Spring 2012

Experimental investigation of RF fading channels and receiver detection

Saurav Kumar Subedi

Department:

EXPERIMENTAL INVESTIGATION OF RF FADING CHANNELS AND RECEIVER DETECTION

by

SAURAV KUMAR SUBEDI

A THESIS

Presented to the Faculty of the Graduate School of the

MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY

In Partial Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

2012

Approved by

Dr. YAHONG ROSA ZHENG
Dr. STEVEN GRANT
Dr. MACIEJ ZAWODNIOK
Dr. MOHAMMAD TAYEB GHASR

PUBLICATION THESIS OPTION

This thesis has been prepared in two papers - the first paper (pages 5 - 21) has been published in IEEE Military Communications Conference (MILCOM) 2011 and the second paper (pages 22 - 37) has been accepted for publication in Society of Photo-Optical Instrumentation Engineers (SPIE) Defense, Security and Sensing Conference 2012. Details of the papers included in this thesis are listed below.

1. Saurav Subedi, Huang Lou, Fei Ren, Mingxi Wang, Y.R. Zheng, **Validation of Triply Selective Fading Channel Model Through MIMO Testbed and Experimental Results**, has been published in IEEE Military Communication Conference (MILCOM) 2011.

2. Saurav Subedi, Zhonghai Wang, Y.R. Zheng, **Improving Detection Range via Correlation of Long PN Codes**, has been accepted for publication in SPIE Defense, Security and Sensing 2012.

ABSTRACT

This thesis includes experimental investigation of Multiple Input Multiple Output (MIMO) Radio Frequency (RF) fading channels and detection of superregenerative receivers. Details of experiment design and hardware implementation, data acquisition and analysis, and results for both studies are chronicled into two papers.

The first paper investigates the validity of the discrete time triply selective fading channel model for fixed mobile-to-mobile MIMO channels. A 2×2 MIMO-OFDM testbed using the Altera Stratix III EP3SL150F field programmable gate array (FPGA) DSP development kit is used for acquiring experimental data. Subsequent offline signal processing and analysis are done in MATLAB. The Channel Impulse Response (CIR) is estimated using the Time domain Least Squares (LS) method. The channel coefficient covariance matrix is decomposed into its Kronecker factors - the spatial correlation matrix, inter-tap correlation matrix, and temporal correlation matrix. This study verifies the theoretical hypothesis and simulation results.

The second paper proposes a novel method for detection of the superregnerative RF receivers. The algorithm is based on active stimulation and correlation of long pseudonoise (PN) sequences. An experimental setup is established using the Universal Software Radio Peripheral (USRP) as the primary component. Simulation results show that the maximum length PN sequences exhibit the best correlation properties among different potential stimulation signals. Proposed method improves range and accuracy of detection as compared to the passive detection and power detection methods.

ACKNOWLEDGMENTS

I would like to extend my gratitude towards all who have been an essential part of my experience as a graduate student. Their support and guidance has been instrumental in my journey towards the completion of this thesis.

First, I would like to thank my advisor Dr. Yahong Rosa Zheng for her professional guidance and forbearance throughout my learning process at Missouri S&T as a graduate student and a research assistant. I would also like to thank Dr. Zhonghai Wang and Dr. Mohammad Tayeb Ghasr for their keen guidance while I was learning the intricacies of experimental research. I would also like to express many thanks to Dr. Steven Grant and Dr. Maciej Zawodniok for their kind support as committee members.

I owe all my success and achievements to my parents, Dr. Bhawani Shankar Subedi and Mrs. Sanila Subedi. Their love and support has been the most significant factor all my life and also while I worked towards my Master's Degree. I thank my sister, Sushmita Subedi, for her love, friendship and all those moments of happiness while I was away from home. Thank you my love, Sushmita Arjyal, for being there at all times with unconditional love, support and an unfaltering belief. You all inspire me to grow not only as a professional but also as a good human being.

Finally, I would like to thank all my friends, who helped me feel at home during my stay at Missouri S&T. Many thanks to Dr. Bipul Luitel for his warm friendship that will always remain special to me.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

1. INTRODUCTION

Radio Frequency (RF) channels exhibit variations over time and frequency. Multitude of parameters define the RF channel characteristics. Theoretical models and simulation studies generally assume idealized conditions to reduce mathematical and computational complexities. Experimental results may, therefore, deviate significantly from the idealized results.

This thesis comprises of two independent experimental studies involving the RF channels. The first paper investigates the validity of the discrete-time triply selective fading channel model using experimental data acquired from an RF Multiple Input Multiple Output (MIMO) testbed. A 2×2 MIMO-OFDM testbed is developed using the Altera Stratix III EP3SL150F field programmable gate array (FPGA) DSP development kit [1]. A series of indoor fixed mobile-to-mobile communication is established to acquire experimental data for channel sounding. The second paper proposes an algorithm based on the active stimulation and correlation method for detection of the superregenerative RF receivers. The algorithm is verified through MATLAB simulations and is implemented using the Universal Software Radio Peripheral (USRP) and associated hardware elements. A wireless doorbell, a commercially available superregenrative receiver, is used as the target for detection.

The MIMO channels exhibit triply selective fading characteristics owing to selectivity in time, frequency and space. This results in temporal correlation, inter-tap correlation, and spatial correlation. The discrete time triply selective fading channel model for the MIMO systems states that their channel coefficient covariance matrix can be expressed as a Kronecker product of the spatial, temporal and intertap correlation matrices under specific assumptions - the power delay profile being similar for all subchannels and the normalized temporal correlation and spatial correlation

being identical for all resolvable multipaths. This model is experimentally validated and an estimation method is proposed to quantitatively measure the correlation matrices from the channel impulse response (CIR) of the MIMO channels. A method is proposed to decompose the channel coefficient covariance matrix into its Kronecker factors.

The experiment for channel sounding is carried out in two different environments - one with both transmitter and receiver located in the same room and the other with the transmitter and receiver located in two different rooms across a hallway. The testbed is designed to support multiple modulation schemes (QPSK, 8PSK and 16QAM). Time domain least squares (LS) method is used for CIR estimation for each subchannel. The CIRs are estimated by using cascading windows method across the length of a long probing sequence. The channel coefficient covariance matrix of the MIMO channel is calculated using the CIR estimations. A method is proposed to decompose the covariance matrix into the spatial correlation matrix and inter-tap covariance matrix. Since the experiment involves fixed mobile-to-mobile communication setup, the temporal correlation is not significant. Correlation Matrix Distance (CMD) is used as a metric to prove identical spatial structure of the intertap covariance matrices for all subchannels. This allows us to compute an average intertap covariance matrix. This allows us to estimate the spatial correlation matrix using the proposed method. It is, thus, verified that the channel coefficient covariance matrix can be written as a Kronecker product of separable spatial, intertap, and temporal correlation matrices, provided the underlying assumptions are satisfied.

The second paper proposes an algorithm for detecting the superregenerative RF receivers using active stimulation and correlation method. The superregenerative receivers can be detected using the unintended emissions from their circuitry. This idea of detecting and identifying electronic devices based on their unintended electromagnetic emissions has been awarded a US patent [2]. Such emissions can

be detected passively. However, passive detection of these receivers is difficult in noisy environments. The emissions from these receivers are stronger when the active stimulation method is used. The stimulated emissions can be used for detection of the RF receivers consistently over a longer range. Choice of the stimulation signal affects the performance of the detection algorithm. It is established through simulation analysis that the maximal length pseudonoise sequences (m-sequences) exhibit superior correlation properties among different options for the stimulation signal. A detection algorithm based on active stimulation and correlation of long PN sequences is proposed. An experiment setup is developed to test the viability and performance of the algorithm. The proposed detection method is practically implemented and simulation results are verified through experimental results. Results show that the proposed algorithm performs better than the passive detection and power detection methods. The range and accuracy of detection is significantly improved even in noisy conditions.

The experiment setup consists of the Universal Software Radio Peripherals (USRPs) [3] equipped with wideband transceiver daughterboards, personal computers (PC) and VHF/ UHF wearable antennas [4]. A Simulink model is developed for generating the stimulation signal. The USRP-Simulink interface provides options to vary transmission/reception parameters such as upconversion/downconversion frequency and transmission/reception gain. A high speed USB connection is used for communication between the PC and the USRP. The long PN sequences are generated using Simulink. The USRP is used to transmit the stimulation signal at the operating frequency of the wireless doorbell. The stimulated emissions are radiated from circuit elements of the wireless doorbell at the carrier frequency and its harmonics. These emissions are modulated with the PN sequence. First harmonic, the strongest unintended emission, is downconverted by the USRP and the PN sequence is extracted. Since the response of the superregenerative receiver drifts in frequency with

the variation in input power, a frequency searching algorithm is implemented before extracting the PN sequence. Estimate of the PN sequence is cross-correlated with the known transmitted sequence. A high cross-correlation gain indicates the presence of the target within a detection range. The experiment is repeated for m-sequences of lengths 63, 1023, 2047, 4095 and 8191 bits. A maximum detection distance of 62 feet is achieved for an 8191 bit m-sequence. The proposed algorithm outperforms the passive detection method and the power detection method in the range and accuracy of detection.

References

[1] Altera Stratix III 3SL150 Development Board Reference Manual, http://www.altera.com/literature/manual/rm_stratixiii_dev_kit_host_board.pdf

[2] D. Beetner, S. Seguin, T. Hubing, Electromagnetic Emissions Stimulation and Detection System, Dec. 9, 2008, U.S. Patent no. 7,464,005.

