Syracuse University

SURFACE

Dissertations - ALL

SURFACE

January 2015

On robust and secure wireless communication system design using software-defined radios

Kapil Meghashyam Borle
Syracuse University

Follow this and additional works at: https://surface.syr.edu/etd

Part of the Engineering Commons

Recommended Citation

Borle, Kapil Meghashyam, "On robust and secure wireless communication system design using software-defined radios" (2015). *Dissertations - ALL*. 321.
https://surface.syr.edu/etd/321

This Dissertation is brought to you for free and open access by the SURFACE at SURFACE. It has been accepted for inclusion in Dissertations - ALL by an authorized administrator of SURFACE. For more information, please contact surface@syr.edu.

ABSTRACT

This dissertation is composed of three parts: airborne multiple input multiple output (MIMO) communications, physical layer authentication, and software radio design for DARPA Spectrum Challenge. A common theme for the three distinct problems is the system perspective that we have adopted throughout this dissertation. Instead of considering isolated issues within these problems, we have provided a holistic design approach to the three problems and have implemented all three systems using the GNU Radio/USRP (Universal Software Radio Peripheral) platform.

In the first part, we develop a MIMO communication system for airborne platforms. MIMO communication has long been considered to be suitable only for environment that is rich in scatterers. This, unfortunately is not the case for airborne platforms. However, this lack of scattering can be compensated by the large aperture of the airborne MIMO platform; this is corroborated by our careful analysis using real measurement data. Our analysis of the airborne MIMO channels leads to the development of a variable rate MIMO transceiver architecture. This architecture is numerically shown to improve the bit error rate (BER) over conventional transceiver architectures that are developed for rich scattering environments. A software radio based MIMO system is then implemented to demonstrate experimentally the efficacy of the developed architecture.

In the second part, we develop a physical layer authentication scheme as a counter measure to primary user emulation attack (PUEA) in cognitive radio (CR) networks. In this attack, a malicious user emulates the signal characteristics of the primary user (PU) when it is silent which prevents unsuspecting secondary users (SUs) from utilizing the network. The developed physical layer authentication is based on embedding cryptographic hash signatures, referred to as authentication tags, within PU's signal constellations. The embedding is performed such that the legacy receivers are not affected. We analyze the scheme using the fast fading Rayleigh channel model and present an optimal scheme to embed signals in PU's constellations which minimizes the tag BER. Experimental results are obtained that corroborate our theoretical claims, thereby establish that reliable

authentication can be achieved without sacrificing signal quality at the primary receivers.

In the final part, we describe in detail our design of software radios developed as part of the DARPA Spectrum Challenge (DSC), a year long competition that started in January 2013 and concluded in March 2014 with the final tournament held in Arlington, VA at the DARPA headquarter. DSC was comprised of two tournaments, competitive and cooperative. In the competitive mode two radio pairs, each composed of a transmitter and a receiver, are pitted against each other to transmit the most amount of data error-free while operating concurrently in the same frequency band. In the cooperative mode, three radio pairs have to share a frequency band in a cooperative manner wherein the goal is to maximize the throughput of all the three pairs. We describe the design of our software radio system that integrates some key technologies crucial in operating in an environment that does not allow user coordination and spectrum pre-planning, including: spectrum sensing, adaptive transmission both in spectrum utilization and transmission rate, opportunistic jamming, and sliding window feedback. The developed radio is robust in the presence of unknown interference and achieves the desired balance between throughput and reliability in an uncoordinated transmission environment.

ON ROBUST AND SECURE WIRELESS COMMUNICATION SYSTEM DESIGN USING SOFTWARE-DEFINED RADIOS

By

Kapil M. Borle
B.E., University of Pune, 2005
M.S., Syracuse University, 2011

THESIS

Submitted in partial fulfillment of the requirements for the degree of
Doctor of Philosophy in Electrical & Computer Engineering

Syracuse University
August 2015

Copyright © 2015 Kapil M. Borle

All rights reserved

To my parents, Savita and Meghashyam, for their eternal love and support

ACKNOWLEDGMENTS

Words cannot express the immense gratitude I feel towards my adviser, Prof. Biao Chen, for his never-ending support, guidance, and patience towards me. However, I would like to take this opportunity to thank him for giving me the opportunity and helping me reach this milestone. I would also like to thank the committee members - Prof. Wenliang Du, Prof. Yingbin Liang, Prof. Peng Gao, Dr. John Matyjas, and Prof. Pramod Varshney - for their time and for their insighful comments on how to improve the dissertation.

Many thanks to Dr. Michael Gans for his numerous technical contributions, his invaluable insights and his persistence in ensuring that our work stays relevant to the Air Force need throughout our collaboration on airborne MIMO communications. We are also grateful for the generous support of Air Force Research Lab through awards FA8750-15-1-0045 and FA8750-11-1-0040.

The DARPA Spectrum Challenge, from February 2013 to March 2014, was hands-down the most exciting and defining part of my academic pursuit at Syracuse University. Without my teammates, Fangfang Zhu, Yu Zhao, and Prof. Biao Chen, it would not have been possible. Prof. Chen was not just a part of the team, he was the team leader any team would envy for. He always made sure we had all the resources at our disposal and were in the right direction. He would even pull all-nighters with us when deadlines were looming!

Without taking any chance of missing out any names, I would like to thank all the friends who made this journey memorable and worthwhile.

Finally, it is only because of the continued support and encouragement from my parents, that I have had the chances to pursue things at my own volition. This particular endeavor is no exception. Merely thanking them for all the things they have done for me would be an understatement. A special shout-out to my sisters, Shruti and Rucha, who are always there to help me.

TABLE OF CONTENTS

Acknowledgments **vi**

List of Figures **xi**

1 Introduction **1**

1.1 Airborne MIMO Communication 4

1.2 Physical Layer Authentication 6

1.3 Software Defined Radio 8

1.4 Thesis Outline 8

1.5 Contribution 10

2 Channel Tracking For D-BLAST **13**

2.1 Introduction 13

2.2 Channel Estimation - Optimal Length 14

2.2.1 Single Input Single Output Case 14

2.2.2 Multiple Input Multiple Output Case 18

2.3 D-BLAST Architecture 20

2.4 Channel Tracking 21

2.5 Simulation 22

2.5.1 Channel Tracking 22

2.5.2 Outage Detection 23

2.6 Summary 24

3 Variable Rate MIMO 26

3.1 Introduction 26

3.2 MIMO Channel State Matrix Measurements 28

3.2.1 Measurement Apparatus 28

3.2.2 Challenges 30

3.3 Variable Rate MIMO 32

3.4 Simulation 35

3.5 Experiment 36

3.6 Summary 39

4 Physical Layer Authentication For Specturm Usage Authentication 41

4.1 Introduction 41

4.2 A Physical Layer Authentication Scheme 42

4.2.1 Tag Generation 43

4.2.2 Tag Transmission 45

4.3 Tag Embedding for General Constellations 45

4.3.1 Uniform Angular Degradation (UAD) 49

4.3.2 Uniform Energy Degradation (UED) 50

4.3.3 Scheme Optimality 51

4.4 Trade-off Analysis 52

4.5 Summary 55

5 Physical Layer Authentication Implementation 56

5.1 Introduction 56

5.2 Experiment Setup 57

5.3 Implementation 58

5.4 Observations 62

5.5 Summary 64

6 A Software Radio Design for Communications in Uncoordinated Networks 67

6.1 Introduction 67
6.2 Orbit-Lab 68
6.3 Strategies 69
6.3.1 Competitive Mode 73
6.3.2 Cooperative Mode 74
6.4 Feedback Scheme 76
6.5 Summary 79

7 Conclusion And Future Work 80

7.1 Conclusion 80
7.2 Future Work Propositions 82

A Proof of Theorem 1 84

B Proof of Proposition 1 88

References 90

LIST OF FIGURES

1 Behavior of MSE of SISO channel for $f_D T_s = 1.25 \times 10^{-4}$ with block length of 200 symbols 17
2 Behavior of MSE of a 4×4 channel for $f_D T_s = 7.72 \times 10^{-5}$ with block length of 324 symbols. 19
3 4×4 D-BLAST tracking MSE w.r.t sub-blocks for $f_D T_s = 7.72 \times 10^{-5}$. 20
4 Behavior of channel estimation mean square error with increasing number of code blocks 22
5 Behavior of the mean magnitude of LLR of decoded LDPC code with increasing number of code blocks 23
6 Behavior of Average Mean Magnitude of Log Likelihood Ratios for an LDPC code with $N = 648$ and $R = \frac{1}{2}$ 24
7 UCAV with square patch antennas. 29
8 Antenna Pattern 30
9 Element Ground Array 31
10 UCAV and Ground Array on the 400 ft. Newport Range. 32
11 Variable rate MIMO transceiver block diagram 34
12 Outage rate for all vertical polarization at rate 4 bits/s/Hz. 36
13 Outage rate for mixed polarization at rate 4 bits/s/Hz. 37
14 USRP Setup 38
15 Transmitter Block Diagram 39
16 Receiver Block Diagram 39

17 Measured outage probability for 2×2 variable rate MIMO 40

18 Physical Layer Authentication. 42
19 Constellation Diagrams 44
20 Average error probability of the tag bit as function of tag signal to noise power ratio for a 16 QAM system with $\rho = 25\,\mathrm{dB}$. 54

21 Measurement Setup 57
22 Transmitter Block Diagram 58
23 Receiver Block Diagram 59
24 Tag Detector Block Diagram 60
26 Measured error rate of the tag bit as function of tag signal to noise power ratio for a 16 QAM system for average $\rho = 26.48$ dB. 62
25 De-spreading 65
27 Received Constellation With & Without Tag 66

28 Final Tournament Node Topology - Primary Arena 69
29 Final Tournament Node Topology - Secondary Arena 70
30 High Level Packet Transmitter Block Diagram 71
31 High Level Packet Receiver Block Diagram 71
32 Packet Transmitter 72
33 Packet Format 72
34 Physical Layer Frame Format 73
35 Packet Receiver 73
36 Competitive Mode Strategy. P, J and F represent packet transfer, jamming and feedback mode respectively. The top row represents the state of the transceiver and the bottom row represents the corresponding duration the transceiver dwells in the state. 74
37 Cooperative Mode Strategy 76

38 Cooperative Mode Baseband Frequency Spectrum 77

39 Feedback Scheme 78

CHAPTER 1

INTRODUCTION

Radio frequency (RF) communication has become an indispensable part of our lives. From communication over short ranges, e.g. radio frequency identification (RFID), to extremely long ranges, e.g. space probes, RF medium is among the most versatile of all communication media. However, its utility as a last mile delivery medium is unparalleled. This particular aspect has resulted in an explosive proliferation of RF communication in recent years. As with all natural resources, wireless medium is a finite resource. An exponential growth in the demand for data in recent years has pushed the need for higher and higher data rates over this finite resource. Consequently, a lot of effort has gone into developing wireless technologies that can help keep up with this ever increasing demand for data. More sophisticated theory and system design have been proposed over the years. A powerful tool for ensuring that the developed theory and technologies stay practically relevant is the use of sofware-defined radio (SDR) for proof of concept system implementation. This enables a system design perspective where the theory and technological innovations to be developed *can be* integrated in a working system. Such a system perspective also provides a profound and meaningful way to identify deficiencies of developed theory or design framework through experimental validation. It is with this system perspective that we investigate three major design issues in wireless systems: throughput, security and robustness to interference.

Conventionally, wireless communication research involves focus on one particular aspect or component within the system. However, with such an approach, the bigger picture - a realizable communication system, where all the components of the system have to interact with each other to provide a reliable means of transferring information - may become very hard to attain or outright impossible with the current state of hardware and software technology. We, on the other hand, have made attempts to solve the problems with the explicit goal of developing a working communication system. It is precisely this approach that lends our work its strength - developing experimental platforms and conducting relevant experiments to support the underlying hypotheses. However, we cannot be complete in describing the systems perspective without stating its limitations. By adopting this approach we can end up leaving a lot of threads hanging that warrant more investigation which can give the appearance of not having a strong theoretical foundation. Hence, as with all engineering pursuits there is trade-off between systems approach and focusing on one particular aspect of the system.

Adopting systems approach is enabled by our ability to conduct experiments. We develop communication system prototypes using SDR which is a relatively recent technology that leverages the power of software to rapidly develop communication systems that can be very flexible in their operation. Typically, this flexibility is precluded when all the components that go into making a communication system are developed in the form of hardware which results in a transceiver that is designed to operate a fixed physical layer protocol. The main cause for baking all or most of the signal processing components in hardware is the need for extremely fast but highly repetitive computation, even for very trivial transceiver design. But, the drawback is the high cost and time associated with developing such hardware systems. Also, the inability in term of changing or tweaking a small component of the hardware transceiver, once it is developed, results in a system that is not very favorable for the experimental approach. SDR technology, however, proposes to move the signal processing components into software such that only the bare minimum communication specific hardware components, e.g., analog to digital converter (ADC), digital to analog converter (DAC), RF front-end, antennas, etc, stay put. As mentioned earlier, SDR is relatively recent and it owes this to the development of high speed personal computers or other such computational platforms. By moving most of the signal processing components to software, we are able to rapidly develop the required signal processing components and modify them as needed. This reduces tremendously the time required to bring up a working communication system. Hence, with the power of SDR, we are able to rapidly prototype the desired communication system and then carry out the necessary experiments to investigate the underlying hypotheses. Thus, through the use of SDR we are able to adopt a systems approach to investigate several design issues within the context of multiple input multiple output (MIMO) and cognitive radio (CR), two wireless technologies that play a key role in ensuring that wireless systems keep up the data demand.

MIMO has the potential to increase by several orders of magnitude the data rates over the same radio frequency spectrum compared with single antenna systems. Introduced relatively recently [7], it takes advantage of spatial dimension to improve the capacity. The gains promised by MIMO are applicable mostly to wireless channels with rich scattering [28]. Nonetheless, we can reap some of the gains even within environments that lack rich scattering. In [9], the author shows that MIMO can offer non-trivial gains in achievable data rates for airborne platforms even though the channel is assumed completely void of scatterers. Traditional MIMO transceiver architectures subsume a rich scattering environment to deliver the gains in data rates through spatial multiplexing. For airborne platforms, these architectures prove to be inadequate, due primarily to the particular characteristics of airborne MIMO channels. To address this problem we develop a transceiver architecture that is shown to perform better than the conventional spatial multiplexing architectures for airborne communication.

CR on the other hand tries to overcome spectrum scarcity as a result of existing spectrum management regime. At present, most of the RF spectrum has been allocated in a pre-determined manner to private/public entities, leaving only a very small chunk for general usage by public. Ironically, it is this small chunk in the public domain, called the ISM band, that is facing the biggest burden of demand. On the other hand, a sizable portion of the spectrum remains severely underutilized in the licensed bands [14,24]. By allowing unlicensed radio nodes, referred to as secondary users (SUs), to operate within licensed bands such that the SUs do not harm the licensee's communication [18], CR provides a mechanism that helps ease the spectrum crunch. But as with any new technology, developing it without taking into account the security implications is akin to a soldier going into to a battlefield without his/her armor. Similarly, developing CR technology without thinking about its vulnerabilities has the potential to jeopardize the technology's utility, or worse, compromise the entire network. We study one such security issue, referred to as primary user emulation attack (PUEA) [1]. This attack works as follows: a malicious user emulates the signal characteristics of the licensee, thereby disallowing the SUs from using the spectrum. A natural counter measure is to develop a method to authenticate the licensee, thereby defeating the impersonation from the malicious user. We provide a solution that accomplishes authentication at the physical layer, which is highly desirable due to its minimum requirement on the secondary user in terms of its compatibility with the licensee's radio protocol.

The following two sections elaborate more on MIMO for airborne platforms and physical layer authentication. We follow that with an introduction to software defined radio, which we use as a tool to perform experiments.

1.1 Airborne MIMO Communication

MIMO communications employ multiple antennas at communicating terminals. Compared to using single antennas for wireless communication, referred to as SISO (single input single output), this technique takes advantage of spatial dimension. The extra dimension has the potential to greatly enhance achievable data rates and reliability. From a Shannon capacity [23] standpoint, the capacity of a MIMO system in a rich scattering environment [28] increases linearly with respect to the minimum of the number of transmit and receive antennas.

MIMO offers gains in data rates through spatial multiplexing. Spatial multiplexing, first proposed in [20], allows concurrent transmission of multiple data streams thereby increasing the aggregate data rate. Each data stream is often transmitted independently using separate transmit antennas while overlapping completely in radio frequency spectrum with other data streams. At the receiver, each data stream is separated and recovered using its unique spatial signature made possible by employing a sufficient number of receive antennas. Thus, the premise underlying spatial multiplexing is that the channel between the transmitter and receiver permits the resolvability of the spatially multiplexed signal. In order to explain this resolvability issue we first describe the channel model that captures the relationship between the transmitted and received signals. Consider a receiver with r antennas and a transmitter with t antennas. We henceforth refer to such a MIMO system as a $r \times t$ MIMO system. Suppose the transmitter sends the signal $\mathbf{x}$ and the receiver receives $\mathbf{y}$, a canonical MIMO channel is modeled as follows.

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{z} \tag{1.1}$$

where $\mathbf{x}$ is the $t \times 1$ transmitted signal vector, $\mathbf{y}$ is the $r \times 1$ received signal vector, $\mathbf{H}$ is the $r \times t$ channel matrix and $\mathbf{z}$ is the noise vector.

Regarding spatial multiplexing, the number of spatial streams that this channel can support is less than or equal to the rank of the channel matrix $\mathbf{H}$. In typical MIMO applications, the transmitter and receiver are located in dense urban environments. This results in a rich scattering environment such that the channel matrix $\mathbf{H}$ is full row or column rank. MIMO transceiver architectures like vertical Bell Laboratories Layered Space-Time (V-BLAST) and diagonal Bell Laboratories Layered Space-Time (D-BLAST) are designed to provide such multiplexing capability when $t \leq r$. V-BLAST can be considered as a simplified version of D-BLAST, such that it removes coding and data rotation across transmit antennas. Under fast fading channel conditions this simplification does not lead to degradation in performance. But this is not true in case of slow fading channels.

In environments that lack sufficient scattering the channel matrix $\mathbf{H}$ can be rank deficient. Under such scenarios V-BLAST and D-BLAST do not deliver the desired multiplexing gain. We illustrate this point by considering a MIMO communication link between a ground station and an airborne platform. In this case, a lack of scattering results in a severely rank deficient channel matrix. Combining this lack of scattering with strict latency requirements and antenna placements in airborne applications, we obtain a slow fading channel with severely rank deficient channel conditions.

For slow fading channels, outage capacity [27] provides a suitable characterization in terms of achievable data rate. We know that D-BLAST transceiver architecture is optimal with regards to channel outage capacity [7]. Such optimality, however, hinges on the very assumption that the channel is full column rank. As we shall see, this rank condition is often violated for airborne platforms even if the receiver antenna number exceeds that of the transmitter. Suitable modification of the D-BLAST architecture is needed and proposed for airborne communications and we show numerically that this architecture provides a better bit error rate (BER) performance as compared to that of D-BLAST over airborne communication channels.

1.2 Physical Layer Authentication

Authentication is typically the first step and an inseparable component of any security mechanism between communicating parties. Identity verification along with secure and tamper-proof communication are the two important components of secure communication that are enabled by authentication. Conventionally, authentication is implemented at higher communication layers, for example IPSec at network layer, SSL at transport layer, etc, implying that communicating parties operate the same protocol at the layer at which authentication is desired. With the advent of CR technology, it is envisioned that heterogeneous radio nodes share spectrum whitepsace. They are heterogeneous in the sense that different radio nodes may serve different purposes such that they operate different protocols at the various communication layers. These heterogeneous radio nodes, also referred to as SUs, comprise a part of a CR network.

A CR network consists primarily of a primary user (PU) and a number of SUs. The PU is the licensed owner of a pre-specified frequency spectrum, while the SUs are allowed to opportunistically use the PU's spectrum so long as they do not degrade PU's communication performance. A simplifying but reasonable assumption that satisfies this requirement is that the SU is allowed to use the spectrum only when the PU is silent, i.e., not transmitting anything. As such, the SU must detect the presence or absence of PU's signals with high reliability. Conventionally, PU's signal detection is implemented using either some form of energy detection or feature detection [13]. These detectors are highly susceptible to attacks where malicious nodes simply emulate PU's signal. Suppose there exists a malicious user in the CR network, which wants to take an unfair share of the spectrum whitespace or simply tries to defeat the spectrum sharing mechanism. The malicious user can simply emulate the PU's signal characteristics whenever the spectrum is unoccupied. This will prevent the benign SUs from using the whitespace thereby defeating the purpose of CR technology. Such an attack is referred to as the primary user emulation attack (PUEA). To prevent primary user emulation attack (PUEA), SUs must be able to identify the authenticity of PU's signal, they need to be able to authenticate the PU. A straightforward way to solve this problem is to use any of the well established authentication mechanisms, e.g. IPSec at network layer to provide the needed authentication process. But this demands that the PU and SUs operate the same protocol at the given layer. There are two major drawbacks to this solution: Firstly, it imposes the constraint on all the radio nodes in the network to operate the same protocol at the appropriate layer. Secondly, any modification to PU's protocol stack to support the authentication mechanism will render the legacy receivers unusable (legacy receivers are the radio nodes that the PU serves). An authentication solution at the lowest layer that doesn't affect the legacy receiver will then be able to circumvent the two previously mentioned drawbacks and thereby solve the PU authentication problem. An additional benefit of implementing physical layer authentication is its ability to thwart the attack at the first possible opportunity thereby minimizing the delay for the authentication process.

1.3 Software Defined Radio

A required component of any scientific inquiry is the physical verifiability of the underlying hypotheses. In our context this translates to the ability to create experimental setups for verifying the developed algorithms by means of over the air experiments. SDR provides a framework to develop such experimental setups rapidly. This is achieved by decoupling the wireless interface and signal processing components. The wireless interface is baked into hardware whereas the signal processing components are developed using some programming language of choice to run on a general purposes processor or a specialized hardware like a digital signal processor or graphical processing units (GPUs).

GNU Radio [10] combined with Universal Software Defined Radio Peripheral (USRP) [29] is one such SDR framework. The USRPs provide the wireless interface that allow us to send and receive wireless signals, while GNU Radio is an open source software defined radio toolkit which supplies the tools necessary to create the different signal processing components of a communication system. Using this framework we can rapidly prototype a communication system that suits our need.

A GNU Radio application consists of connecting various signal processing blocks to create a complete transmit or receive chain. The typical way to achieve this is to implement the computationally intensive signal processing blocks in C++ and then glue them together using Python. This method offers a good trade-off between application development speed and its execution speed - C++ is capable of delivering high performance for the signal processing blocks, whereas Python provides an environment to create rapidly a communication system prototype using the developed signal processing blocks.

1.4 Thesis Outline

The thesis can be roughly divided into three parts, namely, MIMO communication for airborne platforms, physical layer authentication, and software radio implementation. Chapters 2 and 3 study the problem of MIMO communication for airborne platforms. Chapters 4 and 5 deal with developing, analyzing and implementing a physical layer authentication systems over wireless channels. Chapter 6 exposits the SDR implementation details of radio nodes developed during the DARPA Spectrum Challenge.

Chapter 2 studies the problem of finding the optimal length of symbol sequence for estimating continuously varying wireless channel with MIMO airborne platforms. Coherent symbol detection requires knowledge of channel state information. The traditional use of embedding pilot symbols with payload data may not be easy to justify if channel variation is fast and/or data rate requirement is high. We consider the implementation of D-BLAST for airborne platforms and develop channel tracking scheme that eliminates or reduces the use of pilot symbols. In a normal operation mode, channel update is achieved dynamically as each layer of the signal encoded using an LDPC code, is decoded. To ensure that the transceiver can detect outage due to the loss of channel state, an adaptive algorithm is devised utilizing the extremal property of terminating likelihood ratio of an LDPC decoder.

Chapter 3 develops a variable rate MIMO scheme for channels between airborne platforms and ground stations, whose channel matrices are often rank deficient. The prevalent use of unmanned vehicles in military and civilian applications requires the existence of robust and high throughput communication with airborne platforms. Real channel measurements are conducted and the analysis supports the use of MIMO communications for such applications due to its potential throughput advantage. Unique challenges and ways to address them are described in detail. In particular, blockage of line of sight often leads to rank deficient channel matrices, which are exacerbated due to the absence of channel state information at the transmitter. A variable rate MIMO scheme is proposed to overcome these challenges in order to realize the promising throughput gain afforded by MIMO communications.

Chapter 4 develops a physical layer user authentication scheme for wireless systems. The approach can be used as an effective counter measure against the primary user emulation attack in CR networks. The developed scheme applies to general digital constellations and we establish its optimality in terms of error probability for user authentication. Trade-off analysis is provided that balances the performance of the user authentication for the secondary user and symbol detection for the primary user. In particular, we show that arbitrarily reliable user authentication can be achieved at the price of an almost negligible performance degradation for the primary user under realistic system settings

Chapter 5 provides experimental verification for the physical layer authentication scheme developed in Chapter 4. To perform the experiments we developed a software radio system using GNU Radio. This chapter exposits the implementation details and the challenges associated with it. We also show that the theoretical claims of the scheme hold under experimental investigation, albeit, with a few limitations imposed by practical constraints.

Chapter 6 describes a simple software radio design approach to communication and spectrum access in a system without user coordination and spectrum pre-planning. The work is a result of our recent participation in DARPA Spectrum Challenge that provides a venue for head-to-head competitions of software radio designs from teams around the country. Two modes of operations are involved, one is competitive and the other cooperative; each mode calls for completely different way of dealing with interference incurred amongst transceiver pairs. In addition to describing our own design approach, we attempt to provide our own observations on the disconnect between theoretical study of CR/dynamic spectrum access and the state-of-the-art implementation of a functioning radio in a congested environment.

Chapter 7 concludes the thesis by summarizing the efforts and results and with some pointers to future work.

1.5 Contribution

Our main contributions are listed below. Each contribution is followed by the relevant publications.

- We propose a novel channel tracking scheme for D-BLAST transceiver systems in airborne platforms. We derive an expression that gives the optimal length of symbol sequence needed to computed channel estimate in a continuously varying Rayleigh fading channel.

  - K. M. Borle, B. Chen and M. J. Gans, "Channel tracking for D-BLAST for airborne platforms", *Proc. 45th Asilomar Conference on Signals, Systems and Computers*, Monterey, CA, Nov. 2011.

