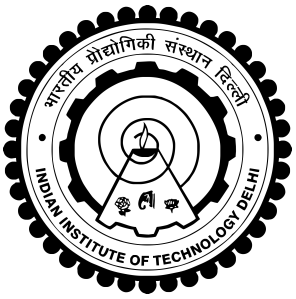
IMPROVING SECRECY AND SPECTRAL UTILIZATION EFFICIENCY IN NETWORKS WITH UNDERLAY COGNITIVE NODES

PRATIK CHAKRABORTY



BHARTI SCHOOL OF TELECOMMUNICATION TECHNOLOGY AND MANAGEMENT
INDIAN INSTITUTE OF TECHNOLOGY DELHI
DECEMBER 2018

IMPROVING SECRECY AND SPECTRAL UTILIZATION EFFICIENCY IN NETWORKS WITH UNDERLAY COGNITIVE NODES

by

PRATIK CHAKRABORTY

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

DECEMBER 2018

CERTIFICATE

This is to certify that the thesis titled **IMPROVING SECRECY AND SPECTRAL UTILIZATION EFFICIENCY IN NETWORKS WITH UNDERLAY COGNITIVE NODES**, submitted by **Mr. Pratik Chakraborty**, to the Indian Institute of Technology Delhi for the award of the degree of **Doctor of Philosophy**, is a bona fide record of the research work done by him under our supervision.

The contents of this thesis, in full or in parts, have not been submitted to any other Institute or University for the award of any degree or diploma.

Dr. Shankar Prakriya
Professor
Department of Electrical Engineering
Indian Institute of Technology Delhi
Hauz Khas New Delhi 110016

Place: New Delhi

ACKNOWLEDGEMENTS

This thesis would not have been possible without the help of some amazing people around me. I take this opportunity to thank them for making my stay at IIT Delhi a memorable and enjoyable one.

First and foremost, I would like to thank my advisor Prof. Shankar Prakriya for his support, encouragement and constructive criticism. Without his constant supervision and able guidance, this thesis would not have been possible. I was first introduced to him during our Digital Communications class. His lectures were deeply engaging and enlightening. I fondly remember the long meetings we had after he became my advisor. The discussions were stimulating and enriching. I have gained a lot from them. I sincerely thank him for the flexibility he has given me to work on areas I am comfortable with. I am grateful for the trouble he has taken to thoroughly read and correct our research papers and my thesis drafts.

I would like to thank my Student Research Committee (SRC) members Prof. Shiv Dutt Joshi, Prof. Brejesh Lall and Prof. Monika Aggarwal for their valuable comments and suggestions during my bi-yearly seminars. It has helped me streamline my work and progress substantially.

Taking a course in an IIT is always a great learning experience. In this regard, I would specially mention Prof. Ranjan Kumar Mallik and Prof. Surendra Prasad, who taught Signal Theory and Detection and Estimation Theory respectively. Learning from them was truly a priceless experience.

I would like to take this opportunity to appreciate and thank the current and the past students Bhupendra Kumar, Komal Janghel, Modem Sudhakar, Anup Mandpura and Late Dileep Verma of our lab for their camaraderie and spirit of collaboration. Thanks to them for keeping the spirit alive.

I would also acknowledge the facilities and resources provided by IIT Delhi in general, and Bharti School of Telecommunication Technology and Management in partic-

ular.

During this long tenure, I faced many highs and lows. At times of distress, it was friends like Bodhibrata Mukhopadhyay, Sourangsu Chowdhury, Shoaib Ali, Mrinmoy Misra, Mousumi Mukherjee, Ankur Bhattacharjee and Kamal Biswas, who kept my morale high. I thank them for their friendship and their encouragement. I owe a lot to them.

Finally, I am much more than grateful to my family – my pillar of strength. Full credit goes to my grandmother, uncle and my parents who believed in me that I would be able to complete this humongous task successfully. Unknowingly they became a part of my roller-coaster journey. My father took keen interest in my work and often asked me to explain my research. While doing so, I mastered the art of explaining complicated equations and technical jargon in lucid vernacular. I think this is the ultimate aim of any research and my father has unknowingly taught me this skill. Thank you *baba*. It is truly impossible to mention all the sacrifices my mother has made for me. It is because of her constant monitoring and strict decisions I am what I am today. Love you *maa*.