[3] Ettus Research USRP1 Bus Series Datasheet, https://www.ettus.com/content/files/Ettus_USRP1_DS_FINAL_1.27.12.pdf

[4] Octane VHF/UHF Wearable Antennas Datasheet, http://www.pharad.com/pdf/VHF%20Wearable%20Antenna%20Datasheet.pdf

PAPER

1. Validation of Triply Selective Fading Channel Through MIMO Testbed and Experimental Results

Saurav Subedi, Huang Lou, Fei Ren, Mingxi Wang, and Y. R. Zheng
Department of Electrical and Computer Engineering,
Missouri University of Science and Technology, Rolla, MO 65409

Abstract

The Multiple-input Multiple-Output (MIMO) channel is often triply selective, meaning that it has spatial, temporal and inter-tap correlation. The temporal correlation is well characterized by its Doppler spectrum, but the spatial and inter-tap correlation and their impact on the MIMO channels are less studied in the literature. A MIMO testbed has been established to measure the impulse response of the MIMO channels and an estimation method is developed to quantitatively measure the correlation matrices from experimental data.

1.1. Introduction

The Multiple-Input Multiple-Output (MIMO) channel is analyzed as a triply-selective fading channel in the existing literature [1], [2]. This model accounts for space-selective, time-selective and frequency-selective nature of the MIMO channels. It is shown in [1] that correlation between channel coefficients of the discrete-time MIMO channel can be written as a Kronecker product of the temporal correlation, inter-tap correlation and spatial correlations. However, it is argued in [2] that this model is not accurate and the Kronecker product for the spatial correlations, in

general, does not hold in the case of a frequency selective channel. Recently, the underlying assumptions in [1] are clarified in [3] and emphatic conclusions are drawn to approve the accuracy of this discrete time model for MIMO triply selective fading channels. Other works devoted to the spatial/temporal correlation properties of mobile-to-base station channels include [4] - [5]. A general space-time cross-correlation function incorporating a wide range of parameters of the MIMO fading channel is proposed in [4]. Vector autoregressive (AR) stochastic models are proposed in [6] to simulate multiple cross-correlated rician fading channels. Joint effect of the spatial and temporal correlation is studied in [5] and an analysis of ergodic capacity of a MIMO channel is presented based on the transmit and receive antenna correlation matrices.

This paper validates the triply selective fading channel model through experimental results for fixed mobile-to-mobile MIMO channels. We verify the results through the decomposition of the channel coefficient covariance matrix into its Kronecker factors. Approaches for decomposition of the Kronecker product into its components are suggested in [7]. However, those methods are applicable only for the real matrices. In this paper, we propose a method for approximating the factors of a Kronecker product, real or complex. Experimental data from a MIMO testbed is

used to estimate the channel impulse response (CIR) and quantitatively estimate the spatial and inter-tap correlation matrices.

1.2. Discrete-Time Triply Selective Fading Model

The input-output relationship of the MIMO channel in discrete-time is described as [1]

$$\mathbf{y}(k) = \sum_{q=-Q_1}^{Q_2} \mathbf{H}(k,q) \cdot \mathbf{x}(k-q) + \mathbf{v}(k) \tag{1.1}$$

where k is the time index, Q_1 and Q_2 are non-negative integers representing the range of delay taps yielding the total channel length $Q = Q_1 + Q_2 + 1$, $\mathbf{x}(k) = [x_1(k), x_2(k), ...x_P(k)]^t$ is the transmitted signal vector, $\mathbf{y}(k) = [y_1(k), y_2(k), ...y_O(k)]^t$ is the received vector and $\mathbf{v}(k) = [v_1(k), v_2(k), ...v_O(k)]^t$ is the additive white gaussian noise. The superscript $(.)^t$ notation represents the matrix transpose operator.

The MIMO channel coefficient matrix $\mathbf{H}(k,q)$ at time instant k and delay tap q is defined by

$$\mathbf{H}(k,q) = \begin{pmatrix} h_{1,1}(k,q) & \cdots & h_{1,P}(k,q) \\ \vdots & \ddots & \vdots \\ h_{O,1}(k,q) & \cdots & h_{O,P}(k,q) \end{pmatrix} \tag{1.2}$$

We reshape the matrix $\mathbf{H}(k,q)$ to an $(OPQ) \times 1$ coefficient vector as

$$\mathbf{h}_{vec}(k) = [\mathbf{h}_{1,1}(k), .., \mathbf{h}_{1,P}(k) \mid .. \mid \mathbf{h}_{O,1}(k), .., \mathbf{h}_{O,P}(k)]^t \tag{1.3}$$

where $\mathbf{h}_{o,p}(k)$ is the coefficient vector of the(o,p)-th sub-channel given by $\mathbf{h}_{o,p}(k) = [h_{o,p}(-Q_1,k),\ ...,\ h_{o,p}(Q_2,k)]$.

It is stated in [1] that the stochastic fading channel coefficient vector, $\mathbf{h}_{vec}(k)$, is zero-mean gaussian distributed and its covariance matrix, $\mathbf{R}$ is given by

$$\begin{aligned}\mathbf{R} &= E[\mathbf{h}_{vec}(k_1)\cdot\mathbf{h}_{vec}^{H}(k_2)] \\ &= (\mathbf{\Psi}_{Rx}\otimes\mathbf{\Psi}_{Tx}\otimes\mathbf{\Psi}_{Tap})\cdot J_0[2\pi f_d(k_1-k_2)T_s]\end{aligned} \tag{1.4}$$

where $(.)^H$ denotes the Hermitian operator, $\otimes$ denotes the Kronecker product, $\mathbf{\Psi}_{Rx}$ and $\mathbf{\Psi}_{Tx}$ are the spatial correlation matrices at the receiver and transmitter respectively and $\mathbf{\Psi}_{Tap}$ is the intertap covariance matrix. These matrices are defined in (1.5), (1.6) and (1.7). The factor $J_0[2\pi f_d(k_1-k_2)T_s]$ describes the temporal correlation where f_d is the maximum doppler frequency and T_s is the sampling period. $J_0(.)$ is the zeroth order Bessel function.

$$\mathbf{\Psi}_{Rx} = \begin{pmatrix} \rho_{Rx}(1,1) & \cdots & \rho_{Rx}(1,O) \\ \vdots & \ddots & \vdots \\ \rho_{Rx}(O,1) & \cdots & \rho_{Rx}(O,O) \end{pmatrix} \tag{1.5}$$

$$\mathbf{\Psi}_{Tx} = \begin{pmatrix} \rho_{Tx}(1,1) & \cdots & \rho_{Tx}(1,P) \\ \vdots & \ddots & \vdots \\ \rho_{Tx}(P,1) & \cdots & \rho_{Tx}(P,P) \end{pmatrix} \tag{1.6}$$

$$\mathbf{\Psi}_{Tap} = \begin{pmatrix} \psi(-Q1,-Q1) & \cdots & \psi(-Q1,Q2) \\ \vdots & \ddots & \vdots \\ \psi(Q2,-Q1) & \cdots & \psi(Q2,Q2) \end{pmatrix} \tag{1.7}$$

where $\rho_{Rx}(m,p)$ is the receive correlation coefficient between the antennas m and p. Similarly, $\rho_{Tx}(n,q)$ is the transmit correlation coefficient between the n and q transmit antennas. Elements of the intertap covariance matrix is determined according to the power delay profiles.

This paper focuses on the validation of the triply selective fading channel model using (1.4) through the estimation of the spatial correlation matrices and the intertap covariance matrix.

1.3. Testbed and Experiment

A 2×2 MIMO-OFDM testbed has been developed using the Altera Stratix III EP3SL150F field-programmable gate array (FPGA) DSP development kit. The discrete-time MIMO triply selective fading channel model in [1] is the basis for the design of this testbed. Hardware implementation of the discrete-time MIMO triply selective fading channel emulators is proposed in [8].

At the transmitter side, two independent data streams are generated in the Stratix III development kit. The outputs are then up-converted to an intermediate frequency (IF) of 17.5 MHz and then the signals are fed into the digital upconverter, RF2-3000UCV1, to be transmitted at 915 MHz. MPA-10-40 is used for power amplification. Devices AFG3252 and FS725 are the clock sources for all other devices. The setup architecture of the transmitter is shown in Fig. 1.1.

