2015-06-01

A Study of Reconfigurable Antennas as a Solution for Efficiency, Robustness, and Security of Wireless Systems

Rashid Mehmood
Brigham Young University - Provo

Follow this and additional works at: https://scholarsarchive.byu.edu/etd
Part of the Electrical and Computer Engineering Commons

BYU ScholarsArchive Citation
https://scholarsarchive.byu.edu/etd/5556

This Dissertation is brought to you for free and open access by BYU ScholarsArchive. It has been accepted for inclusion in All Theses and Dissertations by an authorized administrator of BYU ScholarsArchive. For more information, please contact scholarsarchive@byu.edu, ellen_amatangelo@byu.edu.
A Study of Reconfigurable Antennas as a Solution for Efficiency, Robustness, and Security of Wireless Systems

Rashid Mehmood

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
Jon W. Wallace
Karl F. Warnick
Richard Selfridge
Brian D. Jeffs

Department of Electrical and Computer Engineering
Brigham Young University
June 2015

Copyright © 2015 Rashid Mehmood
All Rights Reserved
ABSTRACT

A Study of Reconfigurable Antennas as a Solution for Efficiency, Robustness, and Security of Wireless Systems

Rashid Mehmood
Department of Electrical and Computer Engineering, BYU
Doctor of Philosophy

The reconfigurable aperture (RECAP) is a reconfigurable antenna consisting of a dense array of electronically controlled elements, which can be manipulated to support many antenna functions within a single architecture. RECAPs are explored herein as an enabling technology for future software defined and cognitive radio architectures, as well as compact wireless devices supporting many bands and services.

First, the concept of a parasitic RECAP is developed and analyzed for various communication applications. This begins with the analysis of existing RECAP topologies (e.g. planar and parasitic) using a hybrid method combining full wave simulations and network analysis. Next, a performance versus complexity analysis is performed to assess the use of a parasitic RECAP for the most critical communications functions: pattern synthesis, MIMO communications and physical-layer wireless security. To verify simulation results, a prototype parasitic RECAP is also built and deployed in real propagation environments.

Given the potential of adaptive and reconfigurable architectures for providing enhanced security, an idealized reconfigurable antenna is analyzed, resulting in the concept of secure array synthesis. The objective is to find optimal array beamforming for secure communication in the presence of a passive eavesdropper in a static line-of-sight (LOS) channel. The method is then extended to the case of multipath propagation environments. The problem is solved by casting it into the form of a semi-definite program, which can be solved with convex optimization. The method is general and can be applied to an arbitrary array topology with or without antenna mutual-coupling. Due to complexity of the problem, initial attention has been restricted to idealized reconfigurable antennas (smart antennas), where excitation amplitude and phase at each element can be controlled independently.

Lastly, reconfigurable antennas are investigated as a solution to support the emerging application of over-the-air (OTA) testing in a low-cost and compact way, resulting in the concept of the reconfigurable over-the-air chamber (ROTAC). First, an idealized two-dimensional ROTAC is analyzed, revealing that the fading distribution, spatial correlation, frequency selectivity, and multipath angular spectrum can be controlled by proper specification of the random loads. Later, a prototype of ROTAC is built to study the fading statistics and angular characteristics of the multipath fields inside a practical chamber.

Keywords: Reconfigurable antennas, RECAP, OTA testing, MIMO Communications, physical layer security, secure pattern synthesis, ROTAC, ERRC
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. Also, I am very highly thankful to my PhD co-advisor Dr. Jon W. Wallace at Lafayette College for his continuous support, enriching discussions and guidance throughout the research work. Furthermore, I will like to thank my PhD committee members: Dr. Karl F. Warnick, Dr. Brian D. Jeffs, and Dr. Richard Selfridge for their time and support.

Last but not the least, I would like to thank my Parents and my beloved wife, Attiya Mahmood whose continuous support has made me able to stand in this position.
## Table of Contents

List of Figures viii

1 Introduction 1
   1.1 New Contributions ..................................................... 2
   1.2 Organization of the Dissertation ..................................... 4

2 Background 6
   2.1 Reconfigurable Antennas .............................................. 6
      2.1.1 RECAP Design .................................................... 7
      2.1.2 Hybrid Full-Wave/Network Analysis of RECAP Antennas ....... 8
      2.1.3 Prototype of a Parasitic RECAP ................................. 11
      2.1.4 Optimization of RECAP .......................................... 12
   2.2 RECAP for Pattern Synthesis and MIMO Communications .......... 13
   2.3 RECAPs for Physical Layer Security ................................. 14

3 MIMO Capacity Enhancement using Reconfigurable Antennas 16
   3.1 Analysis of Parasitic RECAP Structure .............................. 17
      3.1.1 System Model .................................................... 18
      3.1.2 Noise Modeling .................................................. 20
      3.1.3 LNA Specification ............................................... 23
      3.1.4 MIMO Channel Modeling ........................................ 24
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.4.1 Node Locations</td>
<td>62</td>
</tr>
<tr>
<td>4.4.2 Experimental Setup</td>
<td>63</td>
</tr>
<tr>
<td>4.4.3 Results</td>
<td>65</td>
</tr>
<tr>
<td>4.5 Key Establishment in Simulated LOS Channels</td>
<td>69</td>
</tr>
<tr>
<td>4.6 Analysis and Initial Results</td>
<td>70</td>
</tr>
<tr>
<td>4.7 Chapter Summary</td>
<td>73</td>
</tr>
<tr>
<td>5 Secure Pattern Synthesis for Physical Layer Security</td>
<td>74</td>
</tr>
<tr>
<td>5.1 Key Establishment in LOS Channels</td>
<td>75</td>
</tr>
<tr>
<td>5.1.1 Secrecy Capacity</td>
<td>77</td>
</tr>
<tr>
<td>5.1.2 Reciprocal Channel Key Establishment</td>
<td>79</td>
</tr>
<tr>
<td>5.2 Optimization Procedure</td>
<td>83</td>
</tr>
<tr>
<td>5.2.1 Optimization Variables</td>
<td>84</td>
</tr>
<tr>
<td>5.2.2 Constraint (i): Minimum $\alpha$ Threshold</td>
<td>84</td>
</tr>
<tr>
<td>5.2.3 Constraint (ii): Power Constraint</td>
<td>86</td>
</tr>
<tr>
<td>5.2.4 Constraint (iii): PSD Constraint on $R$</td>
<td>86</td>
</tr>
<tr>
<td>5.2.5 Constraint (iv): Non-negativity Constraint on $\gamma$</td>
<td>87</td>
</tr>
<tr>
<td>5.2.6 Solution Using MAXDET</td>
<td>87</td>
</tr>
<tr>
<td>5.3 Signal/Noise Pattern Analysis</td>
<td>88</td>
</tr>
<tr>
<td>5.4 Numerical Examples</td>
<td>90</td>
</tr>
<tr>
<td>5.4.1 Suboptimal Approach for ULA</td>
<td>90</td>
</tr>
<tr>
<td>5.4.2 Uniform Linear Array</td>
<td>91</td>
</tr>
<tr>
<td>5.4.3 Uniform Circular Array</td>
<td>95</td>
</tr>
<tr>
<td>5.5 Key Establishment in Static Multipath Channels</td>
<td>97</td>
</tr>
<tr>
<td>5.5.1 Information Theoretic Analysis</td>
<td>97</td>
</tr>
</tbody>
</table>
6 Reconfigurable Over-the-Air Chamber

6.1 Idealized Chamber Topology ................................................. 106
6.2 Electromagnetic Wave-field Synthesis ..................................... 108
6.3 Synthesis of Channel Fading ................................................. 109
  6.3.1 Generation of Rayleigh Fading ........................................ 110
  6.3.2 Fading Distribution Optimization ...................................... 111
  6.3.3 Rician Fading Example .................................................. 112
  6.3.4 Frequency Selective Fading ............................................. 113
  6.3.5 Channel Delay Spread .................................................. 114
  6.3.6 Directional Propagation Characteristics ............................. 115
6.4 ROTAC Prototype .............................................................. 117
  6.4.1 Fading Statistics Control .............................................. 118
  6.4.2 Power Angular Spectrum Control .................................... 120
6.5 Chapter Summary .............................................................. 124

7 Conclusion

7.1 Summary ................................................................. 125
7.2 Future Work .............................................................. 127

Bibliography ................................................................. 129
List of Figures

2.1 Perspective view of the parasitic RECAP with feed in the middle and other elements are REs ......................................................... 7

2.2 Perspective view of the planar RECAP with $N_E = 4$ logical elements, $N_{RE} = 3$ reconfigurable elements (RE) and one feed (F) ........................................ 8

2.3 Characterization of a generic RECAP antenna ........................................ 9

2.4 RE circuit: (a) schematic, (b) completed RE with circuit board holding components, bias lead, and a monopole inserted into the SMA connector. .... 11

2.5 Reflection coefficient of several REs as a function of the bias voltage ($V_{bias}$) .......................... 12

3.1 Configurations for non-RECAP and RECAP arrays: (a) Perspective view of the parasitic RECAP with 2 feeds.  (b) Top view of RECAP configurations, where red boxes show RE positions, blue stars and circles show feed locations for 2×2 and 4×4 MIMO respectively.  (c) Top view of antenna positions for non-RECAP for 2×2 MIMO (stars) and 4×4 MIMO (circles), where boxes are empty locations. ....... 18

3.2 RECAP structure consisting of a 9×9 dipole array, where $N_{RE}$ elements are terminated with REs (filled circles) and feeds are marked by red squares. .... 19

3.3 MIMO system model and noise matching for LNAs ............................... 20

3.4 Effects of $r_{in}^*$ and $|\Gamma_{in}|^2$ on $F - F_{min}$ ................................................ 24

3.5 MIMO Capacity versus RECAP complexity: (a) 2×2 MIMO with average transmit power constraint (b) 4×4 MIMO with average transmit power constraint (c) 2×2 MIMO with EIRP constraint (d) 4×4 MIMO with EIRP constraint (e) 2×2 MIMO with average SNR constraint (f) 4×4 MIMO with average SNR constraint. Numbers 1 to 5 under curves show $N_{RB}$ values (same pattern used but not labeled in other curves). .......................... 30
3.6 Instantaneous and average MIMO channel capacity for a simple non-RECAP array (dashed lines) and RECAP (solid lines): (a) 2×2 MIMO with $L=4$ (b) 4×4 MIMO with $L=8$ ................................. 32

3.7 Channel capacity for single user 2×2 MIMO with fixed interference for a simple non-RECAP array (dashed lines) and RECAP (solid lines): (a) uniform multipath $L=4$ (b) SVA model ............................................. 33

3.8 Channel capacity for single user 4×4 MIMO with fixed interference for a simple non-RECAP array (dashed lines) and RECAP (solid lines): (a) uniform multipath with $L=8$ (b) SVA model ............................................. 34

3.9 Channel capacity for two-user 2×2 MIMO for a simple non-RECAP array (dashed lines) and RECAP (solid lines): (a) uniform mutli-path with $L=4$ (b) SVA model ............................................. 35

3.10 Channel capacity for two-user 4×4 MIMO for a simple non-RECAP array (dashed lines) and RECAP (solid lines): (a) uniform mutli-path with $L=8$ (b) SVA model ............................................. 36

3.11 Effect of losses for a simple non-RECAP array (dashed lines) and RECAP (solid lines): (a) 2×2 MIMO with uniform multipath and $L=4$ (b) 4×4 MIMO with uniform multipath and $L=8$ ................................. 37

3.12 RECAP capacity for 20 MHz bandwidth and the SVA model for a simple non-RECAP array (dashed lines) and RECAP (solid lines): (a) 2×2 (b) 4×4 38

3.13 Channel-sounder-based setup for MIMO-RECAP measurements ................................. 39

3.14 Location of Tx and Rx node for LOS (Rx1) and non-LOS (Rx2) measurements, where blue circles mark the location of interfering antennas ................................. 40

3.15 Top view of the antenna configurations used for the MIMO-RECAP measurements ................................. 41

3.16 Photo showing the LOS environment where measurements were taken and the relative positions of the Tx and Rx nodes ................................. 42

3.17 Peak measured capacity for a 2 × 2 MIMO system. Random search on left and GA on right of each subplot ................................. 43

3.18 Peak measured capacity for a 4 × 4 MIMO system. Random search on left and GA on right of each subplot ................................. 44
4.1 Top view of the antenna arrangement in the security analysis, where Bob has a single antenna (black square), Alice has a RECAP with a single feed antenna (black square) and programmable REs placed on a regular grid (empty circles), and Eve has an array of antennas surrounding the RECAP (filled circles).

4.2 RECAP structure with elements arranged on a $5 \times 5$ regular grid, where $N_{RE}$ reconfigurable elements (black circles) are terminated with tunable impedances and the center element (black square) is the feed. Dipole or monopole antennas are aligned along the $z$-axis (out of the page).

4.3 Maximum key bits that can be securely generated with a RECAP with limited complexity under static conditions.

4.4 Simulated $I_K$ as a function of $N_{RS}$ for different values of $N_{RE}$, where curves marked with * and ● are respectively obtained using the Gaussian assumption and numerical computation: (a) NLOS channel ($L = 10$), (b) LOS channel ($L = 1$).

4.5 Simulated $I_{SK}$ as a function of $N_E$ for $N_{RE} = 24$ and two values of $N_{RS}$ when Eve knows $b$ alone, $c$ alone, or both $b$ and $c$: (a) NLOS channel ($L = 10$), (b) LOS channel ($L = 1$).

4.6 Simulated $I_K$ and $I_{SK}$ as a function of $N_E$ for different values of $N_{RE}$ and $N_{RS}$, where $I_K$ curves marked with * and ● are respectively obtained using the uncorrected and corrected Gaussian assumption: (a) $I_K$, (b)-(e) $I_{SK}$.

4.7 Relative positions of Bob (B), Alice (A) and Eve (C) at four different locations within an indoor environment. Arrows connect the different node locations for a given location number.

4.8 Photograph of the outdoor measurement environment and the relative positions of Alice, Bob and Eve for $N_{RE} = 8$. The red ‘×’ indicates the antenna in Eve’s array that is not used in measurements.

4.9 2-node and 3-node configurations used to measure channel responses for the legitimate nodes (Alice and Bob) and eavesdropper (Eve).

4.10 Measured $I_K$ as a function of $N_{RS}$ for $N_E = 7$ and $I_{SK}$ as a function of $N_E$ for two values of $N_{RS}$ (both use $N_{RE} = 24$) at indoor Location 1 using a 3-node measurement setup when Eve knows $b$ alone, $c$ alone, or both $b$ and $c$.

4.11 Measured $I_K$ and $I_{SK}$ as a function of $N_E$ for different values of $N_{RE}$ and $N_{RS}$, where $I_K$ curves marked with * and ● are respectively obtained using the uncorrected and corrected Gaussian assumption: (a) $I_K$, (b)-(e) $I_{SK}$. 

x
4.12 Measured values of $I_{SK}$ as a function of $N_E$ for different values of $N_{RE}$ and $N_{RS}$, where the curves for indoor and outdoor measurements represent averages over all experimental results. ................................................................. 67

4.13 Measured $I_{SK}$ and as a function of $N_E$ for different values of $N_{RE}$ and $N_{RS}$, where solid and dashed curves are respectively obtained using average and worst case Eve antenna configuration (a) $N_{RS} = 2$, (b) $N_{RS} = 32$. .......... 68

4.14 Worst-case configuration of Eve’s array for Location 2 (Hallway) where circles indicate positions of Eve’s antennas. ................................................................. 69

4.15 Top view of nodes in the security simulations, where Bob and Eve have a single antenna and Alice has a RECAP with many programmable REs (hollow circles). Black squares show the location of Bob’s antenna and Alice’s feed, while the blue circle shows a possible position of Eve’s antenna depending on $\theta$. ................................................................. 70

4.16 $I_K$ for varying $N_{RS}$ using the numerical expectation method and the Gaussian approximation: (a) Alice having a square RECAP (b) Alice having a circular RECAP. ................................................................. 71

4.17 $I_{SK}$ for varying $\theta$ and $N_{RS}$ using the numerical expectation method and the Gaussian approximation when Alice has a square RECAP. ............... 72

4.18 $I_{SK}$ for varying $\theta$ and $N_{RS}$ the numerical expectation method and the Gaussian approximation when Alice has a circular RECAP. ............... 72

5.1 Generic system model for secure array synthesis in line-of-sight (LOS) propagation environment ................................................................. 75

5.2 Signal model for secrecy capacity. ................................................................. 77

5.3 Signal model for reciprocal channel key establishment. ......................... 80

5.4 Suboptimal method for secure array synthesis employing a ULA with $N_T = 10$, $\phi_B = 90^\circ$, and $\phi_X = 10^\circ$: (a) power allocation to signal and noise patterns, (b) achieved $I_{SK}$ performance for different power allocations. ................................................................. 92

5.5 Performance of the (a) suboptimal and (b) optimal methods for a ULA at Alice with $\phi_X = 10^\circ$. Performance is shown with respect to the number of antennas at Alice ($N_T$) and the transmit angle to Bob ($\phi_B$). ....................... 92

5.6 Achieved $I_{SK}$ for a varying number of antennas in Alice’s ULA and different transmit angles to Bob for $\phi_X = 20^\circ$: (a) optimal solution, (b) suboptimal solution. ................................................................. 93
5.7 Comparison of radiated signal \((P_S)\) and noise \((P_N)\) for the (a) suboptimal and (b) optimal approaches for a ULA at Alice with \(N_T = 10\) elements, \(\phi_X = 10^\circ\), and \(\phi_B = 90^\circ\). The horizontal line is the minimum \(I_{SK}\) outside of the exclusion sector.

5.8 \(I_{SK}\) for a UCA at Alice as the size of the exclusion sector and the number of antennas at Alice are varied.

5.9 \(I_{SK}\) for a varying number of antennas in Alice’s UCA and different transmit directions to Bob for \(\phi_X = 40^\circ\).

5.10 \(I_{SK}\), \(P_S\), and \(P_N\) with respect to Eve’s location for a UCA at Alice with \(N_T = 12\) elements, \(\phi_X = 40^\circ\), and \(\phi_B = 270^\circ\).

5.11 System diagram where Alice is equipped with a ULA of half-wave dipoles while Eve and Bob each have a single half-wave dipole separated by distance \(d\).

5.12 Average secure key rate for both low and high transmit correlation as a function of minimum distance between Bob and Eve. The dashed lines corresponds to the sub-optimal results.

5.13 Ratio of expected noise versus signal power at Eve for both low and high transmit correlation cases as a function of minimum distance between Bob and Eve. The dashed lines corresponds to the sub-optimal results.

5.14 Singular values corresponding to the signal singular vector for the suboptimal SVD case. For the optimal SDP solution, the smaller nonzero singular value is plotted.

5.15 Orthogonal projection of dominant singular vector of channel \(h_{AB}\) on the eigenvectors of optimal transmit covariance matrix \(R_{opt}\) which corresponds to non-zero eigenvalues: (a) High transmit correlation. (b) Low transmit correlation.

6.1 Idealized two-dimensional chamber.

6.2 Synthesis of a multipath wave field using the idealized two-dimensional chamber.

6.3 Chamber topology used for fading studies, where four ports are driven with active sources and the remaining 24 ports are terminated with reconfigurable impedances.

6.4 Amplitude and phase pdfs of the field sampled at the center of the chamber for uniform random loads at the reconfigurable ports.
6.5 Average correlation coefficient of field sample points along the center line of
the chamber, compared with Jakes’ model. ............................................ 111

6.6 Amplitude pdfs of the field sampled at the center of the chamber for uniform
RE reactances, where in each case the distribution parameters are optimized
for a specific value of \( \sigma \) and \( \nu \). .................................................. 113

6.7 Power versus frequency for 4 different realizations of the RE reactances, where
the field was sampled in the middle of the chamber. ............................. 114

6.8 Average frequency- and time-domain power at the center of the ROTAC over
a bandwidth of 40 MHz. ................................................................. 115

6.9 Dependence of propagating power versus arrival angle \( \phi \) generated for various
desired directional profiles. The sectors where propagation is desired in each
case is denoted by the dashed boxes. ................................................. 116

6.10 Prototype ROTAC: (a) Complete chamber from side, (b) a single chamber
panel hosting a \( 3 \times 3 \) grid of dual polarized square patch antennas, (c) bot-
tom view of the chamber with one receive dipole placed in the middle of the
chamber above the ground plane. ....................................................... 117

6.11 S-parameters of a single fabricated patch antenna used in the prototype
ROTAC. ...................................................................................... 118

6.12 Histograms of the phase and amplitude of the field sampled at the DUT
antenna in the ROTAC compared to uniform phase and Rayleigh amplitude
distributions. ........................................................................... 119

6.13 Amplitude pdfs of the field sampled at the DUT antenna in the ROTAC
compared to different Rician distributions, where \( \sigma \) and \( \nu \) control the Rician
statistics. .................................................................................. 120

6.14 Prototype ROTAC for PAS Measurements: (a) Side view of the complete
chamber showing representative feed and RE ports; (b) Bottom view of the
chamber showing the RF cables that connect to an eight-element circular array
of receiving monopole antennas. ....................................................... 121

6.15 Power incident on the DUT as a function of azimuth arrival angle for sources
on the vertical polarization port at the center of each face (Case 1): (a) Single
RE state; (b) Average over 50 RE states. ........................................... 122

6.16 Power incident on the DUT as a function of azimuth arrival angle for sources
on the vertical polarization port at the lower right corner of each face (Case 2):
(a) Single RE state; (b) Average over 50 RE states. ............................ 123
6.17 Power incident on the DUT as a function of azimuth arrival angle for sources on the horizontal polarization port at the lower right corner of each face (Case 3): (a) Single RE state; (b) Average over 50 RE states.
Chapter 1

Introduction

Traditional wireless systems employ a single antenna and have little or no control over how the channel is exploited for physical transmission. Antenna systems and algorithms that can effectively adapt their operation to changing needs and environmental conditions have been the subject of intense research over the past few decades. The need of such architectures has been especially apparent in the realm of wireless communications, due to a dramatic rise in services, applications, and users coupled with the scarcity and high cost of radio-frequency (RF) spectrum.

Smart antennas represent the most adaptive solution, where physical antenna elements are simple transducers whose signals are digitized and jointly processed by powerful digital signal processing (DSP) architectures. Smart antennas can support diversity, beamforming, interference suppression, and spatial multiplexing, thus maximizing user performance for the channels and conditions that are present. Although smart antennas are a very powerful concept, the cost associated with the multiple RF chains and additional DSP resources can limit their use in many practical applications.

In contrast, reconfigurable antennas represent an alternative approach, where the antennas are physically adapted to maximize signal power. These solutions potentially provide a smaller, lower cost, and lower power solution than digital beamforming techniques. Not only do analog reconfigurable architectures support traditional applications such as beam steering [1], pattern null creation [2], and frequency agility [3], but they also enable future software defined and cognitive radio architectures, compact wireless devices supporting many bands and services, spectrally efficient communication, and secure transmission at a potentially lower cost than smart antennas.
Antennas with a much higher degree of reconfigurability that consist of a dense two or three-dimensional array of reconfigurable elements (REs) whose states can be electronically controlled have been referred to as reconfigurable aperture (RECAP) antennas [4, 5]. The goals of the RECAP are similar to those of reconfigurable antennas and switched parasitic arrays, namely to support multiple frequency bands as well as dynamic pattern synthesis in a single aperture. When the degree of reconfigurability of the RECAP is large and loss of the REs sufficiently low, RECAPs have the potential to dynamically synthesize a wide range of antennas, constrained only by the physical aperture of the device. RECAPs have demonstrated the ability to support multiple bands [6], beamforming [7], and gain and impedance optimization [8]. This discussion uses the words RECAP and reconfigurable antenna interchangeably to refer to antennas with a high degree of complexity in terms of number of reconfigurable elements ($N_{RE}$) and number of reconfigurable states ($N_{RS}$) per element.

This dissertation explores the use of reconfigurable antennas and RECAPs for a variety of applications related to wireless communication, physical layer security, and over-the-air (OTA) testing of mobile devices. The new contributions in each of these areas are listed in the following section.

1.1 New Contributions

- An important goal of this research is to characterize the level of RECAP complexity required to achieve near-optimal performance for different communication applications. Previously, both planar and parasitic RECAPs for beamforming [9, 10] and interference suppression were investigated [11]. The work in this dissertation analyzes the parasitic RECAP with multiple feeds for multiple-input multiple-output (MIMO) wireless channel capacity enhancement using different power constraints, a realistic noise model and varying degree of RECAP complexity [12]. As part of this study, a prototype parasitic RECAP was also built and MIMO capacity measurements were performed to support the theoretical results [13].

- Physical layer security methods have been proposed that use the time-varying wireless propagation channel between two nodes to establish secret keys. If an eavesdropper
(Eve) is not located close to one of the nodes, then most of the generated key bits are secure and can be used for encryption purposes. However, this technique has limitations for the case of static or line-of-sight (LOS) channels. In this case, random time variation of an effective propagation channel can be created by a randomly controlling a RECAP, thus restoring the ability to generate keys in LOS, static environments. Although this concept was demonstrated in [14], questions remained about the security of the method with respect to an eavesdropper as well as the required complexity of the reconfigurable antenna to provide peak performance of secure key establishment. These issues are studied in detail in this dissertation. Specifically, the role of reconfigurable antenna complexity for key establishment is analyzed using both simulations and measurements, for the case of a highly equipped eavesdropper surrounding the reconfigurable antenna [15].

- A new array synthesis objective is proposed for physical layer security, whose goal is to maximize secure information shared with a legitimate recipient in the presence of a passive eavesdropper for line-of-sight wireless transmission. By casting the problem into the form of a semi-definite program, it is found that the problem is convex and that optimal solutions can be efficiently found irrespective of the array topology. Furthermore, it is shown that radiated power of the optimal solution can be naturally decomposed into a signal pattern and noise pattern, providing an intuitive description of the optimal solutions and allowing comparison with standard array synthesis techniques. The analysis is further extended to multipath propagation channels, where the expected value of the security metrics is optimized.