Pratik Chakraborty

ABSTRACT

The fifth generation (5G) wireless communication standard aims to provide users with high speed, reliable and secure communication in areas with dense network traffic. However, increase in the number of wireless devices and high-speed multimedia based services has resulted in acute spectrum scarcity. For this reason, there has been a lot of research interest on techniques that can increase spectrum utilization efficiency. In cellular communications, use of a high frequency-reuse factor and deployment of heterogeneous networks are efforts in this direction. Most of such techniques are limited by their tendency to increase co-channel interference. For this reason, interference management techniques are being investigated by researchers in recent years. Underlay cognitive radio framework offers a natural way to manage interference and increase spectrum utilization efficiency. In this thesis, various optimization and resource allocation issues are examined that maximize secondary throughput in such frameworks. Resource allocation and optimization to maximize secondary secrecy performance is also examined, and use of jamming techniques is investigated. Finally, the impact of underlay frameworks on secrecy performance of the primary network is analyzed.

In a two-hop underlay secondary network, an analytical expression is derived for secrecy outage probability, assuming that a passive eavesdropper overhears the secondary transmission. Unlike prior works, the direct channel from the secondary source to destination is not ignored (by not assuming it to be weak), and that optimal combining of the direct and relayed signals at the secondary destination leads to improved secrecy outage performance is established. The fact that transmitters of underlay secondary networks have random powers, and also the fact that relays are expected to be used for communication over short distances to maintain quality of service, ignoring the direct channel leads to a pessimistic estimate of secrecy outage. It is further demonstrated that using a smaller fraction of the available interference temperature limit (ITL) at the secondary source leads to higher secrecy. Though transmit powers are random in underlay cognitive radios, the back-off factor is a statistical quantity that depends on the statistics of the legitimate and wiretap links.

Through an analytical expression for secrecy outage probability, it is established in this thesis that apportioning the ITL in a statistically optimal manner between a secondary source and a friendly jammer improves secrecy of a multi-user underlay downlink secondary network when it is subject to passive eavesdropping. In this framework, the source transmits symbols to the destination, while the jammer transmits artificial noise to confound the passive eavesdropper. A novel method is proposed that selects the best jammer among a set of idle secondary receivers to provide maximum jamming power even when the channel to the eavesdropper is unknown. It is analytically shown that apportioning the ITL always leads to improved secrecy performance as compared the case when it is used entirely for signal transmission.

Performance of two co-existing underlay secondary downlink networks having concurrent transmission capabilities is evaluated in this thesis. Optimum apportioning of the ITL between transmitters of two secondary networks is determined so that secondary throughputs can be improved while maintaining quality of service of the primary network. Network management strategies are evolved, which determine this optimal apportioning, and whether both secondary transmitters should transmit concurrently or not. Both fixed and adaptive rate secondary transmissions are considered. Network management strategies are evolved separately for cases of statistical and instantaneous channel knowledge. The proposed framework can be readily used to improve spectrum utilization efficiency of cellular systems. In such scenarios, the secondary transmitters may either be pico-cell stations or D2D devices that reuse the spectrum of the macrocell.

While reusing the spectrum in underlay frameworks, is important to ensure that the primary network is secure when it shares its spectrum with co-existing secondary networks. Methods to improve network secrecy are proposed for situations where idle receivers of the two secondary downlink networks are untrusted and eavesdrop on the primary transmissions. Through closed-form analytical expressions it is shown that the primary network is most secure when secondary networks apportion the ITL and transmit concurrently. Moreover, there exists an optimum ITL apportioning value that guarantees highest secrecy for the primary network, and this value is different than the one that solely improves secondary throughput.

The insights derived in this thesis form a useful aid to system designers, and can help them optimize performance.

