Impact of Antenna Mutual Coupling, Propagation, and Nonreciprocity on Propagation-Based Key Establishment

Attiya Mahmood
Brigham Young University
Impact of Antenna Mutual Coupling, Propagation, and Nonreciprocity on Propagation-Based Key Establishment

Attiya Mahmood

A dissertation submitted to the faculty of Brigham Young University in partial fulfillment of the requirements for the degree of Doctor of Philosophy

Michael A. Jensen, Chair
Michael Rice
Karl F. Warnick
David Long
Brian D. Jeffs

Department of Electrical and Computer Engineering
Brigham Young University

Copyright © 2018 Attiya Mahmood
All Rights Reserved
ABSTRACT

Impact of Antenna Mutual Coupling, Propagation, and Nonreciprocity on Propagation-Based Key Establishment

Attiya Mahmood
Department of Electrical and Computer Engineering, BYU
Doctor of Philosophy

Propagation-based key establishment is a physical layer method for generating encryption keys based on two radios observing a reciprocal propagation channel. This work explores the impact of mutual coupling when communicating nodes are equipped with multiple antennas, multipath richness in the propagation environment, and practical limitations caused by the nonreciprocal nature of RF circuits on key establishment.

First, network theory is used to formulate a model of a realistic communication system which incorporates transmit sources and receive loads, impedance matching networks, low-noise amplifiers (LNAs), mutually coupled antenna arrays, and a passive eavesdropper. Afterwards, a detailed analysis is performed to quantify the impact of coupling, type of impedance matching network, and proximity of a multi-antenna eavesdropper on key rate metrics. Next, the degradation on key establishment caused by the radiocircuitry non-reciprocal contributions to the propagation channel is analyzed. A calibration technique based on total least square algorithm is used to overcome the non-reciprocity. Results demonstrate that the method is highly effective in removing the impact of non-reciprocal circuit contributions over a range of operational parameters.

Lastly, for key establishment, the propagation conditions can cause the available key rate to be significantly different from the secure key rate which takes into account the presence of a passive eavesdropper. To study this in detail, a realistic multiple-input multiple-output (MIMO) propagation environment is modeled for two communicating radios and an eavesdropper. Afterwards different propagation conditions are assumed and results demonstrate that secure key rate converges to available key rate when $K$-factor is small and the eavesdropper is not located very close ($< 2.5\lambda$) to one of the nodes.

Keywords: Physical layer security, Mutual Coupling, Calibration, Spatial correlation
ACKNOWLEDGMENTS

I would like to offer utmost gratitude to my PhD advisor Dr. Michael A. Jensen for his intellectual support, time, guidance, expertise, kindness, and most of all, for his patience throughout the research work. Furthermore, I will like to thank my PhD committee members: Dr. Karl F. Warnick, Dr. Brian D. Jeffs, Dr. Michael Rice, and Dr. David Long for their time and support.

I owe a special thanks to my parents and siblings who supported and encouraged me throughout my life. I would like to give a special mention to my mother, who provided me with every opportunity to be where I am today. May God bless my mother and father souls. I dedicate this PhD. thesis to my two adorable children, Hamza and Hassan, who are the pride and joy of my life. Last but not the least I would like to thank my Husband, Dr. Rashid, whose continuous support has made me able to stand in this position.
# Table of Contents

List of Tables ......................................................... vi

List of Figures ........................................................ vii

Chapter 1 Introduction ................................................ 1
  1.1 New Contributions ................................................. 3
  1.2 Organization of the Dissertation ................................. 4

Chapter 2 Background .................................................. 5
  2.1 Traditional Cryptography ......................................... 5
    2.1.1 Symmetric-Key Cryptography ............................... 6
    2.1.2 Asymmetric-Key Cryptography ............................. 7
  2.2 Physical Layer Key Generation .................................. 7
    2.2.1 Key Rate Metrics ......................................... 8
  2.3 Propagation Channel Modeling .................................. 14
  2.4 System Calibration ................................................ 16

Chapter 3 Impact of Array Mutual Coupling on Multi-Antenna Propagation-Based Key Establishment .................................................. 19
  3.1 System Model and Analysis ..................................... 20
    3.1.1 Transmitter ............................................... 22
    3.1.2 Signal Received by Bob .................................. 22
    3.1.3 Bob’s Amplifier Noise ................................. 25
    3.1.4 Signal and Noise at Eve ................................ 27
    3.1.5 Signal and Noise at Alice ............................. 27
    3.1.6 Matching Network Specification ......................... 27
  3.2 Performance Evaluation ......................................... 29
    3.2.1 Channel Estimation ..................................... 30
    3.2.2 Channel Covariance ................................... 30
    3.2.3 Error Covariance ....................................... 31
  3.3 Results .......................................................... 32
    3.3.1 Propagation Channel Covariance ......................... 33
    3.3.2 Matching Network Objectives ............................ 35
    3.3.3 Available Key Rate .................................... 35
    3.3.4 Secure Key Rate ......................................... 38
  3.4 Chapter Summary ................................................ 46
List of Tables

5.1 Coefficients for estimating the power spectral density for each cluster parameter. 75
## List of Figures

2.1 Symmetric-key cryptography where Alice and Bob are the two communicating nodes and Eve is a potential Eavesdropper ........................................ 6  
2.2 Diffie-Hellman key exchange algorithm where Alice and Bob are the two communicating nodes .......................................................... 7  
2.3 System model for secure communication, where Alice and Bob are the legitimate nodes and Eve is a passive eavesdropper .......................... 9  
2.4 Graphical representation of $I_K$, $I_{SK}$, and $I_{VK}$ .................................................. 12  
2.5 Available key rate as a function of number of paths ($L$), where both Bob and Alice are equipped with $N$-element arrays, SNR = 15 dB, and $d_B = d_A = 0.5\lambda$ . 13  
2.6 Available key rate as a function of the separation between Bob and Alice antenna arrays and SNR, where $d_B = d_A$, $N = 2$, and $L = 10$ ..................................................... 13  
2.7 Secure key rate as a function of the separation between Bob’s and Eve’s antenna and number of paths, where Bob’s and Eve’s antenna are parallel to each other, SNR=15 dB, and $N = 1$. ..................................................... 14  
2.8 Secure key rate as a function of the separation between Bob and Eve antenna arrays and number of paths, where Bob and Eve antenna arrays are parallel to each other, $d_B = d_A = d_{BE}$, SNR=15 dB, and $N = 2$. ..................................................... 15  
2.9 Network model of MIMO system consisting of mutually coupled transmitting and receiving antennas, matching networks, sources, digital signal processing module, and the propagation channel. ..................................................... 17  

3.1 Network model of a MIMO communication system with legitimate nodes Alice and Bob and a passive eavesdropper Eve. The elements of each array are mutually coupled, and further the elements of Bob’s and Eve’s arrays can be cross coupled. The boxed diagram in the upper left shows two-element arrays for Alice, Bob, and Eve along with the respective element spacings $d_A$, $d_B$, and $d_E$ and the distance $d_{BE}$ between Bob and Eve. ..................................................... 20  
3.2 Simplified network model highlighting the reciprocal channel $T_{BA}$, when Alice and Bob acts as transmit and receive nodes, respectively. ..................................................... 25  
3.3 Representative clustered PAS showing four clusters satisfying a truncated Laplacian distribution. ..................................................... 34  
3.4 Available key rate as a function of Bob’s antenna element spacing ($d_B/\lambda$) for three different matching network conditions when the antenna element efficiency $\mu$ is assumed to be 100% ..................................................... 36  
3.5 Q factor as a function of Bob’s antenna element spacing ($d_B/\lambda$) for two different values of the antenna element efficiency $\mu$. ..................................................... 37
3.6 Available key rate as a function of Bob’s antenna element spacing \((d_B/\lambda)\) for three different matching network conditions when the antenna element efficiency \(\mu\) is assumed to be 90%.  
3.7 Available key rate for \(d_B = 0.12\lambda\) as a function of SNR when \(N_C = 4\).  
3.8 Available key rate for \(d_B = 0.12\lambda\) as a function of the number of clusters \(N_C\) when the SNR is 15 dB.  
3.9 Secure key rate as a function of the separation between Bob’s and Eve’s antenna arrays for three different matching network conditions when high coupling \((d_B = d_E = 0.12\lambda)\) is assumed.  
3.10 Secure key rate as a function of the separation between Bob’s and Eve’s antenna arrays for three different matching network conditions when low coupling \((d_B = d_E = 0.5\lambda)\) is assumed.  
3.11 Secure key rate for \(d_B = d_{BE} = 0.12\lambda\) (a) as a function of SNR when \(N_C = 4\).  
3.12 Secure key rate for \(d_B = d_E = d_{BE} = 0.12\lambda\) as a function of the number of clusters \(N_C\) when the SNR is 15 dB.  
3.13 Secure key rate as a function of the separation between Bob’s and Eve’s antenna arrays for two different matching network conditions with \(d_B = d_E = 0.12\lambda\) and all arrays are of equal size with Bob’s and Eve’s arrays parallel to each other.  
3.14 Secure key rate as a function of the separation between Bob’s and Eve’s antenna arrays for two different matching network conditions with \(d_B = d_E = 0.12\lambda\). Bob’s and Eve’s arrays are perpendicular with \(N_E = 2\) and parallel with \(N_E = 4\) when \(N_A = N_B = 2\).  
3.15 Secure key rate as a function of \(d_{BE}\) with and without cross coupling \(S_{BE}\) for optimal matching networks at Bob and Eve: (a) high coupling \((d_B = d_E = 0.12\lambda)\); (b) low coupling \((d_B = d_E = 0.5\lambda)\).  
3.16 (a) Ratio of \(I_K\) for \(S_{BE} \neq \mathbf{0}\) to \(I_K\) when \(S_{BE} = \mathbf{0}\). (b) Average ratio of the Frobenius norm of \(R_{xz}\) for \(S_{BE} \neq \mathbf{0}\) to that for \(S_{BE} = \mathbf{0}\). Both results use optimal matching networks at Bob and Eve.  

4.1 Network model of a MIMO communication system with legitimate nodes Alice and Bob and a passive eavesdropper Eve.  
4.2 Available key rate \(I_K\) as a function of the maximum phase error \(\phi_{\text{max}}\) for the Reference and Error scenarios when error is applied to the reverse (Rev) or both the forward and reverse (Fw, Rev) channels for both optimal (OMN) and diagonal (DMN) matching networks when \(\text{SNR}_{10\lambda} = 15\ \text{dB}\).  
4.3 Available key rate \(I_K\) for Case 1 as a function of Bob’s array spacing \(d_B\) when either \(\text{SNR}_{C}\) or \(\text{SNR}_{10\lambda}\) are fixed at 15 dB for both optimal (OMN) and diagonal (DMN) matching networks.  
4.4 Achieved average SNR\(_C\) as a function of Bob’s array spacing \(d_B\) for forward \((\hat{h}_x)\), reverse \((\hat{h}_r)\) and calibrated channel \((\hat{h}_c)\) covariance matrices when \(\text{SNR}_{10\lambda} = 15\ \text{dB}\) for both optimal (OMN) and diagonal (DMN) matching networks.  
4.5 (a) Maximum correlation coefficient within each channel and (b) average diagonal and off-diagonal cross correlation coefficient between forward and reverse channels \((\hat{h}_x, \hat{h}_r)\) and forward and calibrated channels \((\hat{h}_x, \hat{h}_c)\) as a function of Bob’s array spacing \(d_B\).
4.6 Secure key rate $I_{SK}$ as a function of the Bob-Eve array separation $d_{BE}$ ($d_B = 0.12\lambda$) for Case 1 for both optimal (OMN) and diagonal (DMN) matching networks. 63

4.7 Available key rate $I_K$ as a function of $d_B$ and secure key rate $I_{SK}$ as a function of $d_{BE}$ ($d_B = 0.12\lambda$) when calibration error is applied to the reverse channel (Case 1) and both forward and reverse channel (Case 2) for optimal matching networks. 64

4.8 Available key rate $I_K$ as a function of $d_B$ and secure key rate $I_{SK}$ as a function of $d_{BE}$ ($d_B = 0.12\lambda$) when calibration error is applied to the reverse channel (Case 1) and both forward and reverse channel (Case 2) for diagonal matching networks. 65

4.9 Available key rate $I_K$ as a function of $d_B$ and secure key rate $I_{SK}$ as a function of $d_{BE}$ ($d_B = 0.12\lambda$) when $K = 10$ or 50, where calibration error is added in both transmit and receive matching networks and $N_A = N_B = N_E = 3$. 66

4.10 Percentage fractional error in $I_K$ before and after calibration as a function of $SNR_C$ for several values of $K$, where $N_A = N_B = 3$ for two different values of Bob’s element spacing $d_B$. 66

4.11 Available key rate $I_K$ as a function of $d_B$ and secure key rate $I_{SK}$ as a function of $d_{BE}$ ($d_B = 0.12\lambda$) error is applied only to the receive matching network (Case 3) versus both transmit and receive matching networks (Case 2) for optimal matching networks. 67

4.12 Available key rate $I_K$ as a function of $d_B$ and secure key rate $I_{SK}$ as a function of $d_{BE}$ ($d_B = 0.12\lambda$) when error is applied only to the receive matching network (Case 3) versus both transmit and receive matching networks (Case 2) for diagonal matching networks. 68

5.1 System model in which Alice and Bob use multiple antennas to communicate in the presence of a multi-antenna passive eavesdropper Eve. 71

5.2 Power image showing evolution of clusters following truncated Laplacian distribution over time and space. a) Clusters at Bob and Eve when $d_{BE} = 0$ b) Clusters at Eve when $d_{BE} = 1.3\lambda$. 78

5.3 (a) Variation in the cluster central arrival angle ($\phi_R$, radians) as a function of Eve’s displacement from Bob computed from the AR multipath model with $L_B = 4$ clusters at Bob. (b) Expanded version of the arrival angle variation for one of the clusters. 79

5.4 CDFs for $I_K$ and $I_{SK}$ when $K = 0$ dB. The designations $(N_\xi, N_A)$ indicate that Bob and Eve have $N_\xi$ antennas each for $\xi \in [B, E]$ and Alice has $N_A$ antennas. 80

5.5 Relative number of vulnerable key bits as a function of Eve’s distance from Bob ($d_{BE}$) and different values of $K$ when $N_A = 4$, $N_B = N_E = 3$, and $AS = 26^\circ$. Dashed lines designate results for a simple propagation model in which Bob and Eve have an identical PAS. 81

5.6 Relative number of vulnerable key bits as a function of Eve’s distance from Bob ($d_{BE}$) for $N_A = 4$, $N_B = N_E = 3$, and $K = -20$ dB and two AS values. Dashed lines designate results for a simple propagation model in which Bob and Eve have an identical PAS. 82

5.7 Relative number of vulnerable key bits as a function of Eve’s distance from Bob ($d_{BE}$) when $AS = 26^\circ$ for different array sizes when $K = 0$ dB. 83
5.8 Relative number of vulnerable key bits as a function of Eve’s distance from Bob
\((d_{BE})\) when AS = 26° for different array sizes when \(K = -20\) dB.  
5.9 Relative number of vulnerable key bits as a function of Eve’s distance from Bob
\((d_{BE})\) and different values of \(K\) when \(N_A = 4, N_B = N_E = 3,\) and AS = 26°
when mutual coupling is included. Dashed lines designate results when mutual
coupling is neglected.
Chapter 1

Introduction

The rapid increase in the use of wireless devices has brought the importance of data security to the forefront. In particular, because wireless transmissions can be monitored by an eavesdropper, secure communications must use key-based data encryption [1]. While establishing a key to achieve perfect secrecy is difficult, practical key establishment techniques such as the Diffie-Hellman exchange [2, 3] are considered computationally secure because of the intensive computational burden required by an eavesdropper for key extraction. However, the emergence of sophisticated and efficient computational algorithms and architectures may increase the vulnerability of traditional cryptographic algorithms [4].

Fortunately, the physics of electromagnetic propagation offers a potential solution to vulnerabilities of existing key establishment techniques. Specifically, because electromagnetic propagation is reciprocal, two nodes that use bidirectional training transmissions to estimate the transfer functions between their antennas will theoretically observe the same results [5–16], and therefore each node can use its own observations to establish a common key. An eavesdropper listening to the training transmissions will observe a different transfer function, although spatial correlation between the channels observed by the legitimate nodes and the eavesdropper can reduce the number of key bits that can be securely generated [17]. If the channel varies in time, then the key can be updated at regular intervals, reducing the amount of time a key is used and dramatically improving the security [1].

Early work on propagation-based key establishment has provided a theoretical basis for the concept [5, 9, 18–21]. Subsequent work has provided practical methods for key generation in radio protocols [12, 22, 23], experimentally explored the achievable performance of real channels [17], studied the impact of spatial and temporal correlation in multi-antenna channels [24], and proposed methods for using low-complexity reconfigurable antennas to
artificially create time-varying channels [25, 26]. While significant work regarding both the theoretical potential and the practical implementation of physical layer key establishment has been done, most prior literature ignores the impact of antenna mutual coupling, radio circuits and realistic propagation modeling. First, antenna mutual coupling, both between elements within a communication antenna array as well as between elements of two different arrays, can change the degree of similarity between the channel observed by a legitimate node and that observed by a proximate eavesdropper. Second, because practical radios use different circuit paths for transmit and receive, incorporation of the circuits as part of the channel destroys the reciprocity and jeopardizes the viability of channel-based key establishment. Finally, the ultimate performance of channel-based key establishment depends on the electromagnetic propagation environment. Therefore, carefully analyzing the impact of the circuits and propagation conditions on the key establishment performance and devising methods to remove the impacts of the non-reciprocal contributors to the channel transfer function are critical to fully understand the potential of the technique.

While the latter issue of exploring the impact of propagation on key establishment is important, one challenge is efficient methods for determining the full spatial covariance matrix of the multiple-input multiple-output (MIMO) channel. The typical analytical approach for channel spatial covariance construction is to integrate the product of the radiation patterns of the antennas of interest and the power angular spectrum (PAS), which is the average propagating field power as a function of angle [27]. While most work applies this technique to the transmitter and receiver separately and then uses a Kronecker product of the resulting matrices to form the full channel covariance, more recent work overcomes this limitation by demonstrating direct computation of the covariance without resorting to the Kronecker product assumption [28]. Extending this work for multi-user MIMO systems helps us to analyze the security of key generation techniques under different propagation conditions.

This dissertation explores the impact of antenna mutual coupling, radio circuitry, and propagation conditions on physical layer key generation, including multi-user propagation modeling for key rate metric computation. The following details the new contributions of this work.
1.1 New Contributions

- While the impact of antenna mutual coupling on multiple-input multiple-output communication performance has been well documented [29], little work has appeared demonstrating how antenna coupling impacts the performance of multi-antenna radios that use reciprocal electromagnetic propagation to establish secret encryption keys. The work in this dissertation uses network theory to analyze the performance of such systems. The presentation includes an eavesdropper whose antennas may be very near and therefore coupled to the antennas of a legitimate node and further demonstrates the signal and noise model when the systems must remove the impact of non-reciprocal circuit elements through calibration. Representative results obtained with the model quantify the impact of coupling and of the type of impedance matching used to connect the antennas to the radio circuitry on the system key establishment performance.

- Prior studies have assumed that the wireless channel used for key generation is reciprocal. While the physical propagation channel between two nodes is generally reciprocal, the transmit/receive radio circuitry introduces non-reciprocal contributions to the overall channel. This dissertation analyzes the impact of channel non-reciprocity on physical layer key generation. A calibration phase based on the total least square (TLS) algorithm [30] is proposed to overcome the effect of non-reciprocal circuitry. Results demonstrate that a calibration phase before key generation can ensure that the effective physical channel between two nodes is reciprocal.

- Despite the advances in covariance modeling, most work focuses on covariance construction for point-to-point channels. However, in multi-user MIMO systems where nodes may be close enough physically to observe closely-related multipath structure, it is interesting to be able to easily transform the correlation in the multipath propagation observed at the two nodes to the correlation between the multi-user MIMO channels. This dissertation extends the approach of [28] to the multi-user case where there is correlation of the parameters representing a spatially-clustered PAS describing the average propagation from a single transmitter to two receivers. The technique is
applied to compute information theoretic bounds on performance for physical layer secret key establishment [5].

