

**ANTI-EAVESDROPPING TECHNIQUES FOR  
ENHANCING PHYSICAL LAYER SECURITY IN  
RESOURCE-LIMITED COMMUNICATIONS**

**SASI VINAY PECHETTI**



**DEPARTMENT OF ELECTRICAL ENGINEERING  
INDIAN INSTITUTE OF TECHNOLOGY DELHI  
NOVEMBER 2020**

©Indian Institute of Technology Delhi (IITD), New Delhi, 2020

**ANTI-EAVESDROPPING TECHNIQUES FOR  
ENHANCING PHYSICAL LAYER SECURITY IN  
RESOURCE-LIMITED COMMUNICATIONS**

by

**SASI VINAY PECHETTI**

DEPARTMENT OF ELECTRICAL ENGINEERING

Submitted

in fulfillment of the requirements of the degree of Doctor of Philosophy

to the



**INDIAN INSTITUTE OF TECHNOLOGY DELHI**

**NOVEMBER 2020**

Dedicated to  
*Family and Friends*

*\* Family is fabulous and friends are the best \**

# Certificate

This is to certify that the thesis entitled “**Anti-eavesdropping techniques for enhancing physical layer security in resource-limited communications**” being submitted by **Mr. Sasi Vinay Pechetti** to the Department of Electrical Engineering, Indian Institute of Technology Delhi, for the award of the degree of **Doctor of Philosophy** is the record of bonafide research work carried out by him under my supervision. In my opinion, the thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted either in part or in full to any other University or Institute for the award of any degree or diploma.

**Dr. Ranjan Bose**

**Professor**

Department of Electrical Engineering  
Indian Institute of Technology Delhi  
Hauz Khas, New Delhi, 110016, India

Date:

Place: New Delhi

# Acknowledgements

First of all, I express my gratitude to my supervisor, **Prof. Ranjan Bose**, for taking me under his guidance and constantly supporting during all the years of my Ph. D. His lovely nature of never saying no to a student has helped me endeavoring better goals every time we formulate a problem-statement. I am thankful to him for believing in me and giving valuable feedback in my hard times, which I will remember for my lifetime.

I want to thank **Dr. Abhishek Jindal** for his valuable discussions during his stay at IIT Delhi. I must emphasize that the discussions we had have helped me in developing major attributes required for pursuing a quality research. I want to thank my research committee members Prof. Shankar Prakriya, Prof. Manav Bhatnagar and Prof. Kolin Paul for their constructive comments during this period. A special thanks to Prof. Shankar Prakriya for being my care-taker supervisor and conducting a smooth transit while Prof. Ranjan Bose is on leave. Most importantly, I want to thank my lab friends, Ms. Sonam Jain, Mr. Kirti Kant Sharma and Ms. Srishti Kulshrestha for their technical discussions during this period.

I want to extend my hearty thanks to my friends at the campus, Mr. Chetan Ralekar, Mr. Usham Dias, Dr. Anshul Jaiswal and Ms. Bhawna Kamra for their wonderful company during my stay at IIT Delhi. Finally and most importantly, I want to thank my parents Mr. Dharma Rao and Mrs. Mutyavati for their unconditional love towards me.

  
Sasi Vinay Pechetti

# Abstract

The magnitude of resources that are being spent for securing the information transfer in various applications such as, health, defence, banking, etc. depicts the importance of the need for secure communication. Thus, the need for secure wireless information message transfer has been ever increasing. To this end, there are a number of techniques developed over the decades to meet the need for secure communication, and encryption techniques are widely used among them. Despite the popularity of the encryption techniques, the difficulty in exchanging the secret-key among the legitimate parties, the mathematical uncertainty on securing the information transfer, and their computationally hungry nature have paved a way for other alternatives. One such alternative is information-theoretic security. Recently, with the advent of multiple-input multiple-output antenna techniques, and other signal processing-based techniques, the concept of information-theoretic security has become more realizable. The combination of signal processing-based techniques and information-theoretic techniques by utilizing the existing randomness in the physical parameters such as channel fading and noise has unfolded the area *physical layer security*. Physical layer security techniques are proven to provide a higher level of security with the help of a few extra resources like multiple antennas, artificial noise, etc. However, these extra resources may not always be affordable by resource-limited devices like the devices deployed in the Internet of Things. With an increase in the number of such devices exchanging the information, there is a growing need for security techniques affordable by these resource-limited devices.