- Although the concept of OTA testing has been established, it is a very complex and costly technology. This dissertation proposes the novel concept of the reconfigurable over-the-air chamber (ROTAC) that consists of a traditional reverberation chamber whose walls are lined with REs. This work explores the potential of the concept through simulation and proof-of-concept implementation. Simulations of two-dimensional chamber reveals that fading distribution, spatial correlation, frequency selectivity, and directional channel response can be controlled to generate useful syn-
thetic propagation channels [16]. Later an 11 × 11 inch prototype of ROTAC is built to demonstrate the practical implementation as well as the limitations associated with proposed scheme.

1.2 Organization of the Dissertation

To provide context for the ideas presented in this dissertation, Chapter 2 covers the background material on RECAPs, simulations and optimization strategies, and explores practical issues like losses and phase tunability. Furthermore, related background work on multiple-input multiple-output (MIMO) communications and wireless security is presented. Chapter 3 analyzes the capacity of MIMO systems employing RECAPs with a realistic thermal noise model for three different power constraints: average receive signal-to-noise ratio (SNR), maximum effective isotropic radiated power (EIRP), and average transmit power. Performance is studied not only for a noise-limited single link, but also in the presence of interference and multiple RECAP-equipped users. The impact of loss and finite bandwidth on the operation of the RECAP is also considered. The simulations are followed by a measurement campaign in line-of-sight (LOS) and non-LOS conditions in an indoor environment.

Chapter 4 explores the use of reconfigurable antennas to create channel randomness for secret key establishment in slow-varying and LOS propagation environments. The goal is to characterize the impact of reconfigurable antenna complexity on the performance of key establishment in the presence of a multi-antenna eavesdropper. To validate simulations, a 3-node measurement campaign is performed which analyzes the practical aspects of reconfigurable antennas associated with secure key establishment.

Chapter 5 focuses on the problem of optimizing an ideal reconfigurable antenna to provide peak physical layer security. The secure transmission problem is posed in a form analogous to that of conventional array synthesis, but in which information theoretic secrecy metrics are constrained as a function of eavesdropper angle or position as opposed to constraining radiated power as a function of transmission angle. The resulting methodology is referred to as secure array synthesis.
In chapter 6 attention is shifted to over-the-air (OTA) testing, and the idea of a reconfigurable over the air chamber (ROTAC) is proposed, whose purpose is to support OTA testing in a compact and cost-effective fashion. In order to demonstrate the effectiveness of the proposed method, a prototype of ROTAC is built and its performance is investigated for generating arbitrary field statistics on a device under test (DUT).

Conclusions and a discussion of future work are given in Chapter 7.
Chapter 2

Background

This chapter presents effective design techniques as well as efficient simulation and optimization strategies for reconfigurable antennas. Prior work on reconfigurable antennas for various communication applications is also discussed briefly.

2.1 Reconfigurable Antennas

Original ideas behind reconfigurable antennas date back to the work by Harrington [17] who studied reactively controlled directive arrays. Since then, work on reconfigurable antennas has referred to these adaptive antenna elements as switched parasitic elements, reconfigurable apertures [5], evolutionary antennas [18], and self-structuring antennas [19], with the different words sometimes having slight differences in meaning but the basic antenna structures having similar goals. Reconfigurability is generally attained by integrating semiconductor switches, such as PIN diodes or FETs, MEMS switches, liquid crystals, or tunable reactances such as varactor diodes inside the antenna.

The switched parasitic array, introduced in [17], is one example of a reconfigurable antenna. In this architecture, one or relatively few elements are connected to active RF circuitry, while the bulk of the antennas are connected to switched reactive loads having two possible states. By changing the state of the loads, the effective pattern of the array is altered. For closely-spaced antenna elements exhibiting mutual coupling, the state of the switched parasitic loads also modifies the active antenna impedance. Prior studies have used reconfigurable antennas extensively to evaluate their performance in beamforming [5], interference suppression [20], supporting multiple frequencies and polarizations.

Although it is completely expected that diminishing returns with increasing RECAP complexity in terms of the number of reconfigurable elements ($N_{RE}$) and number of recon-
figurable states ($N_{RS}$) will be experienced as the performance limit is approached, the level of complexity required to achieve the majority of the performance benefit has not been previously explored. Also, for a limited level of complexity (which might be dictated by an application), it is interesting to study the loss in performance compared to what might be achieved using the optimal solution. Finally, it is of interest to understand whether complexity in the number or type of elements is more important for maximizing complexity-limited performance. Research on these issues is the focus of this dissertation. Important practical issues like bandwidth, component tolerance, and loss, are also considered.

### 2.1.1 RECAP Design

Although many different RECAP architectures can be studied, attention is restricted to two specific architectures or topologies in this dissertation. The first one consists of a square array of half-wave dipole antennas occupying an area of $1\lambda \times 1\lambda$ in the $xy$ plane and height $\lambda/2$ in $z$ as shown in Figure 2.1, where one or more elements serve as feeds and the others are terminated with reconfigurable loads and act as REs. The number of REs can vary in the structure, where each RE can have $N_{RS}$ reconfigurable states (RSs). Ideally, REs can be assumed to be either switches or variable reactances, such that the reflection
coefficient presented at the $k$th port is $\Gamma_k = e^{j\alpha_k}$, where $\alpha_k \in [-180^\circ, 180^\circ]$. However in a practical antenna, losses will be associated with a fabricated REs.

The second reconfigurable aperture considered is a planar RECAP consisting of non-resonant (electrically small) patches connected by switches or variable reactances. Figure 2.2 shows a prototype of an $8 \times 8$ planar patch array structure constrained to a $1\lambda \times 1\lambda$ area. The structure consists of circular patches connected to each other using transmission lines. Patches have a radius of $0.038\lambda$ and are interconnected with transmission lines having length of $0.056\lambda$ and width of $0.015\lambda$. Note that unlike normal patch antennas that are approximately $\lambda/2$ and have a ground plane underneath, this structure is just a single plane with individual patches that are small compared to the operational wavelength. The differential feed used in this case is approximately in the middle of the structure and is marked as ‘F’ in Figure 2.2, where $N_E$ represents number of logical elements. Note that although a planar RECAP was analyzed in the author’s past work [9, 21], this dissertation focuses on the parasitic dipole RECAP explained above.

2.1.2 Hybrid Full-Wave/Network Analysis of RECAP Antennas

Full-wave simulation of RECAP antennas for all required configurations of the REs is computationally expensive, since many thousands of trials are typically required. Therefore an efficient simulation method is adopted that consists of full-wave simulation of the unterminated array combined with network analysis to find impedance or S-parameter char-
characteristics and radiation patterns for arbitrary termination impedances. This hybrid method has been proven to be exact assuming fairly standard assumptions [22].

Figure 2.3 depicts a generic RECAP antenna consisting of a single active feed port (Port 1) and additional ports that are terminated with reconfigurable reactances (Ports 2-N). A complete characterization of the antenna is possible by running $N$ full-wave simulations, where for the $k$th simulation, a source is used to excite the $k$th port and other ports are terminated with a convenient load. For this work, we apply a unit voltage excitation at the $k$th port and terminate all other ports in a short-circuit. We then use the Numerical Electromagnetics Code (NEC) to compute the embedded radiation pattern $e_{sc}^k(\theta, \phi)$ as well as the currents at all $N$ ports (note that we use a custom finite-difference time-domain code [23] for the computation of the planar RECAP). After all $N$ simulations, we have the vector $e_{sc}(\theta, \phi)$ with $k$th element $e_{sc}^k(\theta, \phi)$ and can easily construct the admittance matrix $Y$. As we use S-parameter analysis in this thesis, we can compute the S-parameters using

$$S = (I + Z_0 Y)^{-1}(I - Z_0 Y),$$

(2.1)
where $I$ is the identity matrix, and $Z_0$ is the system impedance. The radiation patterns with all non-excited ports terminated in the system impedance can be computed using

$$e^{mc}(\theta, \phi) = \frac{1}{\sqrt{Z_0}} e^{sc}(\theta, \phi) Y^{-1}(I - S). \quad (2.2)$$

Since this work considers dipole antennas, computations use $Z_0 = 72$ $\Omega$, which is close to the dipole self-impedance.

To compute the antenna characteristics for arbitrary loading of the RE ports, the general formulation begins with

$$\begin{bmatrix} b_F \\ b_R \end{bmatrix} = \begin{bmatrix} S_{FF} & S_{FR} \\ S_{RF} & S_{RR} \end{bmatrix} \begin{bmatrix} a_F \\ a_R \end{bmatrix}, \quad (2.3)$$

where $a$ and $b$ respectively represent vectors of incident and reflected waves at a set of ports. The quantities $a_F$ and $b_F$ are $N_F \times 1$ vectors at the feed ports, $a_R$ and $b_R$ are $N_{RE} \times 1$ vectors at the parasitic RE ports, and $S$ has been appropriately partitioned. Terminating the $k$th RE port with a load having reflection coefficient $\Gamma_{R,k}$ (computed using $Z_0$) that forms the $k$th diagonal element of the diagonal matrix $\Gamma_R$, we have $a_R = \Gamma_R b_R$. Using this in (2.3) yields

$$a_R = \Gamma_R (I - S_{RR} \Gamma_R)^{-1} S_{RF} a_F \quad (2.4)$$

$$b_F = \left[ S_{FF} + S_{FR} \Gamma_R (I - S_{RR} \Gamma_R^{-1}) S_{RF} \right] a_F, \quad (2.5)$$

where $\Gamma_F$ is the $N_F \times N_F$ reflection coefficient matrix looking into RECAP feed ports for the RE termination $\Gamma_R$. The embedded radiation patterns of the RECAP’s feed antennas ($e^{mc}(\theta, \phi)$) given the RE termination are computed using

$$\begin{bmatrix} e^{mc}_F(\theta, \phi) \\ e^{mc}_{RE}(\theta, \phi) \end{bmatrix} \begin{bmatrix} a_F \\ a_R \end{bmatrix} = \begin{bmatrix} e^{mc}_F(\theta, \phi) + e^{mc}_{RE}(\theta, \phi) \Gamma_R (I - S_{RR} \Gamma_R)^{-1} S_{RF} \end{bmatrix} a_F, \quad (2.6)$$
where \( e_{mc}^{FE}(\theta, \phi) \) and \( e_{mc}^{RE}(\theta, \phi) \) represent the portions of \( e_{mc}^{mc}(\theta, \phi) \) corresponding to the feed antennas and the REs, respectively.

### 2.1.3 Prototype of a Parasitic RECAP

Although planar RECAPs are more easily fabricated than parasitic RECAPs, an experimental parasitic RECAP was developed in this research due to its simple design. It consists of a \( 5 \times 5 \) array of parasitic monopole antennas confined to a \( 1\lambda \times 1\lambda \) aperture over a finite ground plane.

Figure 2.4 shows the design of the varactor-diode-based RE used in the prototype RECAP. The tuning voltage \( V_{bias} \) is supplied by an FPGA-controlled circuit that generates a uniformly-quantized bias voltage to each RE for each RE state. The tuning circuitry is fabricated on the lower side of the small printed circuit board at the base of the SMA connector. Figure 2.5 plots the corresponding magnitude and phase of \( S_{11} \) measured for several different REs at 2.54 GHz using a Rohde & Schwarz VNB20 vector network analyzer. \( S_{11} \) is measured at the input of the SMA connector when the monopole antenna is not attached as depicted in Figure 2.4(a). The results show that the REs provide a phase tunability of approximately 200° over \( 0 \leq V_{bias} \leq 5 \) V and that the loss (as manifest through \( |S_{11}| \)) tends to increase with bias voltage. The impedance mismatch loss contribution can be reduced by increasing the value of the series inductance in the circuit, but testing indicated
that this leads to reduced phase tunability. Since the variation of phase is not significant for $V_{\text{bias}} < 1$ V, the range $1 \leq V_{\text{bias}} \leq 5$ V has been quantized uniformly into $N_{\text{RS}}$ reconfigurable states in this work.

### 2.1.4 Optimization of RECAP

Due to the complicated relationship of RECAP operation on the state of the REs, finding the set of REs to achieve the required performance goal is a non-convex optimization, requiring some kind of global search. Although an exhaustive search would find the optimal solution, even with the hybrid simulation strategy the computational burden is too high for moderate and large values of $N_{\text{RE}}$ and $N_{\text{RS}}$.

Global optimization algorithm, such as simulated annealing, ant-colony optimization (ACO), particle swarm optimization (PSO), and genetic algorithms (GAs) are typically employed for RECAP optimization [24]. A GA was used herein to optimize the states of the RECAP, where a detailed implementation of GA is provided in [9]. Because the purpose of this work was not to optimize the genetic algorithm, but rather to use it as a tool to study
the performance benefit with increasing complexity, it is likely that other search methods would lead to very similar conclusions.

Note that global search algorithms may be too expensive for real time optimization, due to the extensive training overhead and computation time required. Some initial work on real time optimization of a parasitic RECAP has been published in [25, 26], which combines direct optimization of a reduced-order reflection model of the RECAP with efficient Newton-based root optimization for beamforming and null steering applications. However, the development of direct RECAP optimization methods that are more suitable for real-time optimization is still largely an open question.

2.2 RECAP for Pattern Synthesis and MIMO Communications

Although RECAPs with limited complexity had previously been used for pattern synthesis, this author’s work was the first to investigate the fundamental dependence of performance and complexity in RECAPs for beamforming and interference suppression applications [9–11, 21]. This analysis revealed that performance in terms of beamforming and interference suppression saturates for approximately eight REs per wavelength, which is similar to the minimum sampling required to sufficiently capture the degrees of freedom of fields in numerical electromagnetic solvers [10]. Additionally, it was found that performance saturates between $N_{RS} = 4$ and 8 states, suggesting that having many simple REs (where the aperture is better sampled) is more important than having fewer REs with more possible states. Finally, it was observed that even in the region of saturated performance, added complexity can be beneficial in terms of the convergence rate of the optimization algorithm, indicating that higher complexity may be favorable for real-time implementation of RECAP architectures [9].

RECAPs are also interesting for MIMO systems, where the optimal antenna array best exploits the multi-path to provide peak capacity while using as few active RF chains as possible. Also, for multi-user systems RECAPs can adapt patterns to dynamically partition spatial reuse of spectral resources. To place the work in this dissertation in the proper context, it is worthwhile to review existing work. A practical antenna solution providing multiple patterns with a single fixed antenna is presented in [27], exhibiting improved performance.
compared to spatially separated dipoles. Capacity maximization using planar RECAPs at transmit and receive is investigated in [28], where each antenna acts as a single RECAP. A reconfigurable MIMO array consisting of two dipole elements is introduced in [29], where by adaptively changing the length of the dipoles, modest increases in single user capacity are possible. The study in [30] shows that MIMO systems with reconfigurable antennas have a maximum diversity order equal to the product of the number of transmit antennas, receive antennas, and the reconfigurable states. This idea is expanded in [31], where not only practical space-time coding methods that code over the antenna state to maximize diversity are developed, but also practical aspects like antenna switching time are considered.

This previous work on reconfigurable MIMO systems has some limitations. First, only simple termination-independent receiver noise was considered, which is known to be inaccurate for analyzing MIMO systems with variable termination [32]. Second, limited reconfigurability was considered, which may be insufficient to exploit the degrees of freedom of the occupied aperture. Third, the role of the power constraint has not been studied in detail, as typically only an average transmit power constraint has been assumed. Finally, capacity maximization for a single link limited by thermal noise has been considered, but multi-user systems with interference are more realistic for today’s wireless scenarios. The work in this dissertation provides a more comprehensive analysis of the capacity enhancement possible with reconfigurable antennas by addressing these previous shortcomings [12, 13, 33]. It is important to mention that apart from the performance versus complexity analysis, most of the simulation-based work on MIMO capacity using RECAPs was also presented in this author’s Masters Thesis in 2010 [34]. However, this material is included in this dissertation for the sake of completeness, allowing comparison with the results from the measurement campaign conducted later in 2012.

2.3 RECAPs for Physical Layer Security

Security is a vital consideration for today’s wireless communications systems, and there is growing interest in physical layer security methods that exploit the antennas and propagation channel to provide an additional layer of protection over existing cryptographic techniques. One such method involves generating secret keys from random reciprocal channel
fluctuations [35, 36], allowing keys to be automatically generated at two nodes without the need for secret information to be shared a priori. This technique is referred to as reciprocal channel key generation (RCKG). As shown in [35], very long keys can be generated rapidly for fading, non line-of-sight (NLOS) channels that exhibit Gaussian statistics and low temporal correlation of channel observations. However, such methods are hindered by channels with high spatial and temporal correlation, like line-of-sight (LOS) and static channels.

The ability to improve security by creating a time-varying effective channel with reconfigurable parasitic arrays was introduced in [37], allowing RCKG to be applied to both LOS and static channels. Although this represents a very encouraging solution in quasi-static situations, several outstanding questions regarding this technique remain. First, exploiting artificially induced channel variation may not be as secure as exploiting fading that occurs naturally, and while it is expected that channel richness and the antenna complexity play a crucial role in the level of security, the sensitivity to these parameters is unclear. Second, the distribution of random channels created by reconfigurable antennas is unknown. Ideally, the variation should be made Gaussian, and it is of interest to see if careful system design can achieve this. In the case that the variations cannot be made Gaussian, performance evaluation needs to be assessed through development of a numerical algorithm for computing the key rate. Finally, the security of these methods in the presence of a very capable eavesdropper needs to be investigated, such as when the RECAP is surrounded by eavesdropper antennas. This dissertation shows extensive analysis employing both simulations and measurements to answer these outstanding questions [15, 38, 39].

These investigations regarding the use of RECAPs in physical layer security raise the question of how an adaptive or reconfigurable array can be optimally controlled to maximize the secure key generation rate, since previously RE control was done in an ad-hoc way. This led to the new concept of secure array synthesis, which jointly synthesizes signal and noise patterns to maximize security metrics with respect to an unknown eavesdropper position. Work detailed in subsequent chapters highlights these developments.
Chapter 3

MIMO Capacity Enhancement using Reconfigurable Antennas

Reliable and high performance transmission continues to be a major goal of wireless communication systems, which is significantly enhanced by arrays employing beamforming and diversity techniques. Multiple-input multiple-output (MIMO) wireless technology emerged in the 1980’s and has gained increasing attention due to the significant gains in channel capacity [40, 41] made possible by exploiting channel multipath with spatial multiplexing. In a communication system, the channel matrix includes effects of the physical propagation environment and antenna radiation and reception characteristics. Antennas can be viewed as transmit and receive filters that are ideally matched to the physical channel, enhancing signals of interest and mitigating noise and interference to maximize capacity [42]. Although for a single fixed antenna, no adaptation of spatial filtering is possible, reconfigurable antennas can be optimized to exploit the multipath propagation environment.

This chapter provides a comprehensive analysis of capacity enhancement possible with reconfigurable antennas using simulations and measurements. First, a parasitic RECAP consisting of a $9 \times 9$ array having sufficient complexity to exploit a compact $1\lambda \times 1\lambda$ aperture is studied with simulation. In contrast to [28], the complete aperture is exploited rather than using separate RECAPs for each MIMO antenna. A realistic noise model is considered in order to take into account the effect of matching on amplifier noise. Three realistic but distinct power constraints are also considered, indicating where RECAPs are most effective: 1) average signal-to-noise (SNR), where transmit and receive power are normalized and the focus of optimization is on channel orthogonality and multipath enhancement, 2) effective isotropic radiated power (EIRP), which allows power enhancement at the receiver but not at the transmitter, which is more practical for many of today’s communication systems,
and 3) average transmit power, which is a commonly assumed constraint allowing power enhancement at both transmit and receive.

In addition to considering a single link limited by thermal noise, fixed interference and multiple RECAP-equipped links are also considered. Furthermore, a complexity versus performance analysis is performed, highlighting the diminishing returns with an increase in complexity of the RECAP for MIMO capacity.

The simulation work is extended by performing actual channel measurements with a prototype RECAP. Measurements with one of the communicating nodes equipped with a 5×5 square parasitic RECAP confirm that several fold capacity increase is possible compared to fixed (non-RECAP) MIMO systems.

### 3.1 Analysis of Parasitic RECAP Structure

The structure considered in this study is depicted in Figure 3.1(a), which is a 9×9 dipole array consisting of z-oriented half-wave dipoles constrained to an area of 1λ×1λ in the xy plane. Each dipole is either an active “feed” (connected to a transmit or a receive chain) or terminated with a reconfigurable element (RE), each of which has \( N_{RS} \) possible reconfigurable states (RSs) to ensure sufficient control over the aperture [10]. The top view of the structure is shown in Figure 3.1(b), where REs and feeds are indicated by squares and circles, respectively. In this work, the propagation is considered in the xy plane, where the two-dimensional array can generate patterns with both endfire and broadside characteristics.

The complexity of the RECAP structure depends first on the number of reconfigurable elements since this defines how many digital (for switched loads) or analog (for variable reactances) outputs must be controlled. Second, complexity is also a function of the number of reconfigurable states that each of the REs can assume, where the number of reconfigurable bits \( N_{RB} = \log_2 N_{RS} \) is used to conveniently define the complexity of the RE states. The total number of states for the complete RECAP is \( N_{TRS} = N_{RS}^{N_{RE}} = 2^{N_{RB}N_{RE}} \), and the total RECAP complexity is defined as \( N_{RB}N_{RE} \), representing the number of bits required to configure all REs.

For performance versus complexity analysis, the number of REs is varied by always having all 81 antennas present, but only terminating \( N_{RE} \) of the antennas with a recon-
Figure 3.1: Configurations for non-RECAP and RECAP arrays: (a) Perspective view of the parasitic RECAP with 2 feeds. (b) Top view of RECAP configurations, where red boxes show RE positions, blue stars and circles show feed locations for 2×2 and 4×4 MIMO respectively. (c) Top view of antenna positions for non-RECAP for 2×2 MIMO (stars) and 4×4 MIMO (circles), where boxes are empty locations.

The set of terminated antennas was chosen to try to maximize the distance between REs, thus sampling the aperture as efficiently as possible. Configurations for values of $N_{RE}$ ranging from 4 to 79, when RECAP has two feed elements are depicted in Figure 3.2. REs are assumed to be variable capacitances, such that the reflection coefficient presented at the $k$th port is $\Gamma_k = e^{j\alpha_k}$, where $\alpha_k \in [-180^\circ, 0^\circ]$. This analysis assumes that $\alpha_k$ is uniformly distributed on $[-180^\circ, 0^\circ]$.

3.1.1 System Model

Efficient simulation of the RECAP is accomplished by combining full-wave simulation of the array with network analysis for RE loading. Based on the analysis presented in
Figure 3.2: RECAP structure consisting of a $9 \times 9$ dipole array, where $N_{RE}$ elements are terminated with REs (filled circles) and feeds are marked by red squares.

Section 2.1.2, $e^{inc}(\theta, \phi)$ is used to represent the matched patterns of feed ports when RE ports are terminated with $\Gamma_R$. This analysis considers using RECAPs at transmitter (Tx) and receiver (Rx) to form a complete system, as depicted in Figure 3.3(a). Note that unprimed and primed RECAP quantities denote those at Tx and Rx, respectively. At Tx the $k$th feed is connected to source voltage $v_{F,k}$ with internal impedance $Z_s = Z_0$. The incident traveling waves $a_F$ on the feed ports are simply $a_F = v_F/(2\sqrt{Z_0})$, and radiated far fields are given by (2.6). The RE-terminated receive array is modeled in a similar manner, except that due to the external incident field, a source wave term $b'_0$ must be included, such that $b'_F = \Gamma'_{F,in}a'_F + b'_0$. Assuming a plane wave arriving at angle $(\theta'_F, \phi'_F)$ and reciprocity,

$$b'_0 = \left[e^{inc}(\theta'_F, \phi'_F)\right]^T e^{inc}(\theta'_F, \phi'_F),$$

where $e^{inc}$ gives the polarization and complex amplitude of the incident plane wave.

A multipath model is assumed consisting of $K$ clusters and $L_k$ paths (or rays) within the $k$th cluster, where the $\ell$th path in the $k$th cluster has angle of departure $(\theta_{k\ell}, \phi_{k\ell})$. 

19
angle of arrival ($\theta'_{k\ell}, \phi'_{k\ell}$), complex amplitude $\alpha_{k\ell}$, and time of arrival $\tau_{k\ell}$, or $e^{inc}((\theta'_{k\ell}, \phi'_{k\ell})) = \alpha_{k\ell}e^{-j\omega \tau_{k\ell}}e^{mc}(\theta_{k\ell}, \phi_{k\ell})$, where $\omega$ is frequency. Although depolarization of the paths is not considered in this work, this could be included by making $\alpha_{k\ell}$ a matrix. Superimposing the waves due to all paths,

$$b'_0 = \sum_{k=1}^{K} \sum_{\ell=1}^{L_k} [e^{mc}(\theta'_{k\ell}, \phi'_{k\ell})]^T \alpha_{k\ell} e^{-j\omega \tau_{k\ell}} e^{mc}(\theta_{k\ell}, \phi_{k\ell}) a_F.$$  \hspace{1cm} (3.2)

### 3.1.2 Noise Modeling

In order to consider a realistic system, where noise from the low-noise amplifier (LNA) at the receiver depends on the feed reflection, an LNA model equivalent to [32] is employed, where equivalent forward ($a_f$) and reverse ($b_r$) traveling noise waves at the LNA input are needed to properly model real transistors. The receiver consists of a matching network, forward and reverse noise sources, and LNA as shown in Figure 3.3(a). The multiport LNA is assumed to consist of multiple uncoupled LNAs with optimal reflection coefficient $\Gamma_{opt}$, normalized equivalent noise resistance $r_n$, and minimum noise figure $F_{min}$, available from a standard LNA data sheet.

