RICE UNIVERSITY

Augmenting Wireless Security Using Zero-Forcing Beamforming

by

Narendra Anand

A THESIS SUBMITTED
IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE

Master of Science

APPROVED, THESIS COMMITTEE:

Edward W. Knightly, Chair
Professor of Electrical and Computer Engineering and Computer Science

Ashutosh Sabharwal
Associate Professor of Electrical and Computer Engineering

Lin Zhong
Assistant Professor of Electrical and Computer Engineering

Houston, Texas

April, 2011

ABSTRACT

Augmenting Wireless Security Using Zero-Forcing Beamforming

by

Narendra Anand

We present the design and experimental evaluation of **S**imultaneous **TR**ansmissions with **O**rthogonally **B**linded **E**avesdroppers (STROBE). STROBE is a cross-layer approach that exploits the multi-stream capabilities of existing technologies such as 802.11n and the upcoming 802.11ac standard where multi-antenna APs construct simultaneous data streams using Zero-Forcing Beamforming (ZFBF). Instead of using this technique for simultaneous data stream generation, STROBE utilizes ZFBF by allowing an AP to use one stream to communicate with an intended user and the remaining streams to orthogonally “blind” (actively interfere) with any potential eavesdropper thereby preventing eavesdroppers from decoding nearby transmissions. Through extensive experimental evaluation, we show that STROBE reliably outperforms Omnidirectional, Single-User Beamforming (SUBF), and directional antenna based transmission methods by keeping the transmitted signal at the intended receiver and shielded from eavesdroppers. In an indoor Wireless LAN environment, STROBE consistently serves an intended user with a signal 15 dB stronger than an eavesdropper.

Acknowledgments

First and foremost I would like to thank my advisor, Dr. Edward Knightly, whose guidance has been invaluable in producing this thesis. Additionally, I would like to thank my thesis committee members for their comments, evaluation, and especially their time spent examining my work.

Additionally, I am grateful for the support of my fellow students in the Rice Networks Group for their help and advice through this entire process. Specifically, I would like to thank my collaborator, Ehsan Aryafar, with whom I created the foundational work for this thesis. I am also grateful for Oscar Bejarano's help in running experiments and keeping me on track with the entire thesis process.

Last but not least, I would would like to thank my parents, N.K. and Veena Anand, and my brother, Shankara Anand, for their unconditional love and guidance. The supportive atmosphere they provided is what has allowed me to succeed.

Contents

Abstract ii

Acknowledgments iii

List of Illustrations vi

1 Introduction 1

2 Background 5

2.1 Conventions 5

2.1.1 System Model 5

2.1.2 Notation 5

2.2 ZFBF Overview 6

2.3 Orthogonal Blinding 7

3 Experimental Setup 9

3.1 Experimental Platform 9

3.2 Experimental Methodology 11

3.2.1 Scheme Comparison 11

3.2.2 Measurement Procedure 13

4 Baseline WLAN Scenario 15

4.1 Experimental Setup 15

4.2 Experimental Results 16

4.3 STROBE vs. CE 19

5 Relative Eavesdropper Location 21

5.1 Eavesdropper Proximity 21
5.1.1 Experimental Setup 22
5.1.2 Experimental Results 22
5.2 Inline Eavesdropper 25
5.2.1 Experimental Setup 25
5.2.2 Experimental Results 26

6 Is Multi-Path Essential? 29
6.1 Experimental Setup 29
6.2 Experimental Results 30

7 The Nomadic Eavesdropper 32
7.1 Experimental Setup 32
7.1.1 Topology 32
7.1.2 Scheme Comparison 33
7.2 Experimental Results 34

8 Related Work 40
8.1 Wireless security exploiting CSI-based secret 40
8.2 Beamforming-based multiple AP cooperation 40
8.3 Information theoretic multi-antenna security 41

9 Conclusion 42

A Additional Plots 43
A.1 Additional Plots for Baseline WLAN Scenario (Chapter 4) 44
A.2 Additional Plots for Inline Eavesdropper Scenario (Chapter 5.2) 45
A.3 Additional Plots for Outdoor Scenario (Chapter 6) 46

Bibliography 47

Illustrations

3.1 STROBE Experimental Platform. 10

4.1 Basic WLAN Topology 15
4.2 SINR at IU and Overheard SINR at $E_{1\text{-}3}$ 16

5.1 Eavesdropper Proximity Topology 22
5.2 SINR of Transmission to IU at varying λs. 23
5.3 Inline Eavesdropper Topology 26
5.4 SINR at IU and $E_{1\text{-}3}$ for in line receivers 27

6.1 SINR at IU over $E_{1\text{-}3}$ in outdoor environment. 30

7.1 Classroom Environment 33
7.2 Beam pattern of 60^o directional antenna 34
7.3 Omnidirectional Transmission (dB) 35
7.4 SUBF Transmission SINR (dB) 36
7.5 Directional Antenna Transmission SINR (dB) 37
7.6 STROBE Transmission SINR (dB) 39

A.1 Baseline WLAN Scenario Topology 44
A.2 Complete results for Chapter 4 44
A.3 Inline Eavesdropper Topology 45

A.4 Complete results for Chapter 5.2 45
A.5 Outdoor Topology 46
A.6 Complete results for Chapter 6 46

Chapter 1

Introduction

The broadcast nature of wireless communication necessitates the development and use of robust security protocols in order to thwart eavesdroppers from intercepting transmissions directed toward an intended user. While encryption mitigates this vulnerability, it is not foolproof. Even industry standard encryption methods such as WEP or WPA have been compromised [1] and readily available software packages* exist that allow malicious users to easily defeat "secure" networks.

One method of enhancing the security of wireless transmissions is to prevent the eavesdropper from receiving or decoding the transmitted signal. A candidate solution is a directional transmission scheme that focuses signal energy toward an intended receiver using a directional antenna, switched-beam, or a single-target adaptive beamforming transmission method. However, in practice, such techniques that depend on the predictable behavior of transmitted beam patterns or that are agnostic to the entire eavesdropper environment fail to prevent eavesdropping as confirmed by our own experiments (see also [2]).

To address this problem, we present a new multi-antenna, 802.11-compatible protocol that adaptively sends a beam toward an intended user while "blinding" (actively interfering with) potential eavesdroppers, STROBE (**S**imultaneous **TR**ansmissions with **O**rthogonally **B**linded **E**avesdroppers). STROBE leverages the potential of a Zero-Forcing Beamforming (ZFBF) transmitter to send a signal toward an intended user while simultaneously trans-

*Aircrack-ng - Available at: `www.aircrack-ng.org` mitting "orthogonally blinding" streams (defined in Chapter 2.3) everywhere else.

ZFBF is a precoding method that allows a multi-antenna access point (AP) to create multiple simultaneous spatial streams [3]. Recent wireless standards such as 802.11n or the upcoming 802.11ac† employ physical layers that implement ZFBF to construct multiple parallel transmission streams to a single user (11n) or simultaneously to multiple users (11ac). Because such existing technologies already have the ability to create multiple parallel streams, STROBE can be easily implemented in these systems with minor AP modification and no client modification.

In particular, this thesis has the following main contributions: First, we design and implement STROBE in an FPGA-based radio platform that allows for over-the-air (OTA) characterization in a variety of different environments. Moreover, for comparative evaluation, we implement (*i*) Omnidirectional, (*ii*) Single-User Beamforming (SUBF), (*iii*) Directional Antenna, (*iv*) and Cooperating Eavesdropper (CE) schemes. CE is an unrealistic scheme in which eavesdroppers cooperate with the transmitter by providing their channel information allowing the transmitter to precisely blind the eavesdropper. While in practice eavesdroppers would never aid the transmitter, CE provides a "best case" benchmark for thwarting eavesdroppers via ZFBF.

Second, we construct a baseline WLAN scenario and evaluate STROBE's performance against the aforementioned baseline schemes. After confirming that STROBE better controls leaked signal energy as compared to Omnidirectional transmissions, we show that STROBE blinds eavesdroppers more than the single-target directional schemes (Single-User Beamforming and Directional Antenna). While the single-target schemes properly direct a beam toward an intended user, they do nothing to prevent that signal energy from reflecting throughout the environment allowing eavesdroppers to overhear the signal. In con-

†See `standards.ieee.org` and `mentor.ieee.org` for the 11n and 11ac standards, respectively.

trast, STROBE actively thwarts eavesdroppers by using simultaneous interference streams to blind them, thereby severely diminishing their ability to eavesdrop.

Additionally, we show that even when compared against the (unrealistic) Cooperating Eavesdropper, STROBE realizes a greater signal energy difference between the intended user and the eavesdropper. CE's ability to decrease the eavesdroppers' overheard signal energy comes at a cost: the intended user's served signal strength also decreases (to a greater extent) as a side effect of ZFBF's "zero-interference" condition. Thus, although CE can precisely blind eavesdroppers decreasing their overheard energy, the net result is STROBE serving a larger signal energy gain between the intended user and eavesdropper than CE.

Third, we show that, despite the use of beamforming in our system design, eavesdropper proximity or orientation relative to the intended user has a *negligible effect* on STROBE's ability to serve an intended user while blinding potential eavesdroppers. STROBE exploits multi-path effects in indoor environments by harnessing signal reflections to reach the intended user. In fact, at a relative eavesdropper proximity of a quarter wavelength (3.25 cm) from the intended user, STROBE still serves the intended user with a 10 db stronger signal than the eavesdropper. Moreover, even an eavesdropper that positions itself directly in front of or behind the intended user is thwarted.

Fourth, we explore STROBE's dependence on multi-path reflections by performing experiments in an open, outdoor environment. Because the environment contains no physical obstacles to cause reflections, STROBE must use the direct, line-of-sight (LOS) path to serve the intended user. We find a marked detrimental effect on STROBE's efficacy as eavesdroppers can easily overhear signal energy at close by locations, i.e., STROBE requires a multi-path rich, WLAN type environment to achieve its goals.

Finally, we consider a nomadic eavesdropper that traverses an environment attempting to find a location to successfully eavesdrop. We show that even if the eavesdropper exhaustively traverses the room, it is still thwarted by STROBE. In contrast, eavesdroppers can very easily find suitable eavesdropping locations for the other transmission schemes considered, including the use of a directional antenna.