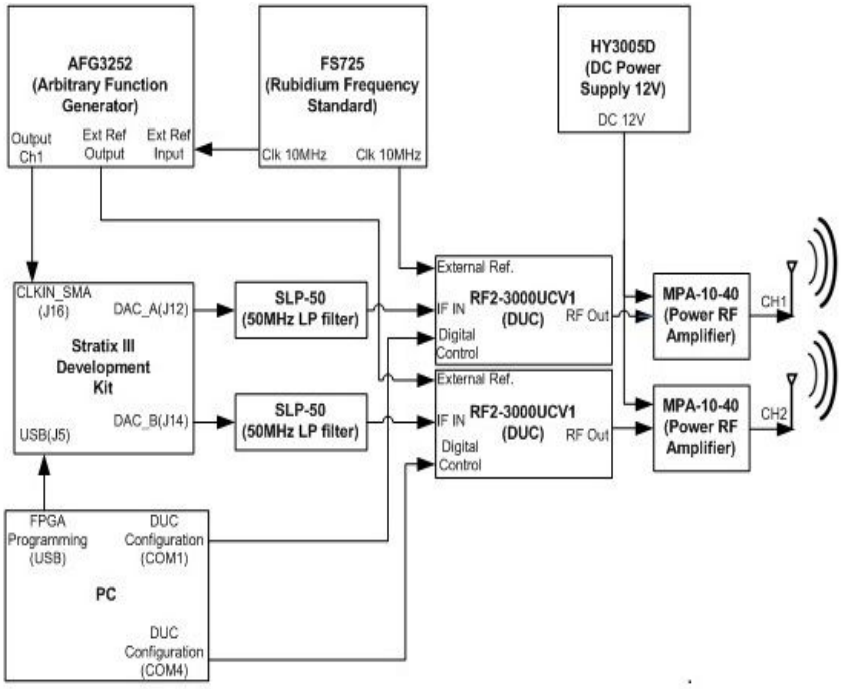

Figure 1.1 Transmitter Setup Architecture

At the receiver side, the RF signals are first down-converted to an IF of 70 MHz by the downconverter, RF200-2500RV1. Baseband data streams are then generated and recorded in the Stratix III development kit and transfered to PC. Devices AFG3252 and FS725 provide clock sources. The receiver setup architecture is shown in Fig. 1.2.

A bandwidth configuration of 3.90 MHz is used in this testbed. The number of OFDM subcarriers is 256 and a cyclic prefix length of 64 samples is used. Experiment has been carried out using three different modulation schemes (QPSK, 8PSK and 16QAM). All received signals are utilized for channel estimation. Although BPSK is sufficient for channel sounding, the transceiver was originally designed for MIMO communications, rather than channel sounding only. Measurements are done for two different experimental setups - one with both transmitter and receiver located in the same room (inside 208) and the other with transmitter and receiver located in two

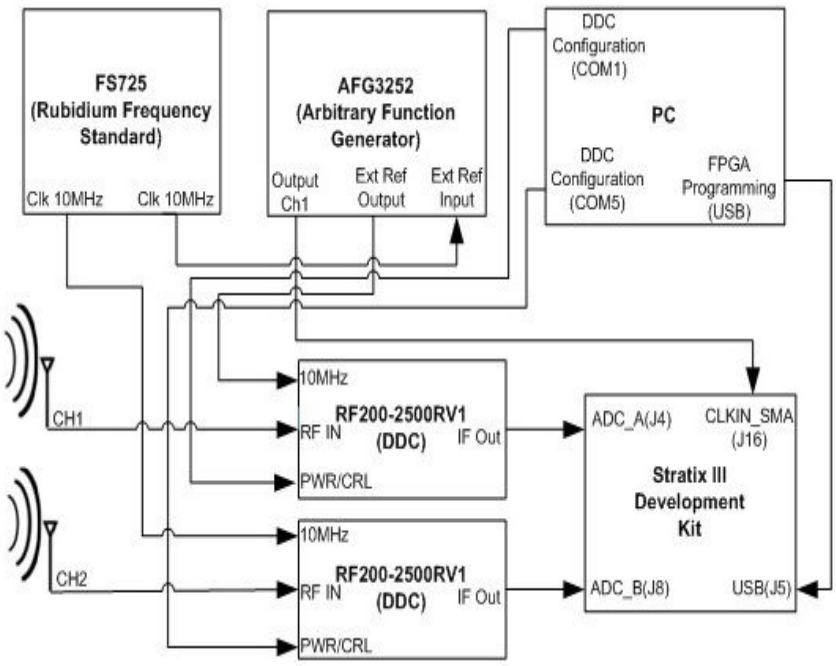

Figure 1.2 Receiver Setup Architecture

different rooms (208 and 212) across a hallway as shown in the floor plan in Fig. 1.3. The rooms are in Emerson Electric Co. Hall, Missouri University of Science and Technology.

Experimental data from this testbed is used for channel estimation and subsequent analysis.

1.4. Procedure, Results and Analysis

1.4.1. Channel Estimation. The Time Domain Least Squares (LS) method is used for the estimation of channel impulse response (CIR) for each subchannel of the 2×2 MIMO system based on the known training sequence and received sequence.

Figure 1.3 Floorplan of the Rooms Used for the Experiment

The LS estimation, detailed in chapter 8 in [9], is obtained as

$$\widehat{\mathbf{h}}_{LS} = (\mathbf{X}^H\mathbf{X})^{-1}\mathbf{X}^H\mathbf{y} \tag{1.8}$$

where $(.)^H$ and $(.)^{-1}$ represent the hermitian and inverse operations respectively, $\mathbf{X}$ is the circulant training sequence matrix and $\mathbf{y}$ is the received sequence. The matrix $\mathbf{X}$ is formed as

$$\mathbf{X} = \begin{pmatrix} x_Q & \cdots & x_1 & x_0 \\ x_{Q+1} & \cdots & x_2 & x_1 \\ \vdots & \ddots & \vdots & \\ x_{Q+P-1} & \cdots & x_P & x_{P-1} \end{pmatrix} \tag{1.9}$$

where Q is the number of channel taps and P is the number of pilot data for each antenna.

A long probing sequence is transmitted and the CIRs are estimated progressively by using cascading windows of size $N_p = 120$ symbols. The 30-tap CIRs of the four subchannels are shown in Fig. 1.4 where 80 cascading windows are used across the length of the transmitted data sequence. Although the signal bandwidth is only 3.9 MHz, the baseband equivalent channel did experience multipath delay spread spanning 30 taps. This is because both transmitter and receiver antennas were placed very low, only a meter above the floor. This is different from the case where one end is placed very high like a base station where multipath may not be significant. This demonstrates the difference between mobile-to-mobile channel and base-station to mobile channel. The number of cascading windows can be increased or overlapping windows can be used for the estimation of CIRs of highly scattering channels if needed.

1.4.2. Estimation of the Channel Coefficient Covariance Matrix. The channel coefficient covariance matrix is calculated using the estimated channel coefficients. The $(OPQ \times OPQ)$ covariance matrix, $\mathbf{R}$, is calculated using (1.4). Magnitude of the estimated channel coefficient covariance matrix is shown in Fig. 1.5.

1.4.3. Decomposition of the Kronecker Product. The Kronecker product of two matrices A and B is defined as

$$\mathbf{C} = \mathbf{A} \otimes \mathbf{B} = \begin{pmatrix} a_{11}\mathbf{B} & \cdots & a_{1n}\mathbf{B} \\ \vdots & \ddots & \vdots \\ a_{m1}\mathbf{B} & \cdots & a_{1n}\mathbf{B} \end{pmatrix} \tag{1.10}$$

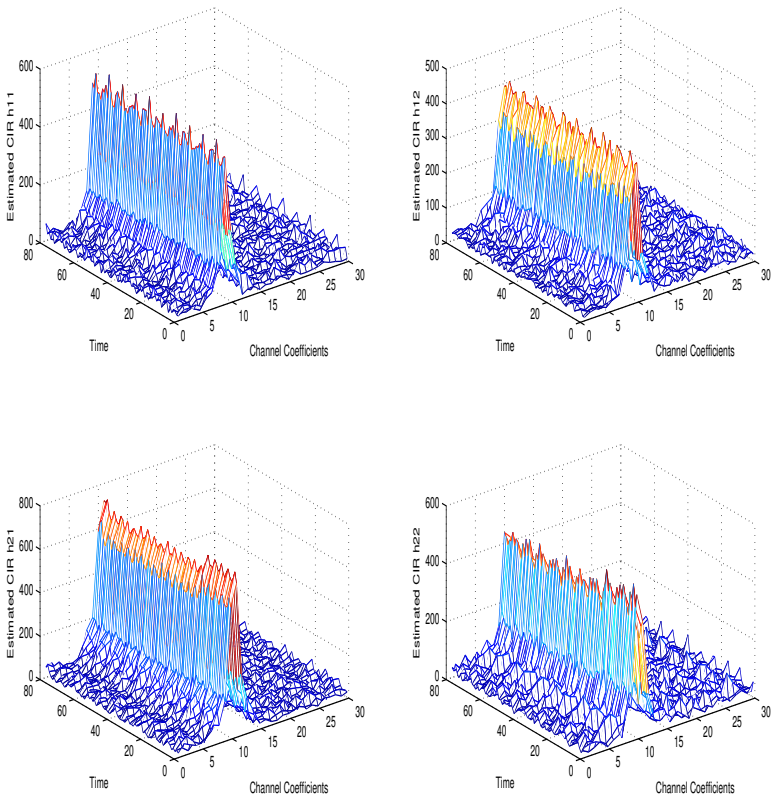

Figure 1.4 Magnitudes of Channel Impulse Responses for Four Subchannels

where $\mathbf{A}$ is $(m \times n)$, $\mathbf{B}$ is $(p \times q)$ matrix, and $\mathbf{C}$, the resultant Kronecker product is of size $(mp \times nq)$.

