large term arising from the time and phase synchronized strongest paths of Alice and Eve, and $\varrho_{\backslash \text{sp,AE}}$ is the residual partial correlation arising from the remaining paths. Since these remaining paths are not synchronized, their partial correlations are usually a set of zero-mean, low variance random variables that add up to a statistically small value. This observation leads us to the following proposal.

To minimize the similarity of the keys generated by Alice and Bob with the key that Eve generates, Alice of Bob should remove the strongest paths of their respective synchronized CIR estimates and use the residual responses to set the keys. We call this method strongest path cancellation (SPC) and use $\bar{c}_{\text{A}}[n]$, $\bar{c}_{\text{B}}[n]$, and $\bar{c}_{\text{E}}[n]$ to denote the residual CIRs for Alice, Bob, and Eve, respectively. For instance, Alice's CIR after removal of strongest path is obtained as

$$\bar{c}_{\text{A}}[n] = \hat{c}_{\text{A}}[n] - |\tilde{\alpha}_{\text{sp,A}}| p[nL_2] \tag{3.15}$$

and similar equations are used to obtain the residual CIRs of Bob and Eve.

Our assumption here, which has been validated through an extensive set of 32.5 MHz wide indoor wireless channel measurements, has confirmed that the residual CIRs have sufficient information to assure highly correlated keys for Alice and Bob, while leading to a dissimilar key for Eve.

3.5 Results

In this section, we first compare the various time/phase alignment procedures discussed thus far. The discussion naturally leads to strongest path cancellation. To aid in our interpretations, we derive the keys using the standard key generation procedure written in (2.13) and described in Section 2.6 - i.e., the passband frequency indices of the CIR estimates define the key. The similarity criteria that we use is the partial-correlation, which is defined between Alice and Bob's keys as

$$\rho_{AB} = |\boldsymbol{\gamma}_B^H \boldsymbol{\gamma}_A|^2 \tag{3.16}$$

and ρ_{AE} is defined similarly with the appropriate substitutions. It will be made clear in the next chapter why we resort to this definition of similarity in the keys.

3.5.1 Time/Phase Align

In this section, the synchronization methods are compared with one another. We resort to comparing time alignment algorithms using the experimental data set, details of which are found in Section 2.7.2. It should be pointed out that the reason the experimental data set is favored over numerical results for this study is because we have heuristically found that when the one-sided exponential power delay profile is used in simulation to evaluate different timing algorithms, the first path is often chosen as the time alignment point simply because there is a relatively well-defined threshold separating noise from the first path. In the measurement data set, we've found that there are often multipath components which come before the strongest path that make the decision of choosing the first strongest path a more difficult one since there isn't a well-defined threshold separating residual multipaths from the first strongest one.

Table 3.1 shows a comparison of the 3 different time alignment methods discussed in this dissertation. We compute the probability that Alice and Bob make the correct timing decision for the different algorithms. A mismatch indicates that Alice and Bob chose different paths as a result of the timing synchronization algorithm. Table 3.1 also shows results for when both parties choose $\beta_{\max}$ and β_{perc} to minimize the probability of mismatch in timing decision. The corresponding $\beta_{\max}$ and β_{perc} are also given. To provide the reader an intuitive description of when the max-based method example may fail, we show Fig. 3.4. In this figure, one pair of realizations of the estimated CIRs from

Table 3.1. Table showing the probability of Alice and Bob choosing the correct timing decision for different fine timing methods using experimental data.

Time Alignment method	Probability that Alice and Bob are synchronized	Parameter Value
Mean Delay Reference	0.9995	-
Max-based Threshold	0.9877	$\beta_{\max} = 1.00$
Max-based Threshold (Best)	0.9928	$\beta_{\max} = 0.85$
Percentile-based Threshold	0.8585	$\beta_{\text{perc}} = 0.50$
Percentile-based Threshold (Best)	0.9858	$\beta_{\text{perc}} = 0.98$

the experimental data set is shown. This particular channel is chosen because it exhibits what we deem to be the 'double-path' problem. The double-path problem occurs when the CIR of the wireless link between Alice and Bob contains two or more paths with similar amplitudes. The presence of the channel noise at Alice and Bob's receivers may lead to different locations for the paths in $c_{\text{A}}[n]$ and $c_{\text{B}}[n]$.

The following observations can be made from Table 3.1. First, it can be seen that the mean delay reference method gives the best results. Hence, if a feedback channel is available for Alice and Bob to use, it is recommended to use it. However, when a feedback channel is unavailable, choosing a threshold of $\beta_{\max} = 0.85$ gives comparable results. Furthermore, it can be seen that a method based on choosing the median value of the path gains (as recommended in [74]) gives the least favorable results. In fact, from our experimental data set, when the percentile is chosen larger (i.e., $\beta_{\text{perc}} = 0.98$), the likelihood of a mismatch due to timing synchronization is the least likely.

As a supplemental tool, we also present Fig. 3.5. Here, the probability of Alice and Bob choosing the same path is plotted versus different values of β_{perc} for the experimental data set. It can be shown from this figure that choosing a threshold closer to the larger values of channel gain (i.e., the stronger paths) gives Alice and Bob the best chance to be synchronized to one another. Hence, a conclusion that can be derived from the observations thus far is that time/phase synchronization is best achieved when the *strongest path* is utilized

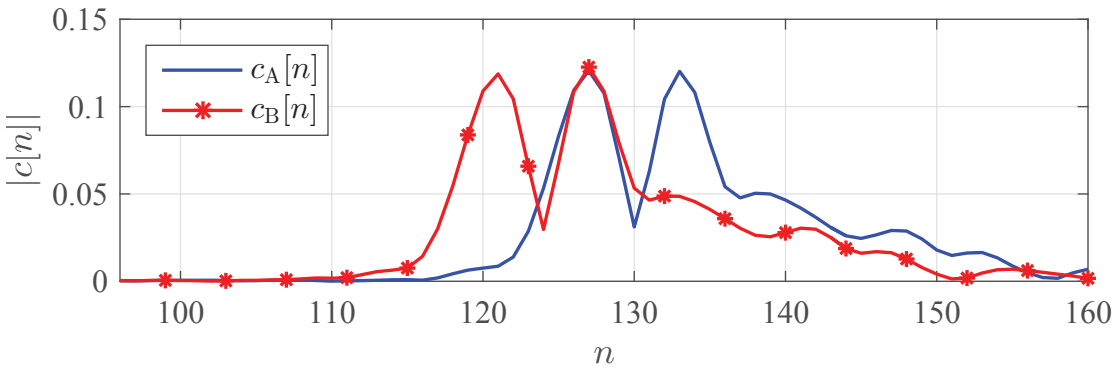

Figure 3.4. Example channel that shows the 'double-path' problem.

for time alignment purposes.

3.5.2 Strongest Path Cancellation

Now the discussion will be extended to include the passive adversary - Eve - who also follows Alice and Bob in time/phase alignment. To show how well the proposed key generation algorithm uses both time and amplitude to its advantage, we resort to real-world and numerical results.

3.5.2.1 Simulation Results

The parameters chosen for the simulation match the experiment. For the simulation, we assume a block fading channel model and no fractional timing offset for all three parties. Given this setup, Monte Carlo simulations were processed according to the following procedure.

1. Alice and Bob generate a probing beacon consisting of 25 periods of a length $N = 64$ ZC sequence. This is interpolated by a factor of $L = 4$ using a square-root raised-cosine filter with a roll-off factor of $1/2$ and transmitted at a sampling rate of $\frac{1}{T_s} = 130$MHz.

2. The beacon is transmitted across a simulated wireless channel. The channel follows the simulation model described in 2.7.1. We use a delay spread of $\bar{T}_m = 50$ ns. Alice and Bob share the same channel and the only difference between the Alice-Bob and Alice-Eve's channels are in the M complex-valued gains.

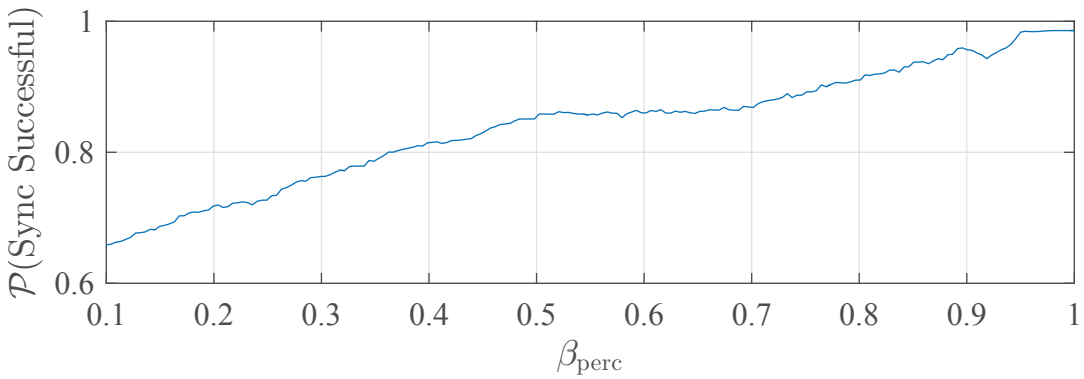

Figure 3.5. Probability of Alice and Bob choosing the correct timing decision versus β_{perc} for the percentile-based time/phase alignment method discussed in Section 3.3.2.1

3. Noise is independently added to the signal received by Alice, Bob, and Eve.

4. Channel estimation, time alignment, and key generation are processed according to the procedure described in Chapter 2. Note that for time alignment, Eve time aligns according to her own strongest path as she has more similarity to the Alice-Bob channel with this approach.

Fig. 3.6 shows the cumulative distribution function (CDF) of ρ_{AB} and ρ_{AE} before and after SPC from 10,000 runs of the described simulation. Alice and Bob have an SNR of 10 dB, while Eve has zero additive noise in her received signal. In addition to these curves, the partial correlation between the M complex gains of the Alice-Bob and Alice-Eve's channels is also plotted and is denoted by ρ_{R}.

A few interesting aspects of the proposed key generation algorithm can be found in Fig. 3.6. First, as expected, a slight decorrelation occurs between Alice and Bob's keys after SPC due to removal of the strongest path. However, this decorrelation is small. In fact, the average value of ρ_{AB} before and after SPC at the present SNR of 10 dB is 0.994 and 0.985, respectively.

Next, consider the curves depicted in Fig. 3.6 which show the partial correlation between Alice and Eve's keys before and after SPC, as well as the parameter ρ_{R}. First, it can be seen that before SPC, timing and phase recovery causes Alice and Eve's keys to be relatively strongly correlated. However, after SPC, the partial correlation bias due to time and phase synchronization in (3.14) is removed and thus the similarity between the keys

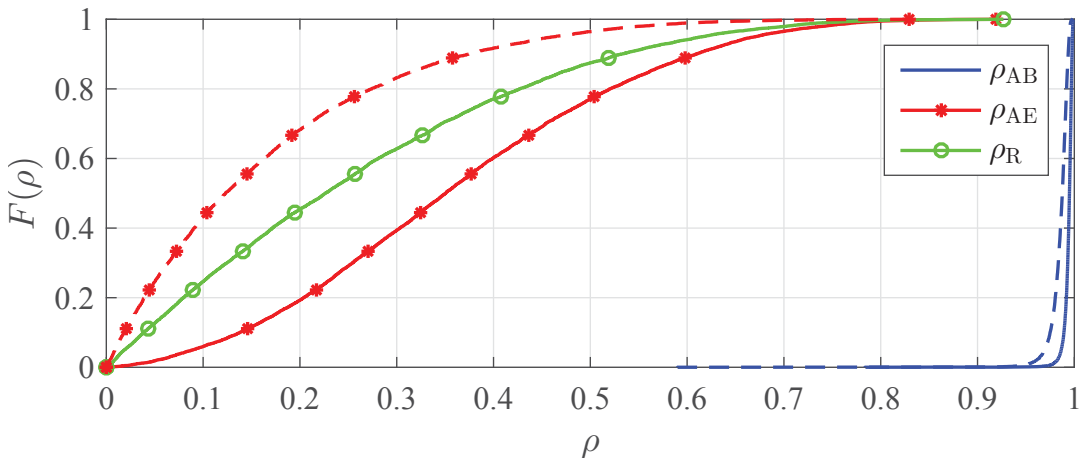

Figure 3.6. CDF of partial correlation between Alice and Bob's keys ρ_{AB} and Alice and Eve's keys ρ_{AE} from simulation results using a channel model in which path gains are derived from an exponential power delay profile with RMS delay spread of 50 *ns*. Dashed lines show results after SPC is applied. Additionally, ρ_R shows the partial correlation between the M complex-valued gains of Alice-Bob and Alice-Eve channels

is significantly less.

To help the reader grasp an understanding of the significance of Fig. 3.6, we present the set of plots in Fig. 3.7. Fig. 3.7 shows one CIR realization of Alice and Eve's channel that we feel is helpful in understanding Fig. 3.6. First, the path gains of this particular CIR realization is shown in the top-left while the filtered path gains are shown in the top-right plot. It can be seen that the second path is the strongest path of Alice's CIR while the first path is the strongest for Eve. It should also be noted that the path in Eve's channel corresponding to the location of Alice's strongest path is very low in power. Next, the two parties time align using the strongest path and the result is shown in the bottom-left plot. It can be seen now that the synchronization has caused both Alice and Eve's strongest paths to be located in the same temporal index, thus increasing the similarities of their CIR responses and subsequently in the keys they generate. Finally, SPC is applied in the bottom-right plot. A few interesting points can be observed in the bottom-right plot. First, it can be seen for this example that when both parties time align according to their strongest path, Eve's CIR shifts to the right while Alice's shifts to the left. This time-shift functions in reducing similarity in the CIRs of Alice and Eve. However, after the time-shift, Alice and Eve's CIRs are highly correlated due to the strongest paths of both node's being located at the same time index. When these paths are removed, as can be seen in the bottom-right

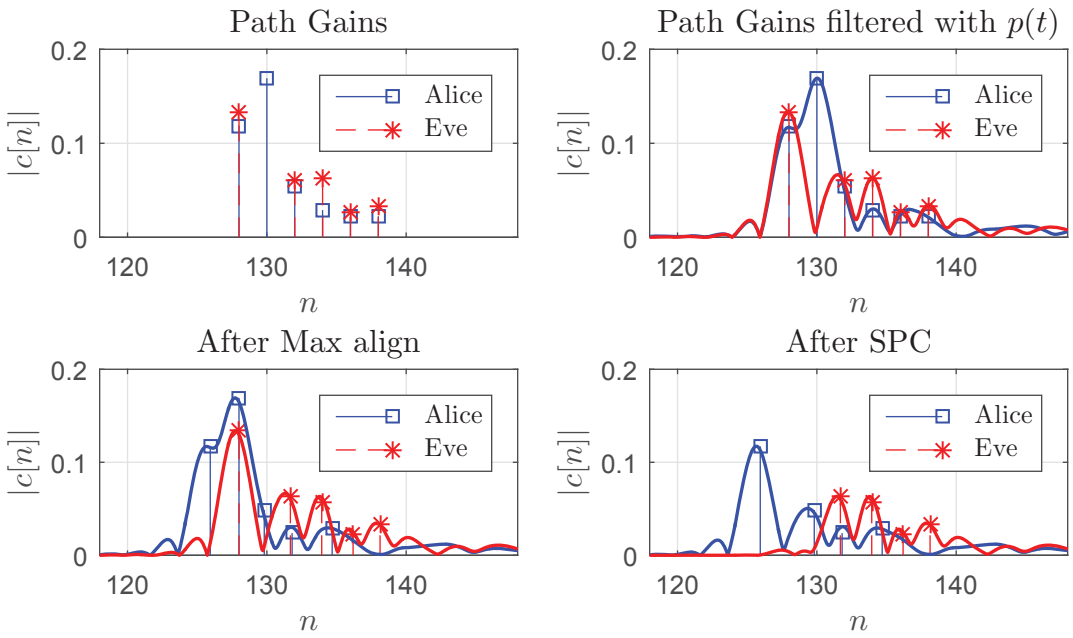

Figure 3.7. These set of plots show the main concept of SPC using one realization of the simulated channels. The top right plot shows the path gains used to generate the CIR at the nodes of Alice and Eve. Next, the path gains are filtered with the probing pulse $p(t)$. The bottom-right plot shows results after time alignment according to the strongest path. Finally, the bottom-left plot shows CIRs when SPC is applied to remove the strongest path. Note that this is the component of the CIRs giving rise to the greatest amount of similarity between Alice and Eve's CIRs after max alignment.

figure, the combination of steps results in Eve's CIR being both unsynchronized (in terms of time) and uncorrelated (in terms of channel gains). In short, Fig. 3.7 helps explain that the proposed augmentation of SPC uses both time and amplitude of the CIRs as a means of enhancing security of the key.

3.5.2.2 Experimentation Results

Fig. 3.8 shows the CDF of ρ_{AB} and ρ_{AE} before and after SPC from the experimental data. Similar to Fig. 3.6, we see a slight decorrelation between Alice and Bob's keys after SPC as well as a significant increase of dissimilarity between Alice and Eve's keys. Results shown in Fig. 3.6 and Fig. 3.8 are fairly similar, though over-the-air measurements show Alice and Eve's keys to be slightly more correlated in the experiment than in the simulation. A possible cause for this is that the channel model used in our simulation contains more randomness and/or paths than observed in the measurements.

Fig. 3.6 and Fig. 3.8 indicate that Eve's key has been decorrelated through SPC. At the

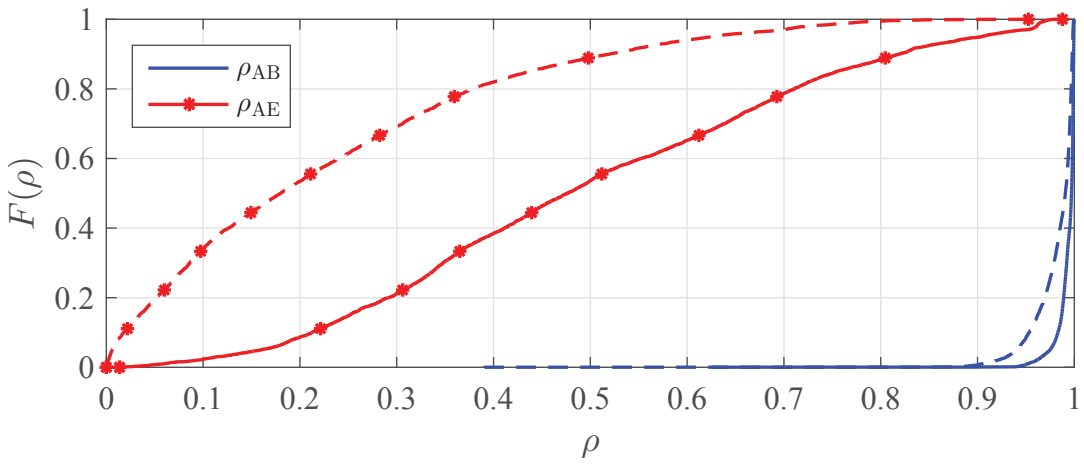

Figure 3.8. CDF of partial correlation between Alice and Bob's keys ρ_{AB} and Alice and Eve's keys ρ_{AE} from over-the-air data obtained from the experiment. Dashed lines show results after SPC is applied.

same time, the keys of Alice and Bob maintain similarity. However, the question looming at this point is whether this is worth the reduction in similarity between Alice and Bob's keys. We will examine this very point in the next chapter.

