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

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 कीइंग 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 कीइंग तारामंडल के संभावित मैपिंग का चयन किया जाता है। चूंकि ईव्सड्रॉपर का चैनल वैध चैनल के स्वतंत्र रूप से फ़ेड करता है, इसलिए ईव्सड्रोपर को जानकारी को डिकोड करना मुश्किल होता है। इसी तरह, ईव्सड्रोपर 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 ईव्सड्रोपर 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 योजनाएं ईवेर्सड्रॉपर 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, उत्तरार्द्ध में योजनाएं 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

List of Figures

List of Tables

List of Abbreviations

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

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