The rest of this thesis is organized as follows: Chapter 2 gives background on ZFBF and the orthogonal blinding method employed by STROBE. Chapter 3 describes our experimental platform and methodology for the evaluation of STROBE. Chapter 4 is a baseline evaluation of STROBE. Chapter 5 explores the effects of eavesdropper proximity and location with relation to the intended user and transmitter. Chapter 6 evaluates STROBE in an open, outdoor environment with fewer multi-path effects. Chapter 7 evaluates the robustness of STROBE against a nomadic eavesdropper. Chapter 8 describes related work and Chapter 9 concludes the thesis.

Chapter 2

Background

In this chapter, we first describe the mechanics of Zero-Forcing Beamforming, the core technique behind STROBE. We then detail the mechanism of "Orthogonal Blinding," the key component of STROBE that enhances wireless security.

2.1 Conventions

2.1.1 System Model

STROBE is a downlink transmission technique. We consider a system consisting of a multi-antenna AP and several single antenna users. This system is typical for current WLAN networks because APs have the ability to support complex, multi-antenna technologies whereas users, such as smartphones, are limited by constraints such as size, computational ability, and power consumption to single antenna methods.

Of the single-antenna users, we call the user to which the transmission is intended the "Intended User" (IU). We call the unintended users who are attempting to overhear the transmission "Eavesdroppers" (E).

2.1.2 Notation

The following section describes the notation used. Further definition and description will follow in the appropriate chapters. N refers to the number of transmit antennas at the AP. M refers to the number of concurrently served, single-antenna users.

The row vector h_m is a $1 \times N$ channel state vector for user m. Each element of h corresponds to the complex exponential gain of one transmit antenna to the user. The matrix $H = [h_1; h_2; \ldots; h_M]$ is the $M \times N$ channel matrix constructed using each users h as its rows.

The column vector w_m is an $N \times 1$ beamsteering weight vector for user m. Each element of w corresponds to the complex exponential gain used by each transmit antenna during transmission. The matrix $W = [w_1 \, w_2 \, \ldots \, w_m]$ is the $N \times M$ steering weight matrix consisting of each users w as its columns.

2.2 ZFBF Overview

ZFBF is a precoding transmission method that allows an AP to construct multiple, concurrent spatial streams that can transmit data to multiple users in parallel. The basic principle is to first take each user's view of the channel, h, and construct a corresponding w for each h. Each user's data stream is then multiplied its corresponding w, summed together and transmitted over the AP's antenna array. Careful selection of w allows for the construction of concurrent spatial streams and parallel transmission of multiple users' data.

The optimal method of constructing W from H to concurrently serve multiple users is known as Dirty Paper Coding (DPC) [4, 5]; however, in practice this method is difficult to implement due to its complexity. Instead of DPC, ZFBF is a W construction method that is a simpler, sub-optimal, approach that is practical to implement [3].

ZFBF selects weights that cause zero inter-user interference (the effect of one beamformed stream on another is "forced" to zero). The authors of [6] have shown that the optimal selection of W to satisfy this zero-interference condition is the pseudo-inverse of

H as shown in Eq. (2.1)*.

$$W = H^{\dagger} = H^{*}(HH^{*})^{-1} \tag{2.1}$$

The use of the pseudo-inverse is how the zero-interference condition is achieved: if $W = H^{\dagger}$ then $h_i w_j = 0$ for $i \neq j$. Additionally, note that the matrix multiplication shown in Eq. (2.1) places a limit on the maximum number of concurrent users (or spatial streams). The number of concurrent streams must be less than or equal to the number of transmit antennas (i.e., $M \leq N$).

In our implementation, we feed back channel state information (CSI), an h vector, via the RTS/CTS in compliance with 802.11ac and 11n.

2.3 Orthogonal Blinding

The key mechanism of STROBE is the concept of "orthogonal blinding" that occurs in parallel with transmission to the intended user.

"Blinding" is the method of actively concealing the intended user's signal by overwhelming any potential eavesdroppers with garbage transmissions. These blinding streams are transmitted concurrently with the transmitter using extra available streams provided by a ZFBF enabled AP. In order to ensure that these blinding streams cause the least possible decrease of the intended user's transmitted signal, these streams are constructed orthogonally to stream of the intended user.

The streams used for the intended user and for blinding correspond to different w vectors, which come from the pseudo-inverse of H. Thus, to construct orthogonal blinding streams, we construct orthogonal h vectors to the intended user's h and then perform ZFBF on the constructed H matrix.

---

*v^{*} refers to the complex conjugate transpose of vector v.

To construct these orthogonal h vectors, we use the Gram-Schmidt process [7]. First, we take the intended user's CSI and set it as h_1. We then pad h_1 with a truncated $(M\text{-}1)\times N$ identity matrix to build a preliminary H matrix. Finally, we construct the CSI matrix with orthogonal rows, $\widehat{H}$ by using the Gram-Schmidt process shown in Eq. (2.2) on the preliminary H.

$$\begin{aligned} \widehat{h_1} &= h_1 \\ \widehat{h_k} &= h_k - \sum_{j=1}^{k-1} \frac{\langle h_k, \widehat{h_j} \rangle}{\|\widehat{h_j}\|^2} \widehat{h_j}, \quad 2 \leq k \leq M \quad \text{where} \\ \langle h_k, \widehat{h_j} \rangle &\equiv (\widehat{h_j}^*)(h_k) \end{aligned} \tag{2.2}$$

The resulting $\widehat{H}$ is unitary. Thus the calculation of its pseudo-inverse is trivial: $W = \widehat{H}^\dagger = \widehat{H}^*$.

Additionally, the Gram-Schmidt process is simple to integrate into an 802.11n/11ac AP. Both of these technologies are capable of ZFBF, an algorithm that requires the computation of a matrix pseudo-inverse. The first step of this calculation is implemented in hardware using QR decomposition [8], an operation that decomposes a matrix into an upper triangular (R) and a unitary matrix (Q). The Gram-Schmidt process can also be computed using the QR method. Thus, the silicon in the physical layer of 802.11n or 802.11ac already exists to perform this algorithm; the only change necessary is how the input matrix is loaded.

Chapter 3

Experimental Setup

In this chapter we present our implementation of STROBE and our experimental evaluation methodology.

3.1 Experimental Platform

We conduct our experiments using WARPLab*, a framework that integrates the versatility of MATLAB with the capabilities of an FPGA based software defined radio platform (WARP). WARPLab gives the ability to rapidly prototype physical layer algorithms in MATLAB while using the WARP nodes to perform over-the-air (OTA) characterizations of those algorithms.

The WARPLab flow consists of two main parts: MATLAB on the host PC and the WARP node. All baseband processing for a physical (PHY) layer algorithm occurs in MATLAB on a host PC while the OTA transmission and reception of the processed signal is handled by the WARP nodes.

A single host PC can be connected to up to 16 WARP nodes through an Ethernet switch. MATLAB on the host PC processes a given bit stream using the prescribed PHY layer algorithm and then downloads the processed I/Q samples through the switch to the transmitting WARP node. The host PC then sends a sequence of control signals that enable connected nodes and trigger the transmission and reception of the OTA signal.

---

*Rice University WARP Project - Available at `warp.rice.edu`

Each node contains four large sample buffers† connected to four 2.4 GHz radio cards. These buffers either accept data over Ethernet for transmission or through the radio card for reception. Receiving nodes can then upload the received samples through the switch for decoding along with received Received Signal Strength (RSS) values in dBm.

For the evaluation of STROBE, the multi-antenna transmitter must sound the channel in order to obtain the relevant CSI (h vector) for the necessary receivers. This channel sounding followed by the transmission is accomplished by implementing the CSI feedback channel through the switch, H and W calculation in MATLAB, and beamforming weight multiplication in the WARP node. For the characterization of STROBE, we use the ZFBF experimental framework we built on top of WARPLab in [9].

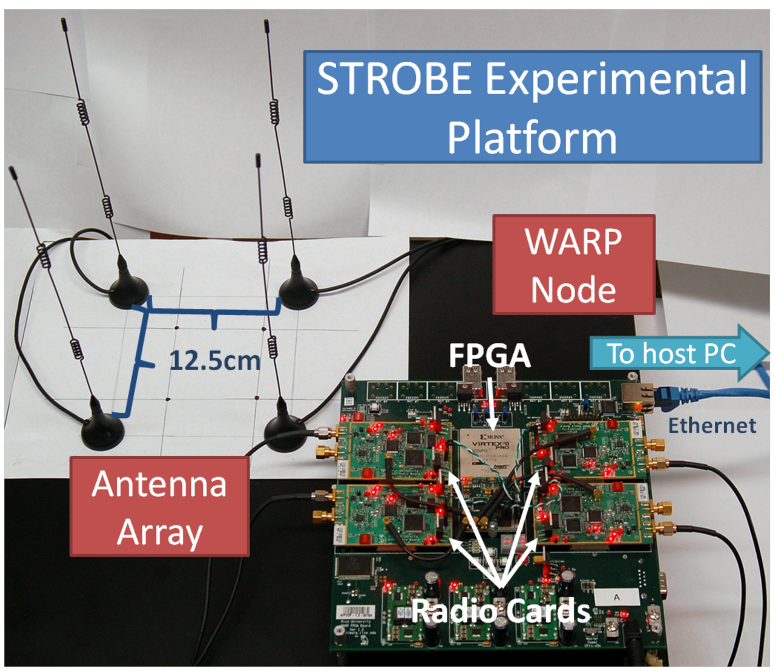


Figure 3.1 : STROBE Experimental Platform.

We employ one transmit antenna for the receivers and all four for the transmitter (thus

†Each buffer can hold 2^{16} I and Q samples

$N = 4$ for our characterization). Our antenna array is circular with the antennas spaced one wavelength apart for 2.4 GHz ($\lambda = 12.5$ cm). An example of the transmitting node is shown in Fig. 3.1.

3.2 Experimental Methodology

In this section we describe how we conduct our experiments. Specifically, we focus on schemes used for baseline comparison and the measurement procedure.

3.2.1 Scheme Comparison

In this section we detail the different baseline transmission schemes compared against STROBE.

Omnidirectional Transmission

The initial baseline scheme we consider is the Omnidirectional transmission. Because this is the most commonly used wireless transmission method, it is important to observe where the intended user's transmitted energy is sent. This method reflects the status quo conditions under which existing wireless transmissions occur.