3.6 Conclusion

This chapter, along with the previous one, conclude the key generation portion of the secure information transmission system. The main topic of this chapter was time and phase alignment. It was first shown that synchronization is needed to be done by Alice and Bob in order to achieve channel reciprocity. However, a consequence of synchronization is that it allows the eavesdropping adversary to also synchronize with the legitimate users. We propose the use of strongest path cancellation (SPC) as a means of maintaining synchronization between the main users while ensuring security of the key. The trade-off in using SPC - that is left to be examined in the next chapter - is whether the gain in secrecy is worth the loss in reciprocity of the key.

CHAPTER 4

ARTIFICIAL NOISE FOR MULTICARRIER SPREAD SPECTRUM SYSTEMS

This chapter ties together the topics discussed so far in this dissertation into one secure information transmission system. The secure information transmission system we propose uses SS technology as a means of communicating confidential information-bearing symbols. In addition, artificial noise is added to enhance secrecy. The key developed in previous parts is introduced as an integral part of this system. First, we discuss background literature on artificial noise. Next, the system model of our SS-based secure information transmission system is detailed and the security level of the system is analyzed. Finally, we present results related to the proposed methodologies and end with concluding remarks.

4.1 Related Work

In their seminal paper, Goel and Negi [24, 25] proposed a unique transmit strategy that uses artificial noise in order to confuse the passive eavesdropper. The main concept of this work is to use the degrees of freedom provided by multiple transmit antennas to generate noise that lies in the null-space of the channel between Alice and Bob. This noise is called artificial noise and it is added to the information signal. At the legitimate receiver, the artificial noise is removed by the channel while the adversary's channel is degraded by this noise.

Fig. 4.1 presents a standard model of the multiple-antenna artificial noise transmit strategy in [24, 25]. The basic model defines Alice to have N_{T} transmit antennas and Bob and Eve to have $N_{\mathrm{R}} = 1$ receive antennas. In Fig. 4.1, Alice transmits the information bearing vector $\mathbf{x}_k$ as

$$\mathbf{x}_k = \frac{\mathbf{C}_k^{\mathrm{H}}}{\|\mathbf{C}_k\|} s_k + \mathbf{v}_k \tag{4.1}$$

where k is a nominal time index, $\mathbf{C}_k$ is a $1 \times N_{\mathrm{T}}$ complex-valued channel vector that

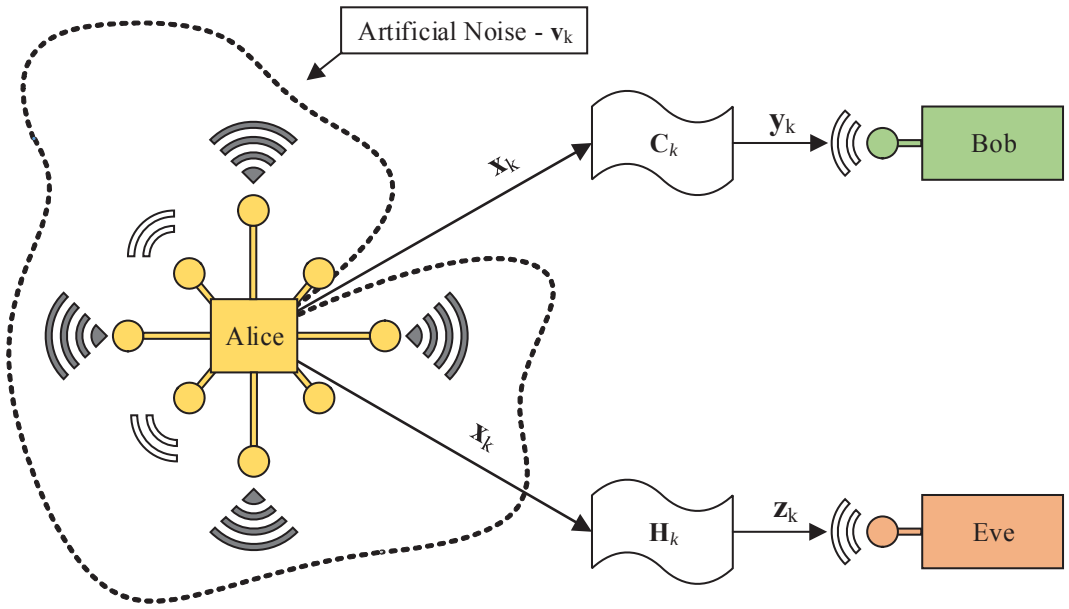

Figure 4.1. Illustration of the artificial noise transmitter.

connects the pair of legitimate users, and $\mathbf{v}_k$ is artificial noise. The artificial noise is chosen to lie in the null-space of the $\mathbf{C}_k$ so that $\mathbf{C}_k\mathbf{v}_k = 0$. Next, Bob and Eve respectively receive $\mathbf{y}_k$ and $\mathbf{z}_k$ as follows

$$y_k = \mathbf{C}_k\mathbf{x}_k + \eta_k \tag{4.2}$$
$$= \frac{\mathbf{C}_k\mathbf{C}_k^{\mathrm{H}}}{\|\mathbf{C}_k\|}s_k + \mathbf{C}_k\mathbf{v}_k + \eta_k \tag{4.3}$$
$$= \|\mathbf{C}_k\|s_k + \eta_k \tag{4.4}$$

$$z_k = \mathbf{H}_k\mathbf{x}_k + \epsilon_k \tag{4.5}$$
$$= \frac{\mathbf{H}_k\mathbf{C}_k^{\mathrm{H}}}{\|\mathbf{C}_k\|}s_k + \mathbf{H}_k\mathbf{v}_k + \epsilon_k \tag{4.6}$$
$$\tag{4.7}$$

where η_k and ϵ_k are i.i.d channel noise and $\mathbf{H}_k$ is the channel that connects Alice and Eve. Notice that the artificial noise is successfully nullified by Bob while it degrades the received response of Eve.

The following are assumptions made in the standard artificial noise signal model. 1) The channel $\mathbf{C}_k$ is assumed to be **perfectly known** by Alice, Bob, and Eve. Most works in this area have used the assumption of perfect CSI knowledge, despite the impracticality

of it. To obtain this characterization, it is typically assumed that $\mathbf{C}_k$ is estimated by Bob and fed back to Alice through a noiseless and insecure link. Since the link is insecure, Eve is therefore assumed to know $\mathbf{C}_k$ perfectly. However, despite Eve's knowledge of $\mathbf{C}_k$, as we've seen in (4.6), the standard artificial noise transmit strategy is built to withstand such adversaries (i.e., see Fig. 4.1 for an illustration). In other words, the secrecy of the artificial noise communication system is independent of the secrecy of the channel gains. 2) The channel vectors $\mathbf{C}_k$ and $\mathbf{H}_k$ have elements which are assumed to be independent zero-mean complex Gaussian random variables. Such a situation would occur in 'rich-scattering' environments, though it is an open problem in the literature to analyze how information-theoretic security results could be extended to other types of channel models. 3) Additionally, a block fading is assumed so that $\mathbf{C}_k$ and $\mathbf{H}_k$ are constant over a block of symbols and independent across blocks. This means that the channel is assumed to be static for the *total time* needed for the artificial communication setup. For a given time index k, this corresponds to the total time required for a) estimating the CSI between Alice and Bob, b) feeding this estimate back to Alice, and c) securely transmitting the information symbols across this channel to nullify the artificial noise generated using this CSI.

A very important parameter of the artificial noise communication system is the signal-to-artificial noise ratio denoted by ϕ. This ratio describes the fraction of total power allocated to the information-bearing signal s_k. The remaining transmit power is filled with artificial noise. In [24, 25], this parameter is found through maximization of the secrecy capacity - where secrecy capacity is defined as the maximum rate at which Alice-Bob can communicate a message without the eavesdropper being able to decode it. The power allocation approach in [25] is only valid when Alice knows the full CSI - i.e., the CSI between herself and Bob and herself and Eve. Though this is an impractical power allocation strategy for a malicious adversary not within the network, it is useful in the sense that it gives the bounds of what is achievable with this secure communication setup.

In [75], a closed-form expression for the lower bound of the ergodic secrecy capacity is obtained. Using this expression, it is found that for non-colluding and noiseless Eves, the optimal power allocation strategy is to distribute power *evenly* between signal and artificial noise in the high SNR regime. This was found to be true even for the case when Eve's CSI

is not known to Alice. In obtaining this result, the authors in [75] assume that Alice has perfect knowledge of the CSI between herself and BoB. Additionally, in [75], they discuss the effect of imperfect CSI on the artificial noise system. They find, surprisingly, that less power should be allocated to information signal as channel estimation error is increased. This is because when Bob has imperfect CSI, it is more efficient to degrade Eve's channel than to improve Bob's.

Other approaches for determining the signal-to-artificial noise ratio depend on the amount of knowledge of Eve's channel available to Alice. In another report [76], Alice is assumed to have full CSI information. The motivation for this study is in situations where Alice is a base-station in a cellular network and knows the CSI between herself and participating users. Some participating users (i.e., Eves) may attempt to access paying services unavailable to them but available to Bob. Another situation applicable to this scenario would be one where Bob is trying to access confidential information and Alice wishes *not* to communicate this data in an isotropic manner so as to minimize the chance that other participating users in the network overhear this private transmission. In such situations, the authors in [76] propose an artificial noise aided transmit beamforming strategy. Here, the knowledge of the full CSI information allows Alice to pattern the artificial noise in a manner helpful to Bob and detrimental to the link quality of Eve.

In our report, we are particularly interested in evaluating the scenario in which Eve's CSI is *unknown* to Alice. In this case, secrecy cannot be guaranteed since Alice does not know how much artificial noise to inject to Eve's channel. The approach taken by [77] is of particular interest when Eve's CSI is unkown. The power allocation strategy that they use in [77] is to meet a target SNR at the intended receiver to satisfy a link quality requirement. The rest of the available transmit power is then devoted to artificial noise.

4.2 System Model for MC-SS With Artificial Noise

Discussion of artificial noise in the literature - e.g., [24, 25, 75–77] - has largely been in the context of multiple antenna systems. Rather than using multiple antennas to obtain the necessary dimensionality with which to transmit artificial noise, we introduce the use of chips in spread spectrum for this purpose. The artificial noise is produced in the null-space of the spreading gain vector generated in the *secure key generation* step discussed in

previous sections of this dissertation.

A block diagram for the proposed MC-SS transmitter with the addition of artificial noise is shown in Fig. 4.2 and its corresponding receiver is in Fig. 4.3. Note that the receiver does not need additional circuitry to account for the artificial noise since it is removed by the despreader and any residual error due to artificial noise leaking into the information space is taken as additive noise. Additionally, the ”Multicarrier Modulator” and ”Multicarrier Demodulator” blocks in Fig. 4.2 and Fig. 4.3 are meant to allow for any MC-SS based waveform design such as OFDM, FB-MC-SS [34], etc. We purposely do not restrict our study to any particular MC-SS-based method as the following system model can be easily extended to any MC-SS waveform. Additionally, it is noted for the reader's benefit that the system model in this section will reuse some of the notations in Section 4.1. The mathematical notations and variables used in Secion 4.1 are local to that section and the notations in this section will be carried out through the chapter.

Following the transmitter in Fig. 4.2, Alice constructs the transmit signal using the key from previous discussions as

$$\mathbf{x}_k = \boldsymbol{\gamma}_{\mathrm{A}} s_k + \mathbf{v}_k \tag{4.8}$$

where $k = 0, 1, \ldots, K-1$ and $\mathbf{v}_k$ is artificial noise vector, added to increase security in presence of an eavesdropper. The artificial noise $\mathbf{v}_k$ is selected to lie in the null-space of $\boldsymbol{\gamma}_{\mathrm{A}}$, so that $\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}} \mathbf{v}_k = 0$. More explicitly, $\mathbf{v}_k$ is generated as the residual between an i.i.d circularly symmetric complex Gaussian noise vector - $\mathbf{w}_k$ - and its projection onto the space of $\boldsymbol{\gamma}_{\mathrm{A}}$ as follows

$$\mathbf{v}_k = \mathbf{w}_k - \boldsymbol{\gamma}_{\mathrm{A}} \boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}} \mathbf{w}_k \,. \tag{4.9}$$

The total transmit power across the entire occupied bandwidth can be obtained by combining (4.8) and (4.9). This gives

$$\begin{aligned} P &= \mathrm{E}[\mathbf{x}_k^{\mathrm{H}} \mathbf{x}_k] \\ &= \sigma_s^2 + \frac{N-1}{N} \sigma_w^2 \end{aligned} \tag{4.10}$$

where

$$\sigma_w^2 = \mathrm{E}[\mathbf{w}_k^{\mathrm{H}} \mathbf{w}_k] \tag{4.11}$$

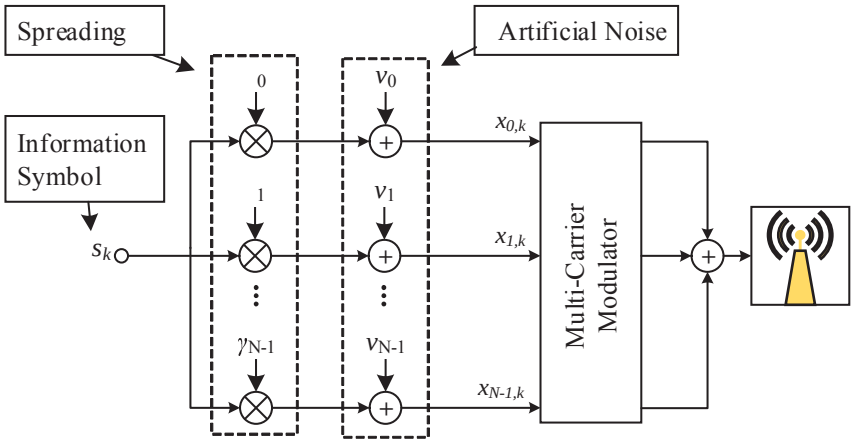

Figure 4.2. MC-SS transmitter block diagram

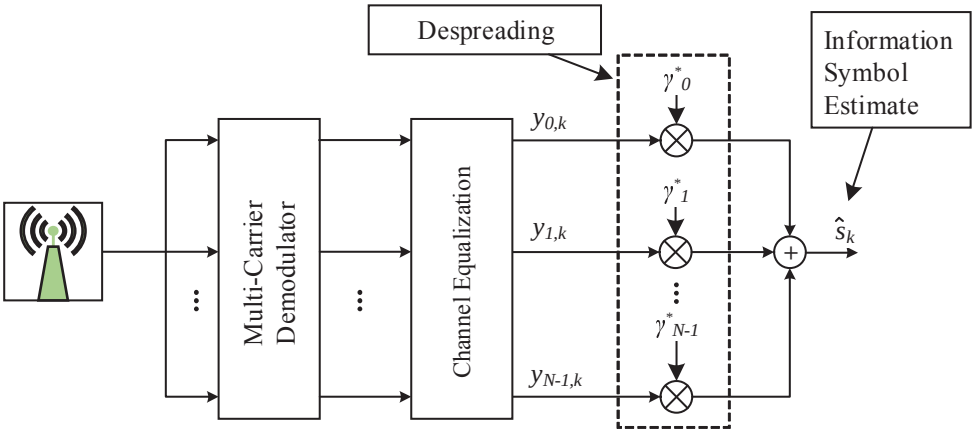

Figure 4.3. MC-SS transmitter block diagram

and the term $\frac{N-1}{N}$ arises from the fact that artificial noise is generated from a complete N-dimensional vector space with one of its dimensions removed. We denote the fraction of power allocated to the information signal as ϕ. This implies that

$$\sigma_s^2 = \phi P \tag{4.12}$$

and

$$\sigma_w^2 = \frac{(1-\phi)P}{N-1}. \tag{4.13}$$

Following (4.8), the signal received by Bob and Eve *after* multicarrier demodulation and application of a zero-forcing channel equalizer is respectively given by

$$\mathbf{y}_k = \mathbf{x}_k + \boldsymbol{\eta}_k \tag{4.14}$$

$$\mathbf{z}_k = \mathbf{x}_k + \boldsymbol{\epsilon}_k \tag{4.15}$$

where the components of $\boldsymbol{\eta}_k$ and $\boldsymbol{\epsilon}_k$ arise from channel noise. Note that the elements of $\boldsymbol{\eta}_k$ and $\boldsymbol{\epsilon}_k$ may not be i.i.d due to frequency selectivity of the channel. The SNR between the Alice-Bob link and Alice-Eve link thus, can be expressed as

$$\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} = \frac{P}{\sigma_{\eta}^2} \tag{4.16}$$

and

$$\mathrm{SNR}_{\mathrm{E}}^{\mathrm{i}} = \frac{P}{\sigma_{\epsilon}^2} \tag{4.17}$$

where $\sigma_{\epsilon}^2 = \mathrm{E}[\boldsymbol{\epsilon}_k^{\mathrm{H}}\boldsymbol{\epsilon}_k]$ and $\sigma_{\epsilon}^2 = \mathrm{E}[\boldsymbol{\epsilon}_k^{\mathrm{H}}\boldsymbol{\epsilon}_k]$.

Next, Bob and Eve despread their received signals from (4.14) and (4.15) with their own spreading gains to get

$$\begin{aligned}\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\mathbf{y}_k &= \boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}(\mathbf{x}_k + \boldsymbol{\eta}_k) \\ &= \boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}s_k + \boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\mathbf{v}_k + \boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\boldsymbol{\eta}_k\end{aligned} \tag{4.18}$$

and

$$\begin{aligned}\boldsymbol{\gamma}_{\mathrm{E}}^{\mathrm{H}}\mathbf{z}_k &= \boldsymbol{\gamma}_{\mathrm{E}}^{\mathrm{H}}(\mathbf{x}_k + \boldsymbol{\epsilon}_k) \\ &= \boldsymbol{\gamma}_{\mathrm{E}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}s_k + \boldsymbol{\gamma}_{\mathrm{E}}^{\mathrm{H}}\mathbf{v}_k + \boldsymbol{\gamma}_{\mathrm{E}}^{\mathrm{H}}\boldsymbol{\epsilon}_k\,.\end{aligned} \tag{4.19}$$

The SNR at Bob's node after the despreader is derived in Appendix A and is found to be

$$\mathrm{SNR}_{\mathrm{B}}^{\mathrm{o}} = \frac{N\phi\rho_{\mathrm{AB}}\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}}{\frac{N}{N-1}(1-\phi)(1-\rho_{\mathrm{AB}})\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} + 1} \tag{4.20}$$

where

$$\rho_{\mathrm{AB}} = |\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}|^2 \tag{4.21}$$

Equations (4.20) and (4.21) are defined similarly for the Alice-Eve link with the appropriate substitutions.

A subtle point of the formulation in this section is that the parameters ρ_{AB} and $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}$ are kept separate from one another, despite the fact that they are related. The reason for this is

that the dissimilarity between keys is not only dependent on SNR, but on other factors as well. One example of this from our algorithm is the precursor step in which time averaging multiple channel probes is taken as a measure to reduce channel noise. The success of this step is dependent on the coherence time of the channel relative to the number of probes per beacon. If the channel is static over the duration of a packet, the time averaging will be relatively successful compared to when there are time-varying factors (i.e., channel variation, frequency offsets, etc.) that may increase error due to incoherent averaging. Another example is estimation error such as time misalignment which may significantly reduce similarity between keys. Moreover, SPC also introduces a decorrelation effect on the keys as well. For these reasons and many more, we keep ρ_{AB} and SNR_B^i separate from one another.