Straightforward analysis at the connection of array and matching network reveals

$$b_M = \Gamma_{FM} a_M + b_{FM}.$$  \hspace{1cm} (3.3)
where

\[ \Gamma_{FM} = S_{M,22} + S_{M,21} \Gamma'_{F,in} (I - S_{M,11} \Gamma'_{F,in})^{-1} S_{M,12}, \]  
(3.4)

\[ b_{FM} = S_{M,21} [I + \Gamma'_{F,in} (I - S_{M,11} \Gamma'_{F,in})^{-1} S_{M,11}] b'_\eta. \]  
(3.5)

The incident wave \( a_A \) into the amplifier is found to be

\[ a_A = \frac{[I - \Gamma_{FM} \Gamma_A]^{-1}}{Q} (\Gamma_{FM} b_\eta + a_\eta + b_{FM}). \]  
(3.6)

In this work, a fixed (non-RECAP) array is used as a reference case for gauging performance improvement, and an identical uncoupled matching network is assumed on each of the \( N'_F \) receive feeds such that \( \Gamma_{FM} \approx \Gamma_{opt} I \) for the reference, where \( \Gamma_{opt} \) is the source reflection coefficient that provides optimal noise performance. The same uncoupled matching network is employed for the RECAP, and noise coupling from one feed to the next and deviation of \( \Gamma_{FM} \) can lead to reduced SNR.

Figure 3.3(b) shows the uncoupled matching arrangement on each branch that transforms \( \Gamma'_{F,in,k} = 0 \) to \( \Gamma_{FM,in,k} = \Gamma_{opt} \) using a reciprocal lossless matching network, such that \( S^H S = I \), where \( S \) is a 2×2 matrix. The required conditions are satisfied with

\[ S_{11} = S_{22} = \Gamma_{opt}, \]  
(3.7)

\[ S_{12} = S_{21} = j \sqrt{1 - |\Gamma_{opt}|^2} e^{j \angle \Gamma_{opt}}. \]  
(3.8)

\( S_M \) is a 2×2 block matrix, where the \( ij \)th block is equal to \( S_{ij} I \) from (3.7) and (3.8), and \( I \) is an \( N'_F \times N'_F \) identity matrix. Note that the fixed matching network can also be lumped into the LNA to form the effective LNA shown in Figure 3.3(b), with new optimal reflection coefficient \( \Gamma'_{opt} \) and equivalent noise resistance \( r'_n \).
Plugging (3.2) into (3.5) and the result into (3.6) yields

\[ y = Q \left( \frac{\Gamma_{FM} b + a}{n} \right) + \sum_{M,11} \left[ I + \Gamma'_{FM} (I - S_{M,11} \Gamma'_{FM})^{-1} S_{M,11} \right] \sum_{Rx,Tx} a_x H \]

where \( H \) is the channel matrix, \( S_{Rx,Tx} \) is from (3.2), \( n \) is noise, and \( x \) and \( y \) are input and output signals. The linear term \( Q \) applied to both signal and noise does not change capacity and is omitted. The noise covariance \( R_{\eta} = \mathbb{E}\{nn^H\} \) is

\[ R_{\eta} = \Gamma_{FM} \Gamma_{FM}^H \sigma_b^2 + \sigma_a^2 + 2 \Re \{ \Gamma_{FM} \sigma_{ba} \}, \tag{3.10} \]

where \( \sigma_b^2, \sigma_a^2, \) and \( \sigma_{ba} \) are [43]

\[ \sigma_b^2 = \mathbb{E}\{|b_{\eta,i}|^2\} = \frac{\sigma_v^2}{Z_0} \left[ -\frac{F_{\min} - 1}{4r_n} + \frac{1}{|1 + \Gamma_{opt}|^2} \right], \tag{3.11} \]

\[ \sigma_a^2 = \mathbb{E}\{|a_{\eta,i}|^2\} = \frac{\sigma_v^2}{Z_0} \left[ \frac{F_{\min} - 1}{4r_n} + \frac{|\Gamma_{opt}|^2}{|1 + \Gamma_{opt}|^2} \right], \tag{3.12} \]

\[ \sigma_{ba} = \mathbb{E}\{b_{\eta,i} a_{\eta,i}^*\} = \frac{\sigma_v^2}{Z_0} \frac{\Gamma_{opt}}{|1 + \Gamma_{opt}|^2} e^{j(\pi - \angle \Gamma_{opt})}, \tag{3.13} \]

where \( r_n = R_n/Z_0 \), \( R_n \) is the equivalent-noise resistance, \( \sigma_v^2 = 4P_{\text{ref}} R_n \) is the noise voltage covariance, \( P_{\text{ref}} = \kappa T_0 W \), \( \kappa \) is Boltzmann’s constant, \( T_0 \) is reference temperature, and \( W \) is bandwidth. Since \( P_{\text{ref}} \) is the same for the reference and RECAP systems and SNR of the reference system is fixed, \( P_{\text{ref}} \) has no effect on capacity and is set to 1.

Note that since a data sheet typically assumes \( Z_0 = 50\Omega \), which is different from the value used in this analysis, the transformation

\[ \Gamma_{opt} = \frac{Z_0^d (1 + \Gamma_{\text{opt}}^d) - Z_0 (1 - \Gamma_{\text{opt}}^d)}{Z_0^d (1 + \Gamma_{\text{opt}}^d) + Z_0 (1 - \Gamma_{\text{opt}}^d)} \tag{3.14} \]

is required, where \( \Gamma_{\text{opt}} \) and \( Z_0^d \) are optimal reflection and reference impedance from the data sheet.
Summarizing, the MIMO input-output relationship is given by (3.9), where RE-dependent noise covariance $R_\eta$ is computed from (3.10)-(3.13), where parameters $R_n$, $\Gamma_{ds}^{\text{opt}}$, and $F_{\text{min}}$ are available from a standard LNA specification. Although computation of the noise covariance in this way seems cumbersome compared to MIMO analyses that directly specify $R_\eta$, the added complexity is necessary to capture noise coupling of the active ports and variable input impedance of the receive array, which both affect capacity when thermal noise is significant compared to interference.

### 3.1.3 LNA Specification

This analysis uses the MAXIM MAX2656 LNA, having $F_{\text{min}} = 1.79$ dB, noise-equivalent resistance $R_n = 43.23\Omega$, and optimum reflection coefficient $\Gamma_{ds}^{\text{opt}} = 0.130\angle124.5^\circ$ (at 1960 MHz and $Z_0^{\text{ds}} = 50\Omega$) [44]. Since the specific LNA may affect the simulations and conclusions, the impact of the LNA choice is briefly analyzed.

Analysis of the RECAP mainly depends on how sensitive the noise figure of the LNA is to the reflection coefficient presented by the RECAP. Noise figure for uncoupled LNAs is [43]

$$F = F_{\text{min}} + 4r_n \frac{|\Gamma_{\text{in}} - \Gamma_{\text{opt}}|^2}{|1 + \Gamma_{\text{opt}}|^2(1 - |\Gamma_{\text{in}}|^2)} $$

(3.15)

where $\Gamma_{\text{in}}$ is the reflection coefficient looking into the output of one of the matching networks. Assuming a lossless matching network shown in Figure 3.3(b) that transforms the source reflection $\Gamma_{F,\text{in},k}' = 0$ to $\Gamma_{F,\text{in},k} = \Gamma_{\text{opt}}$ of the LNA, it can be shown that for $\Gamma_{F,\text{in},k}' \neq 0$,

$$F = F_{\text{min}} + 4r_n \left( \frac{1 - |\Gamma_{\text{opt}}|^2}{1 + |\Gamma_{\text{opt}}|^2} \right) \frac{|\Gamma_{F,\text{in},k}'|^2}{1 - |\Gamma_{F,\text{in},k}'|^2} $$

(3.16)

where $r_n'$ is the the equivalent LNA noise resistance referenced back to the input of the matching network where $\Gamma_{\text{opt}}' = 0$.

Figure 3.4 shows noise figure degradation $F - F_{\text{min}}$ in dB for different values of $r_n'$ and $|\Gamma_{\text{in}}|^2$ using (3.16), where $\Gamma_{\text{in}} \triangleq \Gamma_{F,\text{in},k}$. As $r_n'$ increases, the penalty of mismatch can increase dramatically. However, the amplifier used in this analysis (as indicated in the figure) has moderate sensitivity to mismatch, making it a good candidate for this initial study.
Amplifiers with much higher $r'_n$ would simply increase mismatch penalty, which would more strongly constrain the set of useful RECAP states, possibly resulting in reduced capacity.

### 3.1.4 MIMO Channel Modeling

The channel matrix $H$ is given by (3.9), where $S_{\text{Rx},\text{Tx}}$ is found according to the path-based model in (3.2). In this work attention is restricted to the azimuthal plane ($\theta$ and $\theta'$ are 90°). Two propagation models are assumed for the paths between Tx and Rx:

#### Uniform Model

In this simple model, a single cluster is assumed ($K = 1$) with $L = L_1$ rays having arrival times $\tau_{1\ell} = 0$. Angles of arrival ($\phi'_{1\ell}$) and departure ($\phi_{1\ell}$) are uniformly distributed on $[0^\circ, 360^\circ]$ and $\alpha_{1\ell}$ has a unit variance complex normal distribution.
SVA Model

The more realistic Saleh-Valenzuela angular (SVA) model [45] assumes \( K \) clusters, where the arrival of the \( k \)th cluster (\( \tau_k \)) has the conditional pdf

\[
p(\tau_k|\tau_{k-1}) = \Lambda e^{-\Lambda(\tau_k - \tau_{k-1})}, \quad \tau_{k-1} < \tau_k < \infty, \tau_1 = 0,
\]

(3.17)

where \( \Lambda \) is the arrival rate of the clusters. Relative arrival time of the \( \ell \)th ray within the \( k \)th cluster has the pdf

\[
p(\tau_{k\ell}|\tau_{k,\ell-1}) = \lambda e^{-\lambda(\tau_{k\ell} - \tau_{k,\ell-1})}, \quad \tau_{k,\ell-1} < \tau_{k,\ell} < \infty,
\]

\[
\tau_{k1} = \tau_k,
\]

(3.18)

where \( \lambda \) is the arrival rate of rays.

The complex amplitude of the \( \ell \)th ray in the \( k \)th cluster (\( \alpha_{k\ell} \)) is complex gaussian, where the variance decays exponentially with arrival time according to

\[
E\{|\alpha_{k\ell}|^2\} = e^{-\tau_k/T_C}e^{-(\tau_{k\ell} - \tau_k)/T_R},
\]

(3.19)

and \( T_C \) and \( T_R \) are the cluster and ray decay time constant, respectively. The azimuthal angle of the \( k \)th cluster at transmit and receive is \( \Phi_k \) and \( \Phi'_k \), respectively, which are uniformly distributed on \([0^\circ, 360^\circ]\). The relative transmit and receive angles of the \( \ell \)th ray in the \( k \)th cluster are \( \nu_{k\ell} = \phi_{k\ell} - \Phi_k \) and \( \nu'_{k\ell} = \phi'_{k\ell} - \Phi'_k \), which follow a double-sided Laplacian distribution with pdf \( p(\nu) = 1/(\sqrt{2}\sigma)\exp[-|\sqrt{2}\nu/\sigma|] \), where \( \sigma \) is the angular spread.

Although RECAPs that can adapt to each instantaneous value of \( \alpha_{k\ell}, \phi_{k\ell} \) and \( \phi'_{k\ell} \) are optimal, this rate of adaptation may be unrealistic for practical implementation. Thus a system that adapts average RECAP performance is also considered where the \( \phi_{k\ell} \) and \( \phi'_{k\ell} \) are fixed, but only the \( \alpha_{k\ell} \) are random. The former and latter cases are referred as instantaneous and average RECAP optimization, where average performance is computed in the latter case using 10 realizations of \( \alpha_{k\ell} \).
3.1.5 Genetic Algorithm

Due to the large number of RE combinations, obtaining the optimal solution with an exhaustive search is not feasible, and a genetic algorithm (GA) is employed. The GA employed in this work is basically equivalent to that described in [10], except that REs at both transmit and receive end are jointly optimized to maximize the capacity.

3.2 MIMO Capacity With Constraints

For the analysis of MIMO channel capacity using simulations, the RECAP structure explained in Section 3.1 is used, for both Tx and Rx, forming a MIMO system. In order to properly scale power and assess RECAP capacity gain, a reference non-RECAP antenna array is considered, having the same number of feeds and constrained to the same area as the RECAP and consisting of matched dipoles. Although antennas were placed as far apart as possible for the reference case, some initial experiments were required to find the best placement of feeds for the RECAP to give peak capacity. Having feeds too close to the aperture center or edge reduced the capacity of the RECAP, and a balanced arrangement gave the best performance.

Channel capacity is computed from

$$C = \log_2(\det[I + HR_xH^H R^{-1}_\eta])$$, \hspace{1cm} (3.20)

and for equal power allocation \( R_x = \frac{P_T}{N_F} I \), where \( P_T \) is the total Tx power, and \( N_F \) is the number of Tx feeds. Lumping noise covariance into the channel matrix results in

$$H_{\eta} = HR^{-1/2}_\eta$$, \hspace{1cm} (3.21)

where \( R^{-1/2}_\eta \) is computed using (3.10). Plugging (3.21) into (3.20)

$$C = \log_2(\det[I + \frac{P_T}{N_F} H_{\eta}H^H])$$, \hspace{1cm} (3.22)

which can be interpreted as the capacity of an effective channel \( H_{\eta} \) for i.i.d. noise (unit variance) and transmit power \( P_T \).
A convenient way of enforcing the different power constraints in this study is to first define the average single-input single-output (SISO) gain of a given system as

\[ G_{\text{SISO}}(H) = \frac{\|H\|_F^2}{N_F N_F'}, \quad (3.23) \]

where \( \| \cdot \|_F \) is Frobenius norm and \( N_F' \) is the number of feeds at Rx, which indicates the average power gain provided by channel matrix \( H \) with respect to all active ports. The desired SNR \( \rho \) of a system can then be fixed by normalizing that system by its SISO gain according to

\[ \frac{H}{\eta} = G_{\text{SISO}}^{-1/2}(H_\eta) \quad \frac{H}{\eta}, \quad (3.25) \]

\[ \frac{H}{\eta} = G_{\text{SISO}}^{-1/2}(H_\eta) \quad \frac{H}{\eta}, \quad (3.26) \]

resulting in the equivalent capacity expression

\[ C = \log_2(\det[I + \frac{\rho}{N_F} H_\eta H_\eta^H]), \quad (3.24) \]

where \( \cdot \) represents the normalized quantity. Below it is explained that how this normalization can be used to implement power constraints for three realistic cases:

**Fixed SNR Constraint (Case 1):** In this case, the total amount of transmitted/collected power is the same for both the non-RECAP and RECAP structures. This constraint ensures that the RECAP can only increase capacity by improving channel orthogonality or conditioning. For Case 1, channel matrices corresponding to a non-RECAP reference (REF) and the RECAP are normalized as

\[ \frac{H}{\eta,\text{REF}} = G_{\text{SISO}}^{-1/2}(H_\eta,\text{REF}) \quad \frac{H}{\eta,\text{REF}}, \quad (3.25) \]

\[ \frac{H}{\eta} = G_{\text{SISO}}^{-1/2}(H_\eta) \quad \frac{H}{\eta}, \quad (3.26) \]

Normalizing each system individually by its own SISO gain forces the RECAP and reference case to both have average SISO SNR \( \rho \) when computing capacity with (3.24).

**Max EIRP Constraint (Case 2):** Here the EIRP of the RECAP is constrained to be no larger than that of the reference (non-RECAP) system. This is accomplished by setting transmit power \( P_T \) such that a prescribed SNR \( \rho \) is obtained for the reference system, and this same transmit power is also used for the RECAP system. Maximum EIRP of the
RECAP system is then limited to be equal to or lower than that of the reference system by scaling the embedded RECAP radiation patterns according to

$$e_{i}^{mc}(\phi) = \frac{\max_{\phi} |e_{i,REF}^{mc}(\phi)|}{\zeta_{i}} e_{i}^{mc}(\phi), \quad (3.27)$$

where $e_{i}^{mc}(\phi)$ refers to the radiation pattern of the $i$th feed at Tx, $e_{i,REF}^{mc}(\phi)$ refers to the one corresponding to the $i$th feed of the reference (non-RECAP) Tx, and $e_{i}^{mc}(\phi)$ is used in place of $e_{i}^{mc}(\phi)$ when computing $S_{Rx,Tx}$ in (3.2) when $\zeta_{i}$ is less than or equal to 1 (i.e. when a RECAP feed provides higher maximum gain than a non-RECAP feed). The non-RECAP and RECAP channels are normalized respectively with (3.25) and

$$H_{\eta} = G_{SISO}^{-1/2}(H_{\eta,REF}) H_{\eta}. \quad (3.28)$$

Note that although the advantage of transmit beamforming by the RECAP is removed due to the maximum EIRP normalization, both channels are normalized by the SISO gain of the reference system, preserving possible enhanced power collection with receive RECAP beamforming.

*Average Transmit Power Constraint (Case 3):* In this case, only average transmit power is constrained such that a prescribed SNR $\rho$ is obtained for the reference system, and no constraint is placed on directional gain of Tx or Rx antennas. Specifically, channel matrix normalization is done using (3.25) and (3.28), allowing the RECAP to obtain a power advantage through both transmit and receive beamforming.

### 3.3 Performance Versus Complexity Analysis

In order to study the effect of increasing complexity on the performance of the RECAP structure, both $2 \times 2$ and $4 \times 4$ MIMO systems are considered. Simulations were performed for all combinations of the number of reconfigurable elements $N_{RE} = \{4, 8, 13, 31, 63, 79\}$ for $2 \times 2$ MIMO system, $N_{RE} = \{4, 8, 13, 29, 61, 77\}$ for $4 \times 4$ MIMO system, and the number of reconfigurable states $N_{RS} = \{2, 4, 8, 16, 32\}$. Furthermore, the power constraints presented in Section 3.2 are also considered in this analysis. The channel capacity is computed for a
single user communication using (3.24) with reference SNR of $\rho = 10$ dB, where non-RECAP capacity is independent from the power constraint and is 5.54 bits/s/Hz for a $2 \times 2$ MIMO system with $L = 4$ multipath, and 9.65 bits/s/Hz for a $4 \times 4$ MIMO system with $L = 8$ multipath.

Figure 3.5 plots the optimized capacity for all combinations of $N_{RE}$ and $N_{RS}$ versus total RECAP complexity or $\log_2 N_{TRS} = N_{RE}N_{RB}$. Figure 3.5(a) and (b) plots the results for $2 \times 2$ and $4 \times 4$ MIMO systems respectively, when the average transmit power is constrained (Case 3). The curves clearly show diminishing performance returns with increasing number of reconfigurable elements $N_{RE}$ and number of reconfigurable bits $N_{RB}$. Results reveal that for low values of $N_{RE}$, having more states for a given level of complexity may be more helpful than having more REs. The performance saturates at $N_{RE} = 63$ and $N_{RE} = 61$ for $2 \times 2$ and $4 \times 4$ MIMO systems, respectively. For fixed value of $N_{RE}$, maximum increase in capacity takes place while going from 2 to 4 RSs and is negligible for $N_{RS} > 8$. A comparison with the non-RECAP case reveals that for a RECAP with sufficient complexity, approximately 150% capacity enhancement is possible for the $2 \times 2$ MIMO system and 100% for the $4 \times 4$ MIMO system.

Figure 3.5(c) and (d) plots the corresponding results for max EIRP power constraint (Case 2). The overall trend is the same as observed for average transmit power constraint, however the capacity improvement when compared with non-RECAP reduces to approximately 100% for the $2 \times 2$ and 53% for the $4 \times 4$ MIMO systems. Figure 3.5(e) and (f) plots the results for fixed SNR constraint (Case 1). In this scenario the performance gets saturated much earlier (in terms of $N_{RE}$) as compared to the previous two cases. Also the performance advantage of using RECAPs is reduced to only 25% for the $2 \times 2$ MIMO and 40% for the $4 \times 4$ MIMO systems.

Overall the results depict that RECAPs are most advantageous when beamforming is allowed at receive and/or transmit nodes. The required complexity in RECAP to attain optimal performance depends on the underlying power constraint, and in the best case scenario the performance saturates for approximately eight REs per wavelength with 8 states per RE. Based on these findings, rest of analysis uses $N_{RS} = 8$, $N_{RE} = 79$ for the $2 \times 2$ MIMO system, and $N_{RE} = 77$ for the $4 \times 4$ MIMO system.
Figure 3.5: MIMO Capacity versus RECAP complexity: (a) $2 \times 2$ MIMO with average transmit power constraint (b) $4 \times 4$ MIMO with average transmit power constraint (c) $2 \times 2$ MIMO with EIRP constraint (d) $4 \times 4$ MIMO with EIRP constraint (e) $2 \times 2$ MIMO with average SNR constraint (f) $4 \times 4$ MIMO with average SNR constraint. Numbers 1 to 5 under curves show $N_{RB}$ values (same pattern used but not labeled in other curves).
3.4 MIMO Capacity Analysis Using Simulations

Since the advantage of RECAP may depend on the number of antennas, both $2 \times 2$ and $4 \times 4$ MIMO systems are considered in this analysis. Figure 3.1 shows the top view of transmit/receive antennas for the RECAP and non-RECAP structures for the analyzed $2 \times 2$ and $4 \times 4$ MIMO systems. Results are for the uniform path-based model and reference SNR $\rho = 10$ dB, unless otherwise noted.

3.4.1 Single User MIMO Capacity

Channel capacity for single user communication is computed using (3.24) where $H_\eta$ is computed using the cases in Section 3.2.

$2 \times 2$ MIMO System

Figure 3.6(a) plots the capacity for the RECAP and non-RECAP structures for average and instantaneous optimization. Note that capacity for the non-RECAP does not change with constraint type, since the reference has constant SNR, and the slight difference with respect to optimization type is due to different Monte Carlo realizations. For fixed SNR (Case 1), RECAP capacity is only marginally better than that of the non-RECAP, indicating that two channels of sufficient quality are obtained without reconfigurability, and the RECAP cannot significantly improve this.

The main advantage of RECAP is power, with significant improvements seen when moving to the EIRP constraint (Case 2) and the transmit power constraint (Case 3). It is also apparent that average optimization is only slightly worse than instantaneous optimization, which is reasonable for power enhancement, since multipath directions are mainly important, not the phases of signals sent in those directions.

$4 \times 4$ MIMO System

Figure 3.6(b) shows that RECAP performance is more flat with respect to the constraint type for the $4 \times 4$ MIMO system, suggesting that power advantage is less important and more opportunity for improving channel conditioning exists. Also a more significant gap is seen between average and instantaneous optimization, indicating not only mutli-path
directions but also phases are important to attain peak capacity. Finally it is interesting
that the transmit power constraint for the 2×2 RECAP system gives almost the same per-
formance as the 4×4 system with the EIRP constraint.

### 3.4.2 Single User MIMO Under Interference Constraint

Most practical systems for personal wireless communications are interference limited,
and therefore the effect of interference on single-link capacity is analyzed here in detail. In
order to model the effect of interference, \( \mathbf{R}_\eta' \) is extended to be the covariance matrix of noise
and interference, or

\[
\mathbf{R}_\eta' = \mathbf{R}_\eta + \hat{\mathbf{H}} \hat{\mathbf{H}}^H \frac{\hat{P}_T}{N_F},
\]

where \( \hat{\mathbf{H}} \) represents the channel matrix between the interferer and receiving antennas, other
\( \hat{\cdot} \) quantities are for interferer, analogous to those at Tx, and it is assumed that \( \hat{N}_F = N_F \).
Plugging (3.29) into (3.20) and simplifying yields

\[
C = \log_2(\det[I + \frac{\rho}{N_F}(I + \frac{\rho}{\hat{N}_F} \hat{\mathbf{H}} \hat{\mathbf{H}}^H)^{-1} \mathbf{H}_\eta \mathbf{H}_\eta^H])
\]
Figure 3.7: Channel capacity for single user 2×2 MIMO with fixed interference for a simple non-RECAP array (dashed lines) and RECAP (solid lines): (a) uniform multipath $L=4$ (b) SVA model

where $\hat{\rho} = G_{SISO}(\hat{H}_n)\hat{P}_T$ is interference-to-noise ratio. Since $\hat{\rho}$ depends on proximity of the interferer, values of $\hat{\rho}$ between 0 to 20 dB are considered. It is assumed that the interfering node employs a non-RECAP structure and $\hat{S}_{Rx,Tx}$ is computed as

$$\hat{S}_{Rx,Tx} = \sum_{k=1}^{\tilde{k}} \sum_{\ell=1}^{L_k} \left[ E_{mc}^{m}(\hat{\theta}_k^\ell, \hat{\phi}_k^\ell) \right]^T \hat{\alpha}_k^\ell e^{-j\omega \hat{\tau}_k^\ell} \hat{E}_{mc}^{m} (\hat{\theta}_k^\ell, \hat{\phi}_k^\ell).$$  \hspace{1cm} (3.31)

2×2 MIMO System

Figure 3.7(a) plots the capacity of a 2×2 system with $L = 4$ multipath for both non-RECAP and RECAP. The case for $\hat{\rho} = 0$ dB, is similar to no interference. As $\hat{\rho}$ increases, non-RECAP capacity steadily drops towards zero, since for interference with rank $\tilde{N}_F = N_F$, it is not possible for the non-RECAP to null the effect. Although capacity for both the non-RECAP and RECAP is falling with increasing $\hat{\rho}$, closer inspection reveals that the capacity gain of using the RECAP over the non-RECAP actually increases with increasing $\hat{\rho}$. Performance degradation is much smaller for the RECAP since REs can be used to null interference, suggesting the possibility of aggressive spectral reuse.
Figure 3.8: Channel capacity for single user 4×4 MIMO with fixed interference for a simple non-RECAP array (dashed lines) and RECAP (solid lines): (a) uniform multipath with \( L=8 \) (b) SVA model

4×4 MIMO System

The results for varying \( \hat{\rho} \) are shown in Figure 3.8(a) for \( L=8 \). The overall effect is same as that of 2×2 system, but the curves are flatter with respect to the power constraint, indicating that power advantage is less important for more feeds for fixed interference as well. However, improvement relative to the non-RECAP is still very significant, especially for severe interference.

3.4.3 Multi-User MIMO

Building on the idea of employing aggressive spectral reuse, next a true multi-user scenario is considered where users optimize their RECAPs to maximize sum capacity. This is different from the case of fixed interference, since the role of the transmit RECAP becomes more important to reduce interference to the other user. Although for fixed interference, the user does not have control over interference, he also does not care about how much interference he causes. For the multi-user case, interference can be controlled but users also
impact each other. Capacity degradation due to interference depends on proximity, and \( \hat{\rho} \) between 0 and 20 dB is again considered.