Throughout this thesis, we propose a few schemes affordable by the resource-limited devices for enhancing the physical layer security. In the first part of the thesis, we make use of the randomness existing in the legitimate channel along with the conventional modulation techniques such as  $M$ -ary phase shift keying to serve the objective in terms of resource-

limited secure information transfer. In the latter part of the thesis, we again use the randomness existing in the legitimate channel but with a fairly new modulation technique called index modulation to achieve the enhanced rate and security.

In the first half of the thesis, for enhancing the physical layer security, we propose two schemes without using any of the extra resources like multiple antennas, multiple sub-carriers, energy for artificial noise, etc. More specifically, a mapping out of multiple possible mappings of a given  $M$ -ary phase shift keying constellation is selected based on the gain of the legitimate channel. Since the channel of the eavesdropper fades independently of the legitimate channel, the eavesdropper finds it difficult to decode the information. Likewise, a set of orthogonal pulses is selected out of multiple possible orthogonal sets for pulse shaping to confuse the eavesdropper. Studying these two schemes is even more interesting when the eavesdropper is located near the destination, and has a correlation with the legitimate channel. Although both of these schemes may not guarantee perfect secrecy, with the use of minimal resources, these schemes make the job of the eavesdropper exceedingly difficult in decoding the transmitted data.

In the latter half of the thesis, we move a step ahead and relax the usage of a few of the resources and get additional benefits in terms of enhanced rate and a higher level of security. More specifically, we have relaxed the usage of multiple antennas and energy at the legitimate transmitter to select a pulse at the legitimate receiver for enhancing the rate and security. Further, we have relaxed the usage of multiple antennas at the transmitter and the receiver in a heterogeneous network to exploit the existing cross-tier interference for enhancing the rate and security of the system. In contrast to the schemes proposed in the former part of the thesis, schemes in the latter part guarantee secrecy with the help of additional resources. It is important to note that although the schemes we propose in the latter half of the thesis use extra resources, the system benefits in terms of other resources apart from security. Further, we propose a few research directions at the end the thesis.

## सार

विभिन्न अनुप्रयोगों जैसे कि, स्वास्थ्य, रक्षा, बैंकिंग आदि में सूचना हस्तांतरण को सुरक्षित रखने के लिए खर्च किए जा रहे संसाधनों का परिमाण सुरक्षित संचार की आवश्यकता के महत्व को दर्शाता है। इस प्रकार, सुरक्षित वायरलेस सूचना संदेश हस्तांतरण की आवश्यकता लगातार बढ़ रही है। इस समय तक, सुरक्षित संचार की आवश्यकता को पूरा करने के लिए कई तकनीकों का विकास हुआ है, और एन्क्रिप्शन तकनीकों का व्यापक रूप से उपयोग किया जाता है। एन्क्रिप्शन तकनीकों की लोकप्रियता के बावजूद, वैध पार्टियों के बीच गुप्त-कुंजी के आदान-प्रदान में कठिनाई, सूचना हस्तांतरण को हासिल करने में गणितीय अनिश्चितता, और उनके कम्प्यूटेशनल रूप से भूखे स्वभाव ने अन्य विकल्पों के लिए एक मार्ग प्रशस्त किया है। ऐसा ही एक विकल्प है सूचना-सिद्धांत संबंधी सुरक्षा। हाल ही में, मल्टीपल-इनपुट मल्टीपल-आउटपुट एंटीना तकनीकों, और अन्य सिग्नल प्रोसेसिंग-आधारित तकनीकों के आगमन के साथ, सूचना-सिद्धांत सुरक्षा की अवधारणा अधिक साकार हो गई है। चैनल फ़ेडिंग और रिसीवर-शोर जैसे भौतिक मापदंडों में मौजूदा यादृच्छिकता का उपयोग करके सिग्नल प्रोसेसिंग-आधारित तकनीकों और सूचना-सिद्धांत संबंधी तकनीकों के संयोजन ने क्षेत्र की भौतिक परत सुरक्षा को प्रकट किया है। भौतिक परत सुरक्षा तकनीक कुछ अतिरिक्त संसाधनों जैसे एकाधिक एंटेना, कृत्रिम शोर, आदि की सहायता से उच्च स्तर की सुरक्षा प्रदान करने के लिए सिद्ध होती हैं। हालाँकि, ये अतिरिक्त संसाधन हमेशा संसाधन-सीमित उपकरणों जैसे उपकरणों में तैनात होने से सस्ती नहीं हो सकते हैं। इंटरनेट ऑफ थिंग्स। सूचना का आदान-प्रदान करने वाले ऐसे उपकरणों की संख्या में वृद्धि के साथ, इन संसाधन-सीमित उपकरणों द्वारा सस्ती सुरक्षा तकनीकों की बढ़ती आवश्यकता है।