• In systems using the reciprocal propagation channel to generate encryption keys, the secure key rate quantifying the maximum number of bits that can be generated securely differs from the available key rate that ignores the presence of an eavesdropper. However, prior studies on this difference have largely ignored the impact of propagation conditions in the analysis [17]. This work formulates a model for computing the secure and available key rates for a multi-user scenario involving two legitimate nodes and a passive eavesdropper. Application of the model to a variety of different propagation conditions demonstrates that the secure and available key rates differ appreciably when the $K$-factor is large or when the separation between the eavesdropper and one of the legitimate nodes is small [31].

1.2 Organization of the Dissertation

To provide context for the ideas presented in this dissertation, Chapter 2 covers the background material on physical layer key generation, key rate metrics, and impact of an eavesdropper. Furthermore, related background work on propagation channel modeling and system calibration is presented. Chapter 3 analyzes the impact of radio circuitry on the performance of channel-based key establishment. Network theory is used to formulate a model that incorporates the transmit source and receive load impedances, impedance matching networks, and mutually-coupled antenna elements for multi-antenna as well as multi-user radios [29]. The model is used to analyze the key rate metrics by using a realistic noise model and various matching network conditions.

Chapter 4 investigates the impact of non-reciprocity on key generation and proposes a calibration phase to overcome the non-reciprocal aspects of the propagation channel. Chapter 5 formulates the computation of the multi-user spatial correlation in a MIMO communication environment. This model is used to explore the quantitative relationship between the available and secure key rates for different propagation conditions to investigate the conditions under which the secure key rate is approximately the same as the key rate.

Conclusions and a discussion of future work are given in Chapter 6.
Chapter 2

Background

This chapter presents an overview on traditional cryptography and highlights the importance of physical layer key generation. The key rate metrics and their computation are also discussed briefly. Furthermore, some relevant background work on propagation channel modeling and system calibration is presented.

2.1 Traditional Cryptography

The prevalence of wireless communication has produced an increase in the volume of sensitive information transmitted over radio channels, motivating efforts to find techniques for safeguarding transmissions against malicious attacks. Cryptographic algorithms are generally employed to ensure data security, and they can be divided into two broad categories. Algorithms in the first category are based on information-theoretic security that cannot be broken even with unlimited computing power and time. The one-time pad [32, 33] is an example of such an algorithm. However, these algorithms are very difficult to implement and have limited practical use. Algorithms in the second category are based on mathematical theory and computational hardness. It is theoretically possible to crack these algorithms, but the computational time and resources required are not realistically available. Commonly used examples include data encryption standard (DES) [34] and the Diffie-Hellman key exchange protocol [2, 3].

The computationally expensive algorithms can be further divided into symmetric and asymmetric key cryptography, both of which are discussed below.
2.1.1 Symmetric-Key Cryptography

In symmetric-key cryptography both communicating nodes use the same secret key. Figure 2.1 depicts this scenario where Alice and Bob are two communicating nodes and the message is encrypted and decrypted using a single key. However, that key can change at regular intervals. An eavesdropper (Eve) present in the environment can try to steal the key by observing the relationship between the input and output texts, but the probability of success decreases significantly with an increase in the key size. The Data Encryption Standard (DES) [34] and the Advanced Encryption Standard (AES) [35] are two popular algorithms that employ this scheme.

The biggest limitation of this scheme is the key distribution and management. Either the secure keys have to be distributed in advance among the nodes in the network that may communicate in the future or a secure third party server is required that will perform key distribution in real time. Furthermore, the complexity of key management increases with an increase in the number of nodes in the network. Finally, the keys are pseudo-random in
nature as compared to truly random, and therefore if the key generation process is hacked the security of the complete communication system can be vulnerable.

2.1.2 Asymmetric-Key Cryptography

In asymmetric-key cryptography the encryption is performed using a public key that is known to all nodes in the network. However, for decryption a node requires both the public as well as the private key, where the private key is local to that specific node. Although the public and private keys are related to each other, an eavesdropper cannot estimate the private key based on the public key. Examples of this scheme are the Diffie-Hellman key exchange protocol, diagrammed in Figure 2.2, and the RSA algorithm [36]. A drawback of these algorithms is the key length. Generally they require much longer key lengths than do symmetric key algorithms to ensure the same level of security.

The computational complexity of RSA and Diffie-Hellman key exchange algorithms is related to the integer factorization and discrete logarithm problems, respectively. Although no efficient algorithms exist to date to crack these algorithms, quantum computing or other technologies may allow breaking these schemes in the future.

2.2 Physical Layer Key Generation

While most communication security is accomplished at the upper layers of the protocol stack, there is an increased interest in the use of physical layer techniques to enhance
communication security. As an example, recent research has suggested that if two radios use bidirectional, half-duplex training transmissions to estimate the propagation channel transfer function, then by reciprocity these estimates will differ only due to measurement errors. These estimates can therefore be used as a random source for establishment of secret encryption keys [5, 7]. Not only does such a technique simplify key distribution and allow regular updates of the key, but also the propagation physics provide a source for the keys that is more random than typical pseudo-random number generators [1]. This technique is referred to physical layer key generation in this dissertation.

In the presence of a passive eavesdropper (Eve), the security of generated key bits depends on the correlation between the channels sampled by Eve and those observed by the communicating nodes. Statistically, the key generation process is considered to be very secure if Eve is located a few wavelengths away from both nodes. However, if Eve is very close to one of the communicating nodes, it can have a significant impact on the security of the generated key bits, which is the focus of this work.

Channel fading statistics can also have a significant impact on the key generation, where the key rate is maximized if the propagation channel statistics follow a Gaussian distribution [12]. However for line-of-sight (LOS) or slowly fading channels, randomness in the wireless environment is limited and security of generated key bits can be compromised. Techniques exist in which artificial perturbation in the propagation channel can be induced by using a reconfigurable RF front end or reconfigurable antennas [26]. However, in general for static propagation conditions it may be more advantageous to use channel based key generation as an added layer of security rather than relying on it as the only security mechanism.

2.2.1 Key Rate Metrics

Figure 2.3 shows a communication scenario in which Alice and Bob are two communicating nodes and Eve is a passive eavesdropper. The reciprocal propagation channels sampled by Bob and Alice are $h_x$ and $h_y$, respectively while Eve estimates $h_z$ and $h_g$. Note that $h_i$ can refer to the column wise stacked elements of a multiple-input multiple-output (MIMO) channel, a single channel observed at multiple frequencies, or both. Due to estima-
tion errors, each channel is corrupted by noise and the estimated channels can be expressed as $\hat{h}_i = h_i + \eta_i$, where $i \in \{x, y, z, g\}$ and $\eta_i$ represents estimation error at the designated node. In order to quantify key generation performance, the metrics available key rate and secure key rate are used.

### Available Key Rate

The available key rate $I_K$ (or key rate for short) is the number of key bits available per observation of the reciprocal channel between Alice and Bob, quantified as the mutual information between channels $\hat{h}_x$ and $\hat{h}_y$. If the statistics of the propagation channel are Gaussian, $I_K$ can be computed as [17]

$$I_K = I(\hat{h}_x; \hat{h}_y) = h(\hat{h}_x) + h(\hat{h}_y) - h(\hat{h}_x, \hat{h}_y) = \log_2(\pi e)^{N_A}|\hat{R}_{xx}| + \log_2(\pi e)^{N_B}|\hat{R}_{yy}| + \log_2(\pi e)^{N_AN_B}|\hat{R}_{XY}|$$

$$= \log_2 \frac{|\hat{R}_{xx}| |\hat{R}_{yy}|}{|\hat{R}_{XY}|}. \quad (2.1)$$

where $h(\cdot)$ is the entropy, $|\cdot|$ is the determinant, $I(\cdot; \cdot)$ is the mutual information, $\hat{R}_{\xi\xi'} = E\left\{\hat{h}_\xi \hat{h}_{\xi'}^\dagger\right\}$, and $E\left\{\cdot\right\}$ is an expectation. Furthermore, capital covariance subscripts are notation for

$$\hat{R}_{X_1X_2...X_N} = E\left\{\hat{h}_{X_1X_2...X_N} \hat{h}_{X_1X_2...X_N}^\dagger\right\}. \quad (2.2)$$
where $\hat{h}_{X_1X_2\ldots X_N} = \begin{bmatrix} \hat{h}_{X_1}^\dagger & \hat{h}_{X_2}^\dagger & \ldots & \hat{h}_{X_N}^\dagger \end{bmatrix}^\dagger$. The covariance matrices presented in (4.33) can be expressed as

$$\hat{R}_{xx} = R_{xx} + \sigma_b^2 I, \quad (2.3)$$

$$\hat{R}_{yy} = R_{yy} + \sigma_a^2 I, \quad (2.4)$$

$$\hat{R}_{XY} = \begin{bmatrix} R_{xx} + \sigma_b^2 I & R_{xx} \\ R_{xx} & R_{yy} + \sigma_a^2 I \end{bmatrix}, \quad (2.5)$$

where $\sigma_a^2$ and $\sigma_b^2$ are the estimation error variances at Alice and Bob, respectively and $I$ is the identity matrix. If the channels are reciprocal then $R_{xx} = R_{yy}$. Note that the key rate differs from the more commonly known MIMO channel capacity. Capacity is the mutual information between the input and output of a communication system, while the key rate refers to the mutual information between the propagation channels.

**Secure Key Rate**

If Eve is located close to one of the nodes, then the channels $\hat{h}_z$ and $\hat{h}_g$ observed by Eve may be statistically correlated with the channel $\hat{h}_x$ and $\hat{h}_y$, respectively. As a result, Eve has information that may make some of the bits in $I_K$ insecure. Therefore the *secure key rate* $I_{SK}$ is used to quantify the number of key bits that are secure from the eavesdropper [17], which is given by

$$I_{SK} = I(\hat{h}_x; \hat{h}_y | \hat{h}_z, \hat{h}_g)$$

$$= h(\hat{h}_x | \hat{h}_z, \hat{h}_g) + h(\hat{h}_y | \hat{h}_z, \hat{h}_g) - h(\hat{h}_x, \hat{h}_y | \hat{h}_z, \hat{h}_g)$$

$$= h(\hat{h}_x, \hat{h}_z, \hat{h}_g) + h(\hat{h}_y, \hat{h}_z, \hat{h}_g) - h(\hat{h}_z, \hat{h}_g) - h(\hat{h}_x, \hat{h}_y, \hat{h}_z, \hat{h}_g)$$

$$= \log_2 \frac{|\hat{R}_{XZG}| |\hat{R}_{YZG}|}{|\hat{R}_{ZG}| |\hat{R}_{XYZG}|}. \quad (2.6)$$

Practically, Eve may be located close to one of the nodes. For example, if Eve is located close to Bob, then the propagation channel $\hat{h}_g$ is almost uncorrelated with $\hat{h}_y$. Hence, $\hat{h}_g$
can be ignored in the analysis and (4.35) reduces to

\[
I_{SK} = \log_2 \frac{|\hat{R}_{XZ}||\hat{R}_{YZ}|}{|R_Z||\hat{R}_{XYZ}|}. \tag{2.7}
\]

The corresponding covariances can be computed as

\[
\hat{R}_{XZ} = \begin{bmatrix}
R_{xx} + \sigma_b^2 I & R_{xz} \\
R_{xz}^\dagger & R_{zz} + \sigma_e^2 I
\end{bmatrix}, \tag{2.8}
\]

\[
\hat{R}_{YZ} = \begin{bmatrix}
R_{yy} + \sigma_a^2 I & R_{yz} \\
R_{yz}^\dagger & R_{zz} + \sigma_e^2 I
\end{bmatrix}, \tag{2.9}
\]

\[
\hat{R}_Z = R_{zz} + \sigma_e^2 I, \tag{2.10}
\]

\[
\hat{R}_{XYZ} = \begin{bmatrix}
R_{xx} + \sigma_b^2 I & R_{xy} & R_{xz} \\
R_{yx} & R_{yy} + \sigma_a^2 I & R_{yz} \\
R_{xz}^\dagger & R_{yz}^\dagger & R_{zz} + \sigma_e^2 I
\end{bmatrix}, \tag{2.11}
\]

where \(\sigma_e^2\) is the estimation error variance at Eve and \(\{\cdot\}^\dagger\) is the conjugate transpose. From the two key rates, one can also define the *number of vulnerable key bits* as

\[
I_{VK} = I_K - I_{SK}. \tag{2.12}
\]

Figure 2.4 presents a graphical representation of the key rate metrics, highlighting the fact that a high correlation between channels sampled by Eve and other communicating nodes can increase the vulnerable key bits significantly. Note that the analysis presented above assumes that the propagation channel statistics are Gaussian. For non-Gaussian statistics the mutual information can be computed numerically as presented in [37].

Key rate metrics depend on several factors including the number of antennas equipped at Alice, Bob, and Eve, the signal-to-noise ratio (SNR), the multipath richness of the channel, and the spacing between the elements of the arrays at Alice, Bob, and Eve. In order to understand the basics of the available and secure key rates, a simple study is performed that assumes ideal antennas and a path-based model, where the angles of arrival and departure are uniformly distributed over \([0, 2\pi]\), and the path gains are assumed to be complex Gaussian.
random variables [38]. Alice, Bob, and Eve are equipped with an $N$ element arrays with equally spaced antenna elements with inter-element spacing of $d_A$, $d_B$, and $d_E$ respectively. In order to analyze the impact of multipath richness, the number of paths $L$ in the path based model are varied. All results are averaged over 1000 random covariance matrices. The SNR is defined as the mean squared single-input single-output (SISO) gain to mean squared estimation error.

Figure 2.5 plots the available key rate $I_K$ versus the number of paths $L$ and antennas $N$ at Alice and Bob, where SNR=15 dB, inter-element spacing is $d_B = d_A = 0.5\lambda$, and $\lambda$ is the free space wavelength. The results demonstrate that $I_K$ increases with multipath, especially for larger arrays. For a rich multipath scenario, the key rate increases as $N^2$ as the channel coefficients tend to follow independent and identically distributed (i.i.d.) statistics. Furthermore, $I_K$ saturates as the number of paths increases, where large array size needs more paths (multipath richness) to maximize the available key rate.

Figure 2.6 plots $I_K$ as a function of SNR and inter-element spacing between Alice’s or Bob’s array, where $d_B = d_A$, $N = 2$, $L = 10$, and no mutual coupling is assumed between the antenna elements [37]. Results demonstrate that a lower inter-element spacing $d_B < 0.5\lambda$ can significantly reduce the available key rate, but it saturates for $d_B > 1.0\lambda$. A higher SNR helps to achieve a higher $I_K$, with a logarithmic increase in available key rate with increasing SNR.

Figure 2.7 plots $I_{SK}$ for a single antenna scenario where Eve is assumed to be located near Bob, and the spacing between Bob’s and Eve’s antenna is varied. Note that an ideal
Figure 2.5: Available key rate as a function of number of paths ($L$), where both Bob and Alice are equipped with $N$-element arrays, SNR = 15 dB, and $d_B = d_A = 0.5\lambda$.

Figure 2.6: Available key rate as a function of the separation between Bob and Alice antenna arrays and SNR, where $d_B = d_A$, $N = 2$, and $L = 10$. 
case is considered here with no mutual coupling between the two nodes. For a single antenna scenario the maximum available key rate is 4.05 bits/ch (bits per use of the channel) [38]. Results depict that for a relatively rich multipath scenario most of the generated key bits are safe when $d_{BE} > 0.5\lambda$. Figure 2.8 plots similar results where each node (Bob, Alice, and Eve) is equipped with $N = 2$ antennas, and Bob’s and Eve’s array are parallel to each other. For $N = 2$ the maximum available key rate is 16.2 bits/ch. It is interesting to note that while increasing antennas at each node produces more key bits (higher key rate), most of the generated key bits are vulnerable (not secure) when the separation between Bob’s and Eve’s array is small or the environment is not multipath rich. In other words, increasing the array size at each node can potentially leak more information to Eve.

### 2.3 Propagation Channel Modeling

The effective channel between two nodes includes the impact of both the physical propagation channel as well as the transmit/recieve radio-frequency (RF) circuitry. To explore this further, assume that Alice and Bob are equipped with multiple antennas that are
Figure 2.8: Secure key rate as a function of the separation between Bob and Eve antenna arrays and number of paths, where Bob and Eve antenna arrays are parallel to each other, $d_B = d_A = d_{BE}$, SNR=15 dB, and $N = 2$.

limited to a single polarization. The scalar radiation pattern for the $m$th element in the array of any node is denoted as $e_{\xi,m}(\Omega_{\xi})$, where $\xi \in [A, B, E]$ to denote Alice, Bob, or Eve respectively. If the impact of transmit/receive circuitry is ignored and a simple multi-path model is assumed consisting of $L$ paths, where the $l$th path has angle of departure $(\theta_{A,l}, \phi_{A,l})$ and angle of arrival $(\theta_{B,l}, \phi_{B,l})$ then the propagation channels between the $m$th receive antenna at Bob and $n$th transmit antenna at Alice can be expressed as

$$H_{BA,mn} = \sum_{l=1}^{L} e_{B,m}(\theta_{B,l}, \phi_{B,l}) \alpha_l e_{A,n}(\theta_{A,l}, \phi_{A,l}),$$

(2.13)

where $\alpha_l$ is the complex amplitude associated with $l$th path. Instead of the simple path-based model, if a more realistic cluster based model [39] is used then the same propagation channel can be expressed as

$$H_{BA,mn} = \sum_{k} \int e_{B,m}(\Omega_B) \beta_{B,k}(\Omega_B, \Omega_A) b_{B,k}(\Omega_B, \Omega_A) e_{A,n}(\Omega_A) d\Omega d\Omega_A,$$

(2.14)
where $\beta_{B,k}(\Omega_B, \Omega_A)$ represents a stochastic complex gain function describing propagation of the $k$th cluster from Alice to Bob, $\Omega_A = (\theta_A, \phi_A)$ represents the angle of departure, $\Omega_B = (\theta_B, \phi_B)$ the angle of arrival, $b_{B,\ell}$ is normalized to have unit energy, and $\beta_{B,\ell}$ is a real scalar that sets the relative peak (in terms of field magnitude) of the $k$th cluster at Bob.

The covariance matrices required for key rate metrics can be computed numerically based on channel estimates. A closed form solution for the covariance of individual channels [39] integrates the product of the radiation patterns of the antennas of interest and the power angular spectrum (PAS), which is the average propagating field power as a function of angle. As an example, for Bob the covariance of the channels can be computed as

$$R_{BB[mn,pq]} = E\{H_{BA,mn}^* H_{BA,pq}\}$$

$$= \sum_k \sigma_\beta^2 \int e_{B,m}(\Omega_B) e_{A,n}(\Omega_A) B_k(\Omega_B, \Omega_A) e_{E,p}^*(\Omega_B) e_{A,q}^*(\Omega_A) d\Omega_B d\Omega_A,$$

where $B_k(\Omega_B, \Omega_A) = E\{|b_{B,k}(\Omega_B, \Omega_A)|^2\}$ is the PAS for the $k$th cluster at Bob and $\sigma_\beta^2 = E\{\beta_{B,k}\beta_{B,k}\}$ is the variance of the $k$th cluster gain. Different models for the PAS are considered in prior literature, such as a uniform PAS [40], truncated Gaussian PAS [41], and truncated Laplacian PAS [42], where the latter is most commonly used in modeling. This closed-form computation approach has not been developed for the cross-covariance of channels corresponding to different nodes and therefore is addressed in Chapter 5 of this dissertation.

### 2.4 System Calibration

Figure 3.1 shows a general block diagram of a communication system consisting of RF transmit/receive chains, coupled antenna arrays, matching networks, and a digital signal processing (DSP) block. The propagation channel is sampled by the DSP unit after the RF circuitry at each node. Hence the end-to-end transfer function from Alice to Bob can be expressed as

$$H_{BA}^\prime = C_{RB} H_{BA}^* C_{TA} + \eta_B,$$

16
where \( C_{RB} \) and \( C_{TA} \) incorporate the impact of receive and transmit circuitry at Bob and Alice, respectively and \( \eta_B \) refers to the estimation error at Bob. The structure of \( C_{RB} \) and \( C_{TA} \) depends upon the RF circuitry and transmit/receive antenna arrays. For a MIMO communication system, if these matrices are not diagonal then coupling exists between the sampled propagation channels. A detailed analysis on the impact of RF circuitry on MIMO channel capacity as well as the approaches that can be used to reduce the impact of coupling are presented in [29]. A similar study is presented in Chapter 3 of this dissertation for key generation, which includes the impact of both inter and intra-array coupling when Eve is located close to one of the communicating nodes.