Note when there is no artificial noise, i.e., $\phi = 1$, that (4.20) reduces to $\text{SNR}_B^o = N\rho_{AB}\text{SNR}_B^i$. This shows that the despreading procedure, through coherent linear combination of the received signal vector, allows Bob to achieve an SNR up to N times the link SNR given in (4.16). On the other hand, if Eve can gain access to the spreading code $\boldsymbol{\gamma}_A$, she can decode the information symbols sent by Alice. This highlights the necessity of the algorithm discussed in where Alice and Bob make use of the reciprocal wireless channel to generate a pair of similar keys while Eve, despite following the same steps as the legitimate nodes, generates a significantly different key.

To enlighten the reader on how artificial noise can be used to boost security, we plot SNR_B^o and SNR_E^o as a function of the received signal SNR at $\phi = 1/N$ in Fig. 4.4. We use the terms SNR^i and SNR^o to respectively describe the SNR before and after despreading at either Bob or Eve's node, depending on the context. The values of ρ_{AB} and ρ_{AE} were chosen arbitrarily to show that when Alice and Bob share nearly identical keys, they have a significant SNR advantage compared to the adversary who generates a different key.

4.2.1 Artificial Noise Transmit Strategy

An important parameter for artificial noise transmission systems is the signal-to-artificial noise ratio ϕ. In [25], this parameter is found through maximization of the secrecy capacity. This power allocation strategy is applicable only when Alice has perfect knowledge of the full CSI - e.g., the CSI between herself and Bob and herself and Eve. Since the knowledge

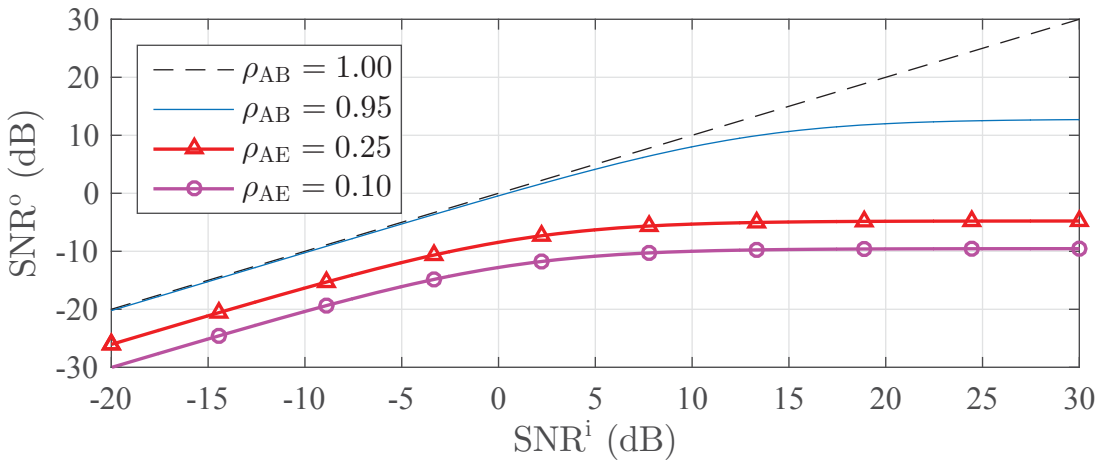

Figure 4.4. Plot of the SNR after despreading vs. receiver SNR for $\phi = 1/N$ and selected values of ρ_{AB} and ρ_{AE}.

of perfect CSI between Bob and Eve is not possible in practice, this method of selection of the artificial noise power may be only of interest from a theoretical point of view.

Here, we are interested in practical scenarios where Eve's CSI is not known to Alice. In this case, secrecy cannot be guaranteed as Alice does not know how much artificial noise to inject to Eve's channel. With the assumption of Eve's CSI remaining unkown, an approach taken by [77] distributes ϕ to meet a target SNR at Bob's node, assuming that the Alice-Bob CSI is perfectly known. The rest of the available transmit power is devoted to artificial noise, hoping this will sufficiently deteriorate the Eve's channel such that she will not be able to decode the transmit message

Our artificial noise power allocation strategy follows the same idea of dedicating enough power to the information subspace to ensure a certain link quality between Alice and Bob, while the low quality of the received signal at Eve is almost surely guaranteed. Furthermore, we do not make the assumption that perfect knowledge of Alice-Bob CSI is available.

Instead, we propose a power allocation strategy in which Alice dedicates enough power to the information symbols to ensure a target SNR is met for Bob so long as the similarity of their keys - quantified by ρ_{AB} - is larger than a threshold ρ_{min}.

The parameter ϕ for our signal-to-artificial noise power allocation strategy can be determined by replacing SNR_B^o in (4.20) with a target SNR - SNR_T^o - and ρ_{AB} with threshold

$\rho_{\min}$. Solving for ϕ with these substitutions in place gives

$$\phi = \frac{\frac{N}{N-1}(1-\rho_{\min})\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} + 1}{\frac{N}{N-1}(1-\rho_{\min})\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} + N\rho_{\min}\frac{\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}}{\mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}}}\,. \tag{4.22}$$

As a check, note that if the spreading codes are assumed perfectly known by Alice and Bob hence, $\rho_{\min} = 1$, the above reduces to

$$\phi = \frac{\mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}}{N\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}}\,. \tag{4.23}$$

This is the same result to the one reported in [77]. Note that the assumption here is that Alice knows the SNR between the main link and uses it to allocate power to the information symbols.

A nice feature of this power allocation strategy is that it connects the values of ρ_{AB} to the SNR seen by Bob's receiver after despreading. In fact, it is shown in Appendix B that if ϕ is obtained from (4.22), then

$$\mathcal{P}(\mathrm{SNR}_{\mathrm{B}}^{\mathrm{o}} < \mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}) = \mathcal{P}(\rho_{\mathrm{AB}} < \rho_{\min})\,. \tag{4.24}$$

To further help in understanding the benefites of the artificial noise power allocation strategy that we propose, we present a plot in Fig. 4.5. In this plot, the CDF of $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{o}}$ is plotted using the experimental data set from Chapter 2. The target SNR is set to 10 dB and the black dots in the figure represent this. Solid lines in Fig. 4.5 represent the case when $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} = 10$ dB and dashed lines show $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} = 0$ dB and N is set to 64. Note that when the link SNR is larger, more artificial noise is used. The value of $\rho_{\min}$ was set to 0.975 and 1 to compare our strategy to the one from [77] which assumes that Alice has perfect knowledge of main link CSI. The signal-to-artificial noise ratio ϕ used to generate the plot is given in Table 4.1 for all cases.

Fig. 4.5 shows the following. If dissimilarity between Alice and Bob's keys is unaccounted for (i.e., $\rho_{\min} = 1$), the target data rate is never met. The problem is worse when ϕ is increased and there is approximately a 2 dB range over which $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{o}}$ is spread across. On the other hand, with our proposed artificial noise power allocation strategy, it can be seen that the probability that the target data rate is met remains at a constant value of $\sim 95\%$ regardless of the value of ϕ.

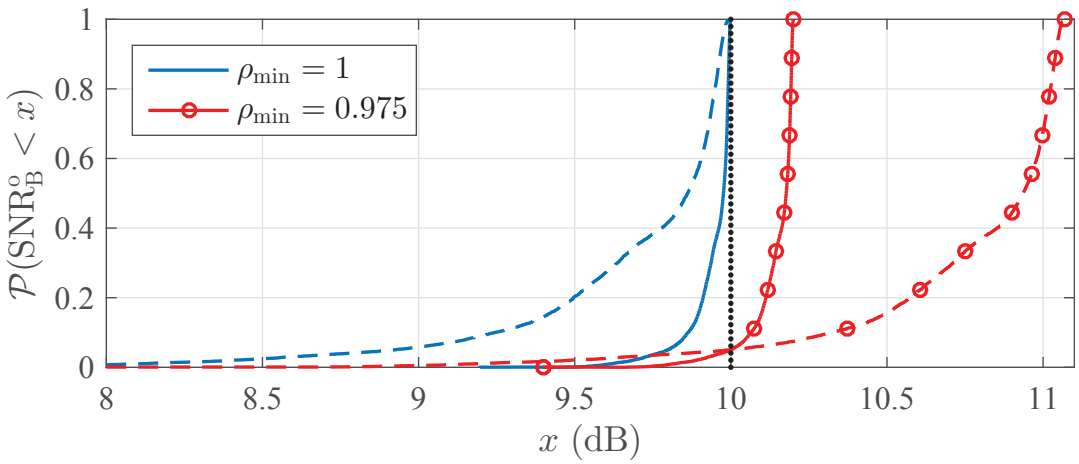

Figure 4.5. CDF of $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{o}}$ for two different values of $\rho_{\min}$ when $\mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}} = 10$ dB. Solid lines show the case when $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} = 0$ dB and dashed lines show when $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} = 10$ dB. The data used here is obtained from the experiment.

Table 4.1. Values of ϕ used to generate Fig 4.5.

$\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}$ (dB)	$\rho_{\min} = 1$	$\rho_{\min} = 0.975$
0	0.1563	0.1637
10	0.0156	0.02

One final point to be noted about our power allocation method is that there is a limit to how low $\rho_{\min}$ can be set for a minimal signal-to-artificial noise ratio $\phi_{\min}$ that a designer would consider, given a target SNR. To determine this limit, we set $\phi = \phi_{\min}$ in (4.22) and solve for $\rho_{\min}$ to get

$$\lim_{\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} \to \infty} \rho_{\min} = \frac{\mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}(1-\phi_{\min})}{\mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}(1-\phi_{\min}) + (N-1)\phi_{\min}} \tag{4.25}$$

We set the parameter $\phi_{\min} = \frac{1}{N}$ for reasons that will become clear later in this dissertation. This signal-to-artificial noise ratio will also be called the **golden ratio** in remaining parts of this dissertation. When $\phi_{\min} = \frac{1}{N}$, the minimum amount of mismatch given a target SNR after despreading at Bob can be shown to be

$$\lim_{\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} \to \infty} \rho_{\min} = \frac{\mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}}{\mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}} + 1} \tag{4.26}$$

In the following, we present two different options for choosing $\rho_{\min}$. One in which training data is utilized to obtain an *a-priori* estimate for $\rho_{\min}$ and another method for which training data is not available.

4.2.1.1 Training Method

The value of $\rho_{\min}$ is determined offline using training data and programmed into the transceivers prior to communication. This may be used by a designer to make sure that a target link reliability condition is met so long as the training data is appropriate for the design. Here, $\rho_{\min}$ is chosen so that

$$\mathcal{P}(\mathrm{SNR}_{\mathrm{B}}^{\mathrm{o}} < \mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}) = \mathcal{P}(\rho_{\mathrm{AB}} < \rho_{\min}) = \delta_{\mathrm{T}}^{\mathrm{o}} \tag{4.27}$$

where $\delta_{\mathrm{T}}^{\mathrm{o}}$ is some reliability constraint chosen by the designer.

A remark should be made about the idea of using training data to find $\rho_{\min}$. First, through our experiment on channel probing, we've seen that non-reciprocities in channel measurements take different forms for different pairs of nodes. One easy way in which this can be visualized is in the situation where one pair of nodes may have a frequency offset of 10Hz while another may have a frequency offset of 100Hz - thus the second pair of nodes may introduce more differences between keys than the first pair of nodes.

In short, each node has its own *radiometric signature* (see [78], where the idea of using radiometric signatures is used as a means of node identification). The radiometric signature of each node can be defined by characteristics unique to it and examples of radiometric signatures which can contribute to differences between a pair of reciprocal channel measurements would be clock skews, carrier frequency offsets, IQ impairments, among other RF hardware traits. Hence, in practice, we recommend to obtain training data between many different pairs of nodes as a means of finding a good estimate for $\rho_{\min}$,

4.2.1.2 Target $\phi_{\min}$

Another idea which does not require training data is one in which $\rho_{\min}$ is chosen so that $\phi = \phi_{\min}$ occurs at $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} = \psi \mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}$. Here, ψ is a constant used in defining the SNR at which the maximum amount of artificial noise would be used. By making the appropriate substitutions to (4.22), we get the following solution by solving for $\rho_{\min}$

$$\rho_{\min} = \frac{\frac{N}{N-1}(1-\phi_{\min})\psi\mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}} + 1}{\frac{N}{N-1}(1-\phi_{\min})\psi\mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}} + \psi} \tag{4.28}$$

and for our proposed design, since $\phi_{\min} = \frac{1}{N}$

$$\rho_{\min}\Big|_{\phi_{\min}=\frac{1}{N}} = \frac{\psi\mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}} + 1}{\psi(\mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}} + 1)}\,. \tag{4.29}$$

To give the reader an intuitive understanding of the concept behind this method, we present a set of plots. In Fig. 4.6, the parameter ϕ is plotted against Bob's receiver SNR for different values of ψ. The target SNR is set to 10 dB and the black circles in the figure represent the point at which ϕ is equal to the golden ratio of $\phi = 1/N$. For all curves, it can be seen that when Bob is SNR limited, more power is allocated to the information symbols so that the target can be met. In other words, ϕ is larger when the $\text{SNR}_\text{B}^\text{i}$ is low so that $\text{SNR}_\text{B}^\text{o} = \text{SNR}_\text{T}^\text{o}$ for a given value of ρ_{min}.

Another aspect that can be seen from Fig. 4.6 is that when ρ_{min} is set lower, the signal-to-artificial noise ratio is strategically increased so that the target SNR of 10 dB can be met. Finally, it can be seen that when $\psi = 1$ and $\rho_{\text{min}} = 1$, the golden ratio is met for $\text{SNR}_\text{B}^\text{i} = \text{SNR}_\text{T}^\text{o}$. Hence, in the ideal scenario in which there is no mismatch between keys, the minimum receiver SNR needed to transmit with the golden ratio is when $\text{SNR}_\text{B}^\text{i} = \text{SNR}_\text{T}^\text{o}$. Moreover, due to (4.29), when $\psi = 2$, the golden ratio is achieved at $\text{SNR}_\text{B}^\text{i} = \psi\text{SNR}_\text{T}^\text{o} = 2\text{SNR}_\text{T}^\text{o}$. Similarly the trend can be extended to increasing values of ψ. In short, this figure shows the basic concept behind the *Target* ϕ method - that when ρ_{min} is set based on (4.29), $\phi = \phi_{\text{min}}$ when $\text{SNR}_\text{B}^\text{i} = \psi\text{SNR}_\text{T}^\text{o}$.

Fig. 4.7 shows ρ_{min} as a function of the target SNR (in dB) for selected values of ψ when $\phi = 1/N$. In this plot, it is shown that when the target SNR is chosen larger, the value of ρ_{min} approaches 1 to meet the high demands of the system - suggesting that higher target rates can only be met when there is very little dissimilarity between keys generated by Alice and Bob. This also agrees with intuition in that high target data rates can only be met for keys obtained at high SNRs. Another observation from Fig. 4.7 is that the system is more forgiving to mismatch in keys when $\text{SNR}_\text{T}^\text{o}$ is low. The value of ρ_{min} significantly drops when the value of ψ is increased from 1 to 2 and when ψ is increased, ρ_{min} asymptotically approaches the dashed line in Fig. 4.7. The dashed line plots (4.26) which gives minimum value of ρ_{min} needed to meet the target SNR for $\phi = 1/N$. Hence, Fig. 4.7 shows that ρ_{min} should be above the dashed line to meet the specified target SNR when $\phi = 1/N$.

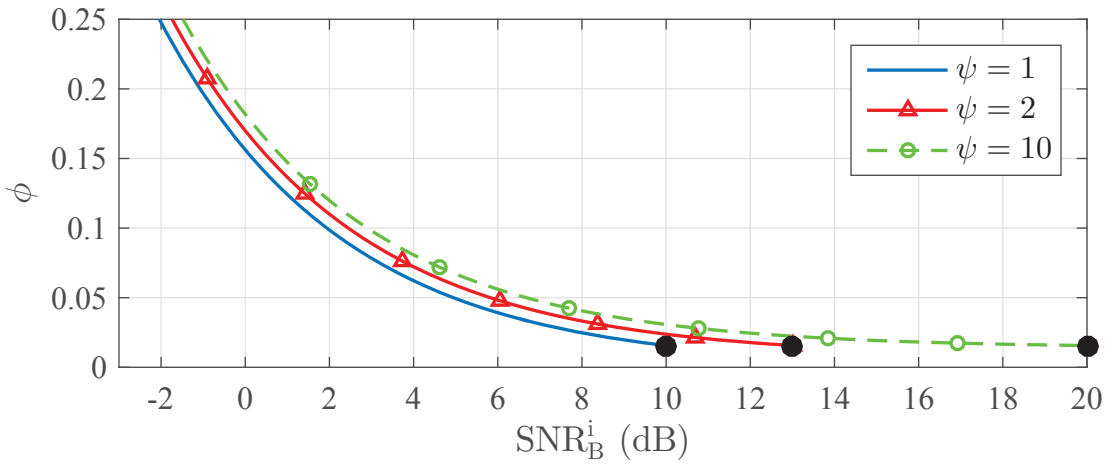

Figure 4.6. Plot of ϕ vs. $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}$ in dB for $\psi = 1, 2$, and 10

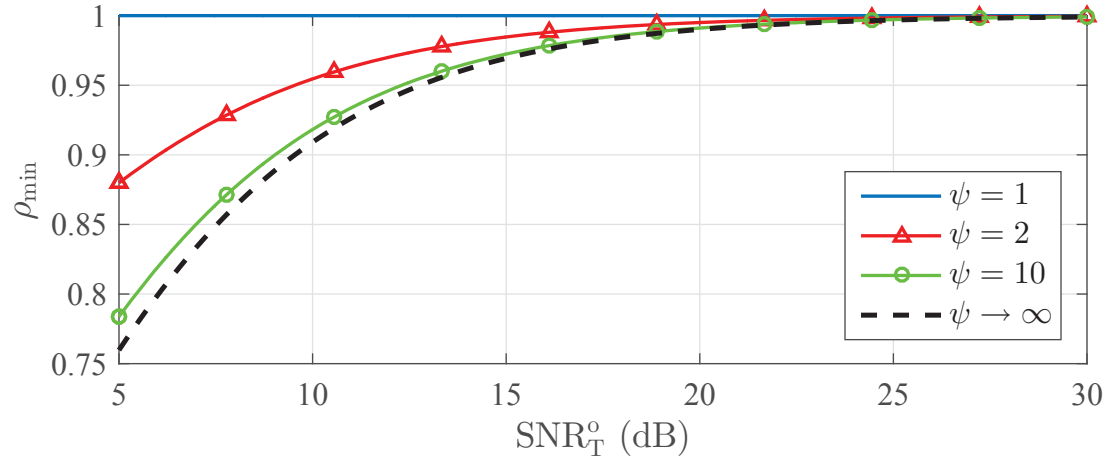

Figure 4.7. Plot of $\rho_{\min}$ vs. $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}$ in dB for selected values of ψ when $\phi = 1/N$.