इस थीसिस के दौरान, हम भौतिक परत सुरक्षा को बढ़ाने के लिए संसाधन-सीमित उपकरणों द्वारा सस्ती कुछ योजनाओं का प्रस्ताव करते हैं। थीसिस के पहले भाग में, हम संसाधन-सीमित सुरक्षित सूचना हस्तांतरण के उद्देश्य से उद्देश्य की पूर्ति के लिए पारंपरिक मॉड्यूलेशन तकनीकों जैसे एम-ऐरी फेज़ शिफ्ट कीडिंग के साथ वैध चैनल में मौजूद यादृच्छिकता का उपयोग करते हैं। थीसिस के उत्तरार्द्ध में, हम फिर से वैध चैनल में मौजूद यादृच्छिकता का उपयोग करते हैं, लेकिन एक काफी नई मॉड्यूलेशन तकनीक के साथ बढ़ाया दर और सुरक्षा प्राप्त करने के लिए इंडेक्स मॉड्यूलेशन कहते हैं।

थीसिस की पहली छमाही में, भौतिक परत सुरक्षा को बढ़ाने के लिए, हम कई एंटेना जैसे कई अतिरिक्त संसाधनों का उपयोग किए बिना दो योजनाओं का प्रस्ताव करते हैं, कई उप-वाहक, कृत्रिम शोर के लिए ऊर्जा, आदि। विशेष रूप से, कई में से एक मैपिंग। वैध एम चैनल के लाभ के आधार पर किसी दिए गए एम-एरी फेज शिफ्ट कीडिंग तारामंडल के संभावित मैपिंग का चयन किया जाता है। चूंकि ईक्सट्रॉपर का चैनल वैध चैनल के स्वतंत्र रूप से फ़ेड करता है, इसलिए ईक्सट्रॉपर को जानकारी को डिकोड करना मुश्किल होता है। इसी तरह, ईक्सट्रॉपर को भ्रमित करने के लिए पल्स को आकार देने के लिए कई संभावित ऑर्थोगोनल सेटों में से ऑर्थोगोनल दालों का एक सेट चुना जाता है। इन दोनों योजनाओं का अध्ययन और भी दिलचस्प है जब ईक्सट्रॉपर गंतव्य के पास स्थित है, और वैध चैनल के साथ संबंध है। हालाँकि ये दोनों योजनाएँ पूर्ण गोपनीयता की गारंटी नहीं दे सकती हैं, लेकिन न्यूनतम संसाधनों के उपयोग के साथ, ये योजनाएँ ईवेर्सट्रॉपर के काम को प्रेषित डेटा को डिकोड करने में अत्यधिक कठिन बनाती हैं।