Physical layer key generation requires the forward and backward channel between Bob and Alice to be reciprocal due to the fact that common randomness between the channels is used for key generation. For \( H_{BA}' \) to be reciprocal, the matrices must satisfy

\[
C_{RB}H_{BA}C_{TA} = \{C_{RA}H_{AB}C_{TB}\}^T, \tag{2.18}
\]

where \( C_{TB} \) and \( C_{RA} \) incorporate the impact of transmit and receive circuitry at Bob and Alice, respectively and \( H_{AB} \) is the propagation channel sampled by Alice. However, practically there may be non-reciprocal components in the RF circuitry and (2.18) may not be satisfied. A calibration phase based on the total least squares (TLS) algorithm is presented in [43], where the goal is to make the propagation channels reciprocal. Chapter 4 investigates the
impact of non-reciprocity on key generation and employs the TLS algorithm to overcome the impact of non-reciprocal channels.
The impact of antenna mutual coupling and impedance matching on the throughput of MIMO systems has been carefully analyzed in prior work [29, 44–49]. However, no work has yet appeared discussing the impact of coupling on key establishment performance using antenna arrays. While this analysis can be performed through modification of existing network analysis approaches, the nature of key establishment creates at least two unique complications that have not been considered previously. First, in fixed unmanned installations, an eavesdropper could place her antennas very close to those of one of the nodes to maximize the information she learns regarding the established key, suggesting the need to model the coupling between the antennas of an eavesdropper and those of a legitimate node. Second, the fact that reciprocal channel estimates are required for key establishment means that the signal models used must accommodate the calibration that will be performed to remove the non-reciprocal contributions to the channel created by the radio circuitry [30].

In this chapter, a perfect calibration is used which assumes that the non-reciprocal part of channel transfer function is already known. In the following chapter, a more generic calibration based solution is proposed to remove non-reciprocities in the end-to-end communication channel.

This chapter addresses these two unique complications by extending network theory analysis of MIMO radios with mutually coupled antennas [29] to the case of reciprocal channel-based key establishment. The development not only demonstrates how to apply the analysis to obtain the channel correlations required for computation of key establishment performance but also adds the complexity of an eavesdropper whose antennas may be coupled to those of one of the legitimate nodes. Furthermore, the presentation formulates the signal
Figure 3.1 presents the communication scenario considered in this analysis where Alice transmits from $N_A$ antennas to Bob who receives the signal with $N_B$ antennas. Eve is a passive eavesdropper that observes the communication between Alice and Bob using $N_E$ antennas. Signals in the network model are represented as forward and reverse traveling waveforms. The model includes elements such as $d_A$, $d_B$, and $d_E$ which represent the element spacings, as well as $d_{BE}$ which represents the distance between Bob and Eve. The network model is used to demonstrate the impact of coupling and sub-optimal but practical impedance matching on performance.

3.1 System Model and Analysis

Figure 3.1 presents the communication scenario considered in this analysis where Alice transmits from $N_A$ antennas to Bob who receives the signal with $N_B$ antennas. Eve is a passive eavesdropper that observes the communication between Alice and Bob using $N_E$ antennas. Signals in the network model are represented as forward and reverse traveling waveforms.
waves denoted as $a_\xi$ and $b_\xi$, respectively, where $\xi$ takes on different designations as seen in Figure 3.1. The network components are represented by their scattering parameter (S-parameter) matrices referenced to a system impedance of $Z_0$. All antenna arrays are mutually coupled, and matching networks are provided to either maximize the power transfer to/from the arrays or to minimize the noise figure of the low-noise amplifiers (LNAs). Circuit elements such as the matching networks are in general expressed as block matrices of the form

$$S = \begin{bmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{bmatrix}.$$  \hspace{1cm} (3.1)

Key establishment requires Alice and Bob to each estimate the end-to-end channel transfer function for transmission in each direction and then to calibrate to remove the impact of non-reciprocal contributors to the channel so that each possesses the same transfer function [43]. For example, when Bob transmits to Alice, Bob will replace the LNAs and loads with transmitting circuitry. Bob’s matching network therefore is divided into two sections: one designed to maximize power transfer between the antennas and independent loads of impedance $Z_0$, and another designed to minimize the LNA noise figure. If the transfer S-parameter matrix for the portion of the circuit in the dotted rectangle in Figure 3.1 is computed, then the effective channel is reciprocal as desired. A limited portion of Bob’s receiver circuit is used for the signal analysis, but it is important to recognize that the LNAs are important noise sources in the system. Therefore, the entire receiver model is used to determine the noise generated by the LNAs referred to the boundary between Bob’s matching networks.

Finally, it is assumed that Bob and Eve are far from Alice but are close enough together that their antennas may experience cross-array mutual coupling. Therefore, Eve’s circuit can impact the effective channels from Alice to Bob and Bob to Alice. It is assumed that Eve knows that Alice and Bob use circuit calibration and therefore uses an identical calibration to ensure that her estimate of the channel from Alice to herself is as close as possible to the channel estimated by Bob.
3.1.1 Transmitter

Using the fact that $b_A = S_{AA}a_A$, the incoming wave at the input of Alice’s transmit antenna terminals is

\[
a_A = S_{A,21}a_{1A} + S_{A,22}b_A = (I - S_{A,22}S_{AA})^{-1}S_{A,21}a_{1A},
\]

(3.2)

where $I$ is the identity matrix, $S_{AA}$ is the S-parameter matrix of Alice’s antenna array, and $S_{A,ij}$ is the block matrix which refers to the maximum power matching network at Alice that relates the incoming waves at port $j$ to the outgoing waves at port $i$.

3.1.2 Signal Received by Bob

Because the antennas of Bob and Eve can be coupled, $S_{BE}$ is defined as the S-parameters relating the output waves on Bob’s array to the input waves on Eve’s array and $S_{EB} = S_{BE}^T$, where $\{\cdot\}^T$ is the transpose, for coupling in the other direction. Using the notation of Figure 3.1,

\[
a_B = b_{SB} + S_{BB}b_B + S_{BE}b_E
\]

(3.3)

\[
a_E = b_{SE} + S_{EB}b_B + S_{EE}b_E,
\]

(3.4)

where $b_{SB}$ and $b_{SE}$ are the waves generated by Bob’s and Eve’s antennas respectively when they are terminated in loads of resistance $Z_0$. The vector $v_{0B} = 2Z_0H_{BA}i_A$ represents the open-circuit voltages on Bob’s antennas, where $i_A$ is the vector of currents driving Alice’s antennas, $H_{BA}$ is a transfer matrix whose entries depend on the propagation and the antenna radiation patterns, and the factor $2Z_0$ keeps $H_{BA}$ dimensionless and offers later convenience. Similarly, $v_{0E} = 2Z_0H_{EA}i_A$ is the vector of open-circuit voltages on Eve’s antennas.

To determine $b_{SB}$, Bob’s receiving antennas are terminated in open circuits, leading to $b_B = a_B$ so that $v_{0B} = 2Z_0^{1/2}a_B$. This leads to

\[
2Z_0H_{BA}i_A = 2Z_0^{1/2}a_B \Rightarrow a_B = Z_0^{1/2}H_{BA}i_A,
\]

(3.5)
with a similar result for Eve of \( a_E = Z_{0}^{1/2}H_{EA}i_A \). Using this open-circuit result in (3.3) and (3.4) along with the fact that \( i_A = Z_0^{-1/2}(I - S_{AA})a_A \) gives

\[
b_{SB} = [(I - S_{BB})H_{BA} - S_{BE}H_{EA}] (I - S_{AA})a_A \tag{3.6}
\]

\[
b_{SE} = [(I - S_{EE})H_{EA} - S_{EB}H_{BA}] (I - S_{AA})a_A. \tag{3.7}
\]

Therefore, (3.3) and (3.4) for arbitrary antenna loading become

\[
a_B = F_Ba_A + S_{BB}b_B + S_{BE}b_E \tag{3.8}
\]

\[
a_E = F_Ea_A + S_{EB}b_B + S_{EE}b_E. \tag{3.9}
\]

For simplicity, the two matching networks at Eve can be combined into a composite S-parameter matrix designated as \( \overline{S}_E \). Using \( a_{2E} = S_{FE,11}b_{2E} \), the expression for \( b_{2E} \) can be derived as

\[
b_{2E} = S_{E,21}a_E + S_{E,22}a_{2E}
= (I - S_{E,22}S_{FE,11})^{-1}S_{E,21}a_E. \tag{3.10}
\]

where \( S_{E,ij} \) and \( S_{FE,ij} \) are the S-parameters for the maximum power and minimum noise figure matching networks respectively at Eve that relate the vector of waves exiting ports \( i \) to the vector of waves incident on ports \( j \). The relationship between \( a_E \) and \( a_{0E} \) is used to compute the composite \( \overline{S}_{E,21} \) given by

\[
a_{0E} = S_{FE,21}b_{2E} = S_{FE,21}(I - S_{E,22}S_{FE,11})^{-1}S_{E,21}a_E = \overline{S}_{E,21}a_E. \tag{3.11}
\]

The composite \( \overline{S}_{E,11} \) can be computed as

\[
b_E = S_{E,11}a_E + S_{E,12}a_{2E}
= [S_{E,11} + S_{E,12}S_{FE,11}(I - S_{E,22}S_{FE,11})^{-1}S_{E,21}]a_E = \overline{S}_{E,11}a_E. \tag{3.12}
\]
Similarly the expression for $\bar{S}_{E,12}$ and $\bar{S}_{E,22}$ can be derived. The final expressions for the blocks of $\bar{S}_E$ are

$$\bar{S}_{E,11} = S_{E,11} + S_{E,12}S_{FE,11}(I - S_{E,22}S_{FE,11})^{-1}S_{E,21} \quad (3.13)$$

$$\bar{S}_{E,21} = S_{FE,21}(I - S_{E,22}S_{FE,11})^{-1}S_{E,21} \quad (3.14)$$

$$\bar{S}_{E,12} = S_{E,12}(I - S_{FE,11}S_{E,22})^{-1}S_{FE,12} \quad (3.15)$$

$$\bar{S}_{E,22} = S_{FE,22} + S_{FE,21}S_{E,22}(I - S_{FE,11}S_{E,22})^{-1}S_{FE,12}. \quad (3.16)$$

It is assumed that the reflection coefficient observed at the input of each LNA is zero for both Bob and Eve, since an amplifier input mismatch will not change the signal-to-noise ratio (SNR) provided that the LNA noise model refers the noise contributions to the amplifier input. A well-established model is used that divides the noise at the input of each LNA into forward and reverse traveling waves, which at Eve are $a_{\eta E}$ and $b_{\eta E}$, respectively. Since Eve’s amplifier inputs are matched to $Z_0$, $b_{0E}$ will only have a noise contribution, or $b_{0E} = b_{\eta E}$. Using network analysis on Eve’s circuit combined with (3.9) yields

$$b_E = \bar{S}_{E,11}a_E + \bar{S}_{E,12}b_{0E}$$
$$= \bar{S}_{E,11}[F_E a_A + S_{EB}b_B + S_{EE}b_E] + \bar{S}_{E,12}b_{0E}$$
$$= (I - \bar{S}_{E,11}S_{EE})^{-1} [\bar{S}_{E,11}(F_E a_A + S_{EB}b_B) + \bar{S}_{E,12}b_{\eta E}]. \quad (3.17)$$

Placing this result in (3.8) and solving for $a_B$ results in

$$a_B = F_B a_A + S_{BB}b_B + S_{BE}(I - \bar{S}_{E,11}S_{EE})^{-1} [\bar{S}_{E,11}(F_E a_A + S_{EB}b_B) + \bar{S}_{E,12}b_{\eta E}]$$
$$= S_{BA}a_A + \Theta_{BE}b_B + \Theta_{E}S_{E,12}b_{\eta E} \quad (3.18)$$

$$\Theta_{E} = S_{BE}(I - \bar{S}_{E,11}S_{EE})^{-1} \quad (3.19)$$

$$S_{BA} = F_B + \Theta_{E}S_{E,11}F_E \quad (3.20)$$

$$\Gamma_{BE} = S_{BB} + \Theta_{E}S_{E,11}S_{EB}. \quad (3.21)$$

To ensure channel reciprocity, the traveling wave $\tilde{b}_{2B}$ (which excludes the noise from Bob’s LNAs) is constructed when Bob’s first matching network is terminated in loads of
impedance $Z_0$. To do that, (3.18) is first updated using $b_B = S_{B,11}a_B$ as

$$a_B = S_{BA}a_A + \Gamma_{BE}S_{B,11}a_B + \Theta_E S_{E,12}b_{\eta E}$$
$$= \left( I - \Gamma_{BE}S_{B,11} \right)^{-1} \left[ S_{BA}a_A + \Theta_E S_{E,12}b_{\eta E} \right] \quad (3.22)$$

Straightforward network analysis based on (3.22) and (3.2) yields

$$\tilde{b}_{2B} = S_{B,21}a_B = T_{BA}a_{1A} + \Upsilon_B b_{\eta E} \quad (3.23)$$

$$T_{BA} = G_B S_{BA} \left( I - S_{A,22}S_{AA} \right)^{-1} S_{A,21} \quad (3.24)$$

$$G_B = S_{B,21} \left( I - \Gamma_{BE}S_{B,11} \right)^{-1} \quad (3.25)$$

$$\Upsilon_B = G_B S_{BE} \left( I - S_{E,11}S_{EE} \right)^{-1} S_{E,12} \quad (3.26)$$

where $T_{BA}$ is the reciprocal channel transfer function as highlighted in Figure 3.2.

### 3.1.3 Bob’s Amplifier Noise

In practice Bob will estimate the channel after the LNAs and then calibrate to remove the effect of the LNAs and the second matching network, meaning that the estimate of $T_{BA}$ will be corrupted by Bob’s LNA noise. Therefore the objective here is to determine the equivalent noise that should be added to $\tilde{b}_{2B}$. Based the proposed model where the input reflection coefficient to each LNA is zero, the expression for $b_{2B}$ with $a_{2B} = S_{FB,11}b_{2B}$ can
be derived as
\[ b_{2B} = T_{BA}a_{1A} + \Gamma_B a_{2B} = T_{BA}a_{1A} + \Gamma_B S_{FB,11} b_{2B} \]
\[ = (I - \Gamma_B S_{FB,11})^{-1} T_{BA} a_{1A}. \] (3.27)

The *noise free* relationship between \( a_{0B} \) and \( a_{1A} \) can then be written as
\[ a_{0B} = S_{FB,21} b_{2B} \]
\[ = S_{FB,21} (I - \Gamma_B S_{FB,11})^{-1} T_{BA} a_{1A}. \] (3.28)

Since \( T_{BA} a_{1A} \) is the signal that goes into matched terminations at the output of Bob’s first matching network, the calibration is technically performed by multiplying the signal \( a_{0B} \) by \((I - \Gamma_B S_{FB,11})S_{FB,21}^{-1}\). The output reflection coefficient \( \Gamma_B \) can be computed based on the relationship between \( b_{2B} \) and \( a_{2B} \) as
\[ b_{2B} = S_{B,22} a_{2B} + S_{B,21} a_B, \] (3.29)

where
\[ a_B = \Gamma_{BE} b_B = \Gamma_{BE} S_{B,11} a_B + \Gamma_{BE} S_{B,12} a_{2B} \]
\[ = (I - \Gamma_{BE} S_{B,11})^{-1} \Gamma_{BE} S_{B,12} a_{2B}. \] (3.30)

Plugging \( a_B \) into (3.29) yields
\[ b_{2B} = \underbrace{S_{B,22} + S_{B,21}(I - \Gamma_{BE} S_{B,11})^{-1} \Gamma_{BE} S_{B,12}}_{\Gamma_B} a_{2B}. \] (3.31)

However, Bob does not know \( \Gamma_{BE} \) and therefore must perform the calibration using the uncoupled output reflection coefficient
\[ \bar{\Gamma}_B = S_{B,22} + S_{B,21}(I - S_{BB} S_{B,11})^{-1} S_{BB} S_{B,12}. \] (3.32)

26
The calibration matrix is therefore

\[ C_B = (I - \Gamma_B S_{FB,11})S_{FB,21}^{-1}. \]  \hfill (3.33)

Since Bob’s forward traveling noise at the input to the amplifiers is given as \( \Gamma_{0B} b_{\eta B} - a_{\eta B} \) [29], the calibration means that the total signal becomes

\[
\begin{align*}
    b_{2B} &= T_{BA} a_{1A} + C_B (\Gamma_{0B} b_{\eta B} - a_{\eta B}) + \Upsilon_B b_{\eta E} \\
    \Gamma_{0B} &= S_{FB,22} + S_{FB,21} (I - \Gamma_B S_{FB,11})^{-1} \Gamma_B S_{FB,12}.
\end{align*}
\]  \hfill (3.34)  \hfill (3.35)

### 3.1.4 Signal and Noise at Eve

To determine the signal and noise that would be delivered to terminations of resistance \( Z_0 \) at the output of Eve’s first matching network, all of the derivations in Sections 3.1.2 and 3.1.3 are used with the simple notational change that all subscripts ‘B’ and ‘E’ are interchanged.

### 3.1.5 Signal and Noise at Alice

Because Eve is far from Alice, Alice’s received signal due to transmission from Bob does not include Eve’s noise contribution. Therefore, the channel from Bob to Alice is given by (3.34) along with the supporting equations after interchanging the subscripts ‘A’ and ‘B’, setting \( b_{\eta E} = 0 \) (vector of all zeros), and using \( T_{AB} = T_{BA}^T \) (reciprocity).

### 3.1.6 Matching Network Specification

The procedure for constructing the S-parameters of a matching network to either maximize power transfer between coupled antennas and loads or to minimize the noise figure of the LNAs has been well documented in the literature [29]. However, because channel-based key establishment requires reciprocal channel estimates, the matching networks must be reciprocal, a constraint not explicitly enforced in prior work. Therefore, a brief summary of the S-parameter computation procedure for reciprocal matching networks is provided below.
Lossless reciprocal matching networks have an S-parameter matrix that satisfies $S^\dagger S = I$ and $S = S^T$, where $\{\cdot\}^\dagger$ is a conjugate transpose. Based on (3.1), the singular value decomposition (SVD) of the matrix sub-blocks can be written as $S_{ij} = U_{ij} A_{ij}^{1/2} V_{ij}^\dagger$ where $U_{ij}$ and $V_{ij}$ are the unitary matrices of singular vectors and $A_{ij}^{1/2}$ is the diagonal matrix of real singular values. It is relatively straightforward to show that the constraints lead to the sub-blocks [45]

$$S_{mn} = \begin{cases} U_{mm} A_{11}^{1/2} U_{mm}^T & m = n \\ j U_{mm} (I - A_{11})^{1/2} U_{nn}^T & m \neq n. \end{cases} \tag{3.36}$$

where a detailed derivation is presented in Appendix A.