4.2.2 Comparison to Physical-Layer Key Generation Systems

In this section, we will compare our proposed secure information communication strategy with traditional physical-layer key generation methods - the core concepts of which are described in Section 1.1.3. Recall from our previous discussion that physical-layer key generation techniques largely follow four steps: 1) randomness sharing, 2) information reconciliation, 3) privacy amplification, and 4) secure communications. In short, the first three steps aim to create a 'secret-key' using measurements of the reciprocal wireless channel. The key's maximum size depends on the secrecy and entropy of the shared randomness.

The result of the first three steps of the traditional physical-layer key generation system

produces a 'secret-key' using measurements of the reciprocal wireless channel. By contrast, the key discussed in our report uses only the first step for reasons that will become clear as we proceed. Regardless of the key being used, the main difference between traditional physical-layer key generation systems and the secure information transmission system discussed in this dissertation is in how the message is encrypted with the key. In other words, the two methods mainly differ in the 'secure communications' step.

The standard approach for secure communications with physical-layer key generation systems is to use a one-time pad. Another option which is not information-theoretically secure but, rather, computationally secure is to use the key as part of a symmetric encryption algorithm. The physical-layer key generation system to which we are making a comparison will use a one-time pad for secure communication.

Given a key and message, Fig. 4.8 shows a comparison between the transmitters of the secure SS communication system and the traditional physical-layer key generation with one-time pad solution. The left-hand side shows the physical-layer key generation method while the right shows the secure SS system.

On the left side of Fig. 4.8, Alice encrypts M message bits with M key bits by performing an XOR operation on the message with the key to generate the codeword $\mathcal{X}$. Note that the criteria of the one-time pad described in Section 1.1.1 should be met in order to ensure information-theoretic security when using the one-time pad. To retrieve the message $\mathcal{M}$, Bob applies an XOR to the $\mathcal{X}$ with the key $\mathcal{K}$.

The secure SS communication system is depicted on the right-hand side of Fig. 4.8. Since our technique is applied at the physical-layer, the message $\mathcal{M}$ bits are converted to symbols by using a digitial modulation scheme, such as BPSK or QAM. The rate of digital modulation - i.e., R_{T} in Fig. 4.8 - defines the number of bits encoded in each symbol. Note here that the key length N is different than the symbol length.

For the proposed secure information transmitter, the key $\boldsymbol{\gamma}$ can be any vector that spans the complex-valued N dimensional space. Because of this, the key is not necessarily limited to the one discussed in our dissertation. In fact, *any* physical-layer key generation system could pass any N length key to the secure SS system. A major benefit of this fact is that the key does not need to be quantized into a finite alphabet. Therefore, information contained in any given reciprocal wireless channel estimate is not lost due to the process

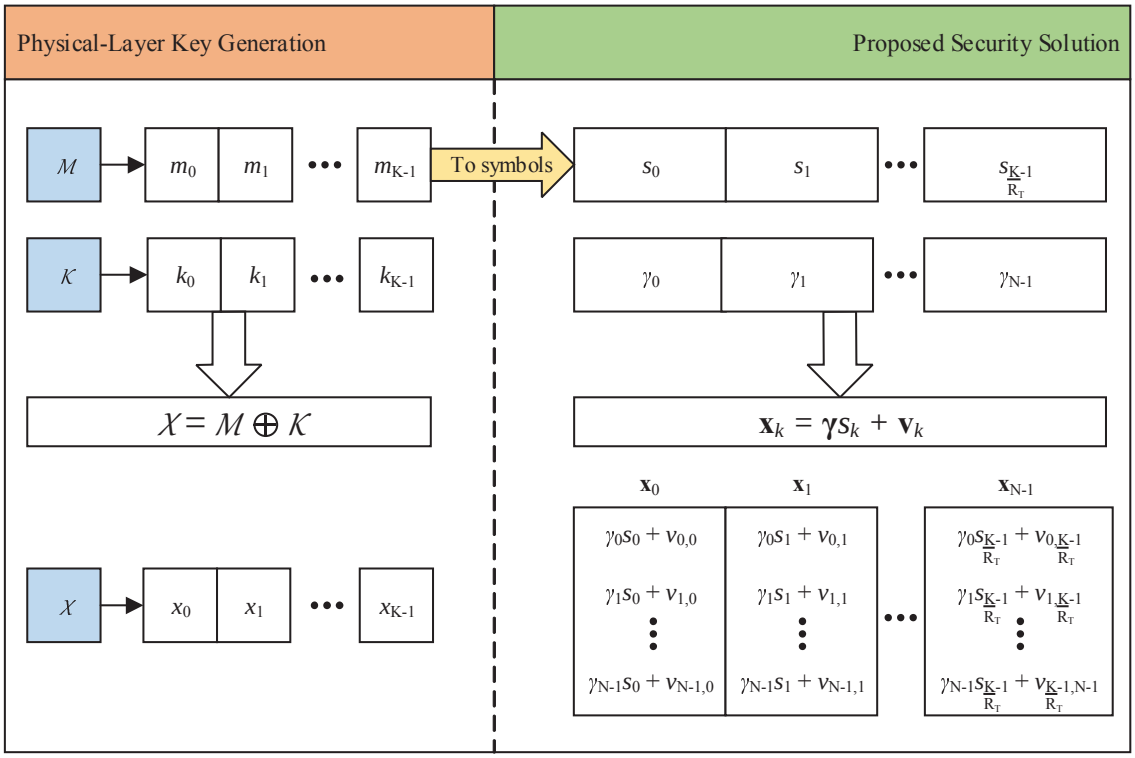

Figure 4.8. MC-SS transmitter block diagram

of quantization.

In our dissertation, we have simply adopted the complex-valued frequency response of the channel as our key. Our key generation algorithm is relatively simple because information reconciliation and privacy amplification steps are not applied to the key. Information reconciliation is not used because the secure SS communication system is fault-tolerant. A detailed discussion of the fault-tolerance property of our method will be discussed later in this section. Privacy amplification is skipped for two reasons. First, since information reconciliation is not applied, there is no information leaked to Eve about the key that Alice and Bob use. Second, we do not remove correlation between elements of the key. This is because when the golden ratio of $\phi = 1/N$ is used - i.e., a lot of artificial noise is added to the transmit signal - the correlation matrix of the transmitted signal is an identity matrix. The reason that the transmitted signal has an identity correlation matrix is described later in Section 4.4.2. As a result of this, even though two elements within a key vector may be highly correlated, the same two elements within the codeword vector are uncorrelated.

To form a codeword using both the message and key, Alice spreads each of the individ-

ual symbols of the message with her key $\boldsymbol{\gamma}_{\mathrm{A}}$. The artificial noise $\mathbf{v}$ is added to the spreaded signal and it lies in the null-space of the key. The transmitted sequence $\mathbf{x}_k$ can be written as

$$\mathbf{x}_k = \boldsymbol{\gamma}_{\mathrm{A}} s_k + \mathbf{v}_k \tag{4.30}$$

Next, Bob decrypts Alice's transmitted signal by despreading the transmitted codeword with his key $\boldsymbol{\gamma}_{\mathrm{B}}$ so that

$$\begin{aligned} \boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}} \mathbf{y}_k &= \boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}} (\mathbf{x}_k + \boldsymbol{\eta}_k) \\ &= \boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}} \boldsymbol{\gamma}_{\mathrm{A}} s_k + \boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}} \mathbf{v}_k + \boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}} \boldsymbol{\eta}_k \end{aligned} \tag{4.31}$$

Recall from the discussion of our artificial noise transmit strategy in Section 4.2.1 that if Bob's key is 'similar enough' to Alice's key such that $\rho_{\mathrm{AB}} > \rho_{\min}$ - and therefore $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{o}} > \mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}$ - then the following approximation of (4.31) is valid

$$\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}} \mathbf{y}_k \approx s_k \,. \tag{4.32}$$

Notice that Bob's key just needs to be 'similar enough' to Alice's to decrypt the message. This implies that it does not have to be *exactly* the same key as Alice. This simple idea describes one fundamental difference between traditional physical-layer key generation methods and our secure SS communication system. Physical-layer key generation methods are inherently designed around minimizing 'bit-disagreements' between Alice and Bob's keys. Any bit disagreements between Alice and Bob's key results in Bob incorrectly decoding the message. Moreover, when the one-time pad is used, and each message is equally likely to occur within its own finite alphabet, a bit disagreement in the key results in Bob decoding the wrong message and having no way of knowing that it *is* the wrong message.

In contrast, for our secure SS communication system, Alice encodes the codeword $\mathbf{x}_k$ to be tolerant to minor differences between Alice and Bob's keys. The amount of fault-tolerance is quantified by $\rho_{\min}$. Making the reasonable assumption that Alice knows the SNR between herself and Bob, Alice calculates the signal-to-artificial noise ratio ϕ using (4.22). As long as the similarity between Alice and Bob's keys - quantified by ρ_{AB} from

(4.21) - is larger than $\rho_{\min}$, then Bob should be able to successfully decode Alice's transmitted signal.

We now give the following example to further explain this concept. Assume that Alice and Bob share a 64 bit key. The key is derived from the reciprocal wireless channel. Due to the many possible non-reciprocities which can cause bit disagreements in the key shared between Alice and Bob, the key has 1 bit error. Using the one-time pad, Bob is unable to decode the message encrypted by Alice. Note that information reconciliation and privacy amplification are a standard approach in physical-layer key generation. A 1 bit discrepancy between Alice and Bob's keys can easily be handled through an information reconciliation protocol such as Cascasde [79]. Nevertheless, we will proceed with the discussion as if there is a 1 bit disagreement between Alice and Bob's codes even after information reconciliation.

For the proposed secure transmission system in this example, $\rho_{\min}$ is set so that the communication is robust against 2 out of 64 bit errors. This gives $\rho_{\min} \sim 0.9375$. For this example, $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}$ is taken to be large enough value so that Alice can dedicate enough power to artificial noise to meet the golden ratio of $\phi = 1/N$. Assuming negligible noise between Alice and Bob and solving (4.22) for target SNR, we get

$$\mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}} = \frac{\rho_{\min}}{(1-\rho_{\min})} \tag{4.33}$$

$$\approx 11.7\mathrm{dB}\,. \tag{4.34}$$

Recall from our discussion in Section 4.2.3 that the target SNR, $\mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}$, defines the desired link quality between Alice and Bob. Again, assuming that noise has minimal impact on the communication in this example, the target SNR is met as long as $\rho_{\mathrm{AB}} > \rho_{\min}$. In this example, the maximum target SNR is 11.7 dB, which means Alice can communicate *up to* a maximum rate of $R_{\mathrm{T}} = \log_2(1 + \mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}) = 4$ bits per symbol. Notice here that Alice can pack more bits per symbol if $\rho_{\min}$ was set to be tolerant to only 1 bit disagreement in the key. This essentially describes a trade-off between fault-tolerance and secure communication rate - i.e., as fault-tolerance is increased, the maximum rate (in bits per symbol) of the confidential message is decreased. To summarize this example, our proposed SS communication system allows Alice to communicate *up to* 4 confidential bits per symbol even if Bob's key differs from Alice's by 2 bits.

At this point, we would like to address a few concerns a reader may have about the proposed secure SS system. First, it can be seen from Fig. 4.8 and similarly in (4.30) that multiple information symbols are spread with the same key. At first glance, it may seem that communicating multiple symbols with just one key may give inadequate security. Indeed, without artificial noise, an adversary could easily determine the key from the transmitted sequence using a blind detection algorithm. In Section 4.3.2, we will discuss how proper design of the artificial noise parameters can allow Alice to securely communicate multiple confidential symbols using the same key against an adversary with advanced blind detection methods.

Another concern the reader may have is regarding the security of our technique against an adversary who performs a brute-force attack. A brute-force attack is one in which the adversary performs an exhaustive search over the key space to determine the key. Admittedly, one benefit of the one-time pad over our secure information transmitter is that it is robust to brute-force attacks. In the one-time pad, every possible M-length key and message within their own defined finite alphabet are equally likely to occur. When Eve tries all possible combinations of the key, she may see the correct message but has no way of knowing that this message is the correct message. Equivalently, Eve has no way of knowing what the right key is. In contrast, for our secure SS technique, when Eve guesses multiple different CIRs to determine the key, she will eventually find one which removes the artificial noise. Therefore, our system has an innate signature through which Eve can differentiate the correct key from incorrect ones. We will address the brute-force attack more thoroughly in Section 4.3.3.

4.2.3 Comparison to the Traditional Artificial Noise Systems from Literature

The secure information transmission system proposed in this dissertation makes use of the chips available to SS systems to produce artificial noise and thus, it is easily adoptable to single-antenna systems. This concept differs significantly from those in the literature - e.g., [18][20] - which use multiple antennas as means of obtaining the necessary dimensionality with which to produce artificial noise.

The original artificial noise system [24, 25] adds noise to the transmit signal that lies in the null-space of the channel, while information is transmitted in the range space of

said channel. In contrast, the secure information transmission system in this dissertation makes use of spreading gain vectors to null out the artificial noise as opposed to the CSI. The spreading codes are obtained *using* the wireless channel; however, they are processed in such a way that the codes are highly similar between Alice and Bob while significantly dissimilar between Alice and Eve.

The idea of using spreading codes, rather than the wireless channel, to null out the artificial noise has a few consequences, both good and bad. First, in traditional artificial noise systems, the wireless channel is used to remove artificial noise and it is assumed that the channel follows a block-fading model. In contrast, our method does not require that the artificial noise be removed by the wireless channel. This is helpful from an implementation standpoint in situations where the wireless channel is not well-approximated by a block-fading channel model.

Another consequence of our approach is regarding Eve's knowledge of the key. For the traditional artificial noise system, even if the adversary perfectly knows the main link channel, it does not help her since artificial noise is leaked into Eve's received signal by the Alice-Eve channel. In fact, this is one of the selling points of the traditional artificial noise method - that security can be assured even if Eve has full CSI knowledge. However, in our approach, if Eve knows the spreading code that Alice is using, security is compromised. This point is not a very significant drawback for our proposed system because Eve having full knowledge of everyone's CSI is an impractical scenario to begin with, despite the strength of that assumption in traditional artificial noise systems.

Finally, another consequence of our artificial noise model compared to the traditional setup is regarding the number of symbols which can be transmitted by Alice. In the conventional transmission system, the number of symbols which can be transmitted by Alice is limited by the assumed duration of the block-fading channel model. For our scenario, we may transmit as many symbols as required with one spreading code sequence. This motivates our study - shown in an upcoming section of the dissertation - in determining the number of symbols which can be transmitted by Alice with one spreading code before security is compromised.

4.3 Security Level of Proposed Solution

In this section, two different attack scenarios are evaluated to justify the security of the proposed solution. In the first scenario, the eavesdropping abilities of Eve are tested and in the second scenario, we look at the blind detection capabilities of the adversary.

4.3.1 Scenario 1: The Passive Eavesdropper

For the first attack scenario, Eve is a passive eavesdropper who tries to decode Alice's transmitted information symbols using the key she generates. Eve is equipped with the same receiver as Bob and the only difference between them is their despreading codes.

To evaluate the security level of this attack, we first consider use of the secrecy characterization from [15], where the notion of secrecy outage probability is expressed as

$$\mathcal{P}_{\text{out}}(R_s) = \mathcal{P}\left(C_{\text{B}} - C_{\text{E}} < R_s\right). \tag{4.35}$$

where $C_{\text{B}} = \log_2(1 + \text{SNR}_{\text{B}}^{\text{o}})$, $C_{\text{E}} = \log_2(1 + \text{SNR}_{\text{E}}^{\text{o}})$.

The definition in (4.35) makes an assumption that the transmitter chooses a strategy that leads to the main link communicating near capacity of the channel. In this way, while $\text{SNR}_{\text{B}}^{\text{o}}$ will allow for sufficient information recovery at Bob's node, $\text{SNR}_{\text{E}}^{\text{o}}$ will be inadequate in decoding information at Eve's node. The parameter R_s is effectively a margin that when chosen larger, increases the secrecy outage probability. An outage is said to occur when a message is either unreliable for Bob to decode or insecure, i.e., there will be a possibility that Eve decodes the message.

A known weakness of the secrecy characterization by (4.35) was first discussed in [16]. It was noted that (4.35) does not distinguish between reliability and security. The secrecy outage probability may be minimized for a given set of design parameters, but it is not obvious from (4.35) whether this is due to an information leak or a reliability issue.

Accordingly, the following alternative definition of the secrecy outage probability was proposed. The outage was defined for when the difference between the target capacity and Eve's capacity is lower than R_s conditioned on the event that a message was transmitted. In our model, we assume that message transmission always occurs since Alice and Bob are operating independent of one another. The secrecy outage probability definition from [16] is thus modified as

$$\mathcal{P}_{\text{out}}(R_s) = \mathcal{P}\left(R_{\text{T}} - C_{\text{E}} < R_s\right) \tag{4.36}$$

where

$$R_{\text{T}} = \log_2(1 + \text{SNR}_{\text{T}}^{\text{o}}) \tag{4.37}$$

The definition of (4.36) states that an outage occurs when the SNR after despreading at Eve's node is within the margin of R_s from the target rate R_{T}. The characterization in (4.36) is useful from a practical standpoint in which Alice and Bob are operating independent of one another. In such a case, Alice chooses a code that optimally works (i.e., error-free) for target rate R_{T}. This is different from the characterization in (4.35) where it is implied that if $\text{SNR}_{\text{B}}^{\text{o}} > \text{SNR}_{\text{T}}^{\text{o}}$, then Alice chooses a different code to work at rate C_{B} rather than the target rate R_{T}. It also follows that if Alice and Bob are communicating near target rate R_{T}, an appropriate definition for an information leak is the scenario in which C_{E} is near R_{T} rather than the case where C_{E} is close to C_{B}.

With regards to the reliability of the main link, we note that a nice feature of our artificial noise power allocation strategy is that it assures a target SNR is met so long as the similarity between the keys generated by Alice and Bob is above a threshold. In other words, it can be easily verified that if ϕ is obtained from (4.22), then $\mathcal{P}(\text{SNR}_{\text{B}}^{\text{o}} < \text{SNR}_{\text{T}}^{\text{o}})$ is equal to $\mathcal{P}(\rho_{\text{AB}} < \rho_{\min})$.

We interpret at the secrecy outage characterization in (4.36) as an SNR difference. Fig. 4.9 is shown to help the reader understand how this equation can be looked at as an SNR difference Here, we take the equation $C_E = R_{\text{T}} - R_s$ and plot the corresponding SNRs for different values of R_s. The curves in Fig. 4.9 show the lines beyond which an outage occurs. It is easy to verify that when $R_s = 0$, the secrecy outage probability reduces to a comparison of the despreaded signal SNR's at Bob and Eve's nodes. When R_s is increased, the requirement for a secrecy outage to occur is stricter since the required difference between Bob and Eve's channel capacity needs to be larger to meet a higher R_s.