Two links are considered, where each receiving user experiences interference from the transmitter of the other link and a joint optimization is done in order to maximize the sum capacity of both links. Individual capacity of each link is calculated using (3.30), except now in (3.31), the Tx RECAP patterns of the other link are employed instead of \( \hat{e}^{mc}(\hat{\theta}_{k\ell}, \hat{\phi}_{k\ell}) \) for a non-RECAP. Figure 3.9(a) shows MIMO channel capacity per user for the 2×2 multi-user system with increasing \( \hat{\rho} \), exhibiting similar RECAP capacity gain as the fixed interference case. The relative gain in moving from Case 1 to Case 2 is higher for multi-user compared the single user case with fixed interference, likely due to the fact that Tx RECAPs can now be controlled to avoid interference.

Figure 3.10(a) shows the results for the 4×4 MIMO system. By increasing \( \hat{\rho} \), the improvement with respect to constraint type becomes even flatter than the 4×4 case for fixed interference. Surprisingly, RECAP capacity per user is now lower than that for fixed interference, indicating that jointly suppressing incoming interference and avoiding outgoing interference becomes more difficult for more active feeds.
3.4.4 SVA Propagation Model

The simple path-based model is convenient, but possibly over-simplistic to represent true propagation scenarios, and hence Saleh Valenzuela Angular (SVA) model [45] is also considered in this analysis. The parameters of the model are assumed to be $T_C = 34$ ns, $T_R = 29$ ns, $1/\Lambda = 17$ ns, $1/\lambda = 5$ ns and $\sigma = 26^\circ$, taken from [45]. The model makes use of a threshold value after which it stops looking for multipath, which is assumed to be -10 dB, generating 50 multipath on average.

Results for SVA channel simulations have been plotted next to the respective plots for the simple path-based model in Figures 3.7 - 3.10. There is not a dramatic impact compared to the simple channel model. For the non-RECAP case, capacity is slightly more degraded in some results with increasing $\hat{\rho}$ due to more paths. For the RECAP case the curve trends are similar, but curves are shifted up slightly in some results showing that RECAP is more advantageous with increased multipath. However, in general changes are only marginal.
3.4.5 Effects of Losses and Bandwidth on Channel Capacity

Bandwidth limitations and RE loss are important considerations in practical RECAP structures, and in this section these two effects are studied. First loss is considered by including a series resistance with each RE ranging from 0-10 Ω. Figure 3.11(a) shows the results corresponding to the 2×2 single user system without any interference. There is no impact of loss for Case 1 since power differences are removed. Moving to Cases 2 and 3, the impact of loss becomes increasingly prominent, resulting from reduced gain of the RECAP, which decreases the channel capacity. More performance loss is observed for the 4×4 MIMO system as shown in Figure 3.11(b).

Another important aspect is finite bandwidth, and in order to study its effect a two sided bandwidth of 20 MHz is assumed at a center frequency of 3 GHz. Capacity is computed as the average capacity at the center frequency and two band edges for a single fixed RECAP structure. Channels are normalized as before, except now the largest (worst case) normalization factor of the three frequencies is used.
Figure 3.12: RECAP capacity for 20 MHz bandwidth and the SVA model for a simple non-RECAP array (dashed lines) and RECAP (solid lines): (a) 2×2 (b) 4×4

Figure 3.12(a) indicates that finite bandwidth results in a small capacity reduction for the 2×2 non-RECAP. Although RECAP performance is minimally impacted in Case 1, for Cases 2 and 3 some reduction is seen, comparable to the difference of average versus instantaneous optimization. Results for the 4×4 system in Figure 3.12(b) are similar with a slightly larger gap between single frequency and finite bandwidth curves.

3.5 MIMO Capacity Analysis Using Measurements

This section extends the work presented earlier in this chapter, by performing actual channel measurements with a prototype RECAP. Since the purpose of measurements was more proof of the concept as compared to a complexity versus performance analysis, so only the receiver (Rx) node is equipped with a 5×5 square parasitic RECAP array confined to an area of 1λ×1λ, where a detailed analysis of the parasitic RECAP is presented in Section 2.1.3. Measurements are performed for both line-of-sight (LOS) and non-LOS scenarios for 2×2 and 4×4 MIMO systems for the case of a finite bandwidth (BW) as well as a single frequency. For real-time optimization, a genetic algorithm is used.
Similar to simulations, the capacity improvement by employing a RECAP is assessed for different power constraints. However, due to hardware limitations it is not possible to apply the max EIRP constraint. Instead, a new case is considered in which non-RECAP capacity is computed for comparison purposes. Based on the analysis presented in Section 3.2 the cases for fixed SNR constraint (Avg Rx SNR) and average transmit power constraint (Fixed $P_T$) are considered in measurements.

3.5.1 Measurement Configuration

This section covers the details regarding relative transmit (Tx) and receive node locations for LOS and non-LOS measurements, experimental setup which was used for channel acquisitions and the RECAP used in this study.

Node Locations

Figure 3.13 shows the basic measurement setup used in this study. It consists of a Tx node which uses a usual (non-RECAP) array as well as interfering antennas. The Rx node has a RECAP with multiple feeds, where the number of feeds depends on whether the $2 \times 2$ or $4 \times 4$ MIMO system is considered. For LOS measurements, both Tx and Rx nodes are placed in a single room separated by 10m as shown in Figure 3.14. Red rectangles mark the location of Tx and Rx nodes while blue circles mark the location of possible interferers. For the non-LOS measurement, the Tx node location stays the same while the Rx node is moved to the hallway (at label Rx2).
Experimental Setup

A MIMO channel sounder similar to the one presented in [46] was used for the measurement campaign, where both Tx and Rx arrays are connected to the MIMO channel sounder. An SPI-based digital-to-analog (D/A) conversion unit was implemented at the receiver to control the bias voltage $V_{\text{bias}}$ on the reconfigurable elements. The measurement setup is depicted with a block diagram in Figure 3.13. The FPGA-based SPI implementation is integrated with the channel sounder, allowing random RECAP states to be streamed in a synchronized fashion to SPI-based D/A converters, providing automatic pairing of the channel snapshots and RECAP states.

Transmit Node

The transmit node consists of an array of 8 monopole antennas with a ground plane below them, which is partitioned in two parts: a usual (non-RECAP) array that represents the transmitter (squares) radiating desired signals, and the remaining 4 elements that represent interfering antennas (filled circles) as shown in Figure 3.15. For analysis of $2 \times 2$ and $4 \times 4$ MIMO systems, blue squares alone or blue and black squares are used for the active transmit elements, respectively. The feeds of the transmit node are located at the corners of an area of $1\lambda \times 1\lambda$.

The signal transmitted by the Tx node consists of eight frequency tones separated by 10 MHz with a center frequency of 2.55 GHz. The total transmit power is 23 dBm. For the analysis of results a signal-to-noise ratio (SNR) of 10 dB is assumed, while the achieved
SNR through practical measurements was approximately 60 dB for LOS channels and 20 dB for non-LOS channels.

3.5.2 Measurement Results

A simple genetic algorithm (GA) is implemented for the optimization of the RECAP and its performance with respect to a random search is presented for MIMO capacity maximization. MIMO capacity results are compared with the case when a usual (non-RECAP) array is present at Rx, verifying the capacity enhancement possible using RECAPs. Figure 3.16 shows the channel measurement setup for the LOS case, marking the relative positions of the transmit and receive node. The measured capacity results for $2 \times 2$ and $4 \times 4$ MIMO systems are depicted in Figure 3.17 and 3.18 respectively. The left plot in each group is for the random search (solid lines) and the right plot is for the GA (dashed lines).

2 × 2 MIMO System

Figure 3.17(a) presents the results for LOS channels corresponding to three normalization cases and varying interference-to-noise ratio ($\hat{\rho}$) per interferer over a bandwidth of 70 MHz. It is observed that although the GA is not fully optimized, it still provides much
better capacity than a random search. Both non-RECAP and RECAP capacity drop with increasing $\hat{\rho}$. However a relative comparison shows that for high interference the performance advantage using RECAP increases (reaching to 200%) for $\hat{\rho}=20$ dB.

Figure 3.17(b) considers the same cases, except that only a single frequency bin is optimized (narrowband system). The increased capacity of the single-frequency optimization is expected, since it is well known that nulling at a single frequency is much simpler than wideband nulling. Overall, fixed transmit power performs better than fixed SNR, indicating that for the single-frequency case, beamforming can provide a significant advantage.

Figure 3.17(c) and (d) show the same configurations as (a) and (b), but now in the non-LOS (hallway) environment. The trends for the 2×2 non-LOS case are similar to the LOS case, except that beamforming advantage for fixed transmit power appears to be higher, even for wide bandwidth.

4 × 4 MIMO System

Figure 3.18(a) and (b) present channel capacity corresponding to a 4 × 4 MIMO system for the LOS environment for wide bandwidth and single frequency. Similar to the
Figure 3.17: Peak measured capacity for a $2 \times 2$ MIMO system. Random search on left and GA on right of each subplot.

$2 \times 2$ system, the GA is able to find much better solutions than the random search, especially for large $\hat{\rho}$. For the results corresponding to the $4 \times 4$ system, it seems that fixed SNR in general performs the same or better than fixed transmit power. This is likely due to the increased difficulty of the optimization problem, since for the same aperture there are more feeds (fewer REs and more paths to enhance), and more interfering antennas need to be nulled out, meaning fewer degrees of freedom are left over for beamforming. Figure 3.18(c) and (d) show similar trends as for the non-LOS environment. The main new observation is
that even the genetic algorithm is unable to provide very large capacity improvement for the wideband non-LOS case.

3.6 Chapter Summary

This work has analyzed MIMO capacity improvements possible with a simple RECAP structure for different scenarios and system power constraints. The results indicate that very large gains relative to fixed antenna MIMO systems are possible, especially for interference-limited and multi-user environments, suggesting that RECAPs may enable ag-
gressive spectral reuse. Consideration of finite bandwidth and losses has indicated that RECAPs can also provide most of this capacity improvement even with these practical impairments. Simulations work was supported with MIMO measurements, highlighting the fact that efficient real-time optimization algorithms are required to provide near-peak capacity with minimum possible optimization time.
Chapter 4

Key Establishment Employing Reconfigurable Antennas

While traditional security measures for wireless communication are implemented at the upper layers of the communication protocol stack, applying appropriate techniques at the physical layer can serve to enhance security. For example, in [35, 36] the idea of exploiting common randomness for secure communications was established, showing that two nodes can achieve perfectly secure communications in an information theoretic sense without the need for a-priori shared information. In [37, 47, 48], the ability to generate secure keys by exploiting this common randomness was analyzed, proving under what conditions perfectly secret keys can be generated by two nodes.

Since electromagnetic propagation and antennas can be theoretically reciprocal, if two radios transmit training data to each other using half-duplex communication and use the received training sequences to estimate the channel transfer function from the transmit to receive antenna terminals, the observed channel estimates will be the same to within estimation errors. Thus, a reciprocal channel can be used as a source of common randomness for key establishment, which was suggested as early as [49]. Later work explores the limits of key establishment using a reciprocal scalar channel [50, 51] and develops practical algorithms based on channel quantization [52–56]. Analysis and measured performance of key establishment for spatially correlated multi-input multiple-output (MIMO) channels was treated in [57–59]. Recently, the impact of channel sparsity in reciprocal channel key generation has been investigated [60].

An important limitation of key establishment using quantization of a shared reciprocal channel occurs when the channel is static or very slowly fading, since the amount of common randomness is limited. In [14] the useful idea of using a reconfigurable antenna for key establishment was presented, where random states of an electronically steerable parasitic
array (ESPAR) are used to create a random reciprocal channel state at the two communicating nodes, even when the underlying propagation channel is static. Since [14] was only a proof-of-concept and did not consider vulnerability with respect to an eavesdropper, this author presented initial simulations and measurements of a scalable reconfigurable antenna in [38] and [39], respectively, suggesting that with sufficient antenna complexity, keys that are secure with respect to a single-antenna eavesdropper can be generated. Note that although this author performed the work presented in [38] and [39], that work is not revisited in this dissertation.

This chapter provides a comprehensive analysis of the security of key establishment methods that employ reconfigurable antennas and channel reciprocity to generate common randomness. This study overcomes limitations of previous work through detailed simulation and direct measurement. First, in contrast to [14], the antenna used in this work has scalable complexity, allowing determination of the full potential of this technology. Second, the case of an eavesdropper equipped with multiple antennas is considered, since only a single-antenna eavesdropper was considered in this author’s previous work. Finally, unlike [39] where due to hardware limitations only two-node measurements were performed, three-node measurements are provided here, providing a more accurate characterization of the secrecy obtained. The analysis reveals not only the conditions under which reconfigurable antennas provide good key generation rates, but also the level of security achieved using the approach in the presence of a close, multi-antenna, passive eavesdropper.

4.1 System Model

Figure 4.1 shows the system model considered in this analysis in which two legitimate nodes designated as Alice and Bob communicate in the presence of an eavesdropper Eve. While Alice possesses a RECAP, Bob is equipped with a single antenna, thus concentrating on the performance improvement obtained with a RECAP without the complexity of coordinating reconfiguration at both radios. Eve possesses an array of $N_E$ elements that is assumed to surround Alice’s RECAP, as this creates a high level of vulnerability. The estimated narrowband scalar (single antenna) channels at Bob and Alice are respectively denoted as $\hat{a}$ and $\hat{a}'$, where the carat (\(^\cdot\)) is used to emphasize that these are estimated quan-
Figure 4.1: Top view of the antenna arrangement in the security analysis, where Bob has a single antenna (black square), Alice has a RECAP with a single feed antenna (black square) and programmable REs placed on a regular grid (empty circles), and Eve has an array of antennas surrounding the RECAP (filled circles).

Because of reciprocity, the differences between these two estimates result only from channel estimation errors, imperfect calibration designed to remove non-reciprocal contributors to the channel (i.e. radio circuitry), channel time variation between estimation of the two channels, or other practical effects. The vectors $\hat{\mathbf{b}}$ and $\hat{\mathbf{c}}$ respectively represent Eve’s estimates of the multi-antenna channels from Alice and Bob. Note that channel variables $a$, $b$, and $c$ indicate ideal channels not corrupted by estimation error.

4.1.1 Parasitic RECAP

Alice’s RECAP consists of a single feed antenna placed at the center of a uniform two-dimensional $5 \times 5$ square grid of area $1\lambda \times 1\lambda$ with an inter-element spacing of $\lambda/4$, as depicted by the square in Figure 4.1. The terminals of this central antenna are connected to the radio transceiver circuitry. Other identical antennas are placed at the other grid positions (open circles in Figure 4.1), with the terminals of each of these parasitic antennas connected to a circuit that can tune the reactance loading the antenna. Each tunable parasitic antenna is therefore termed a reconfigurable element (RE), with $N_{\text{RE}}$ indicating the total number of REs used to construct the RECAP.
Although a very complex RECAP structure is used, the goal of this work is to under-
stand what level and type of reconfigurability is sufficient to capture most of the security
benefit (i.e. the point of diminishing returns). Figure 4.2 shows the four different RECAP
arrangements used in this study, where the filled circles represent placement of the REs on
the grid. It is expected that with more elements, the RECAP will be able to fully exploit the
spatial degrees of freedom within the propagation channel for key establishment, although
REs placed further from the feed element will likely have reduced impact on the achieved
performance. Motivated by this observation, two different arrangements for $N_{RE} = 8$ are
considered to allow exploration of the impact of RE proximity to the feed antenna.

For the simulations presented in this work, the feed antenna and REs use $z$-oriented
half-wave dipole elements that are easily modeled with electromagnetic simulation software.
In contrast, the experiments use $z$-oriented quarter-wave monopole antennas due to their
fabrication simplicity. While using different antennas for the simulations and experiments
may create some differences, having similar (theoretically identical) radiation patterns for
the two elements suggests that the simulations and measurements should result in similar
performance behaviors. The reconfigurable element used in this work is similar to the one
presented in Section 2.1. The number of states ($N_{RS}$) of REs used in study is chosen from
measured results of a varactor-diode based RE, where $N_{RS}$ states are uniformly distributed
over bias voltages ranging from 1 to 5 volts.

4.2 Information Theoretic Analysis

Two information theoretic metrics are used in this work to quantify the impact of RE-
CAP reconfigurability on the key establishment performance. This section briefly discusses
the metrics and their computation using channel observations.

4.2.1 Key Establishment Metrics

Exploiting common randomness for secure communications was first analyzed in an
information theoretic context in [35]. Assuming two legitimate nodes observe random vari-
ables $X$ and $Y$, while an eavesdropper observes $Z$, [35] shows that secrecy capacity is bounded
from above by $\min[I(X;Y|Z), I(X;Y)]$, where $I(\cdot;\cdot)$ is mutual information. Furthermore, it
was shown that this bound can be approached by discussion over a public channel. Later, the same authors analyzed the problem of secure key establishment exploiting common randomness [37, 47, 48], where $I(X;Y|Z)$ is established as a critical security parameter and referred to as the *intrinsic conditional mutual information*. A similar quantity is also used in [60] to measure the theoretical key generation rate.

In the context of the system model in Figure 4.1, $X$ and $Y$ correspond to $\hat{a}$ and $\hat{a}'$, which represent common random information that can be used to establish a common message (or secret key) at the two legitimate nodes. The channels $\hat{b}$ and $\hat{c}$ correspond to $Z$, or the information that Eve can use to guess the secret key. In [57, 58] the possibility of using reciprocal fading MIMO channels as the source of common randomness to generate a shared secret key is considered, where the intrinsic conditional mutual information bound is adopted to define two useful security metrics, as described below.

The first metric is *available key bits*, which refers to the maximum number of independent key bits that can be generated from each observation of the random channel,
\[ I_K = I(\hat{a}; \hat{a}') = \mathbb{E}\left\{ \log_2 \frac{f(\hat{a}, \hat{a}')}{f(\hat{a})f(\hat{a}')} \right\}, \quad (4.1) \]

where \( \mathbb{E}\{\cdot\} \) is expectation, and \( f(\cdot) \) is a probability density function (pdf).

Because Eve’s channel estimates may be correlated with \( \hat{a} \) and \( \hat{a}' \), she may be able to use these estimates to gain information about the established key. In order to account for this a second metric, referred to as secure key bits or \( I_{SK} \), is defined, which is the number of generated key bits per channel observation that can be secure with respect to Eve, given by

\[ I_{SK} = I(\hat{a}; \hat{a}'|\hat{b}, \hat{c}) = \mathbb{E}\left\{ \log_2 \frac{f(\hat{a}, \hat{a}'|\hat{b}, \hat{c})}{f(\hat{a}|\hat{b}, \hat{c})f(\hat{a}'|\hat{b}, \hat{c})} \right\}. \quad (4.2) \]

When Eve’s channels are independent from the Alice-Bob channel, \( I_{SK} = I_K \), indicating all available bits are also secure from the eavesdropper. Note that under static channel conditions and fixed antennas, \( I_K = I_{SK} = 0 \), indicating that no secret key can be generated. However, by using random antenna states, the reciprocal end-to-end channel is randomized, leading to nonzero security metrics.

**Numerical Computation of Key Rate Metrics**

Since it is not known whether the distribution of channels generated with the RECAP will be Gaussian, this work develops a numerical technique that allows \( I_K \) and \( I_{SK} \) to be computed directly from Monte-Carlo simulations. For computation of \( I_K \), the propagation channels \( \hat{a} \) and \( \hat{a}' \) may follow a non-Gaussian distribution, and the pdf \( f(\hat{a}, \hat{a}') \) is not known. However, since the estimation error at Bob and Alice can be considered independent, the conditional pdf \( f(\hat{a}, \hat{a}'|a) \) is just the product of two known noise pdfs for additive Gaussian noise. Using this fact

\[ f(\hat{a}, \hat{a}') = \int f(\hat{a}, \hat{a}'|a)f(a)da = \mathbb{E}_a f(\hat{a}, \hat{a}'|a), \quad (4.3) \]

\[ = \mathbb{E}_a f_n[(\hat{a} - a)/\sigma_a] f_n[(\hat{a}' - a)/\sigma_a'], \quad (4.4) \]
where \( f_n(\cdot) \) is a unit variance complex Gaussian pdf, and \( \sigma^2_a \) and \( \sigma^2_{a'} \) are estimation error variance at Bob and Eve, respectively. Similarly,

\[
f(\hat{a}) = \mathbb{E}_a f(\hat{a}|a) = \mathbb{E}_a f_n[(\hat{a} - a)/\sigma_a],
\]

\[
f(\hat{a}') = \mathbb{E}_a f(\hat{a}'|a) = \mathbb{E}_a f_n[(\hat{a}' - a)/\sigma_{a'}].
\]

Combining (4.4)-(4.6) with (4.1) allows \( I_K \) to be computed with a direct Monte-Carlo procedure without any need to empirically estimate the pdfs of the artificial non-Gaussian channels. First, \( M \) random realizations of \( \hat{a} \) and \( \hat{a}' \) (jointly distributed) denoted \( \hat{a}_m, \hat{a}'_m \) are observed. For each of these realizations, \( N \) random realizations of \( a \) are observed which are independent of \( \hat{a} \) and \( \hat{a}' \), and denoted \( a_{mn} \). The mutual information is estimated using

\[
I_K \approx \frac{1}{M} \sum_m \log_2 \left( \frac{N \sum_n f(\hat{a}_m, \hat{a}'_m|a_{mn})}{\sum_n' f(\hat{a}_m|a_{mn'}) \sum_n'' f(\hat{a}'_m|a_{mn''})} \right).
\]

A similar Monte-Carlo procedure can be employed for computation of \( I_{SK} \) after establishing the following theorem for conditional distributions.

**Theorem 1** \( f(x, y|z) = \int f(x, y|z, \alpha)f(\alpha|z)d\alpha. \)

**Proof:**

\[
\int f(x, y|z, \alpha)f(\alpha|z)d\alpha = \int \frac{f(x, y, z, \alpha)}{f(z)} f(z) \frac{f(z, \alpha)}{f(z)} d\alpha = \frac{1}{f(z)} \int f(x, y, z, \alpha) d\alpha = f(x, y|z).
\]

Theorem 1 can be used to compute the unknown pdf \( f(x, y|z) \) when the conditional distribution \( f(x, y|z, \alpha) \) is known. Note that for simplicity a single antenna is used at Eve in the analysis presented below, however it can be naturally extended to multiple antennas.
The unknown pdfs in (5.27) when Eve has a single antenna can be obtained using Theorem 1 and a Monte-Carlo procedure. Specifically,

\[
f(\hat{a}, \hat{a}'|\hat{b}, \hat{c}) = \int f(\hat{a}, \hat{a}'|\hat{b}, \hat{c}, a, b, c) f(a, b, c|\hat{b}, \hat{c}) da db dc,
\]

\[
= \int \frac{f(\hat{a}, \hat{a}'|\hat{b}, \hat{c}, a, b, c)}{f(\hat{b}, \hat{c})} f(a, b, c|\hat{b}, \hat{c}) da db dc
\]

\[
= \frac{1}{f(\hat{b}, \hat{c})} E_{abc} f(\hat{a}, \hat{a}'|a) f(\hat{b}, \hat{c}|b, c),
\]

where the second equality comes from applying Bayes’ rule to the second term under the integral, and the removal of conditioning variables in the last equality results from conditional independence. Likewise, the pdfs in the denominator of (5.27) are

\[
f(\hat{a}|\hat{b}, \hat{c}) = \frac{1}{f(\hat{b}, \hat{c})} E_{abc} f(\hat{a}|a) f(\hat{b}, \hat{c}|b, c),
\]

\[
f(\hat{b}|\hat{b}, \hat{c}) = E_{b,c} f(\hat{b}, \hat{c}|b, c),
\]

Combining these results, \( I_{SK} \) can be expressed as

\[
I_{SK} = E \log_2 \frac{E_{abc} f(\hat{a}, \hat{a}'|a) f(\hat{b}, \hat{c}|b, c) f(\hat{b}, \hat{c})}{E_{abc} f(\hat{a}|a) f(\hat{b}, \hat{c}|b, c) E_{abc} f(\hat{a}'|a) f(\hat{b}, \hat{c}|b, c)}. \]

Although this looks more complicated than the original expression, note that each of the pdfs involves estimated channels conditioned on the actual channel, and is given directly in terms of the noise pdfs alone. The required pdfs are

\[
f(\hat{a}, \hat{a}'|a) = f_n[(\hat{a} - a)/\sigma_a] f_n[(\hat{a}' - a)/\sigma_{a'}],
\]

\[
f(\hat{b}, \hat{c}|b, c) = f_n[(\hat{b} - b)/\sigma_b] f_n[(\hat{c} - c)/\sigma_c],
\]

\[
f(\hat{b}, \hat{c}) = E_{b,c} f(\hat{b}, \hat{c}|b, c),
\]

(4.5), and (4.6). As before the Monte-Carlo procedure operates by observing \( M \) joint random realizations of the estimated channels (\( \hat{a}_m, \hat{b}_m, \) and \( \hat{c}_m \)) and for each of these generating \( N \) random realizations of the ideal channels (\( a_{mn}, b_{mn}, \) and \( c_{mn} \)) to compute the inner
expectations for each \( m \). Although not shown in this dissertation, this numerical procedure for computing \( I_K \) and \( I_{SK} \) has been validated using correlated Gaussian channels and available closed form expressions [61].