- We propose a modified D-BLAST architecture that improves BER performance over rank deficient channels.
  - M. J. Gans, K. M. Borle, B. Chen, T. Freeland, D. McCarthy, R. Nelson, D. Overrocker and P. Oleski, "Enhancing Connectivity of Unmanned Vehicles Through MIMO Communications", *Proc. of the 2013 IEEE 78th Vehicular Technology Conference*, Las Vegas, Sep. 2013.
- We develop a physical layer authentication scheme to counter PUEA. We analyze the scheme under Rayleigh fading channel and find an optimal method of embedding the authentication bits into PU's QAM digital constellation. Optimality is achieved with respect to BER performance for a given power level.
  - X. Tan, K. M. Borle, W. Du and B. Chen, "Cryptographic Link Signatures For Spectrum Usage Authentication In Cognitive Radio", *Proc. of the 4th ACM conference on Wireless Network Security*, Hamburg, Germany, Jun. 2011.
  - K. M. Borle, B. Chen and W. Du, "A Physical Layer Authentication Scheme For Countering Primary User Emulation Attack", *Proc. of the 38th International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Vancouver, Canada, May 2013.
- We implement the communication system pertaining to the authentication scheme using GNU Radio/USRP SDR framework and experimentally validate the proposed scheme.
  - K. M. Borle, B. Chen and W. Du, "Physical Layer Spectrum Usage Authentication In Cognitive Radio: Analysis and Implementation", to appear in the *IEEE Trans. on Information Forensics and Security*.
- We develop two SDR based communication systems as part of the DARPA Spectrum Challenge. The goal of the first system is to stay online in the presence of heavy interference,

whereas the second system is developed to cooperate with other communication systems in an uncoordinated manner.

- K. M. Borle, F. Zhu, Y. Zhao and B. Chen, “A Software Radio Design for Communications in Uncoordinated Networks”, *Proc. of the 2014 IEEE Workshop on Signal Processing Advances in Wireless Communications*, Toronto, Canada, June 2014.

CHAPTER 2

CHANNEL TRACKING FOR D-BLAST

2.1 Introduction

For communication systems in which either one or both communication parties are in motion, the channel is continuously changing. For coherent detection at the receiver, channel state needs to be constantly updated. The conventional method is to multiplex pilots and data symbols. For the case where there is rapid variation in channel states, this pilot overhead may not be affordable. To tackle this problem we investigate the case in which we use previously detected symbols to estimate channel states for the next block.

For the block fading model, we assume the channel to remain constant during the transmission within a single block. Therefore, channel estimation error arises only because of the additive noise, if estimation uses symbols within each block. Increasing the training length averages out the additive noise component thereby mitigating the estimation error. However, for channels that vary continuously, increasing the training length is not optimal. This is because there is an additional error component induced by temporal channel variation. Increasing training length causes this error component to increase. That is, the symbols used for channel estimation are transmitted through different channel states, thus the longer the symbol block, the more severe the impact of channel variation. As such, simply increasing the training length is not optimal as it decreases the additive noise error component but on the other hand increases the channel variation error component. The problem becomes how do we minimize the error caused by these two factors. We try to solve this problem by first finding the optimal length of symbols needed to minimize the mean squared error of the estimated channel for a SISO (single input single output) channel with Rayleigh fading. Then we generalize this to the MIMO (multi input multi output) case, where we find the length of symbols required to estimate channels in our channel tracking algorithm.

While channel tracking using payload data improves the efficiency, it is imperative for the system to detect an outage, i.e., when the channel tracking becomes unreliable, giving rise to excessive bit errors. Notice that such a problem is not severe with a pilot symbols based system as channels are constantly updated using known pilot symbols. We exploit the extremal property of the terminating Log-Likelihood Ratios (log-likelihood ratio (LLR)s) of Low Density Parity Check (LDPC) codes during the decoding process. We use the property that for decoding success, the mean magnitude of the LLRs increase without bound, whereas in the case of decoding failure, it remains at a small value with respect to the number of decoding (message passing) iterations [16].

Section 2.2 gives the analysis for optimal length to minimize the mean squared error in a Rayleigh fading channel. We then give a brief description of the D-BLAST architecture in Section 2.3. Section 2.4 describes the channel tracking algorithm for D-BLAST, followed by simulation results.

2.2 Channel Estimation - Optimal Length

2.2.1 Single Input Single Output Case

Consider a SISO channel, $y_i = h_i x_i + z_i$, where x_i is the transmitted symbol, z_i is the additive noise and h_i is the fading coefficient in the i^{th} time slot [28]. If the transmitter transmits $N + 1$

symbols in $N+1$ consecutive time slots,

$$\begin{bmatrix} y_N \\ y_{N-1} \\ \vdots \\ y_0 \end{bmatrix} = \begin{bmatrix} h_N & 0 & \dots & 0 \\ 0 & h_{N-1} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & h_1 \end{bmatrix} \begin{bmatrix} x_N \\ x_{N-1} \\ \vdots \\ x_0 \end{bmatrix} + \begin{bmatrix} z_N \\ z_{N-1} \\ \vdots \\ z_0 \end{bmatrix}. \tag{2.1}$$

Write the diagonal matrix of fading coefficients as $h_{N-k} = h_N + \Delta_k$, for $k = 1, 2, \dots N$ [25], eq. (2.1) becomes

$$\begin{bmatrix} y_N \\ y_{N-1} \\ \vdots \\ y_0 \end{bmatrix} = h_N \mathbf{I}_N \mathbf{x} + \begin{bmatrix} 0 & 0 & \dots & 0 \\ 0 & \Delta_1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \Delta_N \end{bmatrix} \begin{bmatrix} x_N \\ x_{N-1} \\ \vdots \\ x_0 \end{bmatrix} + \begin{bmatrix} z_N \\ z_{N-1} \\ \vdots \\ z_0 \end{bmatrix}, \tag{2.2}$$

where $\mathbf{I}_N$ is an $N \times N$ identity matrix and $\mathbf{x} = [x_N \; x_{N-1} \dots x_1]^T$ Multiplying both sides by $\mathbf{x}^H$ we get,

$$\mathbf{x}^H \mathbf{y} = h_N \mathbf{x}^H \mathbf{x} + \sum_{k=1}^{N} \Delta_k x_k x_k^* + \sum_{k=0}^{N} x_k^* z_k. \tag{2.3}$$

For simplicity, let $x_k x_k^* = 1$. The linear least squares estimate is given by,

$$\begin{aligned} \tilde{h}_N &= \frac{1}{N+1} \mathbf{x}^H \mathbf{y} \\ &= h_N + \frac{1}{N+1} \sum_{k=1}^{N} \Delta_k + \frac{1}{N+1} \sum_{k=0}^{N} x_k^* z_k. \end{aligned} \tag{2.4}$$

The error in estimating h_N thus arises from two factors: One due to temporal channel variation and the other due to additive noise component. Our goal is to find the optimum training length that provides the best trade-off between these two error types. This is equivalent to minimizing the average of $|\tilde{h}_N - h_N|^2$. To achieve this we first try to find a tractable form of the mean square error (MSE),

$$
\begin{aligned}
&\mathbf{E}|\tilde{h}_N - h_N|^2 \\
&= \mathbf{E}\Big[\Big(\tilde{h}_N - h_N\Big)\Big(\tilde{h}_N - h_N\Big)^*\Big] && (2.5) \\
&= \frac{1}{(N+1)^2}\mathbf{E}\Bigg[\Bigg(\sum_{k=1}^{N}\Delta_k\Bigg)\Bigg(\sum_{k=1}^{N}\Delta_k^*\Bigg)\Bigg] \;\; + \frac{\sigma_z^2}{N+1}, && (2.6)
\end{aligned}
$$

where σ_z^2 is the noise variance and $\mathbf{E}$ is the expectation operator. The expectation of the cross-product terms is 0 because we assume that the noise is zero mean and is independent of channel coefficients. To evaluate $\mathbf{E}|\tilde{h}_N - h_N|^2$, we first evaluate the expectation in the first term in (2.6). We use the approach similar to [21]. We assume the channel as frequency flat fading with a diffuse scattering channel model, which lends itself mathematical tractability. The following theorem summarizes our result.

Theorem 1. *Define $\Delta_k = h((N-k)T_s) - h(NT_s)$. $h(t)$ is the channel modeled as follows,*

$$h(t) = \sum_{k=1}^{S}\beta_k e^{j2\pi f_k t}, \tag{2.7}$$

where S is the number of scatterers, β_k and f_k are the complex amplitude and Doppler frequency of the k^{th} multipath respectively and T_s is the symbol period, with the following assumptions.

1. *β_k are independent zero mean random variables, and normalized such that $\sum_{k=1}^{S}|\beta_k|^2 = 1$.*
2. *f_k are i.i.d. distributed uniformly on the interval $[-f_D, f_D]$.*
3. *β_k and f_k are independent of each other.*

Then, (See Appendix A)

$$
\begin{aligned}
&\mathbf{E}\Bigg[\Bigg(\sum_{k=1}^{N}\Delta_k\Bigg)\Bigg(\sum_{k=1}^{N}\Delta_k^*\Bigg)\Bigg] \\
&= N(N+1) - \frac{\sin(\pi f_D N T_s)\sin(\pi f_D (N+1) T_s)}{\pi f_D T_s \sin(\pi f_D T_s)}. && (2.8)
\end{aligned}
$$

Therefore, putting (2.8) in (2.6), we get

$$\begin{aligned}\mathbf{E}|\tilde{h}_N - h_N|^2 = & \frac{\sigma_z^2}{N+1} + \frac{N}{N+1} \\ & - \frac{\sin(\pi f_D N T_s)\sin(\pi f_D (N+1) T_s)}{(N+1)^2 \pi f_D T_s \sin(\pi f_D T_s)}.\end{aligned} \tag{2.9}$$

The above expression gives the MSE as a function of maximum Doppler spread, symbol period and number of training symbols. For a given Doppler spread and symbol time, we can find the optimal training length numerically. We consider the MIMO case in the following section.

A plot of MSE against the fraction of code block size used for estimation is given in Fig. 1 for $f_D T_s = 1.25 \times 10^{-4}$, where f_D is the maximum Doppler spread and T_s is the symbol period.

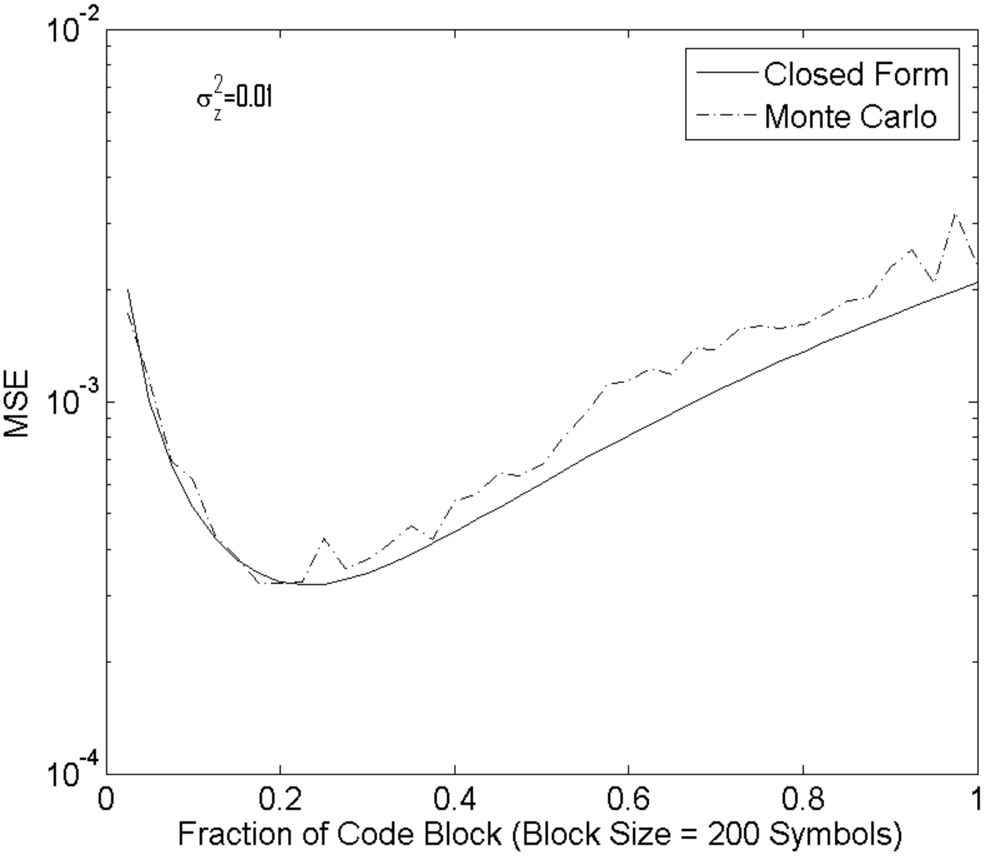


Fig. 1: Behavior of MSE of SISO channel for $f_D T_s = 1.25 \times 10^{-4}$ with block length of 200 symbols

2.2.2 Multiple Input Multiple Output Case

Consider a MIMO system with t transmit antennas and r receive antennas. We assume the following channel model, $\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{z}$, where $\mathbf{x}$ is the $t \times 1$ transmitted vector, $\mathbf{y}$ is the $r \times 1$ received vector, $\mathbf{H}$ is the $r \times t$ channel matrix and $\mathbf{z}$ is the $r \times 1$ noise vector. We assume the noise to be complex Gaussian with zero mean and covariance matrix equal to the identity matrix.

Let the transmitter send $N+1$ symbol vectors in $N+1$ time slots. The $N+1$ transmitted symbols from one antenna are orthogonal to that of other transmit antennas.

$$\begin{aligned}
\mathbf{y_N} &= \mathbf{H_N x_N} + \mathbf{z_N}, && (2.10)\\
\mathbf{y_{N-1}} &= \mathbf{H_{N-1} x_{N-1}} + \mathbf{z_{N-1}} \\
&= \mathbf{H_N x_{N-1}} + \mathbf{\Delta_1 x_{N-1}} + \mathbf{z_{N-1}}, && (2.11)\\
&\vdots \\
\mathbf{y_0} &= \mathbf{H_0 x_0} + \mathbf{z_0} \\
&= \mathbf{H_N x_0} + \mathbf{\Delta_N x_0} + \mathbf{z_0}. && (2.12)
\end{aligned}$$

The MSE in estimating $\tilde{\mathbf{H}}_N$ can be given as follows,

$$\begin{aligned}
\mathbf{E}||\tilde{\mathbf{H}}_N - \mathbf{H}_N||_F^2 &= \mathbf{E}\sum_{i,j}\left|\tilde{h}_N^{(i,j)} - h_N^{(i,j)}\right|^2 && (2.13)\\
&= \sum_{i,j}\mathbf{E}\left|\tilde{h}_N^{(i,j)} - h_N^{(i,j)}\right|^2 && (2.14)\\
&= rt\,\mathbf{E}\left|\tilde{h}_N^{(1,1)} - h_N^{(1,1)}\right|^2. && (2.15)
\end{aligned}$$

$h_N^{(i,j)}$ is the channel coefficient between the i^{th} receiver antenna and the j^{th} transmitter antenna of $\mathbf{H_N}$. The third equality is because all the elements are assumed i.i.d. The expectation in (2.15) can be reduced to that in expression (2.9).

Therefore, we can write the MSE as

$$\begin{aligned}&\mathbf{E}||\tilde{\mathbf{H}}_N - \mathbf{H}_N||_F^2\\&= rt\left(\frac{\sigma_z^2}{N+1} + \frac{N}{N+1}\right.\\&\left.-\frac{\sin(\pi f_D N T_s)\sin(\pi f_D (N+1)T_s)}{(N+1)^2 \pi f_D T_s \sin(\pi f_D T_s)}\right).\end{aligned} \tag{2.16}$$

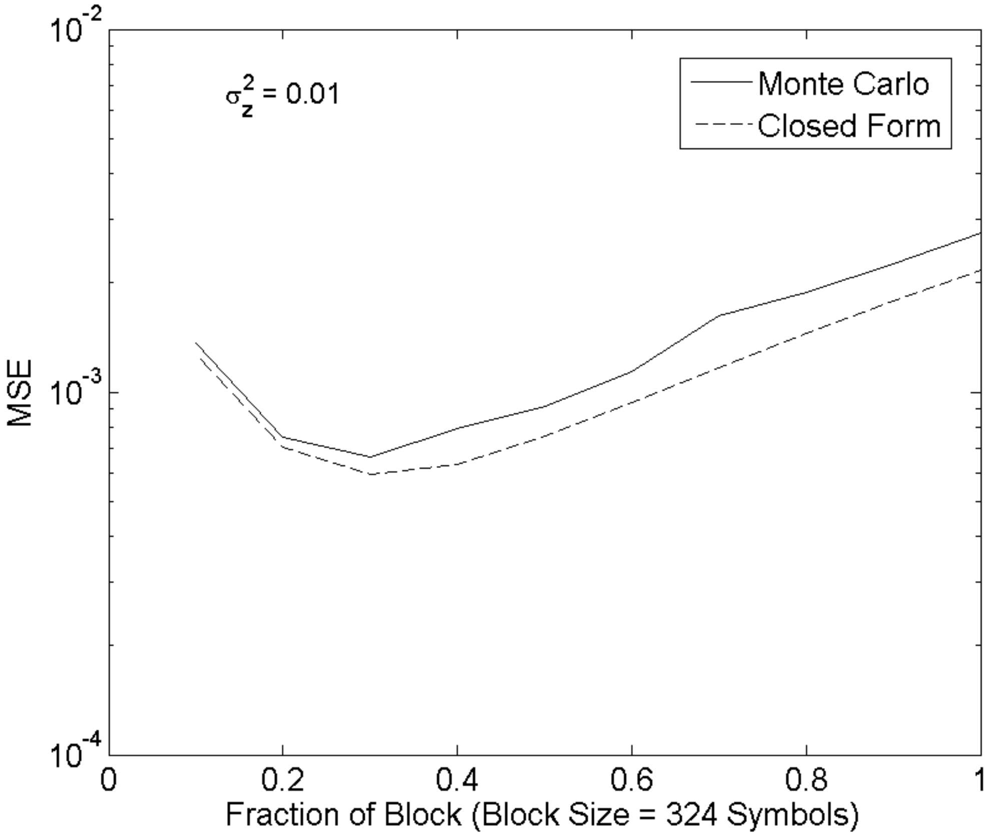


Fig. 2: Behavior of MSE of a 4×4 channel for $f_D T_s = 7.72 \times 10^{-5}$ with block length of 324 symbols.

From Fig. 2 we see that for about 30 percent of a code block of length 324 symbols, lowest MSE is achieved for $f_D T_s = 7.72 \times 10^{-5}$. We can use this as a guideline to set the length of symbols in our tracking algorithm. The tracking algorithm is explained in Section 2.4.

Fig. 3 shows the MSE for our channel tracking algorithm. For a setup similar to above, the lowest MSE for channel estimation is achieved when only about 30 percent of code block is used.

The next section gives a brief explanation of the D-BLAST architecture and then the channel tracking algorithm.

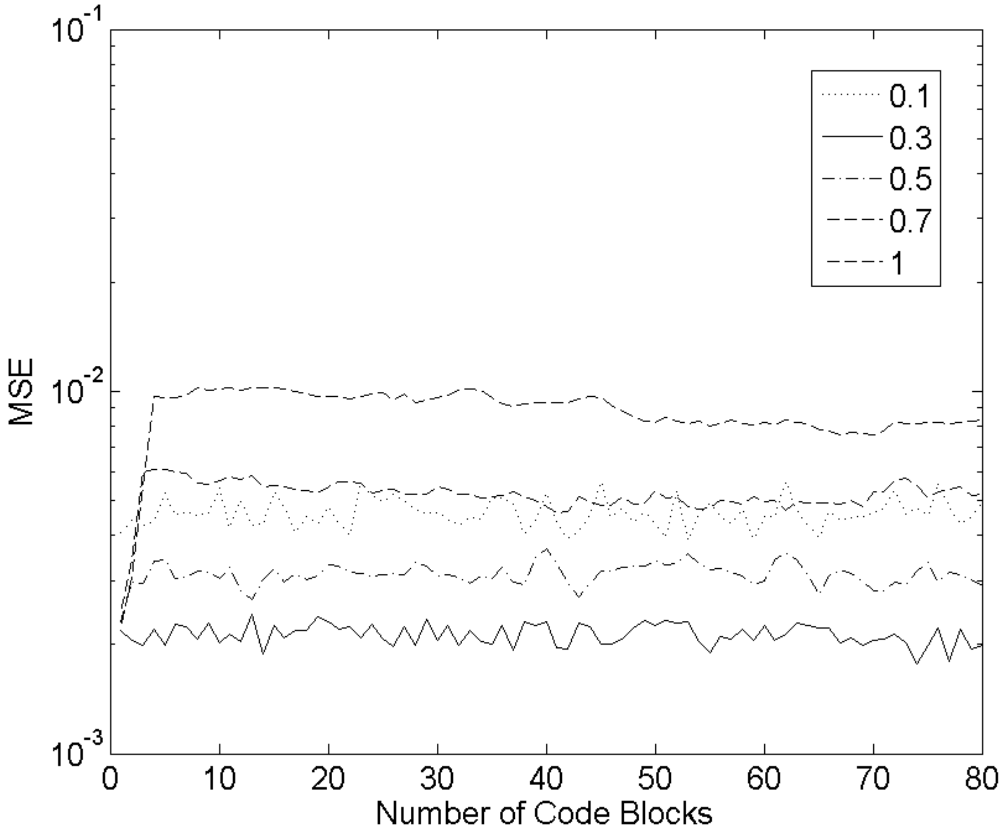


Fig. 3: 4×4 D-BLAST tracking MSE w.r.t sub-blocks for $f_D T_s = 7.72 \times 10^{-5}$.

2.3 D-BLAST Architecture

D-BLAST stands for Diagonal Bell Labs Layered Space Time architecture. It is a transceiver architecture for MIMO systems [6]. For an $r \times t$ (r receive antennas and t transmit antennas) MIMO system, the input data stream is demultiplexed into t streams. We call each demultiplexed stream as a sub stream. The t sub streams are then independently coded and modulated. These t sub streams are then transmitted over the t transmit antennas. However, the association between the sub streams and the antennas is changed in a periodic manner. Each sub stream is rotated through the t transmit antennas during one code block duration. This results in diagonal layering of the sub streams across the antennas and time. At the receiver end, decoding happens one layer at a time. Because of the diagonal structure, each sub stream sees channels from all the transmit antennas and hence has improved diversity compared with V-BLAST [8]. This results in spreading out the errors, in the event that one of the links has a bad channel condition, thereby minimizing the probability of outage. The diagonal structure renders D-BLAST as an outage optimal scheme in slow fading environments [28].

2.4 Channel Tracking

For the sake of illustration we describe our scheme for a 2×2 MIMO system. It can be extended to any $q \times q$ MIMO system in a straightforward manner. The symbol space-time diagram is shown in Table 1. The stream of symbols $\mathbf{x}_{ij}$ denote that they belong to stream i and are transmitted during the j^{th} time block. t_k and a_k denote the time block and antenna number respectively, over which the indexed symbols are transmitted. We use the q^{th} time block abstraction to indicate the time duration during which the transmitter keeps the association between the streams and the antennas constant. $\mathbf{p}$ indicates pilot symbols. l_i denotes i^{th} layer. For example: $x_{11}x_{12}$ is 1^{st} layer, $x_{21}x_{22}$ is 2^{nd} layer and so on.

	t_0	t_1	t_2	t_3	$\dots$
a_1	$\mathbf{p}_{a_1}$	$\mathbf{x}_{11}$	$\mathbf{x}_{21}$	$\mathbf{x}_{13}$	$\dots$
a_2	$\mathbf{p}_{a_2}$	$\mathbf{p}_{a_2}$	$\mathbf{x}_{12}$	$\mathbf{x}_{22}$	$\dots$

Table 1: Symbol Space-Time Diagram

Let $\mathbf{Y}_i$ and $\mathbf{X}_i$ be the received and transmitted set of vector in time block i. We assume that we already have the initial channel estimate $\hat{\mathbf{H}}_0$, found during time block $t_0$using the pilots $\mathbf{p}_{a_1}$ and $\mathbf{p}_{a_2}$ as shown in previous section. We also assume that the pilot $\mathbf{p}_{a_2}$ has been subtracted out from the received vector during t_1.

In this scheme, we use the initial estimate $\hat{\mathbf{H}}_0$ to detect $\mathbf{x}_{11}$ and $\mathbf{x}_{12}$. The receiver then decodes, re-encodes and performs baseband modulation to reconstruct $\hat{\mathbf{x}}_{11}$ and $\hat{\mathbf{x}}_{12}$. $\hat{\mathbf{x}}_{11}$along with $\mathbf{p}_{a_2}$ are used to find a new estimate $\hat{\mathbf{H}}_1$ of the channel. The tensor product of $\hat{\mathbf{x}}_{12}$ and its corresponding channel vector from $\hat{\mathbf{H}}_1$ is then subtracted from $\mathbf{Y}_2$, where $\mathbf{Y}_2$ is the channel output during the time block t_2. This new channel estimate $\hat{\mathbf{H}}_1$ is then used to detect the next layer i.e., $\mathbf{x}_{21}$ and $\mathbf{x}_{22}$, and the process is repeated.

2.5 Simulation

2.5.1 Channel Tracking

For simulation purposes we consider a 4 x 4 MIMO system with a Rayleigh fading channel. For error control coding we use an LDPC (Low Density Parity Check) code of block length 1944. The bit streams are then modulated by 4-quadrature amplitude modulation (QAM) modulators. We show simulation results for 2 cases of channel variations and 2 cases of code rates.