सार

बेतार (वायरलेस) संचार मानक की पांचवीं पीढ़ी (5 जी) का उद्देश्य घने संजाल (नेटवर्क) यातायात वाले क्षेत्रों में उपयोगकर्ताओं को उच्च गति, विश्वसनीय और सुरक्षित संचार प्रदान करना है। हालांकि, बेतार उपकरणों और उच्च गति के बहुमाध्यम आधारित सेवाओं की संख्या में वृद्धि के परिणामस्वरूप तीव्र रूप से वर्णक्रम (स्पेक्ट्रम) में कमी आई है। इस कारण से, तकनीकों पर बहुत अधिक शोध रुचि रही है जो वर्णक्रम उपयोगिता दक्षता में वृद्धि कर सकती है। सेलुलर संचार में, उच्च आवृत्ति पुनः-उपयोग कारक का प्रयोग और विषम संजाल की तैनाती इस दिशा में प्रयास हैं। ऐसी तकनीकें सह-चैनल हस्तक्षेप को बढ़ाने की प्रवृत्ति से सीमित हैं। इस कारण से, हाल के वर्षों में शोधकर्ताओं द्वारा हस्तक्षेप प्रबंधन तकनीकों की जांच की जा रही है। अंडरले संज्ञानात्मक रेडियो फ्रेमवर्क, हस्तक्षेप का प्रबंधन करने और वर्णक्रम उपयोगिता दक्षता बढ़ाने के लिए एक प्राकृतिक तरीका प्रदान करता है। इस शोध प्रबंध में, विभिन्न अनुकूलन और संसाधन आवंटन मुद्दों की जांच की गयी है जो इस तरह के ढांचे में अप्रधान प्रवाह क्षमता (थ्रुपुट) को अधिकतम करते हैं। अप्रधान गोपनीयता (सीकृसी) प्रदर्शन को अधिकतम करने के लिए संसाधन आवंटन और इष्टतमीकरण की भी जांच की गयी है, और जैमिंग तकनीकों का उपयोग की जांच की गयी है। अंततः, प्राथमिक संजाल के गुप्त प्रदर्शन पर अंडरले फ्रेमवर्क का प्रभाव विश्लेषित किया गया है।

दो-हॉप अंडरले अप्रधान संजाल में, सीकृसी आउटेज प्रोबेबिलिटी की एक विश्लेषणात्मक अभिव्यक्ति (गणितीय) निकाली गयी है, यह मानते हुए कि एक निष्क्रिय छिद्रण अप्रधान संचरण को छुपकर सुन लेता है। पूर्व कार्यों के विपरीत, अप्रधान स्रोत से गंतव्य तक सीधी चैनल को अनदेखा नहीं किया गया है (इसे कमजोर मानते हुए नहीं), और अप्रधान गंतव्य पर प्रत्यक्ष और रिलेड सिग्नल के इष्टतम (ऑपटिमल) संयोजन से बढ़ता हुआ आउटेज प्रदर्शन स्थापित होता है। तथ्य यह है कि अंडरले अप्रधान संजाल के ट्रांसमीटरों में यादृच्छिक (रैंडम) शक्तियां होती हैं, और यह भी तथ्य है कि सेवा की गुणवत्ता को बनाए रखने के लिए रिले को कम दूरी पर संचार के लिए उपयोग करने की उम्मीद की जाती है। सीधी चैनल को अनदेखा करने से सीकृसी आउटेज का ग़लत अनुमान होता है। यह आगे दिखाया गया है कि अप्रधान स्रोत पर उपलब्ध हस्तक्षेप तापमान सीमा (आईटीएल) के एक छोटे से अंश का उपयोग उच्च गोपनीयता की ओर जाता है। हालांकि संचार शक्तियां अंडरले संज्ञानात्मक रेडियो में यादृच्छिक होती हैं, बैक-ऑफ कारक एक सांख्यिकीय मात्रा है जो वैध और वायरटैप लिंक के आंकड़ों पर निर्भर करता है।