**Gaussian Channel Assumption**

When Eve has more than one antenna, the large number of realizations required for convergence of numerical computation of information theoretic metrics can lead to excessive computation. Although developing closed-form bounds and low-complexity numerical computations for (4.1) and (5.27) is highly desirable, it is beyond the scope of this dissertation. Instead, to reduce the required computation, one can assume that the channels satisfy a Gaussian distribution, allowing closed-form computation of \( I_K \) and \( I_{SK} \). For channel observations that are correlated zero-mean complex Gaussian random variables, \( I_K \) becomes [57]

\[
I_K = \log_2 \frac{\|\hat{R}_{aa}\|\|\hat{R}_{aa'}\|}{\|\hat{R}_{AA'}\|},
\]

where \( \| \cdot \| \) is the matrix determinant and covariances with lowercase subscripts denote

\[
\hat{R}_{x_1x_2} = E\{\hat{h}_{x_1}\hat{h}_{x_2}^\dagger\}\]

(4.19)

with \( \{ \cdot \}^\dagger \) indicating a conjugate transpose. Note that \( \hat{R}_{aa} \) and \( \hat{R}_{aa'} \) are scalar variances when Bob has a single antenna and Alice’s RECAP has a single feed antenna. Covariances with uppercase subscripts represent those of stacked channel vectors, or

\[
\hat{R}_{X_1X_2...X_N} = E\{[\hat{h}_{x_1}^\dagger \hat{h}_{x_2}^\dagger ... \hat{h}_{x_N}^\dagger] [\hat{h}_{x_1}^\dagger \hat{h}_{x_2}^\dagger ... \hat{h}_{x_N}^\dagger]\},
\]

(4.20)

Using this notation, \( I_{SK} \) becomes

\[
I_{SK} = \log_2 \frac{\|\hat{R}_{ABC}\|\|\hat{R}_{A'BC}\|}{\|\hat{R}_{BC}\|\|\hat{R}_{A'BC}\|}.
\]

(4.21)
4.2.2 Brute-Force Attack for Low RECAP Complexity

A potential concern for RECAP-induced channel fluctuations is that if total number of states for RECAPs at Alice is too limited, a reduced complexity brute-force attack may be possible. Consider the case when Eve has a single antenna but very high signal-to-noise ratio (SNR), so that the channels \( b \) and \( c \) are almost exactly observed. For a static propagation channel, Eve observes a 4-dimensional constellation of points (from 2 complex channels) as Alice picks random RECAP states. Although Eve does not know the mapping of key bits to the observed constellation points, she can record the sequence of constellation points. If the combined RECAP complexity is too low, Eve can learn the key by simply trying all possible mappings, which may be less complex than trying all possible key sequences.

One way to avoid this possibility is to consider how many total secure key bits (\( N_{\text{bits}} \)) are required to be generated by a system during static channel conditions. By making the combined RECAP complexity large enough, such that the number of possible mappings to search is larger than \( 2^{N_{\text{bits}}} \), a reduced-complexity brute-force attack is avoided. Given a single RECAP at Alice with \( N_{\text{RE}} \) reconfigurable elements and \( N_{\text{RS}} \) states, the total number of RECAP states is \( N_{\text{RE}}^{N_{\text{RS}}} \). For a quantization order of \( M \) symbols per channel observation, each constellation point has \( M \) possible mappings. Thus, the total combination of mappings to check for all constellation points is \( M^{(N_{\text{RS}}^{N_{\text{RE}}})} \) and the condition

\[
N_{\text{RS}}^{N_{\text{RE}}} \log_2 M \geq N_{\text{bits}}
\]  

(4.22)

is required to avoid a reduced-complexity brute-force attack. Figure 4.3 plots the left-hand-side of (4.22) for \( M = 4 \) and various values of \( N_{\text{RE}} \) and \( N_{\text{RS}} \), indicating that for RECAPs with modest complexity, a very large number of key bits can be generated securely under static conditions. This also suggests the interesting possibility of using analog noise-like sources to bias the reconfigurable elements, creating a virtually infinite number of reconfigurable states, which appears to completely remove the possibility of the reduced-complexity attack.
Figure 4.3: Maximum key bits that can be securely generated with a RECAP with limited complexity under static conditions

4.3 Modeled Key Establishment Performance

This section covers the security versus complexity analysis of a parasitic RECAP using full-wave simulations and network analysis. The electromagnetic propagation channel is assumed to be static, and any change in the channel can only be caused by the RECAP. Since additional time variation in the propagation would likely increase security, the static channel represents a worst-case scenario.

4.3.1 RECAP Simulation

In this scenario, Eve’s antennas are near the RECAP, and because mutual coupling between the RECAP and Eve’s antennas may reveal information that can help Eve more easily determine the key, this coupling cannot be ignored. Therefore, the Numerical Electromagnetic Code (NEC) is used to model Eve’s and Alice’s arrays together. Since Bob is far from Alice and Eve, his antenna is modeled separately and is assumed to lie in the far-field of the other arrays. An analysis similar to the one presented in Section 2.1 is performed to com-
pute the radiation patterns of Alice’s feed antennas \( (e_A^{\text{mc}}(\theta, \phi)) \) and Eve’s array \( (e_E^{\text{mc}}(\theta, \phi)) \) for a specific RE termination.

### 4.3.2 Communication Channels

This study assumes that propagation is confined to the horizontal \((xy)\) plane, and therefore only the azimuthal radiation pattern \((\theta = \pi/2)\) is considered in this analysis. The multipath model consists of \( L \) paths, where the \( \ell \)th path has angle of departure \((\pi/2, \phi_\ell)\), angle of arrival \((\pi/2, \phi'_\ell)\), and complex amplitude \( \alpha_\ell \). The channels become

\[
a' = \sum_{\ell=1}^{L} e_A^{\text{mc}}(\pi/2, \phi'_\ell) \alpha_\ell e_B^{\text{mc}}(\pi/2, \phi_\ell),
\]

\[
c_i = \sum_{\ell=1}^{L} e_{E,i}^{\text{mc}}(\pi/2, \phi'_\ell) \alpha_\ell e_B^{\text{mc}}(\pi/2, \phi_\ell),
\]

where \( a = a' \) is the error-free reciprocal channel between Bob and Alice, \( c_i \) is the channel between Bob and Eve’s \( i \)th antenna, and \( e_B^{\text{mc}} \) is the azimuthally omnidirectional pattern of Bob’s antenna. Because Eve’s antennas lie close to the RECAP, the computed coupling between Alice’s feed antenna and Eve’s array elements gives the channel \( b \) with \( i \)th element

\[
b_i = \Gamma_F, (1, i+1),
\]

where \( \Gamma_F \) has been ordered such that \( \Gamma_F, (1,1) \) is the input reflection coefficient of the RECAP feed port.

A difficulty in defining the security of the proposed scenario is that Eve may have a much more sensitive receiver than Alice or Bob. Assuming the worst case of zero noise at Eve (or infinite SNR) leads to an information theoretic security of zero, since there will be a one-to-one mapping between the discrete RECAP-induced channel states of the ideal Alice-Bob channel and Eve’s channel. In order to not place any assumptions on the sensitivity of Eve’s receiver, yet limit Eve’s effective SNR, the SNR of the pilot signal used for channel estimation is limited by having Alice and Bob add artificial noise to the pilots they transmit. This synthetic noise is only known by the nodes who transmit it, and therefore it cannot
be subtracted by any other receiving node. Assuming that Alice and Bob have an intrinsic SNR of 13 dB (due to receiver noise, non-reciprocity, etc.) and that Alice and Bob add synthetic noise that is also 13 dB below the pilot signal level, this 3 dB degradation leads to a composite SNR of 10 dB at Alice and Bob. On the other hand, it is assumed that Eve’s receiver is noiseless, and since she only experiences artificial noise, her SNR is 13 dB.

With these SNR values established, the channel estimates at Alice, Bob, and Eve are computed by corrupting the channels in (4.23)-(4.25) with additive estimation errors modeled as zero-mean complex Gaussian random processes whose variances are chosen to achieve the specified SNR values. Finally, $I_K$ and $I_{SK}$ can be computed.

### 4.3.3 Simulation Study

The simulations presented here consider two different channel scenarios: (a) Non-line-of-sight (NLOS) using $L = 10$ paths and (b) line-of-sight (LOS) using $L = 1$. In both scenarios, propagation path characteristics remain fixed and channel estimates are computed for $10^6$ different RECAP states. This allows construction of the relevant covariances required for computing $I_K$ and $I_{SK}$ using the Gaussian assumption and, for some scenarios, allows computation of the metric using the accurate numerical technique. When the channel type is not specified, the NLOS channel is used. For all simulations, the results are averaged over 300 different channel realizations and 8 equally-spaced frequencies from 2.515 to 2.575 GHz. When computing $I_{SK}$ for $N_E < 8$, it is assumed that Eve’s antennas represent a subset of the array of $N_E = 8$ elements shown in Figure 4.1, and the results are averaged over all possible sub-array configurations.

#### Security vs. Antenna Complexity

Figure 4.4 plots $I_K$ as a function of the number of states $N_{RS}$ for different values of the number of reconfigurable elements $N_{RE}$ using the numerical method to compute (4.1) and Gaussian assumption to compute (4.18). The error in the Gaussian assumption (difference between the two curves) decreases as both $N_{RS}$ and $N_{RE}$ increase, demonstrating that the distribution of the channel realizations with more REs and more reconfigurable states becomes increasingly Gaussian. As expected, the Gaussian assumption upper bounds the numerical
computations of $I_K$. Figure 4.4 further shows that under both LOS and NLOS propagation, the value of $I_K$ decreases with increasing $N_{RS}$. With more reconfigurable states, the variance of the channels obtained for different states decreases, reducing the number of available key bits per channel observation. Although these results show that using $N_{RS} = 2$ is beneficial for high $I_K$, care must be taken to ensure that the total complexity of the reconfigurable antenna is not too small, as discussed in Section 4.2.2.

Finally, Figure 4.4 shows that for the same number of RE states, increasing the number of REs improves $I_K$. This occurs because increasing $N_{RE}$ physically adds complexity to the coupling between the parasitic array and the feed element in the RECAP, thereby increasing the range of possible RECAP radiation characteristics. However, the relative benefit of additional REs diminishes as $N_{RE}$ increases, a result that is consistent with previous results on RECAP beamforming [10] demonstrating that 8 parasitic elements per wavelength are sufficient to exploit the degrees of freedom in the propagation channel. Note that although $N_{RE} = 8_2$ gives higher $I_K$ performance than $N_{RE} = 8$, the more critical $I_{SK}$ metric is usually lower, indicating that a larger array with higher spatial selectivity is more beneficial than high coupling between the feed and parasitic elements.

Figure 4.4: Simulated $I_K$ as a function of $N_{RS}$ for different values of $N_{RE}$, where curves marked with * and • are respectively obtained using the Gaussian assumption and numerical computation: (a) NLOS channel ($L = 10$), (b) LOS channel ($L = 1$).
Relative Importance of Eve’s Channels

The results for $I_K$ do not consider the information ($\hat{b}$ and $\hat{c}$) possessed by Eve that can allow her to more easily determine the established key, and therefore $I_{SK}$ is analyzed. When evaluating this metric, it is instructive to determine the relative importance of these two channels in providing information to Eve. Therefore, three different cases for computing $I_{SK}$ are considered:

**Case 1:** Eve knows both $\hat{b}$ and $\hat{c}$,

**Case 2:** Eve knows only $\hat{b}$, and

**Case 3:** Eve knows only $\hat{c}$.

Figure 4.5 plots the corresponding results for $N_{RE} = 24$ computed using the Gaussian assumption, with the results showing that $\hat{b}$ is the main source of information for Eve for both NLOS and LOS scenarios (lower $I_{SK}$ indicates more information leaked to Eve). This result is logical, since fluctuations in $\hat{c}$ arise only from a change in the patterns of Eve’s antennas due to weak near-field coupling with Alice’s RECAP, whereas $\hat{b}$ provides direct
information about RECAP changes. Given this observation, only \( \hat{b} \) is considered when computing \( I_{SK} \) in the subsequent analysis. Interestingly, this observation is in contrast to the case where a random propagation channel (not a random antenna) is used to generate the key, where \( \hat{c} \) gives information to Eve and \( \hat{b} \) is a static channel with no information [58].

Because numerical evaluation of \( I_{SK} \) is computationally demanding for \( N_E > 1 \), \( I_{SK} \) and \( I_{SK,G} \) are constructed using (4.14) and (4.21), respectively, for \( N_E = 1 \) and then their ratio is computed as \( \gamma = I_{SK}/I_{SK,G} \). Then, for \( N_E > 1 \), \( I_{SK} \) is computed using the Gaussian assumption in (4.21) and the results are then scaled by \( \gamma \) to obtain a corrected value of \( I_{SK} \). Comparison of this corrected Gaussian result with values obtained using numerical simulations for \( N_E = 2 \) with \( N_{RE} = 8 \) and \( N_{RS} = 2 \) in an NLOS channel shows that the error in the corrected Gaussian result is less than 4%.

Dependence on Eve’s Array Size

Figures 4.6(b)-(e) plot \( I_{SK} \) as a function of \( N_E \) for different values of \( N_{RE} \) and \( N_{RS} \) using corrected Gaussian assumption. It is interesting to observe that for this worst-case scenario in which Eve can estimate the RECAP pattern that creates the random channel fluctuations, \( I_{SK} \) decreases rapidly as \( N_E \) increases. These results further confirm that the
number of key bits per channel observation is maximized for $N_{RS} = 2$ and for large values of $N_{RE}$. However, it is important to note that the channel statistics for small $N_{RS}$ become less Gaussian, as evidenced by the increased difference between the results from the uncorrected and corrected Gaussian assumption for $I_K$.

Note that for the case with $N_{RS} = 2$ and $N_{RE} = 24$, comparison with Figure 4.6(a) shows that approximately 35% of the available key bits remain secure in the presence of Eve surrounding the RECAP with 8 antennas. This suggests that with proper selection of the antenna topology, key generation using reconfigurable antennas can be made robust to even well-equipped eavesdroppers. On the other hand, having too little or the improper type of reconfigurability may lead to a system that is easily compromised.

4.4 Measured Key Establishment Performance

While the simulations have provided valuable insights into the potential of using sophisticated reconfigurable antennas for key establishment, the results depend on assumptions that may not always be satisfied. Therefore, experimental measurements are conducted to validate the observations drawn from the simulations. The communication scenario used is similar to that used for the simulations, with the exception that $\lambda/4$ monopole antennas mounted on a ground plane are used instead of $\lambda/2$ dipoles. Because of the inferior performance of the $N_{RE} = 8$ RECAP configuration in terms of $I_{SK}$ predicted by the simulations, this topology is excluded in the measurements.

4.4.1 Node Locations

Figure 4.7 identifies the relative positions of Bob, Eve and Alice for four different measurement locations within the Research I building on the Jacobs University Bremen campus. Location 2 is within a hallway while the other locations are in different university laboratories. Outdoor measurements were taken on an open lawn as shown in Figure 4.8, where the distance between Bob and Alice was approximately 40 m. To minimize temporal variations in the channel, all measurements were collected over weekends or at night.
Figure 4.7: Relative positions of Bob (B), Alice (A) and Eve (C) at four different locations within an indoor environment. Arrows connect the different node locations for a given location number.

Figure 4.8: Photograph of the outdoor measurement environment and the relative positions of Alice, Bob and Eve for $N_{RE} = 8$. The red ‘×’ indicates the antenna in Eve’s array that is not used in measurements.

4.4.2 Experimental Setup

The experiments accommodate 2-node measurements ($\hat{\mathbf{a}}$ and $\hat{\mathbf{b}}$) or 3-node measurements ($\hat{\mathbf{a}}$, $\hat{\mathbf{b}}$ and $\hat{\mathbf{c}}$), obtained using the configurations shown in Figures 4.9(a) and (b) respectively. In both cases, an $8 \times 8$ multiple-input multiple-output (MIMO) channel sounder similar to that presented in [46] is used. The transmit signal consists of eight frequency tones.
Figure 4.9: 2-node and 3-node configurations used to measure channel responses for the legitimate nodes (Alice and Bob) and eavesdropper (Eve).

spaced at 10 MHz intervals from 2.515 to 2.575 GHz. The channel for each transmit-receive antenna pair is measured sequentially, with synchronization accomplished using Rubidium references and synchronization (SYNC) units at the different nodes. Because the sounder only has 8 transmit ports one of which is needed for connection to Bob’s antenna, only \(N_E = 7\) antennas are used in Eve’s array.

The RECAP is connected to the MIMO channel sounder receiver, with RE biases controlled using an SPI-based digital-to-analog (D/A) converter. The FPGA-based SPI implementation is integrated with the channel sounder to allow synchronization between the antenna switch states in the MIMO measurement system and the RECAP states. For the 2-node configuration, Bob’s antenna is connected to a single output of the sounder transmitter via a 20 m cable and Eve’s antennas are connected to the remaining 7 transmit ports. The feed antenna on Alice’s RECAP is connected to a single receive port. To avoid receiver saturation, 40 dB attenuators are placed between the transmitter outputs and Eve’s antennas.

In the 3-node configuration, an additional high isolation (>80 dB) switch is used to connect Eve’s antennas to the transmit ports (allowing measurement of \(\hat{b}\)) or to the receive ports (allowing measurement of \(\hat{c}\)). Eve’s low transmission power of \(-20\) dBm again avoids receiver saturation. Bob is implemented using a third radio node with a switch selectively connecting a 23 dBm transmit signal or a terminator to the power amplifier driving Bob’s antenna.
4.4.3 Results

All measured results use $10^6$ channel snapshots to compute covariance matrices using the Gaussian assumption or expectations using the numerical method. All of the results are averaged over the 8 frequency tones in the transmit signal. For $N_E < 7$, the results are averaged over all possible $N_E$-element sub-arrays.

Relative Importance of Eve’s Channels

Once again the relative importance of $\hat{b}$ and $\hat{c}$ is explored in terms of revealing information to Eve. As explained in Section 4.3.3, cases where Eve knows $\hat{b}$, $\hat{c}$ or both are considered in this analysis. Figure 4.10 plots $I_K$ and $I_{SK}$ for a 3-node measurement conducted at indoor Location 1 when $N_{RE} = 24$. These results confirm that $\hat{c}$ provides little information to Eve. As a result of this observation, it is assumed that Eve only knows $\hat{b}$ in the remainder of this analysis, allowing use of the data from the simpler 2-node measurements. Interestingly, the security metrics appear to be higher for Location 1 as compared to other locations.
locations. Since the SNR is fixed in the analysis, the higher metrics are likely due to more favorable multipath.

**Security vs. Antenna Complexity**

Figure 4.11(a) plots $I_K$ as a function of $N_{RS}$ for several values of $N_{RE}$, with the results averaged over the four indoor measurement locations. The difference between the results of the uncorrected and corrected Gaussian assumption observed in the measurements, which for certain circumstances reaches 5%, is larger than that observed in the simulations. As expected, $I_K$ decreases with increasing $N_{RS}$, emphasizing that $N_{RS} = 2$ again leads to the highest number of key bits per channel observation.

Figures 4.11(b)-(e) plot $I_{SK}$ as a function of $N_E$ for different values of $N_{RE}$ and $N_{RS}$, where again the results represent averages over four indoor measurement locations. $I_{SK}$ decreases as $N_E$ increases, confirming the trend observed in the simulations. For this NLOS scenario, provided that Alice has a RECAP with high reconfigurability (large $N_{RE}$), the reduction in $I_{SK}$ created by having a large number of antennas at the eavesdropper relative to an eavesdropper with a single antenna is limited to approximately 50%.
Figure 4.12: Measured values of $I_{SK}$ as a function of $N_E$ for different values of $N_{RE}$ and $N_{RS}$, where the curves for indoor and outdoor measurements represent averages over all experimental results.

**Dependence on Eve’s Array Size**

Figure 4.12 compares selected results for $I_{SK}$ from Figure 4.11 obtained in the indoor environment to comparable results obtained in the outdoor environment. These curves show that the decrease in $I_{SK}$ with increasing $N_E$ is more dramatic for outdoor channels than for the indoor channels, likely due to the fact that the outdoor scenario is characterized by a dominant LOS path while the indoor scenario has stronger multipath components. Even when $N_{RE}$ is large, the value of $I_{SK}$ for $N_E = 7$ is approximately 20% of the value obtained for $N_E = 1$, showing the vulnerability created by the LOS channel that allows Eve to better predict the channels observed at the legitimate nodes.

**Dependence on Eve’s Array Configuration**

The analysis presented above has assumed that Eve’s array surrounds the RECAP, since it is expected that this configuration would allow Eve to best sample the random radiation states of the antenna and track the key generation process. Arguably, this situation would not be feasible in practice, and one may ask if a more natural array configuration for
the eavesdropper would exhibit the same behavior. To explore this idea, each measured data set is processed to determine which subset of Eve’s antennas gives the lowest $I_{SK}$ for a given $N_E$, thus indicating the best that Eve can do with a smaller, more practical array.

Figure 4.13 depicts two sets of curves. In the first case, $I_{SK}$ is averaged over all possible Eve configurations for a given $N_E$, shown by solid lines. In the second case, Eve’s array configuration is identified for each data set that produces the worst-case $I_{SK}$ for a given $N_E$, shown by dashed lines. The results show that for a target $I_{SK}$ level, Eve can typically get by with 1-3 fewer antennas if she can pick her best configuration.

Figure 4.14 shows the worst-case configurations of Eve’s array for Location 2 for different array sizes at Eve. The results for this and other locations (not plotted) typically show that the worst-case configuration is for Eve to place her antennas on one side of Alice’s RECAP. This probably occurs due to a dominant LOS or quasi-LOS component that is present. Therefore, it appears that a more natural and compact array could be judiciously placed by an eavesdropper to obtain nearly the same security reduction as is seen with a full array that surrounds the RECAP.
4.5 Key Establishment in Simulated LOS Channels

The work presented earlier in this chapter demonstrates that RECAPs can effectively enhance security in static multi-path and LOS channels. However, a potential weakness of RECAP-based physical security is an eavesdropper that is present precisely on the LOS path between the communicating nodes, allowing the eavesdropper to sample the same random channel used to generate the key. In this section, the scenario of an eavesdropper on the LOS path is characterized through simulations.

Figure 4.15(a) shows the communications scenario considered. Bob and Eve are equipped with a single half-wave ($\lambda/2$) dipole antenna, while Alice has a $5 \times 5$ square parasitic RECAP confined to an area of $1\lambda \times 1\lambda$. Quantities $\hat{a}$ and $\hat{a}'$ are estimates of the reciprocal channel at Bob and Alice, respectively, while Eve receives the estimated channels $\hat{b}$ and $\hat{c}$. Angular separation between $\hat{a}$ and $\hat{a}'$ is represented by $\theta$, where $\theta = 0^\circ$ corresponds to the case when Eve is exactly on the LOS path between Bob and Alice. An SNR of 10 dB is assumed in the analysis presented below.

Since it is unknown to what extent the RECAP configuration affects security for this scenario, a circular RECAP is also considered as shown in Figure 4.15(b). Elements placed in
Figure 4.15: Top view of nodes in the security simulations, where Bob and Eve have a single antenna and Alice has a RECAP with many programmable REs (hollow circles). Black squares show the location of Bob’s antenna and Alice’s feed, while the blue circle shows a possible position of Eve’s antenna depending on $\theta$.

the inner and outer circle have a radius of $0.25\lambda$ and $0.5\lambda$ respectively. For both square and circular RECAPs, the feed is placed at the center, while all other elements (hollow circles) act as REs.

4.6 Analysis and Initial Results

The goal of this study is to analyze the security of the LOS communications scenario, depending on the angular separation ($\theta$) between $\hat{a}$ and $\hat{b}$. Hence, the states of REs are changed randomly to generate $10^6$ communications channels, and later corresponding secure bits are computed with respect to a certain $\theta$. Note that Eve is in the far-field of Alice, so the impact of $\hat{c}$ on $I_{SK}$ is negligible. The dominant effect will be from $\hat{b}$, and it is expected that the worst-case occurs when $\theta = 0^\circ$. Note that in Figure 4.15, the reference angle $\theta_o$ is the direction of channel $\hat{a}$. For a square RECAP $I_K$ can vary significantly with respect to $\theta_o$. For this reason the results are averaged over the reference angles $\theta_o = [0^\circ, 5^\circ, ..., 45^\circ]$.

Figure 4.16(a) plots $I_K$ for varying $N_{RS}$ when Alice has a square RECAP. The curves corresponding to the numerical computation and the Gaussian approach are close to each
Figure 4.16: $I_K$ for varying $N_{RS}$ using the numerical expectation method and the Gaussian approximation: (a) Alice having a square RECAP (b) Alice having a circular RECAP.

other, indicating that RECAPs can generate close to Gaussian random channels. As demonstrated earlier, the Gaussian approximation upper bounds the numerical computation and $I_K$ is maximized for $N_{RS} = 2$, since extreme RE states appear to maximize the channel variance. Figure 4.16(b) plots $I_K$ when Alice has a circular RECAP. Although the exact values of $I_K$ are slightly different for the two configurations of the RECAP, the general trends are the same.

Figure 4.17 plots $I_{SK}$ with respect to $\theta$ for a square RECAP, and as expected, $N_{RS} = 2$ maximizes $I_{SK}$. Even for $\theta = \theta_0 = 0^\circ$ it is observed that a small number of bits are secure, which is due to Eve’s finite SNR. For $\theta \geq 0^\circ$, $I_{SK}$ increases almost linearly and later converges towards the corresponding $I_K$ value. It is interesting to note that for an angular separation of $30^\circ$ approximately 90% of the bits are secure, while at $\theta = 10^\circ$ approximately 40% of key bits are secure. Also, it is observed that the gap between the numerical approach and the Gaussian approximation increases with $\theta$ for $N_{RS} = 2$, which likely occurs from the lower $N_{RS}$ value producing less Gaussian statistics, where this effect would be more prominent for high values of $I_{SK}$. Figure 4.18 plots the corresponding results for a circular array. The
Figure 4.17: $I_{SK}$ for varying $\theta$ and $N_{RS}$ using the numerical expectation method and the Gaussian approximation when Alice has a square RECAP.

Figure 4.18: $I_{SK}$ for varying $\theta$ and $N_{RS}$ using the numerical expectation method and the Gaussian approximation when Alice has a circular RECAP.
general trends of curves are similar to the square array, emphasizing that exact configuration of parasitic RECAP does not appear to have a significant impact on security.

4.7 Chapter Summary

This chapter has explored the effectiveness of using a highly reconfigurable antenna to generate varying channel estimates that are in turn used to establish secret encryption keys in a time-division duplex communication system. The results demonstrate that an increase in the number of reconfigurable elements plays a vital role in increasing the number of key bits that can be securely generated, where diminishing returns are seen near $N_{RE} = 16$ elements for the $1\lambda \times 1\lambda$ array size. The results also show that using only two impedance states per RE maximizes the number of bits available per RECAP state, meaning that simple switches may represent a practical RE termination.