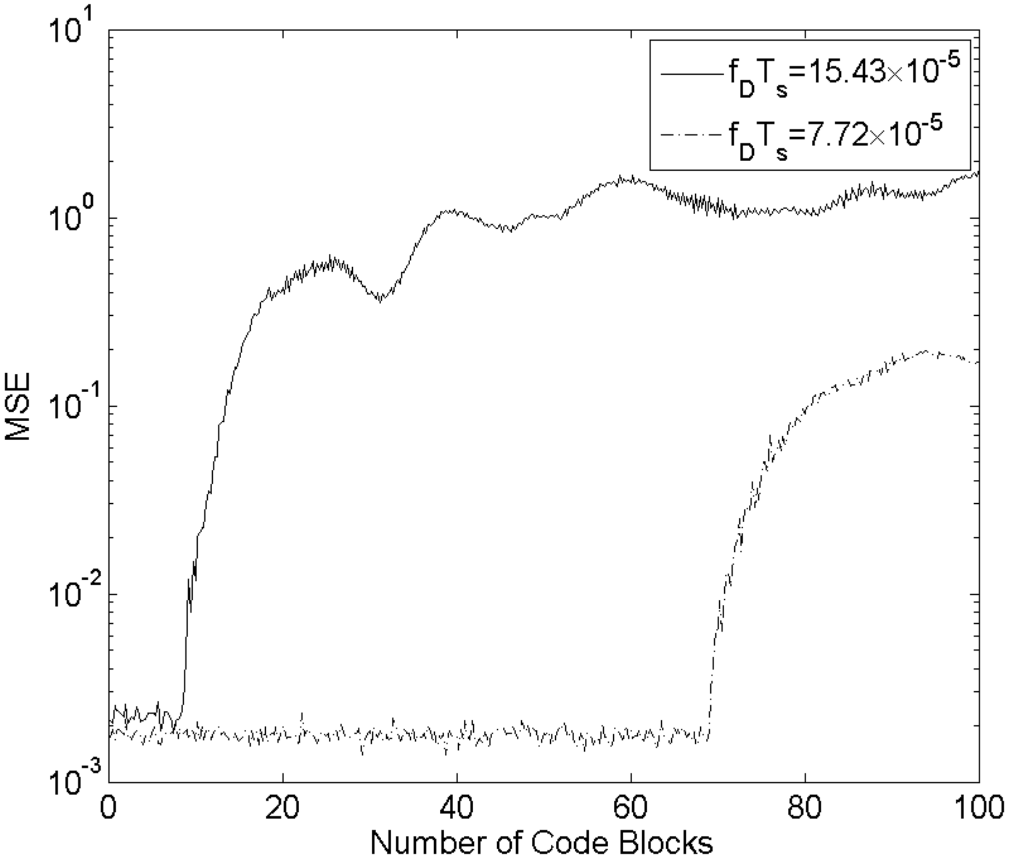


Fig. 4: Behavior of channel estimation mean square error with increasing number of code blocks

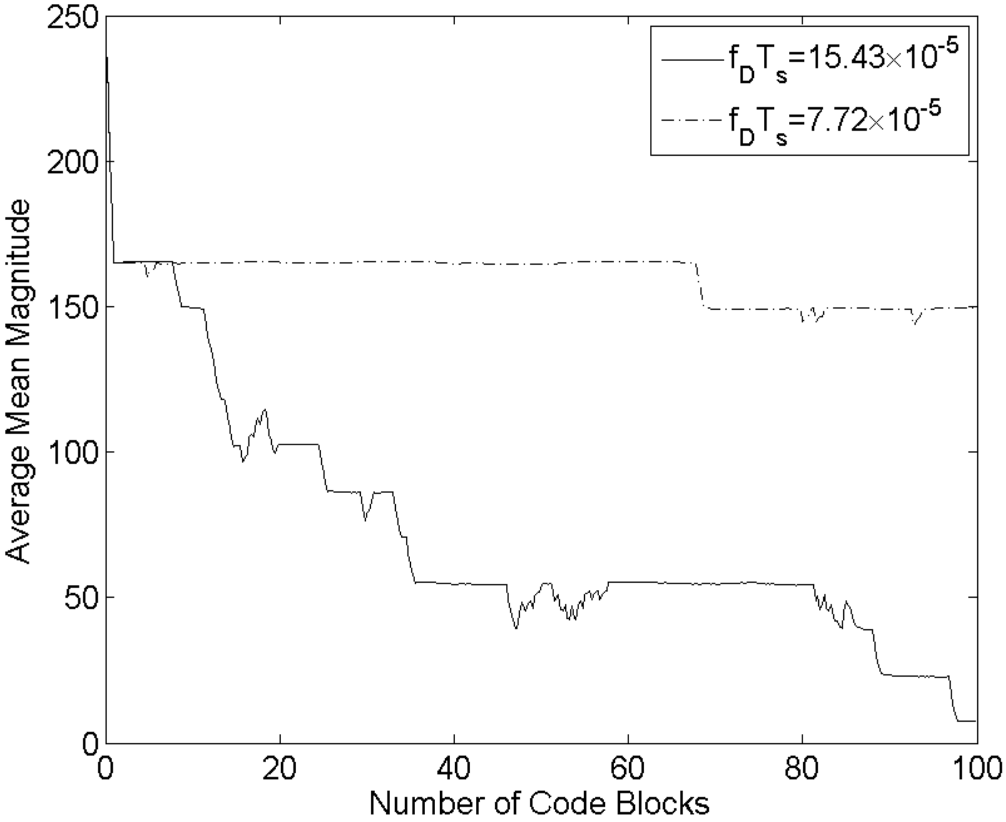


Fig. 5: Behavior of the mean magnitude of LLR of decoded LDPC code with increasing number of code blocks

We can see that for a faster varying channel, the algorithm loses track very early. The sudden jumps in MSE in Figure 4 indicate loss of channel tracking. They correspond to a sudden change in the mean magnitude of LLRs of decoded LDPC codes in Figure 5. We can use these sudden changes to detect outage at the receiver.

2.5.2 Outage Detection

During the tracking process, decoding errors may occur. The incorrectly decoded codeword will lead to an inaccurate channel estimate. In order for the receiver to detect this, and thereby tell the transmitter to reinitialize the transmission, we use the mean magnitude of LLRs of LDPC codes [16]. We found through simulations (see Fig. 6) that the mean magnitude of LLRs of correctly

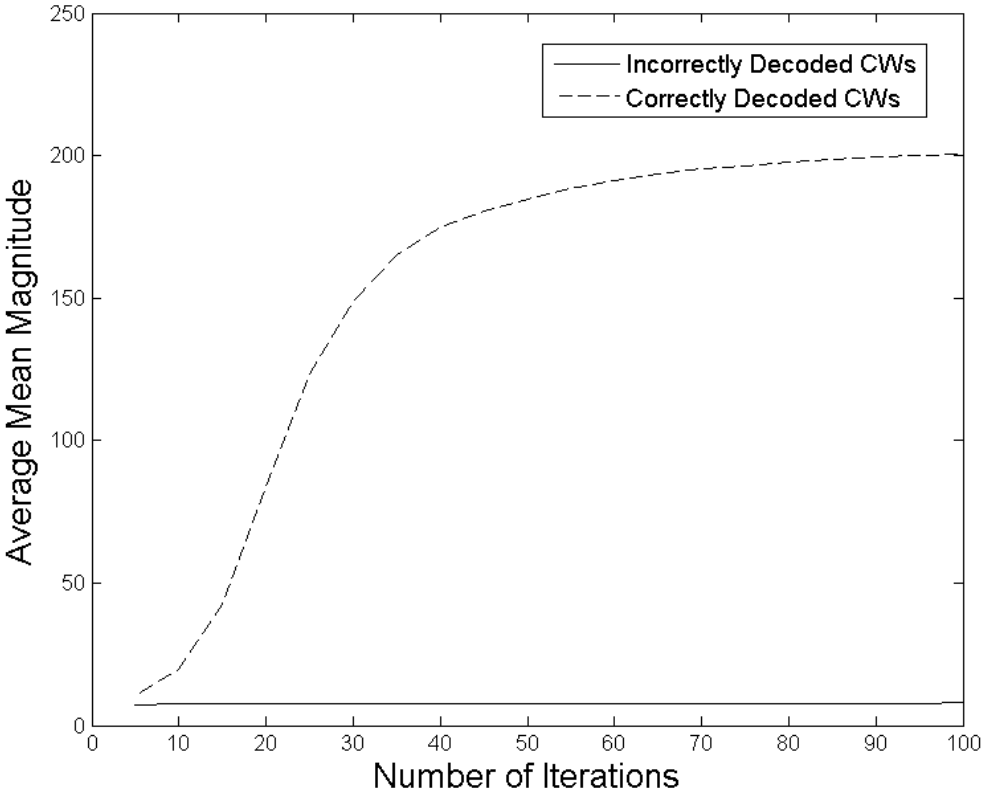


Fig. 6: Behavior of Average Mean Magnitude of Log Likelihood Ratios for an LDPC code with $N = 648$ and $R = \frac{1}{2}$

decoded LDPC codes increases with the number of message passing iterations. In comparison, for incorrectly decoded codewords, the mean magnitude remains constant at some small value. We can use this property to detect the loss in tracking. Loss in tracking results in incorrectly decoded codewords or vice versa, thereby resulting in smaller mean magnitude of the LLRs. Using a threshold detector we can detect this loss in tracking and thus detect outage.

2.6 Summary

In this chapter we studied channel tracking for a D-BLAST communication system using payload data. Since the tracking involves using previously detected data symbols, a closed-form expression for channel MSE as a function of the number of training symbols, maximum Doppler spread and symbol duration was derived for a SISO link in a diffuse scattering environment. This expression was then extended to MIMO links. We use this analysis to find the optimum length of previously detected symbols for channel tracking. In the event the receiver loses track of the channel, we show, using simulations, that using the mean magnitude of log likelihood ratios of LDPC codes can detect the event of a decoding error, which in turn can be used to detect outage.

CHAPTER 3

VARIABLE RATE MIMO

3.1 Introduction

The use of autonomous/unmanned vehicles for various civilian and military applications has become increasingly prevalent. The absence of human pilots on board those unmanned systems, however, make it a challenging task to accomplish various intended missions. For example, these unmanned systems are often remotely piloted and thus having a reliable and robust communication link between the aerial systems and the ground control unit is imperative. Even for systems that are semi-autonomous, having a high throughput communication link is often essential to accomplishing any intended mission. Many remotely piloted aircrafts (RPAs) are used for surveillance applications and the need to stream surveillance data, including real time video data requires a highly reliable and high-throughput communication link from the RPAs to ground units.

Many legacy communication links (e.g., Link 16 with a data rate not more than 16kb/s) operate at a data rate that becomes highly inadequate for applications where video streaming from aerial systems to ground is needed. Merely scaling up the power/bandwidth is both limited by resource and policy constraints as well as the fundamental theoretical limits dictated by the Shannon theory. A promising technology is the use of multiple antenna communication systems [6, 7, 27]. The so-called multiple-input multiple-output (MIMO) communication scales up data rate linearly as the number of antennas increase and thus provides great potential for improving the throughput of air to ground communication. This helps enable many envisioned applications that may otherwise be infeasible.

MIMO communications, however, are traditionally designed for the so-called scattering environment [28] where independent channel variations between different transmit/receive antenna pairs are exploited. For airborne platforms, however, there has been a debate about the feasibility of MIMO communications because of the lack of scattering. However, for certain communication ranges, the large aperture that an aircraft affords makes MIMO an appealing choice of communication that can attain significantly higher throughput given a fixed power/bandwidth budget compared with single antenna systems even in the absence of any scatterers [9].

This chapter describes an ongoing research and development effort that uses MIMO communications to enable robust and high capacity connectivity between RPAs and ground terminals. While the large aperture may compensate for the lack of the scattering, two unique challenges still exist for airborne MIMO communications. The large aperture is only attained when antennas are placed strategically apart on a RPA. In the absence of scattering, i.e., when communications are limited by line-of-sight channels, the fact that some antenna elements on a RPA may be completely out of sight from its communicating party may render the channel matrix ill-conditioned. This is further complicated by the high mobility and maneuverability of the RPA which make it infeasible to have complete channel state information (CSI) at the transmitter. To address these challenges, we propose a variable rate MIMO communication scheme that combines the D-BLAST architecture with per antenna spreading to harvest the maximum possible throughput gain allowed by the channel.

The chapter is organized as follows. Section 3.2 describes the channel measurement apparatus. The measurement data provides guidance on the potential throughput gain for the particular application of interest as well as challenges in realizing the throughput gain to address these challenges. Section 3.3 introduces a modified D-BLAST architecture to address these challenges. Section 3.4 describes simulation results using the real measurement channels to show the potential improvement using the proposed variable MIMO scheme. Section 3.5 reports the experimental efforts and results.

We use the following notations throughout the chapter: * denotes complex conjugate, $\mathcal{CN}$ stands for complex Gaussian, ^{T} is transpose, $^+$ is conjugate transpose, $\mathbf{0}$ is a zero vector and $\mathbf{I}_k$ is a $k \times k$ identity matrix. Small letters denote scalars, bold small letters denote column vectors and bold uppercase letters denote matrices.

3.2 MIMO Channel State Matrix Measurements

3.2.1 Measurement Apparatus

The process of measuring the channel state matrix at the Newport NY radio range required measuring the complex transmission coefficient from each antenna element on the ground array to each element on the unmanned combat air vehicle (unmanned combat air vehicle (UCAV)) model of a remotely piloted aircraft (RPA). The UCAV is shown in Fig. 7.

The UCAV model was coated with Electrodag to shield the cable networks placed inside the model that connect the patch antennas to the switch which feeds the RF (Radio Frequency) receiver. Although this shielding is not necessary in an operational RPA, it helps, in analyzing the measurements, to restrict the received signals to the patch antennas only. Four patches were installed for the uplink band (at carrier frequency 5.1 GHz with a bandwidth of 100 MHz) and four patches for the downlink band (at carrier frequency of 5.8GHz with a bandwidth of 100 MHz). Each patch has two ports which provide perpendicular linear polarization with about 30 dB cross polarization discrimination (isolation between ports). Thus 8 antenna ports are provided for the uplink and for the downlink, respectively. For easy reference these ports are uniquely labeled. For example, RU12 represents the second port on the first uplink patch on the upper side of the UCAV. The antenna patterns were measured on the Newport Range. Two such power patterns are shown in Fig. 8(a) and 8(b).

The power pattern for antenna RU11 gives pretty good coverage above the UCAV because it

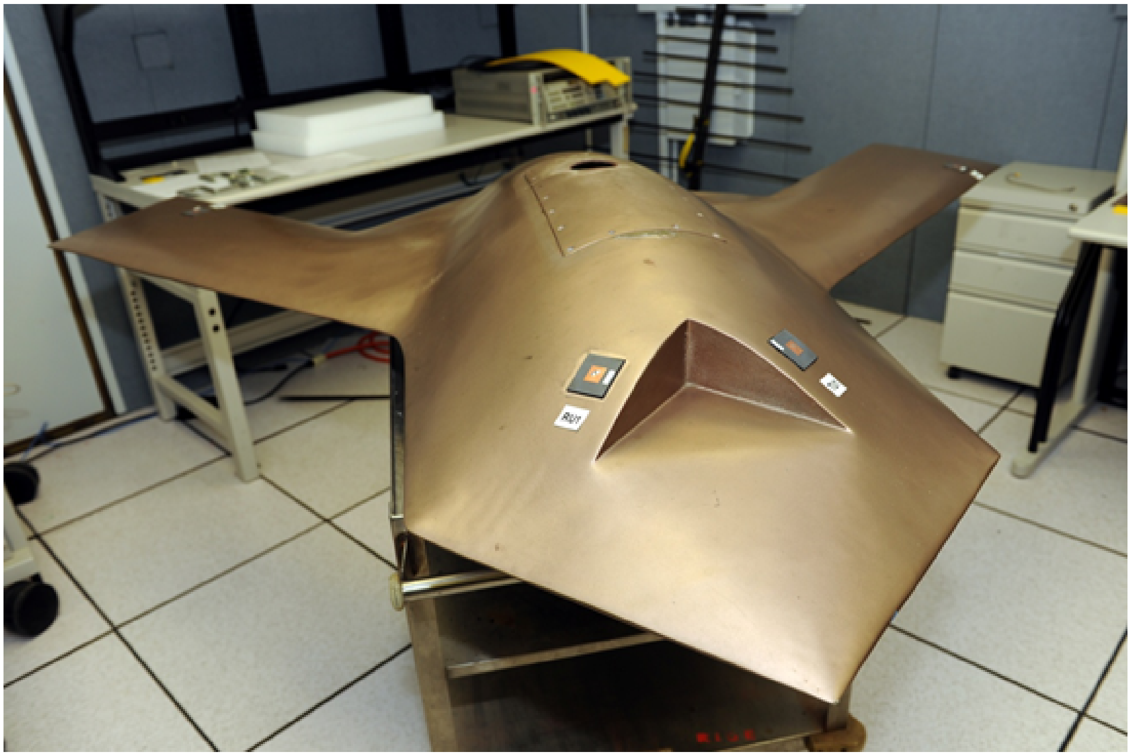
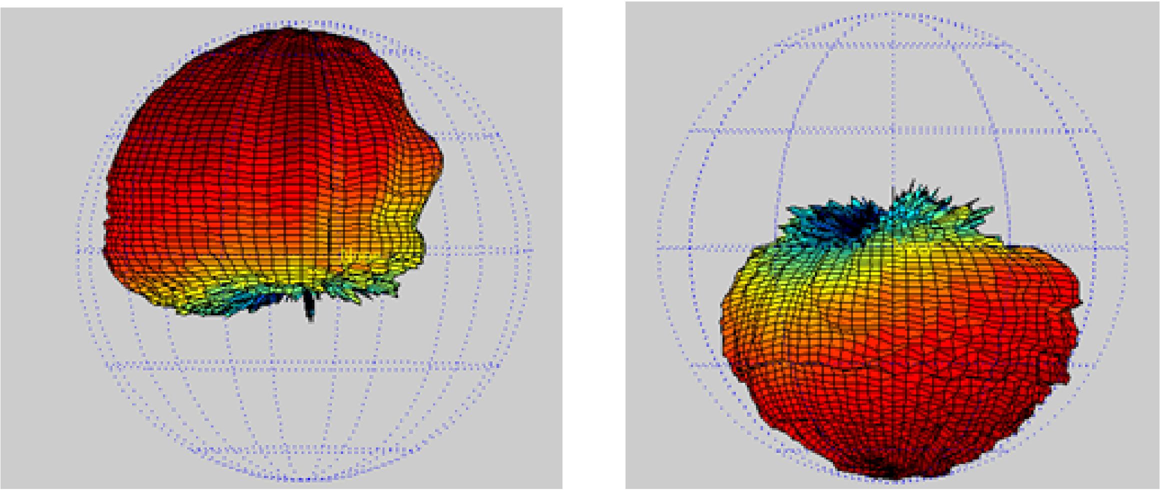


Fig. 7: UCAV with square patch antennas.

is on the upper surface of the UCAV. Antenna RL31 is on the bottom surface of the UCAV wing and has good coverage in the hemisphere below the UCAV but is weak above the UCAV. These patterns emphasize the need for the D-BLAST (Diagonal Bell Labs Layered Space Time) [6] form of MIMO in order to provide full coverage for all data streams.

The ground array utilizes coax-to-waveguide adapters as antenna elements. They provide wide angular coverage (110^o E-Plane and 80^o H-Plane) and wide bandwidth 4.9 GHz to 7.05GHz. The array is mounted with square plates as shown in Fig. 9. The square plates allow a choice of vertical or horizontal polarizations. Typically measurements are made with all vertically polarized antenna elements or with polarizations alternated between vertical and horizontal polarization to see the effect of polarization mixing on MIMO capacity. The elements can be at various spacing by bolting the plates to different positions along the mounting rails. The spacing shown in Fig. 9(c) provide an 80 inch wide array. Another test used a 30 foot wide array. The array is mounted on an expanding tower which allows array heights of 2 feet to 40 feet above ground level.

The UCAV is mounted on a positioning tower at a height of 70 feet. The position of the UCAV



(a) Antenna RU11 (b) Antenna RU31

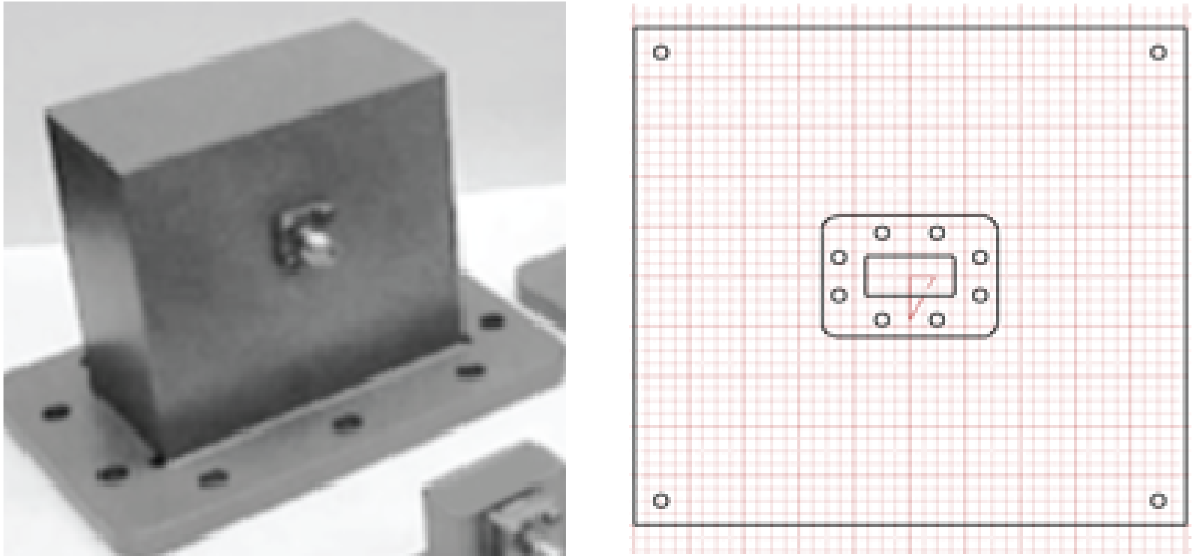
Fig. 8: Antenna Pattern

can be rotated around a vertical axis (relative to ground) for 360 degrees of azimuth. It can also be rotated in pitch and roll over in the range $[-90°, 90°]$. The UCAV support is provided by an absorber covered arm from the top or bottom of the UCAV. A view of the 400 foot range at Newport showing the UCAV and the ground array is shown in Fig. 10. It is seen that the range is relatively free of scattering, so that the MIMO performance should be similar to free space limitations.

The switch at the ground array cycles through the 8 elements in a 20 millisecond period. After each of the ground array cycles, the switch at the UCAV connects to a new antenna port of the 16 UCAV antenna ports (8 uplink and 8 downlink). As this switching is completed the azimuth turntable moves to a new position for a given pattern cut. At each position of the cut, the complex transmission coefficient from each antenna element on the ground array to each element port on the UCAV is recorded. The frequency and pitch and yaw positions can be modified for new cuts.

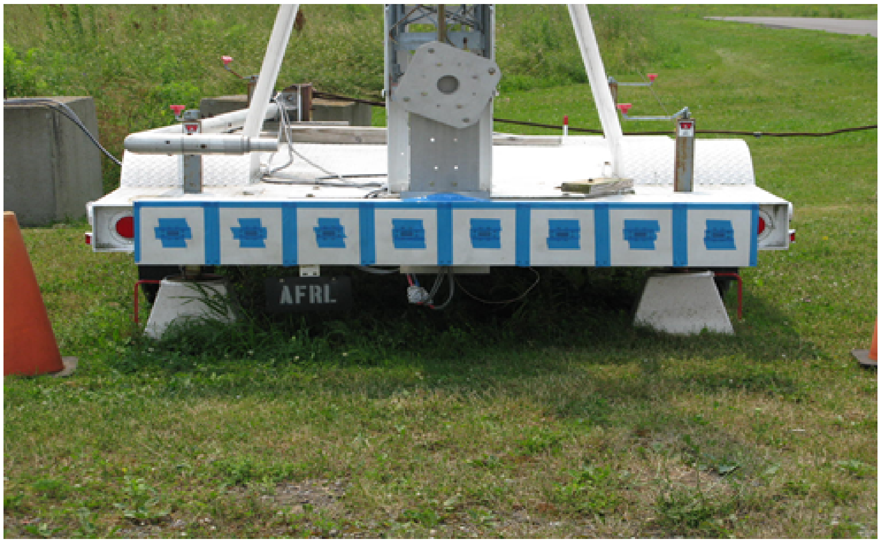
3.2.2 Challenges

Fig. 8(a) and 8(b) illustrate the unique challenges of airborne MIMO. Each antenna element has only limited visibility for communication, depending on the orientations of the transceiver pair. This is further exacerbated by the lack of channel state information at the transmitter - RPAs are not only of high mobility but they may maneuver in-flight which makes it infeasible to constantly



(a) Plate

(b) Plate Schematic



(c) Ground Array

Fig. 9: Element Ground Array

feedback channel state to the transmitter.

Nevertheless, the channel matrices indicate that there exists significant theoretical throughput improvement through MIMO communications if designed properly. In the following, we describe a simple variable rate MIMO scheme to address the above mentioned challenges. We demonstrate through numerical simulation that the proposed scheme is capable of overcoming the above challenges and realizing significant performance gain.

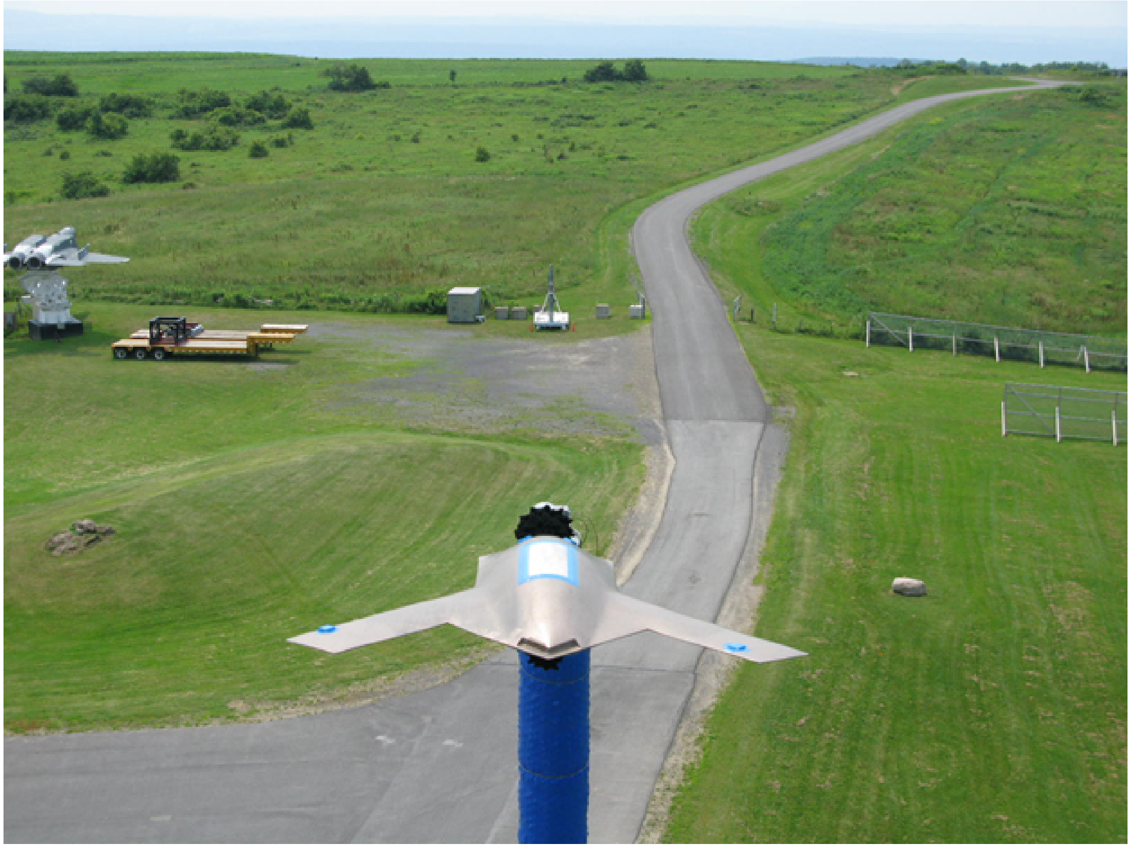


Fig. 10: UCAV and Ground Array on the 400 ft. Newport Range.