While the system includes several matching networks, Bob’s maximum power transfer network is used to illustrate the matching procedure. Obviously during design, the reflection coefficient $\Gamma_{BE}$ that incorporates coupling to Eve is unknown, and therefore rather than designing a network to achieve a certain value of $\Gamma_B$ from (3.31), the matching network is designed to achieve a desired value of $\overline{\Gamma}_B$ from (3.32). Using (3.36) in (3.32) leads to

$$\overline{\Gamma}_B = \overline{U}_B \overline{A}_B^{1/2} \overline{U}_B^T \tag{3.37}$$

$$= S_{B,22} + S_{B,21}(I - S_{BB} S_{B,11})^{-1} S_{BB} S_{B,12}$$

$$= U_{B,22} A_{B,11}^{1/2} U_{B,22}^T - U_{B,22} (I - A_{B,11})^{1/2} U_{B,11}^T (I - S_{BB} U_{B,11} A_{B,11}^{1/2} U_{B,11}^T)^{-1} S_{BB}$$

$$U_{B,11} (I - A_{B,11})^{1/2} U_{B,22}^T$$

$$= U_{B,22} \Psi_B U_{B,22}^T \tag{3.38}$$

$$\Psi_B = A_{B,11}^{1/2} - (I - A_{B,11})^{1/2} \Omega_B (I - A_{B,11})^{1/2} \tag{3.39}$$

$$\Omega_B = U_{B,11} (I - S_{BB} U_{B,11} A_{B,11}^{1/2} U_{B,11}^T)^{-1} S_{BB} U_{B,11}. \tag{3.40}$$
Choosing $U_{B,22} = \bar{U}_B$ and $U_{B,11} = U_{BB}^*$, where $S_{BB} = U_{BB} A_{BB}^{1/2} U_{BB}^T$ is the SVD and $\{ \cdot \}^*$ is the conjugate, and relating (3.37) and (3.38) to solve for $\overline{\Lambda}_B^{1/2}$ leads to

\[
\overline{\Lambda}_B^{1/2} = \Psi_B \\
= \Lambda_{B,11}^{1/2} - (I - \Lambda_{B,11})^{1/2} U_{B,11}^T (I - S_{BB} U_{B,11} \Lambda_{B,11}^{1/2})^{-1} S_{BB} U_{B,11} (I - \Lambda_{B,11})^{1/2} \\
= \Lambda_{B,11}^{1/2} - (I - \Lambda_{B,11}) \Lambda_{BB}^{1/2} (I - \Lambda_{BB}^{1/2} \Lambda_{B,11}^{1/2})^{-1}. \tag{3.41}
\]

Solving this equation for $\Lambda_{B,11}^{1/2}$ yields

\[
\Lambda_{B,11}^{1/2} = (\overline{\Lambda}_B^{1/2} + \Lambda_{BB}^{1/2}) (I + \overline{\Lambda}_B^{1/2} \Lambda_{BB}^{1/2})^{-1}. \tag{3.42}
\]

Therefore, the S-parameter blocks of the matching network are specified by the antenna S-parameters $S_{BB}$ and the desired output reflection coefficient $\overline{\Gamma}_B$.

### 3.2 Performance Evaluation

The performance of secret key establishment based on reciprocal electromagnetic channels is quantified using two key rate metrics: Available key rate ($I_K$) which is the number of key bits available per observation of the reciprocal channel between Alice and Bob and secure key rate ($I_{SK}$) which is used to quantify the number of key bits that are secure from the eavesdropper. In the following, the notation $h_x$ and $h_z$ is used to represent the end-to-end transfer matrices $T_{BA}$ and $T_{EA}$ respectively stacked columnwise into vectors. Similarly, $h_y$ represents $T_{AB}^T$ stacked columnwise so that the ordering of the coefficients matches that of $h_x$. The notation $\hat{h}_\xi$ is used to represent an estimate of the vector $h_\xi$, where $\xi \in [x,y,z]$. Note that $h_y = h_x$, but in general $\hat{h}_y \neq \hat{h}_x$ due to channel estimation errors caused by the noise. $I_K$ and $I_{SK}$ can be computed based on channel covariance matrices as

\[
I_K = I(\hat{h}_x; \hat{h}_y) = \log_2 \frac{|\hat{R}_{xx}| |\hat{R}_{xy}|}{|\hat{R}_{XY}|}, \tag{3.43}
\]

\[
I_{SK} = I(\hat{h}_x; \hat{h}_y|\hat{h}_z) = \log_2 \frac{|\hat{R}_{xz}| |\hat{R}_{yz}|}{|\hat{R}_{Z}| |\hat{R}_{XYZ}|}. \tag{3.44}
\]

A computation procedure for these quantities is detailed in Chapter 2.
3.2.1 Channel Estimation

Equation (3.34) is a model for the signal received by Bob based on transmissions from Alice, but what is really needed for key establishment is an estimate of the channel $T_{BA}$. Consider a channel estimation protocol in which Alice transmits the vector $a_{1A,n} = \sqrt{p}w_n$ during the $n$th time slot, where $p$ is the total transmitted power and $w_n$ is the $n$th column of the $N_A \times N_A$ identity matrix $I_{N_A}$. From this transmission, the $n$th column of $T_{BA}$ can be estimated based on (3.34) given as

$$
\hat{T}_{BA,n} = [B_B H_{BA} A + D_B H_{EA} A]w_n + \frac{1}{\sqrt{p}} \eta_{B,n} \quad (3.45)
$$

$$
A = (I - S_{AA})(I - S_{A,22}S_{AA})^{-1}S_{A,21} \quad (3.46)
$$

$$
B_B = G_B[I - S_{BB} - \Theta_E S_{EE,11} S_{EB}] \quad (3.47)
$$

$$
D_B = G_B[\Theta_E S_{EE,11}(I - S_{EE}) - S_{BE}] \quad (3.48)
$$

where $\eta_{B,n}$ is the $n$th realization of the random noise terms in (3.34). After stacking the resulting $N_A$ vectors into a column vector, the following estimate is created

$$
\hat{h}_x = \left( A^T \otimes B_B \right) h_{BA} + \left( A^T \otimes D_B \right) h_{EA} + \frac{1}{\sqrt{p}} \eta_B, \quad (3.49)
$$

where $h_{BA}$ and $h_{EA}$ are the channels $H_{BA}$ and $H_{EA}$ stacked columnwise and $\eta_B$ is the $N_A N_B \times 1$ vector formed by stacking the $N_A$ vectors $\eta_{B,n}$. The channel $\hat{h}_x$ can be formed by simply by interchanging the subscripts ‘B’ and ‘E’ in (3.49) and all supporting equations.

3.2.2 Channel Covariance

The next step is to construct the required covariances for computation of the key rate metrics. To accomplish this, $K_{\xi\xi'} = E\{h_{\xi A} h_{\xi' A}^\dagger\}$, where $\xi, \xi' \in [B, E]$, is defined as the auto- and cross-covariances of the propagation channels from the transmit to receive antenna terminals. It is relatively straightforward to show that

$$
R_{xx} = E\{h_x h_x^\dagger\} = (P_{BB} K_{BB} + P_{BE} K_{EB}) P_{BB}^\dagger + (P_{BB} K_{BE} + P_{BE} K_{EE}) P_{BE}^\dagger, \quad (3.50)
$$
where $K_{EB} = K_{BE}^\dagger$. Note that $R_yy = R_{xx}$ and the $R_{zz}$ can be formed simply by interchanging the subscripts ‘B’ and ‘E’ in (3.50) and all supporting equations. Similarly, $R_{xx} = R_{xx}^\dagger$ can be computed as

$$R_{xx} = E \{ h_x h_z^\dagger \} = (P_{BB}K_{BB} + P_{BE}K_{EB})P_{EB}^\dagger + (P_{BB}K_{BE} + P_{BE}K_{EE})P_{EE}^\dagger.$$  \hfill (3.51)

### 3.2.3 Error Covariance

The LNA noise generated during two different time slots is assumed to be uncorrelated, or $E \{ \eta_{B,m} \eta_{B,n}^\dagger \} = 0$ for $m \neq n$. Therefore, the estimated covariance matrix can be expressed as

$$\hat{R}_{xx} = R_{xx} + \frac{1}{\rho} I_N \otimes R_{\eta, BB}, \hfill (3.52)$$

where $R_{\eta, BB} = E \{ \eta_B \eta_B^\dagger \}$. Based on the analysis in [29], it is simple to show that

$$R_{\eta, BB} = E \{ [C_B(\Gamma_{0B}b_{\eta B} - a_{\eta B}) + \Upsilon_B b_{\eta E}][C_B(\Gamma_{0B}b_{\eta B} - a_{\eta B}) + \Upsilon_B b_{\eta E}]^\dagger \}$$

$$= \kappa T_{\beta E} \Upsilon_B \Upsilon_B^\dagger + \kappa C_B R_{N, B} C_B^\dagger,$$  \hfill (3.53)

where

$$E \{ a_{\eta \xi} a_{\eta \xi}^\dagger \} = \kappa T_{\alpha \xi} I,$$

$$E \{ b_{\eta \xi} b_{\eta \xi}^\dagger \} = \kappa T_{\beta \xi} I,$$

$$E \{ a_{\eta \xi} b_{\eta \xi}^\dagger \} = \kappa T_{\Gamma \xi} I,$$  \hfill (3.54)

$$R_{N, B} = T_{0B} I - T_{\Gamma B} \Gamma_{0B} - T_{\Gamma B}^\dagger \Gamma_{0B}^\dagger + T_{\beta B} \Gamma_{0B}^\dagger,$$  \hfill (3.55)

and $\kappa$ is Boltzmann constant times the bandwidth and $\xi \in [B, E]$. The equivalent noise temperatures $T_{\alpha \xi}$, $T_{\beta \xi}$ and $T_{\Gamma \xi}$ for $\xi \in [A, B, E]$ define the noise performance of the LNAs and are discussed in more detail in [29]. The covariance $\hat{R}_{zz}$ has an identical form, with $R_{\eta, EE}$ computed from (3.53) and (3.55) by interchanging the subscripts ‘B’ and ‘E’.

A bipolar junction transistor taken from a Hewlett-Packard Application Note [50] is used as the LNA in this work. The S-parameters and noise parameters of this transistor
at 4 GHz are $S_{GB,11} = 0.552\angle 169^\circ$, $S_{GB,12} = 0.049\angle 23^\circ$, $S_{GB,21} = 1.681\angle 26^\circ$, $S_{GB,22} = 0.839\angle -67^\circ$, $F_{\text{min}} = 3.5\text{dB}$, $\Gamma_{\text{opt}} = 0.475\angle 166^\circ$, and $R_n = 3.5\ \Omega$, where $S_{GB}$ refers to the S-parameters of the transistor. $F_{\text{min}}$, $\Gamma_{\text{opt}}$, and $R_n$ represent the minimum noise figure, optimal source termination for noise figure, and effective noise resistance, respectively. These parameters are converted to the effective noise temperatures.

Because of mutual coupling, the total noise observed at Bob and Eve is partially correlated. While the coupled noise is generally weak, for completeness it is recognized that

$$\hat{R}_{xz} = R_{xz} + (1/p)I_{N_A} \otimes R_{\eta,\text{BE}}$$

where

$$R_{\eta,\text{BE}} = E \left\{ \eta_B^\dagger \eta_E \right\} = \kappa Y_B \left[ T_{\beta E} \Gamma_{0E}^\dagger - T_{\Gamma E} I \right] C_E^\dagger + \kappa C_B \left[ T_{\beta B} \Gamma_{0B} - T_{\Gamma B} I \right] Y_E^\dagger. \quad (3.56)$$

Finally, because Alice’s channel vector $h_y$ has been ordered to coincide with the ordering of $h_x$ and because Alice does not observe any of Eve’s noise, her covariance is

$$\hat{R}_{yy} = R_{xx} + (1/p)R_{\eta,AA} \otimes I_{N_B}$$

where $R_{\eta,AA} = \kappa C_A R_{N_A} C_A^\dagger$ with $R_{N_A}$ obtained from (3.55) by replacing the subscript ‘B’ with ‘A’. Furthermore, because the noise generated by different LNAs is uncorrelated, $\hat{R}_{xy} = R_{xy} = R_{xx} = R_{yy}$.

### 3.3 Results

The analysis is applied to a scenario where all nodes have half-wave ($\lambda/2$, where $\lambda$ is the free-space wavelength) wire dipoles. Unless otherwise specified, all results are for $N_A = N_B = N_E = 2$. Alice’s dipoles are separated by $d_A = \lambda/2$, while the element separation $d_B$ and $d_E$ is varied for Bob’s and Eve’s arrays, respectively. When evaluating the secure key rate $I_{SK}$, unless otherwise specified it is assumed that the arrays at Bob and Eve are oriented in the same direction but separated by a distance $d_{BE}$ in a direction perpendicular to the array axes, as shown in the boxed diagram in the upper left of Figure 3.1. The full S-parameter matrices and open-circuit radiation patterns for the coupled antennas are evaluated as a function of the element/node spacings using the Numerical Electromagnetic Code (NEC) [51]. The focus of this analysis is on coupling only at Bob and Eve, and therefore the antenna at Alice is modelled as a simple array of isolated elements ($S_{AA}$ is diagonal).
3.3.1 Propagation Channel Covariance

The typical analytical approach for channel spatial covariance construction involves an integration of the power angular spectrum (PAS) representing the average power in the propagating field as a function of angle and the radiation patterns of the communicating antennas. Experimental analysis and electromagnetic modeling have demonstrated that in many environments, the multipaths are clustered in angle, with the angular variation of the PAS for each cluster described by a common distribution function \( C(\phi) \) that represents the functional form of the PAS. There are many functional forms for \( C(\phi) \) that satisfy different cluster distributions like the Uniform PAS, Truncated Gaussian PAS, or Truncated Laplacian PAS. Experimental analysis has shown that clusters in many environments satisfy a truncated Laplacian distribution given by

\[
C(\phi) = \frac{1}{\sigma \sqrt{2\pi}} \exp \left[ \frac{(\phi - \phi_0)^2}{2\sigma^2} \right] \times [u(\phi - \phi_0 + \Delta \phi) - u(\phi - \phi_0 - \Delta \phi)],
\]

where the cluster is centered at the angle \( \phi_0 \) and has width \( 2\Delta \phi \) and where \( u(\cdot) \) represents the step function. Figure 3.3 shows a power image of a representative clustered PAS where each cluster follows the truncated Laplacian distribution, showing that the multipath energy is concentrated in a few regions in the transmit angle-receive angle space.

The propagation in this work is modelled by a set of \( N_C \) clusters in the horizontal plane, where each cluster is described by a two-dimensional truncated Laplacian distribution function in departure and arrival azimuth angle using the parameters in [28]. The central departure and arrival angles of each cluster are realized as independent uniformly-distributed random variables, and the gain of each cluster is realized as a unit-variance Rayleigh-distributed random variable. For a single random cluster realization, the covariances \( K_{BB}, K_{BE}, \) and \( K_{EE} \) are computed in closed-form based on the clusters and the antenna radiation patterns [28]. Next, the required end-to-end channel covariances are formulated followed by the computation of the key rate for that cluster realization. All key rates presented represent averages over a minimum of 400 cluster realizations and unless otherwise stated are based on \( N_C = 4 \) clusters.
The current analysis focus on cases where Bob and Eve are separated by less than two wavelengths, and therefore for operation frequencies above 1 GHz and for typical environments, it is assumed that they observe the same clusters. However, for larger values of $d_{BE}$ or for scatterers very near to the nodes, accurate calculations require that the cluster characteristics describing the channels to Bob and Eve differ [52]. It is important to note that if the clusters observed by Bob and Eve differ, the cross-channel correlation will decrease and the secure key rate will increase, making the above mentioned assumption a worst-case scenario.

A reference case is defined in which Bob’s antennas are separated by $10\lambda$. For this case, we compute the reference channel covariance $R_{xx}^{\text{ref}}$ and the reference estimation error $R_{\eta,xx}^{\text{ref}} = (1/p)I_{N_A} \otimes R_{\eta,BB}$ for each channel cluster realization. The value of $\kappa/p$ is determined to ensure that the effective channel SNR $\text{Tr}(R_{xx}^{\text{ref}})/\text{Tr}(R_{\eta,xx}^{\text{ref}})$ achieves a specified value, and the resulting value of $\kappa/p$ is used for all subsequent simulations based on that cluster realization. An identical procedure is used to compute the SNR observed by Eve. Unless otherwise specified, all nodes experience an SNR of 15 dB.

Figure 3.3: Representative clustered PAS showing four clusters satisfying a truncated Laplacian distribution.
3.3.2 Matching Network Objectives

Alice’s matching network is designed to match each of the (uncoupled) antennas to an impedance of $Z_0$. Because neither Bob nor Eve will know the cross array coupling $S_{BE}$, their designs assume $S_{BE} = S_{EB} = 0$. The objective of Bob’s maximum power matching network is to achieve $\Gamma_B = 0$, but the design can be based on different assumptions. Optimal matching assumes the full matrix $S_{BB}$ in the design and therefore leads to a matching network that has coupling between the ports to compensate for the antenna coupling. Diagonal matching provides uncoupled terminations on the antennas so that each port is matched to its input impedance [49]. Finally, for no mutual coupling, the antenna mutual coupling is ignored in simulation and matching network design. For all results, Eve’s maximum power matching network uses the optimal design.

Because the goal of the maximum power transfer matching networks is to produce $\bar{\Gamma}_B = \bar{\Gamma}_E = 0$, each minimum noise figure matching network is designed to transform a source impedance of $Z_0I$ to $\Gamma_{0B} = \Gamma_{0E} = \Gamma_{opt}I$, where $\Gamma_{opt}$ is the reflection coefficient that minimizes the LNA noise figure. Because of Bob-Eve coupling and possibly imperfect maximum power transfer matching (e.g. for a diagonal match), $\Gamma_B \neq 0$ and $\Gamma_E \neq 0$, and therefore the desired minimum noise figure may not be achieved. The simulations account for this realized mismatch.

3.3.3 Available Key Rate

Analyzing the available key rate $I_K$ ignores the impact of the eavesdropper Eve. The top plot in Figure 3.4 shows $I_K$ as a function of Bob’s antenna spacing for three different matching network conditions for Bob’s maximum power matching network. For $d_B \leq \lambda/4$, it is observed that $I_K$ for the optimal match remains much higher than it does for the diagonal match or for no mutual coupling. The prior work on MIMO communication shows that this counter-intuitive behavior is the result of array supergain solutions which create a variety of practical problems like high antenna currents, ohmic loss, and narrow operating bandwidth [53]. They can be eliminated by introducing practical antenna loss [54]. For this purpose, a loss resistance can be added to the diagonal elements of Bob’s antenna impedance matrix $Z_{BB}$ before computing the S-parameter matrix $S_{BB}$, with the loss resistance $R_{L,m}$.
added to the $m$th array element quantified by the efficiency $\mu_m = \frac{R_{BB,mm}}{R_{BB,mm} + R_{L,m}}$, where $R_{BB,mm}$ is the radiation resistance of the $m$th antenna.

The level of superdirectivity can be computed based on different metrics, where the $Q$ factor which quantifies the useful bandwidth of array is used in this work [55]. The $Q$ factor for Bob’s array can be computed as

$$Q = \frac{\vec{i}_B^\dagger \vec{i}_B}{\vec{i}_B^\dagger (R_{BB} + R_L) \vec{i}_B},$$

(3.58)

where $\vec{i}_B$ is the vector of excitation current and $\{\cdot\}^\dagger$ represents the conjugate transpose. Figure 3.5 plots the $Q$ factor (in dB) as a function of Bob’s array inter-element spacing. A higher $Q$ factor corresponds to a smaller usable bandwidth which can be improved by adding loss resistance. Results indicate that a high $Q$ factor is observed when $d_B < \lambda/4$ with no added loss resistance ($R_L = 0$). However, it is significantly reduced by adding some loss in the array such that $\mu = 0.9$.  

Figure 3.4: Available key rate as a function of Bob’s antenna element spacing ($d_B/\lambda$) for three different matching network conditions when the antenna element efficiency $\mu$ is assumed to be 100%.
Figure 3.5: Q factor as a function of Bob’s antenna element spacing \((d_B/\lambda)\) for two different values of the antenna element efficiency \(\mu\).

Figure 3.6 recreates the plot shown in Figure 3.4 when antenna efficiency is set at \(\mu_1 = \mu_2 = \mu = 0.9\) (90\%). While the optimal match maximizes the received SNR and therefore outperforms the diagonal match, the addition of the loss causes the curve for the optimal match to decrease with the antenna spacing, as expected. Furthermore, as the element spacing increases and coupling decreases, all curves converge. For the remainder of this work, results are computed for receive antennas that are 90\% efficient. Figure 3.6 also shows the result when Bob’s matching network for minimum noise figure is removed, meaning that the match is designed for maximum power transfer, causing a reduction in the SNR. The results show that this suboptimal receiver matching approach leads to a notable degradation in performance.

Figure 3.6 suggests that the key rate is less sensitive than the communication capacity [29] to the choice of the matching network and the resulting differences in SNR. Despite this reduced sensitivity to matching quality, optimal matching does increase the key rate by approximately 10-15\%. To see if this improvement occurs over a range of scenarios, \(I_K\) is examined as a function of SNR and number of clusters \(N_C\) in Figures 3.7 and 3.8, respectively for \(d_B = 0.12\lambda\). Both plots confirm the observation from Figure 3.6 that the
Figure 3.6: Available key rate as a function of Bob’s antenna element spacing \((d_B/\lambda)\) for three different matching network conditions when the antenna element efficiency \(\mu\) is assumed to be 90%.

