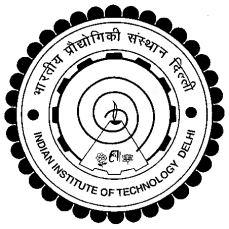
RESOURCE ALLOCATION FOR SECURE OFDMA WITH UNTRUSTED USERS

RAVIKANT SAINI



BHARTI SCHOOL OF TELECOMMUNICATION TECHNOLOGY AND MANAGEMENT
INDIAN INSTITUTE OF TECHNOLOGY DELHI
OCTOBER 2016

RESOURCE ALLOCATION FOR SECURE OFDMA WITH UNTRUSTED USERS

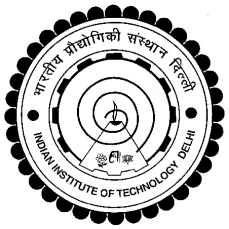
by

RAVIKANT SAINI

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
New Delhi - 110016, India
October 2016

Certificate

This is to certify that the dissertation entitled **Resource Allocation for Secure OFDMA with Untrusted Users**, submitted by **Mr. Ravikant Saini**, a Research Scholar, in the *Bharti School of Telecommunication Technology and Management*, *Indian Institute of Technology Delhi*, *India*, for the award of the degree of **Doctor of Philosophy**, is a record of an original research work carried out by him under my supervision and guidance. The dissertation fulfills all requirements as per the regulations of this Institute and in my opinion has reached the standard needed for submission. Neither this dissertation nor any part of it has been submitted for any degree or academic award elsewhere.

Dr. Swades De
(Supervisor)
Department of Electrical Engineering
Indian Institute of Technology Delhi
New Delhi, 110016, India.

Acknowledgements

PhD is a journey rather than a destination.
I would like to thank all for being a part of it.

First of all, I would like to thank my supervisor Dr. Swades De for his guidance and encouragement which I received throughout this journey. I am thankful for his patience in bearing with me, all of my incapabilities, and helping me come stronger through timely counsellings. His belief in me and his appreciation for all my constraints is really commendable. Finishing a dissertation, in such a constrained domain without his support and care would have been impossible.

I take this opportunity to express my sincere thanks to Prof. Brejesh Lall, Prof. Shankar Prakriya, and Prof. Vinay Ribeiro for their valuable feedback during my end semester presentations.

I would like to thank all my fellow researchers of Computer Networks Research Group, who made this journey a memorable one. Further, I would like to extend them my best wishes for their future endeavors.

Finally, I would like to thank my family members who have supported me in this herculean task with all their might.

Ravikant Saini

Abstract

Physical layer security which finds its basis from the independence of subcarriers, is being considered as a promising solution for security issues in broadcast OFDMA communications systems. The resource allocation problems in the context of physical layer security can be broadly categorized in two scenarios: one has trusted users and an external eavesdropper, and the other has untrusted users.

The focus of this research work has been on resource allocation problems for an OFDMA system with untrusted users. These problems are relatively complex compared to their counterpart with an external eavesdropper, as there are effectively $M-1$ eavesdroppers for each user in a system of M untrusted users. The resource allocation problems are in general non-linear, non-convex, and combinatorial in nature.

In order to help the source in providing secure communication in such a hostile environment, helper nodes can be introduced. Utilization of a helper node for improving the secrecy performance of the system is the key area which has been investigated in the current work. Two types of helper nodes have been considered in two distinct systems models. In one model an exclusive friendly jammer has been considered, and in another model a decode and forward (DF) relay has been considered to aid the secure communication.

In the system model with a friendly jammer two resource allocation problems have been studied. The first problem is weighted sum secure rate maximization, and second problem is Max-min fair resource allocation. Both the considered resource allocation problems are mixed integer non-linear programming (MINLP) problems belonging to the class of NP-hard. Utilization of jammer power introduces new challenge referred as SNR reordering, which complicates the problem further. To handle SNR reordering, a novel strategy referred as constrained jamming is introduced. Additionally, two novel concepts about jammer power utilization, namely, secure rate improvement and subcarrier snatching are described. Secure rate improvement can be utilized for sum rate maximization, and subcarrier snatching can be utilized for fair resource allocation. In the context of fair resource allocation, two strategies based on jammer power usage, namely, proactively fair allocation and on-demand allocation are discussed. Joint source and jammer power allocation is solved using the concepts of alternating optimization and primal decomposition. For all the proposed optimal schemes, suboptimal strategies have been proposed to trade-off between performance and complexity. Asymptotically optimal strategies have

been presented to benchmark optimality of the proposed schemes.