थीसिस के उत्तरार्ध में, हम एक कदम आगे बढ़ते हैं और कुछ संसाधनों के उपयोग को आराम करते हैं और बढ़ी हुई दर और सुरक्षा के उच्च स्तर के संदर्भ में अतिरिक्त लाभ प्राप्त करते हैं। अधिक विशेष रूप से, हमने दर और सुरक्षा को बढ़ाने के लिए वैध रिसीवर पर एक पल्स का चयन करने के लिए वैध ट्रांसमीटर पर कई एंटेना और ऊर्जा के उपयोग को आराम दिया है। इसके अलावा, हमने सिस्टम की दर और सुरक्षा को बढ़ाने के लिए मौजूदा क्रॉस-टियर हस्तक्षेप का फायदा उठाने के लिए ट्रांसमीटर और एक विषम नेटवर्क में रिसीवर पर कई एंटेना के उपयोग को आराम दिया है। थीसिस के पूर्व भाग में प्रस्तावित योजनाओं के विपरीत, उत्तरार्ध में योजनाएँ अतिरिक्त संसाधनों की मदद से गोपनीयता की गारंटी देती हैं। यह ध्यान रखना महत्वपूर्ण है कि यद्यपि हम जिन योजनाओं के उत्तरार्ध में प्रस्ताव रखते हैं, वे अतिरिक्त संसाधनों का उपयोग करते हैं, सिस्टम सुरक्षा के अलावा अन्य संसाधनों के संदर्भ में लाभ उठाता है। इसके अलावा, हम थीसिस के अंत में कुछ शोध निर्देश प्रस्तावित करते हैं।

# Table of Contents

<b>Certificate</b>	<b>i</b>
<b>Acknowledgements</b>	<b>ii</b>
<b>Abstract</b>	<b>iii</b>
<b>List of Figures</b>	<b>ix</b>
<b>List of Tables</b>	<b>xi</b>
<b>List of Abbreviations</b>	<b>xii</b>
<b>1 Wireless Communications and Need for Secure Information Transfer</b>	<b>1</b>
1.1 Overview of Wireless Communications . . . . .	1
1.1.1 Major Challenges in Wireless Communications . . . . .	3
1.1.2 Existing Solutions for the Challenges . . . . .	4
1.2 Physical Layer Security (PLS) . . . . .	5
1.3 Motivation and Thesis Organization . . . . .	9

<b>2</b>	<b>Literature Review</b>	<b>12</b>
2.1	PLS for Resource-Limited Communications . . . . .	12
2.2	PLS for IM . . . . .	14
2.3	PLS in HetNet . . . . .	15
2.4	Research Gaps . . . . .	16
2.5	Thesis Objectives . . . . .	17
<b>3</b>	<b>Channel-Based Mapping Diversity (CBMD)</b>	<b>19</b>
3.1	Introduction . . . . .	19
3.2	System Model . . . . .	21
3.3	CBMD for BPSK . . . . .	22
3.3.1	Optimal Strategies for BPSK . . . . .	23
3.3.2	Preliminary Results . . . . .	31
3.4	CBMD for $M$ -PSK . . . . .	33
3.4.1	Optimal Strategies for $M$ -PSK . . . . .	33
3.5	Lower-Bound on SER . . . . .	46
3.6	Discussion on Computational Complexity and Energy Efficiency . . . . .	47
3.7	Simulation Results . . . . .	47
3.8	Conclusions . . . . .	52
<b>4</b>	<b>Channel-Aware Pulse Selection</b>	<b>53</b>

4.1	Introduction . . . . .	53
4.2	Channel-Aware Artificial Intersymbol Interference (CA-AISI) . . . . .	54
4.2.1	System Model . . . . .	54
4.2.2	Proposed Scheme . . . . .	55
4.2.3	Optimal Strategies and Performance Analysis . . . . .	59
4.2.4	Simulation Results . . . . .	62
4.3	Precoding-Aided Secure Time-Domain Index Modulation (PSTD-IM) . . . . .	64
4.3.1	System Model . . . . .	65
4.3.2	Proposed Scheme . . . . .	66
4.3.3	Performance Analysis . . . . .	68
4.3.4	Simulation Results . . . . .	71
4.4	Conclusion . . . . .	74
<b>5</b>	<b>Precoding-Aided Spatial Modulation for Secure Heterogeneous Network</b>	<b>75</b>
5.1	Introduction . . . . .	76
5.2	System Model . . . . .	78
5.3	Precoding Schemes . . . . .	80
5.3.1	Null Beamforming-PSM (NB-PSM) . . . . .	81
5.3.2	Constructive Interference-based PSM (CI-PSM) . . . . .	84
5.4	Transmit Power Optimization . . . . .	86