4.3.2 Scenario 2: The Sophisticated Eavesdropper

In this attack scenario, Eve is given a significant advantage in decoding the transmitted data. In traditional artificial noise systems, e.g., [24, 25, 75–77], the assumption

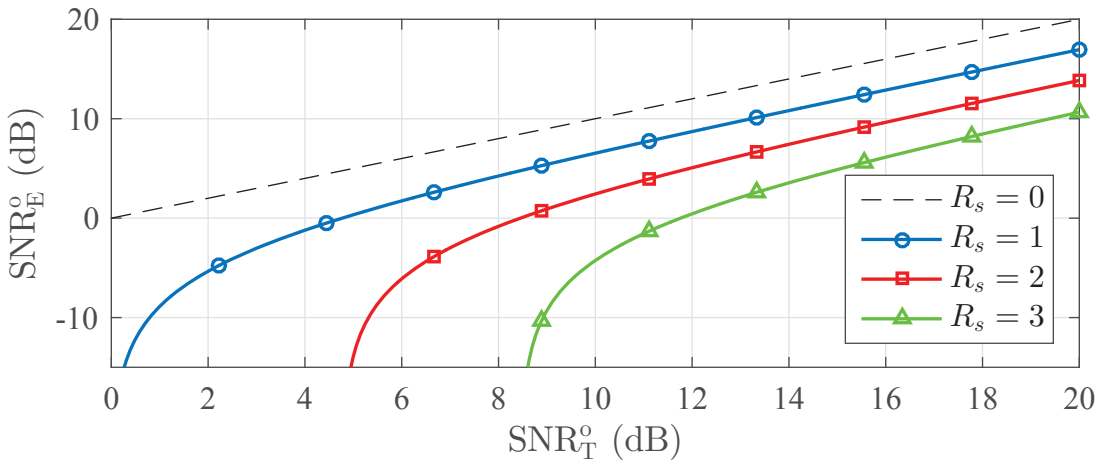

Figure 4.9. Plot of $\mathrm{SNR}_{\mathrm{E}}^{\mathrm{o}}$ vs. $\mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}$ in dB for selected values of R_s.

of a block-fading channel model limits the number of symbols that can be transmitted confidentially. With our formulation, we can transmit as many symbols as needed with a given spreading code since the channel is not used to directly decrypt the information. The consequence of encoding many symbols with the same spreading gain sequence is that a sophisticated adversary may use a *blind method* to identify the information signal subspace and subsequently use that knowledge to decode the communicated data.

Without artificial noise (i.e., $\phi = 1$), secrecy against knowledgeable adversaries could *only* exist for our system model if 1) Eve is at an SNR disadvantage compared to the main link or 2) Alice only transmits one symbol per key, effectively applying a one-time pad to the solution provided the key is generated at channel coherence time intervals. Both of these assumptions are considerably strong to impose on the security of a wireless communication network. Here, we study the use of artificial noise as a way to increase throughput of the secure communication system without assuming Eve to be at a disadvantage.

This attack scenario considers the situation where Alice transmits K symbols with the same spreading code sequence and Eve seeks to estimate $\boldsymbol{\gamma}_{\mathrm{A}}$ from her received signal. To facilitate this study, we redefine (4.15) as a matrix of concatenated received signal vectors spread with the same key

$$\begin{aligned} \mathbf{Z} &= \begin{bmatrix} \mathbf{z}_0 & \mathbf{z}_1 & \dots & \mathbf{z}_{K-1} \end{bmatrix} \\ &= \begin{bmatrix} \mathbf{x}_0 + \boldsymbol{\epsilon}_0 & \mathbf{x}_1 + \boldsymbol{\epsilon}_1 & \dots & \mathbf{x}_{K-1} + \boldsymbol{\epsilon}_{K-1} \end{bmatrix} \end{aligned} \tag{4.38}$$

where $\mathbf{Z} \in \mathbb{C}^{N \times K}$.

The columns of $\mathbf{Z}$ are a set of random vectors. Each of these vectors have the average energy/power of P and the form of (4.15). There is a fixed direction $\boldsymbol{\gamma}_{\mathrm{A}}$ that carries data symbols with the power ϕP. The rest of the power is in a random direction perpendicular to $\boldsymbol{\gamma}_{\mathrm{A}}$. When the golden ratio - i.e., $\phi = 1/N$ - is used, the signal power is equally distributed in all directions, including the direction $\boldsymbol{\gamma}_{\mathrm{A}}$. In this scenario, the signal space will appear to be white with respect to all directions, including the data direction, making it hard for an observer that wishes to find $\boldsymbol{\gamma}_{\mathrm{A}}$. The situation will be different when $\phi \neq 1/N$. In such cases, the intruder can search for the direction that carries a different power than the remaining directions.

The standard solution to find the signal direction, i.e., the spreading gain vector $\boldsymbol{\gamma}_{\mathrm{A}}$, when $\phi > 1/N$, is the following.

1. Construct the $N \times N$ matrix

$$\mathbf{R}_{\mathbf{ZZ}} = \frac{1}{K}\mathbf{Z}\mathbf{Z}^{\mathrm{H}} \tag{4.39}$$

2. Invoking the Rayleigh-Ritz Theorem [80], an estimate of $\boldsymbol{\gamma}_{\mathrm{A}}$ is obtained by solving the following maximization problem

$$\hat{\boldsymbol{\gamma}}_A = \arg \max_{\|\boldsymbol{\gamma}\|=1} \boldsymbol{\gamma}^{\mathrm{H}} \mathbf{R}_{\mathbf{ZZ}} \boldsymbol{\gamma} \tag{4.40}$$

For this procedure to give an accurate estimate, the number of signal samples (i.e., the parameter K) should be sufficiently large. To give an idea of how how large K should be to obtain a reasonable estimate of $\boldsymbol{\gamma}_{\mathrm{A}}$, we resort to some numerical results which are presented in the next section.

4.3.3 Scenario 3: The Brute-Force Attacker

The two passive eavesdropper attacks discussed so far may not necessarily encompass all possible attacks on the proposed system. Another feasible attack that a passive Eve may use is a brute-force attack. In this attack, Eve takes her received signal vector and guesses multiple different CIRs in an attempt to find one which aligns closest to the information-bearing signal space.

The current key generation technique generates a key of length N using the frequency response of a CIR measurement. If the key obtained by Alice and Bob has N' mutual information bits, then Eve needs to try up to $2^{N'}$ CIRs to obtain a sufficient estimate for the spreading code that will remove the artificial noise. Note that the amount of CIRs Eve would need to try depends on many things, including the signal-to-noise ratio associated with both Alice and Bob's spreading codes, the level of fault-tolerance that Alice builds in her transmit signal, and the amount of randomness in the spreading code that Alice and Bob generate.

Nevertheless, we will make an admittedly simple attempt to determine the computational complexity of the brute-force attack. Assume that Alice and Bob have probed the wireless channel and generate spreading codes using the CIR. The spreading code can be any vector that spans the complex-valued N dimensional space. In this dissertation, we have simply adopted the channel's frequency response as the spreading code. Instead of using the key described in Chapter 2, we will assume that Alice and Bob have optimally performed the key generation steps in such a way that the entropy rate of the resulting key approaches the capacity of the wireless channel [81].

Using the method described in [51], we can obtain a rough number for the mutual information in the key for the channel described in Section 2.7.1. Assuming an SNR of 20 dB, the mutual information of a key derived in this channel is 16 bits per channel observation.

One last piece of information about the brute-force attack is regarding the fault-tolerance property of our proposed secure transmission solution. Recall the discussion in Section 4.2.1 about our power allocation strategy in which Alice dedicates enough transmit power to the information symbols to ensure a target SNR is met at Bob's node as long as Alice and Bob's spreading codes are similar enough. The criteria used in describing the similarity between Alice and Bob's keys is quantified by ρ_{AB}. If ρ_{AB} is larger than ρ_{min}, then Bob has sufficient SNR to decode Alice's transmitted information. Essentially, ρ_{min} describes the amount of fault-tolerance in our communication system. As ρ_{min} approaches 1, the secure transmission system becomes less fault-tolerant.

For the brute-force attack, Eve guesses many different CIRs in an attempt to determine one that will remove the artificial noise. If ρ_{min} is chosen to be less than one, then Eve

- similar to Bob - may be able to sufficiently remove artificial noise from the transmitted codeword even if there are differences between Eve's guessed key and the key Alice uses to encrypt the message. In short, we have briefly described a trade-off between fault-tolerance and resilience to brute-force attacks. Alice may choose a low value for $\rho_{\min}$ to increase fault-tolerance, but this comes at a cost to the system's resiliency against brute-force attacks.

For the time being, the study of these details is left for future research. Instead, for our simple brute-force attack model, we will make an assumption that no fault-tolerance is built into the design - i.e., $\rho_{\min} = 1$. As per the discussion above, the spreading codes contain approximately 16 bits per channel observation. Hence, Eve must to try up to 2^{16} different CIRs in order to obtain a key that will remove the artificial noise in her received signal vector. Note that the discussion is this section has also featured a worst-case adversary who receives a noiseless signal vector from Alice.

Other methods of increasing resiliency against the brute-force attack may exist. For example, another option for generating the key would be to take an approach where Alice and Bob use multiple CIRs - sampled at coherence time intervals - to generate a key that is more random than the key discussed in this dissertation. With such a key, the computational complexity of the brute-force attack can be increased significantly, making the task of a brute force attack very demanding.

Another option for increasing computational complexity of the brute-force attack is described by example as follows. Generate 8 independent keys, each containing approximately 16 bits per channel observation. Next, take a length M message and scramble it across 8 packets in such a way that it requires all 8 keys to extract the M length message. This proposed idea would require 8 keys to obtain the message and therefore a brute-force attacker would need to try up to $2^{8\times 16} = 2^{128}$ keys.

In light of the intricacies associated with the brute-force attack, its detailed study remains a problem for future research. In particular, we hope to achieve a better understanding of the system model from an information-theoretic perspective. Using information-theory could potentially allow us to quantify the security of the proposed secure SS communication system.

4.4 Results

The secure information transmission system that we propose adds artificial noise to the traditional MC-SS as a means of enhancing physical-layer secrecy. At this point, we turn our attention to validating the security of the proposed system and its expected performance for the legitimate parties. We take $N = 64$ since it is the value of N that was used in our spreading gain generation experiments as well as in our current implementation of the FB-MC-SS system in [35].

We consider the limit of (4.20) as the SNR approaches infinity. To simplify the discussion here, we define SNR^{o} in (4.20) as the despreaded signal SNR at Bob or Eve's link. Similarly, SNR^{i} and ρ respectively from (4.16) and (4.21) are defined in this way. Using L'Hospital's Rule,

$$\lim_{\text{SNR}^{\text{i}} \to \infty} \text{SNR}^{\text{o}} = \frac{(N-1)\phi\rho}{(1-\phi)(1-\rho)}\,. \tag{4.41}$$

It is trivial to see from (4.41) that if no artificial noise is used (i.e., $\phi = 1$) and as $\text{SNR}_{\text{E}}^{\text{i}} \to \infty$, $\text{SNR}_{\text{E}}^{\text{o}}$ will also increase to infinity hence, no secrecy can be guaranteed regardless of how dissimilar Alice and Eve's keys are. However, the addition of artificial noise (i.e., when ϕ drops below one) provides an intriguing opportunity to securely transmit confidential information despite Eve having a significant SNR advantage. Fig. 4.10 plots (4.41) as a function of ρ for different values of ϕ.

In previous literature of artificial noise, where perfect CSI knowledge is assumed (i.e., $\rho_{\text{AB}} = 1$), high values of secrecy data rates can be achieved. However, as can be seen in Fig. 4.10, if $\rho_{\text{AB}} < 1$, there is an exponential drop in $\text{SNR}_{\text{B}}^{\text{o}}$ which can lead to a significant data reliability issue that gets exacerbated as artificial noise power is increased. This highlights the main advantage of our artificial noise power allocation strategy in (4.22) because it compensates for dissimilarity between Alice and Bob's keys by strategically introducing enough artificial noise such that a target rate is hit for a given ρ_{min} that fits the criteria of (4.25).

In Fig. 4.10, it can also be seen that the limit of the despreaded signal's SNR linearly increases for $\{\rho \mid 0.2 < \rho < 0.8\}$. Moreover, (4.41) asymptotically approaches infinity as $\rho \to 1$ and approaches zero as $\rho \to 0$. In short, this trend is encouraging as it shows that the introduction of artificial noise allows for nodes with the "right" key to reliably decode

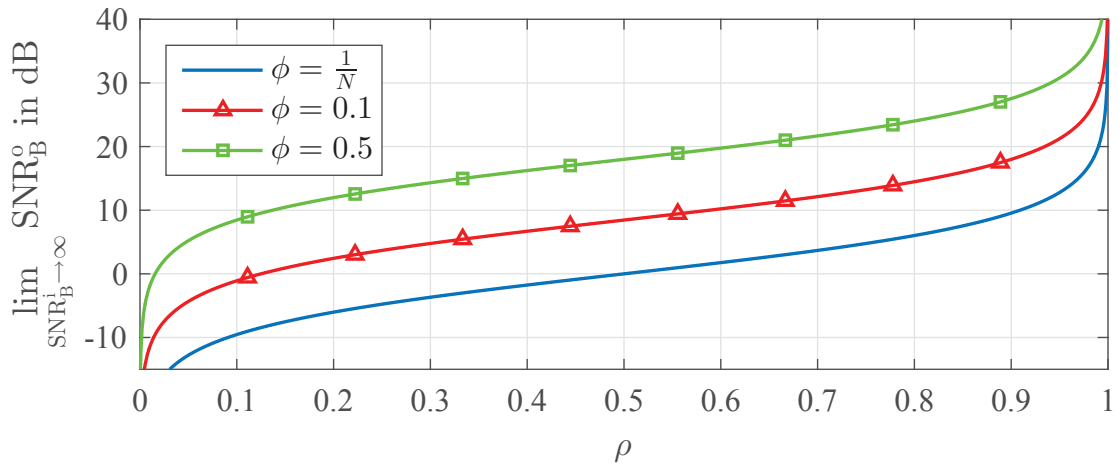

Figure 4.10. Plot of the SNR after despreading - $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{o}}$ - as link SNR approaches infinity as a function of ρ - a measure of similarity between Alice and Bob's keys - for selected values of ϕ.

the confidential information while it hampers the decoding ability of users with different keys, even when they have a considerable SNR advantage.

Next, we discuss the two scenarios of the "passive eavesdropper" and "sophisticated eavesdropper".

4.4.1 Scenario 1: The Passive Eavesdropper

Results from the simulation and experimentation channel models from Chapter 2 are used to evaluate the key generation procedure in the context of the proposed secure information transmission system (note that the simulation channel model that we consider here is the same as the one used to obtain results in Chapter 3). Two sets of keys will be compared: the key generated before SPC and the key after applying SPC.

As discussed before, Eve follows the same steps as the main link in retrieving the transmitted symbols sent by Alice. The effectiveness of this attack is evaluated using the secrecy outage probability in (4.36). To ensure fair comparison between the two sets of keys, $\rho_{\min}$ is set according to the *Training Method* in Section 4.2.1.1 using $\delta_{\mathrm{T}}^{\mathrm{o}} = 95\%$ in (4.27). In this way, 95% of the keys used will meet the target SNR after despreading, i.e.,

$$\mathcal{P}(\mathrm{SNR}_{\mathrm{B}}^{\mathrm{o}} < \mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}) = \mathcal{P}(\rho_{\mathrm{AB}} < \rho_{\min}) = 5\%\,. \tag{4.42}$$

In this way, $\rho_{\min}$ will be smaller for the keys that use SPC due to the slight decorrelation effect that SPC has on the keys. In turn, this means less artificial noise can be added for the keys obtained using SPC. Note that this formulation uses *a-priori* knowledge of ρ_{AB} to determine $\rho_{\min}$, but that this is only used to ensure a fair comparison between the two sets of keys. In practice, when *a-priori* knowledge is not available, $\rho_{\min}$ should be set according to the *Target* $\phi_{\min}$ strategy in 4.2.1.2.

The secure information transmission strategy that we use is one in which the target rate is adapted according to $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}$. For the adaptive target rate strategy, when $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}$ is too low to meet a minimum target rate $R_{\mathrm{T}\min}$ at $\phi = 1/N$, the signal-to-artificial noise ratio is calculated using (4.22). When the SNR at Bob's receiver is high enough and thus, a large amount of artificial noise power can be added (i.e., $\phi = \phi_{\min} = 1/N$), then the target rate is increased. To find the target rate in this scenario, we first solve for $\mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}$ in (4.22) at $\phi = 1/N$ to obtain

$$\mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}} = \frac{\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}\rho_{\min}}{1 + \mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}(1-\rho_{\min})} \tag{4.43}$$

and then calculate R_{T} using (4.37).

Fig. 4.11 shows evaluation of (4.36) at $R_s = 1$ for the passive eavesdropper attack for simulation and experimentation results when using the adaptive target rate strategy. The solid lines correspond to before SPC and the dashed lines correspond to after SPC. To generate this figure, we assume a worst-case scenario where Eve has zero additive noise at the receiver. The minimum target rate $R_{\mathrm{T}\min}$ is set to 2 bits and is incremented according to $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}$. Additionally, a reliability of 95% at the main link is met for all SNR values in Fig. 4.11. Note that to guarantee this reliability, the smallest value for $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}$ corresponds to $\phi = 1$ for the keys applied with SPC. Below the minimum value of $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}$, there is not enough transmit power at Alice's node to allow for the minimum target rate of 2 bits.

To help the reader envision how the plot in Fig. 4.11 is generated, we also present Fig. 4.12. Note that in this figure, the top plot corresponds to the key generated from simulation and the bottom plot shows experimentally derived keys. Similar to Fig. 4.11, solid and dashed lines correspond to keys generated before and after SPC, respectively. In

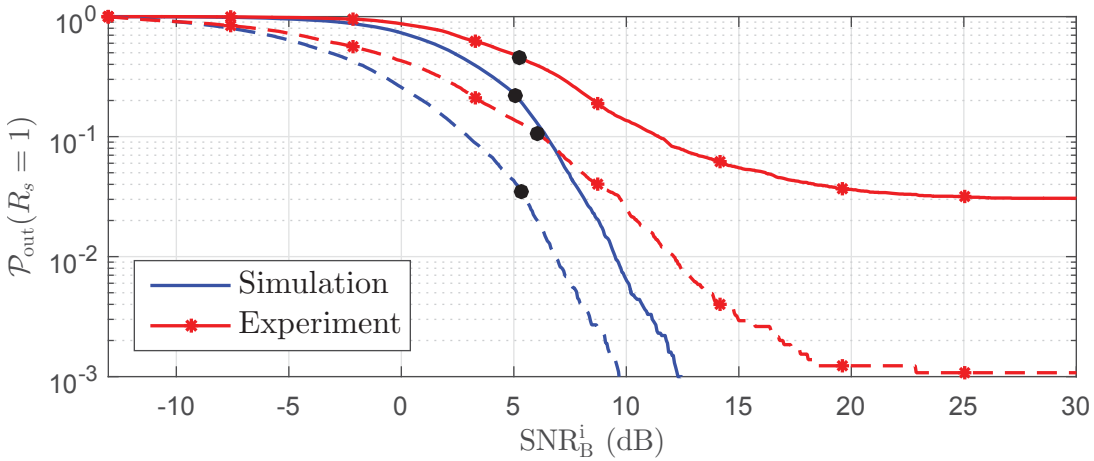

Figure 4.11. Plot of the outage probability of secrecy evaluated at $R_s = 1$ as a function of receiver SNR for the adaptive target rate strategy. The plot was obtained using the ρ_{AB} and ρ_{AE} values from keys obtained through simulation and experiment. Dashed lines show keys after SPC is applied. Black circles indicate the transition point at which the target rate R_{T} starts increasing and the golden ratio $\phi = 1/N$ is used.