Simulations and measurements demonstrate that a compact $5 \times 5$ parasitic reconfigurable antenna can secure up to 50% of the available key bits in a NLOS scenario, even when an eavesdropper has an array surrounding the RECAP and a 3-dB SNR advantage. For a LOS scenario with an eavesdropper on or near the LOS path, simulations reveal that approximately 90% of key bits are secure, if there is an angular separation of at least $30^\circ$ between the eavesdropper and the LOS path. The findings show that RECAPs represent a promising candidate for key establishment based on reciprocal channel estimation for static or slow-fading channels.
Chapter 5

Secure Pattern Synthesis for Physical Layer Security

Security is an important concern for today’s wireless communications systems, where the public nature of the transmission enables potential interception of sensitive information by unauthorized parties. Typically, wireless security is accomplished by encrypting binary information before modulation and transmission over the channel. However, recent work has focused on developing techniques that exploit the physical layer, including the antennas and propagation channel, to provide increased security in wireless transmissions. Examples of such techniques may be found in [14, 15, 49, 56, 58, 62–64]. A detailed analysis of physical layer security using reconfigurable antennas is presented in Chapter 4. However, the optimal control of a reconfigurable or adaptive array for peak security is still an open question, and this topic is addressed in this chapter.

One method for using the physical layer to achieve increased secrecy is to use conventional antenna array synthesis to design a transmit radiation pattern that provides high gain to a desired receiver and low gain in directions of potential eavesdroppers [65]. Such an approach reduces the likelihood that an attacker can decode the information-bearing signal, particularly if the channel coding is carefully matched to the realized channel gain. The information-carrying transmit radiation pattern designed in this way is referred to herein as the *signal pattern*. To further enhance security, artificial noise can be transmitted on *noise patterns* that are ideally designed to be orthogonal to the signal pattern, thereby realizing low artificial noise levels to the desired receiver and higher noise in the direction of eavesdroppers [66–69]. This enables enhanced control over the signal-to-noise ratio (SNR) (and therefore decoding probability) observed at unauthorized nodes.

Although array synthesis is a mature topic, and there are many powerful techniques available for synthesizing an individual pattern with desired properties, existing techniques
do not provide a method to jointly synthesize signal and noise patterns to obtain optimal secrecy. This chapter provides a solution for this outstanding problem of secure array synthesis for both LOS and multipath propagation environments. Sections 5.1-5.4 present the analysis and results for the LOS case, while Section 5.5 extends the analysis to a multipath propagation environment.

5.1 Key Establishment in LOS Channels

Figure 5.1 shows a free-space communications scenario involving three nodes. Although a two-dimensional (azimuth-only), single-carrier scenario is treated in this work, the method is general and can be extended to three dimensions and wideband operation. Alice and Bob are legitimate nodes who wish to communicate securely, while Eve is a passive eavesdropper who attempts to receive and decode Alice’s and Bob’s transmissions. It is assumed that all nodes know the relative Alice-Bob angle ($\phi_B$), whereas the relative Alice-Eve ($\phi_E$) is unknown to Alice and Bob.

Consistent with traditional antenna array synthesis, a free-space or line-of-sight (LOS) channel is assumed with Bob and Eve in the far-field of Alice’s array of $N_T$ elements. It is sufficient to consider a single antenna at Bob and Eve, as arrays only change the SNR.
observed at these nodes and this SNR is already controlled by model parameters. The channels denoted $h_{AB}$, $h_{BA}$, and $h_{AE}$ are vectors that represent the complex baseband gains from Alice’s array to Bob’s antenna, from Bob’s antenna to Alice’s array, and from Alice’s array to Eve’s antenna, respectively. These channel vectors are scaled versions of the electromagnetic steering vectors, or

\begin{align}
    h_{AB,i} &= h_{BA,i} \\
    &= g_i(\phi_B) \exp[jk_0(a_{x,i} \cos \phi_B + a_{y,i} \sin \phi_B)], \quad (5.1) \\
    h_{AE,i} &= g_i(\phi_E) \exp[jk_0(a_{x,i} \cos \phi_E + a_{y,i} \sin \phi_E)], \quad (5.2)
\end{align}

where $k_0$ is the free-space wavenumber and $g_i(\phi)$ and $(a_{x,i}, a_{y,i})$ are respectively the field radiation pattern and two-dimensional coordinate of the $i$th antenna in Alice’s array. It is assumed that Eve knows all of the channel gains whereas Alice and Bob only know $h_{AB}$ and $h_{BA}$.

In this LOS environment, if Bob and Eve are close in angle, it will be difficult for Alice to send different signals to the two based only on beamforming. Therefore, an exclusion sector is defined, which is an angular extent $\phi_X$ ranging from $\phi_1$ to $\phi_2$ that is assumed to be free of eavesdroppers. In some cases it may be possible to ensure that this sector is eavesdropper-free by using visual information or restricting physical access. When this is not possible, having an eavesdropper in the exclusion sector will compromise physical layer security, meaning secrecy must rely on upper-layer protocols alone.

An informal problem statement for secure array synthesis is as follows: Find Alice’s array signaling strategy to maximize the information exchanged between Alice and Bob while minimizing the information given to an eavesdropper outside of the exclusion sector. This is very similar to standard array synthesis where a typical objective is to maximize the gain in the direction of the intended receiver (the main beam direction) while minimizing sidelobe transmission outside of the main beam. While this informal problem statement is helpful, the problem statement is more precisely formulated by considering two specific security metrics mentioned below.
5.1.1 Secrecy Capacity

Secrecy capacity is defined as the maximum amount of information that can be transmitted between legitimate nodes without providing useful information to an eavesdropper. Figure 5.2 depicts a detailed signal model that allows secrecy capacity to be defined for the LOS scenario in Figure 5.1. In this model, for a single use of the channel Alice transmits the complex baseband vector \( w \) that produces the signals \( \hat{y}_B \) and \( \hat{y}_E \) at Bob and Eve, respectively. Mathematically, the received signals can be expressed as

\[
\hat{y}_B = h_{AB}^T w + \epsilon_B, \quad (5.4)
\]

\[
\hat{y}_E = h_{AE}^T w + \epsilon_E, \quad (5.5)
\]

where \( \{\cdot\}^T \) is a transpose and \( \epsilon_B \) and \( \epsilon_E \) represent noise modeled as zero-mean complex Gaussian random variables with \( \text{E} \{ |\epsilon_B|^2 \} = \sigma_0^2 \). Since an eavesdropper’s receiver sensitivity is generally unknown, this analysis uses the worst-case assumption that Eve’s receiver is noiseless (\( \epsilon_E = 0 \)).

Secrecy capacity \( C_S \) for this model is the maximum mutual information that Alice and Bob can attain, conditioned on Eve’s signal when Eve is at the worst-case position for
security. This can be interpreted as the maximum secret information that Alice can transmit to Bob over all possible angles for Eve outside of the exclusion sector, or

$$C_S = \max_{p(w)} \min_{\phi_E} I(w; \hat{y}_B | \hat{y}_E),$$  \hspace{1cm} (5.6)$$

where

$$I(w; \hat{y}_B | \hat{y}_E) = H(\hat{y}_B | \hat{y}_E) - H(\hat{y}_B | w, \hat{y}_E)$$ \hspace{1cm} (5.7)$$

$$= H(\hat{y}_B, \hat{y}_E) - H(\hat{y}_E) - H(\hat{y}_B | w)$$ \hspace{1cm} (5.8)$$

$$= H(\hat{y}_B, \hat{y}_E) - H(\hat{y}_E) - H(\epsilon_B),$$ \hspace{1cm} (5.9)$$

$I(\cdot; \cdot)$ is mutual information, $p(w)$ is the probability density function (pdf) of the vector $w$, and $H(\cdot)$ is differential entropy. Note that in the minimization in (5.6), the minimizing $\phi_E$ can be a function of $p(w)$, which means that all possible Eve angles must be considered simultaneously in the minimization.

Assuming zero-mean complex Gaussian signaling, the pdf $p(w)$ is completely determined by its covariance matrix $R = E\{ww^H\}$, where $\{\cdot\}^H$ is a conjugate transpose. $R$ is constrained to satisfy $\text{Tr}(AR) \leq P_T$, where $\text{Tr}(\cdot)$ is trace, $A$ is a coupling matrix [70], and $P_T$ is the available transmit power. For uncoupled transmit antennas, the coupling matrix gets simplified to $A = I$, where $I$ is the identity matrix. The optimization problem in (5.6) becomes

$$C_S = \max_{R: \text{Tr}(AR) \leq P_T} \min_{\phi_E} I(w; \hat{y}_B | \hat{y}_E),$$ \hspace{1cm} (5.10)$$

$$I(w; \hat{y}_B | \hat{y}_E) = \log_2 \frac{|R_{BE}|}{\sigma_B^2 \sigma_0^2},$$ \hspace{1cm} (5.11)$$
where

\[
R_{BE} = E \{ [\hat{y}_B, \hat{y}_E]^T [\hat{y}_B, \hat{y}_E]^* \} = \\
\begin{bmatrix}
\sigma_0^2 + \sigma_B^2 & \sigma_{BE} \\
\sigma_{BE}^* & \sigma_E^2
\end{bmatrix}, \quad (5.12)
\]

\[
\sigma_B^2 = E \{ |y_B|^2 \} = h_{AB}^T R h_{AB}^*, \quad (5.13)
\]

\[
\sigma_E^2 = E \{ |y_E|^2 \} = h_{AE}^T R h_{AE}^*, \quad (5.14)
\]

\[
\sigma_{BE}^2 = E \{ y_B y_E^* \} = h_{AB}^T R h_{AE}, \quad (5.15)
\]

|·| is the determinant, and {·}* is the conjugate. Using (5.12), (5.11) becomes

\[
I(w; \hat{y}_B|\hat{y}_E) = \log_2 \left( \frac{\sigma_0^2 + \sigma_B^2 - |\sigma_{BE}|^2}{\sigma_E^2 \sigma_0^2} \right), \quad (5.16)
\]

\[
= \log_2 \left[ 1 + \frac{\sigma_B^2}{\sigma_0^2} \left( 1 - \frac{|\sigma_{BE}|^2}{\sigma_B^2 \sigma_E^2} \right) \right], \quad (5.17)
\]

The optimization problem is therefore

\[
C_S = \max_{R: \text{Tr}(AR) \leq P_T} \min_{\phi_E} \log_2[1 + \alpha(R, \phi_E)]. \quad (5.18)
\]

Since \(\log_2(\cdot)\) increases monotonically in its argument, the problem reduces to finding the transmission strategy that maximizes \(\alpha\), or

\[
\alpha_{\text{opt}} = \max_{R: \text{Tr}(AR) \leq P_T} \min_{\phi_E} \alpha(R, \phi_E), \quad (5.19)
\]

where \(C_S = \log_2(1 + \alpha_{\text{opt}})\).

### 5.1.2 Reciprocal Channel Key Establishment

Another way to communicate securely in a wireless environment is to encode transmissions using secret keys [35, 58]. To establish keys at the physical layer, Alice and Bob can each transmit known training data from which the other can estimate the channel, and
because of reciprocity the two estimates will differ only due to measurement errors. These estimates can then be quantized to form the encryption key. In a fading environment, the radios can estimate multiple independent channel observations over time and thereby construct long keys [59].

Unfortunately, the propagation channel does not fade in the LOS scenario, and therefore beamforming weights are used to generate random reciprocal channel observations, analogous to what was done with reconfigurable antennas in Chapter 4. Referring to Figure 5.3, Alice uses a randomly generated weight vector $\mathbf{w}$ to transmit a publicly known scalar pilot $y_A$, resulting in received signals $y_B$ at Bob and $y_E$ at Eve. Next, Bob transmits a publicly known scalar pilot $y_B'$, and Eve observes $y_E'$ while Alice weights the received signals by the vector $\mathbf{w}$ to obtain $y_A'$. By randomly changing $\mathbf{w}$ over time, different channel observations can be realized.

**Figure 5.3:** Signal model for reciprocal channel key establishment.
The effective end-to-end propagation channels created using this procedure are defined as

\[ h_{AB} = y_B / y_A = h_{BA}^T w, \]  
(5.20)

\[ h_{BA} = y_A / y_B = h_{AB}^T w = h_{AB}, \]  
(5.21)

\[ h_{BE} = y_E / y_B', \]  
(5.22)

\[ h_{AE} = y_E / y_A = h_{AE}^T w. \]  
(5.23)

Note that \( h_{BE} \) is not random (has no information) and therefore will be ignored in the subsequent analysis. It is assumed that the received signals are corrupted by zero-mean complex Gaussian noise \( \epsilon_\xi \) with \( \xi \in [A, B, E] \), meaning that only estimates of the channels are obtained, or

\[ \hat{h}_{AB} = h_{AB} + \epsilon_B, \]  
(5.24)

\[ \hat{h}_{BA} = h_{BA} + \epsilon_A, \]  
(5.25)

\[ \hat{h}_{AE} = h_{AE} + \epsilon_E. \]  
(5.26)

The reciprocal fading channels between Alice and Bob can be used to generate secret encryption keys. One secrecy metric for reciprocal channel key establishment is the number of \textit{secure key bits} given by

\[ I_{SK} = I(\hat{h}_{AB}; \hat{h}_{BA}|\hat{h}_{AE}). \]  
(5.27)

Assuming that the random vector \( w \) is drawn from a zero-mean complex Gaussian distribution and independently realized for each measurement, (5.27) can be computed in closed form as

\[ I_{SK} = \log_2 \frac{|R_1||R_2|}{\sigma_B^2|R_3|}, \]  
(5.28)
with

\[ R_1 = E \left\{ [\hat{h}_{AB}, \hat{h}_{AE}]^T [\hat{h}_{AB}, \hat{h}_{AE}]^* \right\} \]

\[ = \begin{bmatrix} \sigma_B^2 + \sigma^2_2 & \sigma_{BE} \\ \sigma_{BE}^* & \sigma_E^2 + \sigma_3^2 \end{bmatrix}, \]  

(5.29)

\[ R_2 = E \left\{ [\hat{h}_{BA}, \hat{h}_{AE}]^T [\hat{h}_{BA}, \hat{h}_{AE}]^* \right\} \]

\[ = \begin{bmatrix} \sigma_B^2 + \sigma^2_1 & \sigma_{BE} \\ \sigma_{BE}^* & \sigma_E^2 + \sigma_3^2 \end{bmatrix}, \]

(5.30)

\[ R_3 = E \left\{ [\hat{h}_{AB}, \hat{h}_{BA}, \hat{h}_{AE}]^T [\hat{h}_{AB}, \hat{h}_{BA}, \hat{h}_{AE}]^* \right\} \]

\[ = \begin{bmatrix} \sigma_B^2 + \sigma^2_2 & \sigma_B^* & \sigma_{BE} \\ \sigma_B^2 & \sigma_B^2 + \sigma^2_1 & \sigma_{BE} \\ \sigma_{BE}^* & \sigma_{BE}^* & \sigma_E^2 + \sigma_3^2 \end{bmatrix}, \]

(5.31)

where

\[ \sigma_B^2 = E \{ |h_{AB}|^2 \} = h_{AB}^T R h_{AB}^*, \]

(5.32)

\[ \sigma_E^2 = E \{ |h_{AE}|^2 \} = h_{AE}^T R h_{AE}^*, \]

(5.33)

\[ \sigma_{BE} = E \{ h_{AB} h_{AE}^* \} = h_{AB}^T R h_{AE}^*, \]

(5.34)

\[ \sigma_1^2 = E \{ |\epsilon_A|^2 \}, \sigma_2^2 = E \{ |\epsilon_B|^2 \}, \text{ and } \sigma_3^3 = E \{ |\epsilon_E|^2 \}. \]

Assuming equal estimation error variance at Alice and Bob (\( \sigma_1^2 = \sigma_2^2 = \sigma_0^2 \)) and a noiseless receiver at Eve (\( \epsilon_E = 0 \)), the determinants in (5.28) can be expanded to obtain

\[ I_{SK} = \log_2 \frac{1}{\sigma_E^2 \sigma_{BE}^2 (\sigma_0^4 + 2\sigma_B^2 \sigma_0^2 - 2\sigma_0^2 |\sigma_{BE}|^2)} \]

\[ = \log_2 \frac{[1 + \alpha(R, \phi_E)]^2}{1 + 2\alpha(R, \phi_E)}, \]

(5.38)

(5.39)

where

\[ \alpha(R, \phi_E) = \frac{\sigma_B^2}{\sigma_0^2} \left( 1 - \frac{|\sigma_{BE}|^2}{\sigma_B^2 \sigma_0^2} \right), \]

(5.40)
which is precisely the same expression for $\alpha$ that was for secrecy capacity in (5.16). Note that $\alpha(R, \phi_E) \geq 0$, and for this case it can be shown that $I_{SK}$ in (5.38) increases monotonically in $\alpha$. Therefore, only $\alpha$ needs to be maximized according to (5.19), after which the optimal $I_{SK}$ is given by

$$I_{SK, \text{opt}} = \log_2 \left[ 1 + \frac{\sigma_0^2 \alpha_{\text{opt}}}{1 + 2 \alpha_{\text{opt}}} \right].$$  \hspace{1cm} (5.41)

It is remarkable that both secrecy capacity and the number of secure key bits depend monotonically on $\alpha(R, \phi_E)$, allowing both problems to be solved using the same procedure. This observation further motivates use of the general term secure array synthesis for the solution.

### 5.2 Optimization Procedure

This section shows that the optimization problem in (5.19) can be written as a standard semi-definite program, indicating that the problem is convex and can be solved in an efficient manner. One form of SDP solves the problem \[71\]

$$\min_x c^T x, \quad \text{s.t.} \quad F(x) = F_0 + \sum_{m=1}^M x_m F_m \geq 0,$$  \hspace{1cm} (5.42)

where $\Gamma \geq 0$ indicates that $\Gamma$ is a positive semi-definite (PSD) matrix. To rewrite the secure array synthesis problem in this form, it is first transformed to the constrained optimization

$$\alpha'_{\text{opt}} = \max_{\gamma, R} \gamma \quad \text{s.t.} \quad \begin{cases} 
(i) & \alpha'(R, \phi_E) \geq \gamma, \forall \phi_E \notin [\phi_1, \phi_2] \\
(ii) & \text{Tr}(AR) \leq P_T \\
(iii) & R \geq 0 \\
(iv) & \gamma \geq 0,
\end{cases}$$  \hspace{1cm} (5.43)

where $\alpha'_{\text{opt}} = \sigma_0^2 \alpha_{\text{opt}}$ and $\alpha'(R, \phi_E) = \sigma_0^2 \alpha(R, \phi_E)$. The following subsections focus on how to cast the optimization into the general form of (5.42) and how each of the constraints (i)-(iv) in (5.43) can be written as a PSD constraint.
5.2.1 Optimization Variables

The unknown covariance matrix $R$ is first parameterized in terms of a set of unknown coefficients. This can be accomplished by expanding $R$ using a matrix basis, or

$$R = \sum_{m=1}^{M-1} r_m R_m.$$  \hfill (5.44)

A suitable set of basis matrices that span all possible positive semi-definite matrices is given by the set $S = S_R \cup S_I$, where

$$S_R = \{I + (E_{mn} + E_{nm})/2\}, m = 1, \ldots, N_T, n \geq m$$ \hfill (5.45)

$$S_I = \{I + j(E_{mn} - E_{nm})/2\}, m = 1, \ldots, N_T, n > m,$$ \hfill (5.46)

and $E_{mn}$ is an elementary matrix with a 1 at position $mn$ and zeros elsewhere. For $N_T = 2$, for example, the basis is

$$S = \left\{ \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{bmatrix}, \begin{bmatrix} 1 & i \frac{1}{2} \\ -i \frac{1}{2} & 1 \end{bmatrix} \right\}.$$ \hfill (5.47)

With this formulation, the unknowns consist of the $M-1$ values of $r_m$ and the value of $\gamma$ in (5.43). Therefore, the $M \times 1$ vector of real optimization variables is

$$x = [r_1, r_2, \ldots, r_{M-1}, \gamma]^T.$$ \hfill (5.48)

The maximization in (5.43) can be cast into the minimization form of (5.42) using $c = [0 \ldots 0 - 1]^T$.

5.2.2 Constraint (i): Minimum $\alpha$ Threshold

The constraint (i) is referred as a minimum $\alpha$ threshold, since its purpose is to ensure that $\alpha$ is no lower than a certain minimum level for all possible Eve angles. One difficulty is that (i) represents an infinite number of constraints, one at each possible value of $\phi_E$ outside of the exclusion sector. This is replaced with a finite set of $K$ constraints by uniformly
sampling Eve's possible angle at \( K \) values outside of the exclusion sector, which are denoted by \( \phi_{E,k} \), where \( \phi_{E,k} \notin [\phi_1, \phi_2] \). This results in the set of constraints

\[
\sigma_0^2 \alpha(R, \phi_{E,k}) \geq \gamma, \quad k = 1, \ldots, K. \tag{5.49}
\]

Substituting the basis expansion (5.44) into (5.40),

\[
\sigma_0^2 \alpha(R, \phi_{E,k}) = \frac{\sigma_B^2 \sigma_E^2 - |\sigma_{BE}|^2}{\sigma_E^2}, \tag{5.50}
\]

\[
= \frac{h_{AB}^T R h_{AB}^* h_{AE}^T R h_{AE}^* - h_{AB}^T R h_{AE}^* h_{AE}^T R h_{AB}^*}{h_{AE}^* R h_{AE}^*}, \tag{5.51}
\]

\[
= u^{(k)T} r v^{(k)T} r - z^{(k)T} r z^{(k)H} r \tag{5.52}
\]

where

\[
u_m = h_{AB}^T R_m h_{AB}^*, \tag{5.53}
\]

\[
u_m^{(k)} = h_{AE}^*(\phi_{E,k})^T R_m h_{AE}(\phi_{E,k})^*, \tag{5.54}
\]

\[
z^{(k)} = h_{AB}^T R_m h_{AE}(\phi_{E,k})^*. \tag{5.55}
\]

The constraint (5.49) can therefore be written as

\[
v^{(k)T} r (u^{(k)T} r - \gamma) - (z^{(k)T} r)(z^{(k)H} r) \geq 0, \quad k = 1, \ldots, K, \tag{5.56}
\]

which can be written as the determinant constraint

\[
\begin{vmatrix}
  u^{(k)T} r - \gamma & z^{(k)T} r \\
  z^{(k)H} r & v^{(k)T} r
\end{vmatrix} \geq 0. \tag{5.57}
\]
This is equivalent to the PSD constraint $F_E^{(k)} \geq 0$. The matrix $F_E^{(k)}$ can be expanded in terms of the unknown optimization variables $r$ and $\gamma$ as

$$F_E^{(k)} = \sum_{m=1}^{M-1} \begin{bmatrix} u_m & z_m^{(k)} & \bar{z}_m \end{bmatrix} r_m + \begin{bmatrix} -1 & 0 \\ 0 & 0 \end{bmatrix} \gamma$$

$$= F_{E,0}^{(k)} + \sum_{m=1}^{M} x_m F_{E,m}^{(k)} \geq 0, \quad (5.58)$$

where $F_{E,0}^{(k)}$ is the zero matrix.

### 5.2.3 Constraint (ii): Power Constraint

Substituting the basis expansion (5.44) into the power constraint (ii) gives

$$\text{Tr}(A R) = \text{Tr} \left( A \sum_{m=1}^{M-1} r_m R_m \right)$$

$$= \sum_{m=1}^{M-1} r_m \text{Tr}(A R_m) \leq P_T, \quad (5.60)$$

or

$$\frac{P_T}{F_{P,0}} + \sum_{m=1}^{M-1} r_m \left[ -\text{Tr}(A R_m) \right] \geq 0. \quad (5.61)$$

To write this in the form of (5.42), it is assumed that $F_{P,M} = 0$.

### 5.2.4 Constraint (iii): PSD Constraint on $R$

Note that although each of the basis matrices is Hermitian and PSD, a linear combination of these matrices is still Hermitian but not necessarily PSD. To represent an admissible solution, the transmit covariance must be PSD, or

$$R = \sum_{m=1}^{M-1} r_m R_m \geq 0, \quad (5.62)$$
which can be represented as a SDP constraint with the definitions

\[
F_{C,m} = \begin{cases} 
0, & m = 0, m = M, \\
R_m, & 1 \leq m \leq M - 1.
\end{cases}
\] (5.63)

5.2.5 Constraint (iv): Non-negativity Constraint on \( \gamma \)

The simple constraint \( \gamma \geq 0 \) can be written as the SDP constraint

\[
F_{\gamma,m} = \begin{cases} 
0, & 0 \leq m \leq M - 1, \\
1, & m = M.
\end{cases}
\] (5.64)

5.2.6 Solution Using MAXDET

Solutions to the SDP problem are found using the freely available MAXDET package \[72\] that solves the problem

\[
\min_x \ c^T x + \log_2 |G(x)|^{-1}
\]
\[\text{s.t. } G(x) > 0, \ F(x) \geq 0, \] (5.65)

where \( F(x) \) has the form given in (5.42) and

\[
G(x) = G_0 + \sum_{m=1}^{M} x_m G_m.
\] (5.66)

Since \( G \) is not needed, it is assumed that \( G_0 = 1 \) and \( G_m = 0, M = 1, \ldots, M \).

While many of the constraint matrices are complex, MAXDET (and many other SDP solvers) require that the constraint matrices be real. Fortunately, it can be shown that a square complex matrix \( F \) satisfies

\[
F \geq 0 \text{ if and only if } \bar{F} \geq 0,
\] (5.67)
where
\[
F \triangleq \begin{bmatrix}
\text{Re}\{F\} & -\text{Im}\{F\} \\
\text{Im}\{F\} & \text{Re}\{F\}
\end{bmatrix}.
\] (5.68)

Therefore, any complex-valued PSD constraint of the form given in (5.42) can be expressed as the equivalent real-valued PSD constraint
\[
F(x) = F_0 + \sum_{m=1}^{M} x_m F_m \geq 0.
\] (5.69)

Given this, the \(K + 3\) PSD constraints given in Sections 5.2.2 through 5.2.5 can be combined into a single PSD constraint using the block diagonal matrix
\[
F_m = \text{diag}\left(\begin{bmatrix}
F^{(1)}_{E,m}, & F^{(2)}_{E,m}, & \ldots, & F^{(K)}_{E,m}, \\
F_{P,m}, & F_{C,m}, & F_{\gamma,m}
\end{bmatrix}\right),
\] (5.70)

where \(\text{diag}(\cdot)\) creates a matrix with the vector elements arranged on the main diagonal.