5.4.1	Transmit Power Optimization for NB-PSM . . . . .	86
5.4.2	Transmit Power Optimization for CI-PSM . . . . .	89
5.5	Achievable Information Rates . . . . .	90
5.6	PLS: Notion of Artificial Interference . . . . .	91
5.6.1	Successive Interference Cancellation (SIC) . . . . .	91
5.6.2	Zero-Forcing Decoder . . . . .	92
5.6.3	Secrecy Rate Using Maximum Likelihood Decoder . . . . .	93
5.7	Simulation Results . . . . .	94
5.8	Conclusion . . . . .	102
<b>6</b>	<b>Conclusions and Future Work</b>	<b>103</b>
6.1	Summary of the Contributions . . . . .	103
6.2	Scope of Future Work . . . . .	105
	<b>Bibliography</b>	<b>105</b>
	<b>Appendices</b>	<b>113</b>
<b>A</b>	<b>Proofs for Chapter 3</b>	<b>114</b>
A.1	Proof for Lemma 3.1 . . . . .	114
A.2	Proof for $C'_{i-j} > 0$ in (A.16) . . . . .	117
A.3	Proof for Lemma 3.2 . . . . .	118

A.4	Steps for Deriving (A.7) . . . . .	119
A.5	Definite Integral for $t_k(x)$ in (3.81) . . . . .	120
<b>B</b>	<b>Proofs for Chapter 4</b>	<b>121</b>
B.1	Power Normalizing Factors $\beta_s$ and $\beta_n$ . . . . .	121
B.2	Diversity Proof for Single User Case in PSTD-IM . . . . .	122
<b>C</b>	<b>Proofs for Chapter 5</b>	<b>123</b>
C.1	Power Normalizing Factor for Null Beamforming-PSM . . . . .	123
C.1.1	ZF Precoder at MBS . . . . .	123
C.1.2	ZF Precoder at FBS <sub>f</sub> . . . . .	125
C.2	Power Normalizing Factors for Constructive Interference- PSM . . . . .	126
C.2.1	ZF Precoder at MBS . . . . .	126
C.2.2	ZF Precoder at FBS <sub>f</sub> . . . . .	127
C.3	Proof for <b>Corollary 5.1</b> . . . . .	130
C.4	Power Normalizing Factors for TS scheme . . . . .	131
	<b>List of Publications</b>	<b>133</b>
	<b>Technical Biography of Author</b>	<b>135</b>

# List of Figures

3.1	(a) Possible mappings for BPSK. (b) Effective channel for $E$ with CBMD. (c) Equivalent BSC for CBMD. . . . .	23
3.2	ABER vs. SNR in dB for different $\tau_M$ : $\tau_M^{th}/2$ , $\tau_M^{th}$ , $\tau_M^{Median}(> \tau_M^{th})$ and $\tau_M^{opt}$ . For imperfect CSI, 1% of error in variance with respect to the main channel variance is considered. . . . .	31
3.3	ABER vs. $\rho$ for different values of SNR at $E$ and $\tau_M$ . . . . .	32
3.4	Selected set of Gray mappings for $M$ –PSK constellation. Every subscript is taken <i>modulo</i> ( $M$ ). . . . .	35
3.5	Selected Set of Gray Mappings for 8–PSK . . . . .	36
3.6	SER vs. $\rho$ for various $\tau_S$ with a 10 dB SNR at $E$ . . . . .	48
3.7	SER vs. $\rho$ , for various $\tau_S$ , with a 10 dB SNR at $E$ . . . . .	49
3.8	SER vs. SNR in dB at a $\rho = 0.4$ . Both simulated SER and closed-form LBs on SER are plotted for different values of $M$ and $\tau_S$ . . . . .	50
3.9	SER at $E$ vs. $\rho$ at a received SNR of 10 dB at $E$ . Simulated SER and closed-form LBs on SER are plotted for different values of $M$ and $\tau_S$ . . . . .	51
4.1	Two possible activation of pulses . . . . .	56