A performance increase of 10-15% created by the optimal match occurs across the range of parameters considered. The results of Figure 3.8 further reveal that increased multipath richness (as measured by an increased number of clusters \(N_C\)) increases the key rate because it reduces the channel spatial correlation. However, once the correlation reduces to a certain level, additional multipaths offer little additional benefit.

### 3.3.4 Secure Key Rate

Next, the case where an eavesdropper Eve is located close to Bob as shown in Figure 3.1 is analyzed. The amount of information about the key that Eve can extract based on her observations of the training exchange depends upon the correlation between \(h_x\) and \(h_z\), which is related to the distance between Bob and Eve \((d_{BE})\). Two scenarios are analyzed: high coupling for which \(d_B = d_E = 0.12\lambda\) and low coupling for which \(d_B = d_E = 0.5\lambda\). Both Bob’s and Eve’s antennas are included together in a single NEC simulation to generate the radiation patterns and S-parameters that incorporate all coupling mechanisms.
Figure 3.7: Available key rate for $d_B = 0.12\lambda$ as a function of SNR when $N_C = 4$.

Figure 3.8: Available key rate for $d_B = 0.12\lambda$ as a function of the number of clusters $N_C$ when the SNR is 15 dB.
Figure 3.9: Secure key rate as a function of the separation between Bob’s and Eve’s antenna arrays for three different matching network conditions when high coupling ($d_B = d_E = 0.12\lambda$) is assumed.

Figure 3.10: Secure key rate as a function of the separation between Bob’s and Eve’s antenna arrays for three different matching network conditions when low coupling ($d_B = d_E = 0.5\lambda$) is assumed.
Figures 3.9 and 3.10 plot $I_{SK}$ as a function of the Bob-Eve separation $d_{BE}$ for high and low coupling, respectively, and for optimal and diagonal matching at Bob. These results demonstrate that as $d_{BE}$ increases, $I_{SK}$ approaches the value of $I_K$ as the channels $h_x$ and $h_z$ become less correlated. However, as $d_{BE}$ decreases, $I_{SK}$ decreases significantly due to the large channel correlation. The results again show that the optimal matching network can increase the key rate for high coupling by approximately 10-15%. Both plots also show the results when the minimum noise figure (NF) matching network at Bob is removed. Once again, performance is reduced by some extent when suboptimal noise matching is used at the receiver, with the results reinforcing the prior observation that the impact of SNR on the key rate is not as significant as what is often observed for MIMO capacity [29].

Figure 3.11 plots $I_{SK}$ as a function of SNR. The results observed here are similar to those observed for sweeping $I_K$ across SNR. Figure 3.12 plots $I_{SK}$ as function of the number of clusters $N_C$. These results show that even for $N_C = 20$, $I_{SK}$ is not saturated which highlights the fact that a richer multipath environment can enhance the secure key rate even after the available key rate may already be saturated as shown in Figure 3.8.
Figure 3.12: Secure key rate for $d_B = d_E = d_{BE} = 0.12\lambda$ as a function of the number of clusters $N_C$ when the SNR is 15 dB.

Figure 3.13: Secure key rate as a function of the separation between Bob’s and Eve’s antenna arrays for two different matching network conditions with $d_B = d_E = 0.12\lambda$ and all arrays are of equal size with Bob’s and Eve’s arrays parallel to each other.
Figure 3.14: Secure key rate as a function of the separation between Bob’s and Eve’s antenna arrays for two different matching network conditions with $d_B = d_E = 0.12\lambda$. Bob’s and Eve’s arrays are perpendicular with $N_E = 2$ and parallel with $N_E = 4$ when $N_A = N_B = 2$.

Figure 3.13 plots $I_{SK}$ as a function of the Bob-Eve separation for high coupling with optimal and diagonal matching at Bob and for $N_A = N_B = N_E = 3$ and 4. These results demonstrate that while the secure key rate increases with larger array sizes, the basic trends are similar to those observed in Figure 3.10. Figure 3.14 plots the same results when all arrays have two elements but Bob’s and Eve’s arrays are perpendicular as illustrated in the figure, again confirming similar trends to those shown previously. This plot also shows the results when Alice and Bob have two antennas while Eve has four, with the antenna arrangement shown in the figure. Because of Eve’s advantage, $I_{SK}$ is reduced, particularly when Bob and Eve are very close. However, once the Bob-Eve separation increases, the impact of this advantage is reduced. Finally, all of the results in Figures 3.13 and 3.14 demonstrate that under some circumstances, the diagonal match can outperform the optimal match due to the fact that the optimal matching does not take into account the unknown impact of the coupling to Eve’s array.

Based on these observations, it is useful to explore the impact of the cross-array mutual coupling on the key rate performance. The covariances and resulting secure key rate
are evaluated by assuming that $S_{BE} = S_{EB} = 0$ and using the radiation patterns for Bob’s and Eve’s arrays in isolation from each other. Figure 3.15 compares $I_{SK}$ for $S_{BE} = 0$ and $S_{BE} \neq 0$ for both high and low coupling when an optimal matching network is used. As expected, for large values of $d_{BE}$ where $S_{BE} \to 0$, the curves converge. However, for small values of $d_{BE}$, the difference between the two curves increases for both values of array element spacing. Based on this result the cross-array coupling may

1. create an impedance mismatch that reduces the channel estimation SNR,

2. introduce an additional propagation “path” where the signal routes through the eavesdropper to Bob (or Alice), impacting the spatial correlation among the elements of $h_x$ (or $h_y$), or

3. change the cross-correlation of the channels $h_x$ and $h_z$ as represented by the covariance matrix $R_{xz}$.

Items #1 and #2 in the above list will impact $I_K$ as well as $I_{SK}$. Therefore, the data from the simulations is taken with Eve present, but $I_K$ is computed instead of $I_{SK}$, meaning that Eve’s impact is included on the channels $h_x$ and $h_y$ but the computation ignores the information she may intercept. Figure 3.16(a) plots the ratio of $I_K$ when $S_{BE} \neq 0$ to $I_{K,NC}$ when $S_{BE} = 0$ for both high and low coupling. For both coupling levels, as $d_{BE}$ decreases the cross-array coupling reduces $I_K$ relative to the value that exists without coupling. This implies a reduced SNR value and/or increased correlation among the elements of $h_x$ due to Eve’s presence. However, this reduction in $I_K$ is contrary to the increase in $I_{SK}$ observed in Figure 3.15 when cross-array coupling is included.

To investigate item #3 in the above list, the matrices $R_{xz}$ and $R_{xz,NC}$ are computed when $S_{BE} \neq 0$ (cross-array coupling included) and $S_{BE} = 0$ (cross-array coupling neglected), respectively. Since the matrices represent the channel cross-correlations, a lower matrix Frobenius norm indicates reduced similarly between the Alice-to-Bob and Alice-to-Eve channels and therefore increased $I_{SK}$. We form the ratio

$$\gamma = E\left\{ \frac{\|R_{xz}\|_F}{\|R_{xz,NC}\|_F} \right\},$$

(3.59)
Figure 3.15: Secure key rate as a function of $d_{BE}$ with and without cross coupling $S_{BE}$ for optimal matching networks at Bob and Eve: (a) high coupling ($d_B = d_E = 0.12\lambda$); (b) low coupling ($d_B = d_E = 0.5\lambda$).

Figure 3.16: (a) Ratio of $I_K$ for $S_{BE} \neq 0$ to $I_K$ when $S_{BE} = 0$. (b) Average ratio of the Frobenius norm of $R_{xz}$ for $S_{BE} \neq 0$ to that for $S_{BE} = 0$. Both results use optimal matching networks at Bob and Eve.
where $\| \cdot \|_F$ indicates the Frobenius norm. Values of $\gamma$ below unity indicate that cross-array coupling reduces the correlation relative to what would be observed if coupling were not present. Figure 3.16(b) plots $\gamma$ as a function of $d_{BE}$, where the expectation is approximated by averaging over 400 channel realizations. As $d_{BE}$ decreases beyond about $\lambda/4$, $\gamma$ drops dramatically, indicating that for a given value of $d_{BE}$ inclusion of the cross-array coupling reduces the correlation between the channels observed by Bob and Eve. This cross-channel correlation reduction more than offsets the decrease in SNR or increase in correlation among the elements of $h_x$, resulting in the observed behavior from Figure 3.15 that $I_{SK}$ when cross-array coupling is included is higher than that observed when cross-array coupling is neglected. Note that this is a reduction relative to what would be observed if cross-array coupling were ignored, as even with this coupling decreasing separation $d_{BE}$ increases the cross-channel correlation and reduces the secure key rate.

3.4 Chapter Summary

This chapter shows the analysis of key rate performance of a MIMO communication system that uses bi-directional channel estimation to establish secret encryption keys. The analysis incorporates the impact of antenna mutual coupling, the impedance match between the arrays and the circuitry, and a realistic noise model for LNAs in order to precisely characterize the overall performance. Moreover, the formulation includes the additional complexity of an eavesdropper whose antennas may be very close to and therefore coupled with the antennas of one of the legitimate nodes. The results show that high mutual coupling impacts the key rate performance, and that use of practical matching can degrade the key rate performance by 10-15% relative to the performance when less practical but optimal impedance matching is implemented. Furthermore, the results show that cross coupling between the arrays of the legitimate node and eavesdropper reduces the correlation between the channels observed by these two nodes and therefore increases the secure key rate realized.
Chapter 4

Non-Reciprocal Radio System Calibration for Propagation-Based Key Establishment

Prior studies on propagation-based key establishment have assumed that the wireless channel used for key generation is reciprocal and have ignored the fact that typical radios have different signal paths during transmit and receive, introducing non-reciprocal contributions to the overall channel that includes the radio analog circuitry. While it is possible to measure the transfer function of these portions of the circuit in the factory and store them in the radio for use during key establishment [56], changing environmental conditions and device aging can alter these responses from their initial values, suggesting the need for a protocol that allows periodic calibration during radio operation [57].

Because multiple-input multiple-output (MIMO) communication systems can benefit from channel reciprocity in certain applications, prior work has appeared on radio calibration. One approach uses dedicated hardware paths to allow periodic measurement of the transmit and receive circuit transfer functions [58, 59], although this adds hardware complexity and does not incorporate antenna array mutual coupling. An alternate approach is to use relative calibration based on bidirectional channel estimation and a total least squares (TLS) calibration algorithm to construct reciprocal channel estimates from the non-reciprocal observations [60, 61], avoiding the deliberate design of calibration circuit paths. Recent work has demonstrated practical application of the method to MIMO communication algorithms [62]. Despite these contributions, no prior work has appeared illustrating application of radio calibration to channel-based encryption key establishment.

The objective of this chapter is to demonstrate the impact of channel non-reciprocity on propagation-based key establishment performance and to study the effectiveness of a practical calibration method based on the TLS algorithm that enables the two nodes to obtain
the same channel estimate despite the non-reciprocal contributions of the radio circuitry. The MIMO radio system model used for this study is similar to the one used in Chapter 3 and incorporates transmit sources and receiver loads, impedance matching networks, low-noise amplifiers (LNAs), mutually coupled antennas, and an eavesdropper [56]. The analysis shows that non-reciprocal channel contributions from matching networks and LNAs reduces key establishment performance, but that application of the TLS calibration is highly effective in removing the impact of such non-reciprocal channel elements over a range of operational parameters [63, 64]. The training required for effective method implementation increases as the number of antennas increases or the signal-to-noise ratio (SNR) decreases.

4.1 System Model

Figure 4.1 shows the radio model used for this analysis. This model is a modification of the model used in Figure 3.1 to study the impact of antenna array mutual coupling on channel-based key establishment performance. Therefore, only a brief summary of the analysis is presented in this chapter to highlight the mathematics required to perform system calibration, relying on Fig. 4.1 to define most of the S-parameters and traveling waves discussed.

Alice and Bob are two radios with $N_A$ transmit and $N_B$ receive antennas, respectively, and Eve is a passive eavesdropper with $N_E$ receive antennas. Each circuit component is represented by a S-parameter matrix, and signals are modeled using forward and reverse traveling waves $a_\xi$ and $b_\xi$ respectively, where $\xi$ assumes the different designations shown in Fig. 4.1. The matching networks either maximize the power transfer to/from the antennas or minimize the noise figure of the low-noise amplifiers (LNAs). S-parameter matrices of matching networks and amplifiers are block matrices of the form

$$S = \begin{bmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{bmatrix},$$  \hspace{1cm} (4.1)$$

where $S_{ij}$ relates the vector of waves exiting ports $i$ to the vector of waves incident on ports $j$. Furthermore, it is assumed that Eve and Bob can be physically close enough to each other that their antennas will experience cross-array mutual coupling, leading to a full S-parameter
matrix for these two antenna arrays of

\[ \begin{bmatrix} S_{BB} & S_{BE} \\ S_{EB} & S_{EE} \end{bmatrix}, \tag{4.2} \]

where the diagonal terms represent the reflection coefficient matrices for Bob’s and Eve’s arrays (which include any mutual coupling within the array) and the off-diagonal terms represent cross-array mutual coupling. Because channel-based key establishment depends on Alice and Bob both obtaining an estimate of the channel transfer function through training, both the forward channel (Alice transmitting to Bob) and reverse channel (Bob transmitting to Alice) transfer functions are formulated.

### 4.1.1 Forward Channel Transfer Function

Mathematically formulating the forward channel transfer function requires writing an expression for the output wave \( a_{LB} \) as a function of the input wave \( a_{TA} \). To begin, the wave...
incident on Alice’s antenna terminals can be written as
\[
a_A = (I - S_{TA,22}S_{AA})^{-1}S_{TA,21} a_{TA}, \tag{4.3}
\]
where \( I \) is the identity matrix.

The incoming wave at Bob is
\[
a_B = b_{SB} + S_{BB}b_B + S_{BE}b_E, \tag{4.4}
\]
where \( b_{SB} \) represents the waves out of Bob’s antennas when they are terminated with matched loads. To determine \( b_{SB} \) and \( b_E \), the network theory framework detailed in Chapter 3 is applied. The term \( b_{SB} \) can be expressed as
\[
b_{SB} = [(I - S_{BB})H_{BA} - S_{BE}H_{EA}] (I - S_{AA}) a_A, \tag{4.5}
\]
where \( H_{BA} \) and \( H_{EA} \) refer to the physical propagation channels shown in Fig. 4.1. Also, \( b_E \) can be constructed as
\[
b_E = (I - \Gamma_{E}S_{EE})^{-1}[\Gamma_{E}b_{SE} + \Gamma_{E}S_{EB}b_B + n_E], \tag{4.6}
\]
where
\[
b_{SE} = [(I - S_{EE})H_{EA} - S_{EB}H_{BA}] (I - S_{AA}) a_A, \tag{4.7}
\]
\[
n_E = S_{RE,12}(I - \Gamma_{GE}S_{RE,22})^{-1}(b_{RE} - \Gamma_{GE}a_{RE}), \tag{4.8}
\]
\[
\Gamma_{GE} = S_{GE,11} + S_{GE,12}\Gamma_{LE}(I - S_{GE,22}\Gamma_{LE})^{-1}S_{GE,21}, \tag{4.9}
\]
\[
\Gamma_{E} = S_{RE,11} + S_{RE,12}\Gamma_{GE}(I - S_{RE,22}\Gamma_{GE})^{-1}S_{RE,21}, \tag{4.10}
\]
and the terms \( a_{RE} \) and \( b_{RE} \) represent the noise contribution from Eve’s LNAs \[56\].
Substituting (4.5) and (4.6) into (4.4) and using (4.3) yields,

\[ a_B = S_{BA}C_{TA}a_{TA} + \Gamma_{BE}b_B + \Theta_{BE}n_E, \]  

(4.11)

where

\[ \Theta_{BE} = S_{BE}(I - \Gamma_E S_{EE})^{-1}, \]  

(4.12)

\[ S_{BA} = F_B + \Theta_{BE}\Gamma_E F_E, \]  

(4.13)

\[ \Gamma_{BE} = S_{BB} + \Theta_{BE}\Gamma_E S_{EB}. \]  

(4.14)

Finally, the outgoing wave \( a_{LB} \) from Bob's LNA can be expressed as

\[ a_{LB} = C_{RB}S_{BA}C_{TA}a_{TA} + \eta_B, \]  

(4.15)

where

\[ C_{RB} = (I - \Gamma_{GB}\Gamma_{LB})^{-1}\Theta_{GB}\Theta_B, \]  

(4.16)

\[ \Theta_B = S_{RB,21}(I - \Gamma_{BE}S_{RB,11})^{-1}, \]  

(4.17)

\[ \Theta_{GB} = S_{GB,21}(I - \Gamma_B S_{GB,11})^{-1}, \]  

(4.18)

\[ \Gamma_B = S_{RB,22} + \Theta_B\Gamma_E S_{RB,12}, \]  

(4.19)

\[ \Gamma_{GB} = S_{GB,22} + \Theta_{GB}\Gamma_B S_{GB,12}, \]  

(4.20)

\[ \eta_B = C_{RB} \left[ \Theta_{BE}n_E + \Theta_B^{-1}(\Gamma_B b_{\eta B} - a_{\eta B}) \right], \]  

(4.21)

and \( a_{\eta B} \) and \( b_{\eta B} \) model Bob's LNA noise.

While this analysis involves significant algebraic complexity, the simple final form of (4.15) represents the noise free channel transfer function in terms of the reciprocal channel contribution \( S_{BA} \) and the non-reciprocal channel contributions \( C_{TA} \) and \( C_{RB} \). It is important to recognize that to compute key establishment performance, the transfer function from Alice to Eve needs to be formulated. This can be accomplished using a straightforward modification of (4.15) as detailed in Chapter 3.
4.1.2 Reverse Channel Transfer Function

The basic analysis for the case of Bob transmitting to Alice mirrors that in Section 4.1.1 under the following assumptions:

1. The antennas at all nodes and the propagation media are reciprocal. This means that $S_{EB} = S_{BE}^{T}$, $H_{AB} = H_{BA}^{T}$, and $H_{AE} = H_{EA}^{T}$, where $\{\cdot\}^{T}$ is a matrix transpose. It also means that $S_{\xi\xi} = S_{\xi\xi}^{T}$, where $\xi \in [A, B, E]$, and therefore $F_{B}^{T}$ and $F_{E}^{T}$ describe the propagation from Bob to Alice and Eve to Alice, respectively.

2. Because Eve is a passive eavesdropper, her radio remains in the same state regardless of who is transmitting.

3. Bob’s transmit circuitry becomes a matching network to maximize power transfer, and Alice’s receive circuitry becomes LNAs (including the minimum noise figure matching network) and terminations.

4. Eve’s LNA noise is insignificant relative to Alice’s LNA noise and therefore is disregarded in the analysis.

5. The directions of $a_{\xi}$ and $b_{\xi}$ for $\xi \in [A, B]$ are reversed and the signal incident on Bob’s matching network is designated as $a_{TB}$ and that incident on Alice’s loads is designated as $a_{LA}$. If a symbol used in this analysis is the same as a symbol used in Section 4.1.1 but with a change in subscript (A to B or B to A), then the subscripts are changed within any expressions defining those symbols.

