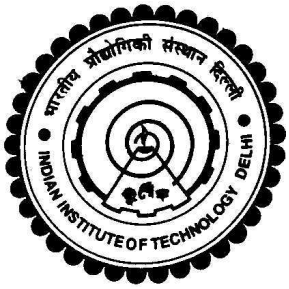
RESOURCE ALLOCATION AND PERFORMANCE ANALYSIS FOR SECRECY IN AMPLIFY-AND-FORWARD RELAY SYSTEM

ABHISHEK JINDAL



BHARTI SCHOOL OF TELECOMMUNICATION
TECHNOLOGY AND MANAGEMENT
INDIAN INSTITUTE OF TECHNOLOGY DELHI
MAY 2017

©Indian Institute of Technology Delhi (IITD), New Delhi, 2017

RESOURCE ALLOCATION AND PERFORMANCE ANALYSIS FOR SECRECY IN AMPLIFY-AND-FORWARD RELAY SYSTEM

by

ABHISHEK JINDAL

BHARTI SCHOOL OF TELECOMMUNICATION TECHNOLOGY
AND MANAGEMENT

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

INDIAN INSTITUTE OF TECHNOLOGY DELHI
MAY 2017

Certificate

This is to certify that the thesis entitled **"Resource allocation and performance analysis for secrecy in amplify-and-forward relay system"** being submitted by **Mr. Abhishek Jindal** to the Bharti School of Telecommunication Technology and Management, 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
and
Bharti School of Telecommunication
Technology & Management
Indian Institute of Technology Delhi

Date:
Place: New Delhi

Acknowledgments

First of all, I express gratitude to my supervisor, Prof. Ranjan Bose, for taking me under his guidance. He has been a constant support during all the years of my Ph.D. With him, I have learnt to formulate and solve a problem from the basic motivation. Also, his encouragement made me capable enough to face the challenges associated with difficult problems and to come up with innovative solutions. I hope to memorize this for my lifetime.

I would like to thank my research committee members Prof. Shankar Prakriya, Dr. Manav Bhatnagar and Dr. Vinay Ribiero for their critical but constructive comments during this period which polished my work. A special thanks goes to Dr. Swades De of Department of Electrical Engineering, and fellow research scholars Ravikant Saini, Sasi Vinay Pechetti, and Chinmoy Kundu for a lot of insightful discussions during the problems solved jointly. I also sincerely thank fellow research scholar Sabyasachi Gupta for being a true friend and support. In addition to research, I learnt a lot from him during our chats. He is more like an elder brother to me.

Any acknowledgment is not complete without mentioning the source of strength which led to the completion of the work. Hence, I thank my parents, younger brother and younger sister for being selfless supporters of my aims during the lifetime. Their encouragement led me to take up this challenging task and complete it to the best of my potential. I wholeheartedly thank my to be wife for being extremely supportive during the last phase of completion of Ph.D. I also take this opportunity to thank Prof. Natarajan Kalyanasundaram and my friend Anindya Gupta of Jaypee Institute of Information Technology, Noida, India for teaching me initial steps of doing research which ultimately motivated me to enroll for a Ph.D.

Abhishek Jindal

Dedicated to my parents
Mr. Ram Saran Jindal and Mrs. Anita Jindal
and
my brother and sister
Mr. Sumeet Jindal and Ms. Shweta Jindal
and
my extremely supportive to be wife
Ms. Priyanka Gupta

Abstract

Wireless communication is an important part of our lives and is gaining importance with the development of newer applications around it. Hence, security of the data transmitted over wireless is of utmost concern due to the openness of the medium. Any unauthorized node can tap and decode the information, which is undesirable. Hence, cryptographic techniques are used to design keys at the upper layers which rely on the limited computing capability of an eavesdropper and hence its inability to decipher the key by exhaustive search. However, in wireless communication, the information exchange about the key may be easily intercepted by eavesdropper and thus this may not provide a permanent solution.

In this thesis, we investigate physical layer security in dual-hop (DH) amplify-and-forward (AF) relay system under the two scenarios of links between source, destination and source, eavesdropper - (i) with direct link (WDL); (ii) without direct link (WoDL).

In the first part, we study the secrecy outage probability (SOP) of the DH-AF-WoDL system. We show that obtaining closed-form expression is difficult but lower and upper bounds can be obtained with suitable bounds on the end-to-end signal to noise ratios. The bounds find direct application in obtaining the bounds on SOP for relay selection in the DH-AF-WoDL multi-relay system. However, this work assumes that the channel state information (CSI) of eavesdropper is available. We extend our results to the case when instantaneous CSI is unknown but statistical CSI of eavesdropper is known.