The problem at hand is to find the estimations of $\mathbf{A}$ and $\mathbf{B}$ from a given Kronecker product $\mathbf{C}$. Let us consider the first block of elements of matrix $\mathbf{C}$, say $\mathbf{C}_{11}$ which is a $(p \times q)$ matrix given by

$$\mathbf{C}_{11} = a_{11}\mathbf{B} \tag{1.11}$$

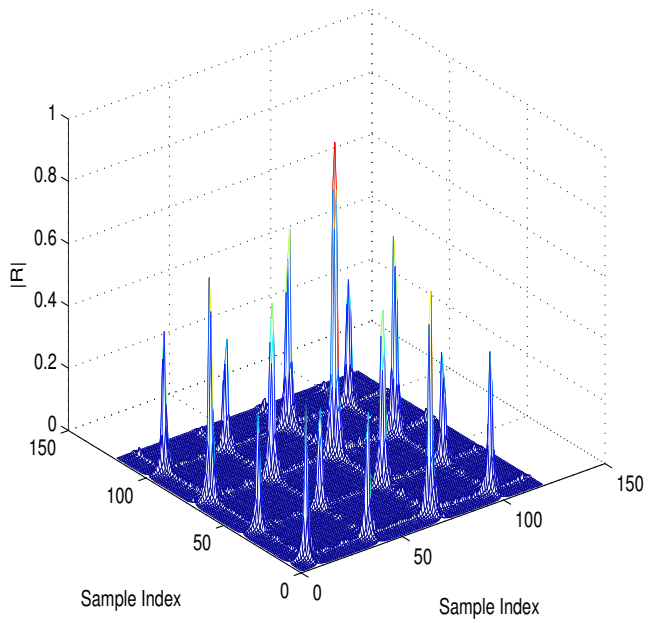

Figure 1.5 Magnitude of Estimated Channel Coefficient Covariance Matrix

If we calculate an ensemble average of all the elements of $\mathbf{C}_{11}$, that essentially results in scalar multiplication of a_{11} and mean of all the elements of $\mathbf{B}$ as shown in 1.12.

$$E[\mathbf{C}_{11}] = a_{11}E[\mathbf{B}] \tag{1.12}$$

This isolates the first element of $\mathbf{A}$ from the Kronecker product. We repeat the same process to obtain other elements of $\mathbf{A}$. The resulting estimation of matrix $\mathbf{A}$, therefore, is a scaled version of the actual $\mathbf{A}$ and retains its spatial properties.

In this paper, we estimate the spatial correlation matrix $\mathbf{\Psi}_{Trx}$ from the channel coefficient covariance matrix $\mathbf{R}$ using the method explained in (1.12).

1.4.4. Estimation of Intertap Covariance Matrix and Spatial Correlation Matrix. We estimate the $(Q \times Q)$ intertap covariance matrices for each subchannel. Using correlation matrix distance (CMD) as a metric [10], we show that these intertap covariance matrices have identical spatial structure. CMD, the distance between two correlation matrices **R1** and **R2** is defined as

$$d_{corr}(\mathbf{R1}, \mathbf{R2}) = 1 - \frac{tr\{\mathbf{R1R2}\}}{\|\mathbf{R1}\|_f \|\mathbf{R2}\|_f} \tag{1.13}$$

where $tr\{.\}$ represents the trace of the matrix and $\|.\|_f$ is the Frobenius norm. CMD becomes zero if the correlation matrices are equal up to a scaling factor and one if they differ from each other. The smaller value, thus, verifies that the matrices are spatially identical. Results are summarized in Table 1.1 for data obtained from different experimental setups.

Table 1.1 Comparison of Correlation Matrices Using CMD

Experiment Setup	**Attenuation (dB)**	**CMD** $R11, R12$	**CMD** $R11, R21$	**CMD** $R11, R22$	**CMD** $R21, R12$	**CMD** $R21, R22$	**CMD** R, R_{verify}
In 208	22	0.0259	0.0129	0.0959	0.0259	0.0713	0.0196
	26	0.0255	0.0169	0.5789	0.0255	0.0744	0.0966
	30	0.0159	0.0192	0.3133	0.0159	0.0647	0.0465
208 and 212	2	0.2550	0.0822	0.1003	0.2550	0.0908	0.0942
	6	0.0751	0.0230	0.0785	0.0751	0.0569	0.0355
	10	0.1208	0.0244	0.0690	0.1208	0.1433	0.0403

These results comply with the assumption in [3] that the power delay profile of the physical channel model is identical for all transmit and receive antenna indices. We compute an average intertap covariance matrix and use it as one of the Kronecker factors of the channel coefficient covariance matrix to estimate the spatial correlation

matrix. The spatial similarity among the intertap covariance matrices of the four subchannels can be observed in Fig. 1.6. The average intertap covariance matrix, $\mathbf{\Psi}_{Tap}$, is shown in Fig. 1.7.

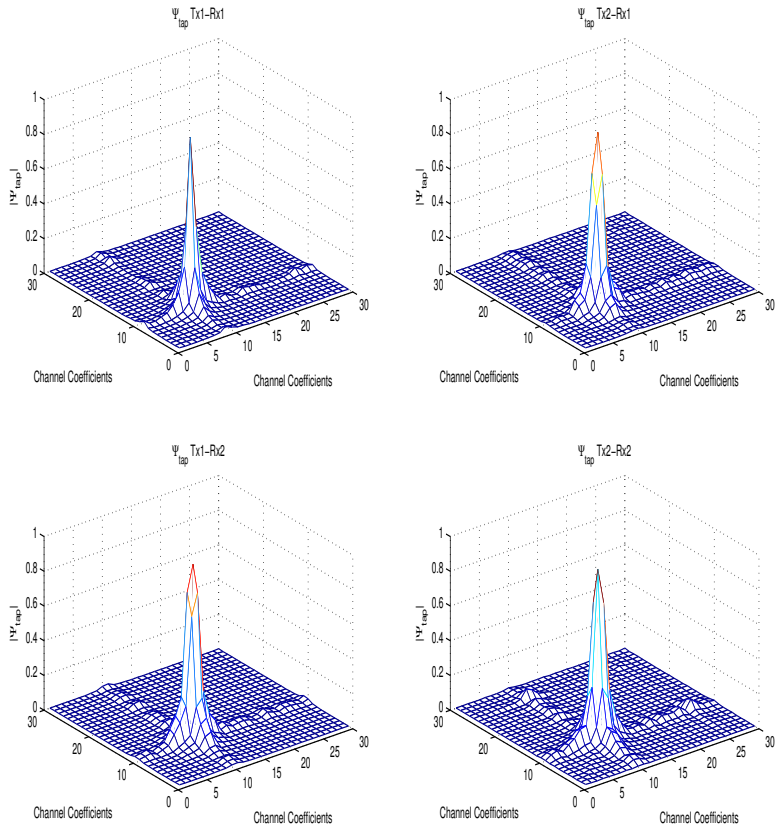

Figure 1.6 Magnitudes of Intertap Covariance Matrices for Each Subchannel

The elements of the spatial correlation matrix are estimated from the channel coefficient covariance matrix $\mathbf{R}$. The process in (1.12) yields a matrix spatially identical with $\mathbf{\Psi}_{TRx}$. We again calculate the Kronecker product of the estimated spatial

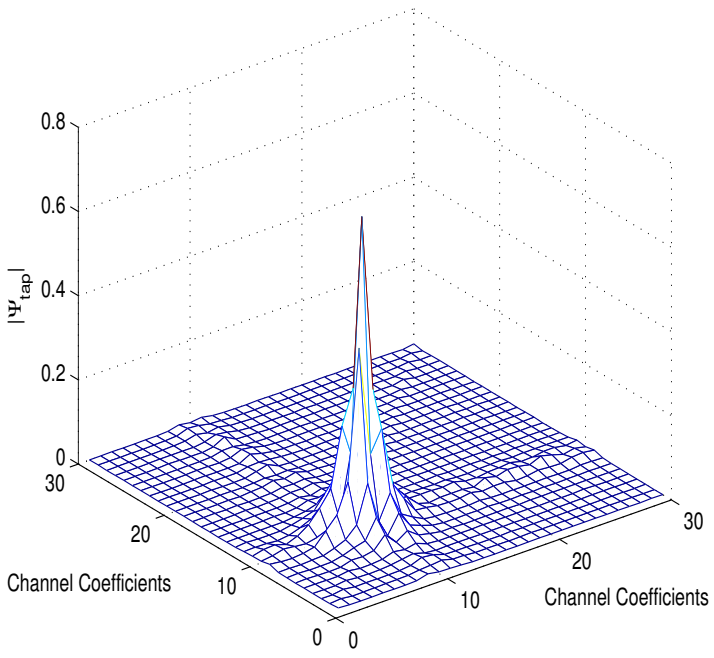

Figure 1.7 Magnitude of Averaged Intertap Covariance Matrix,Ψ_{Tap}

correlation matrix,$\mathbf{\Psi}_{TRx}$ and the average intertap covariance matrix, $\mathbf{\Psi}_{Tap}$ using

$$\mathbf{R}_{verify} = \mathbf{\Psi}_{TRx} \otimes \mathbf{\Psi}_{Tap} \tag{1.14}$$

to validate the approach used for the decomposition of the Kronecker product. Since the transmitter-receiver setup in this experiment was static, the temporal correlation does not have a significant impact on the results. The CMD metric is used to compare the similarity between the channel coefficient covariance matrix calculated using (1.11) and (1.14). Results for six different instances are shown in Table 1.1. The matrices $\mathbf{R}ij$ are the correlation matrices of the ij-th subchannel. The channel

coefficient covariance matrix estimated using (1.14) is shown in Fig.1.8. The (4×4) spatial correlation matrix, $\mathbf{\Psi}_{TRx}$, is itself a Kronecker product of $\mathbf{\Psi}_{Tx}$ and $\mathbf{\Psi}_{Rx}$.