आउटेज प्रोबेबिलिटी के लिए एक विश्लेषणात्मक अभिव्यक्ति के माध्यम से, यह इस शोध प्रबंध में स्थापित किया गया है कि एक बहु-उपयोगकर्ता अंडरले डाउनलिंक अप्रधान संजाल की गुप्तता में सुधार होता है जब यह निष्क्रिय ईवज़ड्रॉपिंग के अधीन होता है और आईटीएल को एक अप्रधान स्रोत और एक अनुकूल जैमर के बीच सांख्यिकीय रूप से इष्टतम तरीके से विभाजित किया जाता है। इस ढांचे में, स्रोत गंतव्य के प्रतीकों को प्रसारित करता है, जबकि जैमर कृत्रिम शोर को निष्क्रिय ईवज़ड्रॉपिंग को भंग करने के लिए प्रसारित करता है। इस शोध

प्रबंध (थीसिस) में एक नवीन विधि का प्रस्ताव किया है जिसमे निष्क्रिय अप्रधान रिसीवर के एक सेट के बीच सबसे अच्छा जैमर का चुनाव करता है ताकि अधिकतम जैमिंग पावर प्रदान किया जा सके, भले ही ईवज़ड्रॉपर के लिए चैनल अज्ञात हो। यह विश्लेषणात्मक रूप से दिखाया गया है कि आईटीएल को विभाजित करने से हमेशा सिग्नल ट्रांसमिशन के लिए इस्तेमाल होने वाले मामले की तुलना में बेहतर गोपनीयता प्रदर्शन होता है।

इस शोध प्रबंध में समवर्ती संचरण क्षमताओं वाले दो सह-विद्यमान अंडरले अप्रधान डाउनलिंक संजालों का प्रदर्शन मूल्यांकन किया गया है। दो अप्रधान संजाल के ट्रांसमीटरों के बीच आईटीएल का इष्टतम विभाजन निर्धारित किया गया है ताकि प्राथमिक संजाल की सेवा को बनाए रखने के दौरान अप्रधान प्रवाह क्षमता (थ्रुपुट) को बेहतर किया जा सके। संजाल प्रबंधन रणनीतियों का विकास किया गया है, जो इस इष्टतम विभाजन को निर्धारित करते हैं, और यह बताते हैं कि क्या दोनों अप्रधान ट्रांसमीटरों को समवर्ती रूप से संचारित करना चाहिए या नहीं। दोनों निश्चित और अनुकूली रेट अप्रधान प्रसारण को माना गया है। सांख्यिकीय और तात्कालिक चैनल ज्ञान के मामलों के लिए संजाल प्रबंधन रणनीतियों को अलग से विकसित किया गया है। प्रस्तावित रूपरेखा का उपयोग सेलुलर निकाय (सिस्टम) की वर्णक्रम उपयोगिता दक्षता में सुधार के लिए आसानी से किया जा सकता है। ऐसे परिदृश्यों में, अप्रधान ट्रांसमीटर या तो पिको-सेल स्टेशन या डी-2-डी उपकरण हो सकते हैं जो मैक्रो-सेल के वर्णक्रम का पुन: उपयोग करते हैं।

अंडरले फ्रेमवर्क में वर्णक्रम का पुन: उपयोग करते समय, यह सुनिश्चित करना महत्वपूर्ण है कि प्राथमिक संजाल सुरक्षित है जब यह सह-मौजूदा अप्रधान संजालों के साथ अपने वर्णक्रम को साझा करता है। संजाल गोपनीयता में सुधार करने के तरीके उन परिस्थितियों के लिए प्रस्तावित किए गए हैं जहां दो अप्रधान डाउनलिंक संजाल के निष्क्रिय रिसीवर अविश्वसनीय होते हैं और प्राथमिक प्रसारण पर नजर रखते हैं। विश्लेषणात्मक अभिव्यक्तियों के माध्यम से यह दिखाया गया है कि प्राथमिक संजाल सबसे सुरक्षित है जब दोनों अप्रधान संजाल आईटीएल को विभाजित करते हैं और साथ ही संचारित करते हैं। इसके अलावा, एक इष्टतम आईटीएल विभाजन मूल्य मौजूद है जो प्राथमिक संजाल के लिए उच्चतम गोपनीयता की प्रत्याभूति देता है, और यह मान उस माध्यम से अलग है जो अप्रधान प्रवाह क्षमता (थ्रुपुट) को पूरी तरह से सुधारता है।

