RATELESS-CODING-BASED SECURE TRANSMISSION SCHEMES IN A DELAY-CONSTRAINED ENVIRONMENT

SONAM JAIN

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY DELHI
AUGUST 2020

RATELESS-CODING-BASED SECURE TRANSMISSION SCHEMES IN A DELAY-CONSTRAINED ENVIRONMENT

by

SONAM JAIN

DEPARTMENT OF ELECTRICAL ENGINEERING

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

INDIAN INSTITUTE OF TECHNOLOGY DELHI

AUGUST 2020

DEDICATED TO

My Mother

Certificate

This is to certify that the thesis entitled **"Rateless-coding-based secure transmission schemes in a delay-constrained environment "** being submitted by **Ms. Sonam Jain** 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 her 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
New Delhi, India-110016

Date:
Place: New Delhi

Acknowledgements

First and foremost, I express my sincere gratitude to my research supervisor, **Prof. Ranjan Bose**, for his unrelenting belief in my capability. Without his continuous optimism, insightful and timely suggestions, this work would not have been possible. Also, he has been very patient in giving me the freedom to manage my research work with ease. The entire process contributed immensely to my self development too and for that I will be forever grateful to my supervisor.

I would like to thank my research committee members - Prof. Shankar Prakriya, Prof. Kolin Paul and Prof. Manav Bhatnagar for their constructive comments during this period. Most importantly, I want to thank my friends Mr. Sasi Vinay Pechetti, Mr. Kirti Kant Sharma, Ms. Srishti Kulshrestha for a lot of insightful discussions and their constant support. A special thanks goes to my seniors Ms. Sarbani Ghose and Mr. Abhisekh Jindal for their guidance.

Any acknowledgment is not complete without mentioning the source of strength which led to the completion of the work. Hence, I thank my family and friends for being selfless supporters of my aims during the lifetime.

Sonam Jain

Sonam Jain

Abstract

Broadcast nature of the wireless channel makes secure information transfer quite challenging. Therefore, to ensure secure information transfer, various advanced physical layer security (PLS) techniques are proposed, such as, cooperative relaying, jamming etc. To ensure perfect secrecy during PLS schemes, complete outage should occur at the eavesdropper and, the data rate of the legitimate receiver gets bounded by the secrecy capacity, this may result in an unendurable delay. Practically, if the information to be transmitted is correlated and a certain fixed number of packets are required to recover the entire information, then such protection mechanism is not required. In this context, by introducing rateless codes (RC) such as Luby transform (LT) codes or raptor codes into PLS protocol design, secrecy and lower transmission delay can be achieved.

In RC-aided transmission, ideally, an infinite number of encoded packets can be generated, since each generated encoded packet is the XOR of the source packets chosen randomly. Many of the applications today are delay-sensitive and hence, the channel usages allowed are limited. Generally, RC are used for forward error correction (FEC) at the application layer to deliver files without retransmission. RC have a property that a file consisting of K number of source packets can be completely recovered when the destination accumulates N ($N = (1+\delta)K$) rateless packets in any order, where N is moderately larger than K. Security can be obtained by utilizing the aforementioned characteristic, if, the legitimate user accumulates N packets before eavesdropper does.

In this work, we begin by investigating schemes in which cross-layer rateless encoding is exploited to achieve secrecy in a delay-constrained environment. In the first scheme proposed, transmit antenna selection (TAS) is employed at the base station to improve the main channel and, artificial noise (AN) is generated by the use of a cooperative jammer to degrade

the eavesdropper's channel. Quality of violation probability (QVP), which consists of both the delay violation probability and the intercept probability, is used as a performance metric. A closed-form expression for QVP is derived. Our study reveals that on increasing the number of antennas at the source (N_A) while using TAS along with AN, QVP decreases for delay sensitive services, whereas, in case of delay tolerant applications, increasing N_A is effective at low SNR.

Employing multiple antennas at a node is costly and limited by the size of the node. In this direction, we address the issue by a two-slot cooperative relaying scheme in which destination assisted cooperative jamming is utilized to expedite the decoding rate of the packets at the intended user. Both feedback-aided transmission (FT) and un-aided transmission (UT) are studied and closed-form expression for QVP is derived. Result shows that for FT, an increase in the total power reduces QVP, and by increasing the number of source packets the intercept probability decays for both UT and FT.

In cross-layer rateless encoding, goals and requirements of one layer FEC method compromises the performance of the other layer FEC method. To overcome this, we propose a secure scheme in which RC are used for FEC at the physical layer (PHY) in a cooperative delay-constrained environment. The probability of violation (Pr_{vio}) is used as a performance metric which consists of: 1) reliability outage probability, i.e., the probability with which the information cannot be successfully decoded within the time constraint *T* and 2) information intercept probability, that reflects the secrecy performance. Since RC can adjust the rate on the fly, we analyse the system performance when the relay transmits a part of the message and the receiver does energy accumulation (EA). We derive a closed-form expression of Pr_{vio} in a single-relay system at high signal to noise ratio (SNR) when the receiver either accumulates energy or mutual information (MI) from the received signals. Overall, the results show significant benefits of PHY-RC for guaranteeing the quality of service (QoS) requirements which include secrecy, reliability and low latency.