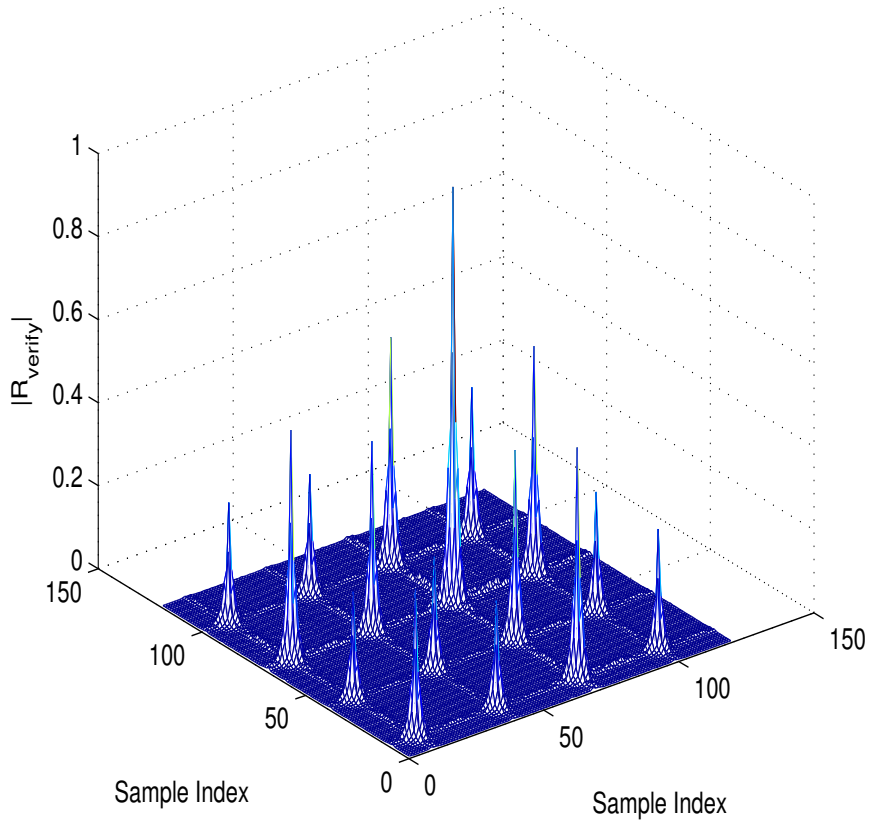

Figure 1.8 Kronecker Product of Estimated Ψ_{TRx} and Ψ_{Tap}

1.5. Conclusions

In this paper, we validated the triply selective fading channel model through a MIMO testbed and experimental results. The experimental results demonstrate that the discrete-time triply selective fading channel can be expressed as separable

temporal, inter-tap and spatial correlations. Using correlation matrix distance as a metric we show that the intertap correlations for all the subchannels are spatially identical. This permits the estimation of spatial correlations matrices through the decomposition of the channel coefficient covariance matrix. Finally, we verify our results by recalculating the Kronecker product of the estimated correlation matrices and comparing the result with the covariance matrix obtained directly from the estimated channel coefficients.

References

[1] C. Xiao, J. Wu, S.-Y. Leong, Y. R. Zheng, and K. Letaief, "A discrete-time model for triply selective mimo rayleigh fading channels," *IEEE Transactions on Wireless Communications*, vol. 3, no. 5, pp. 1678 – 1688, 2004.

[2] J. Mietzner and P. Hoeher, "A rigorous analysis of the statistical properties of the discrete-time triply-selective mimo rayleigh fading channel model," *IEEE Transactions on Wireless Communications*, vol. 6, no. 12, pp. 4199 –4203, 2007.

[3] J. Mietzner, C. Xiao, P. Hoeher, and K. Ben Letaief, "A note on discrete-time triply-selective mimo rayleigh fading channel models," *IEEE Transactions on Wireless Communications*, vol. 7, no. 3, p. 837, 2008.

[4] A. Abdi and M. Kaveh, "A space-time correlation model for multielement antenna systems in mobile fading channels," *IEEE Journal on selected areas in Communications*, vol. 20, no. 3, pp. 550 –560, Apr 2002.

[5] G. Byers and F. Takawira, "Spatially and temporally correlated mimo channels: modeling and capacity analysis," *IEEE Transactions on Vehicular Technology*, vol. 53, no. 3, pp. 634 – 643, May 2004.

[6] K. Baddour and N. Beaulieu, "Accurate simulation of multiple cross-correlated rician fading channels," *IEEE Transactions on Communications*, vol. 52, no. 11, pp. 1980 – 1987, Nov 2004.

[7] C. V. Loan and N. Pitsianis, *Approximation with Kronecker products*. Kluwer Publications, 1993, pp. 293–314.

[8] F. Ren and Y. Zheng, "A novel emulator for discrete-time mimo triply selective fading channels," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 57, no. 9, pp. 2542 –2551, 2010.

[9] S. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*, ser. Prentice Hall signal processing series. Prentice-Hall PTR, 1998.

[10] M. Herdin, N. Czink, H. Ozcelik, and E. Bonek, "Correlation matrix distance, a meaningful measure for evaluation of non-stationary MIMO channels," in *IEEE 61st Vehicular Technology Conference*, vol. 1, May-June 2005, pp. 136 – 140 Vol. 1.

2. Improving Detection Range Via Correlation of Long PN Codes

Saurav Subedi, Zhonghai Wang and Y. R. Zheng

Department of Electrical and Computer Engineering,

Missouri University of Science and Technology, Rolla, MO 65409

Abstract

This paper proposes a correlation method for detecting super-regenerative RF receivers via stimulation. Long PN sequences are used to stimulate the unintended emissions from the RF receivers. A high correlation between the known PN sequence and stimulated unintended emissions from the RF receivers helps improving the detection range compared to the passive detection and power detection methods. Although the RF receivers generate unintended emissions from their nonlinear devices, without stimulation, the power of these unintended emission is usually lower than -70dBm, as per the FCC regulations. Direct detection (passive detection) of these emissions is a challenging task specially in noisy conditions. When a stimulation signal is transmitted from a distance, the superregenerative receivers generate unintended emissions that contain the stimulation signal and its harmonics. An excellent correlation property of the PN sequence enables us to improve the range and accuracy of detecting the super-regenerative receivers through the stimulation method even in noisy conditions. The experiment involves detection of a wireless doorbell, a commercially available super-regenerative receiver. The USRP is used for transmitting the

stimulant signal and receiving the unintended stimulated emissions from the doorbell. Results show that the detection range of the proposed method with long PN sequences is much larger than the passive detection and power detection methods.

2.1. Introduction

The Radio Frequency (RF) receivers radiate specific emissions from their electronic circuitry. These emissions are not strong enough to violate the FCC regulations. However, these emissions can be used to detect the receivers.

Several methods of detecting and locating RF receivers have been proposed in existing literature. The detection methods can be broadly categorized into two classes - passive detection and active detection methods. The passive detection method concentrates on detecting the recurring characteristics in the observed radiation to extract information about the presence of the RF receiver [1]. Active detection methods, on the other hand, use a stimulation signal to instigate the unintended emissions from the receiver and extract relevant information from those emissions [2].

The passive detection methods [1], [2] are viable but they are of limited range in noisy environments. The consistency and accuracy of these detection methods decrease significantly in noisy environments. This susceptibility is analyzed and a better passive detection method using cascading correlation technique proposed in [1]. The Receiver Operator Characteristic (ROC) curve is used as a tool for comparison to show the improvement over the regular matched filter technique. Other methods like periodogram method [3] and matched filter method [4] are also used for passive detection.

The methods based on active stimulation provide marked improvement in the accuracy and consistency of detection. Some form of stimulation signal is used to modulate a carrier signal in the operating band of the RF receiver. The RF

receiver reciprocates to this stimulation by emitting the unintended radiations at the specific spectral locations. These emissions are modulated with the stimulation signal. The stimulation signal can be extracted from these unintended emissions. A suitable detection algorithm can then be deployed to detect the device. Both super-regenerative and superheterodyne type receivers can be detected using active stimulation based detection methods. [1], [2].

In this paper, we propose a method for detection of the superregenerative RF receivers based on active stimulation and correlation of long PN codes. A pseudo-noise (PN) sequence of specific length is used as the stimulation signal. The stimulation signal is modulated on a carrier frequency of the receiver. When an RF receiver receives the stimulation signal, it generates the unintended emissions modulated with the PN sequence. At the detector, we extract the PN sequence from such unintended emissions and use correlation method to detect the RF receiver. We also compare the results with the stimulation and power detection method. The method is verified through experiments using a wireless doorbell, a commercially available super-regenerative type receiver. Since this method ensures a longer detection range and better accuracy, it can be extended for the localization of the device by using multiple detectors.

This paper is organized as follows. The emission characteristics of the super-regenerative RF receivers is discussed in Section II. Section III explains about the fundamentals of the stimulation and correlation detection method, the selection, and design of the stimulation signal. The stimulation and power detection method is also

described in Section III. The experiment and results are included in Section IV. The conclusions are drawn in Section V.

2.2. Emission Characteristics of Super-regenerative RF Receivers

A super-regenerative receiver works on the principle of positive feedback. A generalized block diagram of a superregenerative receiver is shown in Fig. 2.1. A tuned LC circuit in the receiver allows positive feedback only at its resonant frequency. The tuned circuit is also connected to the antenna and serves to select the radio frequency to be received. Gain of the feedback loop is adjusted to a level required for oscillation to increase the gain of the amplifier by a large factor only at the resonant frequency. A second lower frequency oscillation periodically interrupts the main RF oscillation. This is called "Quenching". Quenching causes the RF oscillation to grow exponentially and then permits them to stop [5]. Thus, the resultant signal closely resembles a sawtooth wave. Ideally, the receiver is not supposed to radiate any signals, neither the quenches nor the RF oscillations. However, in practice, these signals and their harmonics are radiated out from the receiver's electronic circuitry. A computer based model and simulation tool is presented in [6] for a general characterization of the superregenerative receivers .