Fig. 4.12, the dashed line at $R_s = 1$ indicates the point at which the outage probability for 4.11 is evaluated and we show the outage probability as a function of R_s for $\text{SNR}_{\text{B}}^{\text{i}} = 0$ dB and $\text{SNR}_{\text{B}}^{\text{i}} = 10$ dB. It can be seen that as the receiver SNR at Bob's node is increased, the capacity difference between the target rate and Eve's channel capacity increased and hence, the secrecy outage probability descreased. Furthermore, when a large amount of artificial noise is used, the difference in secrecy outage probability is less between that derived with and without SPC. This is because when a large amount of artificial noise can be used, a slight mismatch in keys becomes sufficient in confusing the eavesdropper.

Results from Fig. 4.11 indicate that the keys derived using SPC provide a significant boost to the security of the system. This is despite the fact that less artificial noise is being broadcast at lower values of SNRs (i.e., the $\text{SNR}_{\text{B}}^{\text{i}}$ values to the left of the black circles) as a result of the way ρ_{min} was obtained. It can also be seen that when $\text{SNR}_{\text{B}}^{\text{i}}$ is high and $\phi = 1/N$, the probability of secrecy outage approaches a steady state. For the experiment data set, the steady state value for the secrecy outage probability is $\approx 3\%$ for keys that do not use SPC, while keys applied with SPC are $\approx 0.1\%$. Therefore, the minimum amount of security is better with SPC than without. Finally, we note that this transmit strategy allows us to use high levels of artificial noise power ($\phi = 1/N$), which is not only good in

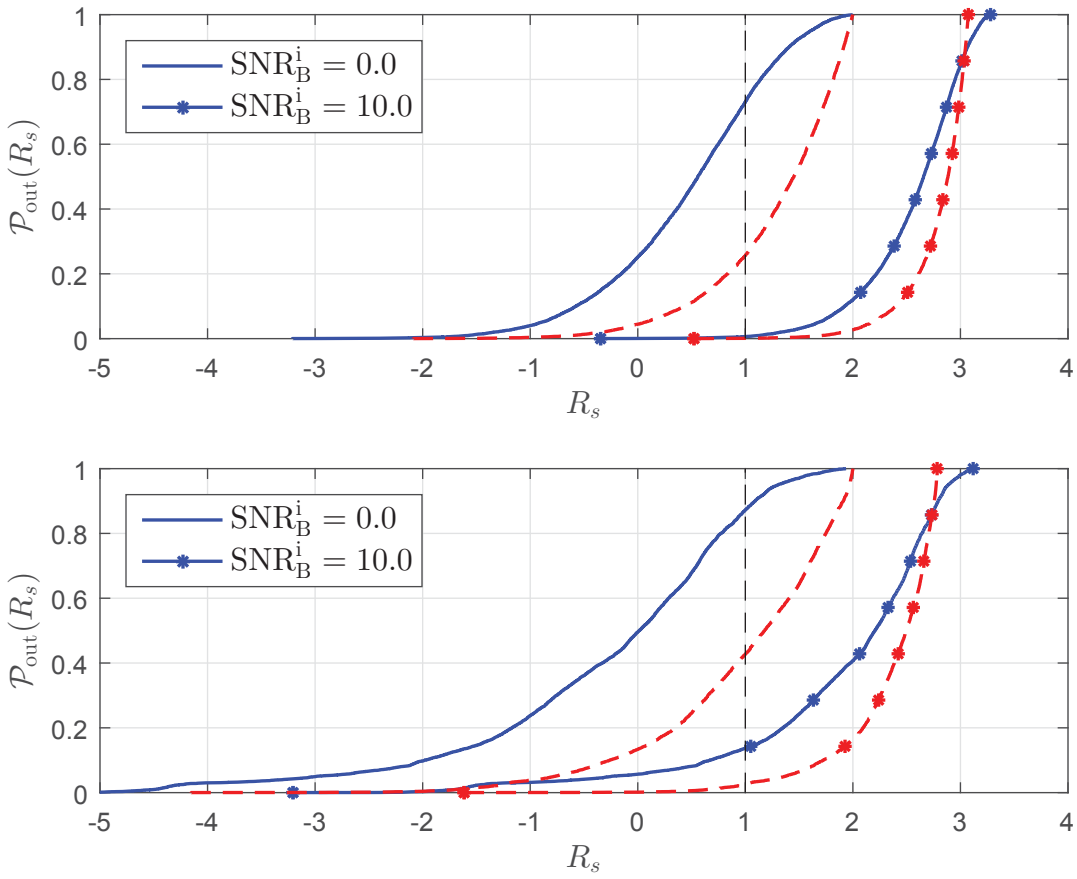

Figure 4.12. Plot of $\mathcal{P}_{\mathrm{out}}(R_s)$ vs. R_s for keys generated through simulation (top) and experiment (bottom). Solid and dashed curves coincide with keys generated with and without SPC, respectively. Two values of $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}$ are shown so that the probability of a secrecy outage can be compared for different levels of ϕ.

securing communications from a secrecy outage standpoint but also beneficial in thwarting the efforts of the more sophisticated adversary that we discuss next.

4.4.2 Scenario 2: The Sophisticated Eavesdropper

In this section, we show two different sets of results pertaining to the case wherein multiple symbols are transmitted with the same spreading code sequence. First, we examine the transmitted sequence correlation matrix. Here, it is shown that the correlation between elements of the transmitted signal is approximately zero when the golden ratio of $\phi = 1/N$ is used, despite there being a high amount of correlation between elements of the key. Next, we examine the amount of symbols that can be transmitted with one key as artificial noise power is varied.

First, consider the transmitted data vector $\mathbf{x}_k$ from (4.8). It is shown in Appendix C that the covariance matrix of this signal for a given $\boldsymbol{\gamma}_{\mathrm{A}}$ can be expressed as

$$\mathrm{E}[\mathbf{x}_k \mathbf{x}_k^{\mathrm{H}}] = \frac{1}{N}\sigma_w^2 \mathbf{I}_{\mathrm{N}} + \left(\sigma_s^2 - \frac{1}{N}\sigma_w^2\right)\boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}} \tag{4.44}$$

where $\mathbf{I}_N$ is an $N \times N$ identity matrix.

Fig. 4.13 plots the magnitude of the covariance matrix of an example $\boldsymbol{\gamma}_{\mathrm{A}}$ coming from our experimental data set for four distinct cases of ϕ. Here, it is interesting to see that when $\phi = 1/N$, the second term in (4.44) vanishes and hence, the covariance matrix of the transmit sequence will be identity. The significance of this finding is that when the golden ratio is used, the signal direction $\boldsymbol{\gamma}_{\mathrm{A}}$ will not be observable in the correlation matrix $\mathrm{E}[\mathbf{x}_k \mathbf{x}_k^{\mathrm{H}}]$ and thus, any method that seeks to estimate $\boldsymbol{\gamma}_{\mathrm{A}}$ by exploring the second order moments of $\mathbf{x}_k$ will be unsuccessful.

Next, we use numerical results to evaluate the effectiveness of the blind attack from a sophisticated adversary as discussed in Section 4.3.2. The goal of this simulation is to examine the number of symbols K that can be sent with a given key $\boldsymbol{\gamma}_{\mathrm{A}}$. To start, Alice transmits K symbols with a given spreading code sequence obtained from the experimental data set. The information symbols are encoded with binary phase-shift keying (BPSK) so that $s_k = \pm\, \sigma_s$ and we assume the worst-case eavesdropper who has zero channel noise, and thus, $\mathbf{z}_k = \mathbf{x}_k$.

Once Eve receives K symbols, she constructs the matrix $\mathbf{Z}$ as in (4.38). Next, the Rayleigh-Ritz theorem (4.40) is applied to obtain a blind estimate of the spreading code sequence. This process is run for increasing values of K from 4 to 256, and different choices of ϕ. To evaluate the effectiveness of this attack, we calculate the similarity between $\hat{\boldsymbol{\gamma}}_A$ and $\boldsymbol{\gamma}_{\mathrm{A}}$ using (4.21).

A set of plots is shown in Fig. 4.14 to enlighten the reader's understanding of the blind detection method we use. In this set of plots, the eigenvalues of $\mathbf{Z}$ are shown for different values of ϕ and K. The N eigenvalues of $\mathbf{Z}$ are normalized to unit length. Since $\mathbf{Z}$ is a correlation matrix, its eigenvalues are all real and non-negative [82].

In these plots, it can be seen that when K is large (and thus, $\mathbf{Z}$ is a rectangular matrix), the information bearing subspace becomes easier to deduce from the artificial noise subspace for $\phi = 2/N$ and $\phi = 8/N$. The reason for this is that the basis vectors that span

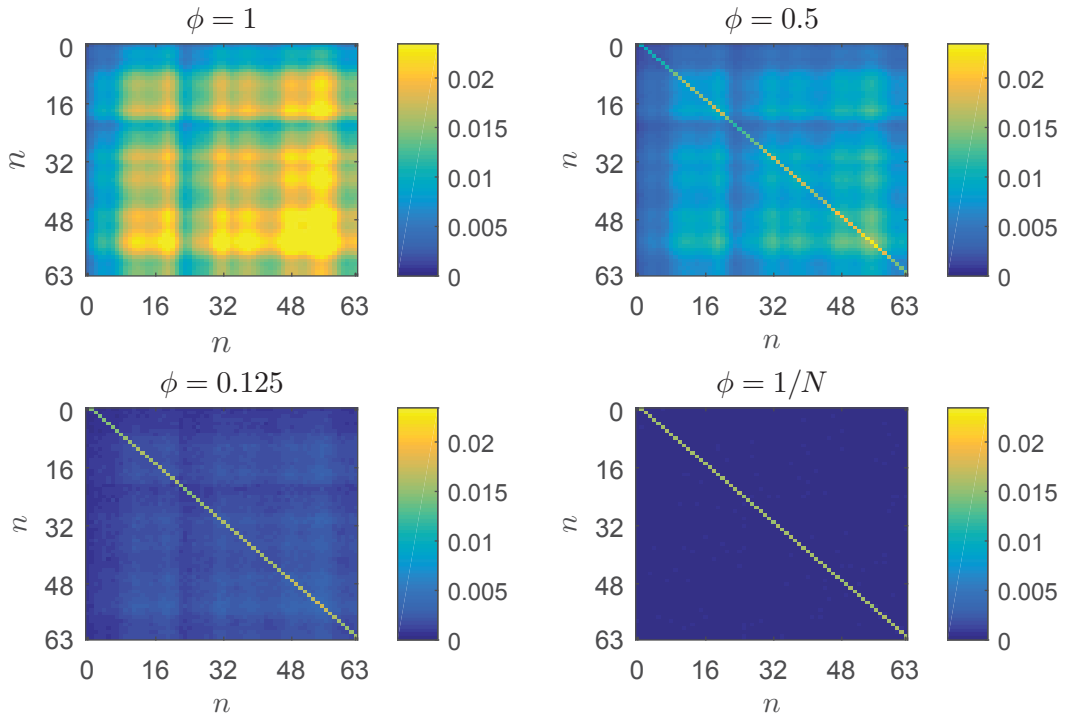

Figure 4.13. Plot of the magnitude of covariance matrix of $\mathbf{x}_k$ for one $\boldsymbol{\gamma}_{\mathrm{A}}$ from the experiment data set for selected values of ϕ

the N dimensions in $\mathbf{x}_k$ are estimated better for large K relative to N. Hence, the artificial noise subspace which contains $N-1$ basis vectors is better estimated for large K as is the remainder subspace which carries the key. However, as it can be seen in Fig. 4.14, when the golden ratio is used - i.e., $\phi = 1/N$ -, it is very difficult to distinguish between the artificial noise and information signal subspaces through an eigenvalue decomposition because power is evenly distributed across all N dimensions even for large values of K relative to N.

Fig. 4.15 plots the 99th percentile of ρ_{AE}, when $\boldsymbol{\gamma}_{\mathrm{E}}$ is set equal to $\hat{\boldsymbol{\gamma}}_A$ (the key found through blind detection by Eve), as a function of K for varying values of ϕ. The 99th percentile shows the line where 99% of the time, ρ_{AE} remains below it. As observed for larger values of ϕ, i.e., when the level of artificial noise is relatively low, the eavesdropper may be able to obtain a reasonable estimate of $\boldsymbol{\gamma}_{\mathrm{A}}$ within a relatively small number of observed samples. However, as ϕ increases, it becomes more difficult to estimate $\boldsymbol{\gamma}_{\mathrm{A}}$. For the golden ratio of $\phi = 1/N$, since $\mathrm{E}[\mathbf{x}_k \mathbf{x}_k^{\mathrm{H}}]$ become the identity matrix, almost all the estimates of $\boldsymbol{\gamma}_{\mathrm{A}}$ remain nearly orthogonal to $\boldsymbol{\gamma}_{\mathrm{A}}$ hence, guaranteeing secure communication.

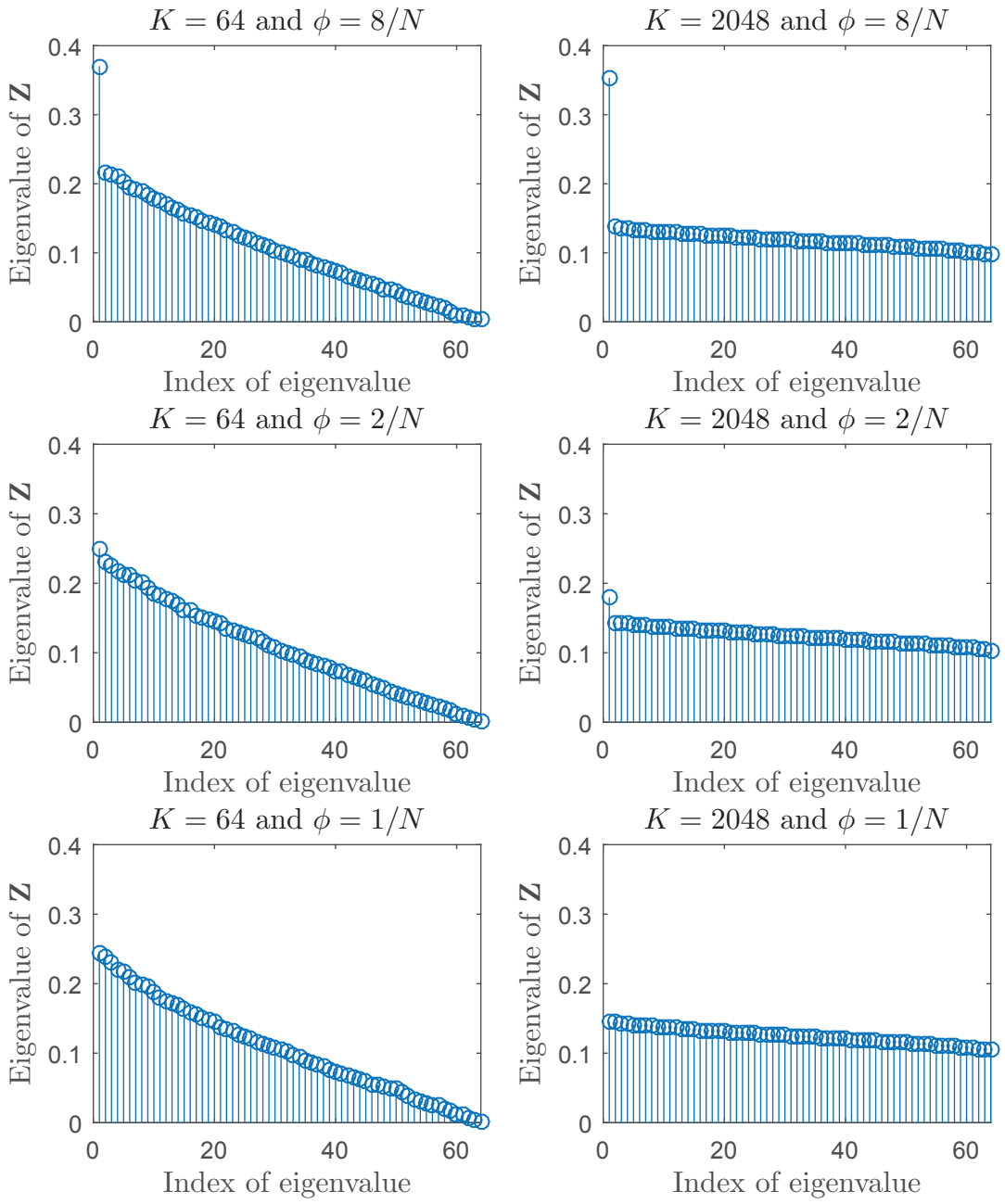

Figure 4.14. Plot of the eigenvalues of $\mathbf{Z}$ for chosen values of K and ϕ.

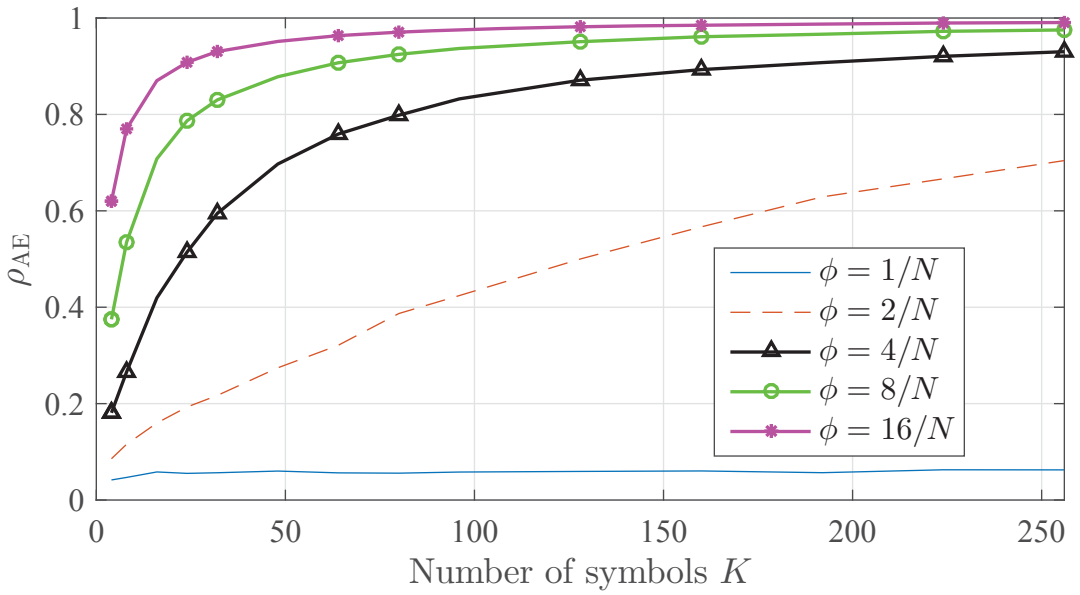

Figure 4.15. Plot of the 99th percentile of ρ_{AE} as a function of K. Note that the 99th percentile indicates that 99% of the time, ρ_{AE} is below the lines indicated in the graph.

4.4.3 Comparison of keys

This section will be used to compare keys that have been proposed in this dissertation. The comparison will consider the passive eavesdropper attack (i.e., Scenario 1 from Section 4.3.1). This is because for the second attack scenario, it does not matter how the key is obtained since the suggested blind detection algorithm merely observes the power of the information-bearing subspace to find the key. The reason that this comparison is given is so we can determine whether the loss in similarity due to removing the strongest path of the channel is worth the effort. Moreover, we also study the key that we proposed in one of our previous reports in [42].