In the remaining thesis, we assume a multicarrier (MC) setup and study the benefits of MC diversity to security. This will involve pairing the carriers at the relay i.e. instead of forwarding the signal on the same carrier on which it is received, it is forwarded on a different carrier to optimize the design objective. This also involves the decision to relay or not i.e., the mode of transmission on a carrier to be relay-aided or source-only. The considered problems belong to the class of mixed integer non-linear programs and

are difficult to solve. We propose tractable solutions for each problem.

In the second part of the thesis, we study a fundamental problem of distrust among the nodes involved in communication. We consider a MC-DH-AF-WoDL system with multiple untrusted users. In this setup we solve the following problems: secure sum rate maximization, max-min fair resource allocation and total power minimization for per user secure sum rate demand. We propose locally optimal solutions based on alternate optimization in which some variables are fixed and the optimization is done with respect to others and vice versa.

In the third part of the thesis, we consider a MC-DH-AF-WDL system. The availability of the direct link increases the degrees of freedom of the system since a relay can either aid in increasing the secure rate or achieving positive rate on carriers with zero rate otherwise. We study resource allocation in the setup as a two part problem. The first part assumes individual power constraints, while the second considers total power constraint on the powers used at source and relay. In individual power constraint, we solve relay power allocation and pairing jointly for a known source power allocation and vice versa. In total power constraint, we propose two schemes based on sequential geometric programming. Both the schemes are based on obtaining subcarrier pairing for a fixed power allocation at the nodes and vice versa. Under both the constraints we obtain several properties of the secure rate function which gives a deep insight in the system performance. We also obtain a closed-form joint power allocation and subcarrier pairing under both the considered constraints based on a different objective function which is an upper bound on the original. Although, this proves to be suboptimal, but there is a trade of between performance and complexity.

सार

बेतार संचार हमारे जीवन का एक महत्वपूर्ण हिस्सा है और इसके आसपास नए अनुप्रयोगों के विकास के साथ महत्व प्राप्त कर रहा है। इसलिए, वायरलेस माध्यम के खुलेपन के कारण, संचारित डेटा की सुरक्षा अत्यधिक चिंता का विषय है। कोई अनधिकृत नोड जानकारी की व्याख्या कर सकती है, जो अवांछनीय है। अतः, क्रिप्टोग्राफिक तकनीकों का इस्तेमाल ऊपरी परतों पर कुंजियों को डिजाइन करने के लिए किया जाता है जो अनधिकृत नोड की सीमित कंप्यूटिंग क्षमता पर निर्भर होते हैं, जिससे वह इन्हे संपूर्ण खोज द्वारा समझने में असमर्थत रहे। हालांकि, वायरलेस संचार में, कुंजी के बारे में आदान-प्रदान के दौरान, आसानी से छिपकर इसके बारे में जानकारी हो सकती है, इसीलिए संभवतः कुंजी स्थायी समाधान प्रदान नहीं करें।

इस थीसिस में, हम भौतिक परत सुरक्षा की जांच दोहरी-हॉप (डीएच) बढ़ोतरी-आगे (एएफ) रिले प्रणाली में स्रोत, गंतव्य और स्रोत, अनधिकृत नोड के बीच संपर्क के दो परिदृश्यों के तहत करते हैं- (i) सीधा संपर्क (डब्ल्यूडीएल) के साथ; (ii) सीधा संपर्क के बिना (डब्ल्यूओडीएल)।

पहले भाग में, हम डीएच-एएफ-डब्ल्यूओडीएल में गोपनीयता आउटेज संभावना (एसओपी) का अध्ययन करते हैं। हम दिखाते हैं कि बंद-अभिव्यक्ति प्राप्त करना कठिन है, लेकिन कम और ऊपरी सीमा अंत-से-अंत सिग्नल-से-शोर अनुपात पर उचित सीमा से प्राप्त किया जा सकता है। प्राप्त की गई सीमाओं से डीएच-एएफ़-डब्ल्यूओडीएल बहु रिले प्रणाली में रिले चयन के लिए एसओपी पर सीमाएं प्राप्त होती है। हालांकि, यह काम मानता है कि अनधिकृत नोड की चैनल दशा (सीएसआई) उपलब्ध है। हम इस मामले में अपने परिणामों का विस्तार करते हैं जब तात्कालिक सीएसआई अज्ञात है लेकिन सांख्यिक सीएसआई उपलब्ध है।