Single-User Beamforming

Single-User Beamforming (SUBF) is the fundamental, adaptive directional technique. It is a transmission method that employs an antenna array to steer a beam toward an intended user based on that user's CSI (h vector). SUBF can be considered a subset of ZFBF in that the number of "concurrent" users is one. Because there is only one intended user, the zero-interference condition does not exist (since there is no other stream to interfere with) so the selection of weights results in the maximum possible received signal energy at the intended user (for a ZFBF type scheme).

Calculation of the SUBF steering weight is trivial since the H matrix consists of only vector. Plugging in a single row H matrix (the case where $M = 1$) results in: $(H_{1\times N})^{\dagger} = (H_{1\times N})^{*} = W_{N\times 1}$. Thus, the intended user's steering weight for SUBF is its complex conjugate transpose, which is equivalent to the intended user's weight for STROBE.

However, in order to ensure a fair comparison, the power allocation to the steering weights of SUBF and STROBE differs, which contributes to a difference in intended user's received signal energy. This difference, which will be further discussed in Chapter 3.2.2, results in 4x greater transmit power allocated to the intended user's steering weight when using SUBF compared to STROBE.

Thus, SUBF is a necessary baseline because it is the existing scheme that maximizes the signal energy at the intended user.

Cooperating Eavesdropper

Finally, we compare STROBE against the unfeasible baseline, the Cooperating Eavesdropper (CE). This scheme explores the unrealistic scenario where the eavesdropper actively aids in their blinding by providing the transmitter with their channel estimates. While this scenario would never occur in practice, it is essentially an upper limit of a ZFBF-based scheme's potential performance.

With knowledge of eavesdropper channel information (the eavesdroppers' h vectors), the transmitter has access to the "true" H matrix. This allows the transmitter to precisely blind eavesdroppers because of the zero-interference condition. Specifically, this condition signifies that the intended user's signal will result in zero overheard signal (zero interference) at the cooperating eavesdropper's locations. Thus, even if the transmitter does not use the additional streams for blinding signals, the eavesdroppers will still be unable to overhear the intended user's signal. We showed in [9] that a four antenna transmitter serving four concurrent users causes less than 1 dB of inter-user interference.

Although this implies that CE can construct a beam to the intended user that cannot be overheard by the (cooperating) eavesdroppers, we still use the remaining three streams for blinding to ensure a fair comparison.

Thus, CE is a necessary baseline because it minimizes the signal energy overheard by the eavesdroppers.

3.2.2 Measurement Procedure

In this section we describe how and what measurements are taken to characterize STROBE.

Performance Metric

Our performance metric for the evaluation of STROBE is Signal to Noise Ratio (SNR) or Signal to Interference plus Noise Ratio (SINR) expressed in dB. As mentioned in Section 3.1, the WARPLab platform allows us to measure RSS in terms of dBm; however, the inherent differences in RSS measurements between radio transceivers result in dBm readings that cannot be fairly compared.

To overcome this, we calculate SNR and SINR values from the difference between two back-to-back measurements performed at the intended user and all eavesdroppers. For example, for Omnidirectional and SUBF transmissions, we first measure the RSS with the transmission (the signal) and then measure the RSS again without a transmission (the noise). The difference between the two is the SNR. The multi-stream methods are measured similarly. For STROBE and CE, we first transmit all four data streams and measure the RSS (the signal). Then we set the intended user's steering weight to zeros and redo the measurement. The second measurement at the intended user and the eavesdropper represents the signal energy from the blinding streams in addition to the noise floor (the interference plus noise). The difference between these two measurements is the SINR. For the remainder of this thesis, we refer to this received signal energy as the SINR.

Power Allocation

To ensure a fair comparison, we set the net transmit power for all schemes equivalent regardless of the number of antennas or streams used. Omnidirectional (one antenna) and SUBF (four antennas) transmissions use equivalent power to serve the intended user. STROBE and CE generate N transmit streams so the intended user's stream is allocated $1/N^{\text{th}}$ the overall transmit power. This net transmit power control is implemented by the appropriate normalization of the W matrix.

Data Collection

For each data point in our results, we averaged 30 OTA transmission measurements. All data points presented standard deviations of 1 dB or less. All experiments were conducted in an interference-free channel.[‡]

[‡]OTA experiments were conducted using the 802.11-2.4 GHz channel 14, which consumer WiFi devices are not allowed to use in the USA.

Chapter 4

Baseline WLAN Scenario

In this chapter we evaluate STROBE using a baseline WLAN topology. Namely, we explore STROBE's ability to exploit a rich, multi-path fading (indoor) environment in order to not only serve an intended user but also to blind the intended signal to the eavesdroppers.

4.1 Experimental Setup

To realize a typical WLAN scenario, our initial experiment is comprised of a conference room topology. In particular, as depicted in Fig. 4.1, four receivers are placed along the far edge of a large table. The room itself is in the shape of a long rectangle filled with metal chairs and surrounded by metal blinds making it a multi-path rich environment. The receivers are separated by 1.25 m and the AP is separated from the group of users by a 5 m distance. We set one receiver to be the intended user (labeled IU) and the other three

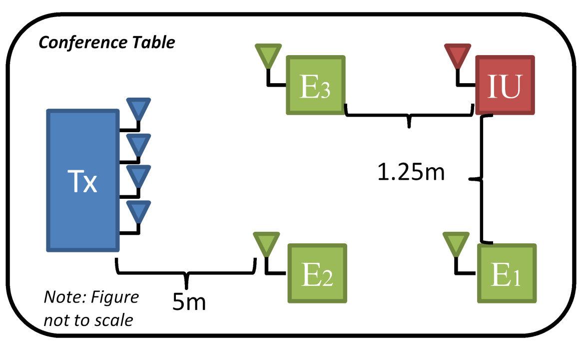


Figure 4.1 : Basic WLAN Topology

receivers to be eavesdroppers (labeled $E_{1\text{-}3}$). In addition to evaluating the performance of STROBE, we also perform experiments with Omnidirectional, SUBF, and CE as baselines for comparison. Additionally, we perform the experiments with the intended user in the other three eavesdropper locations and obtained similar results (included in Appendix A.1).

4.2 Experimental Results

Fig. 4.2 shows the received SINR at each of the four receivers when data was transmitted toward the intended user. In this graph, the SINR at the intended user is indicative of the

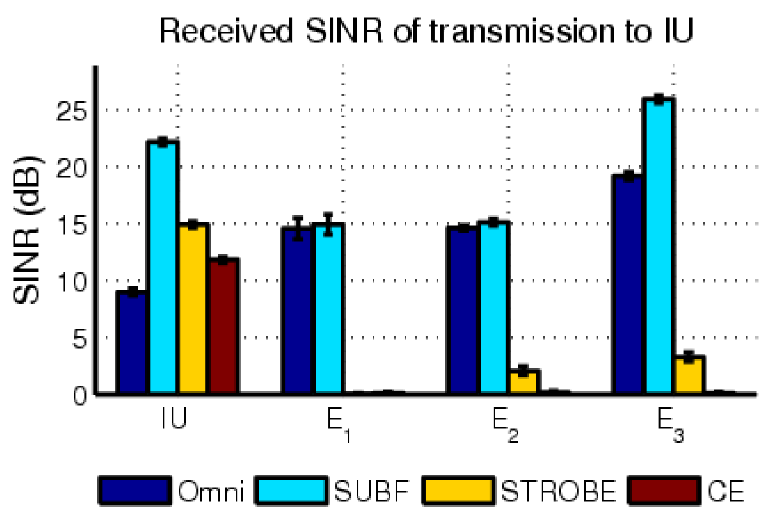


Figure 4.2 : SINR at IU and Overheard SINR at $E_{1\text{-}3}$

intended received signal energy while the SINR at $E_{1\text{-}3}$ shows the power of the intended user's signal the eavesdroppers overheard.

Omnidirectional Transmission

The use of an Omnidirectional transmission (depicted in dark blue), yields an even greater SINR at the eavesdropper locations than the intended user for this topology. This highlights the high vulnerability of existing systems to transmissions overheard by eavesdroppers, a critical security issue when encryption protocols are unused or defeated.

Single-User Beamforming

Compared to an Omnidirectional transmission, SUBF (light blue) better directs a signal's energy toward the intended user. However, there is nonetheless a large amount of energy available at other locations for the eavesdroppers to overhear and intercept. Indeed, in this topology, the energy at the eavesdropper locations is equivalent to or greater than the Omnidirectional case. This behavior is not a flaw; rather, it is a consequence of the design. SUBF's only goal is to maximize the SINR at the intended user, but does so completely agnostic to other locations. For this reason, the signal transmitted by SUBF does not remain solely at the intended user but instead spills over to various other areas causing the scheme to be as vulnerable as an Omnidirectional transmission. This specific consequence of SUBF is further highlighted by the transmit power allocation method. As mentioned in Chapter 3.2.2, in order to ensure a fair comparison, the net transmit power for all schemes is equivalent regardless of the number of antennas used. Thus, the eavesdroppers overheard the intended user's signal just as well (if not better as at E_3) as the Omnidirectional transmission even with equivalent transmit powers and SUBF's inherently directional nature.

STROBE

Unlike Omnidirectional and SUBF transmissions, STROBE (yellow) blinds the eavesdroppers and mitigates the possibility of overhearing the signal to the intended user. As described in Chapter 2.3, STROBE blinds eavesdroppers by creating multiple, simultaneous, transmission streams, using one to transmit to the intended user and using the others to interfere with any other user's attempt to overhear the intended signal. Actively blinding potential eavesdropper locations results in a maximum 3 dB eavesdropper SINR (at E_3) for this topology. Although the intended user's steering weight is identical to SUBF (as discussed in Chapter 3.2.1), the use of additional, orthogonal, blinding weights allows STROBE to diminish the SINR at the eavesdroppers while still maximizing the SINR at the intended user. Again, this effect is further emphasized by the power allocation scheme; not only does the net transmit power remain fixed regardless of the number of antennas used but also regardless of the number of spatial streams employed. The use of four streams in our evaluation results in a 4x decrease in the transmit power allocated to the intended user's stream. However, for the price of this resulting 6 dB SINR decrease at the intended user, STROBE causes a *15-22 dB decrease* in SINR at the eavesdroppers.