The comparison will make use of the secrecy characterization from (4.36) which can be written and expanded as follows

$$\begin{aligned}\mathcal{P}_{\text{out}}(R_s) &= \mathcal{P}\left(R_{\text{T}} - C_{\text{E}} < R_s\right) \\ &= \mathcal{P}\left(\log_2\left(1+\frac{N\phi\rho_{\min}\text{SNR}_{\text{B}}^{\text{i}}}{\frac{N}{N-1}(1-\phi)(1-\rho_{\min})\text{SNR}_{\text{B}}^{\text{i}}+1}\right) - \dots \right. \\ &\qquad \left. \log_2\left(1+\frac{N\phi\rho_{\text{AE}}}{\frac{N}{N-1}(1-\phi)(1-\rho_{\text{AE}})}\right) < R_s\right). \end{aligned} \tag{4.45}$$

Note that in (4.45), we have implicitly taken Eve's receiver to be noiseless and the expression from R_{T} comes from the signal-to-artificial noise ratio equation from (4.22). It can be seen from (4.45) that there are 6 total variables in this characterization: N, ϕ, $\rho_{\min}$, $\text{SNR}_{\text{B}}^{\text{i}}$, ρ_{AE}, and R_s. As a way of simplifying the secrecy characterization for comparing keys, we point out that only the golden ratio of $\phi = \frac{1}{N}$ is considered since it is found to be optimal for the second attack scenario. Moreover, we will hold $\rho_{\min}$ based on the same rule used in Section 4.4.1 so that 95% reliability can be ensured for the communication between the main link. This simplifies (4.45) to the following expression

$$\mathcal{P}_{\text{out}}(R_s) = \mathcal{P}\left(\log_2\left(\frac{(\text{SNR}_{\text{B}}^{\text{i}}+1)(1-\rho_{\text{AE}})}{(1-\rho_{\min})\text{SNR}_{\text{B}}^{\text{i}}+1}\right) < R_s\right) \tag{4.46}$$

To summarize the discussion so far, the secrecy characterization we use simplifies to (4.46). This is effectively the rate difference - R_d - between the target rate R_{T} and Eve's channel capacity C_{E} evaluated at some $\text{SNR}_{\text{B}}^{\text{i}}$, with $\phi = 1/N$, and $\text{SNR}_{\text{E}}^{\text{i}} \to \infty$. The value

of $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}$ that we use for the simulation data will be 10 dB which is the SNR value used to obtain keys in the simulation.

To evaluate measurement data, we use an estimate of the instantaneous SNR between Alice and Bob of each channel realization to get $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}$. This means that the target rate R_{T} will be a function of $\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}$. This method allows us to interpret the secrecy characterization in a way that is closer to how it would be implemented on a practical system.

To help the reader intuitively understand the results of the comparison, we plot, in Fig. 4.16, the partial correlations of the keys between Alice-Bob and Alice-Eve for the three following types of keys:

Key 1: The standard key generation approach used in this dissertation which follows (2.13) (solid lines in Fig. 4.16).

Key 2: The same as *Key 1* but generated after SPC is applied (dashed lines in Fig. 4.16).

Key 3: The key discussed in [42] from (2.14) in which the key is taken to be the summation of the phasors of the CIR with a shuffled version of the same signal. We only consider SPC-augmented keys here for brevity (dotted lines in Fig. 4.16).

The partial correlations in Fig. 4.16 show that *Key 3* gives keys which are most dissimilar for the Alice-Eve pair. However, this key also significantly decorrelates the Alice-Bob keys as well. At this point, we are ready to compare the keys using the secrecy characterization described in this section to quantify whether the loss in reciprocity is worth the gain in secrecy of these keys.

Fig. 4.17 shows a pair of plots for the simulated channel and Fig. 4.18 shows the same plots for the experimental data set. In the left-hand plot, the probability of a secrecy outage in (4.46) is plotted versus R_s while in the right-hand plot, a CDF of the adversary's channel capacity C_{E} is shown to help interpret the data in the left-hand plot.

The following interpretations can be made about Fig. 4.17 and Fig. 4.18 in comparing the keys. 1) It can be seen from the right-hand plot that *Key 3* succeeds the most in terms of keeping information from Eve (i.e., keeping C_{E} smallest). However, the decorrelation between Alice and Bob's keys for *Key 3* limits the maximum target rate than can be used. Hence, the reduction in key similarity between Alice and Bob due to phase shuffling results in *Key 3* harming the secure information transmission system more than helping it. 2)

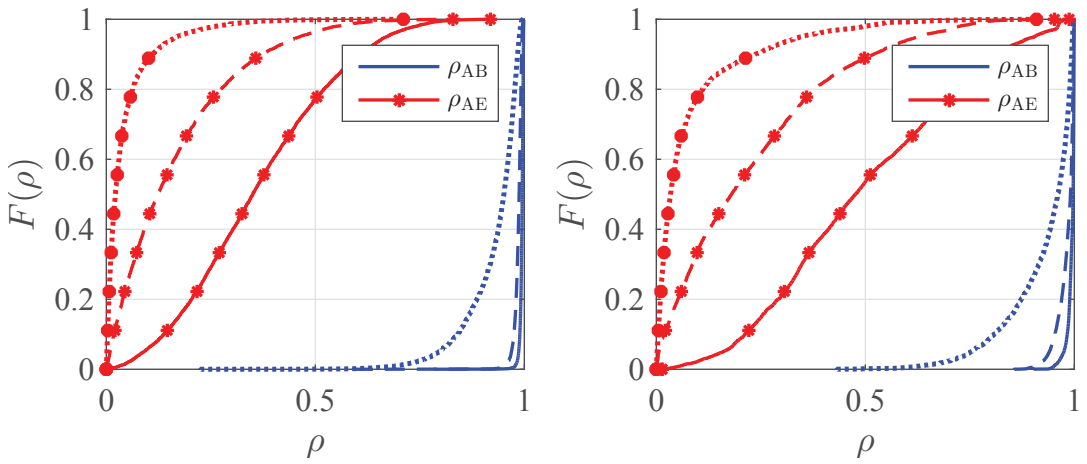

Figure 4.16. CDF of partial correlation between Alice and Bob's keys ρ_{AB} and Alice and Eve's keys ρ_{AE}. The plot on the left side shows simulation results while the right-hand side shows experimentation results. Note that these plots add the partial correlations of *key 3*, but otherwise are the exact same as Fig. 3.6 and Fig. 3.8 for the left and right side plots, respectively. In these plots, *key 1* is represented with solid lines, *key 2* with dashed lines, and *key 3* with dotted lines.

Although the largest target data rate R_T can be achieved with *Key 1* - due mostly to the fact that no additional processing is applied to this key - the downfall of this key is that Eve's keys are too similar to those shared between the main link. 3) *Key 2* provides the best balance between *Key 1* and *Key 3*. It can be seen that the probability of a secrecy outage is lowest for larger values of R_s when *Key 2* is used. Thus, the slight reduction in similarity due to removal of the strongest path is outweighed by the decorrelation that SPC adds to Eve's keys.

Interpretation of the experimental data from Fig. 4.18 is a bit more complicated. Here, the probability of secrecy outage overlaps at different points for the three keys. *Key 3* still exhibits the same problem observed in the simulation data - i.e., the largest rate that can be achieved by this key when a large amount of artificial noise is used is very limited. For the other keys, the probability of secrecy outage is higher for *Key 1* until $R_s \sim 3$, after which it is higher for *Key 2*. This period of transition is largely attributed to the fact that *Key 1* can support a higher R_T than *Key 2*. Although the probability of secrecy outage is smaller for large R_s with *Key 1*, the adversary's capacity C_E is significantly higher for *Key 1* than any other key. Additionally, the probability of secrecy outage with *Key 1* is $\sim 10\%$ at $R_s = 0$, suggesting that 10% of the generated keys will result in an information leak to

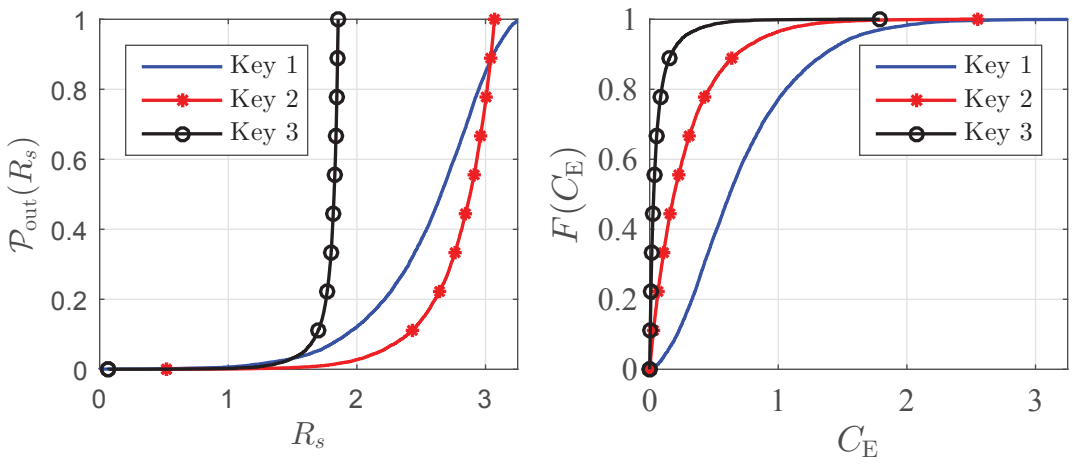

Figure 4.17. Plot of the probability of secrecy outage vs. R_s (Left) and a plot of the CDF of C_{E} (Right) using the simulated channel data.

Eve. Therefore, we can conclude that since *Key 1* allows for too great of a possibility of an information leak *and* since *Key 3* significantly hinders the communication of the main link, *Key 2* is the preferred key because it simultaneously allows for a relatively high target rate for the legitimate parties while ensuring a very low probability of information leaked to Eve's node.

4.5 Conclusion

This chapter completes the study of the proposed secure information transmission system discussed throughout this dissertation. A large part of this chapter was devoted to the concept of artificial noise and its use for spread spectrum communications. Two types of attacks were studied on the system and both considered a noiseless adversary. In the first attack, a passive eavesdropping adversary with the same receiver as the legitimate users was considered. It was shown that this adversary can be thwarted when Alice and Bob are not SNR constrained and thus, can use a large amount of artificial noise. For the second attack, we considered a more sophisticated Eve with significant blind detection capabilities. Here, it was found that when Eve studies the second-order moments of the transmitted signal, she cannot determine the information-bearing subspace when the golden signal-to-artificial noise ratio of $\phi = 1/N$ is used. Finally, in the last segment of this chapter, it was shown that keys derived using SPC gave the best performance results in context of the proposed secure information design.

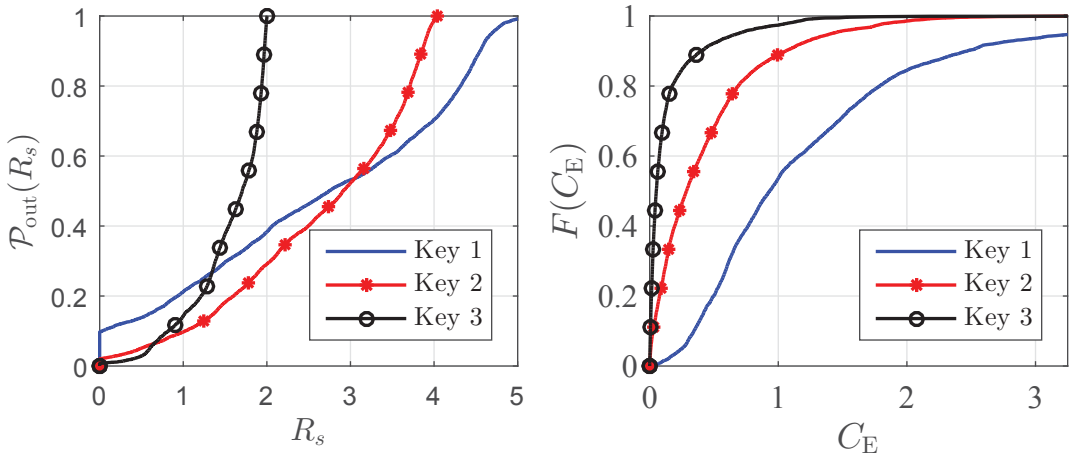

Figure 4.18. Plot of the probability of secrecy outage vs. R_s (Left) and a plot of the CDF of C_{E} (Right) using over the air measurement data.

CHAPTER 5

CONCLUSION AND FUTURE WORK

5.1 Conclusion

In this dissertation, we proposed and studied a secret-key enabled secure information transmission system for spread spectrum communication. We presented a method through which two asynchronous radios can exchange a set of spreading codes through the use of the reciprocal wireless channel. The key itself is shown to have been made stronger through the use of a method that we named SPC (Strongest Path Cancellation). We validated our approach through both simulation and experimentation and showed that the use of SPC greatly aids our proposed secure information transmission solution.

The secure information transmission system proposed in this dissertation introduced the concept of artificial noise to multicarrier spread spectrum systems as a means of enhancing the physical-layer security in wide band communications. The solution was tested against both a passive eavesdropper who follows the same procedure of Alice and Bob as well as a more sophisticated adversary who seeks to blindly detect the key transmitted by Alice. In the first situation, it was shown that despite SPC introducing a slight decorrelation between keys of Alice and Bob, the probability of a secrecy outage remains in favor of the key generated using SPC. For the more sophisticated adversary, we made the following observation. When Alice and Bob have enough SNR to take advantage of, by adding sufficient artificial noise, they will be able to communicate many information symbols securely.

5.2 Future Work

In this dissertation, we have proposed a practical technique for secure information transmission using the reciprocal wireless channel. In fact, the secure information transmission step should only require a slight modification at the physical-layer transmitter to add artificial noise. Although the channel probing protocol has been successfully imple-

mented, the validation of the secure information transmission setup on an MC-SS platform is something to be considered for future research. Moreover, with our developed FB-MC-SS technique, the receiver needs to properly detect a packet, equalize the channel, correct timing and frequency offsets, etc. Therefore, something that needs to be examined in the future is how the addition of artificial noise interacts with deficiencies associated with the physical-layer. An interesting demo resulting from this future development could show how an eavesdropper - even with a significant SNR advantage - cannot decode the confidential information of Alice.

One assumption that we make in the adversary model in Section 1.4 is the assumption of a clean channel so that channel reciprocity can be maintained. This assumption is common for most, if not all, literature on physical-layer security solutions which make use of reciprocity of the wireless channel. The assumption of a clean channel, however, contradicts with the environment in which spread spectrum technology is typically associated with - e.g., a harsh interference and noise environment. Therefore, a possible area for future research would be in the development of a dynamic spectrum access technology which could allow for two nodes to agree on a common clean channel with which to generate a key from. Such a technology would not be too dissimilar from the one discussed by Wasden et al. in [29, 34]. Furthermore, it goes without saying that such a system would be beneficial to those in the field of physical-layer security since interference and active adversaries are often assumed to be turned off. Along with this idea, the ability to estimate the channel at variable bandwidths could also be useful. The idea here is that the bandwidth of the channel estimate could depend on the level of use and interference within the band.

In physical-layer security, the wireless channel must be probed using a given transmit sequence. In the field of *physical-layer key generation* and *secure information transmission*, many works, including the famous [21, 83], transmit a set of tones across different frequencies as a method to probe the channel. In these cases, masquerading attacks can occur if Alice transmits a tone to Bob and Eve transmits the same sequence back to Alice. Since the tones don't have a *signature* through which Alice can properly associate with a legitimate user, masquerading attacks can easily occur and are a weakness of these systems. To solve this problem, we have noted that the Zadoff-Chu sequence allows for a

unique signature to be attached to the transmit sequence. The concept here is that Alice can identify Bob's channel probe using fairly simple signal processing techniques with the aid of the signature. This is an area which has largely remained outside the scope of this dissertation as is true for other works within the literature, but is recommended for further development.

Regarding the secure information transmission system in Chapter 4, we note the following points about the sophisticated eavesdropper attack examined in Section 4.3. First, we recognize that BPSK is a non-ideal encoding scheme to use since the information signal subspace is strictly ± 1 when using BPSK. Second, the blind detection algorithm used in this scenario may be optimal for situations where $\phi > 1/N$ due to the Rayleigh-Ritz theorem (4.40). However, when $\phi = 1/N$, there may exist a better blind detection method. Future research should take these two considerations into account. Obtaining analytic expressions to determine the exact amount of symbols which can be sent across the channel in an information-theoretic manner would be the first step of this research. Another step that should follow this research would be to characterize the use of a significant amount of artificial noise (i.e., when $\phi = 1/N$) as a way to mask the randomness (or lack thereof) of the key.

Finally, we recommend a comparative study on the use of artificial noise in different types of SS systems. In particular, the study would consider how artificial noise would impact the the standard transceivers of DS-SS and MC-SS systems. When CSI information is imperfect, how does each SS system react to differences in spreading codes with artificial noise? Another important matter which should be investigated in this line of research is whether the use of a single-tap equalizer in MC-SS gives a competitive advantage over DS-SS.