The unintended emissions include the RF signal and its harmonics. The harmonic components are present because of the quenching mechanism. Effect of the active stimulation can be observed at the RF frequency as well as the harmonics. The harmonics are modulated with the stimulation signal and can be used to detect the receiver.

A wireless doorbell is used to represent the superregenerative receiver for our experiment. It is controlled by a remote controller with specific code. The device is not triggered unless the codes at the two ends (doorbell and controller) match

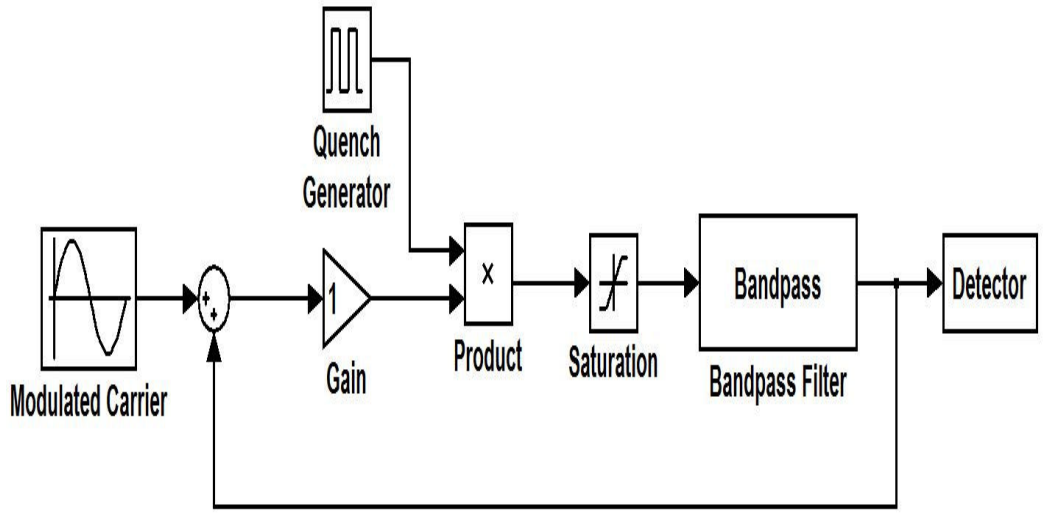

Figure 2.1 Block Diagram of a Typical Superregenerative Receiver

each other. Thus, we can stimulate it, collect the stimulated emissions and detect it, without triggering the receiver. The response of the doorbell to a stimulation signal with modulation is shown in Fig. 2.2. When the stimulation signal is a single tone without any modulation, we get its harmonics in the unintended emissions. When it is a BPSK signal, we observe that the phase of the baseband signal demodulated from one of the harmonics is changed non-linearly.

The wireless doorbell operates at a frequency of 315.2231MHz. The quenching mechanism creates a saw-tooth pattern of the emissions. This can be observed from a significant number of harmonics present in the spectra shown in Fig. 2.3.

Upon stimulating the device by transmitting a signal from the USRP at its operating frequency, the emissions from the device are stronger. The stimulated emissions can be observed in Fig. 2.4. Therefore, one of the stronger harmonics can be selected to retrieve the stimulation signal for further processing.

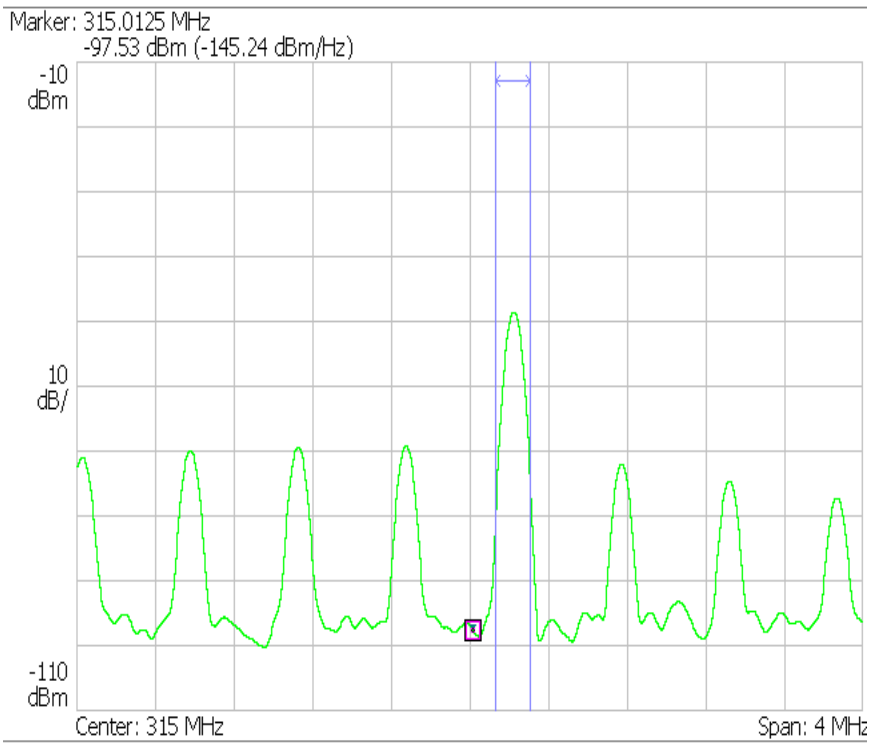

Figure 2.2 Stimulant Signal at RF Carrier Frequency and Harmonics

2.3. Correlation Method for Detection

2.3.1. Correlation. The cross-correlation between two signals $x_1(t)$ and $x_2(t)$ is defined as $R_{x_1x_2}(\tau) = E[x_1(t)x_2(t-\tau)]$, where $E[.]$ denotes the expectation operator. The correlation gain is calculated as shown in (2.1). The maximum correlation gain is obtained at time $\tau = 0$ [7].

$$Corrgain(dB) = 20log_{10}|R_{x_1x_2}(\tau)| \tag{2.1}$$

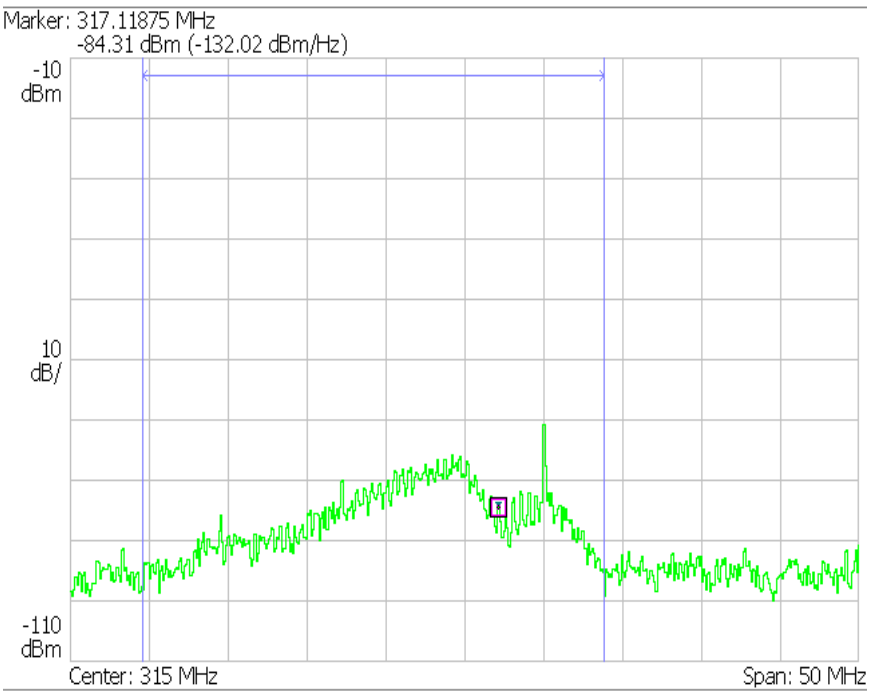

Figure 2.3 Emission from Wireless Doorbell Without Stimulant

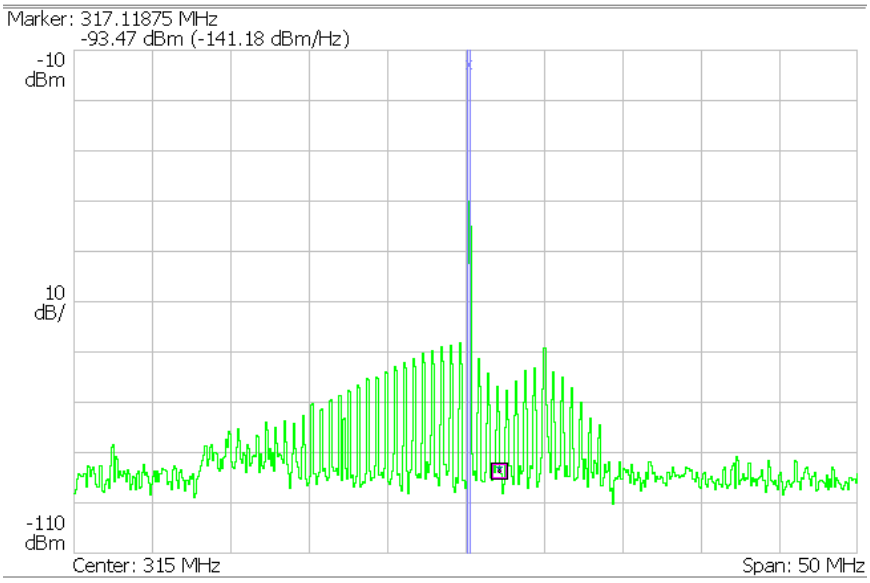

Figure 2.4 Emission from Wireless Doorbell With Stimulant

For detection purpose, the maximum value of correlation is compared to a predefined threshold which depends on the background analysis. If the peak of the correlation is larger than the threshold, it confirms the presence of the receiver within the detection range. In the proposed method, $x_1(t)$ is the known baseband signal and $x_2(t)$ is the estimate of the baseband signal acquired from the unintended stimulated emission of the target receiver.