To estimate how STROBE's measured energy levels would perform in a commodity device, we employ the theoretical Gaussian model for BPSK (for a conservative estimate) and compute approximate bit error rates (BERs) for the observed SINRs. The intended user's served SINR of 14 dB corresponds to a BER of approximately 5.4×10^{-5} whereas the maximum eavesdropper SINR of 4 dB corresponds to an approximate BER of 2.3×10^{-2}. This conservative estimate shows that STROBE serves an intended user with a BER three orders of magnitude lower than the eavesdropper, thus significantly decreasing the likelihood of an eavesdropper decoding an intended user's transmission.

Cooperating Eavesdropper

As a baseline for evaluating STROBE, we examine the realistically unfeasible scenario of the cooperating eavesdropper (red) where the eavesdroppers provide their channel information to the transmitter to aid in their blinding. The extra information provided to the CE scheme allows it to precisely blind potential eavesdroppers. This additional accuracy manifests as the eavesdroppers' SINRs equaling approximately 0 dB, but the only benefit over STROBE is a maximum 3 dB decrease in the overheard signal at E_3. However, this decrease comes at the cost of a 3 dB decrease in the intended user's SINR so the relative gain of CE at the intended user over the eavesdropper is equivalent at E_3 and less at $E_{1\text{-}2}$ than STROBE. This effect is further explored in Chapter 4.3.

4.3 STROBE vs. CE

For our comparisons between STROBE and CE, we purposely set the number of overall receivers to four, a decision that results in the "best case" results for CE. This decision and the observed results also highlight a subtle difference in the two schemes' mechanisms.

The precision of any ZFBF based transmission scheme is dependent on the number of transmit antennas. The number of spatial streams that may be constructed is equal to the size of the transmit antenna array. Although both CE and STROBE are able to create an equivalent number of streams, STROBE creates its blinding streams solely based on the channel state of the intended user whereas CE considers all users. The consequence of this characteristic is that CE is only able to precisely blind as many eavesdroppers as one less than the number of transmit antennas. If we were to perform this experiment with additional eavesdroppers, our four antenna transmitter (when employing CE) would only be able precisely blind three of the eavesdroppers; the remaining eavesdroppers would overhear the signal with an SINR comparable to STROBE.

Both STROBE and CE construct multiple blinding streams using ZFBF. However, the manner in which STROBE constructs the channel matrix around the intended user's channel state (h vector) guarantees a maximum served SINR to the intended user (using some weight w) because the constructed matrix is unitary and the resulting intended user's $w = h^*$ (as detailed in Chapter 2.3). This resulting w vector is equivalent to the SUBF weight and is the best that ZFBF can provide. The resulting W matrix still satisfies ZFBF's zero interference condition. However, CE 's construction of the H matrix is based on all users' channel estimates. For CE to satisfy the zero interference condition, the intended user's weight loses magnitude.

Thus, the signal energy at an eavesdropper from STROBE and CE (after the maximal number of eavesdroppers) is equivalent; however, STROBE will always be able to serve the intended user with a higher SINR. We verify this in Fig. 4.2 where CE results in less overheard signal energy but also less served energy to the intended user. Although CE is completely unfeasible in a real system and uses ZFBF in its intended manner for precise blinding, STROBE will still always provide a higher SINR to the intended user and the benefits of this scheme will still function regardless of the number of eavesdroppers.

Chapter 5

Relative Eavesdropper Location

In this chapter we evaluate the effect of eavesdropper position relative to the transmitter and the intended user. This analysis is done in two parts. In Chapter 5.1, we examine the effect of eavesdropper proximity to the intended user. Then, in Chapter 5.2, we examine the effect of eavesdroppers in line with the intended user and transmitter. We conduct both experiments in the same setting as the experiment in Chapter 4.

5.1 Eavesdropper Proximity

The purpose of this experiment is to quantify the effect of eavesdropper distance relative to the intended user. Because this is a spatially based transmission method, we will examine how close the eavesdroppers can be to the intended user before the efficacy of STROBE begins to diminish. Specifically, the motivation for this experiment is from the observed correlation in Chapter 4 between the proximity of the eavesdroppers to the intended user and the performance of beamforming based schemes. The results for that experiment (Fig. 4.2) show an increased overheard SINR at E_3 for SUBF and STROBE (although only a slight increase for the latter).

In [9], we showed that separation distance between receivers has a negligible effect on the served SINR when using a ZFBF based transmission scheme (such as CE). While we expect CE to cause low inter-user interference because the AP has knowledge of all users' channels, the efficacy of STROBE is unclear in this situation. We do not expect STROBE to match the intra-user interference reduction performance of CE (because STROBE only has the intended user's channel information); however, we do expect the blinding streams to compensate for this by overwhelming the overheard signal to the point where the overheard SINR is similarly minimal.

5.1.1 Experimental Setup

We evaluate the effect of eavesdropper proximity on STROBE by placing the intended user at a fixed, 5 m distance from the transmitter with a direct line-of-sight (LOS) path and surrounding it by a circle of three eavesdroppers as shown in Fig. 5.1. For each measurement, we vary the radius of this circle (d) and express the distance in terms of λ. We place the eavesdroppers from a distance of 10λ (the separation distance for Chapter 4's experiment) to $\lambda/4$ (the closest we can physically place the antennas together).

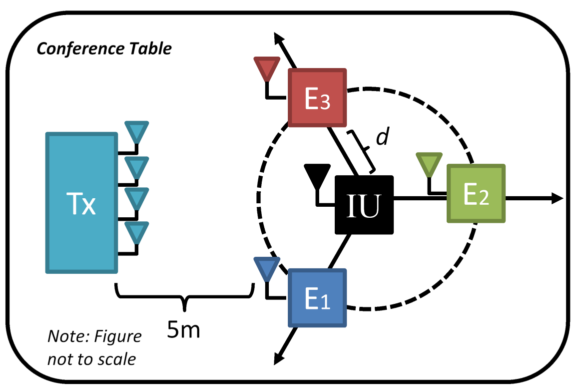


Figure 5.1 : Eavesdropper Proximity Topology

5.1.2 Experimental Results

Fig. 5.2 shows the SINR at the intended user (black) and the three eavesdroppers (blue, green, and red respectively) at varying proximity distances.

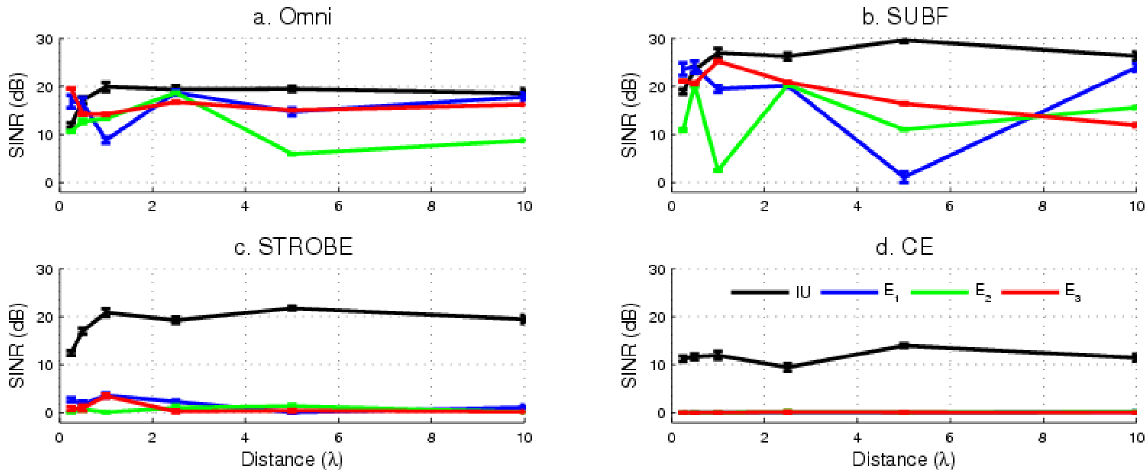


Figure 5.2 : SINR of Transmission to IU at varying λs.

Omnidirectional Transmission

As similarly observed in Chapter 4, the eavesdroppers' overheard signal from the Omnidirectional transmission is relatively high as seen in Fig. 5.2a. The only scenario in which the Omnidirectional scheme results in overheard signal energies substantially lower than the intended user is a combination of increased transmitter to eavesdropper distance and an obstructed eavesdropper LOS (E_2 at $d \geq 5\lambda$). The unpredictable behavior for all distances for this transmission scheme highlights the effect of multi-path signal propagation in indoor environments. The intended user's position at the center of the table and conference room (farthest away from walls, chairs, and other reflectors) allowed its SINR to remain consistent.

Single-User Beamforming

Similarly, indoor multi-path effects are observed in the received SINR's of the eavesdroppers when transmitting with SUBF (Fig. 5.2b). In fact, because the transmitted energy is being actively focused, a greater variation of overheard SINR occurs at the eavesdroppers. For example, the position difference from $\lambda/2$ to $\lambda/4$ at E_2 results in an 18 dB drop in signal strength even though the relative distance to the transmitter remains similar. The combination of a focused transmission and apparent randomness of multi-path occasionally helps SUBF reduce the overheard signal energy (such as at E_1 for $d = 5\lambda$), but this accidental nulling is in no way reliable.

STROBE

Regardless of eavesdropper proximity, the ability of STROBE to consistently blind the eavesdroppers while still serving the intended user regardless of proximity distance is shown in Fig. 5.2c. The multi-path effects on the transmitted signal that cause the high variation in eavesdropper performance when using Omnidirectional or SUBF schemes have the opposite effect on STROBE. The overheard SINR range of a blinded eavesdropper from STROBE shown in Fig. 5.2c is 5 dB whereas Omnidirectional and SUBF transmission's ranges are 14 and 24 dB respectively. The ability of the multi-stream methods to separate receivers regardless of their relative distances observed in Fig. 5.2c and d matches the results shown in [9].

The only separation distance with an appreciable loss of SINR to the intended user for STROBE is $\lambda/4$ (12 dB); at all other proximity distances, the intended user is consistently sent a 20 dB signal. However, considering that this proximity distance is physically the closest our test antennas could be placed (the antenna bases were adjacent), the 12 dB SINR at the intended user and 10 dB SINR gain over the eavesdropper shows promise for STROBE. In fact, this result at a proximity distance of 3.125 cm ($\lambda/4$) implies that STROBE could potentially protect against covert eavesdropping devices secretly attached to the *intended user device itself*.