3.3 Variable Rate MIMO

While the channel matrix measurements exhibit potential for significant throughput improvement via MIMO communications, significant challenges exist that need to be overcome in order to realize this potential. In particular, the lack of scattering makes the channel susceptible to ill-conditioning when antenna elements may be out of sight to the communicating party. In the absence of complete channel state information (CSI) at the transmitter, there is a need to ensure that any independent data stream is not stuck with an antenna element that is out-of-sight. This makes D-BLAST a very natural candidate for such applications. D-BLAST is an outage optimal transceiver architecture for MIMO communication system [6, 28]. The architecture essentially involves independent coding and modulation of N data streams and rotating each stream through all the transmit antennas. Here, N is the number of transmit antennas. The rotation is performed in a way that makes sure that each stream experiences the channel from all the transmit antennas and all levels of interference *i.e.,* no interference to experiencing interference from all of the other $N-1$ streams at the receiver as each stream rotates in the space-time domain.

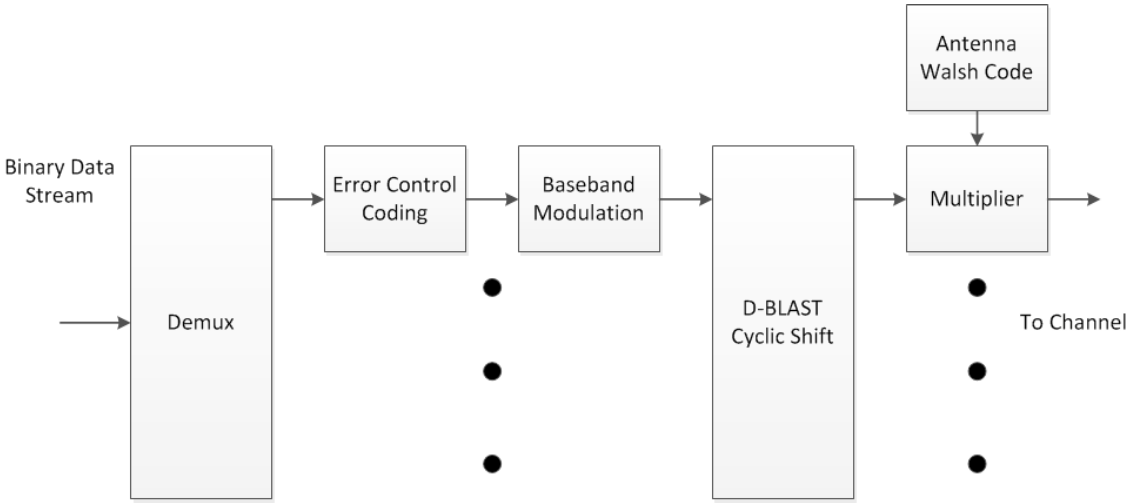
The verbatim application of D-BLAST, however, is still inadequate when channel matrices are highly ill-conditioned. The existence of antennas that experience channel outage due to blockage will drag down the overall performance. From a theoretical viewpoint, the independent data streams accommodated in a MIMO channel should be no larger than the effective rank of the matrix. The challenge is, in the absence of complete CSI at the transmitter, how to utilize the advantage of D-BLAST while being able to handle the potential rank deficiency of channel matrices.

We propose a simple scheme of variable rate MIMO - the variable rate is not only achieved though the traditional means of controlling the coding rate as well as modulation order, but the number of independent data streams is also adapted through per antenna spreading. The modified D-BLAST architecture is illustrated in Fig. 11. Without loss of generality, we assume the MIMO system has N transmit and N receive antennas. At the transmitter side, spreading is done on a per antenna basis with a length M Walsh code for each antenna where $M < N$. As such, a group of N/M antennas will share the same Walsh code and the effective number of data streams is reduced to N/M. At the receiver side, de-spreading is embedded in the D-BLAST receiver to facilitate successive interference cancellation.

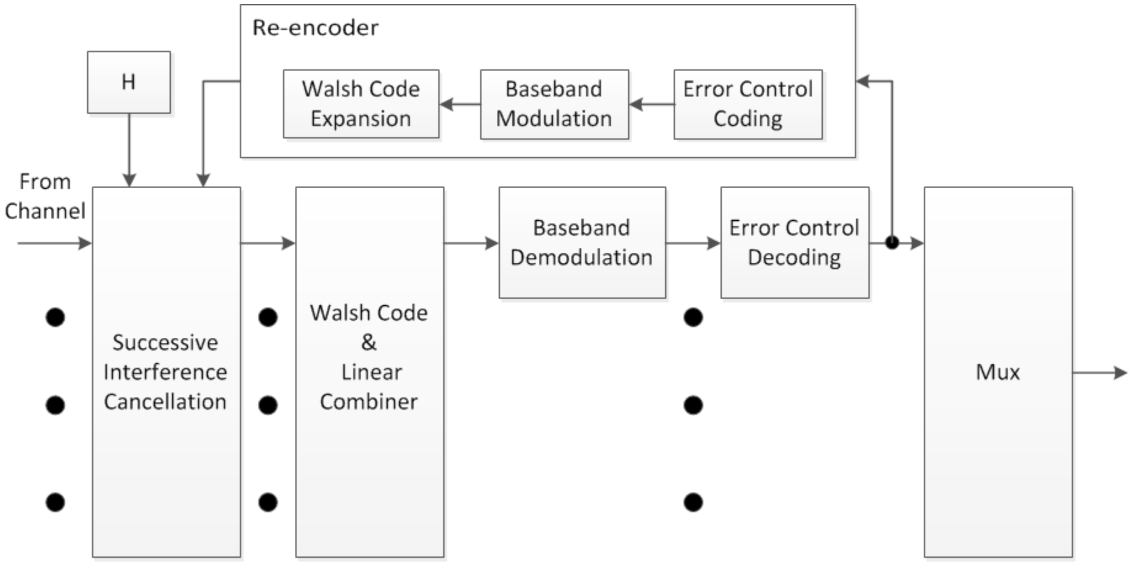
As an illustration, consider an 8×8 MIMO system. Let $a_0, a_1, \ldots, a_7$ denote the 8 transmit antennas. Let each symbol from any 4 antennas, say a_0, a_1, a_2, a_3 be spread by $[1\ 1]^T$. Similarly, let each symbols from the remaining 4 antennas, a_4, a_5, a_6, a_7 be spread using $[-1\ 1]^T$. Notice that $[1\ 1]^T$ and $[-1\ 1]^T$ are orthogonal to each other. At the receiver, de-spreading effectively reduces the number of mutually interfering streams from 8 to 4.

The illustration in the previous paragraph implicitly assumes that the transmitter and the receiver have agreed on some spreading factor, M, and the corresponding Walsh codes. As the transmitter does not possess any CSI, our assumption holds true only if there exists a very low rate feedback link from the receiver to the transmitter. The receiver, which knows the CSI, can feedback the spreading factor to the transmitter, which then can adapt the transmission strategy to the channel conditions. For example, in the 8×8 case, one needs a total of 2 bits for the spreading factor of 1 (no spreading), 2, 4, and 8 where the last one corresponds to essentially a beamforming strategy.

In the next section we simulate the variable rate MIMO scheme over measured channels to examine the performance of the proposed variable rate MIMO D-BLAST for low rank channels.



(a) Transmitter



(b) Receiver

Fig. 11: Variable rate MIMO transceiver block diagram

3.4 Simulation

We assess the performance of the variable rate D-BLAST scheme by comparing it with the original D-BLAST for the following two channel measurement configurations.

- All Vertical Polarization (VP).
- Mixed Polarization (MP).

As mentioned earlier, we are motivated to use VP and MP to see the effect of polarization mixing on MIMO capacity. The channels obtained using VP tend be rank deficient. On the other hand, channels obtained using MP tend to have a higher rank than that of VP. This is because the two polarizations effectively serve to create two orthogonal channels. This leads to more well-conditioned MP channel matrices than the corresponding VP ones.

For each of the above two configurations we have obtained about 13,000 channel measurements, each of which corresponds to a unique combination of azimuth and elevation. During simulation, we select 10% of the channels at random, and measure the average outage over these channels.

Fig. 12 compares the outage behavior of the variable rate D-BLAST scheme with the original D-BLAST at a fixed rate of 4 bits/s/Hz. The variable rate D-BLAST scheme uses a spreading factor of 2, QPSK modulation and $1/2$ rate LDPC code. While the D-BLAST scheme uses BPSK modulation and $1/2$ rate LDPC code. Clearly, at low outage probabilities, the variable rate D-BLAST scheme provides an signal to noise power ratio (SNR) gain of about 4 dB over the original D-BLAST.

Fig. 13, on the other hand, shows that the variable rate D-BLAST scheme is inefficient for mixed polarization channels. The original D-BLAST outperforms variable rate D-BLAST by about 6 dB SNR at low outage probabilities.

The above simulation results show that for the low rank channel matrices obtained by only vertical polarization, the variable rate D-BLAST scheme outperforms D-BLAST, while for well conditioned channel matrices, the original D-BLAST architecture suffices.

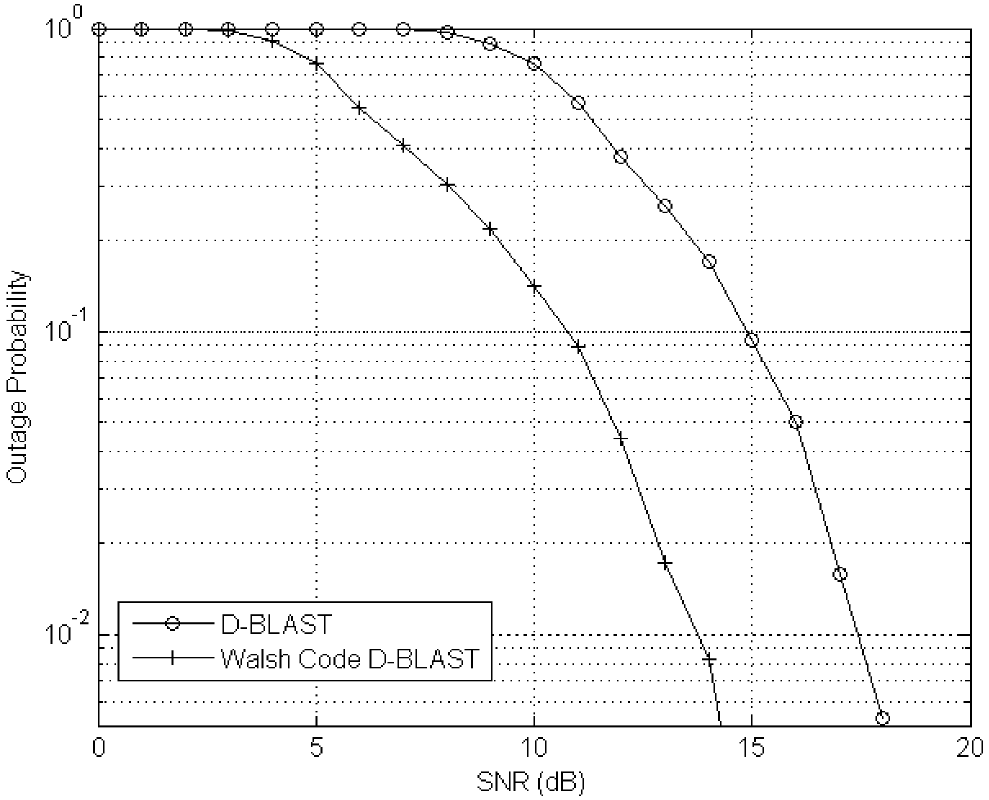


Fig. 12: Outage rate for all vertical polarization at rate 4 bits/s/Hz.

Next, we report the results of experimental investigation of the variable rate MIMO scheme.

3.5 Experiment

In this section we describe the experimental effort where a software defind radio implementation of the various rate MIMO system is developed. The software radio is implemented using the GNU Radio software radio toolkit [10] such that all the necessary signal processing components are developed using the toolkit. On the other hand, over the air transmission and reception is enabled by USRPs [29]. In this setup we use 4 USRPs - two of them configured as the two antenna MIMO transmitter as seen in Fig. 14(a) and the other two as the two antenna MIMO receiver as seen in Fig. 14(b). Thus, this setup allows us to perform experiments over a 2×2 MIMO system.

In the previous section we showed numerically that the variable rate MIMO scheme is more

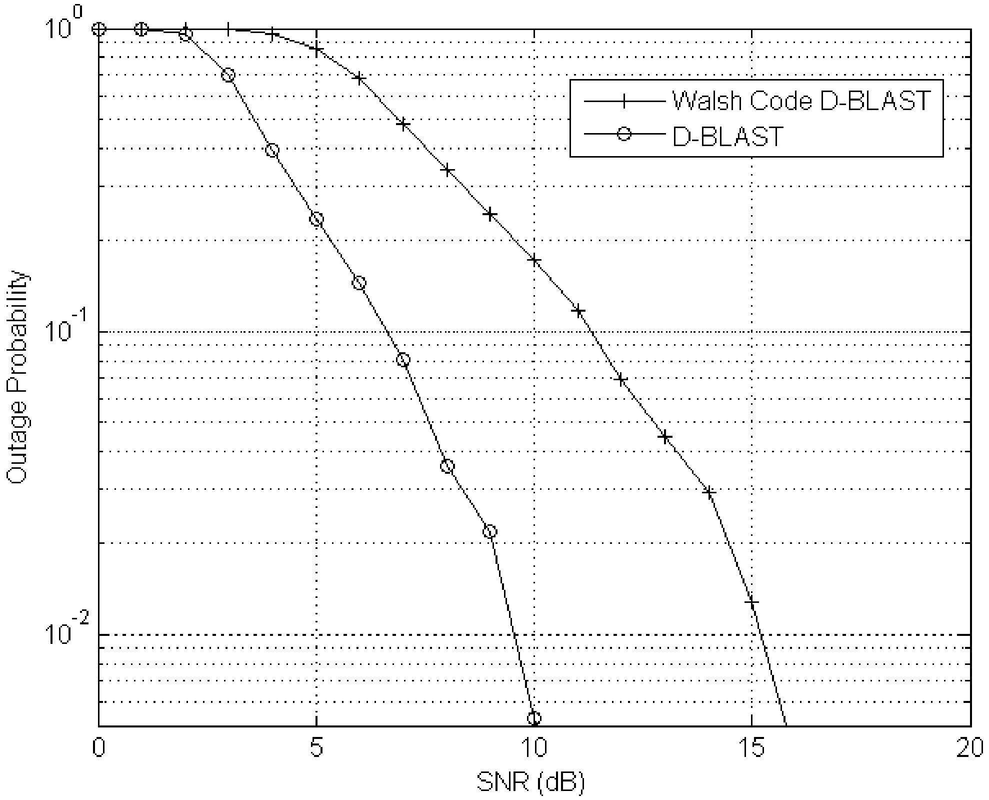
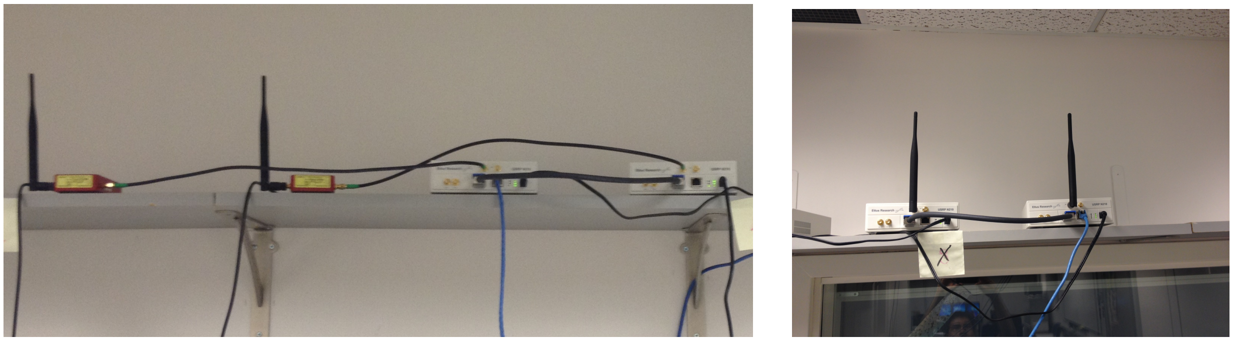


Fig. 13: Outage rate for mixed polarization at rate 4 bits/s/Hz.

effective in the presence of low rank channel conditions. Therefore, to demonstrate this experimentally, within the constraints of a laboratory setting, we have placed the transmitter and receiver such that there is a strong line of sight component between them. This ensures that the channel is rank deficient, thereby providing us with the opportunity to experimentally verify the effectiveness of the variable rate MIMO scheme as compared D-BLAST.

In the following text, we describe the design of the software radio sub-system followed by our observations.

Figs. 15 and 16 show the block diagram of the variable rate transmitter and receiver, respectively. At the transmitter a bit stream is split up into two sub-streams by the *De-Mux* block. Each of these sub-streams is then fed to the *Constellation Mapping* block which maps the incoming bits to complex valued constellation symbols. For our experiment, we use BPSK modulation and hence the *Constellation Mapping* block in this case simply maps the incoming bits to their respec-



(a) Transmitter (b) Receiver

Fig. 14: USRP Setup

tive BPSK symbols. The outputs of the mapping blocks are given to the *D-BLAST Cyclic Shift* block, which takes in the sub-streams and rearranges the symbols in the spatial and time domain to achieve diagonal layering. These D-BLAST formatted sub-streams are then subjected to spreading, if spreading is enabled. If spreading is disabled, the system acts as a D-BLAST transmitter. But if it is enabled, then each symbol in a sub-stream is spread using the Walsh code assigned to the respective antenna. In our case, when spreading is enabled, $[1, 1]$ is assigned to antenna 1 and $[1, -1]$ is assigned to antenna 2. After spreading, preamble symbols are multiplexed into each sub-stream for frame synchronization. A frame is defined as one D-BLAST coded block along with the preamble. These frames are then filtered using root raised cosine (RRC) filter [22] and then given to the USRPs for over the air transmission at the desired center frequency which is 2.45GHz in this case.

At the receiver, the *Symbol Timing Sync* blocks covert the incoming baseband samples to T-spaced samples. Only one sub-stream is fed to the *Preamble Detection* block as we insert the same preamble on all the sub-streams. This block detects the beginning of the frame, which is used by the following block to delineate the preamble and consequently perform carrier frequency offset (CFO) correction and channel estimation. At this stage, the preamble is stripped from the outgoing sub-streams. The CFO corrected output is then despread, if spreading is enabled, otherwise the *Despreading* block is bypassed. The output of this stage is then given to the D-BLAST decoder, which performs minimum mean squared error (MMSE) detection with successive interference cancellation (SIC).

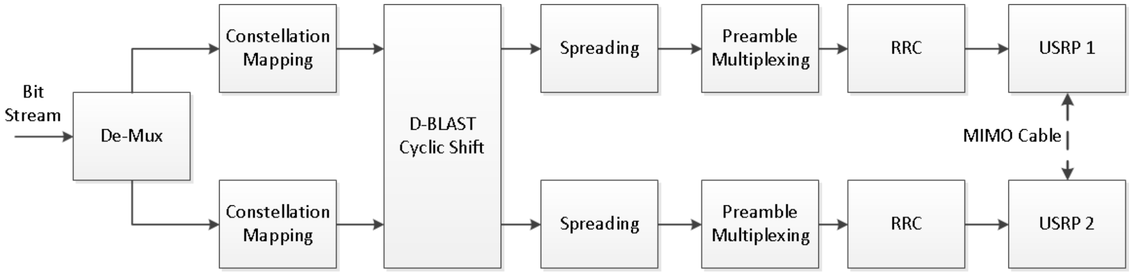


Fig. 15: Transmitter Block Diagram

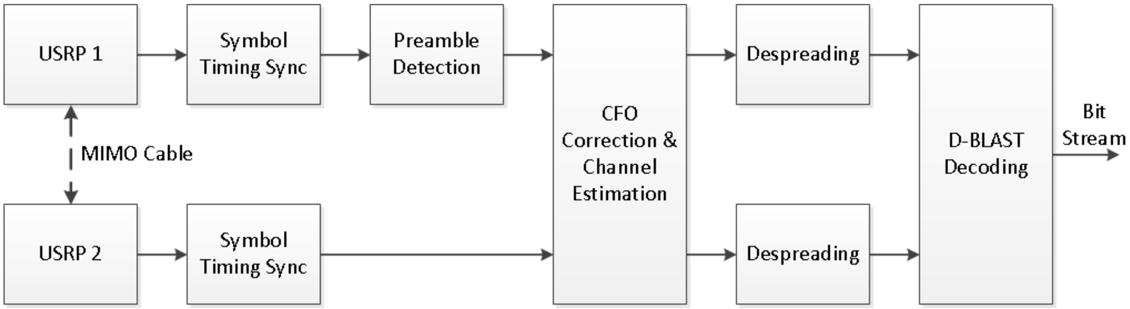


Fig. 16: Receiver Block Diagram

Fig. 17 plots the observed outage against the observed signal to noise ratio (SNR). Here, outage is defined as the event that error occurs in decoding a D-BLAST coded block. The variations in SNR are induced by means of digitally controlled attenuators connected between the antennas and their respective ports at the transmitter as shown in Fig. 14(a).

We notice that the outage decreases marginally for D-BLAST transmission (no spreading) in contrast to when spreading is enabled. This shows that in the presence of a strong line of sight component, i.e., rank deficient channels, the variable rate MIMO scheme performs better than D-BLAST.

3.6 Summary

In this chapter we introduced a new scheme to transmit data over MIMO channels which may be ill-conditioned. In the absence of channel state information at the transmitter the scheme overcomes this challenge by per antenna spreading in the D-BLAST architecture, thereby effectively

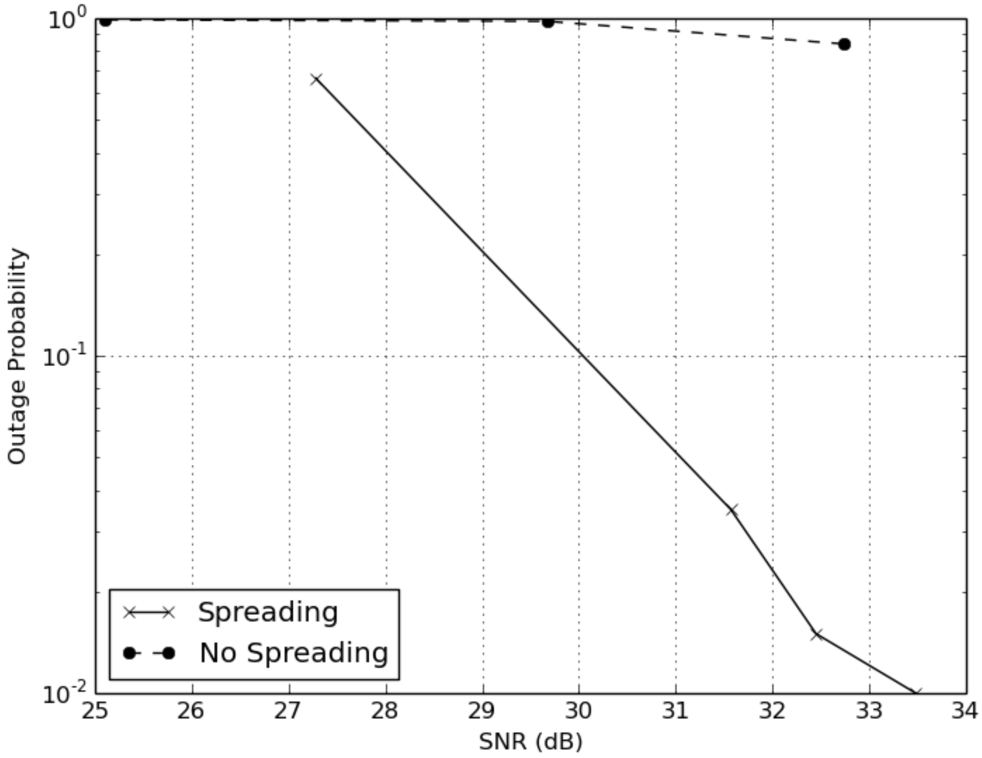


Fig. 17: Measured outage probability for 2×2 variable rate MIMO

reducing the number of independent data streams. Using real measurement channels we demonstrated through simulations that one can achieve significant SNR gain over the original D-BLAST for rank deficient channel matrices.

We developed a GNU Radio/USRP software defined radio framework based software radio to experimentally validate the analysis. The experiments show that the variable rate MIMO scheme outperforms D-BLAST in the presence of strong line of sight component, i.e., rank deficient channel matrices.

CHAPTER 4

PHYSICAL LAYER AUTHENTICATION FOR SPECTURM USAGE AUTHENTICATION

4.1 Introduction

In a typical cognitive radio (CR) system [18], a *primary user* (PU) is the spectrum license holder. A *secondary user* (SU) is an unlicensed user who intends to use the spectrum opportunistically. Priority is given to the PU in the sense that an SU can only transmit if its transmission is deemed to be harmless to that of the PU. Often times this is done through the policy that an SU is not allowed to transmit whenever the PU is transmitting, a premise adopted in this chapter. Consequently, it requires the SU to reliably detect the PU's transmission, which is typically done through either the simple energy detection or more sophisticated schemes involving transmission features of the PU [11, 13, 31]. These approaches, however, can often be compromised by a malicious *user* who may emulate the characteristics of the PU's signals.

Referred to as the primary user emulation attack (PUEA) [1], such an attack intends to mislead a benign SU into believing that the PU is transmitting, while in fact the PU is silent. This results in spectrum under-utilization, thereby defeating the purpose of CR. An effective countermeasure to PUEA is user authentication, *i.e.*, the SU is capable of authenticating the PU's transmission.

Contemporary authentication solutions exist in layers above the physical layer. For example, IP layer can use IPSec protocol to address the authentication problem, transport layer can use SSL, application layer can use SSH and so on. The problem with these solutions is that they need the PU and the SU to use the same protocol at the layer where authentication takes place and often require recovering at the SU information transmitted by the PU. In many existing and potential applications, the SU and the PU do not necessarily operate the same protocols at these higher layers. Furthermore, they may not even have the same layered network architecture. It is therefore desirable to achieve user authentication at the lowest possible layer. Physical layer authentication, first proposed in [30], appears to be an attractive solution.

The physical layer authentication scheme developed here is done in two stages: authentication tag generation using a one-way hash chain and tag embedding through constellation shift. The developed scheme is transparent to the primary receiver, requires minimum alteration of the primary transmitter, and allows simple detection scheme at the *SU*. Note that such a tag embedding scheme resembles that of digital watermarking where the embedded tag needs to induce minimum distortion of the cover signal [2]. It is not clear *a priori* what is the optimal way of generalizing the tag embedding scheme to more general digital constellations. Moreover, as the one-way hash chain is highly sensitive to tag bit error, it is imperative to carry out a thorough trade-off analysis such that the tag bit detection error probability can be controlled to be arbitrarily small under realistic wireless channel conditions.