In the latter part of this thesis, we study the secrecy performance of a system with regenerative relays using RC and propose a relay selection technique to minimize the QVP. We also analyse the secrecy of a dual-hop cooperative system consisting of multiple decode-forward relays in a delay-constrained environment using RC, where there exists a separate time limit for both the hops.

सार

वायरलेस चैनल की प्रसारण प्रकृति सुरक्षित सूचना हस्तांतरण को काफी चुनौतीपूर्ण बनाती है। इसलिए, सुरक्षित सूचना हस्तांतरण, विभिन्न उन्नत भौतिक परत सुरक्षा सुनिश्चित करने के लिए (पीएलएस) तकनीक प्रस्तावित हैं, जैसे, सहकारी रिले, जामिंग आदि पीएलएस योजनाओं के दौरान गोपनीयता, ईवेसड्रोपर और, पर पूर्ण आउटेज होना चाहिए वैध रिसीवर की डेटा दर गोपनीयता क्षमता से बंधी हुई है, इसका परिणाम हो सकता है एक अनुचित देरी में। व्यावहारिक रूप से, यदि प्रेषित की जाने वाली जानकारी सहसंबद्ध है और संपूर्ण जानकारी को पुनर्प्राप्त करने के लिए कुछ निश्चित पैकेटों की आवश्यकता होती है, फिर ऐसे सुरक्षा तंत्र की आवश्यकता नहीं है। इस संदर्भ में, अनुत्पादक कोड (आरसी) की शुरुआत करके जैसे कि लुबी ट्रांसफ़ॉर्म (LT) कोड या PLS प्रोटोकॉल डिज़ाइन, गोपनीयता और में रैप्टर कोड कम संचरण देरी प्राप्त की जा सकती है।

आरसी-एडेड ट्रांसमिशन में, आदर्श रूप से, अनंत संख्या में एन्कोडेड पैकेट उत्पन्न किए जा सकते हैं, चूंकि प्रत्येक उत्पन्न एन्कोडेड पैकेट बेतरतीब ढंग से चुना गया स्रोत पैकेट का XOR है। आज के कई एप्लिकेशन विलंब-संवेदी हैं और इसलिए, चैनल के उपयोग की अनुमति है सीमित। आमतौर पर, RC का उपयोग अनुप्रयोग स्तर पर फॉरवर्ड एरर करेक्शन (FEC) के लिए किया जाता है पुनर्प्राप्ति के बिना फ़ाइलों को वितरित करने के लिए। RC में एक गुण होता है जो K नंबर वाली फ़ाइल होती है स्रोत के पैकेट को पूरी तरह से पुनर्प्राप्त किया जा सकता है जब गंतव्य एन (एन = 1+K) को जमा करता है किसी भी क्रम में बिना गियर वाले पैकेट, जहाँ N, K. सुरक्षा से मामूली बड़ा होता है उपर्युक्त विशेषता का उपयोग करके प्राप्त किया जाता है, यदि, वैध उपयोगकर्ता N को जमा करता है ईव्सड्रोपर से पहले पैकेट करता है।

इस काम में, हम उन योजनाओं की जांच शुरू करते हैं जिनमें क्रॉस-लेयर रैटलेस एन्कोडिंग है विलंबित वातावरण में गोपनीयता हासिल करने के लिए शोषण किया जाता है। प्रस्तावित पहली योजना में, संचारित एंटीना चयन (TAS) मुख्य स्टेशन को बेहतर बनाने के लिए बेस स्टेशन पर कार्यरत है चैनल और, कृत्रिम शोर (एएन) एक सहकारी जैमर के उपयोग से नीचा दिखाना है ईव्सड्रोपर का चैनल। उल्लंघन की गुणवत्ता की संभावना (QVP), जिसमें दोनों शामिल हैं देरी उल्लंघन संभावना और अवरोधन संभावना, का उपयोग प्रदर्शन मीट्रिक के रूप में किया जाता है। QVP के लिए एक क्लोज-फॉर्म अभिव्यक्ति व्युत्पन्न है। हमारे अध्ययन से पता चलता है कि संख्या बढ़ाने पर एएन के साथ टीएएस का उपयोग करते समय स्रोत (एनए) पर एंटेना की देरी के लिए क्यूवीपी घट जाती है संवेदनशील सेवाएं, जबकि, सहनशील अनुप्रयोगों में देरी के मामले में, एनए को बढ़ाना प्रभावी है कम SNR पर।