### 5.3 Signal/Noise Pattern Analysis

Once the optimal covariance matrix \(R\) has been found using the outlined secure array synthesis procedure, it is desirable to visualize the solution. While one can simply plot the secrecy metric \(C_S\) or \(I_{SK}\) with respect to Eve’s angle, such plots only indicate what security is possible and give no insight into how it is achieved. An analysis that provides a more constructive visualization is possible by decomposing the transmit power pattern into signal and noise patterns.

Since Gaussian signaling is used, Eve’s receive quantity \(y_E\) (or \(h_{AE}\)) for a fixed angle \(\phi_E\) can be decomposed into a sum of two terms as
\[
y_E = \beta_C y_B + y_{UC},
\] (5.71)

where the first term is a Gaussian random variable that is perfectly correlated with Bob’s signal (\(\beta_C\) is a constant) and the second term \(y_{UC}\) is a Gaussian random variable that is
uncorrelated with Bob’s signal. While Eve can extract useful information from the signal \( \beta_C y_B \), the noise \( y_{UC} \) has no useful information content and serves to confuse Eve. Therefore, the following quantities are defined

\[
P_S = |\beta_C|^2 E \{ |y_B|^2 \}, \quad (5.72)\\
P_N = E \{ |y_{UC}|^2 \}, \quad (5.73)
\]
as the signal and noise power, respectively, observed by Eve. Plotting these quantities as a function of Eve’s angle produces signal and noise patterns that provide a meaningful visualization of the results.

To compute these quantities from the solution \( \mathbf{R} \) obtained from the SDP optimization, it is recognized that

\[
E \{ |y_E|^2 \} = \sigma_E^2 = |\beta_C|^2 E \{ |y_B|^2 \} + E \{ |y_{UC}|^2 \}, \quad (5.74)\\
E \{ y_B y_E^* \} = \sigma_{BE} = \beta_C^* E \{ |y_B|^2 \}, \quad (5.75)
\]
where \( E \{ y_B y_{UC}^* \} = 0 \) based on the definition of \( y_{UC} \). Comparing this to (5.12), it is simple to solve (5.74) and (5.75) to obtain

\[
P_S = \frac{|\sigma_{BE}|^2}{\sigma_B^2}, \quad (5.76)\\
P_N = \sigma_E^2 - \frac{|\sigma_{BE}|^2}{\sigma_B^2}. \quad (5.77)
\]

It is important to emphasize that the signal/noise pattern interpretation given in (5.76) and (5.77) provides the information required to compute \( C_S \) and \( I_{SK} \). To see this \( \alpha \) can be expressed as,

\[
\alpha(\mathbf{R}, \phi_E) = \frac{\sigma_B^2}{\sigma_0 \sigma_E^2} \left( \sigma_E^2 - \frac{|\sigma_{BE}|^2}{\sigma_B^2} \right) = \frac{\sigma_B^2}{\sigma_0^2} \frac{P_N}{P_S + P_N} = \frac{\text{SNR}_{Bob}}{1 + \text{SNR}_{Eve}}. \quad (5.78)
\]

89
5.4 Numerical Examples

This section illustrates application of the secure array synthesis method to some practical examples. While a uniform linear array (ULA) and a uniform circular array (UCA) of idealized patch antennas is used for these examples, the method is general and can be used for any array topology. The inter-element spacing for all cases is assumed to be \( \lambda/2 \), where \( \lambda \) is the free-space wavelength.

Since both \( I_{SK} \) and \( C_S \) have a monotonic relationship with respect to \( \alpha \), results have focused on \( I_{SK} \) in this analysis. Simulations are performed by varying the exclusion zone \( (\phi_X) \), location of Bob \( (\phi_B) \) and Eve \( (\phi_E) \), and the number of transmit antennas at Alice \( (N_T) \). In all simulations, angles for Eve outside of the exclusion zone are sampled uniformly in \( 1^\circ \) increments on \( \phi_E \in [0, \phi_1] \cup [\phi_1, 180^\circ] \) for the ULA and \( \phi_E \in [0, \phi_1] \cup [\phi_2, 360^\circ] \) for the UCA. Also, the specific element pattern used for the patches is given by

\[
g(\phi) = \frac{2\sin\left(k_0 h/2 \cos \phi \right)}{k_0 h \cos \phi} \cos \left(\frac{k_0 L}{2}\right) \sin \phi,
\]

where \( h = 0.003\lambda \) and \( L = 0.5\lambda \).

5.4.1 Suboptimal Approach for ULA

It is instructive to consider the security of a simple but suboptimal array synthesis approach to illustrate the performance advantage enabled by the secure array synthesis method. Specifically, for a ULA the Dolph-Chebyshev beam weights \( \mathbf{w} \) are computed that place maximum gain in the direction of Bob (angle \( \phi_B \)) for a specified sidelobe level \( L_{SL} \). The pattern associated with \( \mathbf{w} \) is referred as the signal pattern, as it is used to transmit useful information to Bob. The singular value decomposition of \( \mathbf{w} \) is computed as

\[
\mathbf{w} = \mathbf{U}\Lambda\mathbf{V}^H = [\mathbf{u}_1 \mathbf{U}_0] \begin{bmatrix} \lambda_1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} \mathbf{V}_1^H \\ \mathbf{V}_0^H \end{bmatrix},
\]

where \( \mathbf{u}_1 \) is a unit-length version of the vector \( \mathbf{w} \) and the matrix \( \mathbf{U}_0 \) consists of unit-length, mutually-orthogonal column vectors that are orthogonal to \( \mathbf{u}_1 \). The vectors in \( \mathbf{U}_0 \) are then
used to transmit noise to confuse Eve, with the resulting patterns again denoted as \textit{noise} patterns.

Given these beamforming weights, \( \zeta \) is used to represent the fraction of transmit power devoted to the signal pattern and \( \bar{\zeta} \) to represent the fraction of power devoted to each noise pattern so that \( \bar{\zeta} = (1 - \zeta)/(N_T - 1) \). The covariance of the transmit signals is then given by

\[
R' = U\Sigma U^H,
\]

(5.82)

where \( \Sigma = \text{diag} \left( [\zeta, \bar{\zeta}, \ldots, \bar{\zeta}] \right) \). Finally, \( R' \) is scaled to ensure satisfaction of the transmit power constraint using

\[
R = R'/\text{Tr}(AR').
\]

(5.83)

Using this form of the covariance \( R \), \( \alpha \) in (5.40) can be computed as a function of \( L_{SL} \) and \( \zeta \). A brute-force search on \( \zeta \in [0, 1] \) and \( L_{SL} \in [0, 20] \) dB is used to determine the values of \( \zeta \) and \( L_{SL} \) that maximize the minimum value of \( \alpha \) for all values of \( \phi_E \) outside the exclusion sector.

### 5.4.2 Uniform Linear Array

The suboptimal procedure is first applied to a 10-element ULA at Alice with Bob at \( \phi_B = 90^\circ \) (broadside to the ULA) and an exclusion sector around Bob of \( \phi_X = 20^\circ \). The optimization produces \( \zeta = 0.723 \) and \( L_{SL} = 15.6 \) dB for this scenario. Figure 5.4(a) plots the signal (or Dolph-Chebyshev) pattern scaled by the signal power fraction \( \zeta \) as well as the linear combination of the equally-weighted noise patterns for the optimal parameter values. As expected, Bob observes more signal than noise, while an eavesdropper outside of the exclusion sector observes more noise than signal. Note that although the Dolph-Chebyshev solution produces an array factor with equal sidelobes, the patch element radiation pattern also shapes the signal and noise patterns. Figure 5.4(b) plots \( I_{SK} \) for different values of \( \zeta \) and demonstrates how the optimal value of \( \zeta = 0.723 \) maximizes the minimum value of \( I_{SK} \).

Figures 5.5(a) and (b) plot the performance achieved using the suboptimal and optimal approaches, respectively, as a function of Bob’s angle \( \phi_B \) ranging from array endfire
Figure 5.4: Suboptimal method for secure array synthesis employing a ULA with $N_T = 10$, $\phi_B = 90^\circ$, and $\phi_X = 10^\circ$: (a) power allocation to signal and noise patterns, (b) achieved $I_{SK}$ performance for different power allocations.

Figure 5.5: Performance of the (a) suboptimal and (b) optimal methods for a ULA at Alice with $\phi_X = 10^\circ$. Performance is shown with respect to the number of antennas at Alice ($N_T$) and the transmit angle to Bob ($\phi_B$).
Figure 5.6: Achieved $I_{SK}$ for a varying number of antennas in Alice’s ULA and different transmit angles to Bob for $\phi_X = 20^\circ$: (a) optimal solution, (b) suboptimal solution.

($\phi_B = 0^\circ$) to broadside ($\phi_B = 90^\circ$) for an exclusion sector of $\phi_X = 10^\circ$ and different values of $N_T$.

The results for the suboptimal technique show that the worst-case value of $I_{SK}$ is reduced significantly when either Bob moves towards the endfire direction or the size of Alice’s array is reduced because of the inferior beamforming capabilities of the ULA under these conditions. While similar trends appear in the results for the optimal solution, the secure array beamforming technique provides performance gains of nearly 50% for the smallest array when Bob is close to the broadside direction. Furthermore, the optimal beamforming technique maintains higher values of $I_{SK}$ as Bob moves towards endfire.

Figure 5.6 repeats the analysis of Fig. 5.5 for a larger exclusion sector of $\phi_X = 20^\circ$. In this case, the performance of the suboptimal and optimal solutions is similar for large array sizes when Bob is at array broadside. However, as Bob moves toward array endfire, $I_{SK}$ falls more rapidly for the suboptimal than for the optimal method. This highlights the fact that the secure array synthesis approach has the potential to offer significant performance gains over heuristic methods in a dynamic system where Bob’s position is variable.
Figure 5.7: Comparison of radiated signal ($P_S$) and noise ($P_N$) for the (a) suboptimal and (b) optimal approaches for a ULA at Alice with $N_T = 10$ elements, $\phi_X = 10^\circ$, and $\phi_B = 90^\circ$. The horizontal line is the minimum $I_{SK}$ outside of the exclusion sector.

It is instructive to use the signal/noise pattern analysis developed in Section 5.3 to further understand the behavior of the two solutions. Figure 5.7 plots the number of secure key bits, signal power, and noise power as a function of Eve’s angle $\phi_E$ for $N_T = 10$, $\phi_X = 10^\circ$, and $\phi_B = 90^\circ$. The straight horizontal line in each plot shows the minimum value of $I_{SK}$ obtained outside of the exclusion sector. At Bob’s position, both solutions place a peak in the signal power and null in the noise power as expected, meaning that security would be compromised if Eve were to reside in the exclusion sector.

Outside of the exclusion sector, a null in $P_S$ corresponds to a peak in $I_{SK}$, which is intuitive since no signal power reaches Eve for these angles. Conversely, a minimum value in $I_{SK}$ coincides with the peak of each sidelobe in $P_S$, with the noise pattern $P_N$ placing sufficient noise power at these points to keep $I_{SK}$ at or above the minimum value (horizontal line). It is observed that as compared to the optimal synthesis, the suboptimal synthesis directs more signal energy outside of the exclusion sector, resulting in a higher minimum threshold. Furthermore, the optimal method achieves an exact equal ripple response (the minima of
5.4.3 Uniform Circular Array

In order to demonstrate that the secure array synthesis can be applied to any array topology, a UCA is considered in this section. Since the suboptimal approach is based on Dolph-Chebyshev synthesis for a ULA, it is not considered here. Figure 5.8 plots the average achieved minimum value of $I_{SK}$ as a function of $N_T$ for different values of $\phi_X$, where the average is taken over $\phi_B \in [90^\circ, 180^\circ]$ with a step size of 1°. As expected, $I_{SK}$ increases with the number of antennas and the exclusion sector angle.

Figure 5.9 plots $I_{SK}$ as a function of Bob’s location for $\phi_X = 40^\circ$ and several values of $N_T$. These results show that the relative variation with $\phi_B$ is significant for small arrays and less significant as $N_T$ increases. Finally, Figure 5.10 analyzes the optimal solution using signal and noise patterns. Although the $I_{SK}$ ripple with angle is less regular for the UCA than for the ULA, the synthesized array still ensures that $I_{SK}$ remains above a minimum
Figure 5.9: $I_{SK}$ for a varying number of antennas in Alice’s UCA and different transmit directions to Bob for $\phi_X = 40^\circ$.

Figure 5.10: $I_{SK}$, $P_S$, and $P_N$ with respect to Eve’s location for a UCA at Alice with $N_T = 12$ elements, $\phi_X = 40^\circ$, and $\phi_B = 270^\circ$. 
value. Within the exclusion sector, the behavior of the signal and noise patterns follow the trends previously observed for the ULA.

5.5 Key Establishment in Static Multipath Channels

This section extends the method presented earlier to the case of a static multipath channel. The channel is modeled by assuming a specific power angular spectrum (PAS) at the nodes, and the optimization procedure maximizes the secure key generation rate for the worst-case position of an eavesdropper.

5.5.1 Information Theoretic Analysis

Figure 5.11 shows the communication scenario, where Eve is close to Bob such that there can be correlation between the channel from Alice to Bob and the channel from Alice to Eve. Although the optimization method is general with respect to the array topology and antenna types, this analysis concentrates on an illustrative example where all antennas are half-wave dipoles and Alice’s array is a uniform linear array (ULA) with $N_T$ elements and $\lambda/2$ inter-element spacing. For a multipath propagation environment, rather than a separation angle it is more practical to define a minimum distance between between Bob and Eve ($d_{\text{min}}$), which is used in this analysis.
Consistent with the scenario in Section 5.1, it is assumed that Eve can be no closer to Bob than $d_{\text{min}}$, since when Eve is too close, very little additional security is possible using physical layer techniques. However, in the LOS scenario considered earlier, Alice knows the channel that Eve would observe as a function of Eve’s position and therefore can optimize the channel estimation to minimize $I_{SK}$ over all possible Eve locations. In contrast, in this multipath channel Alice cannot know the channel to Eve for any of her positions, and therefore Alice must perform her optimization based on the possible statistical correlation between the Alice-to-Bob and Alice-to-Eve channels. This means that $\sigma_E^2$, $\sigma_{BE}^2$, and $I_{SK}$ are random variables. Although there are many possible criteria for optimal security, this work focuses on maximizing the minimum average value of $\alpha$ over all possible locations for Eve, as this should lead to high $I_{SK}$. The average value of $\alpha$ is defined as

$$\alpha_{\text{avg}} = \frac{\sigma_B^2 \mathbb{E}\{ \sigma_E^2 \} - \mathbb{E}\{|\sigma_{BE}|^2\}}{\mathbb{E}\{\sigma_E^2\} \sigma_0^3}, \tag{5.84}$$

where $\mathbb{E}\{\sigma_E^2\} = \text{Tr}\{RR_E^*\}$, $\mathbb{E}\{|\sigma_{BE}|^2\} = h_{AB}^T R_{BE}^* R_{AE}^* h_{AE}^T$, $R_E = \mathbb{E}\{h_{AE}^* h_{AE}^T\}$, and $\text{Tr}\{\cdot\}$ is the trace.

The goal of this optimization is to find the value of $R$ for a fixed $h_{AB}$ that maximizes the minimum value of $\alpha_{\text{avg}}$ over all possible locations of Eve satisfying $d > d_{\text{min}}$. To model the correlation between the Alice-to-Bob and Alice-to-Eve channels the von Mises distribution is used for the PAS at Alice and Bob/Eve. This PAS results in a closed form expression for the spatial correlation [73] given by

$$\rho(\Delta) = \frac{I_0(\sqrt{\kappa^2 - 4\pi^2 \Delta^2} + j 4\pi \kappa \cos(\theta_p) \Delta)}{I_0(\kappa)}, \tag{5.85}$$

where $\Delta$ is the electrical distance between antennas, $\kappa$ defines the angular distribution of the multipath departures or arrivals, $\theta_p$ is the mean angle of arrival/departure (assumed to be 0 in this analysis) and $I_0$ is the zero-order modified Bessel function. Note that the von Mises distribution is uniform for $\kappa = 0$ and becomes more Gaussian as $\kappa$ increases. If both transmit and receive correlation are known, the Kronecker model can be used to generate
channels with the specified correlation according to

\[
\begin{bmatrix}
    h_{AE} \\
    h_{AB}
\end{bmatrix}
= R_t^{1/2} \mathbf{H}' R_r^{1/2},
\]

(5.86)

where \( R_t \) and \( R_r \) are \( N_T \times N_T \) transmit and \( 2 \times 2 \) receive correlation matrices, respectively, and \( \mathbf{H}' \) is \( 2 \times N_T \) zero-mean complex Gaussian distributed random matrix. Note that the separation between Alice’s antennas is fixed at \( \lambda/2 \) while the distance \( d \) between Eve’s antenna and Bob’s antenna is variable.

The covariance matrix of stacked channels \( h_{AE} \) and \( h_{AB} \) can be expressed as

\[
C_S = \begin{bmatrix}
    C_E & C_{EB} \\
    C_{BE} & C_B
\end{bmatrix}.
\]

(5.87)

Let \( \mu_{AB} \) and \( \mu_{AE} \) be the mean of the channels \( h_{AB} \) and \( h_{AE} \) respectively, then the mean and covariance matrix of the multivariate normal distribution of \( h_{AE} \) conditioned on a specific observation of \( h_{AB} \) can be computed using

\[
\bar{\mu}_{AE} = \mu_{AE} + C_{EB} C_B^{-1} (h - \mu_{AB}),
\]

(5.88)

\[
\bar{C}_E = C_E - C_{EB} C_B^{-1} C_{BE}.
\]

(5.89)

Finally the correlation matrix of the Alice to Eve channel can be expressed as \( R_E = \bar{C}_E + \bar{\mu}_{AE} \bar{\mu}_{AE}^H \). Note that because of the propagation channel statistics, \( \mu_{AE} = \mu_{AB} = 0 \).

5.5.2 Analysis and Results

In order to understand the impact of transmit correlation, two different cases i.e., \( \kappa = 0 \) (low transmit correlation) and \( \kappa = 10 \) (high transmit correlation) are used at Alice. At Bob/Eve it is assumed that \( \kappa = 2 \). Similar to the LOS case, semidefinite programming (SDP) is used to find the optimal value of \( R \) when \( d > d_{min} \). Figure 5.12 presents the resulting value of \( I_{SK} \) averaged over 1000 realizations of \( h_{AB} \) as a function of \( d_{min} \) for both high and low transmit correlation. As expected, an increase in the distance between Bob
and Eve increases $I_{SK}$ by reducing the receive correlation between $h_{AB}$ and $h_{AE}$. The results further show that high transmit correlation notably reduces $I_{SK}$.

The results presented above are then compared to those from a suboptimal approach in which signal (the secret key) is transmitted on the dominant dimension of the Alice-to-Bob channel and artificial noise is transmitted uniformly on the orthogonal complement to the dominant dimension, where the dominant dimension and its orthogonal complement are found using the singular value decomposition (SVD) i.e., $h_{AB} = U\Lambda V^H$. The transmit covariance is then formed according to $R = UA'U^H$, where $A' = \text{diag}(\gamma, \gamma', \ldots, \gamma')$, and $\gamma' = (1 - \gamma) / (N_a - 1)$. The performance of the suboptimal approach is maximized by numerically searching for the optimal value of $\gamma$ for each realization of $h_{AB}$. Figure 5.12 compares the optimal solution found using SDP to that obtained from the suboptimal SVD approach. The results show that the optimal approach significantly outperforms the suboptimal approach, with the relative improvement increasing with the transmit correlation.

In order to better understand the results a signal/noise pattern analysis is performed similar to the one presented in Section 5.3. However, since the propagation channel between Alice and Eve is unknown, expectation is used to compute the signal and noise powers given
Figure 5.13: Ratio of expected noise versus signal power at Eve for both low and high transmit correlation cases as a function of minimum distance between Bob and Eve. The dashed lines corresponds to the sub-optimal results.

by

\[
P_S' = \frac{E\{|\sigma_{ab}|^2\}}{\sigma_a^2},
\]

\[
P_N' = \frac{E\{\sigma_b^2\} - E\{|\sigma_{ab}|^2\}}{\sigma_a^2}.
\]

Figure 5.13 plots the ratio \(E\{P_N'\}/E\{P_S'\}\) for the same cases as depicted in Figure 5.12, where the expectation is taken over \(10^3\) realizations of \(h_{AB}\). Results demonstrate that as compared to the SDP solution noise power is significantly lower than signal power for the suboptimal approach, which reduces the corresponding \(I_{SK}\). It is important to note that for the suboptimal approach there is a significant difference between high and low transmit correlation cases, which is depicted in \(I_{SK}\) also. However the signaling strategy of the SDP solution is almost the same.

Although the signal and noise pattern analysis identifies the differences between the two approaches, it does not reveal differences in the structure of the covariance matrix. For this purpose, the singular value decomposition of optimal and sub-optimal covariance matrices is performed. The analysis reveals that for the optimal covariance matrix (\(R_{opt}\))
only two non-zero singular values exist. On the other hand for the sub-optimal case \((\mathbf{R}_{\text{sopt}})\), a full-rank covariance is used, with \(\gamma\) for the signal singular value and \((1 - \gamma)/N_T\) for the noise singular values.

Figure 5.14 plots the singular value corresponding to the signal pattern for the sub-optimal case. For the optimal case, it is not clear whether both of the singular values contribute to the signal pattern or not. It is hypothesized that the subspace associated with the smaller singular value is signal, due to its similarity with the suboptimal solution. Hence, for illustration purpose the smaller non-zero singular value for \(\mathbf{R}_{\text{opt}}\) is plotted. As expected the results depict that for high transmit correlation there is less power on the signal pattern and more on the noise patterns. Aside from this observation there is no apparent relation between optimal and sub-optimal approaches.

Next, the correlation between the singular vectors of optimal and suboptimal covariance matrices is analyzed. For this purpose the dominant singular vector of \(\mathbf{h}_{\text{AB}}\), i.e., \(\mathbf{V}(\cdot;1)\), is projected on the eigenvectors \((\mathbf{Q})\) of \(\mathbf{R}_{\text{opt}}\), which correspond to non-zero eigenvalues. Figure 5.15(a) plots the corresponding results for the high transmit correlation case, where dashed lines refer to the projection on the dominant eigenvector of \(\mathbf{R}_{\text{opt}}\). It is inter-
Figure 5.15: Orthogonal projection of dominant singular vector of channel $h_{AB}$ on the eigenvectors of optimal transmit covariance matrix $R_{opt}$ which corresponds to non-zero eigenvalues: (a) High transmit correlation. (b) Low transmit correlation.

esting to note that the orthogonality with respect to the non-dominant eigenvector of $R_{opt}$ reduces with distance which results in an increased difference in $I_{SK}$. Figure 5.15(b) plots the corresponding results for the low transmit correlation case with similar observations. Although, it is hard to make a direct comparison between SVD of the covariance matrix and the corresponding $I_{SK}$ but the results depict that the difference in signaling strategy in terms of eigenvectors gives the optimal approach an significant advantage.

5.6 Chapter Summary

This work has posed the problem of secure array synthesis, which maximizes the information transmitted to a desired location while minimizing the information leaked to an eavesdropper at all possible locations outside a specified exclusion sector. Whereas traditional array synthesis focuses on a single pattern, secure array synthesis involves joint optimization of two radiation patterns: one that transmits useful signal and another that transmits artificial noise. The synthesis problem is solved by casting the problem into a form suitable for existing semi-definite programming solvers. Comparison of results produced by this optimization with those obtained from a suboptimal approach demonstrates that the
optimization can significantly improve the realized secure key rate and secrecy capacity in both LOS and realistic multipath scenarios.
Chapter 6

Reconfigurable Over-the-Air Chamber

As wireless devices become more sophisticated, exploiting multiple polarizations and multiple spatial degrees of freedom, the ability to characterize and assess relative performance in a repeatable way becomes increasingly difficult. Theoretically, the performance of a multiport antenna system can be characterized separately from higher-level signal processing, modulation, and coding, but doing so in a device and algorithm-independent way is very difficult.

In contrast to isolated antenna system characterization, over-the-air (OTA) testing measures the performance of complete end-to-end communications in a controlled propagation environment. One method for OTA testing is demonstrated in [74–76], where the device under test (DUT) is surrounded by an array of antennas in an anechoic chamber, allowing several realistic multipath environments to be simulated in a repeatable way. A more economical and compact method is to use a mode stirred reverberation chamber [77, 78], also allowing repeatable end-to-end testing of devices. While adding controllable delay lines to a reverberation chamber increases control over the field emulation [79], the ability to control the detailed propagation parameters for reverberation chambers is often limited.

Inspired by developments in reconfigurable antennas, the idea of a reconfigurable OTA chamber (ROTAC) is explored in this chapter. The ROTAC can be seen as a device whose walls are lined with antennas, a few of which may be attached to a channel emulator and the balance of which are connected to reconfigurable impedances. This chapter presents the design of a ROTAC and covers the simulations conducted to control the field statistics inside the chamber. An experimental prototype of ROTAC is also built and presented to indicate the degree of control over the synthesized channel spatial characteristics.
6.1 Idealized Chamber Topology

In this section, a circular two-dimensional chamber is simulated, but the idea can be naturally extended to three-dimensional operation. The idealized chamber is depicted in Figure 6.1, consisting of an outer wall whose surface is densely covered with radiating antennas that are accessible at external ports. Exciting these ports generates waves that radiate into the chamber, generating a desired wave field at the device under test (DUT). Additionally, loads can be placed at the ports to absorb outgoing waves that are scattered by the DUT.