4.2 A Physical Layer Authentication Scheme

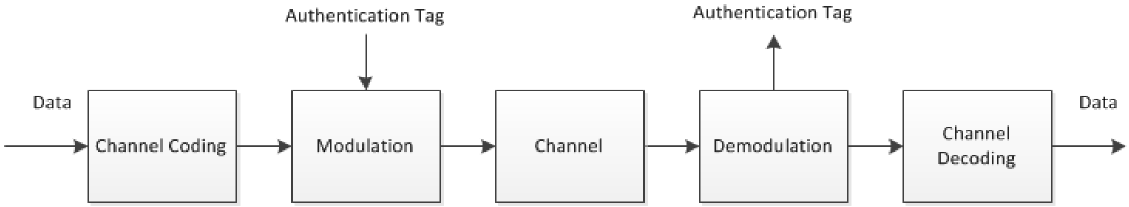


Fig. 18: Physical Layer Authentication.

Fig. 18 shows a high level communication block diagram between the PU and the SU. We piggyback the authentication **tag** at the PU on the modulated signal and then extract it at the SU for verification. This authentication mechanism can be logically divided into two stages: **tag generation** and **tag transmission**.

Tag generation, as the name suggests, deals with how tags are generated by the PU and then used at the SU for authentication. This process assumes that there is a reliable link between the PU and the SU over which tags are transmitted. The setting up of such reliable link is addressed by the tag transmission stage. Our work here focuses on this later part of the authentication mechanism wherein we describe and analyze the methodology we use to transmit and receive the authentication tag on the digitally modulated signal. In the following we provide brief overview of the two authentication stages.

4.2.1 Tag Generation

Tag generation is done using a one-way hash chain [26]. A hash chain is a successive application of a hash function to the input data [15].

A one-way hash function takes in a string of data and returns a fixed length string. It is characterized by the following properties.

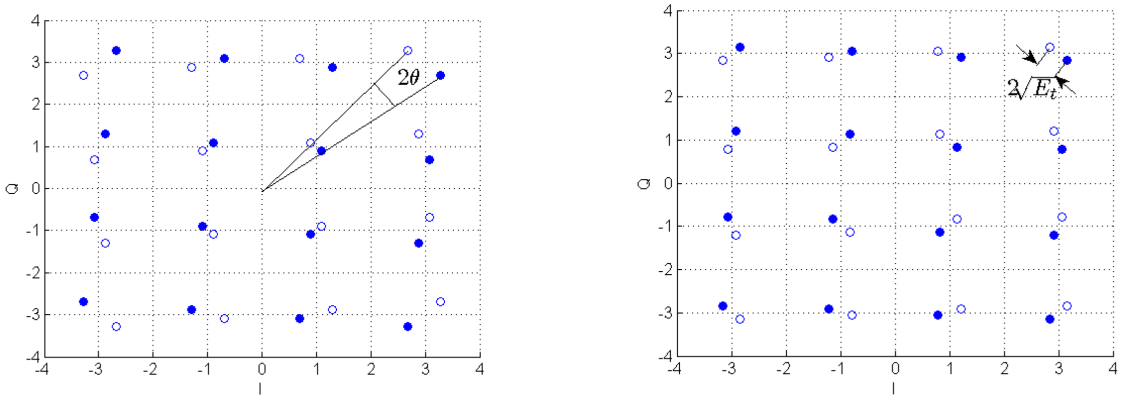
Property 1: Given the input string, the output string can be computed easily but given the output string it is computationally infeasible to recover the input string.

Property 2: It is very sensitive to changes in the input, e.g., two input strings that differ by a single bit can give completely different output strings.

The PU sets its initial tag bit string h_n, which is known only to itself. It then uses a hash chain to generate a sequence of tags.

$$h_n \rightarrow h_{n-1} \rightarrow \cdots \rightarrow h_1 \rightarrow h_0, \tag{4.1}$$

where $h_i = \text{hash}(h_{i+1})$ and $\text{hash}(\cdot)$ is a hash function.



(a) Tagging over 16 QAM with uniform angular degradation.

(b) Tagging over 16 QAM with uniform energy degradation.

Fig. 19: Constellation Diagrams

The last tag h_0 is broadcast to all users, hence is known to both the cognitive receivers and any adversaries. The subscript i of h_i indicates the time index during which the PU will transmit the tag h_i. For example, at time $t = 1$, which is indicative of a short time window, the PU transmits h_1.

The cognitive receivers, upon receiving the PU's transmitted signal, constructs its estimate of h_1, say, $\hat{h}_1$. It then computes $\hat{h}_0 = \text{hash}(\hat{h}_1)$ and compare it to the known h_0. If $\hat{h}_0 = h_0$, authentication is successful, *i.e.*, the PU is believed to be transmitting. It then continues the authentication processing at the next time interval by estimating h_2 and applying to the hash function and compare with h_1. The process repeats until we use up the entire hash chain. At any interval i, if the computed $\hat{h}_{i-1} = \text{hash}(\hat{h}_i)$ differs from h_i obtained from the previous interval, the SU declares that the signal is not from the legitimate PU and appropriate measures can be taken.

From Property 2, it is clear that at each stage the SU needs to detect the tag bits correctly in order for the authentication process to continue. Therefore, it is imperative that tag bit detection error be controlled to be arbitrarily small.

4.2.2 Tag Transmission

A straightforward method to transmit a tag bit over an arbitrary digital constellation is to rotate the symbol to be transmitted by a small angle θ in the I-Q plane if the tag bit is 1. Otherwise, if the tag bit is 0 then rotate the symbol by $-\theta$. Fig 19(a) shows the resulting constellation diagram when this approach is applied to 16 QAM modulation. Let us refer to this scheme as uniform angular degradation (UAD) scheme.

Another general approach for tag bit transmission is illustrated in Fig. 19(b). In this approach the symbol to be transmitted is rotated by a constant-length offset, where the offset direction depends on the value of the tag bit. We refer to this scheme as uniform energy degradation (UED) scheme

The two schemes introduced above will result in PU's signal degradation. As mentioned earlier we do not want the legacy receivers to take any noticeable performance hit because of this tag embedding. To achieve this, tag power level should be kept to a minimum ensuring that PU's signal distortion is within acceptable limits. Reducing tag power level will result in decreased tag bit detection performance. But we also want to make sure that tags are transmitted with as much reliability as possible. These opposing requirement warrant a thorough analysis of such embedding schemes. In the next section we define and analyze a generalized tag embedding scheme whose results are then applied to the aforementioned UAD and UED schemes.

4.3 Tag Embedding for General Constellations

In this section we formally define tag embedding for any arbitrary digital constellation and then provide probability error analysis of the same assuming a narrowband Rayleigh fading channel. The derived error probability can then be applied to the UAD and UED schemes.

Let $\mathcal{S} = \{s_0, s_1, \ldots, s_{M-1}\}$ be the original set of constellation points in the **I-Q** plane for a given M-ary modulation scheme. The primary transmitter selects a symbol, $s \in \mathcal{S}$, from this set in the absence of tag. Let $t \in \{0, 1\}$ denote the tag bit to be embedded. Tag embedding is thus defined by a mapping from (t, s) to a new constellation point $s_{t,i} = g(t, s)$.

Depending on the data symbol s, and the tag bit t, suppose the PU transmits the symbol $x = g(t, s)$ and the SU receives it as y. The communication medium between the PU and the SU being wireless, we model it as a narrowband Rayleigh fading channel [28]. Let h be the channel coefficient and z be the additive white Gaussian noise distributed as $\mathcal{CN}(0, \sigma_z^2)$. Then y is given by,

$$y = hx + z \tag{4.2}$$

We further assume that the receiver knows the channel coefficient h perfectly, and that symbols s and tag bits t follow independent and identically distributed (i.i.d) uniform distribution over their respective support sets.

At the SU the goal is to detect the tag bits as accurately as possible. In order to detect the tag bits, the SU has to detect which constellation the symbol belongs to. This is basically a hypothesis testing problem where the *SU* wants to test whether the transmitted symbol belongs to either the set of symbols generated by tag bit 1, $\mathcal{S}_0$ or tag bit 0, $\mathcal{S}_1$. These sets are defined as follows.

$$\mathcal{S}_0 = \{s_{0,i} : s_{0,i} = g(0, s_i), s_i \in \mathcal{S}\} \tag{4.3}$$

$$\mathcal{S}_1 = \{s_{1,i} : s_{1,i} = g(1, s_i), s_i \in \mathcal{S}\} \tag{4.4}$$

We want to detect the tag bits with as few errors as possible. Let, the PU send a tag bit t and the SU decode it as $\hat{t}$. Let P_e be the tag bit error probability.

$$P_e = p(t \neq \hat{t})$$

Minimizing P_e entails a Bayesian detector [12] and the corresponding decision rule is given as follows.

$$\hat{t} = \begin{cases} 0 & \text{if } p(y|x \in \mathcal{S}_0) > p(y|x \in \mathcal{S}_1) \\ 1 & \text{otherwise} \end{cases} \tag{4.5}$$

Plugging in the Rayleigh fading channel model gives us the following.

$$\hat{t} = \begin{cases} 0 & \text{if } \sum_{i=0}^{M-1} e^{-\frac{1}{\sigma^2}|y-hs_{0,i}|^2} > \sum_{j=0}^{M-1} e^{-\frac{1}{\sigma^2}|y-hs_{1,j}|^2} \\ 1 & \text{otherwise} \end{cases} \tag{4.6}$$

In the high SNR regime, $\rho >> 1$, the decision rule can be approximated as,

$$\hat{t} = \begin{cases} 0 & \text{if } \min_i\{|y-hs_{0,i}|^2\} < \min_j\{|y-hs_{1,j}|^2\} \\ 1 & \text{otherwise} \end{cases} \tag{4.7}$$

SNR is defined as follows.

$$\rho = \frac{E}{\sigma_z^2}, \tag{4.8}$$

$$\text{where, } E = \frac{1}{M}\sum_{i=0}^{M-1}\frac{|s_{0,i}|^2 + |s_{1,i}|^2}{2}. \tag{4.9}$$

While error probability analysis is generally intractable for the above detector, closed form expression can be obtained under an additional assumption of low tag to noise power (TNR), $\rho_t << 1$. TNR is defined as follows.

$$\rho_t = \frac{E_t}{\sigma_z^2}\ , \tag{4.10}$$

$$\text{where, } E_t = \frac{1}{M}\sum_{i=0}^{M-1}\frac{|s_{0,i} - s_{1,i}|^2}{4}. \tag{4.11}$$

Thus, a high SNR and low TNR regime lends analytical tractability to analyzing the error probability of the detector at hand and a closed form expression of the tag bit error probability is given by the following proposition.

Proposition 1. *Suppose the PU transmits* $s_{t,i} = g(t, s_i)$ *for the given tag bit* t *and data symbol* s_i*. Under high SNR conditions and low TNR at the SU expressed as* $\rho \gg 1$ *and* $\rho_t \ll 1$*, respectively, the tag bit error probability,* P_e *is given by,*

$$P_e \approx \frac{1}{M} \sum_{i=0}^{M-1} \frac{1}{2} \left(1 - \sqrt{\frac{|s_{0,i} - s_{1,i}|^2 / 2\sigma_z^2}{1 + |s_{0,i} - s_{1,i}|^2 / 2\sigma_z^2}} \right) \tag{4.12}$$

Proof. See Appendix B. □

Additionally, constraining the TNR to very small values ensures that the distortion introduced by the tag signal is minimal. With these constraints in place, the tag detector can be further reduced to the following rule.

$$\hat{t} = \begin{cases} 0 & \text{if } \mathrm{Re}(yh^* \hat{s}_{0,j}^*) > \mathrm{Re}(yh^* \hat{s}_{1,j}^*) \\ 1 & \text{otherwise} \end{cases} \tag{4.13}$$

where $\hat{s}_j \in \mathcal{S}$, $\hat{s}_{0,j} = g(0, \hat{s}_j)$, $\hat{s}_{1,j} = g(1, \hat{s}_j)$ and $\hat{s}_j = \arg\min |y - hs_i|^2, \forall s_i \in \mathcal{S}$, * is the conjugate operator and $\mathrm{Re}(\cdot)$ is the real operator. The above rule can be explained as follows: In the high SNR and low TNR regime, the received symbol can be decoded to the correct data symbol with a high probability, practically with the same probability as that in the absence of the tag signal. In this event, the tag detector is essentially a correlator between the received symbol and the tag symbols for the detected data symbol. As compared to the rule in (4.7) the rule in (4.13) is simple and has less complexity for two reasons. Firstly, it removes the search space over all the constellation symbols as given in (4.7). Secondly, it can take advantage of any optimized detector implementation of the constellation symbols used to transmit data symbols. Lower detection complexity is particularly important when implementing a real time system.

Having derived the tag bit error probability of a general tag embedding in an arbitrary digital constellation, we apply these results to the UED and UAD schemes. Next we formally define the two schemes and state their tag bit error probability which can be trivially derived from Proposition 1.

4.3.1 Uniform Angular Degradation (UAD)

In this scheme, each constellation point is rotated by a fixed angle in the I-Q plane, as shown in Fig 19(a). It can be defined as follows.

$$g_1(t, s_i) = s_i e^{j(1-2t)\theta} \tag{4.14}$$

where $\theta > 0$ such that $\theta \ll 1$. Using proposition 1, the tag bit error probability for this scheme is given as follows.

$$P_e \approx \frac{1}{M} \sum_{i=0}^{M-1} \frac{1}{2} \left(1 - \sqrt{\frac{|2\theta s_i|^2/2\sigma_z^2}{1 + |2\theta s_i|^2/2\sigma_z^2}} \right) \tag{4.15}$$

As the scheme needs to be transparent to the primary receiver, θ needs to be small and the rule of thumb is that the induced offset on the signal constellation should be much smaller than that of the noise standard deviation. For small θ, the scheme induces an SNR degradation at s_i that is proportional to $|s_i|^2$, i.e., the degradation is proportional to the SNR at the constellation point. Assuming that the constellation points have equal prior probabilities, the average SNR degradation of this scheme is given in the following lemma.

Lemma 1. *Let θ be small such that $\theta^2 |s_i|^2 \ll N_0$, where $s_i \in \mathcal{S}$, N_0 is the noise spectral density.*

With constant angular offset the SNR at the primary receiver is given by

$$\rho' \approx \rho(1 - \rho\theta^2) \tag{4.16}$$

where $\rho = \frac{1}{M}\sum_0^{M-1}\frac{|s_i|^2}{N_0}$ is the SNR in the absence of tag.

Proof. For small θ, the offset at s_i is simply $\theta|s_i|$. The SNR can be computed as

$$\begin{aligned}
\rho' &= \frac{1}{M}\sum_0^{M-1}\frac{|s_i|^2}{|s_i|^2\theta^2 + N_0} \\
&= \frac{1}{M}\sum_0^{M-1}\frac{|s_i|^2}{N_0}\left(1 - \frac{\theta^2|s_i|^2}{|s_i|^2\theta^2 + N_0}\right) \\
&\approx \rho(1 - \rho\theta^2) \qquad (4.17)
\end{aligned}$$

The last step follows form the condition $\theta^2|s_i|^2 \ll N_0$. □

While N_0 above is the noise power density at the primary receiver, we assume for simplicity that the noise power at the SU is identical to N_0. Otherwise, the derivation still holds except new notations need to be defined.

4.3.2 Uniform Energy Degradation (UED)

In this scheme, each symbol is rotated by a constant-length offset in the I-Q plane, as shown in Fig 19(b). The symbol mapping is defined as follows.

$$g_2(t, s_i) = s_i e^{j(1-2t)\theta_i} \tag{4.18}$$

where, $\theta_i = \sin^{-1}\sqrt{E_t/|s_i|^2}$. This condition indicates that $|g_2(0, s_i) - g_2(1, s_i)| = \sqrt{E_t}\ \ \forall i$. Using proposition 1, the tag bit error probability for this scheme can be derived as follows.

$$P_e \approx \frac{1}{2}\left(1 - \sqrt{\frac{E_t/\sigma^2}{1 + E_t/\sigma^2}}\right) \tag{4.19}$$

where, E_t is defined in (4.11). Similar to the UAD scheme, this scheme causes SNR degradation at the PU. The following lemma states the effective SNR, ρ' at the PU in presence of tag signal, whose proof is similar to that of Lemma 1

Lemma 2. *Let E_t be small such that $E_t \ll N_0$. In the high SNR region, $E/\sigma^2 \gg 1$, the effective SNR at the PU in the presence of tag is given by,*

$$\rho' \approx \rho(1 - \rho_t) \tag{4.20}$$

It is clear that for PSK modulations, the two schemes are identical to each other, with respect to tag bit error probability and the induced SNR degradation at the PU. For the general QAM modulations, however, the first scheme will result in an SNR degradation of the PU signal that is roughly proportional to the SNR of the constellation point. For the second scheme, a constant SNR degradation is imposed on all constellation points. In the next section we show that the UED scheme is optimal in terms of tag bit error probability in high SNR and low TNR regime.

4.3.3 Scheme Optimality

We now establish that the second scheme, i.e., the one that shifts the constellation by a constant offset $\sqrt{E_t}$ is optimal under high SNR condition for a Rayleigh fading channel. This is given in the following theorem.

Theorem 2. *Let P_e' and P_e bet the tag bit error probabilities of any general tag and UED embedding schemes, respectively. Then, under the following assumptions,*

1. *High SNR: The signal to noise ratio at the SU in the absence of tag is high, $\rho >> 1$.*
2. *Low TNR: The tag signal to noise ratio at SU is low, $\rho_t << 1$.*

the following result holds.

$$P_e \le P_e' \tag{4.21}$$

Proof. The probability of error P_e of the UED scheme is given in (4.19). The probability of error P_e' for the channel model in (4.2) given in (4.12) is stated again in the following.

$$P_e' \approx \frac{1}{M}\sum_{i=0}^{M-1}\frac{1}{2}\left(1-\sqrt{\frac{|s_{0,i}-s_{1,i}|^2/2\sigma_z^2}{1+|s_{0,i}-s_{1,i}|^2/2\sigma_z^2}}\right) \tag{4.22}$$

Using the concavity of the expression $\sqrt{\frac{x}{1+x}}$, we can show that the RHS of (4.22) is greater than or equal to the RHS of (4.19). Hence, $P_e \le P_e'$. □

Though the UED scheme is optimal with respect to tag bit error probability in the high SNR and low TNR regime, the operating error rate is not sufficiently low to use the scheme, as is, for tag transmission. For example, when the SNR is sufficiently high, say ≥ 25 dB and the TNR is about -10 dB, the tag bit error probability can be computed from (4.19) to be about 0.35. This value is too high for any practical purposes. A simple but effective way to reduce the error probability is to use repetition code. Repetition code permits ML decoding at a complexity which is quadratic in the number of repetitions and at the same time brings down the error probability to a small value such that the desired error probability depends on the number of repetitions. In the next section we analyze the effect of repetition coding on tag bit error probability in the Rayleigh fading channel.

4.4 Trade-off Analysis

The requirement that the primary receiver not be affected dictates that ρ_t has to be very small, which leads to a high value of P_e. A simple way to reduce the raw tag bit detection error probability P_e is to repeat the same tag bit multiple times (i.e., using a repetition code). An additional benefit is that it may utilize the time diversity in a fast fading channel. By the optimality argument in the previous section, we limit our attentions to the UED scheme, where the tag induced offset is independent of the primary symbol to be transmitted.

Consider sending the same tag bit t, K times using K primary symbols. For simplicity we assume that the channel realizations are independent for the K symbols. Let, $k \in \{0, 1, \ldots, K-1\}$ and the received sequence is given by

$$y_k = h_k x_k + z_k \tag{4.23}$$

where h_k is distributed as $\mathcal{CN}(0,1)$ and z_k is the additive white noise distributed as $\mathcal{CN}(0,\sigma_z^2)$.

The transmitted symbols $x_k = g_2(s_k, t)$ are the result of the mapping with identical t but independent s_k. The maximum likelihood decision rule that minimizes the probability of error is given as follows.

$$\hat{t} = \begin{cases} 0 \quad \text{if} & \sum_{k=0}^{K-1} \log\left(\sum_{i=0}^{M-1} e^{-\frac{1}{\sigma^2}|y_k - h_k s_{0,i}|^2}\right) > \\ & \sum_{k=0}^{K-1} \log\left(\sum_{i=0}^{M-1} e^{-\frac{1}{\sigma^2}|y_k - h_k s_{1,i}|^2}\right) \\ 1 \quad \text{if} & \text{otherwise} \end{cases} \tag{4.24}$$

For high SNR and low TNR regime, the decision rule can be approximated as follows.

$$\hat{t} = \begin{cases} 0 \quad \text{if} & \sum_{k=0}^{K-1} \min_{s_{0,i}} |y_k - h_k s_{0,i}|^2 < \\ & \sum_{k=0}^{K-1} \min_{s_{1,i}} |y_k - h_k s_{1,i}|^2 \\ 1 \quad \text{if} & \text{otherwise} \end{cases} \tag{4.25}$$

Similarly to the case with no repetition we can approximate the tag bit error probability as follows.

$$P_{e,K} \approx \left(\frac{1-\mu}{2}\right)^K \sum_{k=0}^{K-1} \binom{K-1+k}{k} \left(\frac{1+\mu}{2}\right)^k \tag{4.26}$$

where, $\mu = \sqrt{\frac{\rho_t}{1+\rho_t}}$. $P_{e,K}$ has the same form as that of BPSK signaling with repetition coding over Rayleigh fading channel [28]. From Fig. 20 we can see that the analytical approximations agree quite well with the Monte Carlo simulation results at an SNR of 25 dB and a 16 QAM signal constellation. For typical authentication purposes, tag length in the order of 100 bits is considered sufficiently secure. Thus the error probability in the order of $< 10^{-5}$ can essentially guarantee error free tag bit detection.

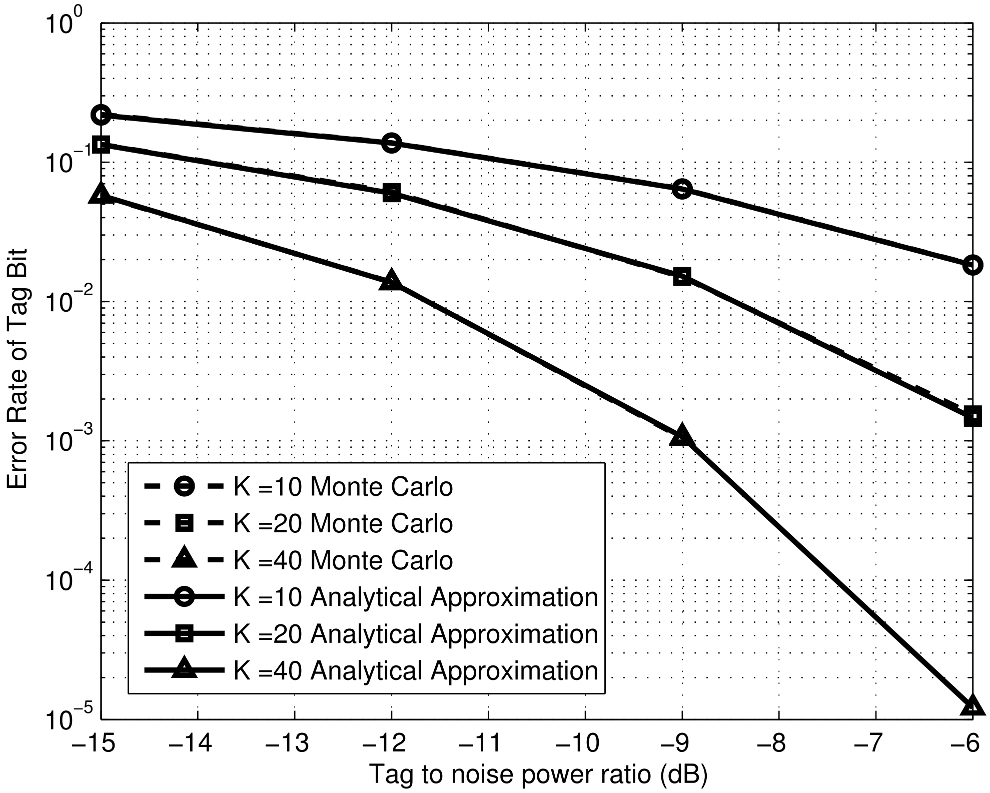


Fig. 20: Average error probability of the tag bit as function of tag signal to noise power ratio for a 16 QAM system with $\rho = 25\,\text{dB}$.

We now discuss briefly the effect of the constellation shift on the primary receiver's performance. The offset $\sqrt{E_t}$ introduces an SNR degradation at the primary receiver. According to Lemma 2, PU observes the following SNR in the presence of tag signals.

$$\rho' \approx \rho(1 - \rho_t) \tag{4.27}$$

As an example, suppose that the primary receiver is operating at a high SNR of, say 25 dB, and the tag to noise power ratio is kept less than -10 dB, then ρ' will differ from the nominal SNR by no more than 0.05 dB. Thus, by proper choice of E_t and K we can make sure that the tag bits are transmitted reliably with negligible SNR degradation at the legacy receivers.

4.5 Summary

In this chapter we have provided a method to reliably transmit cryptographic signatures at the modulation level, without compromising the performance at the legacy receivers, for the purpose of countering PUEA attacks.

One can further improve the tag bit detection performance by replacing the repetition code with a strong error correcting code (ECC). ECCs perform poorly when the number of errors in the codeword are comparable to that of their error correcting capability [5]. A compromise is to use a simple code that permits maximum likelihood decoding with low complexity (such as the repetition code) as an inner code to bring down the raw tag bit error rate in the range of $10^{-2} - 10^{-3}$. We can then use an appropriate ECC as an outer code to guarantee essentially perfect tag recovery at the *secondary user*.