इस शोध प्रबंध में उत्पन्न अंतर्दृष्टि, निकाय अभियंता के लिए उपयोगी सहायता बनाती है, और प्रदर्शन को अनुकूलित करने में उनकी सहायता कर सकती है।

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

3G	3^{rd} Generation
4G	4^{th} Generation
5G	5^{th} Generation
AF	Amplify and Forward
AN	Artificial Noise
AP	Access Point
ART	Adaptive Rate Transmission
BS	Base Station
CANM	Channel Aware Network Management
CDF	Cumulative Distribution Function
CDMA	Code Division Multiple Access
CR	Cognitive Radio
CSI	Channel State Information
D2D	Device to Device
DES	Data Encryption Standard
DF	Decode and Forward
DMC	Discrete Memoryless Channel
DSA	Dynamic Spectrum Access
DSSS	Direct-Sequence Spread Spectrum
FHSS	Frequency-Hop Spread Spectrum
FNM	Fixed Network Management
FRT	Fixed Rate Transmission
GSC	Generalized Selection Combining
GSM	Global System for Mobile
HetNet	Heterogeneous Network
IoT	Internet of Things
ITL	Interference Temperature Limit
IIT	Indian Institute of Technology

LTE	Long Term Evolution
MRC	Maximal Ratio Combining
NM	Network Management
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
PDF	Probability Density Function
QoS	Quality of Service
RS	Relay Station
RSA	Rivest Shamir Adleman
SC	Selection Combining
SINR	Signal to Interference plus Noise Ratio
SNR	Signal to Noise Ratio

NOTATION

$\lvert\,.\,\rvert$	Absolute value
α	Interference temperature limit apportioning parameter
β	Secondary peak power apportioning parameter
$\Gamma[\,.\,]$	Gamma function defined on the complex plane except for 0 and, negative integers, where $\Gamma(z) = \int_0^\infty t^{z-1}e^{-t}\,dt$
ϕ	Path loss exponent
σ_n^2	Noise variance
τ	Throughput
C	Instantaneous channel capacity
$\bar{C}$	Ergodic capacity
C_S	Instantaneous secrecy capacity
$\bar{C}_S$	Ergodic secrecy capacity
$\mathcal{CN}(0,a)$	Zero mean complex Gaussian distribution with variance a
D	Diversity order
$Di_2[\,.\,]$	Dilogarithm function in terms of Spence's integral, where $Di_2[x] = -\int_1^x \frac{\ln(t)}{t-1}\,dt$
$\exp[\,.\,]$	Exponential function
$Ei[\,.\,]$	Exponential integral for real non-zero values, where $Ei[x] = -\int_{-x}^\infty t^{-1}e^{-t}\,dt$
$E_n[\,.\,]$	Generalized exponential integral for real non-zero values of order n, where $E_n[x] = \int_1^\infty t^{-n}e^{-xt}\,dt$ $(n = 0, 1, 2, \dots)$
$\mathbb{E}_X$	Expectation over random variables X
$\mathbb{E}_{X_1,X_2,\dots,X_N}$	Expectation over random variables $X_1, X_2, \dots, X_N$
$f_X(x)$	Probability density function of random variable X
$F_X(x)$	Cumulative distribution function of random variable X
I_P	Interference temperature limit
$I_{P_{(c)}}$	Critical interference temperature limit
$K_n[\,.\,]$	n^{th} order modified Bessel's function of second kind, where $K_n[x] = \frac{1}{2}\left(\frac{x}{2}\right)^n \int_0^\infty t^{n-1}e^{-\frac{1}{t}-\left(\frac{x}{2}\right)^2 t}\,dt$
$Li_2[\,.\,]$	Euler dilogarithm function, where $Li_2[x] = -\int_0^x \frac{\ln(1-t)}{t}\,dt$
$\max(.)$	Maximum
$\min(.)$	Minimum
p_o	Outage probability
p_{os}	Secrecy outage probability

P	Secondary peak power
P_P	Primary peak power
R	Target rate
R_c	Critical target rate
R_S	Secrecy target rate