4.2	Achievable secrecy rate vs. Transmit SNR. . . . .	62
4.3	SOP vs. SNR at D. . . . .	63
4.4	SER at E and D vs. Transmit SNR. . . . .	64
4.5	Rate vs. Transmit SNR in dB for $K=4$ . . . . .	71
4.6	Rate vs. $N_E$ at a transmit SNR of 20 dB for $K=4$ . . . . .	72
4.7	BER vs. SNR in dB for $K = 4, \alpha = 0.5$ and $ \mathcal{B}  = 2$ . . . . .	73
5.1	System model for NB-PSM . . . . .	78
5.2	System model for CI-PSM . . . . .	78
5.3	Transmit power per femtocell user and macrocell user vs. Target SNR ( $\zeta$ ) at each user . . . . .	94
5.4	Total macrocell information rate vs. Transmit SNR at BS for different $K_M$ . . . . .	95
5.5	Total macrocell information rate vs. Transmit SNR at BS for different $K_f$ . . . . .	96
5.6	Macrocell information rate vs. Number of transmit antennas at FBS . . . . .	97
5.7	Transmit power at various base stations vs. Number of antennas at FBS . . . . .	98
5.8	Transmit power at various base stations Vs Number of femtocells . . . . .	99
5.9	Secrecy rate of femtocell information vs. Target SNR with different $F$ . . . . .	100
5.10	Secrecy rate of femtocell information vs. Target SNR with different $N_E$ . . . . .	101

# List of Tables

2.1	Research work done in the literature and existing loopholes (gaps). . . . .	17
3.1	Mapping selection for 8-PSK based on the estimated legitimate channel gain $y_{(.)}$ . . . . .	36
3.2	Probability of errors by the eavesdropper's channel so that the transmitted symbol is correctly decoded at $E$ . . . . .	38
5.1	Channel Coefficients Description . . . . .	79
5.2	Channel Coefficients in Vector Form . . . . .	79
6.1	Proposed schemes in the thesis to fill in the research gaps. . . . .	105

# List of Abbreviations

<b>ABER</b>	Average bit error rate
<b>AN</b>	Artificial noise
<b>APM</b>	Amplitude phase modulation
<b>ASER</b>	Average symbol error rate
<b>AWGN</b>	Additive white Gaussian noise
<b>BER</b>	Bit error rate
<b>BPSK</b>	Binary-phase shift keying
<b>BSC</b>	Binary symmetric channel
<b>CA-AISI</b>	Channel-aware artificial intersymbol interference
<b>CBMD</b>	Channel based mapping diversity
<b>CI-PSM</b>	Constructive interference-PSM
<b>CSI</b>	Channel state information
<b>CSIT</b>	Channel state information at transmitter
<b>CVX</b>	Software for disciplined convex programming
<b>DCMC</b>	discrete-input continuous-output memory-less channel
<b>DoF</b>	Degrees of freedom
<b>FBS</b>	Femtocell base station
<b>FTN</b>	Faster-than-Nyquist
<b>GSVD</b>	Generalized singular value decomposition
<b>HetNet</b>	Heterogeneous network
<b>IM</b>	Index modulation
<b>IoT</b>	Internet of Things
<b>ISI</b>	Intersymbol interference
<b>JD</b>	Joint detection
<b>LB</b>	Lower-bound

<b>MBS</b>	Macrocell base station
<b>MIMO</b>	Multiple-input multiple-output
<b>MIMOME</b>	Multiple-input multiple-output multiple-eavesdropper
<b>ML</b>	Maximum likelihood
<b>MMSE</b>	Minimum mean square estimator
<b><i>M</i>-PSK</b>	<i>M</i> -ary phase shift keying
<b>NB-PSM</b>	Null beamforming-PSM
<b>OFDM</b>	Orthogonal frequency division multiplexing
<b>PDF</b>	Probability density function
<b>PEP</b>	Pairwise error probability
<b>PLS</b>	Physical layer security
<b>PSK</b>	Phase shift keying
<b>PSM</b>	Precoding-aided spatial modulation
<b>PSTD-IM</b>	Precoding-aided secure time-domain index modulation
<b>QoS</b>	Quality of Service
<b>QPSK</b>	Quadrature-phase shift keying
<b>SD</b>	Separate detection
<b>SER</b>	Symbol error rate
<b>SIC</b>	Successive interference cancellation
<b>SISO</b>	Single-input single-output
<b>SM</b>	Spatial modulation
<b>SNR</b>	Signal-to-noise ratio
<b>SOP</b>	Secrecy outage probability
<b>TD</b>	Time domain
<b>TS</b>	Time sharing
<b>UB</b>	Upper-bound
<b>ZF</b>	Zero-forcing