CHAPTER 5

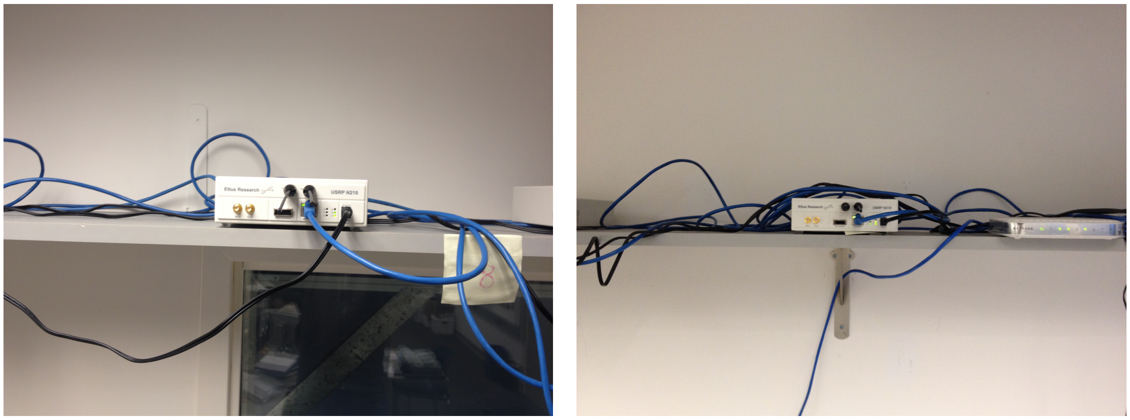
PHYSICAL LAYER AUTHENTICATION IMPLEMENTATION

5.1 Introduction

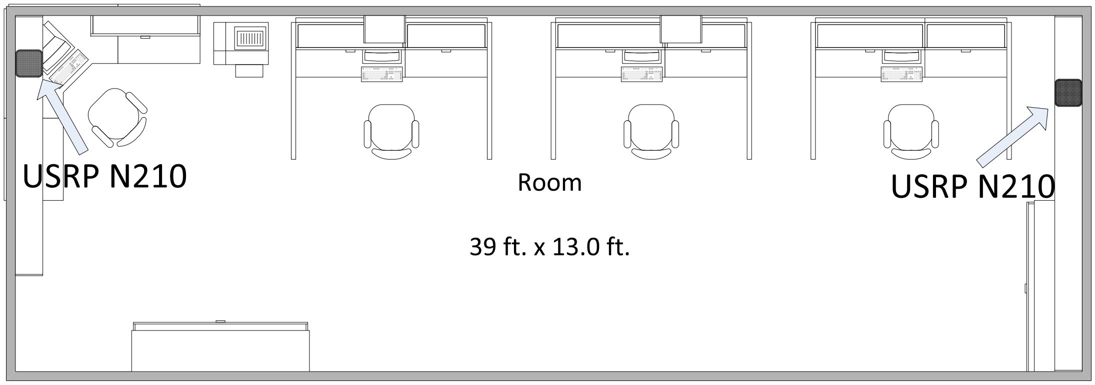
This chapter presents experimental results for the physical layer authentication scheme developed in Chapter 4. We evaluate experimentally the optimal tag embedding scheme by implementing it using GNU Radio/USRP [10, 29] platform. We show that we can transmit authentication tags very reliably but at the same time not affect the PU's signal detection performance. Achieving this practical realization has its unique challenges because a verbatim application of the theoretical effort described in Chapter 4 is not possible. For example, the process of tag verification necessitates that the tag bit error probability is as small as possible. But at the same time we cannot assign too much power to the tag as it may then distort PU's signal. It was shown in Chapter 4 that just repeating a tag bit sufficient number of times will bring down the tag bit error probability to the desired small level. But in real setting this claim does not hold up and we need to find ways to overcome the limitation. Nevertheless, our present work not only validates the insights derived in Chapter 4 but also provides a practically viable solution to the physical layer authentication problem. Next, we briefly describe the experimental setup, then provide the implementation related details & challenges and finally present our experimental findings.

5.2 Experiment Setup

The setup consists of two USRP N210 [29] placed along the opposite ends of a room with dimensions 39ft. × 13ft. as shown in Fig. 21. Each USRP is equipped with an SBX daughterboard. We used GNU Radio as a building block to implement our idea.



(a) USRP N210 Transmitter (b) USRP N210 Receiver



(c) Experiment Room Setup

Fig. 21: Measurement Setup

To perform the experiments we have chosen differential 16 QAM as the modulation scheme for data signaling, within which we embed the tag. Nevertheless, our implementation is scalable to any type of QAM modulation. As mentioned in the previous section, to maintain transparency at the legacy receiver we have to make sure the tag to noise power ratio (TNR) is very small. We control the TNR by defining a new term called, tag to data power ratio (TDR). Then, once you measure the data signal to noise power ratio (SNR), it is straightforward to compute the TNR, TNR (dB) = TDR (dB) + SNR (dB). In the next section we describe the implementation related details and then present our findings.

5.3 Implementation

In this section we provide details about the transmitter and receiver implementations. We first give their high level block diagrams along with their description. Then we give a more detailed exposition of the tag detection process.

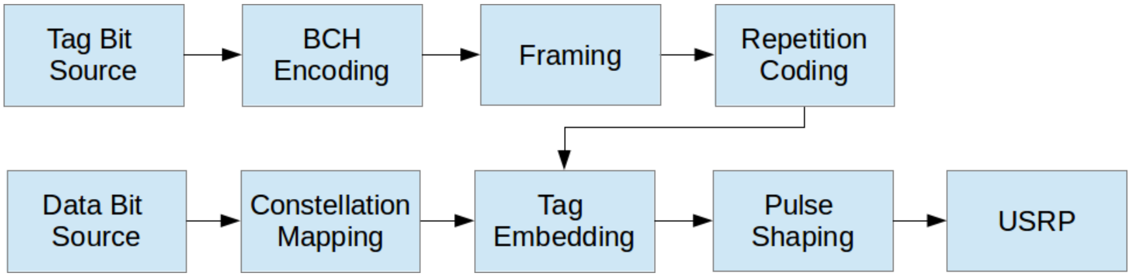


Fig. 22: Transmitter Block Diagram

Fig. 22 shows the block diagram of the transmitter. The *Constellation Mapping* block takes in data bits and maps them into differential 16 QAM symbols, which are then given to the *Tag Embedding* block. The other input to the *Tag Embedding* block comes from the other sub-chain that generates the tag bits. The tag bits are first encoded using an appropriate length and rate BCH code as an outer code and then given to the *Framing* block. This block inserts a fixed length pilot, which is essentially a PN sequence [22], after every few codewords for synchronization. In other words, the PN sequence facilities codeword boundary delineation. The *Repetition Coding* block after the *Framing* block modulates another PN sequence such that if the incoming bit value is 1, then the output is the PN sequence and if the incoming bit is 0 the output is bitwise inverted PN sequence. This, in effect is a $(K, 1)$ repetition code if the PN sequence is of length K bits. The

Tag Embedding blocks takes in the data symbols and the tag bits from its two inputs and uses the mapping function given in (4.18) to generate the output symbols. These symbols are fed to an upsampling root raised cosine (RRC) filter [22] and then sent to the USRP for over the air transmission.

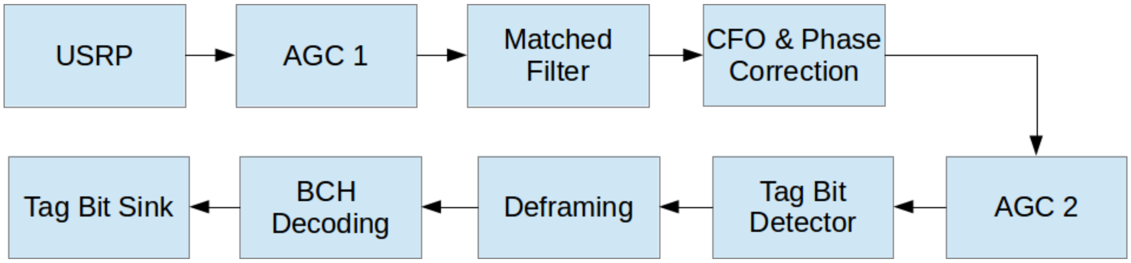


Fig. 23: Receiver Block Diagram

On the receiver side, shown in Fig. 23, the output from *USRP* is passed through *AGC 1* (automatic gain control) which adjusts the receiver front end gain. In the *Matched Filter* [22] block, the signal is RRC filtered, which gives each received symbol an effective raised cosine pulse shape. This RRC filtered data is then processed to determine symbol timing estimate and sampled accordingly. The downsampled signal is then sent through the Carrier Frequency Offset (CFO) & Phase correction block which adjusts for the difference in frequency offsets between the transmitter and receiver local oscillators using decision feedback equalization [22]. In practice, we do not need frequency correction to decode differentially encoded symbols if the phase offset between consecutive symbols is very small compared to the CFO. But for tag detection we need the received constellation to be amplitude, frequency and phase corrected. The amplitude correction is achieved by the final gain control *AGC 2* which maintains the received power level to that of the reference level. The output of *AGC 2* is then fed to the *Tag Detector* which operates by decoding each repetition code. The details of the *Tag Detector* are given in the following paragraphs. The detected bit stream from the *Tag Detector* is then correlated with the pilot (a PN sequence), mentioned previously for frame synchronization. Once the codeword boundaries are determined, the *BCH Decoding* block decodes the received codewords and sends them to the *Tag Bit Sink*.

As mentioned previously, to achieve repetition coding we modulate an appropriate length PN sequence, instead of naively repeating each tag bit. This is done in order to overcome the literal ML decoding of the repetition code as given in rule (4.24), which is computationally very expensive. Using a PN sequence simplifies the process of decoding each tag bit, likening to that of de-spreading received symbols through the means of a correlator and sampler. Fig 24 shows the operations performed by the tag detector.

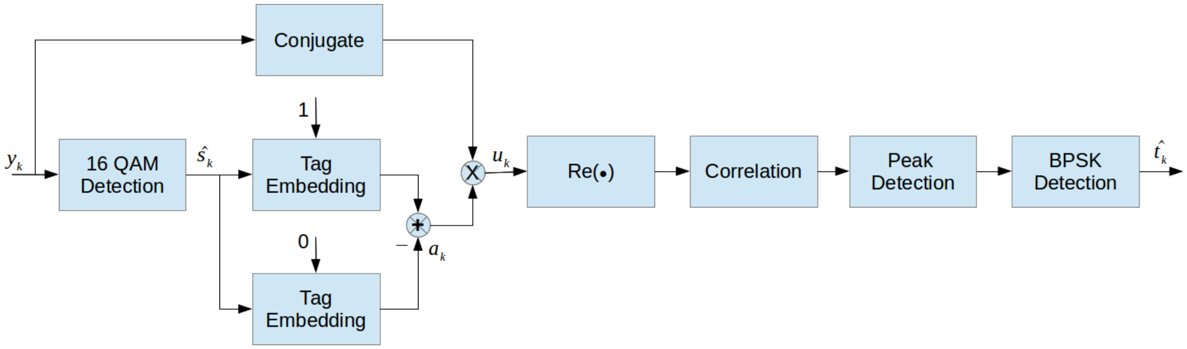


Fig. 24: Tag Detector Block Diagram

As shown in Fig. 24, the tag detector first performs ML decoding on a received symbol y_k to find the data symbol, $\hat{s}_k \in \mathcal{S}$. It then computes the following statistics.

$$a_k = g_2(\hat{s}_k, 1) - g_2(\hat{s}_k, 0) \tag{5.1}$$

$$u_k = \text{Re}(y_k^* a_k) \tag{5.2}$$

Assuming correct data symbol detection, which is a reasonable assumption given high SNR and low TNR conditions, (5.2) is simply the statistic derived in (4.13). a_k can be considered as a 2 dimensional vector, the real and imaginary components of a_k being the two elements, that contains the two antipodal signals, $g_2(\hat{s}_k, 0)$ and $g_2(\hat{s}_k, 1)$. And, u_k is the projection of the received vector y_k onto the axis that contains the two antipodal signals. The relation between the received vector y_k and the detected symbol $\hat{s}_k$ can be given as $y_k = \hat{s}_k + e_k$ such that e_k is the error vector. For the scheme at hand, *i.e* UED, a_k is orthogonal to $\hat{s}_k$. Hence, $u = \text{Re}(y_k a_k^*)$ can be reduced to $u = \text{Re}(e_k a_k^*)$. The tag detector essentially converts the data and tag dependent received signal into data independent and only tag dependent BPSK signal. Thus, the received incoming stream

$\{\ldots, y_{k-1}, y_k, y_{k+1}, \ldots\}$ is converted into $\{\ldots, u_{k-1}, u_k, u_{k+1}, \ldots\}$ which is then correlated with the BPSK modulated PN sequence (this PN sequence was used earlier at the transmitter for encoding each tag bit). The output of the correlator will have peaks at intervals separated by K samples as shown in Fig. 25(a). The peaks are marked red and their polarity depends on the encoded tag bits such that positive peaks indicate tag bit 1 whereas negative peaks indicate tag bit 0. Fig. 25(a) plots correlator output of 10 tag bits coded with $(63, 1)$ repetition code such that there are 630 samples on the plot. As can be seen from the plot, the red marked peaks are not very prominent and hard to detect without further processing. To detect them we devise the following technique.

Let $[u_0, u_1, \ldots]$ be the output of the correlator. Using our knowledge of the repetition code block length K, we compute the following statistic.

$$v_j = \sum_{m=0}^{N_t-1} |u_{j+Km}| \quad j = 0, 1, \ldots, K-1 \tag{5.3}$$

where N_t is some positive integer. Then the peak location can be found as an offset l at which the statistic v_i gives a maximum value.

$$l = \arg\min_{j} \ \{v_j\} \tag{5.4}$$

Thus the location of peaks are given by $[l, l+K, l+2K, \ldots]$ such that the samples from the incoming stream, $[u_l, u_{l+K}, u_{l+2K}, \ldots]$, correspond to the peaks. As N_t increases, the reliability of this statistic in determining the correlator peak increases. In Fig. 25((b)), we have plotted the output of the statistic v_j for $N_t = 100$ and $K = 63$. A much clear peak can now be observed in Fig. 25((b)) as compared to those in Fig. 25((a)). Hence, the correlator peak location can be found using the location of the maximum of the the statistic in (5.3). Once the correlator peak locations are known the incoming stream $[u_0, u_1, ...]$ is sampled at those locations to output the stream $[u_l, u_{l+K}, u_{l+2K}, \ldots]$. The sampled output is then passed through the *BPSK Detection* block which outputs the detected the tag bits.

5.4 Observations

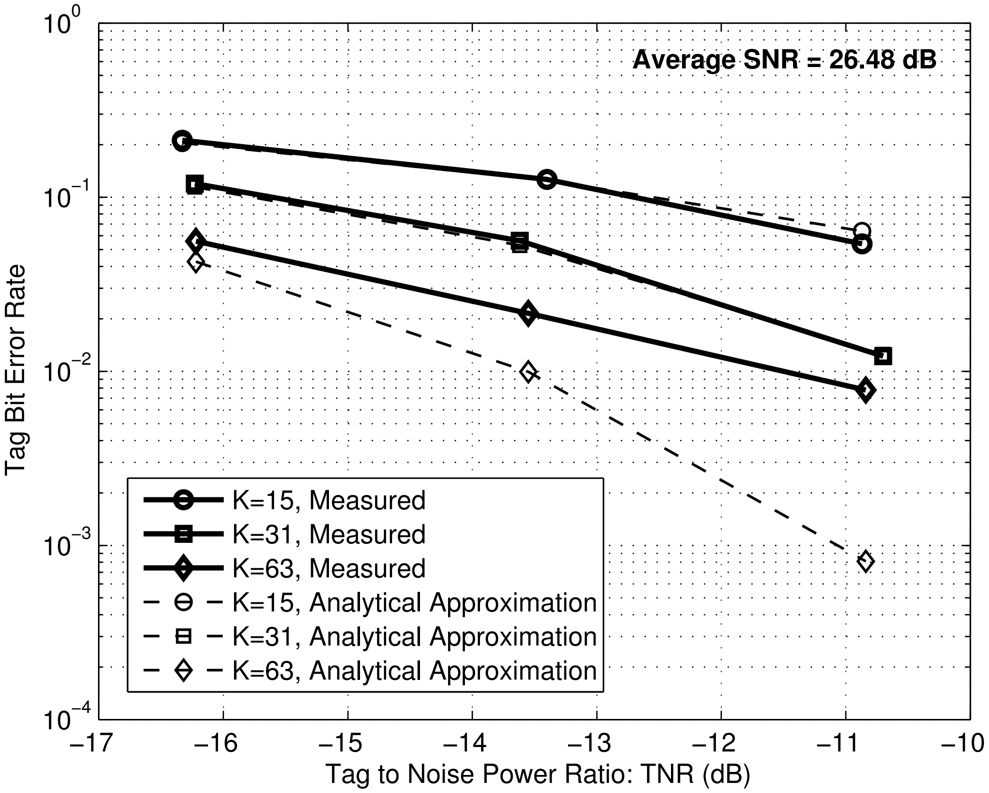


Fig. 26: Measured error rate of the tag bit as function of tag signal to noise power ratio for a 16 QAM system for average $\rho = 26.48$ dB.

Fig. 26 shows the tag bit error rate after repetition coding, measured for different lengths of repetition code. We observe that for $K = 15$ and 31, the measured tag bit error rates are consistent with the analytical approximation. But for $K = 63$, the measured error rate is higher than the analytical approximation. We hypothesize that this behavior is a manifestation of some error floor phenomenon, which we haven't investigated yet. None of the measured rates in the plot is sufficient enough to transmit an authentication tag, assuming it is 128 bits long, reliably. For example, take the point corresponding to $K = 31$ and TNR $= -13.5$ dB. The observed tag bit error rate at this point is about 5.62×10^{-2}. At this rate, the chance of transmitting a 128 bit tag correctly is approximately 0.06%.

If we let tag error rate be the probability that at least one tag bit is in error then theoretically, *cf.* (4.26), we can achieve an arbitrarily small tag error rate by repeating the tag bit sufficient number of times. But the error floor phenomenon, observed in 26, prevents us from achieving this through means of only repetition coding. We overcome this by encoding the tag using an appropriate BCH code [17]. Thus, the BCH code serves as an outer code while the repetition code serves as an inner code. For sake of implementation simplicity we choose an (n, k) BCH code such that $k \geq 128$. This allows us to encode one tag per codeword. We achieve this by padding the 128 bit tag with $k - 128$ zeros and then encoding the k bits. Since, we encode each tag using one codeword, the tag error rate will be identical to codeword error rate. Therefore, (5.5) gives an upperbound for the tag error rate, P_{tag}, wherein the right hand side is the codeword error rate upperbound [17].

$$P_{\text{tag}} \leq 1 - \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i} \tag{5.5}$$

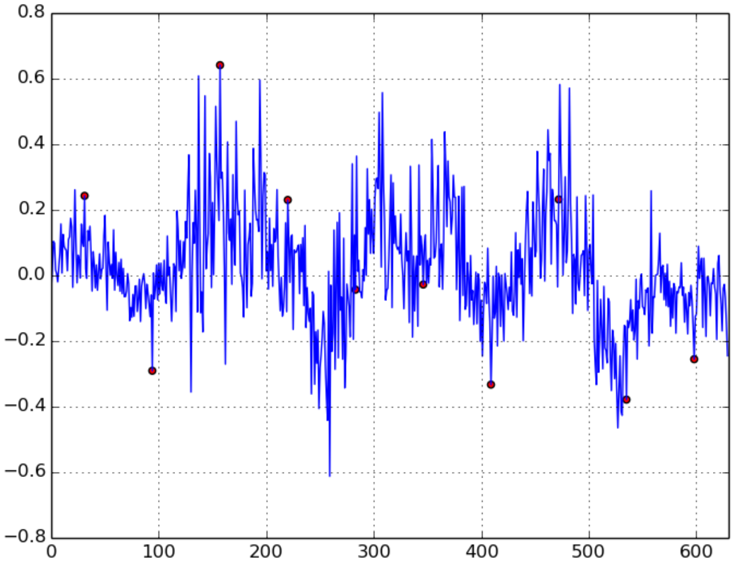
where p is the independent and identically distributed tag bit error rate after repetition coding and t is the random error correction capability of the (n, k) code.

We proceed by comparing two BCH codes, *viz.*, $(255, 131)$ and $(511, 130)$ with random error correction capability, t, being 18 and 55, respectively. Plugging in the corresponding n and t values in (5.5) we obtain tag error rates of 0.13 and 1.95×10^{-6} for $(255, 131)$ and $(511, 130)$ codes, respectively. The tag error rate, 0.13, is quite high for our application and therefore we choose the $(511, 130)$ code to encode each tag.

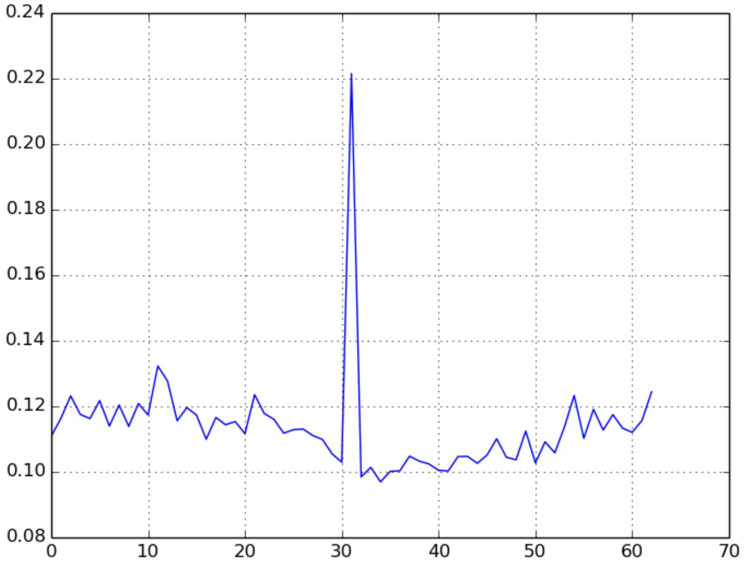
We now experimentally verify that using the $(511, 130)$ code yields virtually 0 tag error rate. We also observe no degradation in the measured bit error rate of the data signal for the level of power we assign to the tags. For sake of visual exposition Fig. 27(a) and Fig. 27(b) show the received 16 QAM scatter plot with and without tag embedding respectively. Hence, we demonstrate transmission of authentication tags very reliably and at the same time ensure minimal SNR degradation or for that matter minimal host signal distortion at the receiver.

5.5 Summary

In the process of developing the sofware radio for experimentation, we encountered and overcome some unique challenges pertinent to real time implementation. In doing so, we have successfully demonstrated a method to reliably transmit cryptographic signatures at the modulation level, without compromising the performance at the legacy receivers, for the purpose of countering PUEA attacks. Though we developed this technique for authentication purposes, it can be used to superimpose low rate information over existing digital signalling methods.

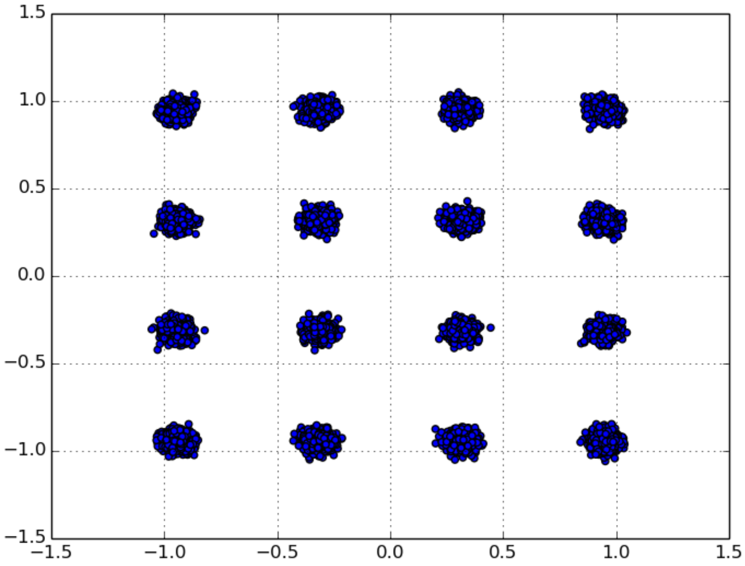


(a) Correlator Output

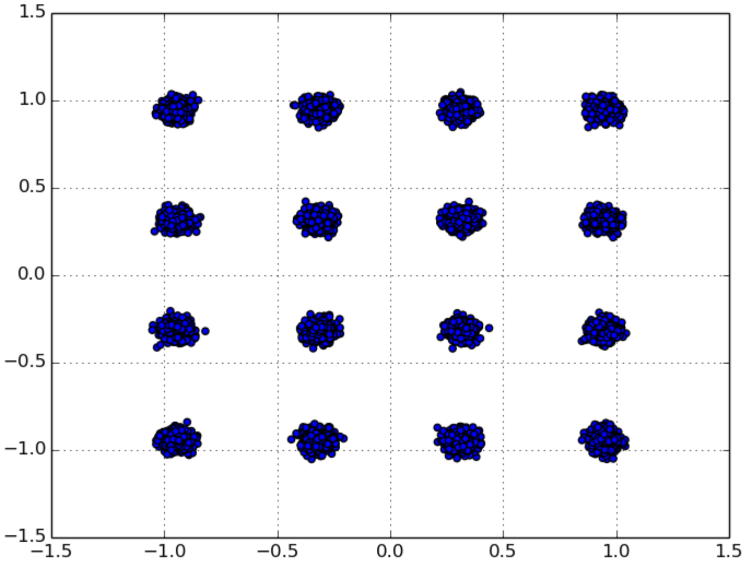


(b) Peak Detection

Fig. 25: De-spreading



(a) Received 16 QAM Constellation with tag embedding, TNR = -13.5 dB & Observed SNR = 26.81



(b) Received 16 QAM Constellation without tag embedding, Observed SNR = 27

Fig. 27: Received Constellation With & Without Tag

CHAPTER 6

A SOFTWARE RADIO DESIGN FOR COMMUNICATIONS IN UNCOORDINATED NETWORKS

6.1 Introduction

DARPA Spectrum Challenge (DSC) was a competition to develop robust and agile software radio transceivers [3]. The competing teams design software based radio systems that transmit and receive wireless signals using Universal Software Radio Peripheral (USRP) [29] devices. The teams compete with each other in two modes, *viz.*, competitive mode and cooperative mode. In competitive mode, two teams compete against each other to deliver the most amount of data within a given time limit. In cooperative mode, three teams are supposed to share a frequency band such that they participate and encourage sharing of the allocated spectrum.

The challenge consisted of three major events. Initial selection hurdles, primary tournament and final tournament. During the selection hurdles that took place in March 2013, top 15 qualifying teams were selected out of 90 competing teams. Later, 3 teams were selected right before the primary tournament in the wild-card selection process. Thereafter a total of 18 teams competed with each other during the preliminary and final tournament with each tournament having the competitive and cooperative modes. The preliminary tournament took place in September 2013, while the final tournament in March 2014. Both the tournaments were similar in format except for some change in competitive mode and monetary reward.

The competition took place on the Orbit-Lab testbed at Rutgers University [19]. Orbit-Lab is a laboratory-based wireless network emulator consisting of, not exclusively, a two dimensional grid of 400 radio nodes which can be dynamically interconnected into specified topologies with reproducible wireless channel [19]. Each of these nodes is a personal computer (PC), connected to or having one of many available wireless interfaces for experimentation. For the challenge, USRP devices are used as the wireless interfaces.

In the next section we provide a brief description of Orbit Lab and the setup used there for the challenge. In Section 6.3 we provide detailed description about the strategies we devised for the competitive and cooperative modes of the final tournament. Section 6.4 details the feedback scheme used in our transceivers and Section 3.6 concludes the paper.

6.2 Orbit-Lab

The challenge took place on the 20 by 20 grid of radio nodes [19]. Fig 28 and Fig 29 show the primary and secondary node configuration on the grid used during the final tournament, respectively. Nodes denoted by Team Xp, Yp, Xs and Ys are used for competitive mode. Letters “X” and “Y” denote two different teams. Whereas nodes denoted by Ap, Bp, Cp, As, Bs and Cs are used for cooperative mode. Here, letters “A”, “B” and “C” denote three different teams. The suffixes “p” and “s” denote primary arena and secondary arena, respectively. Each team is assigned two nodes, one being the transmitter and the other being the receiver.