Cooperating Eavesdropper

Differences in eavesdropper blinding abilities between STROBE and the impossible baseline CE confirm the findings of Chapter 4. As detailed in Chapter 4.3, full knowledge of the eavesdroppers' channels allows for the complete blinding of the eavesdroppers as shown in Fig. 5.2 (the eavesdroppers lines are on top of one another). However, this precision comes at the cost of an SINR decrease for the intended user of 10 dB below STROBE. Additionally, CE's ability to serve the intended user remains constant even at $\lambda/4$. However, at that proximity distance, STROBE is still serves the intended user with a stronger signal.

5.2 Inline Eavesdropper

In this section we evaluate the effect of eavesdroppers inline with the intended user. The goal is to quantify the effects of eavesdroppers blocking and along the LOS path from the transmitter to the intended user.

We expect the multi-path effects of the indoor environment to aid STROBE in blinding the eavesdroppers and serving the intended user as hypothesized in Chapter 5.1. However, the major component of any transmitted signal is the LOS path so the potential for a beamforming based scheme to select this path and inadvertently serve an eavesdropper on that path exists.

5.2.1 Experimental Setup

To evaluate the effect of eavesdroppers inline with the intended user, we set the transmitter a fixed distance (3 m) away from a line of receivers as shown in Fig. 5.3. We perform four iterations of the experiments setting each receiving node as the intended user and the other three as eavesdroppers. Although the four iterations produce similar results, the topology shown where the intended user is second from the back results in the worst case performance for STROBE. (The remaining results are included in Appendix A.2.) We present and analyze the results obtained from this topology.

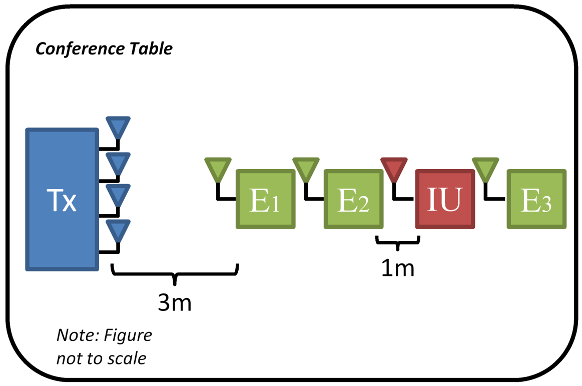


Figure 5.3 : Inline Eavesdropper Topology

5.2.2 Experimental Results

Fig. 5.4 shows the received SINRs at the intended user and the eavesdropper. Recall from Fig. 5.3 that IU is located between E_2 and E_3.

Omnidirectional Transmission

As observed in previous experiments, the received SINR of the Omnidirectional transmission at the three eavesdropper positions is similar to the intended user. However, the received SINR at E_1 is the lowest even though it is located closest to the transmitter with no other antenna blocking its LOS. This and the similar deficits in E_2's SINR offer further examples of multi-path effects in an indoor environment.

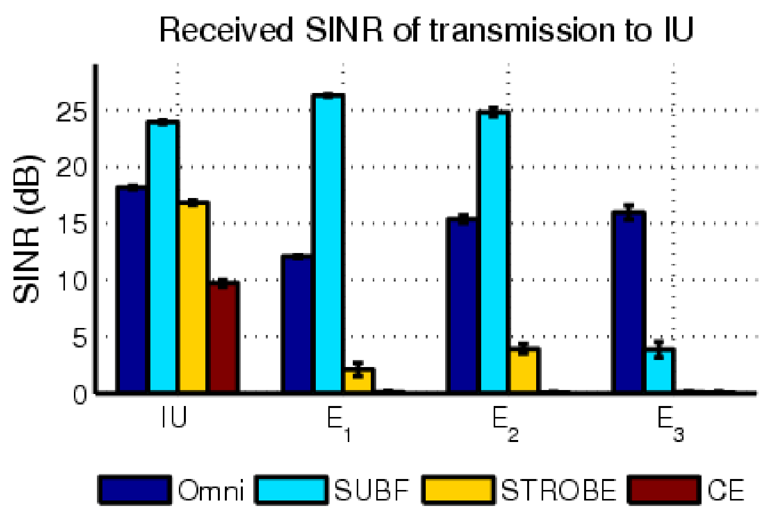


Figure 5.4 : SINR at IU and $E_{1\text{-}3}$ for in line receivers

Single-User Beamforming

The received SINR from the SUBF transmission at $E_{1\text{-}2}$ surpasses the SINR at the intended user. Unlike the Omnidirectional transmission, SUBF focuses energy toward the intended user and takes the direct LOS path. This results in the highest SINR at E_1 followed by E_2 and then by the intended user (the exact order in which they are located). This result shows that the best way to intercept a signal transmitted using SUBF is to simply eavesdrop in the LOS path of the intended user.

STROBE

STROBE serves the intended user with an SINR of 17 dB while allowing an eavesdropper to overhear, at most, an SINR of 4 dB (at E_2). Unlike SUBF, STROBE handles the in line, LOS blocking eavesdroppers effectively by blinding them even given their positions. As previously stated, this intended user location did result in the worst case results for STROBE but even so, STROBE leverages multi-path effects and provides the intended user with a 13 dB gain over the eavesdropper.

Cooperating Eavesdropper

As seen in previous topologies, CE precisely blinds the eavesdroppers allowing none of the intended user's signal energy to be overheard while serving the intended user with a 10 dB signal as a result. Although the relative separation distances between the nodes were similar between this experiment and Chapter 4, the SINR difference at the intended user between STROBE and CE is almost twice as much (3 dB to 6 dB). The increased difficulty in compensating for in line eavesdroppers blocking LOS paths causes a greater hit in the intended user's SINR when CE attempts to precisely blind the eavesdroppers. Even if using this unrealistic scheme, the served SINR and relative gain over the eavesdropper SINR is still below that of STROBE.

Chapter 6

Is Multi-Path Essential?

STROBE's efficacy relies on multi-path effects in an indoor environment as described in Chapter 5. However, in outdoor environments (with significantly fewer multi-path effects), the authors of [10] claim that receiver separation distances of 70 m are required to serve users in parallel with ZFBF schemes. Multi-path is the hypothesized explanation for the ability of STROBE (along with CE) to function successfully indoors regardless of eavesdropper proximity, relative position, or location. If this assumption can be validated, we can expose another benefit of STROBE. Increased multi-path effects are caused by "busier" environments (i.e. more physical obstacles such as furniture). The "busier" an environment is, the larger the possibility for there to be eavesdroppers attempting to intercept an IU's signal. Thus, if STROBE benefits from multi-path, environments that support more eavesdroppers may actually help STROBE further secure a wireless transmission.

6.1 Experimental Setup

In order to evaluate the effects of decreased multi-path on STROBE, we redo the experiment described in Chapter 4 in an open space outdoors at considerable distance from buildings and other obstacles. The topology and relative distances between the nodes are identical to Fig. 4.1. Again, we perform four experiments setting each receiver as the intended user and the other three as eavesdroppers. All experiments produced similar results and hence for a direct comparison, we use the intended user location shown in Fig. 4.1

whose indoor results are displayed in Fig. 4.2 (The remaining results are included in Appendix A.3).

6.2 Experimental Results

Fig. 6.1 shows the resulting SINRs when the transmitter sends a signal to the intended user in an open outdoor environment. The performance of Omnidirectional and SUBF transmissions are similar to the results from other indoor topologies.

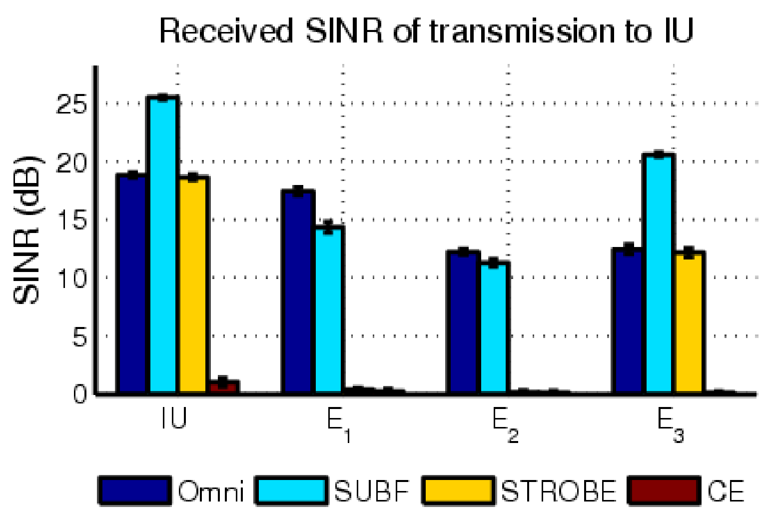


Figure 6.1 : SINR at IU over $E_{1\text{-}3}$ in outdoor environment.

However, the recreation of the initial experiment in an environment with far fewer multi-path effects results in drastic changes for the multi-stream methods. Observe the 2 dB served SINR when using CE to the intended user indicating the absolute failure of this multi-stream method. CE relies on its ability to separate the receivers channels in order to serve the intended user and precisely blind the eavesdroppers. Without multi-path, it is unable to do so.

In contrast, the served SINR at the intended user when using STROBE is almost 19 dB but the blinding abilities of STROBE completely fail at E_3 where a 13 dB signal is overheard. Recall from Fig. 4.1 that E_3 is located in front of the intended user and $E_{1\text{-}2}$ together on the opposite side. The eavesdropper SINR at $E_{1\text{-}2}$ is approximately 0 dB indicating that, without multi-path, STROBE is very susceptible to relative eavesdropper position and separation distance. Other results from setting the intended user at the different receiver positions confirm that without multi-path, STROBE becomes very directional and defeating the protocol simply requires approaching the intended user.

Chapter 7

The Nomadic Eavesdropper

In this chapter we consider a nomadic eavesdropper that traverses throughout an an indoor environment looking for the most opportune eavesdropping location. Previous experiments have demonstrated the wide variations in channel state from one position to the next due to multi-path effects. This randomness could permit a determined eavesdropper to exhaustively search an environment looking for such an opportune location.