The power detection method, on the other hand, uses an average value of the power detected from the stimulated unintended emissions. This value is compared with a threshold determined according to the background power level. When the superregenerative receiver is present within a certain range, it responds to the stimulation signal. This may cause the average power of the received signal to be larger than the threshold.

2.3.2. Selection of Stimulation Signal. The choice of the stimulation signal affects the range and accuracy of detection. The maximum achievable correlation gain is the criteria for selecting a stimulation signal. Due to the nonlinear phase response of the superregenerative receiver, phase modulated signal may not be used as the stimulation signal. A linear FM chirp can be used as the stimulation signal as mentioned in [2]. However, the non-linear phase response of the superregenerative receiver will reduce the achievable correlation gain.

In this experiment, we use a pseudo-noise (PN) sequence modulated on the carrier using On-off keying (OOK) method. In OOK demodulation, phase information is not significant. Thus, the nonlinear phase response of the the receiver will not affect the correlation gain. In addition, a higher correlation gain can be achieved using longer codes. The higher correlation gain leads to a larger detection range. Also, for a given distance, the probability of false detection reduces as the correlation gain becomes larger.

Different classes of PN sequences were considered. The autocorrelation of three categories of pseudorandom sequences including the maximal length sequences (m-sequences), gold sequences and Walsh sequences are compared in Fig. 2.5. The correlation gain increases with the length of the code. It is evident from the simulation results that the m-sequence outperforms the other two in terms of the peak to average power ratio (PAPR). Therefore, we select the m-sequence as the stimulation signal for our experiment.

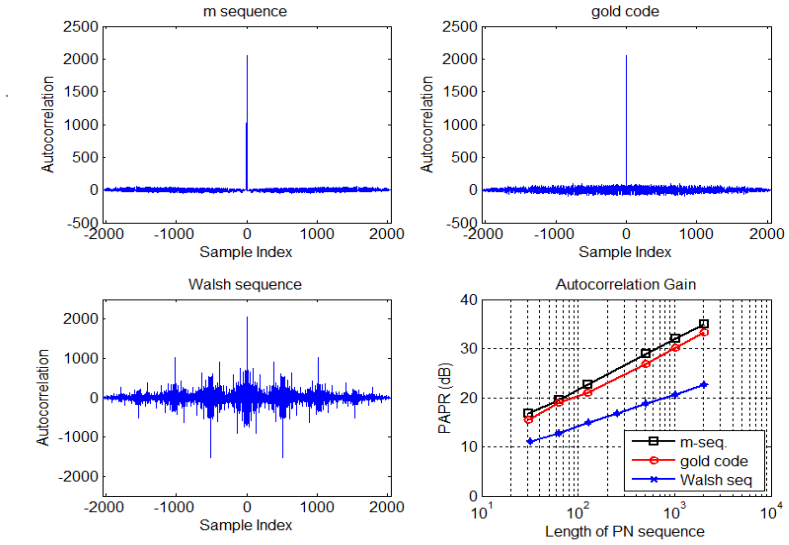

Figure 2.5 Three Classes of PN Sequences and Their Correlation Performance

2.3.3. Generation and Transmission of Stimulation Signal. Simulink is used to generate the stimulation signal for transmission and the Universal Software Radio Peripheral (USRP) is used for transmission. The transmission model is shown in Fig. 2.6. A high-speed USB cable is used to communicate between the PC and the USRP. The USRP modulates the baseband signal on the desired carrier frequency.

In this experiment, we use 315.22331 MHz as the carrier frequency for transmitting the stimulation signal.

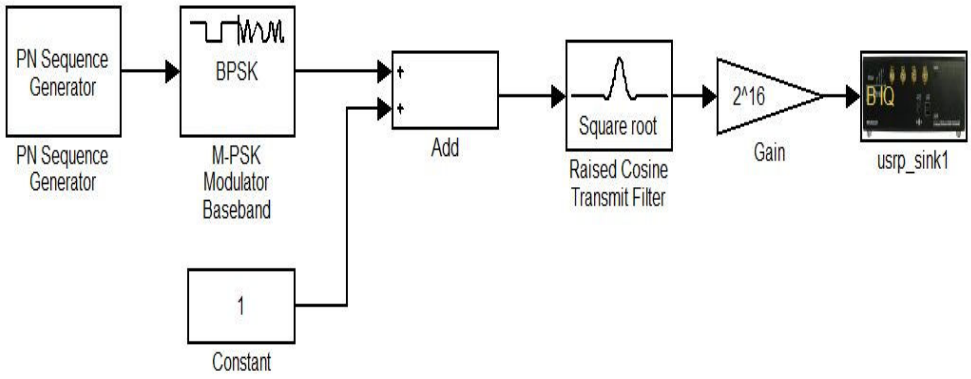

Figure 2.6 Transmission Model Designed in MATLAB/Simulink

The PN sequence generator block is used to generate m-sequences of different lengths. A symbol rate of 12.5 KHz is used, which is selected depending upon the operational bandwidth of the RF receiver. The PN sequence is converted to an On-Off Keying (OOK) modulated baseband signal. The signal is then pulse shaped using a square-root raised cosine filter which is then fed into the USRP-Simulink interface. An important parameter to be considered while using this interface is the interpolation factor. This parameter specifies the number to be used inside the USRP to bring the baseband sampling rate to 128 MSps. The output frequency can be manipulated at the USRP as required depending on the daughterboard being used. In our experiment, the WBX (50 MHz to 2.2 GHz) transceivers are used to transmit the stimulation signal at 315.22331 MHz, corresponding to the carrier frequency of the wireless doorbells. The interface also provides us an option to change the transmission gain of the USRP.

2.3.4. Reception of the Stimulation Signal. The USRP WBX daughterboard is used to receive the unintended stimulated emission. The first harmonic is used for receiver detection because it is the strongest among all unintended emission as shown in Fig. 2.4. The first harmonic frequency changes with the input stimulation signal power. Therefore, a frequency searching algorithm is used to approximate the the first harmonic frequency. The OOK modulated signal is then extracted from the first harmonics . The power of a segment of the received signal demodulated from the first harmonics is shown in Fig. 2.7. Comparing the baseband signal with a threshold, we get an estimate of the PN sequence. This estimate is cross-correlated with the known transmitted sequence to obtain a cross-correlation output as demonstrated in Fig. 2.8. A maximum cross-correlation gain of 2^L-1 would be achieved (L is the length of the PN sequence used as the stimulation signal) in an ideal condition. As illustrated in Fig. 2.8, multiple frames of the received signal are cross-correlated with a frame of the known stimualtion signal. The cross-correlation output close to 2^L-1 (larger than the predefined threshold) assures the presence of an RF receiver. In Fig. 2.8, it can be observed that the crosscorrelation output does not reach a maximum value of 1023. This is because the first harmonic frequency changes with the power of the stimulation signal and since the emitted signal bandwidth is larger than the receiver bandwidth, a small portion of the signal is missed at the receiver.

Correlation method using PN sequences also prevents any false detection. Thus detection accuracy is improved. This is because of the correlation properties of these PN sequences. The correlation output cannot reach a value larger than the threshold unless the detector receives the unintended stimulated emission from the doorbell. This ensures that the cross-correlation method provides better accuracy than the passive detection method or the power detection method.

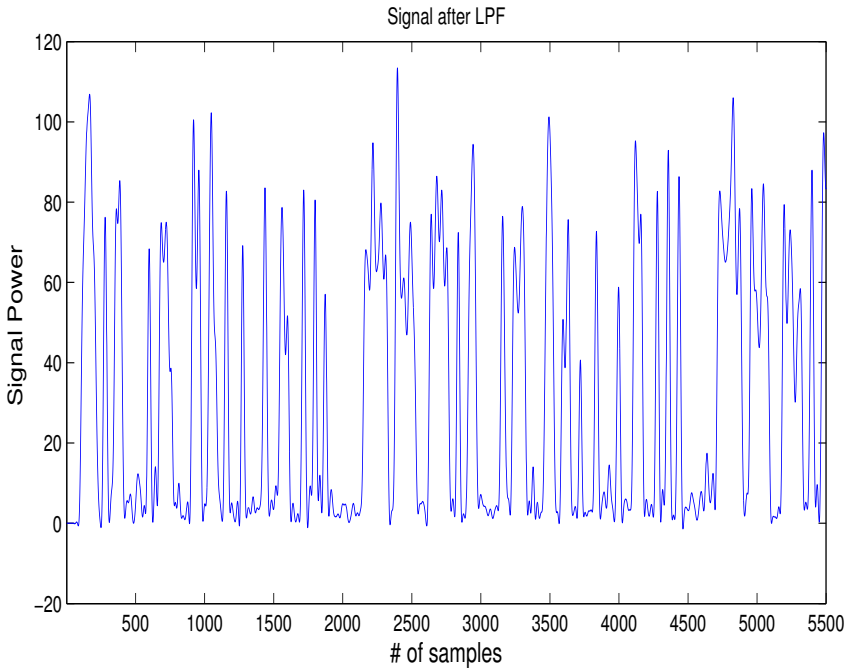

Figure 2.7 Power of a Segment of the Received Signal

2.4. Experiments and Results

The experiment setup is shown in Fig. 2.9. The baseband signal is generated in the Simulink and is transferred to the USRP via a high-speed USB cable. At the receiver side, we use another USRP to receive the desired harmonic transmitted by the doorbell and downconverts it to the baseband. The experiment is repeated for the PN sequences of different lengths and maximum achievable detection range is measured for each case. Results have been summarized in Table 2.1. These results are obtained from indoor experiments conducted in a hallway.