एक नोड पर कई एंटेना को रोजगार देना नोड के आकार से महंगा और सीमित है। इसमें दिशा, हम इस मुद्दे को किस स्थान पर दो-स्तरीय सहकारी रिले योजना द्वारा संबोधित करते हैं सहायक सहकारी ठेला का उपयोग पैकेटों की डिकोडिंग दर में तेजी लाने के लिए किया जाता है उपयोगकर्ता का इरादा है। फीडबैक-एडेड ट्रांसमिशन (एफटी) और अन-एडेड ट्रांसमिशन (यूटी) दोनों हैं QVP के लिए अध्ययन और क्लोज-फॉर्म अभिव्यक्ति व्युत्पन्न है। परिणाम से पता चलता है कि एफटी के लिए, एक वृद्धि कुल शक्ति में QVP कम हो जाता है, और स्रोत पैकेटों की संख्या में वृद्धि करके अवरोधन बनता है संभावना UT और FT दोनों के लिए तय होती है

क्रॉस-लेयर रैटलेस एन्कोडिंग में, एक लेयर FEC विधि के लक्ष्य और आवश्यकताएं समझौता करती हैं अन्य परत FEC विधि का प्रदर्शन। इसे दूर करने के लिए, हम एक प्रस्ताव देते हैं सुरक्षित योजना जिसमें आरसी का उपयोग FEC के लिए भौतिक परत (PHY) में सहकारी में किया जाता है देरी-विवश वातावरण। उल्लंघन की संभावना (Prvio) का उपयोग प्रदर्शन के रूप में किया जाता है मीट्रिक जिसमें शामिल हैं: 1) विश्वसनीयता आउटेज प्रायिकता, अर्थात्, संभावना जिसके साथ जानकारी को समय की कमी और टी) जानकारी के भीतर सफलतापूर्वक डिकोड नहीं किया जा सकता है अवरोधन संभावना, जो गोपनीयता प्रदर्शन को दर्शाता है। चूंकि आरसी दर को समायोजित कर सकता है मक्खी, हम सिस्टम प्रदर्शन का विश्लेषण करते हैं जब रिले संदेश का एक हिस्सा प्रसारित करता है और रिसीवर ऊर्जा संचय (ईए) करता है। हम Prvio की एक बंद फॉर्म अभिव्यक्ति प्राप्त करते हैं शोर अनुपात (SNR) के लिए उच्च सिग्नल पर एकल-रिले प्रणाली जब रिसीवर या तो जमा होता है प्राप्त संकेतों से ऊर्जा या पारस्परिक जानकारी (एमआई)। कुल मिलाकर, परिणाम दिखाते हैं सेवा की गुणवत्ता (क्यूओएस) आवश्यकताओं की गारंटी के लिए PHY-RC के महत्वपूर्ण लाभ जिसमें गोपनीयता, विश्वसनीयता और कम विलंबता शामिल हैं।

इस थीसिस के उत्तरार्ध में, हम पुनर्योजी के साथ एक प्रणाली के गोपनीयता प्रदर्शन का अध्ययन करते हैं आरसी का उपयोग करके रिले और क्यूवीपी को कम करने के लिए रिले चयन तकनीक का प्रस्ताव करता है। हम भी एक दोहरे-हॉप सहकारी प्रणाली की गोपनीयता का विश्लेषण करें जिसमें कई डीकोड-फॉरवर्ड शामिल हैं आरसी का उपयोग करने में देरी-विवश वातावरण में रिले करता है, जहां एक अलग समय सीमा मौजूद है दोनों हॉप्स के लिए।

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AN	Artificial Noise
APP	Application Layer
BER	Bit Error Rate
CSI	Channel State Information
CDF	Cumulative Distribution Function
CCDF	Complementary Cumulative Distribution Function
CDMA	Code Division Multiple Access
dB	Decibel
DF	Decode-and-forward
DSS	Direct Sequence Spreading
EA	Energy Accumulation
FEC	Forward Error Correction
FT	Feedback-aided transmission
IoT	Internet-of-Things
IIoT	Industrial-Internet-of-Things
IFT	Inverse Fourier Transform
ITRS	Improved Traditional Relay Selection
i.i.d	Independent and Identically Distributed
LT	Luby Transform
MRC	Maximal-Ratio-Combining
MI	Mutual-Information
MIMO	Multiple-Input-Multiple-Output
MISO	Multiple-Input-Single-Output
MGF	Moment Generating Function
NB	Negative-Binomial

ORS Optimal Relay Selection
PHY Physical layer
PDF Probability Distribution Function
PLS Physical Layer Security
QVP Quality of Violation-Probability
QoS Quality of Service
RC Rateless codes
R.V. Random-Variable
SNR Signal to Noise Ratio
SOP Secrecy Outage Probability
SC Selection Combining
SINR Signal-to-noise-plus-interference-ratio
TRS Traditional Relay Selection
TAS Transmit Antenna Selection
UT Un-aided Transmission