In this work, the idealized chamber is efficiently modeled using the surface-based method-of-moments framework presented in [80], which was applied for on-body propagation. In this two-dimensional framework, the TM$_z$ fields in the chamber are completely determined by $E_z$ and $\partial E_z / \partial n$ on the outer boundary, where

\begin{align}
E_z(x, y) &= \sum_{m=1}^{M} a_m f_m(x, y) \quad (6.1) \\
\frac{\partial E_z(x, y)}{\partial n} &= \sum_{m=1}^{M} b_m f_m(x, y), \quad (6.2)
\end{align}
\( a_m \) and \( b_m \) are unknown coefficients, \( f_m(x,y) \) is a pulse basis function for the \( m \)th surface element, and \( \hat{n} \) is the outward surface normal. Applying the moment method, a system of equations for the chamber is found as

\[
[I + Q]a = Sb, \tag{6.3}
\]

where \( I \) is the identity matrix and expressions for the matrices \( Q \) and \( S \) are given in [80].

Next an equivalent-circuit model of this system is developed. Denoting tangential electric and magnetic field intensities at the boundary as \( E_0 \) and \( H_0 \), respectively, and considering propagation at a single planar boundary reveals

\[
E_0 = E_z \triangleq v \tag{6.4}
\]
\[
H_0 = \frac{1}{j k_0 \eta_0} \frac{\partial E_z}{\partial n} \triangleq i, \tag{6.5}
\]

where \( k_0 \) and \( \eta_0 \) are the wavenumber and intrinsic impedance of free space, and \( v \) and \( i \) denote equivalent voltage and current quantities. This result can be combined with (6.3) to obtain,

\[
[I + Q]^{-1} S(j k_0 \eta_0) i = v, \tag{6.6}
\]

where \( Z \) is equivalent impedance matrix of the system. The matrix equation (6.6) allows the chamber to be analyzed with equivalent-circuit techniques, where sources and loads can be placed on the ports, and the current and voltage vectors \( i \) and \( v \) can be found. Interior fields of the chamber can then be found by solving for \( a \) and \( b \) and applying [80]

\[
E_z(x,y) = -Q(x,y)a + S(x,y)b. \tag{6.7}
\]

Although in this work an idealized two-dimensional ROTAC is considered, where fields on the boundary are directly excited at idealized ports, a practical implementation would be possible by using conformal slots and/or patches on the wall of a three-dimensional structure, which is presented in Section 6.4.
6.2 Electromagnetic Wave-field Synthesis

A straightforward but costly way to use the chamber is to excite each port of the chamber with an independent source. To provide absorption of waves scattered by a DUT, the sources should have an embedded impedance that absorbs signals flowing out the port. In initial investigations, it was found that terminating the ports with the free-space wave impedance (377 Ω) provides reasonable absorption of outgoing waves.

Figure 6.2 illustrates how a multipath wave field can be almost exactly realized using this technique. Here the chamber has a diameter of 4λ, where λ is the free space wavelength, and the outer boundary is excited at 101 equally spaced ports, where each port is driven with a voltage source having an internal impedance of 377 Ω. The desired wave field was generated by superimposing 20 plane wave components, each having Rayleigh amplitude, uniform phase, and uniform arrival angle. The source voltages at the ports are then specified by computing the desired field in an inner 2λ diameter control region in the middle of the chamber and inverting the equivalent-circuit model to find the required currents (and therefore source voltages) at the boundary. As shown in the figure, the complicated incident wave field is almost exactly reconstructed using this technique, which should be expected based on Huygens’ principle.
Although the independent excitation of each port provides nearly arbitrary specification of incident fields in the chamber, a more cost-effective method is to use the chamber in a manner similar to mode-stirred reverberation chambers. However, instead of using mechanical movement of scatterers in the chamber, reconfigurable loads are used at the boundary ports to provide control over incident fields in the chamber, which is the idea of the ROTAC.

### 6.3 Synthesis of Channel Fading

This section illustrates how channel fading can be simulated using a simpler structure than one where sources are placed on all ports. The same 4λ chamber is considered, but in this case with only 32 ports, as depicted in Figure 6.3. The ROTAC is realized by driving only four ports with active sources with constant amplitude and phase, while terminating the other 28 ports with lossy reconfigurable elements (REs).
6.3.1 Generation of Rayleigh Fading

First the possibility of generating close to Rayleigh fading is considered by attempting
to make the fields in the chamber as random as possible. For this case, the voltages of the
active sources are chosen to be $v_s = [1 \quad j \quad -1 \quad -j]^T$, where $j = \sqrt{-1}$, and a source impedance
of $R_{s,i} = 377 \, \Omega$. The impedance of the $i$th RE is given by $Z_i = R_i + jX_i$, where a constant
resistance of $34 \, \Omega$ is assumed and $X_i \sim \mathcal{U}(-500 \, \Omega, 500 \, \Omega)$, where $\mathcal{U}(x_1, x_2)$ denotes a uniform
distribution on the interval $[x_1, x_2]$. The statistics of the fading in the chamber are analyzed
by storing the fields at 24 sample points separated by $0.04\lambda$ placed along the line $L$ in
Figure 6.3.

A simulation of $10^4$ random realizations is performed, where only the RE reactances
are randomly varied as described above. Figures 6.4 and 6.5 plot the amplitude/phase
probability density functions (pdfs) at the center sample point and the average correlation
coefficient along the line $L$, respectively. As can be seen, the statistics are close to an ideal
Rayleigh distribution. Further improvement and fitting of other distributions is possible by
more careful selection of the RE impedances, as described below.
6.3.2 Fading Distribution Optimization

Next, how the parameters of the ROTAC port terminations can be controlled in order to generate a particular channel fading environment inside the chamber is illustrated. In this study, the optimization of the following parameters is considered:

1. The source excitation voltage vector $v_s$, whose elements can be arbitrary complex values (amplitude and phase) under the constraint $0 \leq |v_{s,i}| \leq 1$.

2. The constant resistance $R_0$ of the RE impedances ($R_i = R_0$), where the constraint $R_0 \in [10, 145]$ Ω is assumed.

3. The endpoints $X_{\min}$ and $X_{\max}$ of the uniform distribution used for the RE reactances, where $X_i \sim U(X_{\min}, X_{\max})$. The bounds $X_{\min}, X_{\max} \in [-2\eta_0, 2\eta_0]$ and $X_{\min} < X_{\max}$ are assumed.

These parameters are collected into the 11-element vector

$$w = [|v_s^T| \angle v_s^T R_0 X_{\min} X_{\max}]^T,$$

(6.8)
where optimization of the parameters is performed using a genetic algorithm (GA) using the fitness function
\[ F(w) = -\max_i |f_{\text{ideal}}(x_i) - f_{\text{actual}}(x_i|w)|^2, \] (6.9)
which minimizes the maximum squared error between the ideal and actual pdfs.

The GA starts with a randomization phase having an initial population of \( N_I = 100 \) vectors, where each population vector has the format given in (6.8) and whose entries are generated uniformly over the allowable range. The fitness function is computed for the initial population, and the best \( N_B = 10 \) vectors (those with the highest fitness) are retained. The GA uses \( N_B \) population vectors to generate \( N_{\text{GA}} = 60 \) new population vectors using mutations and cross-overs, where cross-overs are only possible within the same parameter type (e.g. source voltages with source voltages), and the mutation probability is varied from 10% to 50%. The fitness function is evaluated for \( N_{\text{GA}} \) population vectors and only the best \( N_B \) vectors are retained.

The steps in the previous paragraph are repeated \( N_R = 100 \) times and the vector in the final population having the highest fitness is declared to be the solution.

6.3.3 Rician Fading Example

As an example, synthesis of a Rician distribution is considered which is given by
\[ f(x|\nu, \sigma) = \frac{x}{\sigma^2} \exp \left[ -\frac{(x^2 + \nu^2)}{2\sigma^2} \right] I_0 \left( \frac{x\nu}{\sigma^2} \right), \] (6.10)
where \( I_0 \) is the modified Bessel function of the first kind with order zero. In simulations, the ROTAC parameters are optimized for a few different values of \( \sigma \) for a constant value of \( \nu \). For fitness computations, the actual pdf for a single parameter vector \( w \) is obtained using \( 10^4 \) random realizations of the RE loads and computing a histogram.

Figure 6.6 plots the Rician probability distribution function (pdf) obtained using (6.10) and the optimal solution from the GA, where the field was sampled at the center of the chamber. As can be seen, a very close fit to the desired distribution can be obtained by proper selection of the RE parameters.
Figure 6.6: Amplitude pdfs of the field sampled at the center of the chamber for uniform RE reactances, where in each case the distribution parameters are optimized for a specific value of $\sigma$ and $\nu$.

6.3.4 Frequency Selective Fading

Previous sections have demonstrated that the ROTAC is capable of providing useful fading distributions at a single frequency. However, due to the small size of the chamber, one may question whether useful frequency-selective fading is possible. To provide frequency selectivity, the chamber must reverberate, or in other words, the signal transmitted from a source port must be involved in multiple bounces in the chamber before decaying to a negligible level.

In order to analyze the frequency response characteristics of the field generated inside the chamber, the structure is simulated from 280 to 320 MHz, where the chamber diameter is 4 m (or $4\lambda$ at 300 MHz). The control parameters used in this case are the ones that generated the Rayleigh amplitude distribution in the first example. Figure 6.7 plots the field power in dB at the center of the chamber versus frequency for 4 random realizations of RE reactances. As is evident, significant and diverse frequency selectivity is obtained for the different random states.
Figure 6.7: Power versus frequency for 4 different realizations of the RE reactances, where the field was sampled in the middle of the chamber.

6.3.5 Channel Delay Spread

One potential application of the ROTAC is to produce a certain delay spread of multipath to simulate a specific wireless channel. Here the delay spread is obtained for a single set of parameters, suggesting that delay-spread optimization is also possible using the optimization techniques described previously. In this study $10^4$ random realizations of RE impedance states are used, where for each realization the frequency-dependent field $E_z(f)$ at the center of the chamber and the associated time-domain response $E_z(t)$ is computed using an inverse Fourier transform. The mean power of the frequency- and time-domain responses is computed by averaging $|E_z(f)|^2$ and $|E_z(t)|^2$ respectively over the $10^4$ realizations.

Figure 6.8 plots the average frequency- and time-domain power over the 40 MHz bandwidth. Both plots are normalized to obtain a maximum value of 1 (0 dB). The frequency step size was chosen to be 0.25 MHz, which corresponds to a maximum unambiguous delay of $4 \, \mu$s. Since 161 points are used to cover 40 MHz bandwidth, the time resolution is 25 ns. The results demonstrate that the average power delivered to each frequency is fairly constant and that the average delay spread is on the order of 150 ns. Note that the time for a propagating wave to travel the width of the chamber (4 m) is 13 ns, which indicates a useful level of
reverberation. As stated previously, more precise control of the delay spread is likely to be possible using optimization techniques.

6.3.6 Directional Propagation Characteristics

Another potential application of the chamber is to generate multipath with a certain power angle spectrum (PAS). For example, in many wireless propagation environments, multipath tend to come in clusters, and one may desire to specify a PAS composed of one or more such clusters. In order to explore the idea of generating different PAS profiles, fields inside the chamber can be transformed from element space into wavenumber (or propagation direction) space using the equation

\[
S(\phi) = \int_A E(x, y) \exp[-jk_0(x \cos \phi + y \sin \phi)] \, dA, \tag{6.11}
\]

where the two-dimensional integral is performed over the circular area \(A\) having a diameter of \(\lambda/3\) positioned at the center of the chamber.
Figure 6.9: Dependence of propagating power versus arrival angle $\phi$ generated for various desired directional profiles. The sectors where propagation is desired in each case is denoted by the dashed boxes.

In this initial test, a desired directional profile is obtained by first generating a library of solutions as follows. Source voltages and resistances are fixed as $\mathbf{v}_s = [1 \ j \ -1 \ -j]^T$ and $R_i = 37 \ \Omega$, respectively. A set of 100 pairs of $X_{\min}$ and $X_{\max}$ are generated with $X_{\min} \sim \mathcal{U}(-2\eta_0, 2\eta_0)$ and $X_{\max} \sim \mathcal{U}(X_{\min}, 2\eta_0)$. For each pair of $X_{\min}$ and $X_{\max}$, $10^4$ realizations of the loads are generated, where $X_i \sim \mathcal{U}(X_{\min}, X_{\max})$. This process results in a library of $10^6$ random solutions. For a desired directional profile, the best $10^3$ solutions from the library that produce propagation in the desired directions are kept and replayed to simulate fading with the desired directional bias.

Figure 6.9 illustrates that the library of solutions contains useful and diverse directional profiles. For each case sectors of desired receive power (dashed lines) are specified, and the best $10^3$ solutions that concentrate power to the sectors are averaged and plotted. This simple example illustrates that even without detailed optimization, useful directional properties of the wave field can be controlled.
Figure 6.10: Prototype ROTAC: (a) Complete chamber from side, (b) a single chamber panel hosting a $3 \times 3$ grid of dual polarized square patch antennas, (c) bottom view of the chamber with one receive dipole placed in the middle of the chamber above the ground plane.

6.4 ROTAC Prototype

After the initial analysis using simulations, a functional prototype ROTAC was built to experimentally confirm that the technique has the potential to provide flexible, low-cost OTA testing. Figure 6.10(a) depicts the initial prototype ROTAC, which is a cube formed from five panels that are 11 inches square. Each individual panel, an example of which is shown in Figure 6.10(b), hosts a $3 \times 3$ grid of dual-port, dual-polarization patch elements separated by $\lambda/2$, where $\lambda$ is the free space wavelength. The cube is placed on a ground
plane, as shown in Figure 6.10(c), which is perforated with a grid of small holes that allow cable access to a DUT within the chamber.

Figure 6.11 shows the individual dual-polarized patch antenna used on the ROTAC panels. The patch is fabricated on 60 mil Taconic RF substrate with a relative permittivity of 3.5. Quarter-wave transformers are used on each feeding transmission line to match the antenna input impedance to 50 Ω. Figure 6.11 also plots the reflection coefficients ($S_{11}$ and $S_{22}$) and cross coupling coefficient ($S_{12}$) of the fabricated antenna. The antenna is resonant near 2.53 GHz, with a 3 dB bandwidth of approximately 80 MHz. Cross-coupling between the two feed ports is less than $-30$ dB. The 18 ports on each of the five panels provide a total of 90 ports that can be connected either to RF sources (feed ports) or REs (reconfigurable ports). The RE used, which is similar to that reported in Section 2.1.3, enables a phase tuning range of 200° with a maximum power loss of 3 dB.

### 6.4.1 Fading Statistics Control

This section focuses on the control of fading statistics inside the ROTAC. In order to acquire initial measurements, the vertical polarization port of the center antenna on each of the four side panels is fed while the vertical polarization ports of the antennas at the four
corners of these side panels are loaded with REs as shown in Figure 6.10(a). Ports connected neither to sources nor to REs are left unterminated (open circuit). The field is measured using a monopole in the middle of the chamber above the ground plane, with the antenna connected to the receiver by a cable through the ground plane as shown in Figure 6.10(c).

Measurements were performed using an $8 \times 8$ multiple-input multiple-output channel sounder, where four sounder transmit ports were connected to the four ROTAC feed antennas and a single sounder receive port was connected to the monopole. The transmit RF signal consisted of four tones separated by 5 MHz and centered at 2.53 GHz. Because the sounder activates one transmit port at a time, it measures the transfer function $h_i[n]$ from the $i$th feed port to the receive port, where $n$ is the frequency bin index. Measurements of the four transfer functions, $1 \leq i \leq 4$, were captured for $10^6$ different combinations of random RE states (bias voltages). If the phase of the signal transmitted from the $i$th feed port is $\phi_i$, the realized channel response from the transmitter to the DUT at the $n$th frequency is computed as

$$h_R[n] = \sum_{i=1}^{N_F} h_i[n] e^{j \phi_i}, \quad (6.12)$$

where $N_F$ is the number of feed ports.
Based on the measured data and (6.12), a brute-force optimization is performed in which $10^4$ random phase combinations are realized. Next, the single phase combination is selected that produces channel responses whose magnitude and phase distributions are approximately Rayleigh and uniform, respectively. Figure 6.12 shows the realized field histograms along with the target amplitude and phase distributions. To achieve Rician fading, the phases are fixed at $\phi_i = 0$ and select a subset of the RE states that achieves the desired field amplitude distributions. Figure 6.13 shows the pdfs for these results for different target Rician distributions, where the Rician parameters are presented in (6.10). These results demonstrate that the ROTAC is capable of providing a range of different fading distributions.

### 6.4.2 Power Angular Spectrum Control

Next, the degree of control over the synthesized channel spatial characteristics is explored. The vertical polarization port of eight antennas on each panel are terminated with an RE whose bias voltage is provided by an FPGA-controlled D/A, for a total of 40 independently-controlled terminations. One antenna on each of the four side panels is then
fed by an independently-controlled source, with the feed antenna selected according to the following cases: **Case 1** – the vertical polarization port at each panel center; **Case 2** – the vertical polarization port at the panel lower right corner; **Case 3** – the horizontal polarization port at the panel lower right corner. Cases 2 and 3 are illustrated in Figure 6.14(a). Note that all remaining ports remain unterminated (open circuit). To measure the fields inside the chamber, an array of eight monopole antennas arranged in a circle of radius $\lambda/2$ is placed at the center of the chamber, with each monopole connected to the receiver using RF cables as shown in Figure 6.14(b).

Let $\hat{h}_{k\ell}[n]$ represent the transfer coefficient from the $\ell$th transmit to the $k$th receive antenna at the $n$th discrete frequency bin for one set of RE bias voltages (state). The signal at the $k$th receive antenna for this frequency is

$$h_k[n] = \sum_{\ell=1}^{N_{\ell}} a_{\ell} e^{j\theta_{\ell}} \hat{h}_{k\ell}[n], \quad (6.13)$$

where $a_{\ell} e^{j\theta_{\ell}}$ is the complex gain applied to the $\ell$th feed port signal and normalized such that $\sum_{\ell} a_{\ell} = 1$. The measurement record includes channels for $10^4$ different RE states.

For each RE state, a randomly-chosen set of $10^4$ complex gains $a_{\ell} e^{j\theta_{\ell}}$ is applied followed by the use of a Bartlett beamformer on the circular array to estimate the PAS.
each gain combination, the peak of the the PAS is computed and the sidelobe level (SLL) is defined as the peak power observed at angles beyond the array beamwidth, which is the angular range between PAS first nulls for an incident plane wave. For each gain combination, the SLL for each state as well as the SLL averaged over the 50 states that achieve the lowest SLL for that gain is stored.

Figures 6.15-6.17 plot the azimuth PAS for Cases 1-3. In each case, the solid and dashed lines depict the cases with the lowest and highest SLL, respectively. Furthermore, the top and bottom plots show SLL results for each state and averaged over the best 50 states, respectively. The results demonstrate that the SLL depends on the peak angle of arrival. Furthermore, while the SLL is higher for the averaged results, the difference is generally small, meaning that a single gain combination can be effective for multiple different RE states. The results for different feed ports show that the worst case SLL is improved by moving the feed location to the corner and transmitting on the horizontal polarization. The most important observation is that the ROTAC offers considerable control over the PAS.
Figure 6.16: Power incident on the DUT as a function of azimuth arrival angle for sources on the vertical polarization port at the lower right corner of each face (Case 2): (a) Single RE state; (b) Average over 50 RE states.

Figure 6.17: Power incident on the DUT as a function of azimuth arrival angle for sources on the horizontal polarization port at the lower right corner of each face (Case 3): (a) Single RE state; (b) Average over 50 RE states.
6.5 Chapter Summary

This work has explored the idea of an reconfigurable OTA chamber (ROTAC) whose purpose is to allow realistic OTA testing of wireless devices in a cost effective way. The initial study of an idealized two dimensional chamber suggests that such chambers may allow fading distribution, spatial correlation, frequency selectivity, and directional bias of different multipath channels to be simulated. To authenticate simulations, an experimental prototype ROTAC was also built. Results demonstrate that it can be used to generate Rayleigh and Rician fading statistics at the DUT by controlling the impedance of the REs along with the phase shift applied to the signal from each transmit port. Furthermore, the power angular spectrum at a DUT can be controlled by optimizing the feed locations and gains.
Chapter 7

Conclusion

This dissertation provides a comprehensive analysis of reconfigurable antennas for various communication applications using both simulations and direct measurements. Results have not only highlighted the performance advantage achieved using reconfigurable antennas, but also the practical limitations associated with their implementation.

7.1 Summary

In order to efficiently analyze RECAP structures, a hybrid approach was developed in Chapter 2 that uses full-wave simulations combined with the network analysis of the structure. Furthermore an efficient implementation of a genetic algorithm (GA) was done in order to optimize the structure for different applications and study the detailed dependence of performance on fixed complexity.

MIMO capacity improvements possible with a parasitic RECAP structure for different propagation scenarios were studied in detail in Chapter 3. Results were presented for both 2×2 and 4×4 MIMO systems in both wide band and narrow band optimization scenarios. Both noise-limited as well as interference-limited cases were considered with varying level of interference under three different realistic power constraints: average receive signal-to-noise ratio, effective isotropic radiated power (EIRP), and fixed total transmit power. For the practical EIRP constraint, results demonstrated that a compact 9×9 MIMO RECAP (1λ×1λ) provides 30%-50% capacity improvement for a single link. It was also found that RECAPs are even more beneficial in interference-limited and multiuser scenarios, where capacity was increased by 50% to 800% depending on the severity of the interference.

The results from simulations were verified by measurements in both LOS and non-LOS indoor environments. Measurements were performed by using a 5×5 parasitic RECAP
at the receiver for a bandwidth of 70 MHz centered at 2.55 GHz. For RECAP optimization a simple genetic algorithm was implemented and its performance was compared with that of a random search. Measurements confirm that a large increase in capacity is possible, particularly when there is high interference present. Also, this work highlighted the need of an efficient optimization algorithm, as it is not possible to find a good solution by a random search. Overall the results indicate that RECAPs are an attractive solution for future wireless systems employing aggressive spectral reuse.

Chapter 4 used simulations and experimental measurements to characterize the impact of reconfigurable antenna complexity on the performance of key establishment in different static propagation environments and in the presence of a multi-antenna eavesdropper. Analysis was performed using a $5 \times 5$ parasitic RECAP confined to an area of $1\lambda \times 1\lambda$. Since the artificial channel fluctuations created by RECAP structures are not necessarily Gaussian, a numerical procedure for computing available and secure key bits was developed that is applicable to channels with arbitrary fading.

Numerical examples of the parasitic RECAP with varying levels of complexity illustrated that reconfigurable antennas can significantly enhance the security, even when the eavesdropper antennas are adjacent to or surround one of the legitimate nodes. Furthermore a close agreement between simulations and measurements was found. The results demonstrated that increasing the number of reconfigurable parasitic elements notably increases the achieved performance, where two states per element maximize the number of bits available per RECAP state.

Chapter 5 explored optimal array beamforming for secure communication in the presence of a passive eavesdropper for both LOS and static multipath propagation environments. The problem was cast as a convex optimization problem, that was solved using semi-definite programming. For the LOS environment, a suboptimal pattern synthesis approach was also presented which makes use of Dolph-Chebyshev pattern synthesis. Numerical examples for a uniform linear array revealed that although in some cases the performance of the suboptimal approach was similar to that achieved with the optimal secure array synthesis, in other cases the performance of the suboptimal approach was dramatically inferior. Application of the method to a uniform circular array demonstrated the generality of the secure array synthesis.
approach. The analysis was further extended to a static multipath environment, where the average key rate performance was optimized. A comparison with the suboptimal approach based on the singular value decomposition of the propagation channel revealed a significant performance advantage.

Chapter 6 presented the idea of a reconfigurable over-the-air chamber (ROTAC) for over-the-air (OTA) testing in a compact and cost-effective way. The ROTAC makes use of reconfigurable antennas on the walls of a metal chamber to vary field statistics inside the chamber. Analysis was performed using an idealized two-dimensional chamber in simulations as well as by building an experimental ROTAC prototype. Results demonstrated that by proper control of the reconfigurable elements, realistic multipath propagation conditions can be generated on the device under test.

7.2 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:

- This work has analyzed a parasitic RECAP by considering the practical aspects like losses, phase tunability and finite bandwidth associated with reconfigurable elements (REs). In contrast to a parasitic array, RE losses can have a significant impact on the performance of a planar RECAP structure. Hence, design and analysis of an RE for a planar RECAP that can provide a significant phase tunability with lower loss is an interesting problem.

- Non-parasitic RECAP that employ variable interconnection and planar RECAP structures may provide a more practical solution and could be studied in depth. Also, a prototype of a planar RECAP could be built and used in propagation measurements to explore its performance advantage compared to the parasitic RECAP.

- A global optimization based method was developed to analyze MIMO capacity enhancement using parasitic RECAPs. It is of interest to study what radiation patterns
give high capacity and whether or not the pattern can be directly controlled to enhance capacity. Also, the development of more efficient direct optimization methods for RECAPs still requires significant work.

• For physical layer security, the states of the reconfigurable elements were changed randomly according to a uniform distribution to generate artificial fading in the propagation channel. An interesting open problem is to find the distribution that optimizes security, Perhaps this can be solved by extending the work on secure pattern synthesis, where ‘ideal’ reconfigurable antennas are replaced with more practical elements.

• The analysis presented in Chapter 5 for secure pattern synthesis assumed Gaussian signaling. However, the Gaussian assumption may not hold for a practical system employing other modulation schemes like BPSK or QPSK. Hence, a practical method needs to be developed that can use the developments in Chapter 5 for arbitrary modulation schemes. Also, the impact of estimation error for Bob’s location is ignored, which may have a significant impact based on the uncertainty in the estimate. Lastly, an analysis of complexity (in terms of number of elements) and computational time of semi-definite programming will highlight the practicality of the proposed method for a real-time implementation.

• A random search was used to analyze the performance of the ROTAC prototype in Chapter 6. More efficient real-time optimization algorithms for the ROTAC need to be developed. Also, direct measurement demonstrated the promise of the ROTAC concept, but hid the mechanisms governing ROTAC operation. A detailed and realistic simulation of the ROTAC prototype could be developed, which would reveal these mechanisms, providing a better understanding of the proposed ROTAC concept.
Bibliography


[44] MAXIM. (2004, July) Low-noise amplifier (LNA) matching techniques for optimizing noise figures. 23