7.1 Experimental Setup

7.1.1 Topology

To evaluate the potential of a location-based brute-force attack, we construct the topology shown in Fig. 7.1 in a large classroom (where each circle represents a seat). The classroom is filled with tables, chairs, and other objects that contribute to the rich multi-path characteristics of the environment. We place the transmitter at the head of the room in front of the classroom podium and the intended user approximately 6 m away on a direct LOS path. We transmit data to the intended user while placing the eavesdroppers at 24 different locations around the classroom. The variety of different locations emulate the behavior of a determined eavesdropper searching for the optimal overhearing location.

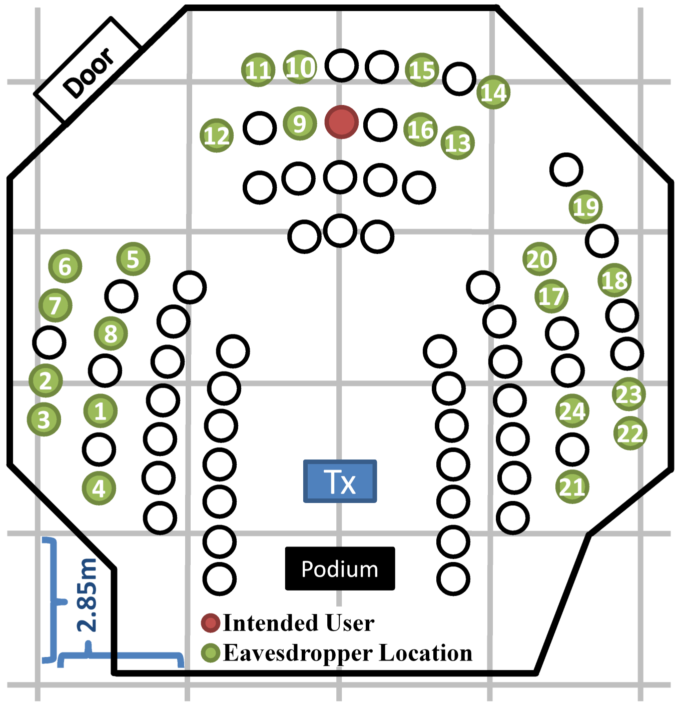


Figure 7.1 : Classroom Environment

7.1.2 Scheme Comparison

Unlike previous experiments, we compare the performance of STROBE against a directional antenna instead of the unfeasible CE scheme. As described in Chapter 4.3, CE is only capable of precisely blinding one less than the number of transmit antennas eavesdroppers (three) and for this topology we have 24. Additionally, the simplest way to focus signal energy in a particular direction is to use a directional antenna. Regardless of the antenna's transmission angle, a directionally based transmission should put energy toward a particular location but not elsewhere. This makes such an antenna a promising candidate for directionally motivated security.

The antenna chosen for comparison is a Trendnet TEW-AO09D* 60^o, 9 dBi antenna

*Trendnet TEW-AO09D Directional Antenna - Available at: `www.trendnet.com`

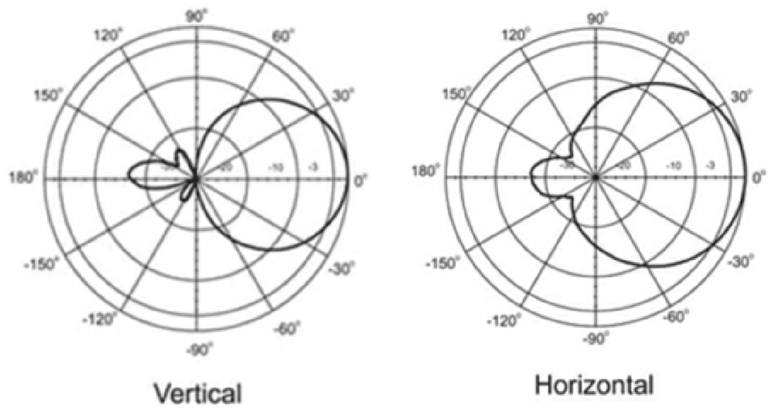


Figure 7.2 : Beam pattern of 60^o directional antenna

with a radiation pattern shown in Fig. 7.2. Although the width of the beam pattern precludes the possibility of perfectly removing overheard signal energy, the beam's shape suggests that regions of the environment can be spared from leaked signal strength.

7.2 Experimental Results

The results shown in Figs. 7.3, 7.4, 7.5, and 7.6 are presented as maps of received signal energy where colors correspond to the different received signal strengths. Dark blues represent lower SINR whereas dark reds represent high SINRs. The maps are to the scale of Fig. 7.1 with intended user and eavesdropper circles corresponding to the separate squares on the maps. The numbers indicated in Fig. 7.1 will be used to identify individual eavesdropper locations.

Omnidirectional Transmission

As in previous experiments, observe the inherent randomness of multi-path effects when agnostically transmitting energy with an Omnidirectional scheme as shown in Fig. 7.3.

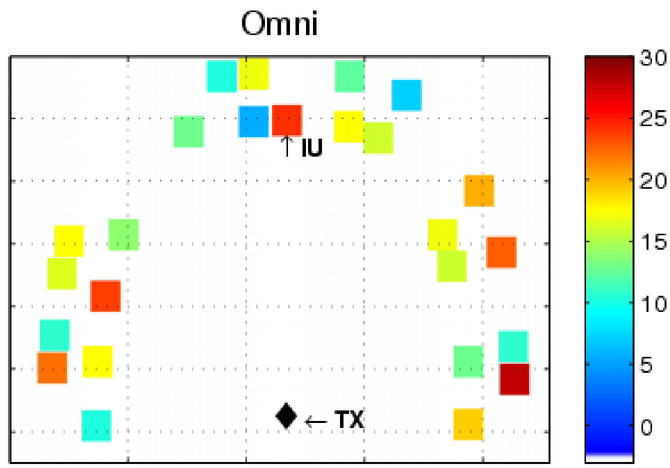


Figure 7.3 : Omnidirectional Transmission (dB)

Note that the lowest received SINR for this scheme (location 9, 5 dB) is located in the seat next to the intended user who received an SINR of 25 dB. Additionally, observe the wide color variation in eavesdropper SINR with regards to location. There is no correlation between distance from the transmitter and received SINR. However, other than the low measurements at locations 9 and 14, all other eavesdroppers were able to overhear a signal of at least 10 dB while the intended user received a signal of 24 dB.

The maximum received SINR from the Omnidirectional transmission is at location 22 (27 dB) while the average SINR overheard by the eavesdroppers at all locations is 16 dB. Thus, even with the inherent randomness of signal strength due to multi-path, it is relatively easy for an eavesdropper to find the opportune location to overhear an Omnidirectional transmission.

Single-User Beamforming

Again, the results for SUBF from previous experiments with simpler topologies are confirmed as shown in Fig. 7.4.

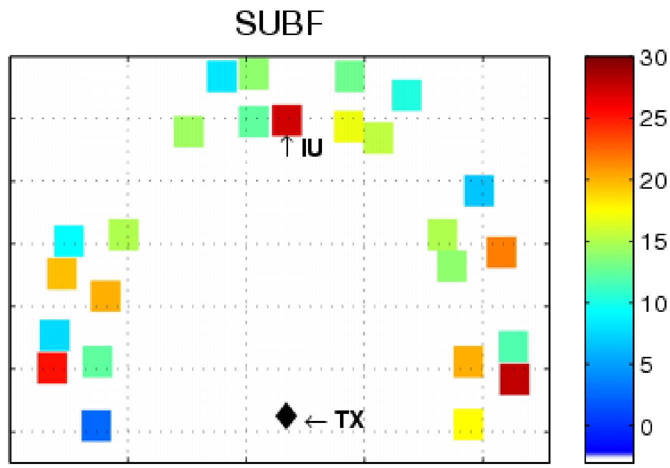


Figure 7.4 : SUBF Transmission SINR (dB)

SUBF serves the highest SINR to the intended user (27 dB) out of all schemes. Although the energy is focused toward a particular receiver, the high eavesdropper SINRs are located in places similar to that of the Omnidirectional transmission.

For example, location 22 overheard the signal with an SINR of 27 dB, which is of equal power to the Omnidirectional transmission (and equal power to the intended user in this scheme). Locations 18, 8, and 3 also had similarly high received SINRs for both Omnidirectional and SUBF transmissions (20-25 dB). These locations receiving high SINRs relative to the intended user are understandable for an Omnidirectional transmission due to the shorter eavesdropper to transmitter distance. Although SUBF focuses energy toward the intended user, it still suffers from the generation of side lobes. When this effect is combined with multi-path, the result is a high overheard SINR at locations that are far away from the intended user.

Overall, the average overheard SINR for the SUBF transmission is 14 dB. The strong overheard signal combined with the lack of correlation between eavesdropper location and overheard signal strength show that SUBF can be defeated by a nomadic eavesdropper.

Directional Antenna

The passive directional transmission from the directional antenna focuses energy toward where it is physically pointed unlike SUBF. Although beamforming based methods are aided by multi-path, the side effect is the potential for random signal reflections to increase SINRs at unintended locations (such as location 22 for SUBF). Observe in Fig. 7.5 the ability of the directional antenna to passively focus energy toward a particular direction allowing the directional antenna to better cope with multi-path induced randomness seen in previous schemes.

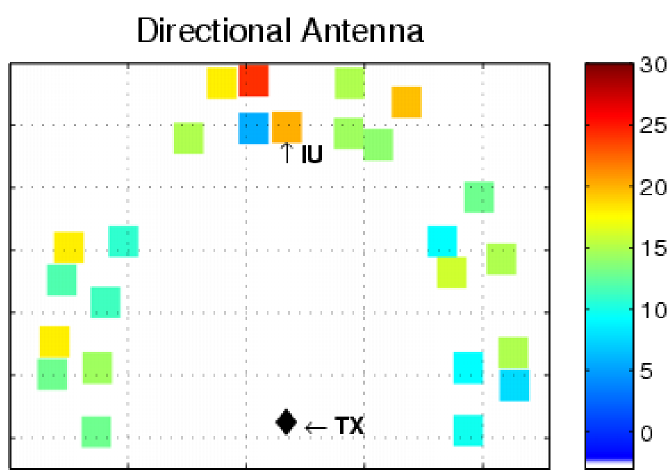


Figure 7.5 : Directional Antenna Transmission SINR (dB)

Specifically, note the received SINR at location 22 (8 dB). This particular location receives a strong signal reflection for the Omnidirectional and SUBF schemes (27 dB) but is far lower for the directional antenna. Other examples of this phenomenon include locations 18, 8, and 3, which all received approximately 10 dB weaker overheard signals than the Omnidirectional and SUBF transmissions. Even so, the overheard signal at these locations is still strong, between 11-15 dB, while the intended user's SINR is 20 dB (4 and

7 dB less than the previous schemes).