These assumptions allow a relatively simple summary of the analysis. First, $a_{B}$ can be written as

$$a_{B} = \frac{(I - S_{TB,22}^{T} \Gamma_{BE})^{-1} S_{TB,21}^{T} a_{TB}}{c_{TB}}$$

(4.22)

where in comparison with (4.3), $\Gamma_{BE}$ has replaced the role of the transmit antenna reflection coefficient matrix because of the coupling between Bob and Eve.
When constructing \( b_E \), the analysis leading to (4.6) can be used without the noise or the term due to propagation from Alice. The result is

\[
b_E = (I - \Gamma_E S_{EE})^{-1} \Gamma_E S_{EB} C_{TB} a_{TB}.
\] (4.23)

The signal out of Alice’s antennas when terminated with matched loads is then

\[
b_{SA} = F_B^T b_B + F_E^T b_E.
\] (4.24)

Using these results, the final reverse transfer function becomes

\[
a_{LA} = C_{RA} S_{AB} C_{TB} a_{TB} + \eta_A.
\] (4.25)

where

\[
C_{RA} = (I - \Gamma_{GA} \Gamma_{LA})^{-1} \Theta_{GA} \Theta_A,
\] (4.26)

\[
\eta_A = C_{RA} \Theta_A^{-1} (\Gamma_A b_{\eta A} - a_{\eta A}).
\] (4.27)

### 4.2 Calibration Algorithm and Performance

The goal of system calibration is to remove the differences between the channels observed by Alice and Bob due to non-reciprocity, recognizing that each will be estimating their channels independently and therefore subject to independent channel estimation errors. From (4.15) and (4.25), and recognizing that because of the assumptions of reciprocal antennas and propagation media \( S_{AB} = S_{BA}^T \), \( H_x \) can be written as

\[
H_x = C_{RB} C_{TB}^{-T} H_y^T C_{TA}^{-T} C_{TB}.
\] (4.28)

The calibration objective is to find the calibration matrices \( C_A \) and \( C_B \) such that Alice can compute an estimate of \( H_x \) based on her estimate of \( H_y \). Since both Alice and Bob then have the same channel estimate (ignoring noise/channel estimation errors), they can each
use their estimate to form a secret encryption key. Of course, inaccurate construction of
the calibration matrices will diminish the agreement of the keys created at each radio and
therefore reduce key establishment performance. The metrics that quantify this performance
are provided in Section 4.2.2.

4.2.1 Total Least Squares (TLS) Calibration

Calibration involves $K$ channel measurements. During the $k$th measurement, Alice
and Bob exchange pilot signals from which Bob estimates $\hat{H}_{x,k}$ and Alice estimates $\hat{H}_{y,k}$,
where $\{\cdot\}$ is used to designate that the quantity is an estimate. Bob transmits his estimate
$\hat{H}_{x,k}$ to Alice so that she knows both channel estimates. Note that, since Bob transmits his
channel estimate publicly, the channel estimates used during calibration cannot be used for
key establishment.

For the $k$th measurement (4.28) can be re-written as

$$\hat{H}_{x,k} C_B^{-1} - C_A \hat{H}_y^T = 0$$  \hspace{1cm} (4.29)

or equivalently as

$$\begin{bmatrix} I_N \otimes \hat{H}_{x,k} - \hat{H}_{y,k} \otimes I_N \end{bmatrix} \begin{bmatrix} \text{vec}(C_B^{-1}) \\ \text{vec}(C_A) \end{bmatrix} = 0,$$  \hspace{1cm} (4.30)

where $\otimes$ is a Kronecker product, $I_N$ is an $N \times N$ identity matrix, and vec{$\cdot$} forms a column
vector by stacking its argument columnwise. Stacking all $K$ measurements into a single
matrix expression produces the overdetermined system

$$\begin{bmatrix} L_1^T & \ldots & L_K^T \end{bmatrix}^T \begin{bmatrix} \text{vec}(C_B^{-1}) \\ \text{vec}(C_A) \end{bmatrix} = 0.$$  \hspace{1cm} (4.31)

Eq. (4.31) can be solved using TLS [60]. The number of channel measurements required for
calibration are chosen such that $K > N_B/N_A + N_A/N_B$, and the singular value decomposition
$L = U \Sigma V^H$ is performed, where $U$ and $V$ are unitary matrices of singular vectors and $\Sigma$ is
a diagonal matrix of real singular values. The estimate \( \hat{c} \) of \( c \) is a scalar \( \alpha \) times the singular vector of \( V \) corresponding to the smallest singular value in \( \Sigma \). According to (4.30), the unknown scalar \( \alpha \) is in the numerator and denominator of the estimated calibration matrices \( \hat{C}_A \) and \( \hat{C}_B \), respectively. It therefore disappears when Alice computes the calibrated reverse channel

\[
\hat{H}_x' = \hat{C}_A \hat{H}_y^T \hat{C}_B
\]  

(4.32)

based on her channel estimate \( \hat{H}_y \). In the absence of estimation errors, \( H_x' = H_x \), and therefore Bob and Alice have the same channel coefficients for encryption key generation.

4.2.2 Key Rate

The information theoretic key rate represents the theoretical maximum number of key bits that can be generated from a single observation of the channel by Alice and Bob. The available key rate \( I_K \) ignores the presence of Eve and therefore effectively quantifies the similarity between the final channel estimates. For Gaussian channel coefficients and letting \( \hat{h}_i \) represent the reverse channel estimate, \( I_K \) can be computed in closed form [17] as

\[
I_K = I(\hat{h}_x; \hat{h}_r) = \log_2 \frac{|\hat{R}_{xx}| |\hat{R}_{rr}|}{|\hat{R}_{XR}|},
\]  

(4.33)

where \( \hat{h}_x = \text{vec}\{\hat{H}_x\} \), \( \hat{h}_r = \text{vec}\{\hat{H}_r\} \), \( |·| \) is the determinant, \( I(·;·) \) is the mutual information, \( \hat{R}_{\xi\psi} = E\{\hat{h}_\xi \hat{h}_\psi^\dagger\} \), \( E\{·\} \) is an expectation, \( \{·\}^\dagger \) is a conjugate transpose, and

\[
\hat{R}_{XR} = E\{[\hat{h}_x^\dagger \hat{h}_r^\dagger][\hat{h}_x^\dagger \hat{h}_r^\dagger]\}.
\]  

(4.34)

The secure key rate \( I_{SK} \) quantifies the number of key bits that can be generated per channel observation that are secure from the eavesdropper and is given by

\[
I_{SK} = I(\hat{h}_x; \hat{h}_r | \hat{h}_z) = \log_2 \frac{|\hat{R}_{xz}| |\hat{R}_{RZ}|}{|\hat{R}_{zz}| |\hat{R}_{XRZ}|},
\]  

(4.35)
where \( \hat{h}_z \) is the columnwise stacked version of the channel observed by Eve and the covariances with upper case subscripts are defined based on (4.34). Details on the computation of the signal and noise covariance matrices required to compute \( I_K \) and \( I_{SK} \) are presented in Chapter 2.

4.3 Performance Evaluation

Simulations are used to demonstrate the performance of the calibration procedure. Several aspects of the simulations require some discussion.

4.3.1 Matching Network Design

All matching networks are designed such that they are lossless and reciprocal, and the design procedure is detailed in Appendix A for maximizing power transfer or minimizing LNA noise figure. As discussed in Chapter 3, two different levels of matching network design complexity are considered in this work. The \textit{Optimal Matching Network} (OMN) is designed using the full S-parameter matrix of the antenna array and therefore introduces cross-port coupling to compensate for the antenna coupling. The \textit{Diagonal Matching Network} (DMN) is designed using only the diagonal elements of the array S-parameter matrix, meaning that when coupling is significant, the matching network will not achieve the design goal (maximum power or minimum noise figure).

In the following, when the matching is specified as OMN or DMN, it applies to the matching network at both Alice and Bob. When computing \( I_{SK} \), Eve is given the advantage of always having an optimal minimum noise figure matching network with the assumption that there is no error in her knowledge of her calibration matrices.
4.3.2 Calibration Error Modeling

The S-parameters of a lossless, reciprocal matching network can be expressed as [56]

\[ S_{11} = U_{11} \Lambda_{11}^{1/2} U_{11}^T \]
\[ S_{12} = jU_{11}(I - \Lambda_{11})^{1/2} U_{22}^T \]
\[ S_{21} = jU_{22}(I - \Lambda_{11})^{1/2} U_{11}^T \]
\[ S_{22} = U_{22} \Lambda_{11}^{1/2} U_{22}^T, \]  \hspace{1cm} (4.36)

where \( U_{ii} \) is the unitary matrix of left singular vectors of \( S_{ii} \) and \( \Lambda_{11} \) is the diagonal matrix of real singular values of \( S_{11} \). The design procedure in Appendix A specifies these matrices based on the design goals. Once they are specified, phase error can be introduced into the design through the simple transformations

\[ \overline{U}_{11} = P^{(1)} U_{11} P^{(2)}, \]
\[ \overline{U}_{22} = P^{(3)} U_{22} P^{(4)}, \]  \hspace{1cm} (4.37)

where \( P^{(i)} \) is the \( i \)th realization of a diagonal matrix with \( m \)th diagonal entry \( e^{j\phi_m} \), \( \phi_m \) is an independent random variable uniformly distributed over \([-\phi_{max}, \phi_{max}]\), and \( \phi_{max} \) is the maximum phase error. Modified matching network S-parameters are computed from (4.36) with \( \overline{U}_{ii} \) in place of \( U_{ii} \).

The modified S-parameters are used to compute the forward and reverse channels observed by Alice and Bob, and the calibration procedure is applied to these observations to estimate the calibration matrices for these modified channels. In a real system, because different matching networks are used by a radio depending on whether it is transmitting or receiving, the S-parameters will drift independently for forward and reverse channels, and therefore that is the default behavior in the simulations. However, the case where only the S-parameters for the reverse channel drift is also considered to demonstrate the impact of this error introduction without the added complexity of error being modeled in both channels.
The gain errors can also be introduced in the model through the LNA gains. However, simulations show that such gain errors have minimal impact on performance, and therefore all simulations shown here are limited to the case of matching network phase errors.

4.3.3 Signal-to-Noise Ratio (SNR)

SNR is defined in two different ways. In the first case, the channel covariance $R_{\xi\xi}^{(10\lambda)}$ for $\xi \in [x,y,z]$ is computed assuming the array element spacing is $d_\xi = 10\lambda$, where $\lambda$ is the free space wavelength, and the noise covariance $R_{\eta,\xi\xi}^{(10\lambda)}$ is scaled such that the SNR computed as

$$\text{SNR}_{10\lambda} = \frac{\text{Tr}\{R_{\xi\xi}^{(10\lambda)}\}}{\text{Tr}\{R_{\eta,\xi\xi}^{(10\lambda)}\}}$$

(4.38)

achieves the specified value, where Tr{·} is the matrix trace. Once this noise is specified, it is used for all antenna configurations and therefore demonstrates the impact of reduced SNR due to imperfect impedance matching. In the second case, the channel covariance matrix $R_{\xi\xi}$ is computed for each antenna spacing and the noise covariance $R_{\eta,\xi\xi}$ is scaled such that the SNR computed as

$$\text{SNR}_C = \frac{\text{Tr}\{R_{\xi\xi}\}}{\text{Tr}\{R_{\eta,\xi\xi}\}}$$

(4.39)

achieves the specified value for each spacing. This definition removes changes in SNR as a factor in determining the key rate. Unless otherwise stated, a SNR of 15 dB is used.

4.3.4 Results

In all simulations, the antennas are half-wave dipoles ($\lambda/2$), and unless otherwise stated, $N_A = N_B = N_E = 2$. The element spacing for Alice is $d_A = \lambda/2$, while $d_B$ and $d_E$ can vary (see inset in Fig. 4.1). When computing $I_{SK}$, the separation $d_{BE}$ also varies. All antennas are modelled using the Numerical Electromagnetics Code (NEC) to obtain their open-circuit radiation patterns and full (coupled) S-parameter matrices. The arrays of Bob and Eve are simulated as a single array to capture the cross-array mutual coupling. The propagation channel is realized using a simple path based model, where $N_P = 10$ distinct paths are realized, each with its own complex gain, angle of departure, and angle of arrival.
Figure 4.2: Available key rate $I_K$ as a function of the maximum phase error $\phi_{\text{max}}$ for the Reference and Error scenarios when error is applied to the reverse (Rev) or both the forward and reverse (Fw, Rev) channels for both optimal (OMN) and diagonal (DMN) matching networks when $\text{SNR}_{10\lambda} = 15$ dB.

For simplicity, it is assumed that path gains and angle of arrival/departure are the same at both Bob and Eve.

Results for three channel reciprocity conditions appear in the following. For the Reference condition, $\hat{h}_r = \hat{h}_x$, meaning the forward and reverse channels are identical. Note that if errors are introduced in the forward channel $\hat{h}_x$, then the forward channel impedance match will be degraded and performance will decrease. For the Error condition, the errors are introduced in the channels but calibration is not applied before computing the key rates, or $\hat{h}_r = \hat{h}_y$. Finally, for the Calibration condition, it is assumed that $\hat{h}_r = \hat{h}_x'$ which is computed using TLS calibration. Unless otherwise stated, $K = 50$ channel realizations are used for calibration.

It is first useful to demonstrate the impact of calibration matrix error on the key rate $I_K$ as a function of the maximum phase error $\phi_{\text{max}}$. Figure 4.2 plots the results averaged over $N_R = 10,000$ error realizations of $\mathbf{U}_{11}$ and $\mathbf{U}_{22}$, where $\phi_m$ is uniformly distributed for $d_B = 1\lambda$ and $\text{SNR}_{10\lambda} = 15$ dB for both Reference and Error conditions and when errors are
Figure 4.3: Available key rate $I_K$ for Case 1 as a function of Bob’s array spacing $d_B$ when either $\text{SNR}_C$ or $\text{SNR}_{10\lambda}$ are fixed at 15 dB for both optimal (OMN) and diagonal (DMN) matching networks.

applied only to the reverse channel or to both. Note that when errors are applied only to the reverse channel, the *Reference* condition suffers no degradation as the reverse channel for *Reference* case is set to the forward channel, where the forward channel is error free. However, for *Error* case the reverse channel is not set to the forward channel, and we see performance degradation due to the error in the reverse channel.

When the forward channel also has errors, the *Reference* case suffers because of the imperfect match, although the forward and reverse channels are same. It is also noticed that introducing phase errors in both channels effectively doubles the penalty relative to errors in only the reverse channel, and that the performance using OMN is more sensitive to errors than when using DMN, likely because it takes little perturbation to disturb the perfect design whereas the DMN is suboptimal even without the introduction of explicit errors. Finally, Fig. 4.2 shows that the key rate degradation with phase error can be significant. Based on these results, the remaining simulations use $\phi_{\text{max}} = 45^\circ$. 
**Figure 4.4:** Achieved average SNR$_C$ as a function of Bob’s array spacing $d_B$ for forward ($\hat{h}_x$), reverse ($\hat{h}_r$) and calibrated channel ($\hat{h}_{x'}$) covariance matrices when SNR$_{10\lambda} = 15$ dB for both optimal (OMN) and diagonal (DMN) matching networks.

**Case 1 – Error in Reverse Channel**

It is first assumed that calibration errors are introduced only in the reverse channel, meaning that the *Reference* result suffers no impedance mismatch. Figure 4.3 plots the available key rate $I_K$ versus Bob’s array spacing $d_B$ when Bob has an optimal or diagonal matching network for both SNR$_{10\lambda} = 15$ dB and SNR$_C = 15$ dB. These results reveal that while incorporation of error reduces $I_K$ by approximately 5%, application of the TLS calibration effectively recovers all of the lost performance. The overall performance degradation for diagonal matching relative to that for optimal matching observed when SNR$_{10\lambda}$ is held constant is simply a result of the fact that the non-exact diagonal matching has a lower realized SNR when antenna coupling is high. Regardless, the TLS calibration is effective for both types of matching network.

The observed reduction in $I_K$ created by calibration error can be caused by 1) SNR mismatch between the forward and reverse channels (observed only when using SNR$_{10\lambda}$), 2) increased correlation within the elements of the reverse channel vector $\hat{h}_r$, and/or 3) reduced correlation between the forward and reverse channels $\hat{h}_x$ and $\hat{h}_r$. Therefore each of these
contributors are explored. Figure 4.4 plots $\text{SNR}_C$ for the forward, reverse, and calibrated channel covariance matrices. These results reveal that an SNR mismatch occurs, with the reverse channel SNR being lower for the optimal match for high coupling ($d_B < 0.4\lambda$) and higher for the diagonal match for low coupling ($d_B > 0.3\lambda$). Given this observation, for the remainder of this chapter, this SNR inconsistency is removed by setting $\text{SNR}_C = 15$ dB so that SNR is independent of antenna coupling and matching.

Next, the correlation is considered. The off-diagonal elements of the matrix $\mathbf{R}_{\xi\xi}$ quantify the similarity between different channel coefficients within a single channel, with higher correlation resulting in reduced key rate since it means that each channel coefficient offers reduced independent information. Figure 4.5(a) plots the maximum correlation coefficient (normalized correlation with a peak of unity) taken from all off-diagonal elements of the correlation matrix for the forward, reverse and calibrated channels. Recalling that only the reverse channel has errors introduced, it is observed that these errors increase the channel correlation, but that the calibration effectively reduces the correlation back to the levels of
Figure 4.6: Secure key rate $I_{SK}$ as a function of the Bob-Eve array separation $d_{BE}$ ($d_B = 0.12\lambda$) for Case 1 for both optimal (OMN) and diagonal (DMN) matching networks.

the error-free forward channel. Figure 4.5(b) plots the averaged cross correlation coefficient between the channel pairs $(\hat{h}_x, \hat{h}_y)$ and $(\hat{h}_x, \hat{h}_x')$. The error reduces the diagonal entries in the cross-correlation, which represents the correlation between the same channel coefficients observed by Alice and Bob (desired to be one). The error also increases the correlation between different channel coefficients, which is undesired for key establishment. However, once again, the calibration improves the overall correlation.

Finally, Figure 4.6 plots $I_{SK}$ as a function of the Bob-Eve array spacing $d_{BE}$ when $d_B = 0.12\lambda$. As previously indicated, Eve’s calibration is assumed perfect, but the impact of calibration errors in the reverse channel due to Bob and Alice reduces $I_K$ as well as $I_{SK}$. As expected, TLS calibration overcomes the reduced performance in terms of $I_{SK}$ for both matching network types. Since the Reference and Calibration results are virtually indistinguishable, the Reference results are omitted for the remainder of this chapter.

Case 2 – Error in Forward and Reverse Channels

While including error only in the reverse channel has allowed to study the impact of channel errors and calibration on the underlying contributors to key rate, such a situation
is not realistic. In this case, errors are included in both forward and reverse channels. Figure 4.7 compares both key rates for Cases 1 and 2 for optimal matching networks. As expected $I_K$ reduces beyond that observed for Case 1 as error is incorporated in the forward channel, although the relative difference between the Error and Calibration results remains approximately the same. While it may seem that the Calibration results should be identical for both Cases 1 and 2, it is important to remember that the calibration simply makes the forward and reverse channels the same, but it can not compensate for the SNR reduction created by errors in the matching network. Figure 4.8 presents a similar comparison when diagonal matching networks are used. Overall the results are similar to the one observed for the optimal matching network, apart from the fact that impact of error is slightly reduced due to the fact that the diagonal matching networks are already suboptimal.

This case is also used to explore the impact of increasing the array size as well as using different numbers of channel observations during the calibration phase. Since the matching network type does not materially impact the trends observed, only the diagonal matching networks are used for this analysis. Figure 4.9 plots the key rates for $N_A = N_B = N_E = 3$
and for $K = 10$ and 50. The Reference results are included here, as using $K = 10$ does not achieve error free calibration under any conditions and even using $K = 50$ does not achieve perfect calibration for certain conditions with the larger array sizes. These results suggest that with larger array sizes, more channel observations are required to achieve accurate calibration.

Finally, the fractional error $(I_{K,\text{Ref}} - I_{K,\text{Cal}})/I_{K,\text{Ref}}$ is computed, where ‘Ref’ indicates Reference and ‘Cal’ indicates Calibration results. Figure 4.10 plots the percentage fractional error as a function of SNR$_C$ when there is high ($d_B = 0.12\lambda$) and low ($d_B = 1\lambda$) mutual coupling in Bob’s array for $N_A = N_B = 3$. The curve marked ‘Error’ is computed by substituting $I_K$ for the Error result in place of $I_{K,\text{Cal}}$. Results for different numbers of channel observations used in the calibration phase demonstrate that the error increases for low $K$, especially at low SNR. The results also show that reduced antenna mutual coupling reduces the complexity of the calibration estimation since fewer channel observations are required to achieve the same error performance.
Figure 4.9: Available key rate $I_K$ as a function of $d_B$ and secure key rate $I_{SK}$ as a function of $d_{BE}$ ($d_B = 0.12\lambda$) when $K = 10$ or 50, where calibration error is added in both transmit and receive matching networks and $N_A = N_B = N_E = 3$.