APPENDIX A

DERIVATION OF SNR AFTER DESPREADING

The SNR after despreading with artificial noise is derived in this section. To start, recall that Bob's received signal after despreading is

$$\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\mathbf{y}_k = \boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}s + \boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\mathbf{v} + \boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\boldsymbol{\eta}\,. \tag{A.1}$$

The SNR after despreading is taken to be

$$\mathrm{SNR}_{\mathrm{B}}^{\mathrm{o}} = \frac{\mathrm{Var}[\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}s]}{\mathrm{Var}[\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\mathbf{v} + \boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\boldsymbol{\eta}]} \tag{A.2}$$

The numerator is evaluated as

$$\begin{aligned}\mathrm{Var}[\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{B}}s_k] &= \mathrm{E}\left[|\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{B}}s|^2\right] \\ &= |\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}|^2\sigma_s^2\end{aligned} \tag{A.3}$$

For the denominator, we know that the noise and artificial noise are uncorrelated and consequently, the variance of the two terms can be separated. Next, using the expression of artificial noise in (4.9),

$$\begin{aligned}\mathrm{Var}[\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\mathbf{v}] &= \mathrm{E}\left[|\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\mathbf{v}|^2\right] \\ &= \mathrm{E}\left[(\mathbf{w} - \boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}}\mathbf{w})^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{B}}\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}(\mathbf{w}_k - \boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}}\mathbf{w})\right]\end{aligned} \tag{A.4}$$

The four terms in (A.4) can be evaluated as

$$\mathrm{E}\left[\mathbf{w}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{B}}\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\mathbf{w}\right] = \sigma_w^2 \tag{A.5}$$

$$\begin{aligned} -\mathrm{E}\left[\mathbf{w}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{B}}\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}}\mathbf{w}\right] &= -\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}\,\mathrm{E}\left[\mathbf{w}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{B}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}}\mathbf{w}\right] \\ &= -\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{B}}\sigma_w^2 \\ &= -|\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}|^2\sigma_w^2 \end{aligned} \tag{A.6}$$

$$\begin{aligned} -\mathrm{E}\left[\mathbf{w}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{B}}\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\mathbf{w}\right] &= -\mathrm{E}\left[(\mathbf{w}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{B}}\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}}\mathbf{w})^{\mathrm{H}}\right] \\ &= -|\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}|^2\sigma_w^2 \end{aligned} \tag{A.7}$$

$$\begin{aligned} \mathrm{E}\left[\mathbf{w}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{B}}\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}}\mathbf{w}\right] &= \boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{B}}\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}\,\mathrm{E}\left[\mathbf{w}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}}\mathbf{w}\right] \\ &= |\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}|^2\sigma_w^2\,. \end{aligned} \tag{A.8}$$

Combining (A.5), (A.6), (A.7), and (A.8), we get

$$\mathrm{Var}[\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\mathbf{v}] = \sigma_w^2(1 - |\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}|^2) \tag{A.9}$$

and it can be shown that since the noise and $\boldsymbol{\gamma}_{\mathrm{B}}$ are uncorrelated,

$$\mathrm{Var}(\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\boldsymbol{\eta}) = \frac{\sigma_\eta^2}{N} \tag{A.10}$$

where σ_η^2 is the total noise power across the occupied bandwidth. Finally, by combining (A.3), (A.9), and (A.10), and recalling that

$$\rho_{\mathrm{AB}} = |\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}|^2 \tag{A.11}$$

$$\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} = \frac{P}{\sigma_\eta^2} \tag{A.12}$$

we get the expression

$$\begin{aligned} \mathrm{SNR}_{\mathrm{B}}^{\mathrm{o}} &= \frac{|\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}|^2\sigma_s^2}{(1 - |\boldsymbol{\gamma}_{\mathrm{B}}^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}|^2)\sigma_w^2 + \frac{\sigma_\eta^2}{N}} \\ &= \frac{N\phi\rho_{\mathrm{AB}}\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}}{\frac{N}{N-1}(1-\phi)(1-\rho_{\mathrm{AB}})\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} + 1}\,. \end{aligned} \tag{A.13}$$

APPENDIX B

DERIVATION OF PROBABILITY THAT THE SNR AFTER DESPREADING MEETS TARGET SNR

In this section, it is shown that if Alice follows the artificial noise power allocation strategy discussed in Section 4.2.1, the probability that the target SNR $\mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}$ is met so long as the similarity between Alice and Bob's keys are above a threshold $\rho_{\min}$. Note that this section also serves as a verification of the result in (4.22).

We start from the final result from (4.24) and solve in reverse order i.e.,

$$\mathcal{P}(\rho_{\mathrm{AB}} > \rho_{\min}) = \mathcal{P}(\mathrm{SNR}_{\mathrm{B}}^{\mathrm{o}} > \mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}) \tag{B.1}$$

$$= \mathcal{P}\left(N\phi\rho_{\mathrm{AB}}\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}\frac{N}{N-1}(1-\phi)(1-\rho_{\mathrm{AB}})\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} + 1 > \mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}\right) \tag{B.2}$$

$$= \mathcal{P}\left(N\phi\rho_{\mathrm{AB}}\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} > \mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}\big([\frac{N}{N-1}(1-\phi)(1-\rho_{\mathrm{AB}})\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} + 1)\right) \tag{B.3}$$

Next, the parameter ϕ and $(1-\phi)$ can be written as

$$\phi = \frac{\frac{N}{N-1}(1-\rho_{\min})\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} + 1}{\frac{N}{N-1}(1-\rho_{\min})\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} + N\rho_{\min}\frac{\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}}{\mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}}} \tag{B.4}$$

and

$$1-\phi = \frac{N\rho_{\min}\frac{\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}}{\mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}} - 1}{\frac{N}{N-1}(1-\rho_{\min})\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} + N\rho_{\min}\frac{\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}}}{\mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}}} \tag{B.5}$$

Substitution of (B.4) and (B.5) into (B.3) gives

$$\mathcal{P}\Bigg(\frac{N(1-\rho_{\min})\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} + (N-1)\rho_{\mathrm{AB}}}{N-1} + > \dots \tag{B.6}$$

$$\frac{(1-\rho_{\mathrm{AB}})(N\rho_{\min}\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} - \mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}) + \mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}(1-\rho_{\min}) + (N-1)\rho_{\min}}{N-1} + \Bigg). \tag{B.7}$$

Next, all terms involving ρ_{AB} and $\rho_{\min}$ are put on opposite sides so that

$$\mathcal{P}\left(\rho_{\mathrm{AB}}\left(\frac{(N-1) + N\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} - \mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}}{N-1}\right) > \rho_{\min}\left(\frac{(N-1) + N\mathrm{SNR}_{\mathrm{B}}^{\mathrm{i}} - \mathrm{SNR}_{\mathrm{T}}^{\mathrm{o}}}{N-1}\right)\right) \tag{B.8}$$

which can be simplified to give the final result.

$$\mathcal{P}(\rho_{AB} > \rho_{min}) = \mathcal{P}(SNR_B^o > SNR_T^o)\,. \tag{B.9}$$

APPENDIX C

DERIVATION OF COVARIANCE MATRIX OF TRANSMIT SEQUENCE

The covariance matrix of the transmit signal $\mathbf{x}_k$ is evaluated in this section. We start by using the definition of the transmit signal equation from (4.8) to obtain

$$\mathrm{E}[\mathbf{x}_k\mathbf{x}_k^{\mathrm{H}}] = \mathrm{E}[(\boldsymbol{\gamma}_{\mathrm{A}}s_k + \mathbf{v}_k)(\boldsymbol{\gamma}_{\mathrm{A}}s_k + \mathbf{v}_k)^{\mathrm{H}}] \tag{C.1}$$

The terms in (C.1) can be evaluated as follows

$$\mathrm{E}[\boldsymbol{\gamma}_{\mathrm{A}}s_k s_k^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}}] = \sigma_s^2\boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}} \tag{C.2}$$

$$\mathrm{E}[\boldsymbol{\gamma}_{\mathrm{A}}s_k\mathbf{v}_k^{\mathrm{H}}] = \mathrm{E}[\mathbf{v}_k s_k^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}}] = 0 \tag{C.3}$$

$$\mathrm{E}[\mathbf{v}_k\mathbf{v}_k^{\mathrm{H}}] = \mathrm{E}[(\mathbf{w}_k - \boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}}\mathbf{w}_k)(\mathbf{w}_k - \boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}}\mathbf{w}_k)^{\mathrm{H}}] \tag{C.4}$$

where (C.3) follows from the assumption that artificial noise is uncorrelated to the information symbols s_k. There are four terms in (C.4) and they can be evaluated as follows

$$\mathrm{E}[\mathbf{w}_k\mathbf{w}_k^{\mathrm{H}}] = \sigma_w^2\mathbf{I}_{\mathrm{N}} \tag{C.5}$$

$$\mathrm{E}[-\mathbf{w}_k\mathbf{w}_k^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}}] = -\sigma_w^2\boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}} \tag{C.6}$$

$$\mathrm{E}[-\boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}}\mathbf{w}_k\mathbf{w}_k^{\mathrm{H}}] = -\sigma_w^2\boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}} \tag{C.7}$$

$$\mathrm{E}[-\boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}}\mathbf{w}_k\mathbf{w}_k^{\mathrm{H}}\boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}}] = \boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}}\sigma_w^2\boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}} \tag{C.8}$$

$$= \sigma_w^2\boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}} \tag{C.9}$$

where in writing (C.5), we have recalled the definition of σ_w^2 from (4.11). Also, the simplification in C.8 comes from the fact that the key is normalized to unit length, i.e., $\|\boldsymbol{\gamma}_{\mathrm{A}}\| = 1$.

The results in (C.5), (C.6), (C.7), and (C.9) can be merged together to obtain

$$\mathrm{E}[\mathbf{v}_k\mathbf{v}_k^{\mathrm{H}}] = \frac{1}{N}\sigma_w^2\mathbf{I}_{\mathrm{N}} - \frac{1}{N}\sigma_w^2\boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}} \tag{C.10}$$

Combining the results in (C.2), (C.3), and (C.10) leads to

$$\mathrm{E}[\mathbf{x}_k\mathbf{x}_k^{\mathrm{H}}] = \frac{1}{N}\sigma_w^2\mathbf{I}_{\mathrm{N}} + \frac{1}{N}(\sigma_s^2 - \sigma_w^2)\boldsymbol{\gamma}_{\mathrm{A}}\boldsymbol{\gamma}_{\mathrm{A}}^{\mathrm{H}} \tag{C.11}$$

REFERENCES

[1] M. Bloch and J. Barros, *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

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

[3] R. Liu and W. Trappe, *Securing wireless communications at the physical layer*. Springer, 2010, vol. 7.

[4] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[5] H. Imai, *Wireless communications security*. Artech House, Inc., 2005.

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

[7] 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.

[8] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[9] Y. E. H. Shehadeh and D. Hogrefe, "A survey on secret key generation mechanisms on the physical layer in wireless networks," *Security and Communication Networks*, vol. 8, no. 2, pp. 332–341, 2015.

[10] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Communications*, vol. 18, no. 4, pp. 6–12, 2011.

[11] G. D. Durgin, *Space-time wireless channels*. Prentice Hall Professional, 2003.

[12] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[13] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[14] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[15] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Information Theory*, Jul. 2006, pp. 356–360.

[16] X. Zhou, M. R. McKay, B. Maham, and A. Hjorungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Communications Letters*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[17] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the gaussian MIMO wiretap channel," in *2007 IEEE International Symposium on Information Theory*. IEEE, 2007, pp. 2471–2475.

[18] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

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

[20] Z. Li, R. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in *2007 IEEE International Symposium on Information Theory*. IEEE, 2007, pp. 1296–1300.

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

[22] A. O. Hero III, "Secure space-time communication," *IEEE Transactions on Information Theory*, vol. 49, no. 12, pp. 3235–3249, 2003.

[23] G. R. Tsouri and D. Wulich, "Reverse piloting protocol for securing time varying wireless channels," in *Wireless Telecommunications Symposium, 2008. WTS 2008*. IEEE, 2008, pp. 125–131.

[24] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference*, vol. 62, no. 3. IEEE; 1999, 2005, p. 1906.

[25] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

[26] T. S. Rappaport *et al.*, *Wireless communications: principles and practice*. Prentice Hall PTR New Jersey, 1996, vol. 2.

[27] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.

[28] M. Pätzold, *Mobile radio channels*. John Wiley & Sons, 2011.

[29] D. L. Wasden, "Filter bank multicarrier spread spectrum communications," Ph.D. dissertation, The University of Utah, 2014.

[30] K. Fazel and S. Kaiser, *Multi-Carrier and Spread Spectrum Systems: From OFDM and MC-CDMA to LTE and WiMAX: Second Edition*. Wiley, 2008.

[31] S. Hara and R. Prasad, "Overview of multicarrier CDMA," *IEEE Communications Magazine*, vol. 35, no. 12, pp. 126–133, 1997.

[32] K. Cheun, K. Choi, H. Lim, and K. Lee, "Antijamming performance of a multicarrier direct-sequence spread-spectrum system," *IEEE Transactions on Communications*, vol. 47, no. 12, pp. 1781–1784, 1999.

[33] G. K. Kaleh, "Frequency-diversity spread-spectrum communication system to counter bandlimited gaussian interference," *IEEE Transactions on Communications*, vol. 44, no. 7, pp. 886–893, 1996.

[34] D. L. Wasden, H. Moradi, and B. Farhang-Boroujeny, "Design and implementation of an underlay control channel for cognitive radios," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 10, pp. 1875–1889, 2012.

[35] T. Haddadin, S. A. Laraway, A. Majid, T. Sibbett, D. L. Wasden, B. F. Lo, L. Landon, D. Couch, H. Moradi, and B. Farhang-Boroujeny, "An underlay communication channel for 5G cognitive mesh networks: Packet design, implementation, analysis, and experimental results," in *2016 IEEE International Conference on Communications Workshops*, May 2016, pp. 498–504.

[36] D. L. Wasden, H. Moradi, and B. Farhang-Boroujeny, "Comparison of direct sequence spread spectrum rake receiver with a maximum ratio combining multicarrier spread spectrum receiver," in *2014 IEEE International Conference on Communications*. IEEE, 2014, pp. 4656–4661.

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

[38] T. Kang, X. Li, C. Yu, and J. Kim, "A survey of security mechanisms with direct sequence spread spectrum signals," *Journal of Computing Science and Engineering*, vol. 7, no. 3, pp. 187–197, 2013.

[39] M. A. Abu-Rgheff, *Introduction to CDMA wireless communications*. Academic Press, 2007.

[40] T. Li, Q. Ling, and J. Ren, "Physical layer built-in security analysis and enhancement algorithms for CDMA systems," *EURASIP Journal on Wireless Communications and Networking*, vol. 2007, no. 3, p. 7, 2007.

[41] D. L. Wasden, J. A. Loera, A. J. Majid, H. Moradi, and B. Farhang-Boroujeny, "Design and implementation of an underlay control channel for cognitive radios," in *2012 IEEE International Symposium on Dynamic Spectrum Access Networks*, Oct 2012, pp. 280–281.

[42] A. Majid, H. Moradi, and B. Farhang-Boroujeny, "Secure information transmittion for filter bank multi-carrier spread spectrum systems," in *2015 IEEE Military Communications Conference*, 2015.

[43] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 11, pp. 3776–3784, 2005.

[44] R. Mehmood and J. W. Wallace, "Wireless security enhancement using parasitic reconfigurable aperture antennas," in *Proc. 5th European Conf. Antennas and Propagation*, Apr. 2011, pp. 2761–2765.

[45] J. Zhang, S. K. Kasera, and N. Patwari, "Mobility assisted secret key generation using wireless link signatures," in *2010 Proceedings IEEE INFOCOM*. IEEE, 2010, pp. 1–5.

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

[47] S. N. Premnath, S. K. Kasera, and N. Patwari, "Secret key extraction in MIMO-like sensor networks using wireless signal strength," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 14, no. 1, pp. 7–9, 2010.

[48] S. N. Premnath, J. Croft, N. Patwari, and S. K. Kasera, "Efficient high-rate secret key extraction in wireless sensor networks using collaboration," *ACM Transactions on Sensor Networks*, vol. 11, no. 1, p. 2, 2014.

[49] 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," *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 917–930, May 2013.

[50] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 364–375, 2007.

[51] C. Ye, A. Reznik, G. Sternburg, and Y. Shah, "On the secrecy capabilities of ITU channels," in *2007 IEEE 66th Vehicular Technology Conference*. IEEE, 2007, pp. 2030–2034.

[52] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1484–1497, 2012.

[53] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*. ACM, 2008, pp. 128–139.

[54] S. N. Premnath, P. L. Gowda, S. K. Kasera, N. Patwari, and R. Ricci, "Secret key extraction using Bluetooth wireless signal strength measurements," in *2014 Eleventh Annual IEEE International Conference on Sensing, Communication, and Networking*, Jun. 2014, pp. 293–301.

[55] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17–30, 2010.

[56] J. Croft, N. Patwari, and S. K. Kasera, "Robust uncorrelated bit extraction methodologies for wireless sensors," in *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks*. ACM, 2010, pp. 70–81.

[57] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation," in *2011 Proceedings IEEE INFOCOM*. IEEE, 2011, pp. 2165–2173.

[58] M. G. Madiseh, S. W. Neville, and M. L. McGuire, "Time correlation analysis of secret key generation via UWB channels," in *2010 IEEE Global Telecommunications Conference*. IEEE, 2010, pp. 1–6.

[59] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Secure key generation from OFDM subcarriers' channel responses," in *2014 IEEE Globecom Workshops*, 2014, pp. 1302–1307.

[60] S. T. B. Hamida, J.-B. Pierrot, and C. Castelluccia, "An adaptive quantization algorithm for secret key generation using radio channel measurements." in *NTMS*, 2009, pp. 1–5.

[61] S. T.-B. Hamida, J.-B. Pierrot, and C. Castelluccia, "Empirical analysis of UWB channel characteristics for secret key generation in indoor environments," in *2010 IEEE 21st International Symposium on Personal Indoor and Mobile Radio Communications*. IEEE, 2010, pp. 1984–1989.

[62] M. Zafer, D. Agrawal, and M. Srivatsa, "Limitations of generating a secret key using wireless fading under active adversary," *IEEE/ACM Transactions on Networking (TON)*, vol. 20, no. 5, pp. 1440–1451, 2012.

[63] R. Frank, S. Zadoff, and R. Heimiller, "Phase shift pulse codes with good periodic correlation properties (corresp.)," *IRE Transactions on Information Theory*, vol. 6, no. 8, pp. 381–382, 1962.

[64] D. Chu, "Polyphase codes with good periodic correlation properties (corresp.)," *IEEE Transactions on Information Theory*, pp. 531–532, 1972.

[65] S. Sesia, I. Toufik, and M. Baker, *LTE: the UMTS long term evolution*. Wiley Online Library, 2009.

[66] B. Farhang-Boroujeny, *Signal processing techniques for software radios*. Lulu publishing house, 2008.

[67] B. O'hara and A. Petrick, *IEEE 802.11 handbook: a designer's companion*. IEEE Standards Association, 2005.

[68] Y. El Hajj Shehadeh, O. Alfandi, and D. Hogrefe, "Towards robust key extraction from multipath wireless channels," *Journal of Communications and Networks*, vol. 14, no. 4, pp. 385–395, 2012.

[69] M. G. Madiseh, S. He, M. L. McGuire, S. W. Neville, and X. Dong, "Verification of secret key generation from UWB channel observations," in *2009 IEEE International Conference on Communications*. IEEE, 2009, pp. 1–5.

[70] J. Huang and T. Jiang, "Secret key generation exploiting ultra-wideband indoor wireless channel characteristics," *Security and Communication Networks*, vol. 8, no. 13, pp. 2329–2337, 2015.

[71] A. Sayeed and A. Perrig, "Secure wireless communications: secret keys through multipath," in *2008 IEEE International Conference on Acoustics, Speech and Signal Processing*. IEEE, 2008, pp. 3013–3016.

[72] M. Wilhelm, I. Martinovic, and J. B. Schmitt, "Secure key generation in sensor networks based on frequency-selective channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1779–1790, 2013.

[73] M. G. Madiseh, M. L. McGuire, S. W. Neville, and A. A. B. Shirazi, "Secret key extraction in ultra wideband channels for unsynchronized radios," in *2008 6th Annual Communication Networks and Services Research Conference*. IEEE, 2008, pp. 88–95.

[74] J. E. D. Croft, "Shared secret key establishment using wireless channel measurements," Ph.D. dissertation, The University of Utah, 2011.

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

[76] W. C. Liao, T. H. Chang, W. K. Ma, and C. Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[77] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *2009 IEEE International Conference on Acoustics, Speech and Signal Processing*. IEEE, 2009, pp. 2437–2440.

[78] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*. ACM, 2008, pp. 116–127.

[79] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, 1993, pp. 410–423.

[80] F. Zhang, *Matrix theory: basic results and techniques*. Springer Science & Business Media, 2011.

[81] U. M. Maurer and S. Wolf, "Unconditionally secure key agreement and the intrinsic conditional information," *IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 499–514, 1999.

[82] B. Farhang-Boroujeny, *Adaptive filters: theory and applications*. John Wiley & Sons, 2013.

[83] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Transactions on Communications*, vol. 43, no. 1, pp. 3–6, 1995.