However, the Directional Antenna's ability to passively focus energy does not make it immune to multi-path effects. The randomness caused by multi-path is simply constrained to the area where the Directional Antenna is sending the energy. Consider location 9's received SINR of 6 dB. The intended user receives the signal at 20 dB even though it is located in the adjacent seat to location 9. Additionally, location 10 received the strongest signal overall (24 dB) from this transmission method by being behind the intended user and catching a strong reflection from the back wall of the classroom.

Although the Directional Antenna reduces multi-path randomness on the sides of the classroom, it is still affected by multi-path effects where it actually sends the signal. Additionally, the passive, directional transmission does not eliminate the overheard signal outside of its specified beampattern because of the constrained nature of the indoor environment. The average overheard SINR is still 13 dB and because there is some correlation between location and overheard SINR, it is feasible for an eavesdropper to move toward the intended user looking for favorable signal strength.

STROBE

As similarly observed in previous, simpler topologies, STROBE successfully blinds eavesdroppers as depicted in Fig. 7.6.

Observe that while the intended user receives a signal of 20 dB (shown as orange), all eavesdropper locations receive far less signal energy (all shades of blue). The maximum overheard signal is at location 16 (5 dB). Additionally, 60% of the overheard signal strengths are less than 1 dB. By employing orthogonal blinding, STROBE successfully and consistently diminishes eavesdropper SINR regardless of location.

STROBE's ability to handle multi-path randomness is also pronounced. Not only does

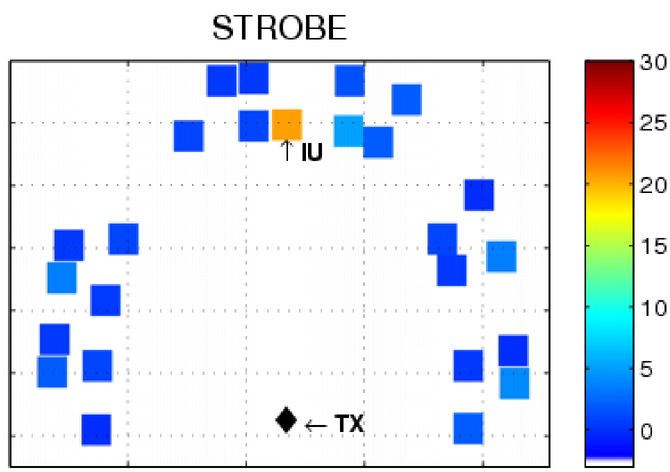


Figure 7.6 : STROBE Transmission SINR (dB)

STROBE consistently blind eavesdroppers, it also handles irregular reflection locations (such as location 22) far better than Omnidirectional and SUBF transmissions. Although location 22 resulted in the second strongest overheard location, the eavesdropper SINR was limited to 4 dB, far less than the 27 dB overheard SINR for the first two schemes.

Additionally, the overall average SINR for STROBE was only *1.3 dB*, showing that STROBE outperformed the other three schemes by 12-14 dB in overheard SINR. These consistently low overheard SINRs, regardless of eavesdropper location, show that STROBE can easily withstand a determined eavesdropper attempting to search for an opportune eavesdropping location.

Chapter 8

Related Work

8.1 Wireless security exploiting CSI-based secret

One method of guarding a transmitter from an eavesdropper is CSI-based secret sharing. For example, the authors of [11] directly use intended user's CSI as a secret generation method while the authors of [12] use the intended user's CSI to actively disrupt OFDM subcarriers in order to confuse eavesdroppers. In contrast, our implementation uses the CSI to beamform a signal toward the intended user while simultaneously blinding eavesdroppers. Moreover, because our method's use of CSI is independent of the aforementioned works, the two methods are complementary.

8.2 Beamforming-based multiple AP cooperation

Beamforming schemes that rely on groups of cooperating APs have also been proposed to secure wireless networks. The authors of [13] propose a method of securing wireless communications using a collection of phased arrays working in tandem to serve an intended user with a data stream. Each AP provides partial information of the overall data transfer and relies on precise, directionally based transmissions to ensure the intersection of all partial streams at a particular geographic location. Additionally, the authors of [14] propose a set of multiple AP methods that allow information to be focused toward an intended user but away from an eavesdropper. Although the authors propose the use of adaptive array beamformers, the weight construction technique employed is directly based on the physical shape of the constructed beam. However, such techniques can be unpredictable in indoor environments as shown in [2] and verified by our experiments in Chapter 7. Furthermore, both of these works propose schemes that require multiple APs and custom hardware whereas STROBEuses a single AP and is compatible with 802.11ac and 11n. STROBE is able to accomplish the same goal from a single transmitter because the scheme leverages the capabilities of multi-stream transmission methods.

8.3 Information theoretic multi-antenna security

There have been a number of information theoretic studies that examine the theoretical performance of multi-antenna based security methods [15, 16]. In particular, these works define the fundamental limits of secrecy capacity. For example, [16] proves that a non-zero rate of communication can be guaranteed to be secret for any eavesdropper position. In contrast, our focus is on protocol design and experimental evaluation with alternate schemes. Likewise, [17] explores how eavesdroppers can be thwarted by a cooperative communication scheme.

Chapter 9

Conclusion

In this thesis, we design and experimentally characterize STROBE, a method of enhancing wireless security using Zero-Forcing Beamforming. We implement STROBE in the WARPLab experimental platform allowing us to comparatively evaluate it against Omnidirectional, Single-User Beamforming, Directional Antenna, and Cooperating Eavesdropper transmission schemes. We show that STROBE achieves a higher SINR difference between the intended user and the eavesdropper than the single-target schemes because of its ability to blind. Additionally, we show that STROBE achieves a higher SINR difference that the unrealistic Cooperating Eavesdropper scheme because STROBE maximizes the SINR at the intended receiver while blinding eavesdroppers. We also demonstrate the performance of STROBE in a variety of indoor, multi-path rich environments and show its efficacy regardless of eavesdropper proximity or obstruction from the transmitter. We verify that STROBE's performance is due in part to the presence of multi-path effects in indoor environments by observing STROBE's diminished efficacy outdoors. Finally, we show STROBE's resilience from the nomadic eavesdropper that traverses an environment continuously searching for an opportune eavesdropping location. Thus, STROBE is a minimally invasive, viable method of augmenting wireless security using existing wireless technologies.

Appendix A

Additional Plots

This appendix contains all plots for the experiments in Chapters 4, 5.2, and 6. Each of these experiments used four receivers setting one as the intended user and the others as the eavesdroppers. In each of the aforementioned chapters, only one intended user/eavesdropper permutation was presented. The rest can be found in this appendix.

A.1 Additional Plots for Baseline WLAN Scenario (Chapter 4)

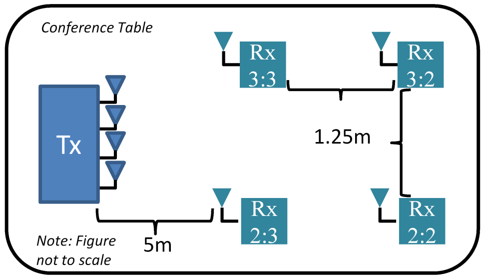
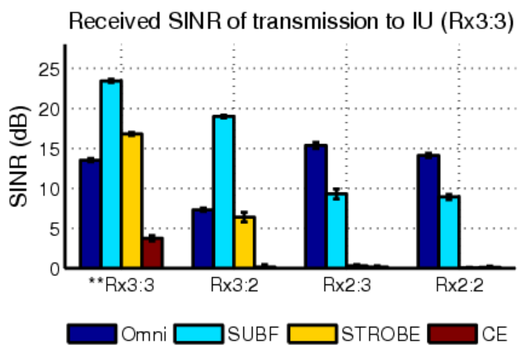
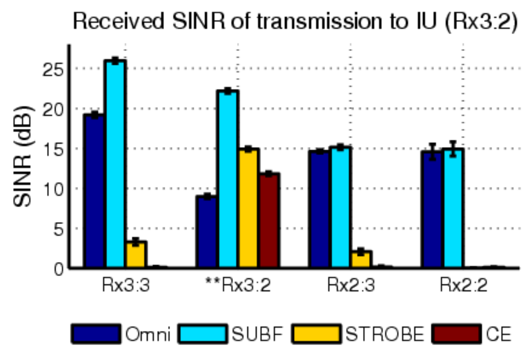


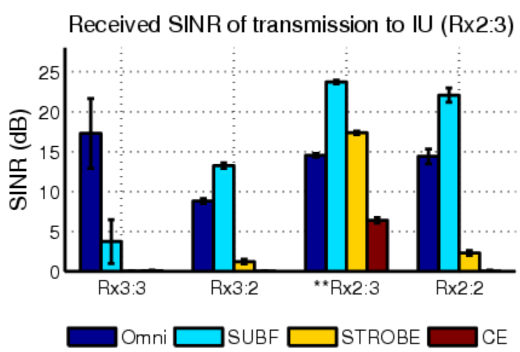
Figure A.1 : Baseline WLAN Scenario Topology



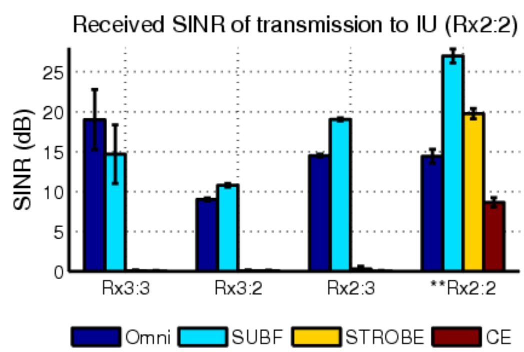
(a)



(b)



(c)



(d)

Figure A.2 : Complete results for Chapter 4

The results and plot shown in Fig. A.2(b) were presented in Chapter 4.