In competitive mode, a game consists of two matches of 3 minutes each on the same arena but with the nodes of teams “X” and “Y” swapped between the two matches. Whereas in the cooperative mode, a games consists of one match of 3 minutes between teams “A”, “B” and “C”.

Each arena is used alternatively during the matches, *i.e.* when a match is being executed on one arena, a match from another game is loaded on the other arena. By the time the first match gets over, the other arena is ready to be used for the next match. This serves the purpose of reducing the interval between two consecutive matches as there is a few minute setup time required to run each and every match [19]

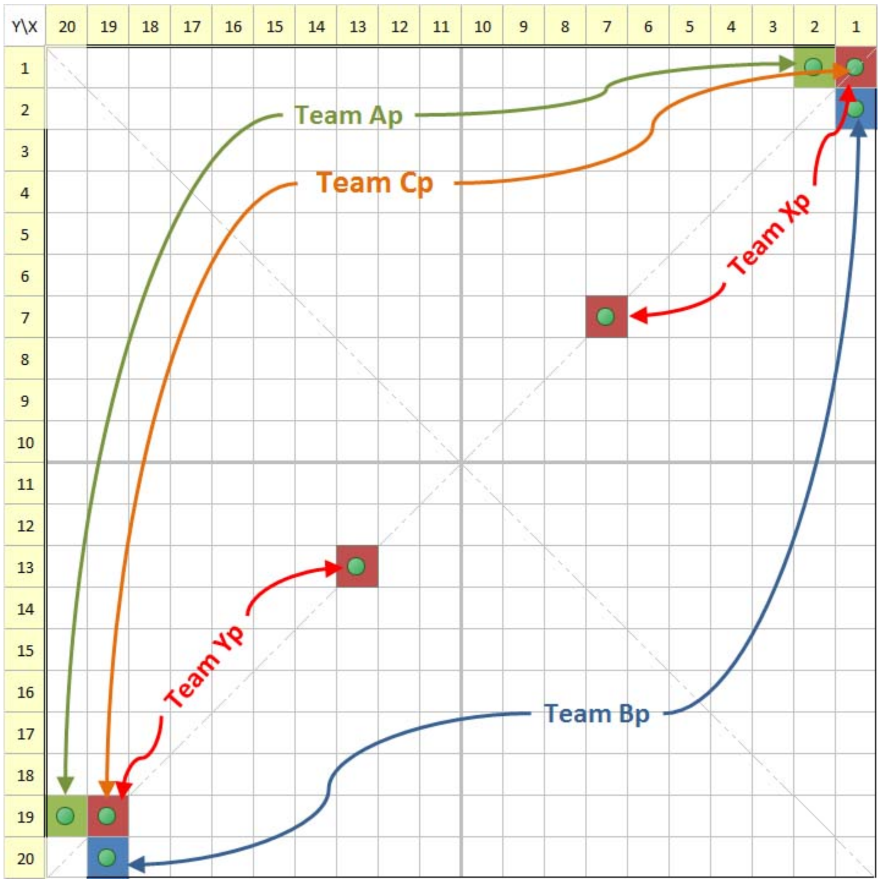


Fig. 28: Final Tournament Node Topology - Primary Arena

6.3 Strategies

A very high level block diagram of the transmitter and receiver is given in Fig. 30 and Fig. 31, respectively. The transmitter fetches packets from the packet server and transmits them through the wireless channel and listens for feedback from the receiver. On the other hand, the receiver listens for packets from the transmitter and sends timely feedback to ensure reliable packet transfer.

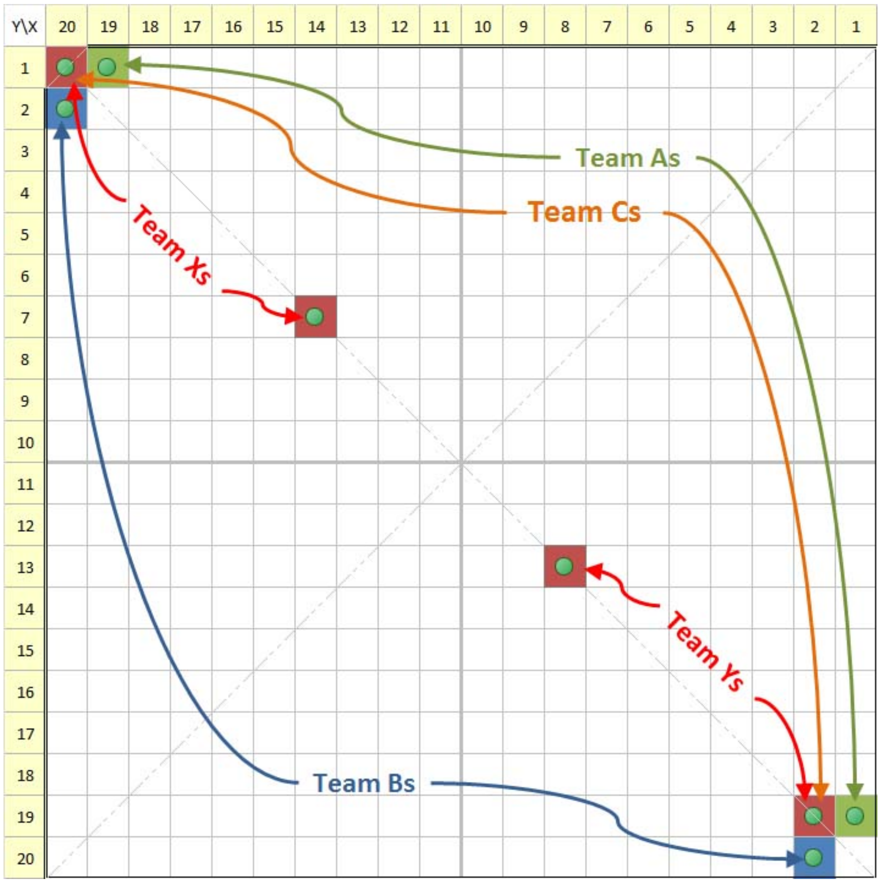


Fig. 29: Final Tournament Node Topology - Secondary Arena

The overall strategy for both the modes include having feedback and small packets. The purpose of feedback is packet reliability, which is achieved by feeding back the indices of lost packets to enable the transmitter to retransmit them and by adapting the data rate to suit the channel condition.

Each input packet from the packet server is of size 1440 bytes. We split this packet into smaller packets for the following reasons. Firstly, smaller packets have higher transfer success rate as compared to the input packets for the same channel conditions. Secondly, it allows us to use Reed-Solomon codes [4, 17] of block length 255 bytes, provided the packet size is smaller than 255 bytes. These codes, compared to the LDPC/BCH concatenated codes [17] that we used in the preliminary round, have much faster encoding and decoding speed but at the cost of some error correction capability.

Fig. 32 shows the block diagram of the packet transmitter. As stated earlier, each packet from

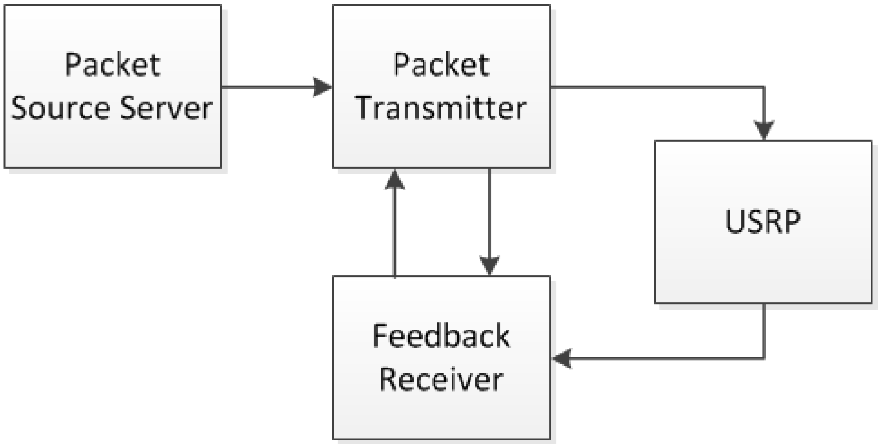


Fig. 30: High Level Packet Transmitter Block Diagram

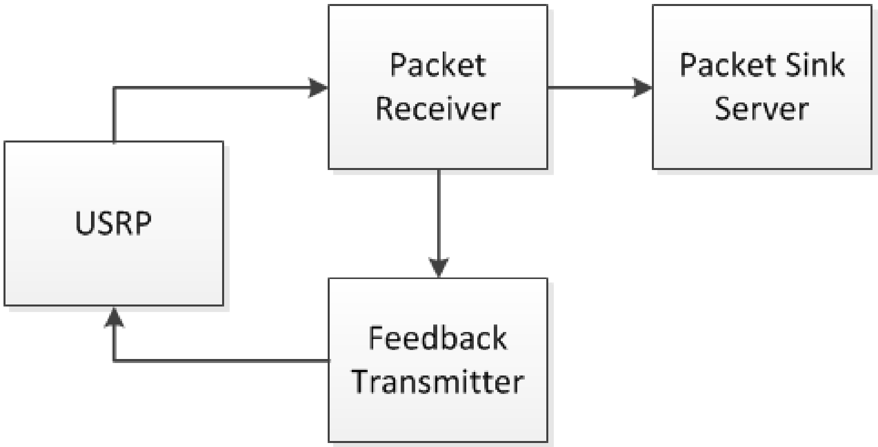


Fig. 31: High Level Packet Receiver Block Diagram

the server is of size 1440 bytes. We pad this with 2 bytes and split it in 7 parts. We then add header of about 8 bytes which includes the packet number and a 32 bit cyclic redundancy check (CRC) [17]. This gives us a data unit of length 214 bytes. We define this as an *Unencoded Small Packet* (USP). Fig. 33 gives the structure of an USP. This is then fed to a $(255, 214)$ Reed-Solomon encoder, the output of which we call as an *Encoded Small Packet* (ESP).

These ESPs of size 255 bytes are then grouped together depending on the modulation scheme to maintain same physical layer frame size through all modulation schemes. Possible modulation schemes are BPSK, QPSK, 8PSK and 16QAM [22]. As shown in Fig. 34, each physical layer frame consists of 8341 symbols including 127 symbol wide preamble, 30 symbol wide control sequence, 8160 symbols wide payload corresponding to the appropriate number of ESPs and the

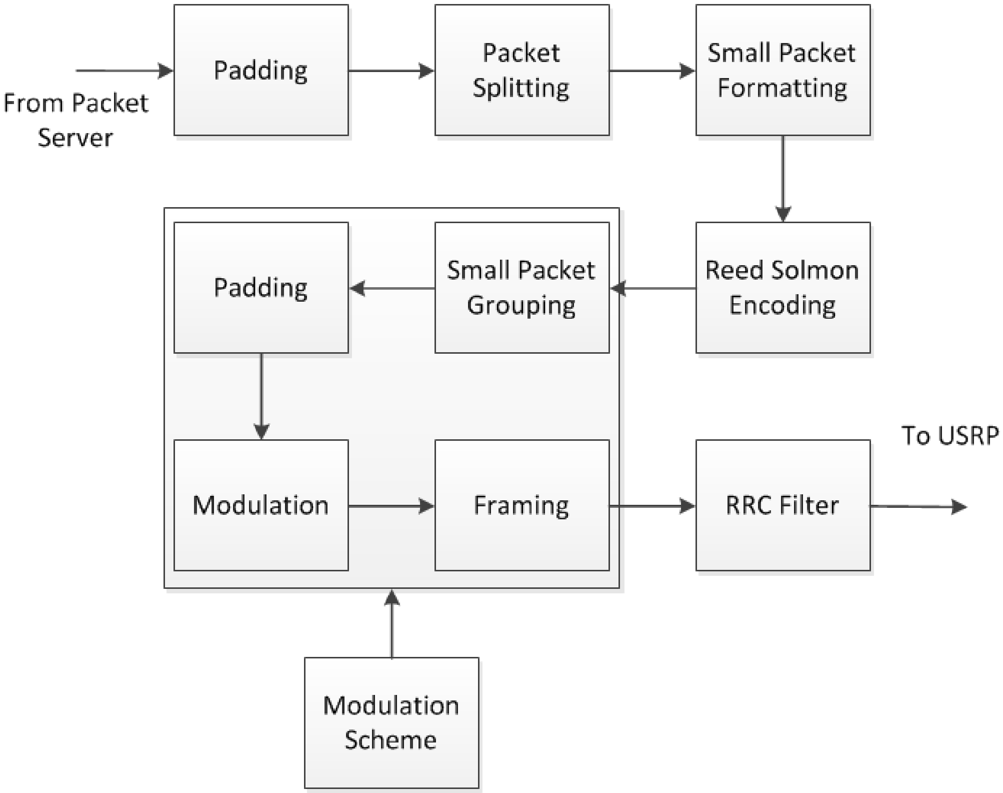


Fig. 32: Packet Transmitter

CRC	Packet Number	Packet
4 bytes	4 bytes	206 bytes

Fig. 33: Packet Format

remaining 24 being padding symbols. The preamble allows the receiver to find frame boundary. The control sequence, composed of two identical *m-sequences* [22] of length 15 symbols, helps us identify the payload modulation scheme uniquely. The padding symbols are there to take care of initial phase and frequency acquisition.

Fig. 35 shows the block diagram of the packet receiver. The received signal is match filtered then passed through a correlator to find the preamble, which in turn allows us to delimit the frames. Using the received control sequence, the modulation detector detects the payload modulation scheme. As previously mentioned, the control sequence is composed of two identical *m-sequences* of length 15 symbols. A modulation scheme is uniquely identified if the two received *m-sequences* give maximum correlation with the *m-sequence* assigned to that particular modulation scheme. The payload is demodulated using the detected modulation scheme and consequently unpadded to give multiple ESPs. These ESPs are then sent through the Reed-Solomon decoder to give USPs. If the CRC of a USP is consistent then the packet is sent to the small packet gleaner which re-assembles the USPs together to deliver the original 1440 bytes packets.

Preamble	Control Sequence	Padding Symbols	Payload
127 symbols	30 symbols	24 symbols	8160 symbols

Fig. 34: Physical Layer Frame Format

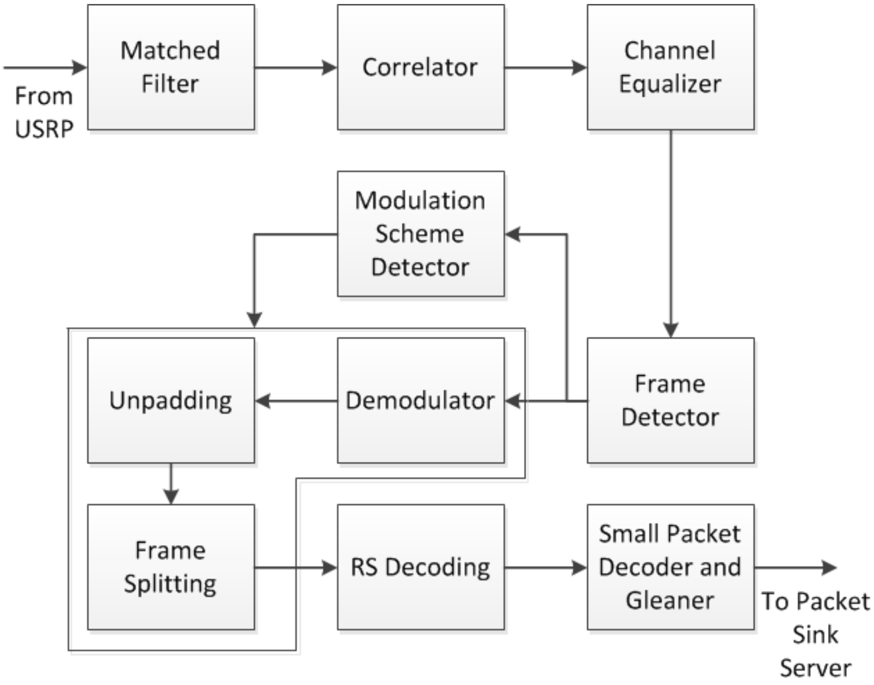


Fig. 35: Packet Receiver

6.3.1 Competitive Mode

The goal of competitive mode is to transfer more packets than the other team. Each team is given 15000 packets each of size 1440 bytes. Whichever team finishes transmitting all the 15000 packets first, within 3 minutes time limit, or transmits most error free packets in the time limit wins the match. According to our tests on the grid, we found out that some nodes cannot support more than differential BPSK while the rest cannot support more than differential QPSK under steady interference from the other transmitter. Therefore, we devised a strategy that locks on to the appropriate constellation scheme for the given nodes as early as possible during the 3 minutes. We describe our strategy in detail in the following.

There are initial 4 bursts of 3 seconds each, which are used to lock on to the appropriate constellation. The 3 seconds are composed of 1.5 seconds for packet transfer, 1 second for jamming and 0.5 seconds for feedback. During the design process we made the assumption that the interference from the competitor will be rather stable during the time of the match. We start first burst with QPSK. If during the 4 initial bursts the receiver experiences high packet error rate (PER) for QPSK modulation scheme then we lock on to BPSK modulation scheme for the rest of the game. Fig. 36 depicts the strategy we used for this mode. One can observe jamming state right after every forward state. This was done to overcome the slow packet processing at our receiver whenever QPSK modulation scheme is used for packet transmission.

Initial Adaptation	Long Bursts	Final Adaptation
12	46.5	rest of 180 seconds

(a) High Level Strategy

P	J	F	P	J	F	P	J	F	P	J	F
1.5	1	0.5	1.5	1	0.5	1.5	1	0.5	1.5	1	0.5

(b) Initial Adaptation

P	J	F	P	J	F	P	J	F
10	5	0.5	10	5	0.5	10	5	0.5

(c) Long Bursts

P	J	F	···
4	1	0.5	···

(d) Final Adaptation

Fig. 36: Competitive Mode Strategy. P, J and F represent packet transfer, jamming and feedback mode respectively. The top row represents the state of the transceiver and the bottom row represents the corresponding duration the transceiver dwells in the state.

6.3.2 Cooperative Mode

The goal of cooperative mode is to use the spectrum in a manner which not only transfers our own packets but also allows other teams to transfer their packets. A match consists of three teams sharing the same frequency band, with each team possessing 15000 packets each of 1440 bytes and a time limit of 3 minutes. At the end of 3 minutes each team's score is calculated by adding it's number of packets successfully transferred with the maximum of that of the other two teams. Formally, let the three teams be team A, team B and team C. Let q_A, q_b and q_c be the number of packets transferred successfully by the teams respectively at the end of 3 minutes. Then the scores s_A, s_B and s_C are defined as below.

$$s_i = q_i + \max_{j \in \{A,B,C\} \setminus \{i\}} \{q_j\},\ i \in \{A, B, C\} \tag{6.1}$$

As such, each team's score can range from 0 to 30,000. Next we describe our strategy in detail.

We are given a bandwidth of 5 MHz which we split in 5 sub-bands each of width 800 KHz. Fig. 38 illustrate the frequency domain representation of the five bands. We employ transmit side spectrum sensing to detect weather a band is occupied or not. If the measured energy in a band is greater than a preset threshold, lets call it "sensing threshold", then we flag that band as being occupied otherwise empty. Once a band is detected as empty we "enable" the band and the transmitter starts packet transmission on that band. Otherwise we "disable" the band meaning we do not transmit anything on that band. Note that all the five bands are enabled only if the measured energy in all the bands in less than the sensing threshold. If none of the bands is found to be empty it enables the band with the lowest measured energy. This is done in order to prevent excessive passive behavior on our part. We have included one more policy to prevent such passive behavior. Whenever only one band is enabled, the transmitter forces packet transmission on the sub-band with second lowest observed energy if it is closest to the enabled sub-band with respect to the observed energy levels.

Fig. 37 shows the strategy for cooperative mode. Before the transmitter starts packet transmission, it senses the spectrum for empty bands. At the end of the "Sense" state it enables those bands which are deemed empty. After "Sense" state, the transmitter starts transmitting packets for 4 seconds. Then it goes into "Feedback" mode to listen to feedback from the receiver. While at the receive side, whenever the transmitter is in the "Sense" and "Packet Transmission" state the receiver goes into "Packet Reception" state. And the "Feedback" state at the receiver indicates the time during which it sends feedback to the transmitter.

Each sub-band adapts independently depending on the observed PER in that band, assuming the band is enabled. Adaptation is achieved through feedback. The receiver monitors the PER for each band and feeds back accordingly. Feedback is also used for packet reliability. In the "Feedback" state we transmit feedback on all the sub-bands. This is done in order to maximize the chance of getting the feedback through as the transmit side SNR can be low because of the adjacent transmitters.

···	Sense	Packet Transmission	Feedback	Sense	···
···	0.5	4	0.5	0.5	···

(a) Transmitter Strategy

···	Packet Reception	Feedback	Packet Reception	···
···	4.5	0.5	4.5	···

(b) Receiver Strategy

Fig. 37: Cooperative Mode Strategy

6.4 Feedback Scheme

The purpose of feedback is two fold. First to ensure link reliability and second to make sure all packets are transferred. Our metric for link reliability is packet error rate (PER). Link reliability is achieved through rate adaption which in turn is achieved via change in modulation scheme. We use BPSK, QPSK, 8PSK and 16QAM modulation schemes and fix the code rate. In competitive mode a feedback packet is of length 214 bytes which is then encoded using $(255, 214)$ Reed-Solomon code. Similarly, in cooperative mode a feedback packet is of length 318 bytes which is then encoded using two $(255, 159)$ Reed-Solomon codes. In cooperative mode, the transmitter may be subjected to low SNR conditions because of other adjacent transmitters. Hence, there is a higher chance of the feedback getting lost than that in competitive mode. A stronger RS code tries to overcome the issue of lower SNR in case the feedback packet gets through. As the feedback

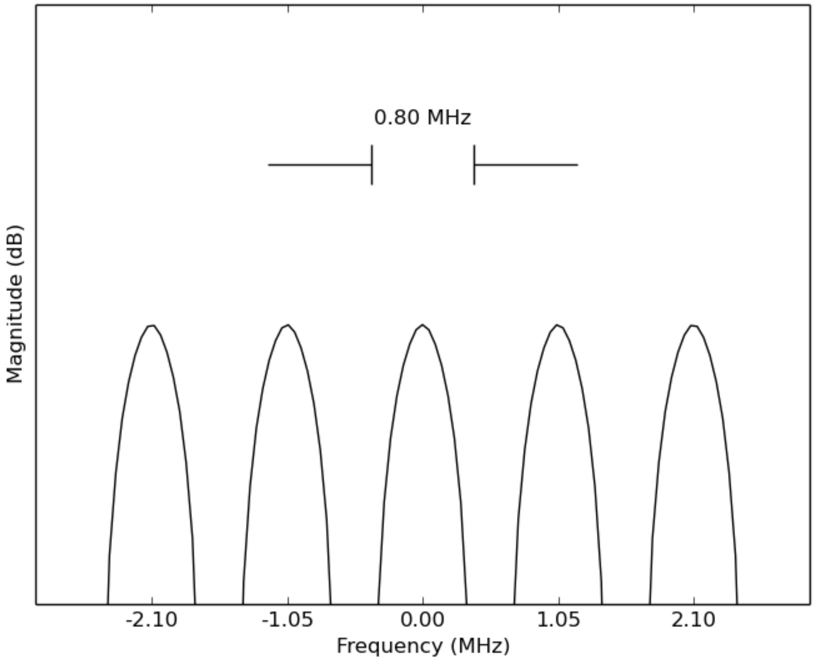


Fig. 38: Cooperative Mode Baseband Frequency Spectrum

packet is not guaranteed to reach the transmitter all the time, we need to make sure it contains the indices of all the lost encoded small packets (ESPs). Hence, we use a larger feedback packet size as compared to competitive mode.

To make sure that all the packets are transferred, the transmitter needs to know the indices of all the lost packets and a data rate that the channel allows with relatively low bit error rate. As mentioned previously, rate adaptation is achieved through changing the modulation scheme at the transmitter. This adaptation is achieved by a three state qualitative variable, which is a function of PER, a low threshold and a high threshold, sent in the feedback packet by the receiver. If the PER is below the low threshold, the receiver encodes information in the feedback packet to increase its rate to next possible higher rate. If it is already at the highest rate, then it stays put. Similarly, if the PER is above the high threshold, then the receiver encodes information in the feedback packet to lower its rate to the next possible lower rate. If it is already at the lowest rate, then it stays put. Otherwise, if the PER is between the low and the high threshold, the feedback tells the receiver to maintain its current rate.

Unless the transmitter knows the indices of all the lost packets, it will lead to redundant retransmission of packets. For example, at the end of the first pass of sending 105000 ESPs, about 10% of packets are lost, which means about 10500 packets are lost. Suppose in the next feedback packet the receiver can encode the indices of only a fraction of these 10500 lost packets. Assuming the transmitter gets the feedback packet, the transmitter will first send packets with indices it found in the feedback packet, and then start retransmitting the rest of the packets during the remainder of the packet transmission burst. Hence, we get redundant packet retransmission once the transmitter finishes transmitting the packets whose indices it received in the feedback packet. In order to overcome this, we have devised the following scheme.

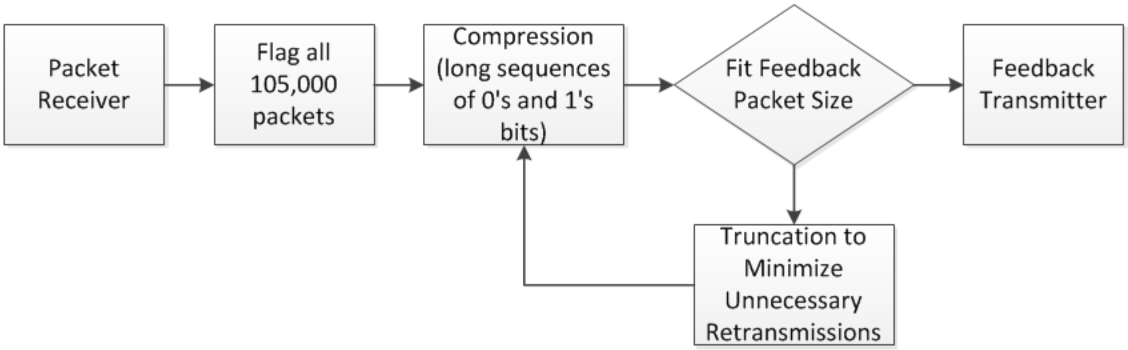

Packet Receiver
Flag all 105,000 packets
Compression (long sequences of 0's and 1's bits)
Fit Feedback Packet Size
Feedback Transmitter
Truncation to Minimize Unnecessary Retransmissions

Fig. 39: Feedback Scheme

We know before hand that there are a total of 105000 ESPs each of length 255 bytes. The unencoded feedback packet in competitive mode is only 214 bytes wide while that in cooperative mode it is 318 bytes wide. To represent each packet uniquely we need at least 17 bits. Naively we can represent each packet number as a 4 byte unsigned integer and then compress [33] all the packet numbers that need to be feedback. Instead, we can represent each of the 105000 packet numbers uniquely as a flag in a sequence of 105000 bits, which can be represented as a sequence of 13125 bytes. Then put this sequence of 13125 bytes through a compression algorithm. Because of the bursty nature of packet loss, we get contiguous sub sequences of 1's or 0's. This makes the compression algorithm work more effectively on these 13125 bytes. In the event we cannot put the indices of all the lost packets we keep truncating the indices list by half up until it fits in the feedback packet.