Figure 4.10: Percentage fractional error in $I_K$ before and after calibration as a function of SNR$_C$ for several values of $K$, where $N_A = N_B = 3$ for two different values of Bob’s element spacing $d_B$. 
Case 3 – Error in Receiver

As a final case, calibration error is assumed in both the forward and reverse channels but only incorporated into the minimum noise figure matching network at the receivers. Figure 4.11 compares both key rates for Cases 2 and 3 for optimal matching networks. While the overall reduction in channel error does increase the key rates for both cases, the fact that this increase in key rate is small suggests that errors at the receiver dominate the performance under the SNR normalization protocol. Figure 4.12 presents a similar comparison when diagonal matching networks are used. Once again, the impact of the errors is reduced due to the suboptimal diagonal matching.

4.4 Chapter Summary

This chapter formulates a detailed model of a wireless communication system that incorporates non-reciprocal contributions to the channel transfer function due to the radio frequency circuitry and uses the model to demonstrate the performance degradation created by the non-reciprocal channel elements for propagation-based secret key establishment. It
also explores use of a TLS calibration method that allows one of the two radios to estimate the non-reciprocal contributors to the channel and use them to compute a channel transfer function that matches that observed by the other radio. Simulation results show that the method is effective and enables high key establishment performance. However, as the number of antennas or the degree of mutual coupling increases and as SNR decreases, the complexity of the calibration phase must increase in order to maintain performance. Overall, the method appears practical for implementation in operational radio systems.

Figure 4.12: Available key rate $I_K$ as a function of $d_B$ and secure key rate $I_{SK}$ as a function of $d_{BE}$ ($d_B = 0.12\lambda$) when error is applied only to the receive matching network (Case 3) versus both transmit and receive matching networks (Case 2) for diagonal matching networks.
Chapter 5

Impact of Propagation on the Vulnerability of Channel-Based Key Establishment

5.1 Introduction

While the performance of key generation is bounded by the available key rate, this quantity ignores the information about the key inferred by a passive eavesdropper whose channel is correlated with that between the two communicating nodes. This deficiency can be overcome by bounding performance using the more realistic secure key rate that incorporates the impact of this correlation [17]. Chapters 3 and 4 have focused on the impact of mutual coupling and reciprocity on key generation using the wireless propagation channel and have used both available key rate and secure key rate to quantize the performance, but with little real commentary on the relationship between these quantities.

The secure key rate as a performance metric is optimal, but the legitimate nodes do not possess information regarding the eavesdropper channel observations and therefore cannot compute this quantity. Furthermore, recent work has identified techniques for maximizing the available key rate, but these techniques have not been applied to the secure key rate due to its more complicated mathematical form [65, 66]. It is therefore useful to explore the quantitative relationship between the available and secure key rates for different propagation conditions to enable understanding regarding when it is acceptable to use the available key rate as a surrogate for the more complex secure key rate. While recent work has provided some simple simulations and measurements that provide such a comparison [17, 38], past simulations have given little consideration to different propagation conditions, and past experiments provide too limited an opportunity to explore the impact of these conditions on the observed differences in the key rates.
This chapter analyzes the relationship between available and secure key rates by first formulating a model from which these key rates can be computed. The analysis extends recent work on analytical computation of multi-antenna spatial correlation [28] to a multi-user scenario where the multipath structure at one of the legitimate nodes and a nearby eavesdropper has related but different characteristics. This formulation is then used with an experimentally-validated cluster-based model of the propagation that provides the relationship between the multipath characteristics at the two displaced nodes [52]. Finally, this combined model is applied to explore the impact of propagation and system conditions such as $K$-factor, cluster angular spread, and array sizes on the different key rates. The results show that the simpler available key rate is a reasonably accurate representation of the secure key rate provided that the separation between the eavesdropper and a legitimate node is greater than 2.5 wavelengths and the propagation $K$-factor is lower than 0 dB. The results also show that using a simple model for the multipath where the eavesdropper and nearby legitimate node observe the same multipath characteristics can significantly over predict the fraction of bits that are vulnerable to the eavesdropper.

5.2 System Model and Analysis

Figure 5.1 presents the multiple-input multiple-output (MIMO) communication model considered, where Alice and Bob use $N_A$ and $N_B$ antennas, respectively, to communicate securely in the presence of a passive eavesdropper (Eve) who observes the communication using $N_E$ antennas. In comparison with Chapters 3 and 4, a simplified system model is considered in this work to focus on the propagation channel. Furthermore, slightly different notation is used in this chapter for the propagation channel and covariance matrices to make the mathematical analysis more clear and understandable. The element $H_{mn}^{(B)}$ of the $N_B \times N_A$ matrix $H^{(B)}$ is the narrowband transfer impedance that gives the open-circuit voltage on Bob’s $m$th antenna for unit driving current on Alice’s $n$th antenna. If the $N_B \times N_A$ matrix $H^{(A)}$ similarly represents a transfer impedance for transmission from Bob to Alice arranged such that the matrix element row and column indices again correspond to the antenna indices at Bob and Alice, respectively, then for reciprocal antennas and propagation media,
$H^{(B)} = H^{(A)}$. Similar definitions exist for the $N_E \times N_A$ matrix $H^{(E)}$ and $N_E \times N_B$ matrix $H^{(E')}$ shown in Figure 5.1.

Alice and Bob each in turn transmit known training sequences to the other at the same frequency. Alice uses her received waveform to form her estimate $\hat{H}^{(A)}$ of the actual channel $H^{(A)}$, and Bob similarly forms the estimate $\hat{H}^{(B)}$ of the actual channel $H^{(B)}$. This training allows Eve to obtain estimates $\hat{H}^{(E)}$ and $\hat{H}^{(E')}$ of her channels. Effectively, the objective is to determine the conditions under which Eve’s channel estimates provide information regarding the channel $H^{(B)} = H^{(A)}$ and therefore about the key established by Alice and Bob.

Due to the notational differences from the expressions of $I_K$ and $I_{SK}$ presented in Chapter 3, we explicitly specify the expressions used to compute key rate metrics here. The available key rate $I_K$ can be computed from

$$I_K = I(\hat{h}^{(B)}; \hat{h}^{(A)}) = \log_2 \frac{|\hat{R}^{(BB)}||\hat{R}^{(AA)}|}{|K_{BA}|}, \quad (5.1)$$

where $\hat{h}^{(\xi)}$ is a vector formed by stacking $\hat{H}^{(\xi)}$ columnwise for $\xi \in [A, B, E]$, $I(\cdot; \cdot)$ is the mutual information, and $|\cdot|$ is the determinant. The covariances in the numerator are

$$\hat{R}^{(\xi\xi)} = E\left\{\hat{h}^{(\xi)}\hat{h}^{(\xi)\dagger}\right\} = R^{(\xi\xi)} + \sigma^2_\xi I \quad (5.2)$$
for $\xi \in [A, B, E]$ where $E \{ \cdot \}$ is an expectation, $\{ \cdot \}^\dagger$ is a conjugate transpose, $R^{(\xi \xi)} = E \{ h^{(\xi)} h^{(\xi)\dagger} \}$, $I$ is the identity matrix, and $\sigma^2_\xi$ is the variance of the zero-mean complex Gaussian error observed for channel estimate $\hat{h}^{(\xi)}$. The quantity used in the denominator of (4.33) is notation for
\[
\hat{K}_{X_1 X_2 \ldots X_N} = E \left\{ \hat{h}_{X_1 X_2 \ldots X_N} \hat{h}_{X_1 X_2 \ldots X_N}^\dagger \right\},
\]
where $\hat{h}_{X_1 X_2 \ldots X_N} = \begin{bmatrix} \hat{h}^{(X_1)} \hat{h}^{(X_2)} \ldots \hat{h}^{(X_N)} \end{bmatrix}^\dagger$.

In this work it is assumed that Eve is located near Bob and that both are far from Alice. This means that $H^{(E')} = H^{(B)}$ are uncorrelated in any practical environment, consistent with prior findings [17]. However, since $H^{(E)}$ may be correlated with $H^{(B)}$, the secure key rate is defined as the maximum number of bits that can be generated per observation of the channel that are secure from Eve, which can be computed from [17]
\[
I_{SK} = I(\hat{h}^{(B)}; \hat{h}^{(A)} | \hat{h}^{(E)}) = \log_2 \frac{|\hat{K}_{BE}| |\hat{K}_{AE}|}{|R^{(EE)}| |\hat{K}_{BAE}|}.
\]
Lastly, the number of vulnerable key bits are defined as
\[
I_{VK} = I_K - I_{SK}.
\]

5.2.1 Multi-Channel Covariance Formulation

Computation of $I_{SK}$ in (5.4) requires construction of the channel cross-covariance $R^{(BE)} = E \{ h^{(B)} h^{(E)\dagger} \}$ in addition to the auto-covariances $R^{(\xi \xi)}$ for $\xi \in [A, B, E]$. While the auto-covariances can be computed easily in closed form based on the antenna field radiation patterns and the power angular spectrum (PAS) of the multipath propagation [28], accurate computation of $I_{SK}$ requires not only properly modeling the relationship between the fields (via the PAS) at Bob and at Eve but also constructing the cross-covariance based on that model. Therefore this work extends the procedure provided in [28] to the multi-user case.
As taught in [28], the notation \( \Omega = (\theta, \phi) \) is used to represent angular coordinates and describe the propagation between Alice and Bob using the dyadic function

\[
\Omega^{(B)}(\Omega_B, \Omega_A) = \begin{bmatrix}
\beta^{(B)}_{\theta\theta}(\Omega_B, \Omega_A) & \beta^{(B)}_{\theta\phi}(\Omega_B, \Omega_A) \\
\beta^{(B)}_{\phi\theta}(\Omega_B, \Omega_A) & \beta^{(B)}_{\phi\phi}(\Omega_B, \Omega_A)
\end{bmatrix},
\]

(5.6)

where each dyad entry \( \beta^{(B)}_{uv}(\Omega_B, \Omega_A) \) represents the complex gain for a multipath component departing from Alice at the angle \( \Omega_A \) with polarization \( v \in [\theta, \phi] \) and arriving at Bob at the angle \( \Omega_B \) with polarization \( u \in [\theta, \phi] \) [67, 68]. For notational simplicity, the shorthand \( \Omega_{\xi\xi'} = (\Omega_\xi, \Omega_{\xi'}) \) is used in this work.

The dyad \( \Omega^{(B)} \) is stacked columnwise to form the column vector \( b^{(B)}(\Omega_B, \Omega_A) \). Expressing the radiation patterns of the \( n \)th transmit and \( m \)th receive antennas as column vectors \( \mathbf{s}^{(A)}_n(\Omega_A) \) and \( \mathbf{s}^{(B)}_m(\Omega_B) \), respectively, where the vector elements correspond to the two far-field electromagnetic polarizations, we can write

\[
H^{(B)}_{mn} = \int \mathbf{s}^{(BA)}_m(\Omega_{BA})^T \mathbf{b}^{(B)}(\Omega_{BA}) d\Omega_{BA},
\]

(5.7)

where \( \mathbf{s}^{(BA)}_m(\Omega_{BA}) = \mathbf{s}^{(B)}_m(\Omega_B) \otimes \mathbf{s}^{(A)}_n(\Omega_A) \), \( \otimes \) represents a Kronecker product, and \( \{\cdot\}^T \) is a transpose. Using similar definitions, we can write

\[
H^{(E)}_{pq} = \int \mathbf{s}^{(EA)}_p(\Omega_{EA})^T \mathbf{b}^{(E)}(\Omega_{EA}) d\Omega_{EA}.
\]

(5.8)

The assumption that Bob and Eve are in close proximity to one another allows us to express the arriving fields and antenna radiation patterns for Bob and Eve in a common coordinate frame, or \( \Omega_E = \Omega_B \). Based on [28], each element of \( \mathbf{R}^{(BE)} \) can be written using (5.7) and (5.8) as

\[
R^{(BE)}_{mn,pq} = E \{ H^{(B)}_{mn} H^{(E)*}_{pq} \}
\]

(5.9)

\[
= \int \int \mathbf{s}^{(BA)}_m(\Omega_{BA})^T \mathbf{P}^{(BE)}(\Omega_{BA}; \Omega'_{BA}) \mathbf{s}^{(EA)*}_p(\Omega'_{BA}) d\Omega_{BA} d\Omega'_{BA},
\]

(5.10)
where $\{\cdot\}^*$ represents a conjugate and

$$P^{(BE)}(\Omega_{BA}; \Omega'_{BA}) = \mathbb{E}\{b^{(B)}(\Omega_{BA})b^{(E)*}(\Omega'_{BA})\}.$$  \hfill (5.11)

Given the similarity between the quantity in (5.11) and the traditional PAS, $P^{(BE)}(\Omega_{BA}; \Omega'_{BA})$ is referred to as the cross power angular spectrum (CPAS) that measures the statistical similarity between the propagation characteristics observed at Bob and Eve given transmission from Alice.

### 5.2.2 CPAS Formulation

The next step in the analysis is to formulate the CPAS and subsequently construct the cross-covariance in (5.10). While different models could be used for this formulation, this work uses an experimentally-validated autoregressive (AR) model that describes how the gain, angle of departure, and angle of arrival of the multipath components evolve with time as the nodes move through an environment [52]. The model includes appearance of new multipaths and disappearance of existing ones. Specifically, the cluster gains, AOA, and AOD are extracted from the measured data and then each parameter is described by a single wide-sense stationary stochastic representation which consists of the probability density function (pdf) approximated by a histogram and the power spectral density (PSD). The PSD is then computed as

$$P_\gamma(z) = H_\gamma(z)H_\gamma^*(1/z^*),$$  \hfill (5.12)

where $\{\cdot\}^*$ is the conjugate. It is assumed that $H_\gamma(z)$ can be expressed using an AR model as

$$H_\gamma(z) = \frac{b_\gamma(z)}{1 + a_{\gamma,1}z^{-1} + a_{\gamma,2}z^{-2} + \ldots + a_{\gamma,p}z^{-p}},$$  \hfill (5.13)

where $b_\gamma$ and $a_{\gamma,i}$ for $1 \leq i \leq p$ are unknown coefficients. Table 5.1 shows the coefficients used in the AR model to estimate the PSD for the AOA, the AOD, and the power gain using the order $p = 3$, $4$, and $3$, respectively [52]. The principles associated with this model that are relevant for constructing the CPAS are:
Table 5.1: Coefficients for estimating the power spectral density for each cluster parameter.

<table>
<thead>
<tr>
<th>$\gamma$</th>
<th>AOD</th>
<th>AOA</th>
<th>Power Gain</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a_{\gamma,1}$</td>
<td>-2.8918</td>
<td>-2.9023</td>
<td>-1.8902</td>
</tr>
<tr>
<td>$a_{\gamma,2}$</td>
<td>2.7704</td>
<td>2.8082</td>
<td>0.8208</td>
</tr>
<tr>
<td>$a_{\gamma,3}$</td>
<td>-0.8604</td>
<td>-0.9058</td>
<td>0.0742</td>
</tr>
<tr>
<td>$a_{\gamma,4}$</td>
<td>-0.0182</td>
<td>6.0594×10^{-4}</td>
<td>4.0648×10^{-4}</td>
</tr>
<tr>
<td>$b_{\gamma}$</td>
<td>0.023</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Different groups of approximately 50 multipaths are clustered together in that their angles of departure and arrival and complex amplitudes (gains) are drawn from common statistical distributions. This enables us to write the $i$th element of the vector $\mathbf{b}(\xi)$ as

$$b_i^{(\xi)}(\Omega_{BA}) = \sum_{\ell=1}^{L} \alpha^{(\xi)}_{\ell i} b_{\ell i}^{(\xi)*}(\Omega_{BA}),$$

where $\xi \in [B, E]$, $L$ is the total number of clusters, $b_{\ell i}^{(\xi)}(\Omega_{BA})$ is the transfer function for the $\ell$th cluster normalized such that the integral of $E\left\{b_i^{(\xi)}(\Omega_{BA})b_i^{(\xi)*}(\Omega_{BA})\right\}$ over $\Omega_{B}$ and $\Omega_{A}$ is unity, and $\alpha^{(\xi)}_{\ell i}$ represents a real scalar that sets the relative peak (in terms of field magnitude) of the $\ell$th cluster.

2. The gains of different multipaths within a cluster or across different clusters (including those for different polarizations [27]) are statistically uncorrelated, or

$$E\left\{b_i^{(B)}(\Omega_{BA})b_{i,j}^{(B)*}(\Omega_{BA}')\right\} = 0 \quad \ell \neq \ell', i \neq j \quad (5.15)$$

$$E\left\{b_i^{(B)}(\Omega_{BA})b_{i,i}^{(B)*}(\Omega_{BA}')\right\} = B_{i i}^{(B)}(\Omega_{BA})\delta(\Omega_{BA} - \Omega_{BA}'), \quad (5.16)$$

where $\delta(\cdot)$ is the Dirac delta function and the PAS is

$$B_{i i}^{(B)}(\Omega_{BA}) = E\left\{b_i^{(B)}(\Omega_{BA})b_i^{(B)*}(\Omega_{BA})\right\}. \quad (5.17)$$

3. As a node moves, the departure/arrival angles and peak of each cluster shift continuously. The AR model achieves good results by moving all multipaths within the cluster by the same angular offsets and multiplying their gains by the same real scalar.
Therefore, when Bob and Eve are displaced,

\[ b_{\ell i}^{(E)}(\Omega_B, \Omega_A) = b_{\ell i}^{(B)}(\Omega_B - \Delta \Omega_{B,\ell i}, \Omega_A - \Delta \Omega_{A,\ell i}), \quad (5.18) \]

where \( \Delta \Omega_{\xi,\ell i} \) is the angular shift of the \( \ell \)th cluster in departure (\( \xi = A \)) and arrival (\( \xi = B \)) angle.

Using these results, the CPAS in (5.11) is diagonal with elements given by

\[ P_{ii}^{(BE)}(\Omega_{BA}; \Omega_{BA}) = \sum_{\ell=1}^{L} \Gamma_{\ell i}^{(BE)} B_{\ell i}^{(B)}(\Omega_{BA}) \delta(\Omega_B - \Omega_B' + \Delta \Omega_{B,\ell i}) \delta(\Omega_A - \Omega_A' + \Delta \Omega_{A,\ell i}), \quad (5.19) \]

where \( \Gamma_{\ell i}^{(BE)} = \alpha_{\ell i}^{(B)} \alpha_{\ell i}^{(E)*} \).

With this representation of the CPAS, we can define the diagonal matrices \( \Gamma_{\ell i}^{(BE)} \) and \( B_{\ell i}^{(B)}(\Omega_{BA}) \) with \( \ell \)th diagonal elements \( \Gamma_{\ell i}^{(BE)} \) and \( B_{\ell i}^{(B)}(\Omega_{BA}) \), respectively. The notation \( s_{pq}^{(EA)}(\Omega_{BA} + \Delta \Omega_{BA,\ell}) \) is further used to represent the vector with \( \ell \)th element

\[ s_{pq,i}^{(EA)}(\Omega_B + \Delta \Omega_{B,\ell i}, \Omega_A + \Delta \Omega_{A,\ell i}). \quad (5.20) \]

The boldface \( \Delta \) means that each element of the vector \( s_{pq}^{(EA)}(\Omega_{BA}) \) is evaluated at a unique angular offset, and the indexing in \( \ell \) means that these offsets are further unique for each cluster. The final form of the covariance is therefore

\[ R_{mn,pq}^{(BE)} = \sum_{\ell=1}^{L} \int s_{mn}^{(BA)}(\Omega_{BA}) \Gamma_{\ell i}^{(BE)} B_{\ell i}^{(B)}(\Omega_{BA}) s_{pq}^{(EA)*}(\Omega_{BA} + \Delta \Omega_{BA,\ell}) d\Omega_{BA}. \quad (5.21) \]

### 5.3 Analysis

The above presented model is used to explore the difference between the available and secure key rates \( I_K \) and \( I_{SK} \), respectively, for different propagation conditions. Throughout the analysis, it is assumed that each node is equipped with an array of half-wave \( (\lambda/2) \) dipole antennas, where \( \lambda \) is the free-space wavelength. Unless otherwise indicated, the antenna mutual coupling is neglected. Because the focus of this work is the impact of propagation conditions on the information about the Alice-Bob channel that Eve can obtain from her
channel observations, Bob and Eve are close to one another and separated by a distance $d_{BE}$ using the arrangement shown in Figure 5.1. The signal-to-noise ratio (SNR) for each channel is defined as $\text{SNR}_\xi = \text{Tr}(\mathbf{R}(\xi))/N_\xi \sigma_\xi^2$ for $\xi \in [A, B, E]$ where $\text{Tr}(\cdot)$ is the matrix trace, and $\sigma_\xi^2$ is computed to achieve a specified SNR. It is assumed that Alice and Bob have the same SNR of 15 dB. Since Eve is close to Bob and because the focus is on the impact of channel spatial characteristics, it is also assumed that Eve has an SNR of 15 dB. Naturally, if Eve has an SNR advantage (disadvantage), then the value of $I_{SK}$ will be lower (higher) than the values reported here.