A.2 Additional Plots for Inline Eavesdropper Scenario (Chapter 5.2)

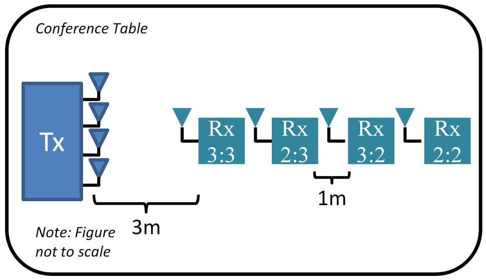


Figure A.3 : Inline Eavesdropper Topology

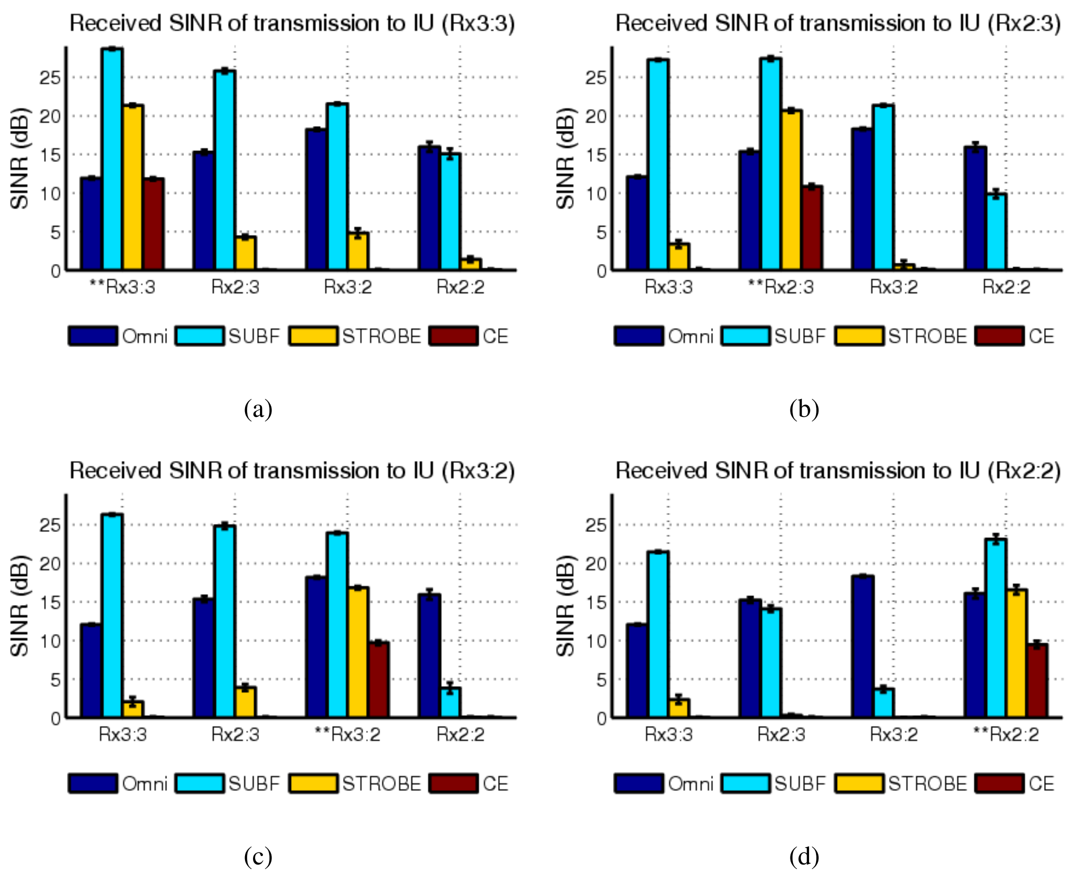


Figure A.4 : Complete results for Chapter 5.2

The results and plot shown in Fig. A.4(c) were presented in Chapter 5.2.

A.3 Additional Plots for Outdoor Scenario (Chapter 6)

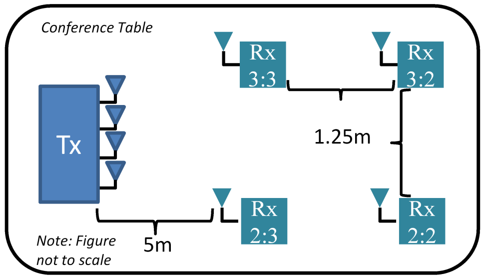
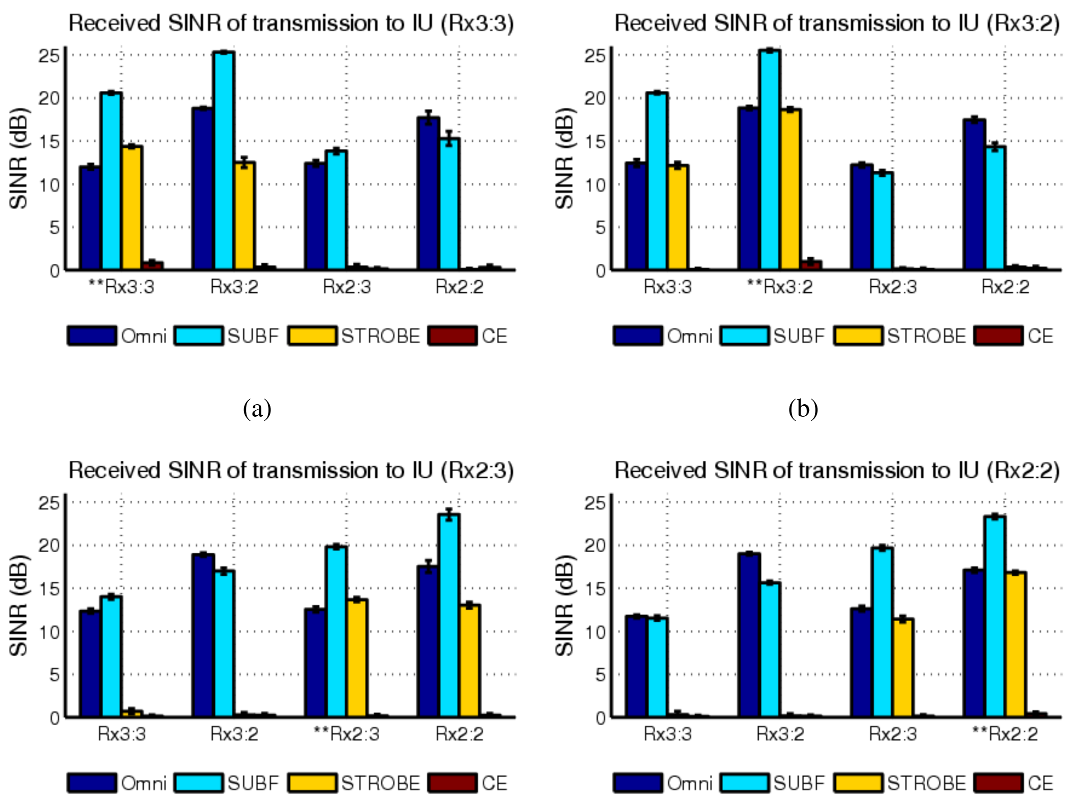


Figure A.5 : Outdoor Topology



(a) (b)

(c) (d)

Figure A.6 : Complete results for Chapter 6

The results and plot shown in Fig. A.6(b) were presented in Chapter 6.

Bibliography

[1] E. Tews and M. Beck, "Practical attacks against WEP and WPA," in *Proc. of ACM WiSec*, 2009.

[2] M. Buettner, E. Anderson, G. Yee, D. Saha, A. Sheth, D. Sicker, and D. Grunwald, "A phased array antenna testbed for evaluating directionality in wireless networks," in *MobiEval*, 2007.

[3] T. Yoo and A. Goldsmith, "On the optimality of multiantenna broadcast scheduling using zero-forcing beamforming," *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 528–541, March 2006.

[4] M. Costa, "Writing on dirty paper (corresp.)," *IEEE Transactions on Information Theory*, vol. 29, pp. 439–441, May 1983.

[5] H. Weingarten, Y. Steinberg, and S. Shamai, "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Transactions on Information Theory*, vol. 52, pp. 3936–3964, Sept. 2006.

[6] A. Wiesel, Y. Eldar, and S. Shamai, "Zero-forcing precoding and generalized inverses," *IEEE Transactions on Signal Processing*, vol. 56, pp. 4409–4418, September 2008.

[7] S. Friedberg, A. Insel, and L. Spence, *Linear Algebra*. Prentice Hall, 4^{th} ed., 2003.

[8] A. Maltsev, V. Pestretsov, R. Maslennikov, and A. Khoryaev, “Triangular systolic array with reduced latency for QR-decomposition of complex matrices,” in *Proc. IEEE International Symposium on Circuits and Systems (ISCAS)*, 2006.

[9] E. Aryafar, N. Anand, T. Salonidis, and E. Knightly, “Design and experimental evaluation of multi-user beamforming in Wireless LANs,” in *Proc. ACM MobiCom*, (Chicago, Illinois), September 2010.

[10] F. Kaltenberger, M. Kountouris, D. Gesbert, and R. Knopp, “On the trade-off between feedback and capacity in measured MU-MIMO channels,” *IEEE Transactions on Communications*, vol. 8, pp. 4866–4875, September 2009.

[11] Z. Li, W. Xu, R. Miller, and W. Trappe, “Securing wireless systems via lower layer enforcements,” in *Proc. of ACM Wireless Security Workshop*, 2006.

[12] S. Gollakota and D. Katabi, “Physical layer wireless security made fast and channel-independent,” in *Proc. IEEE INFOCOM*, (Shanghai, China), April 2011.

[13] J. Carey and D. Grunwald, “Enhancing WLAN security with smart antennas: a physical layer response for information assurance,” in *Proc. IEEE Vehicular Technology Conference*, September 2004.

[14] S. Lakshmanan, C. Tsao, R. Sivakumar, and K. Sundaresan, “Securing Wireless Data Networks against Eavesdropping using Smart Antennas,” in *The 28th International Conference on Distributed Computing Systems*, (Beijing, China), June 2008.

[15] R. Negi and S. Goel, “Secret communication using artificial noise,” in *Proc. IEEE Vehicular Technology Conference*, September 2005.

[16] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Transactions on Communications*, vol. 7, pp. 2180–2189, June 2008.

[17] L. Dong, Z. Han, A. Petropulu, and V. Poor, “Improving wireless physical layer security via cooperating relays,” *IEEE Transactions on Signal Processing*, vol. 58, pp. 1875–1888, March 2010.