शेष थीसिस में, हम एक बहु-वाहक (एमसी) व्यवस्था को मानते हैं और एमसी विविधता के लाभों का अध्ययन सुरक्षा के लिए करते हैं। इसमें रिले में वाहकों को जोड़ा जाएगा, अर्थात इसके बजाय कि जिस वाहक पर संकेत प्राप्त किया गया है उसी पर आगे भेजा जाए, एक अलग वाहक पर भेजा जाएगा ताकि निर्धारित उद्देश्य अनुकूलित किया जा सके। इसमें यह भी निर्णय लेने के लिए शामिल है कि एक वाहक पर संचरण रिले की सहायता से होगा या केवल स्रोत ही संचरण करेगा। अध्ययन की गयी समस्याएं मिश्रित पूर्णांक गैर-रैखिक कार्यक्रमों की

श्रेणी से संबंधित हैं और हल करने के लिए कठिन हैं। हम प्रत्येक समस्या के लिए विनयशील समाधान का प्रस्ताव देते हैं।

थीसिस के दूसरे भाग में, हम संचार में शामिल नोड्स में अविश्वास की एक बुनियादी समस्या का अध्ययन करते हैं। हम एक एमसी-डीएच-एएफ़-डब्ल्यूओडीएल सिस्टम पर विचार करते हैं जिसमें बहु अविश्वस्त उपयोगकर्ता हैं। इस व्यवस्था में हम निम्नलिखित समस्याओं का समाधान करते हैं: अधिकतम सुरक्षित योग दर, अधिकतम-न्यूनतम निष्पक्ष संसाधन आवंटन और कुल बिजली कम से कम में उपयोगकर्ता की सुरक्षित योग दर की मांग को पूरा करना। हम वैकल्पिक अनुकूलन पर आधारित स्थानीय रूप से इष्टतम समाधान का प्रस्ताव करते हैं। जिसमें कुछ चर तय हैं और बाकि का अनुकूलन किया जाता है और फिर इसके विपरीत।

थीसिस के तीसरे भाग में, हम एक एमसी-डीएच-एएफ़-डब्ल्यूडीएल व्यवस्था पर विचार करते हैं। सीधे लिंक से व्यवस्था की स्वतंत्रता की हद बढ़ जाती है क्योंकि रिले शून्य दर के साथ वाहकों पर सुरक्षित दर बढ़ाने या सकारात्मक दर प्राप्त करने में सहायता कर सकता है। हम संसाधन आवंटन की समस्या का अध्ययन दो भाग में करते हैं। प्रथम भाग स्रोत और रिले पे व्यक्तिगत बिजली की बाधा को मानता है, जबकि दूसरा कुल बिजली की बाधा को। व्यक्तिगत बिजली की बाधा में, हम ज्ञात स्रोत बिजली आवंटन के लिए संयुक्त रूप से रिले बिजली आवंटन और वाहक जोड़ने को हल करते हैं और फिर इसके विपरीत। कुल बिजली बाधा में, हम क्रमबद्ध ज्यामितिक प्रोग्रामिंग के आधार पर दो योजनाओं का प्रस्ताव करते हैं। दोनों योजनाएं नोड्स में ज्ञात बिजली आवंटन के लिए वाहक जोड़ने पर और फिर इसके विपरीत करने पर आधारित हैं। दोनों बाधाओं के तहत हमने सुरक्षित दर के कई गुण प्राप्त करें हैं जो कि हमें गहन अंतर्दृष्टि प्रदान करते हैं। हम एक बंद-अभिव्यक्ति संयुक्त बिजली आवंटन और वाहक जोड़ना भी प्राप्त करते हैं जो कि मूल दर के ऊपरी बाध्य पर आधारित है। यद्यपि, यह उपइष्टतम साबित होता है, लेकिन प्रदर्शन और जटिलता के बीच एक व्यापार है।

Table of Contents

List of Figures

List of Tables

List of Algorithms

List of Abbreviations

AF	Amplify-and-forward
AM	Alternate maximization
AWGN	Additive white Gaussian noise
CSI	Channel state information
DF	Decode-and-forward
DH	Dual-hop
DL	Direct link
FCSI	Full channel state information
ICSI	Instantaneous channel state information
LB	Lower bound
MC	Multicarrier
MILP	Mixed integer linear program
MINLP	Mixed integer non-linear program
NP	No pairing
NT	No transmission
OFDMA	Orthogonal frequency-division multiple access
OFDM	Orthogonal frequency-division multiplexing
P	Pairing
PLS	Physical layer security
RA	Relay aided mode
SC	Subcarrier
SCSI	Statistical channel state information
SGP	Sequential geometric programming
SNR	Signal-to-noise ratio
SO	Source only transmission
SOP	Secrecy outage probability

SRM	Sum rate maximization
SU	Suboptimal solution
UB	Upper bound
WDL	With direct link
WoDL	Without direct link
wrt	with respect to