5.3.1 Multi-User Propagation Description

For simplicity, the propagation is restricted to vertically-polarized fields traveling parallel to the azimuth plane ($\theta_\xi = 90^\circ$). Each cluster is modeled in the PAS as a truncated Laplacian function [28] with a specified angular spread (AS). A line-of-sight (LOS) path is added into the model with gain $\Gamma_{0}^{(BB)}$ resulting in the $K$-factor defined by

$$K = \frac{1}{\Gamma_{0}^{(BB)}} \sum_{\ell=1}^{L} \Gamma_{\ell}^{(BB)}.$$  \hfill (5.22)

The gain of each multipath in a cluster is a zero-mean, unit-variance Gaussian random variable scaled by the time-variant cluster gain coefficient provided by the model, and therefore the overall channel coefficient statistics are Gaussian as required for the key rate expressions.

The AR model detailed in [52] stochastically generates the cluster gains and central departure and arrival angles for the channel from Alice to Bob and then evolves these cluster parameters as Eve moves away from Bob. The model allows specification of the number of clusters $L_B$ at Bob, but as $d_{BE}$ increases, the model stochastically generates new clusters (birth) or eliminates existing clusters (death), meaning that the total number of clusters at Eve may differ from $L_B$. Figure 5.2 plots an example which shows the evolution of clusters at Eve over time. In the start for $d_{BE} = 0$ both Bob and Eve have same clusters. When Eve is located further away from Bob such that $d_{BE} = 1.3\lambda$, two new clusters are born, and the old clusters are displaced in terms of location as well as power.
Figure 5.2: Power image showing evolution of clusters following truncated Laplacian distribution over time and space. a) Clusters at Bob and Eve when $d_{BE} = 0$ b) Clusters at Eve when $d_{BE} = 1.3\lambda$.

Figure 5.3(a) plots the cluster center arrival angle at Eve as a function of the Bob-Eve separation $d_{BE}$ for $L_B = 4$ clusters at Bob. As can be seen, as Eve moves from Bob, one cluster dies and two new ones are born. Figure 5.3(b) shows an expanded plot of the arrival angle for one of the clusters to allow better visualization of the extent of cluster angle variation. Similar curves exist describing the cluster arrival angles and gains. The remaining computations use $L_B = 4$. The exploration of other values of $L_B$ have shown that while $L_B$ impacts $I_K$, it weakly influences the ratio of $I_{SK}$ to $I_K$, which is the focus of this study.

5.3.2 Model Validation

Before applying the proposed model to detailed analysis of the key rates, it is important to verify that it provides results that match experimental observations. Fortunately, recent measurements comparing $I_K$ and $I_{SK}$ for a limited set of scenarios appears in [17]. To mimic the experimental arrangement of [17], Alice uses a uniform circular array of $N_A = 8$ elements with an inter-element spacing of $0.47\lambda$ (circle diameter of $1.2\lambda$), while Bob and Eve each have square arrays ($N_B = N_E = 4$) with side lengths of $0.43\lambda$. When showing
the results for $N_A = 4$ or 2, we respectively use a subset forming the square array of filled triangle symbols or the linear array of unfilled triangle symbols shown in Fig. 5.1. Similarly, when showing results for $N_B = N_E = 3$ or 2, we respectively use the arrays marked by the three triangle symbols or the two unfilled triangle symbols shown in Fig. 5.1.

Figure 5.4 plots the cumulative distribution function (CDF) of $I_K$ and $I_{SK}$ for different array sizes assuming a cluster AS of $26^\circ$ and $K = 0$ dB. CDFs are obtained by fixing the distance between Bob and Eve to be 10 cm ($0.85\lambda$) or 2 m ($17\lambda$) and then generating 2000 random realizations of the PAS at Bob and correspondingly at Eve to compute $I_K$ and $I_{SK}$. As expected the results reveal that for a large separation between Bob and Eve, $I_K$ and $I_{SK}$ are similar. It is important to note that while the difference between $I_K$ and $I_{SK}$ increases with larger arrays, the fractional difference remains similar at approximately $15 – 20\%$ for $d_{BE} = 10$ cm and around $5 – 9\%$ for $d_{BE} = 2$ m.

A comparison of these results with those presented in Figure 14 of [17] reveals that the general observations from the two are the same, with the exception of two major differences. First, the variance of the measured results is larger than that of the simulations, likely due
to the fact that measurements are averages of observations at several different locations with significantly different propagation conditions. Despite this difference, the average simulated and measured values match very closely. Second, for the case when $N_A = 8$, $N_B = N_E = 4$ and $d_{BE} = 2$ m, the measured difference between $I_K$ and $I_{SK}$ is larger than the difference predicted by the simulations. This may be due to a higher value of $K$ for the measured channels. Despite these differences, this comparison demonstrates that the simulation model provides realistic trends and accurate average key rate values.

5.3.3 Role of $K$-Factor

In the following, the ratio $I_{VK}/I_K$ is explored, which represents the fraction of the available key bits that are vulnerable to determination by Eve due to non-zero correlation $E\{h^{(B)}h^{(E)\dagger}\}$. The antenna configuration from Figure 5.4 with $N_A = 4$ and $N_B = N_E = 3$ is chosen as a representative case. Figure 5.5 plots this fraction of vulnerable key bits as a function of the Bob-Eve separation for different values of the $K$-factor when AS = 26°. The solid and dashed lines show the results when the AR model is used to generate the multipath clusters and when Eve’s PAS is assumed identical to Bob’s, respectively. As expected, in a

**Figure 5.4**: CDFs for $I_K$ and $I_{SK}$ when $K = 0$ dB. The designations $(N_\xi, N_A)$ indicate that Bob and Eve have $N_\xi$ antennas each for $\xi \in [B, E]$ and Alice has $N_A$ antennas.
non-LOS (NLOS) propagation environment ($K = -20$ dB), the difference between $I_K$ and $I_{SK}$ decreases with an increase in $d_{BE}$, with the fraction of vulnerable key bits approaching zero as $d_{BE}$ increases. However, as $K$ increases the dominant LOS path creates considerable correlation between $h(B)$ and $h(E)$, leading to a larger difference between $I_K$ and $I_{SK}$.

The results for the model in which the multipaths are assumed identical at Bob and Eve show that while this simple model gives similar trends, allowing the clusters to evolve using the experimentally-validated AR model creates a more rapid decline in the fraction of vulnerable key bits with Bob-Eve separation. However, as $d_{BE}$ increases, the decorrelation created by the multipath propagation causes the curves for the two models to converge. Regardless of the model used, simulation results show that the simpler expression for $I_K$ is within 5% of the more complicated computation for $I_{SK}$ for $d_{BE} > 2.5\lambda$ and $K < -10$ dB.

5.3.4 Role of Angular Spread

Next the impact of cluster angular spread on key rate behavior is considered. Figure 5.6 plots the ratio $I_{VK}/I_K$ as a function of the Bob-Eve separation for two different
values of AS (26° and 10°) when $K = -20$ dB, $N_A = 4$, and $N_B = N_E = 3$. The results demonstrate that a reduction in AS increases the vulnerable key bits, as reduced AS causes the channel to be more directional which in turn leads to higher correlation between $h^{(B)}$ and $h^{(E)}$. However, for small AS, the angular deviation of the cluster central angles by the AR model is a larger fraction of the cluster width, and the change in the overall PAS created by cluster birth/death processes is significant. Therefore, the performance difference between the results obtained with the AR model and those given by the simpler model (in which Bob and Eve have an identical PAS) is more significant for smaller AS values, with the fraction of vulnerable bits predicted by the simple model being approximately twice that predicted by the more sophisticated spatially-variant AR model. The results generally show that for smaller values of AS $d_{BE}$ must be a large value before we can use $I_K$ in place of $I_{SK}$.

5.3.5 Role of Number of Antennas

Finally, the impact of the number of antennas at different nodes on the key rate behavior is explored. Figure 5.7 plots the ratio $I_{VK}/I_K$ as a function of the Bob-Eve separation.
for different combinations of $N_A$, $N_B$, and $N_E$ when $AS = 26^\circ$ and $K = 0$ dB. Figure 5.8 presents similar results when $K = -20$ dB. These results demonstrate that the fraction of key bits that are vulnerable to Eve declines more rapidly with $d_{BE}$ for smaller arrays, meaning that for small node separation Eve is able to obtain more information about $h(B)$ as her array size increases. The results further show that Eve enjoys an advantage when she is close to Bob if she possesses more antennas than Alice and Bob. This is mainly due to improved SNR due to increased multi-antenna gain, as the channels to the additional antennas do not offer improved correlation between $h(B)$ and $h(E)$. Regardless of array size, the results confirm that $d_{BE}$ must be greater than about $1\lambda$ before one can begin to ignore the difference between $I_K$ and $I_{SK}$ in an analysis.

### 5.3.6 Role of Antenna Coupling

While the impact of antenna mutual coupling is ignored for this analysis, for small values of $d_{BE}$, cross-array mutual coupling can impact the results. Therefore the model presented in Figure 3.1 is used to explore the impact on the key rate of coupling both within each array and across both arrays. Figure 5.9 repeats the computation shown in
Figure 5.8: Relative number of vulnerable key bits as a function of Eve’s distance from Bob ($d_{BE}$) when AS = 26° for different array sizes when $K = -20$ dB.

Figure 5.5 using the full propagation model, where the solid curves show the result when Bob and Eve are equipped with an impedance matching network that optimally transfers power from the antennas to the loads while the dashed curves show the result when mutual coupling is ignored. The value of $I_K$ for both cases assumes no cross-array coupling, since $I_K$ is the key rate when the eavesdropper is not present. The results generally indicate that mutual coupling has only a small impact on the fraction of available key bits that are vulnerable and virtually no impact on the conclusions one may draw from the computations shown here. However, as shown in [56], coupling does have a significant impact on the underlying quantities $I_K$ and $I_{SK}$ and is therefore important to include in general studies on key establishment.

5.4 Chapter Summary

This chapter formulates a straightforward yet realistic model for computing the secure key rate for two legitimate nodes who establish their secret key using observations of the reciprocal electromagnetic propagation channel in the presence of a passive eavesdropper. By applying the model to compute the available and secure key rates for a variety of different
Figure 5.9: Relative number of vulnerable key bits as a function of Eve’s distance from Bob ($d_{BE}$) and different values of $K$ when $N_A = 4$, $N_B = N_E = 3$, and AS = 26° when mutual coupling is included. Dashed lines designate results when mutual coupling is neglected.

Multipath parameters, it is demonstrated that the secure key rate is approximately equal to the available key rate when the separation between the nodes is adequately large (more than 2.5 wavelengths) and the propagation $K$-factor is smaller than 0 dB. This suggests that in analyses that ignore the impact of the eavesdropper and focus on the available key rate, the results are approximately representative of the secure key rate under these propagation conditions. The analysis also contrasts performance differences when assuming the multipath parameters change as a function of the distance between the eavesdropper and the legitimate node to those obtained when it is assumed that both nodes observe the same multipath. While the results demonstrate that both models provide the same trends, using the simple model over predicts the fraction of bits that are vulnerable to an eavesdropper by as much as a factor of two.
Chapter 6

Conclusion

This dissertation provides a comprehensive analysis of practical issues related to physical layer key generation. Specifically, this work focuses on the impact of array mutual coupling in a MIMO communication environment, channel fading statistics between the communicating nodes, and practical limitations such as non-reciprocity that arises from the RF circuits used in the radios.

6.1 Summary

An overview of different cryptography techniques and their comparison with key generation using reciprocal propagation channel is presented in Chapter 2. Next, the performance metrics for physical layer security, namely the available key rate which refers to the number of bits that can be generated per observation of propagation channel between two radios and the secure key rate which quantifies the number of key bits which are secure from a passive eavesdropper are presented. Furthermore, the impact of array size, multipath richness, and spacing between the communicating nodes and an eavesdropper on key rate metrics is analyzed for a path based model which assumes ideal isotropic antennas and no array mutual coupling.

The impact of array mutual coupling on key rate metrics is analyzed in Chapter 3. This is accomplished by developing a realistic network model of a MIMO communication system between two communicating nodes and an eavesdropper that can be very near to one of the nodes. This model incorporates the impact of matching networks, array coupling, and noise that depends on LNA parameters and uses a cluster based propagation model. Results demonstrate that high mutual coupling can have a significant impact on key rate metrics, which can be overcome by the use of proper matching network, where optimal
matching network is found to offer key rates that are 10-15% higher than those offered by a suboptimal diagonal matching network. Furthermore, if an eavesdropper is located near (< 0.5λ) one of the legitimate nodes, then the secure key rate reduces significantly.

Chapter 4 focuses on the fact that due to non-reciprocity of transmit and receive RF circuits inside the radio, the end-to-end propagation channel between two nodes may not be reciprocal. The network model developed in Chapter 3 is modified to incorporate the non-reciprocal contributions. The simulations show that non-reciprocity can effectively reduce both the available as well as the secure key rate. Next, the use of a calibration technique based on total least square (TLS) algorithm is explored. Results demonstrate that the software based calibration technique can effectively make the propagation channel reciprocal. However the time required for calibration increases with an increase in array size or degradation in SNR.

A cluster based propagation model which can be used to quantify the difference between available and secure key rate in the presence of a nearby eavesdropper under different propagation conditions is proposed in Chapter 5. This model is validated based on measurements acquired in recent experiments [17]. Using this model, the impact of the number of clusters, cluster angular spread, $K$-factor, and array size on key rate metrics is studied. Analysis reveals that the secure key rate is approximately equivalent to the available key rate when the environment is multipath rich ($K$-factor less than 0 dB) and the spacing between the legitimate node and the eavesdropper is large (> 2.5λ). Results also demonstrate that if multipath characteristics are assumed to be same at an eavesdropper and a nearby legitimate node, then the computed secure key rate can be significantly lower, which highlights the importance of proper modeling of the propagation channel.

6.2 Future Work

There are several possible directions for future research related to the topics presented in this dissertation. A few of the ideas are presented below:

1. This work has assumed a single eavesdropper located near one of the communicating nodes. In practice there can be multiple eavesdropper nodes in the environment which can collaborate with each other to reduce the secure key rate. The work presented in
this dissertation on array mutual coupling and propagation channel conditions can be extended to model multiple eavesdroppers to analyze their impact on the secure key rate.

2. Only a passive eavesdropper is considered in this work. The presence of an active eavesdropper poses many challenges, as its physical location may be away from the communicating nodes, but it can transmit false information to both legitimate nodes. This is especially important for calibration, as Bob must send his channel estimate to Alice. This problem can be avoided by using an authentication mechanism in addition to physical layer security which ensures that key bits are generated based only on the communication between legitimate nodes.

3. The non-reciprocity in the propagation channel is modeled in Chapter 4 using phase errors in the matching network. However, in practical systems gain errors can also occur in matching networks, but they are relatively hard to model. The present work can be extended to study in detail the effect of gain error in the matching networks.

4. The calibration study presented in Chapter 4 is based on simulations. The current work can be extended by an experimental campaign in which the impact of non-reciprocity in the propagation channel on the key rate metrics can be quantified. Also, the proposed calibration technique based on the TLS algorithm can be applied in real time to explore the overall effectiveness of the algorithm.

5. Finally, the experimental campaign mentioned above can also be used to quantize the impact of array mutual coupling. This can be accomplished by varying the inter-element spacing between the array elements and placing the eavesdropper at different distance offsets from one of the communicating nodes. This would provide a very useful comparison to the results presented in Chapter 3.
Appendix A

Appendix

A.1 Lossless and Reciprocal Matching Network Design

Lossless reciprocal matching networks are characterized by unitary S-matrices such that $S^\dagger S = I$ and $S = S^T$, where $\{\cdot\}^\dagger$ and $\{\cdot\}^T$ are conjugate transpose and transpose, respectively. This appendix demonstrates the design of a lossless matching network and then shows how to further simplify the expressions to ensure reciprocity.

To design a lossless matching network, the SVD of sub-blocks $S_{ij} = U_{ij} \Lambda_{ij}^{1/2} V_{ij}^\dagger$ (see (3.1)) are substituted into the lossless constraint to obtain

$$V_{ij} \Theta_{ij} = V_{jj} \quad \Lambda_{ij} = I - \Lambda_{jj} \quad i \neq j,$$

where $\Theta_{ij}$ is a diagonal matrix with unit-magnitude entries. This operation also leads to

$$\Lambda_{11}^{1/2} U_{11}^\dagger U_{12}(I - \Lambda_{22})^{1/2} \Theta_{12} = -\Theta_{21}^\dagger (I - \Lambda_{11})^{1/2} U_{21}^\dagger U_{22} \Lambda_{22}^{1/2}. \quad \text{(A.2)}$$

The sub-blocks of the matrix $S$ that ensure the matching network is lossless can then be expressed as

\begin{align*}
S_{11} &= U_{11} \Lambda_{11}^{1/2} V_{11}^\dagger, \\
S_{12} &= U_{12} \Theta_{12}(I - \Lambda_{22})^{1/2} V_{22}^\dagger, \\
S_{21} &= U_{21} \Theta_{21}(I - \Lambda_{11})^{1/2} V_{11}^\dagger, \\
S_{22} &= U_{22} \Lambda_{22}^{1/2} V_{22}^\dagger. \quad \text{(A.3)}
\end{align*}
If the network is reciprocal, we must have $S = S^T$ which mean

$$S_{11} = S_{11}^T \Rightarrow V_{11} = U_{11}^*,$$
$$S_{22} = S_{22}^T \Rightarrow V_{22} = U_{22}^*, $$
$$S_{12} = S_{21}^T \Rightarrow U_{12} \Theta_{12} (I - \Lambda_{22})^{1/2} U_{22}^T = U_{11} (I - \Lambda_{11})^{1/2} \Theta_{21}^T U_{21}^T,$$
$$\Rightarrow U_{12} (I - \Lambda_{22})^{1/2} \Theta_{12} = U_{11} (I - \Lambda_{11})^{1/2} \Theta_{21}^T U_{21}^T U_{22}^*.$$ (A.4)

Inserting (A.4) into (A.2) leads to

$$\Lambda_{11}^{1/2} = -U_c \Lambda_{22}^{1/2} U_c^T$$
$$U_c = \Theta_{21}^T U_{21}^T U_{22}^*.$$ (A.5)

Assuming $U_c = -j U_o$ leads to

$$\Lambda_{11}^{1/2} = U_o \Lambda_{22}^{1/2} U_o^T,$$ (A.6)

which suggests that $U_o \Lambda_{22}^{1/2} U_o^T$ is the SVD of the real diagonal matrix $\Lambda_{11}^{1/2}$. There exists a complete family of matching networks that satisfies these conditions. Since we are interested in only one lossless reciprocal matching network that achieves the design goal, we can further specify the singular vectors and values. Choosing $U_o = I$ and $\Lambda_{22} = \Lambda_{11}$ leads to

$$\Theta_{21}^T U_{21}^T U_{22}^* = -jI \Rightarrow U_{21} \Theta_{21} = j U_{22}.$$ (A.7)

Inserting (A.7) into (A.4) leads to

$$U_{12} (I - \Lambda_{11})^{1/2} \Theta_{12} = j U_{11} (I - \Lambda_{11})^{1/2} U_{22}^T U_{22}^* \Rightarrow U_{12} \Theta_{12} = j U_{11}.$$ (A.8)
Using the above expression in (A.3), the sub-blocks of $S$ that ensure the design is both lossless and reciprocal can then be expressed as

\[
\begin{align*}
S_{11} &= U_{11} A_{11}^{1/2} U_{11}^T \\
S_{12} &= j U_{11} (I - A_{11})^{1/2} U_{22}^T \\
S_{21} &= j U_{22} (I - A_{11})^{1/2} U_{11}^T \\
S_{22} &= U_{22} A_{22}^{1/2} U_{22}^T. \quad (A.9)
\end{align*}
\]
Bibliography