6.5 Summary

During this one year DARPA Spectrum Challenge we implemented real-time communication systems to tackle two important problems in today's wireless communication environment. One is the environment in which a robust and reliable link is desired in presence of interference *a.k.a*, competitive mode. While the other is the one in which different parties compete for the same slice of spectrum such that all the parties can carry out their respective communication reliably without any prior agreement on protocol *a.k.a*, cooperative mode. We also developed a novel feedback scheme which can send a number of packet indices within relatively small number of bytes.

CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1 Conclusion

To summarize, this thesis broadly deals with the problem of communication system design. The first part of the thesis addresses the problems that arise in airborne multiple input multiple output (MIMO) communication. The second part develops authentication scheme to counter primary user emulation attack (PUEA) in cognitive radio (CR) networks. The third part details the sofware-defined radio (SDR) based communication systems that we developed in the process of competing in the DARPA Spectrum Challenge.

Chapters 2 and 3 tackle problems encountered in airborne MIMO communications. Specifically, in Chapter 2 we developed a novel channel tracking scheme for airborne MIMO transceivers employing diagonal Bell Laboratories Layered Space-Time (D-BLAST) architecture. We derived an expression that gives the optimal length of data symbols used to compute the channel estimate using linear least squares method that minimizes the mean squared error under a continuously varying Rayleigh fading channel. In Chapter 3, we developed a variable rate MIMO transceiver architecture that improves bit error rate (BER) performance over rank deficient channels. We analyzed the scheme numerically using channel measurements obtained at the Air Force Research Laboratories facility at Newport, NY and showed that our scheme improves BER performance as compared to D-BLAST under rank deficient channel conditions. The numerical results are supported experimentally by developing a 2×2 MIMO system using the GNU Radio/USRP platform and thus we demonstrated that the developed scheme outperforms D-BLAST for rank deficient channels. The channel tracking mentioned earlier can be used as is with the variable rate MIMO scheme to provide an improved communication system for MIMO airborne platforms that increases the throughput by reducing the need for frequent pilot retransmissions and by enabling spatial multiplexing on ill-conditioned channel matrices.

Chapters 4 and 5 provide a complete communication system design of a countermeasure to the PUEA attack in CR networks. The developed scheme is transparent to the legacy receivers and provides a reliable mode of transmitting authentication information. We analyzed the scheme under Rayleigh fading channel conditions and found an optimal method of embedding the authentication bits into primary user (PU)'s quadrature amplitude modulation (QAM) digital constellation that minimizes the authentication BER. To experimentally verify the efficacy of the proposed authentication system, we developed a GNU Radio/USRP based SDR as described in Chapter 5. We developed a fast maximum likelihood detector that is more suitable for real time implementation. Using this setup we were able to experimentally verify the BER performance of the designed authentication system. Thus, we showed that PU authentication be achieved with arbitrary reliability at secondary users (SUs) with minimal signal degradation at legacy receivers.

Chapter 6 details our efforts leading up to the final tournament of the DARPA Spectrum Challenge to develop two software radio systems, each designed to provide communication capability in the presence of interference but with different approaches. The first system, developed for the competitive tournament, can transmit in the presence of heavy interference. On the other hand, the second system was developed for the cooperative tournament wherein we demonstrated, in principle, uncoordinated spectrum sharing.

7.2 Future Work Propositions

In this section, we describe in general the directions in which our work can be taken forward for further investigation.

The variable rate MIMO architecture proposed in Chapter 3 improved over D-BLAST in its BER performance when the channel matrices are rank deficient. Alternative schemes that utilize, for example, space time coding, combined with D-BLAST can be constructed and a more thorough comparison is warranted to justify the actual use of the variable rate MIMO via spreading. Additionally, our experimental implementation is limited to a 2×2 system. More thorough experimental studies using larger antenna arrays are needed to thoroughly understand the actual performance trade-off for the proposed architecture. A drawback of the variable rate MIMO scheme is that the current version is rather rigid in that the number of spatial streams can be chosen as a power of 2. This is due to the way spreading is implemented. This may cause under-utilization of the channel in certain scenarios. To mitigate this issue, it will be instructive to explore spreading mechanisms such that an arbitrary number of spatial streams can be pushed through the channel reliably.

In Chapters 4 and 5 we developed a physical layer authentication scheme to thwart PUEA in CR networks. The scheme developed therein not only facilitates PU authentication but also maintains PU's transmission compatibility with the legacy receivers. This latter aspect of the scheme, that allows information to be overlaid without breaking the status quo, can potentially be used to develop new applications on existing standards without having to replace the currently in-use user-devices. To illustrate this point, consider the following example: Most of the contemporary indoor positioning algorithms utilize the knowledge of ambient WiFi signatures to localize. The accuracy resulting from such a state of the art scheme has a margin of error in the range of 2-3 meters. Most of the research and development focus is directed towards improving the capability on the user side and not the infrastructure side (i.e., WiFi access points). This is done to avoid any breakage in usability of the existing users. However, if some additional information can be transmitted from the access points themselves, e.g., a common clock information, then a much higher localization accuracy may be attainable by employing techniques similar to that in GPS based localization.

This additional information can be transmitted using the developed transmission scheme such that existing user-devices are not affected but the ones that can take advantage of the additional information can enhance their localization capabilities. Thus, finding new applications which do not require high rate communication and strict backwards compatibility at the physical layer, can be a promising future research direction.

In Chapter 6 we detailed the design of software radios that were developed for the DARPA Spectrum Challenge (DSC). The radio that was developed for the cooperative tournament attempts to share a given spectrum band with two other users such that the throughput of all the three users is maximized. None of the three users are aware of each others transmission schemes, protocols or any other communication parameters. The only thing known is the frequency band to be shared. From the perspective of CR networks, this is a scenario which comes after the detection of spectrum holes. There can be potentially many heterogeneous SUs that are vying to use the spectrum holes. Therefore, there must be a mechanism in place to allow the sharing of the spectrum holes in a fair manner among the heterogeneous SUs. To achieve this, the SUs can coordinate with each other through some commonly accessible database. However, such an approach is beset by a potentially large infrastructure investment and its management cost. A much more desirable approach is to let the SUs share the spectrum in an uncoordinated manner. This preempts the need for a central authority thereby removes the potentially large investment and its management cost. However, when the the responsibility of sharing is transferred over to individual SUs, there is a need to ensure that one particular SU or a group of SUs do not dominate spectrum usage. The uncoordinated sharing does not only need to be fair, but efficient in terms of computation and power, as many envisioned CR applications may require battery operated SUs. Thus, ensuring fair and efficient access to the spectrum holes in an uncoordinated manner is an interesting research direction to explore.

APPENDIX A

PROOF OF THEOREM 1

Proof. Using the assumptions mentioned in the text, we first evaluate $\mathbf{E}(\Delta_p \Delta_p^*)$.

$$
\begin{aligned}
&\mathbf{E}(\Delta_p \Delta_q^*) \\
&= \mathbf{E}\Bigg[\sum_{k=1}^{S} \beta_k \left(e^{j2\pi f_k (N-p) T_s} - e^{j2\pi f_k N T_s}\right) \sum_{l=1}^{S} \beta_l^* \left(e^{-j2\pi f_l (N-q) T_s} - e^{-j2\pi f_l N T_s}\right)\Bigg] \\
&= \mathbf{E}\Bigg[\sum_{k=1}^{S} |\beta_k|^2 \left(e^{j2\pi f_k (N-p) T_s} - e^{j2\pi f_k N T_s}\right) \left(e^{-j2\pi f_k (N-q) T_s} - e^{-j2\pi f_k N T_s}\right)\Bigg] \\
&\quad + \mathbf{E}\Bigg[\sum_{k \neq l} \beta_k \beta_l \left(e^{-j2\pi f_l (N-p) T_s} - e^{-j2\pi f_l N T_s}\right) \left(e^{-j2\pi f_l (N-q) T_s} - e^{-j2\pi f_l N T_s}\right)\Bigg] \\
&\overset{(a)}{=} \mathbf{E}\Big[\left(1 - e^{-j2\pi f_k p T_s}\right) \left(1 - e^{j2\pi f_k q T_s}\right)\Big] \mathbf{E}\Bigg[\sum_{k=1}^{S} |\beta_k|^2\Bigg] \\
&\overset{(b)}{=} \mathbf{E}\Big[\left(1 - e^{-j2\pi f_k p T_s}\right) \left(1 - e^{j2\pi f_k q T_s}\right)\Big] \\
&= 1 - \mathrm{sinc}(2\pi f_D p T_s) - \mathrm{sinc}(2\pi f_D q T_s) + \mathrm{sinc}(2\pi f_D (p-q) T_s),
\end{aligned}
\tag{A.1}
$$

where $\mathrm{sinc}(x) = \frac{\sin(x)}{x}$. (a) because the second expectation in the second step is zero. (b) because of the assumption $\sum_{k=1}^{S} |\beta_k|^2 = 1$.

From the above expression we see that,

$$
\mathbf{E}(\Delta_p \Delta_q^*) = \mathbf{E}(\Delta_q \Delta_p^*). \tag{A.2}
$$

Also, putting $p = q$ in expression (A.1), we get,

$$\mathbf{E}(\Delta_p \Delta_p^*) = 2(1 - \text{sinc}(2\pi f_D p T_s)). \tag{A.3}$$

We now simplify the expectation term in equation (2.6). Using brute force we can show that,

$$\mathbf{E}\left[\left(\sum_{k=1}^{2} \Delta_k\right)\left(\sum_{k=1}^{2} \Delta_k^*\right)\right] = 2\left[\sum_{k=1}^{2} k - \sum_{k=1}^{2} k \ \text{sinc}(2\pi f_D k T_s)\right], \tag{A.4}$$

$$\mathbf{E}\left[\left(\sum_{k=1}^{3} \Delta_k\right)\left(\sum_{k=1}^{3} \Delta_k^*\right)\right] = 2\left[\sum_{k=1}^{3} k - \sum_{k=1}^{3} k \ \text{sinc}(2\pi f_D k T_s)\right]. \tag{A.5}$$

We now simplify the expectation term in equation (2.6). We use proof by induction. Suppose the following is true,

$$\mathbf{E}\left[\left(\sum_{k=1}^{N} \Delta_k\right)\left(\sum_{k=1}^{N} \Delta_k^*\right)\right] = 2\left[\sum_{k=1}^{N} k - \sum_{k=1}^{N} k \ \text{sinc}(2\pi f_D k T_s)\right]. \tag{A.6}$$

Now,

$$\mathbf{E}\left[\left(\sum_{k=1}^{N+1} \Delta_k\right)\left(\sum_{k=1}^{N+1} \Delta_k^*\right)\right] = \mathbf{E}\left[\left(\sum_{k=1}^{N} \Delta_k + \Delta_{N+1}\right)\left(\sum_{k=1}^{N} \Delta_k^* + \Delta_{N+1}^*\right)\right]. \tag{A.7}$$

Let, $\left(\sum_{k=1}^{N} \Delta_k\right) = D$.

$$\mathbf{E}\left[\left(\sum_{k=1}^{N+1} \Delta_k\right)\left(\sum_{k=1}^{N+1} \Delta_k^*\right)\right] = \mathbf{E}\Big[(D + \Delta_{N+1})\left(D^* + \Delta_{N+1}^*\right)\Big] \tag{A.8}$$

$$= \mathbf{E}(DD^*) + \mathbf{E}(D\Delta_{N+1}^*) + \mathbf{E}(\Delta_{N+1}D^*) + \mathbf{E}(\Delta_{N+1}\Delta_{N+1}^*). \tag{A.9}$$

We know $\mathbf{E}(DD^*)$ from equation (A.6). We need to find the last three terms.

$$\begin{aligned}
&\mathbf{E}(D\Delta_{N+1}^*) \\
&= \mathbf{E}\left[(\Delta_1 + \Delta_2 + \ldots + \Delta_N)\Delta_{N+1}^*)\right] && \text{(A.10)} \\
&= \mathbf{E}(\Delta_1\Delta_{N+1}^*) + \mathbf{E}(\Delta_2\Delta_{N+1}^*) + \ldots + \mathbf{E}(\Delta_1\Delta_{N+1}^*) && \text{(A.11)} \\
&= N - \sum_{k=1}^{N} \text{sinc}(2\pi f_D k T_s) - \sum_{k=1}^{N} \text{sinc}(2\pi f_D (N+1) T_s) \\
&\quad + \sum_{k=1}^{N} \text{sinc}(2\pi f_D (N+1-k) T_s) && \text{(A.12)} \\
&= N - N\,\text{sinc}(2\pi f_D (N+1) T_s). && \text{(A.13)}
\end{aligned}$$

From equation (A.3),

$$\mathbf{E}(\Delta_{N+1}\Delta_{N+1}^*) = 2(1 - \text{sinc}(2\pi f_D (N+1) T_s)). \tag{A.14}$$

From equations (A.2) and (A.11),

$$\mathbf{E}(D\Delta_{N+1}^*) = \mathbf{E}(\Delta_{N+1} D^*). \tag{A.15}$$

From equations (A.6), (A.9), (A.13), (A.14) and (A.15), we get

$$\begin{aligned}
&\mathbf{E}\left[\left(\sum_{k=1}^{N+1} \Delta_k\right)\left(\sum_{k=1}^{N+1} \Delta_k^*\right)\right] \\
&= 2\left[\sum_{k=1}^{N} k - \sum_{k=1}^{N} k\,\text{sinc}(2\pi f_D k T_s)\right] \\
&\quad +2(N - N\text{sinc}(2\pi f_D (N+1) T_s)) \\
&\quad +2(1 - \text{sinc}(2\pi f_D (N+1) T_s)) && \text{(A.16)} \\
&= 2\left[\sum_{k=1}^{N+1} k - \sum_{k=1}^{N+1} k\,\text{sinc}(2\pi f_D k T_s)\right]. && \text{(A.17)}
\end{aligned}$$

The last term in the above expression is of the form $\sum_{k=1}^{N} k \text{ sinc}(ck)$, where c is a constant.

$$\begin{aligned}
&\sum_{k=1}^{N} k \text{ sinc(ck)} \\
&= \sum_{k=1}^{N} k \, \frac{\sin ck}{ck} \\
&= \frac{1}{c} \sum_{k=1}^{N} \sin ck \\
&= \frac{1}{c} \, \sin\left(\frac{Nc}{2}\right) \sin\left(\frac{(N+1)c}{2}\right) \csc\left(\frac{c}{2}\right). \qquad \text{(A.18)}
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\mathbf{E}\left[\left(\sum_{k=1}^{N} \Delta_k\right)\left(\sum_{k=1}^{N} \Delta_k^*\right)\right] \\
&= 2\left[\sum_{k=1}^{N} k - \sum_{k=1}^{N} k \; sinc(2\pi f_D k T_s)\right] \qquad \text{(A.19)} \\
&= N(N+1) - \frac{\sin(\pi f_D N T_s)\sin(\pi f_D (N+1) T_s)}{\pi f_D T_s \sin(\pi f_D T_s)}. \qquad \text{(A.20)}
\end{aligned}$$

□

APPENDIX B

PROOF OF PROPOSITION 1

By our assumption that the tag bits are equally likely, the tag bit error rate conditioned on the channel is $p(\hat{t} = 1|t = 0, h)$.

$$
\begin{aligned}
&p(\hat{t} = 1|t = 0, h) \\
&= \sum_{s_i \in \mathcal{S}} (\hat{t} = 1, \hat{s} = s_i, s = s_i|t = 0, h) \\
&\quad + p(\hat{t} = 1, \hat{s} \neq s_i, s = s_i|t = 0, h) && \text{(B.1)} \\
&= \sum_{s_i \in \mathcal{S}} p(\hat{s} = s_i, s = s_i)p(\hat{t} = 1|\hat{s} = s_i, s = s_i, t = 0) \\
&\quad + p(\hat{s} \neq s_i, s = s_i)p(\hat{t} = 1|\hat{s} \neq s_i, s = s_i t = 0) && \text{(B.2)} \\
&\overset{(a)}{=} \frac{1}{M} \sum_{s_i \in \mathcal{S}} p(\hat{s} = s_i|s = s_i)p(\hat{t} = 1|\hat{s} = s_i, s = s_i, t = 0) \\
&\quad + p(\hat{s} \neq s_i|s = s_i)p(\hat{t} = 1|\hat{s} \neq s_i, s = s_i t = 0) && \text{(B.3)} \\
&\overset{(b)}{\approx} \frac{1}{M} \sum_{s_i \in \mathcal{S}} p(\hat{t} = 1|\hat{s} = s_i, s = s_i, t = 0) && \text{(B.4)} \\
&= \frac{1}{M} \sum_{s_i \in \mathcal{S}} Pr\{|y - hs_{1,i}| < |y - hs_{0,i}| \mid \hat{s} = s_i, s = s_i, t = 0\} \\
&\overset{(c)}{\approx} \frac{1}{M} \sum_{s_i \in \mathcal{S}} Q\left(|h|\sqrt{\frac{|s_{1,i} - s_{0,1}|^2}{2\sigma_z^2}}\right) && \text{(B.5)}
\end{aligned}
$$

(a) by the assumption that data symbols are equally likely. (b) follows from the assumption that $E >> E_t$ and $\frac{E_t}{\sigma_z^2} << 1$. As for (c), the expression in the previous step resembles that of BPSK error probability, with $s_{1,i}$ and $s_{0,i}$ being the antipodals signals. The average tag bit error probability with respect to the Rayleigh distributed channel h is approximated as follows.

$$\begin{aligned}
&p(\hat{t} = 1 | t = 0) \\
&\approx \mathbf{E}_h \left[\frac{1}{M} \sum_{s_i \in \mathcal{S}} Q \left(|h| \sqrt{\frac{|s_{1,i} - s_{0,1}|^2}{2\sigma_z^2}} \right) \right] && \text{(B.6)} \\
&= \frac{1}{M} \sum_{s_i \in \mathcal{S}} \mathbf{E}_h \left[Q \left(|h| \sqrt{\frac{|s_{1,i} - s_{0,1}|^2}{2\sigma_z^2}} \right) \right] && \text{(B.7)} \\
&\overset{(a)}{=} \frac{1}{M} \sum_{s_i \in \mathcal{S}} \frac{1}{2} \left(\sqrt{\frac{|s_{1,i} - s_{0,1}|^2}{2\sigma_z^2 + |s_{1,i} - s_{0,1}|^2}} \right) && \text{(B.8)}
\end{aligned}$$

(a) is the bit error probability for BPSK modulation over a fast fading Rayleigh channel [28].

REFERENCES

[1] R. Chen and J. Park, “Ensuring trustworthy spectrum sensing in cognitive radio networks,” in *Proc. 1st IEEE Workshop Networking Technologies for Software Define Radio Networks (SDR ‘06)*, Reston, VA, USA, Sep. 2006.

[2] I. Cox, M. Miller, J. Bloom, and C. Honsinger, *Digital Watermarking*. San Francisco, CA: Morgan Kaufman, 2001.

[3] DARPA Spectrum Challenge, accessed September 2013. [Online]. Available: http://www.darpa.mil/spectrumchallenge

[4] DSP and FEC Library, accessed September 2013. [Online]. Available: http://www.ka9q.net/code/fec/

[5] D. Forney, “*6.451 Principles of Digital Communication II, Spring 2005*,” (Massachusetts Institute of Technology: MIT OpenCourseWare), http://ocw.mit.edu (Accessed Oct 10, 2012). License: Creative Commons BY-NC-SA.

[6] G. J. Foschini, “Layered Space-Time Architecture for Wireless Communication in a Fading Environment When Using Multi-Element Antennas,” *Bell Laboratories Technical Journal*, vol. 1, no. 2, pp. 41–59, 1996.

[7] G. J. Foschini and M. J. Gans, “On Limits Of Wireless Communications in a Fading Environment When Using Multiple Antennas,” *Wireless Personal Commun.*, vol. 6, no. 3, pp. 311–335, 1998.

[8] G. Foschini, D. Chizhik, M. Gans, C. Papadias, and R. Valenzuela, “Analysis and performance of some basic space-time architectures,” *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 3, pp. 303–320, 2003.

[9] M. J. Gans, “Aircraft Free-Space MIMO Communications,” in *Proc 43rd Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, Nov. 2009.

[10] GNU Radio, accessed September 2013. [Online]. Available: http://www.gnuradio.org

[11] L. Goh, Z. Lei, and F. Chin, “DVB detector for cognitive radio,” in *Proc. IEEE Int. Conf. on Commun.*, Glasgow, Scotland, Jun. 2007.

[12] S. Kay, *Fundamentals of Statistical Signal Processing II: Detection Theory.* Englewood Cliffs, NJ: Prentice Hall, 1998.

[13] H. Kim and K. Shin, “In-band spectrum sensing in cognitive radio networks: Energy detection or feature detection,” in *Proc. 14th ACM Int. Conf. on Mobile Computing and Networking (MobiCom ‘08)*, San Francisco, California, USA, Sep. 2008.

[14] P. Kolodzy and I. Avoidance, “Spectrum policy task force,” *Federal Commun. Comm., Washington, DC, Rep. ET Docket*, no. 02-135, 2002.

[15] L. Lamport, “Password authentication with insecure communication,” *Commun. of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[16] J. Li, X. You, and J. Li, “Early stopping for LDPC decoding: convergence of mean magnitude (cmm),” *IEEE Commun. Lett.*, vol. 10, no. 9, pp. 667–669, 2006.

[17] S. Lin and D. Costello, *Error Control Coding: Fundamentals and Applications.* Englewood Cliffs, NJ: Prentice-Hall, 1983.

[18] J. Mitola III and G. Maguire Jr., “Cognitive radio: making software radios more personal,” *IEEE Personal Communications Magazine*, vol. 6, no. 4, pp. 13 –18, Aug 1999.

[19] Open-Access Research Testbed for Next-Generation Wireless Networks (ORBIT), accessed September 2013. [Online]. Available: http://www.orbit-lab.org/

[20] A. Paulraj and T. Kailath, "Increasing capacity in wireless broadcast systems using distributed transmission/directional reception (dtdr)," uS Patent 5,345,599.

[21] V. Pohl, P. Nguyen, V. Jungnickel, and C. von Helmolt, "Continuous flat-fading MIMO channels: Achievable rate and optimal length of the training and data phases," *IEEE Trans. Wireless Commun.*, vol. 4, no. 4, pp. 1889–1900, 2005.

[22] J. G. Proakis and M. Salehi, *Fundamentals of Communication Systems*. New York, NY: McGraw-Hill Higher Education, 2007.

[23] C. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379–423, 1948.

[24] G. Staple and K. Werbach, "The end of spectrum scarcity [spectrum allocation and utilization]," *Spectrum, IEEE*, vol. 41, no. 3, pp. 48–52, 2004.

[25] Q. Sun, D. Cox, H. Huang, and A. Lozano, "Estimation of continuous flat fading MIMO channels," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 549–553, 2002.

[26] X. Tan, K. Borle, W. Du, and B. Chen, "Cryptographic link signatures for spectrum usage authentication in cognitive radio," in *Proc. 4th ACM conf. on Wireless Network Security (WiSec '11)*, Hamburg, Germany, Jun. 2011.

[27] E. Telatar, "Capacity of Multi-antenna Gaussian Channels," *Europ. Trans. Telecommun.*, vol. 10, no. 6, pp. 585–595, 1999.

[28] D. Tse and P. Viswanath, *Fundamentals of Wireless Communications*. Cambridge, UK: Cambridge University Press, 2005.

[29] USRP: Universal Software Radio Peripheral, accessed September 2013. [Online]. Available: http://www.ettus.com

[30] P. Yu, J. Baras, and B. Sadler, "Physical-layer authentication," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 38–51, 2008.

[31] Q. Yuan, P. Tao, W. Wang, and R. Qian, "Cyclostationarity-based spectrum sensing for wideband cognitive radio," in *Proc. WRI Int. Conf. on Commun. and Mobile Computing*, Kunming, Yunnan, China, Jan. 2009.

[32] L. Zheng and D. Tse, "Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels," *IEEE Trans. Inf. Theory*, vol. 49, pp. 1073–1096, May 2003.

[33] zlib:A Massively Spiffy Yet Delicately Unobtrusive Compression Library, accessed September 2013. [Online]. Available: http://www.zlib.net

VITA

NAME OF AUTHOR: Kapil M. Borle

PLACE OF BIRTH: Aurangabad, Maharashtra, India

DATE OF BIRTH: July 22, 1984

GRADUATE AND UNDERGRADUATE SCHOOLS ATTENDED:

Syracuse University, Syracuse, NY, USA, 2006-2015

University of Pune, Pune, Maharashtra, India, 2001-2005

DEGREES AWARDED:

M.S. Electrical Engineering, 2011, Syracuse University, Syracuse, NY, USA

B.E. Electronics and Telecomm. Engg., 2005, University of Pune, Pune, Maharashtra, India

PROFESSIONAL EXPERIENCE:

Engineering Intern, Bosch Security Systems, Lancaster, PA, May 2007 - Aug 2007

Research Intern, Mitsubishi Electric Research Labs, Cambridge, MA, May 2014 - Nov 2014

PUBLICATIONS:

- X. Tan, K. M. Borle, W. Du and B. Chen, “Cryptographic Link Signatures For Spectrum Usage Authentication In Cognitive Radio”, *Proc. of the 4th ACM conference on Wireless Network Security*, Hamburg, Germany, Jun. 2011.
- K. M. Borle, B. Chen and M. J. Gans, “Channel tracking for D-BLAST for airborne platforms”, *Proc. 45th Asilomar Conference on Signals, Systems and Computers*, Monterey, CA, Nov. 2011.
- K. M. Borle, B. Chen and W. Du, “A Physical Layer Authentication Scheme For Countering Primary User Emulation Attack”, *Proc. of the 38th International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Vancouver, Canada, May 2013.
- M. J. Gans, K. M. Borle, B. Chen, T. Freeland, D. McCarthy, R. Nelson, D. Overrocker and P. Oleski, “Enhancing Connectivity of Unmanned Vehicles Through MIMO Communications”, *Proc. of the 2013 IEEE 78th Vehicular Technology Conference*, Las Vegas, Sep. 2013.
- K. M. Borle, F. Zhu, Y. Zhao and B. Chen, “A Software Radio Design for Communications in Uncoordinated Networks”, *Proc. of the 2014 IEEE Workshop on Signal Processing Advances in Wireless Communications*, Toronto, Canada, June 2014.
- K. M. Borle, B. Chen and W. Du, “Physical Layer Spectrum Usage Authentication In Cognitive Radio: Analysis and Implementation”, to appear in the *IEEE Trans. on Information Forensics and Security*.