We observe that the detection range increases with the length of the code. The maximum achievable distance is also limited by the strength of the signal reaching

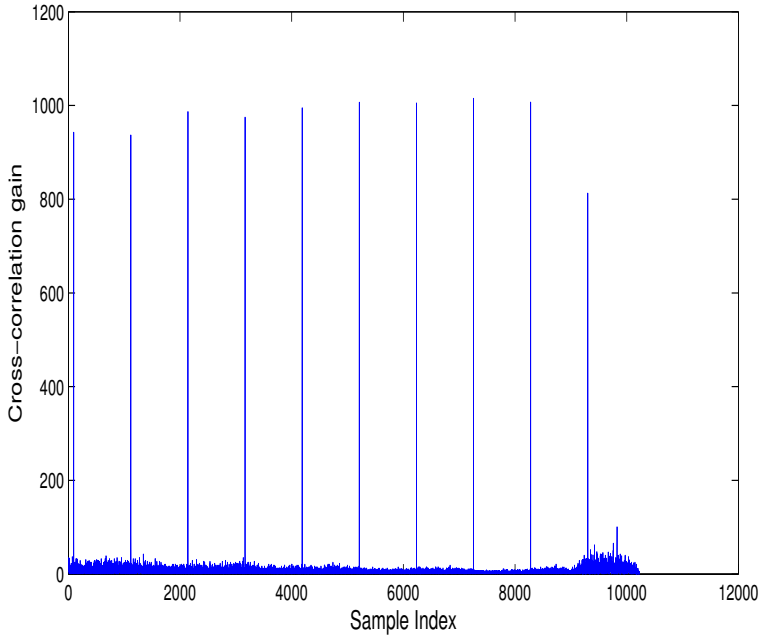

Figure 2.8 Cross-correlation Gain for 1023 Bits PN Sequence

the wireless doorbell. The correlation method can work only if the some response is received from the doorbell. If the distance between the transmitter and doorbell is very large, the signal attenuates to a value below which the doorbell cannot respond. This distance also depends on the channel conditions.

Another interesting observation during this experiment was that the frequency of the harmonics changes with power from the transmitter. Since OOK modulation is used, power of the signal reaching the doorbell varies and we can observe a frequency drift in the response from the doorbell.

2.5. Conclusions

We proposed a detection method of the superregenerative receivers using active stimulation and correlation. We show that the proposed method provides better range

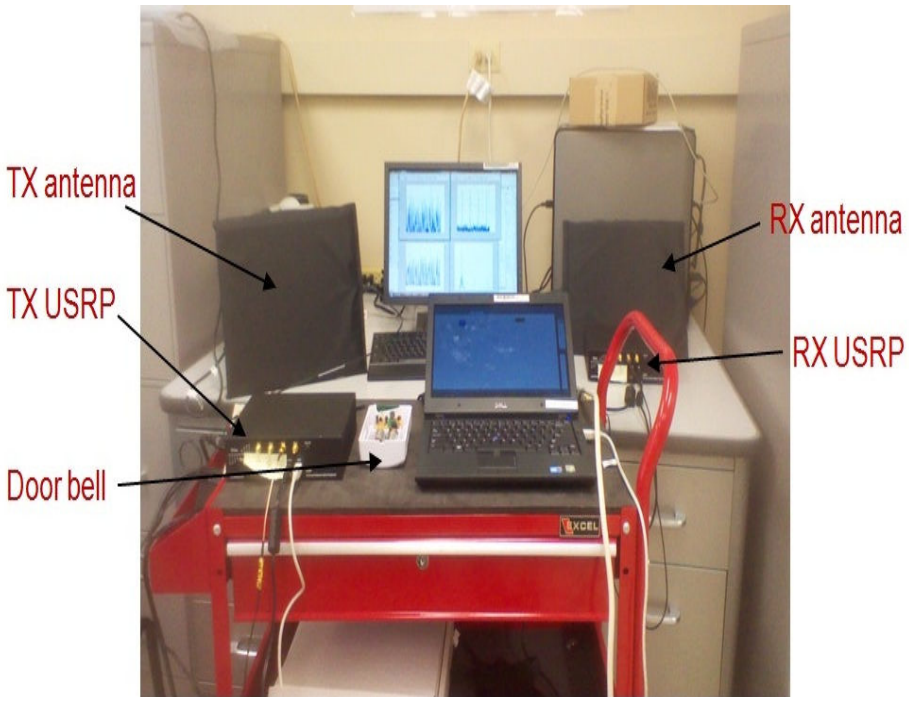

Figure 2.9 Experiment Setup

Table 2.1 Detection Ranges for Methods Based on Power Detection and Cross Correlation

Detection Method	**Maximum Range of Detection (feet)**
Power Detection	20
63 bit M-sequence cross-correlation	26
1023 bit M-sequence cross-correlation	40
2047 bit M-sequence cross-correlation	48
4095 bit M-sequence cross-correlation	56
8191 bit M-sequence cross-correlation	62

and accuracy in detecting these devices as compared to the passive detection and power detection methods. Furthermore, we show that the use of longer m-sequences

as the stimulation signal provides higher correlation gain and helps improving the detection range.

References

[1] Seguin, S. A., "Detection of low cost radio frequency receivers based on their unintended electromagnetic emissions and an active stimulation," Ph.D. dissertation, Missouri University of Science and Technology, 2009.

[2] Stagner, C., Conrad, A., Osterwise, C., Beetner, D., and Grant, S., "A practical superheterodyne-receiver detector using stimulated emissions," *IEEE Transactions on Instrumentation and Measurement*, vol. 60, no. 4,1461 –1468,(2011).

[3] So, H., Chan, Y., Ma, Q., and Ching, P., "Comparison of various periodograms for sinusoid detection and frequency estimation," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 35, no. 3,945 –952, Jul 1999.

[4] Shaik, A., Weng, H., Dong, X., Hubing, X., and Beetner, D., "Matched filte detection and identification of electronic circuits based on their unintentional radiated emissions," in *IEEE International Symposium on Electromagnetic Compatibility,2006.*, vol. 3, 853 –856, Aug 2006.

[5] Frink, F., "The basic principles of super-regenerative reception," *Proceedings of the Institute of Radio Engineers*, vol. 26, no. 1, 76 – 106, Jan 1938.

[6] Feick, R. and Rojas, O., "Modeling and simulation of the superregenerative receiver," *IEEE International Symposium on Consumer Electronics*, vol. 43, no. 2, 92 –102, May 1997.

[7] Knapp, C. and Carter, G., "The generalized correlation method for estimation of time delay," *IEEE International Symposium on Acoustics, Speech and Signal Processing*, vol. 24, no. 4, 320 – 327, Aug 1976.

SECTION

2. CONCLUSIONS

Two independent problems involving radio frequency channels are investigated through experimental studies. Discrete time triply selective fading channel model is experimentally validated using data collected from a 2×2 MIMO-OFDM testbed. A method is proposed to estimate the spatial and inter-tap correlation matrices from the channel impulse response of the MIMO channel. Results show that the channel coefficient covariance matrix of MIMO channels can be decomposed into its Kronecker factors. In another study, an algorithm based on active stimulation and correlation of long PN codes is proposed for detection of superregenerative RF receivers. The algorithm is practically implemented and it is verified through experimental results that the proposed method provides longer detection range and better accuracy than the passive detection method and power detection method, even in noisy environments.

VITA

Saurav Kumar Subedi graduated with his Bachelor's degree in Electronics and Communication Engineering from Purbanchal University, Nepal in May 2008. He held an undergraduate research position in the Department of Computer and Electronics & Communication Enginering at Acme Engineering College from June 2007 to December 2007. After graduation, he worked as an Assistant Lecturer at Acme Engineering College till June 2009. From June 2009 to July 2010, he worked at Nepal Telecom as a GSM BSS Engineer. He joined Masters of Science in Electrical Engineering program at Missouri University of Science and Technology in Fall 2010. He worked as a graduate research assistant at Center for Real Time Adaptive Signal Processing. He also worked as graduate teaching assistant in the Department of Electrical and Computer Engineering for the courses Communication Systems and Introduction to Electronic Devices. He published two papers, one in Military Communications Conference (MILCOM) 2011 and the other in Society of Photo-Optical Instrumentation Engineers (SPIE) 2012. He is expected to receive a Master's Degree in Electrical Engineering at Missouri University of Science and Technology in May 2012.