In the DF relay assisted cooperative communication system, two complimentary resource allocation problems, namely, sum rate maximization and sum power minimization, are considered. Both the resource allocation problems are in general MINLP problems. It is shown that both the problems belong to the class of generalized convex problems which can be solved optimally. Optimal subcarrier allocation is obtained while investigating secure rate positivity conditions, and optimal power allocation is achieved by solving KKT conditions. Optimal subcarrier pairing is proposed for efficient resource utilization.

The complex resource allocation problem in the presence of friendly jammer is solved by breaking it in parts: first finding optimal subcarrier allocation at source, then taking decision on jammer power utilization, and finally completing joint optimal source and jammer power allocation. The resource allocation problem in cooperative communication assisted by DF relay is solved by first obtaining optimal subcarrier allocation and then completing optimal power allocation. Utilization of a helper node in an untrusted users' scenario is shown to improve the secrecy performance of a multiuser multicarrier communication system. The performance of the proposed schemes have been shown to outperform a benchmark scheme, namely, equal power allocation.

Contents

List of Figures

List of Tables

List of Symbols

$a_y, b_y, c_y, d_y, e_y, c'_y, d'_y, e'_y$	Coefficients of the fourth order equation
Ab_m	Set of best subcarriers allocated to user m
As_m	Set of snatched subcarriers by user m
B_m	Set of best subcarriers of user m
$C_{i,j}$	Indicator for jth constraint in ith optimization problem
c_i	Indicator for subcarrier i
C	Set of leftover subcarriers in the system
e	Indicator for equivalent eavesdropper on the subcarrier
f	Internal function for short notation of optimal power allocation
F, G	Encoder and Decoder mapping function in wiretap channel model
$f_{i,n}$	Relay to ith user channel coefficient on subcarrier n
$g_{i,n}$	Jammer to ith user channel coefficient on subcarrier n
$h_{i,n}$	Source to ith user channel coefficient on subcarrier n
$h_{R,n}$	Source to Relay channel coefficient on subcarrier n
I_{ao}	Number of iterations in AO procedure
I_{pd}	Number of iterations in PD procedure
I_m	Set of subcarrier of user m over which jammer power can be applied
$\mathcal{J}_0$	Set of subcarriers that are not using jammer power
$\mathcal{J}_1$	Set of subcarriers that are using jammer power
k	Indicator for the rest of the $(M-2)$ users other than m and e
$\mathcal{L}$	Lagrangian of the optimization problems
M	Number of untrusted users
m	Indicator for main user of a subcarrier
N	Number of subcarriers
n	Indicator for a selected subcarrier
N_1	Number of subcarriers not using jammer power
N_2	Number of subcarriers using jammer power

o	Indicator for the rest of the $(M-1)$ users other than m
P_S	Source power budget
P_J	Jammer power budget
P_{s_n}	Source power over subcarrier n
P_{j_n}	Jammer power over subcarrier n
P_{r_n}	Relay power over subcarrier n
$P_{j_n}^{th_i}$	Jammer power threshold for rate improvement over subcarrier n
$P_{s_n}^{th_i}$	Source power threshold for rate improvement over subcarrier n
$P_{j_n}^{o}$	Optimal jammer power achieving maximum secure rate over subcarrier n
$P_{j_n}^{\star}$	Optimal jammer power after constraining $P_{j_n}^{o}$ under jammer power bounds
$P_{j_n}^{r}$	Real root of the fourth order equation
$P_{j_n}^{\diamond}$	Optimal jammer power after constraining $P_{j_n}^{r}$ under jammer power bounds
$P_{j_{k,n}}^{l}$	Lower jammer power bound raised by user k over subcarrier n
$P_{j_{k,n}}^{u}$	Upper jammer power bound raised by user k over subcarrier n
$P_{j_n}^{l}$	Effective lower jammer power bound over subcarrier n
$P_{j_n}^{u}$	Effective upper jammer power bound over subcarrier n
$P_{s_n}^{eq}$	Equal source power on subcarrier n
$P_{j_n}^{eq}$	Equal jammer power on subcarrier n
$P_{s_x}^{*}$	Optimal source power over subcarrier x
$P_{j_{m,n}}$	Jammer power utilised to help user m over subcarrier n
$P_{j_{m,n}}^{*}$	Optimal jammer power using the suboptimal method
$\mathcal{P}_i$	Identifier for optimization problem i
R_m	Sum secure rate of user m
$R_{s_{m,n}}$	Secure rate of user m on subcarrier n
$R_{m,n}$	Rate of user m on subcarrier n
R_{sr_n}	Rate of source to relay link on subcarrier n
R_{rm_n}	Rate of relay to mth user link on subcarrier n
$R_s, \widehat{R_s}$	Sum secure rate of relay assisted system
R_{ssr}	Minimum support secure rate requirement for each user
S_m	Set of subcarriers that user m can snatch
t_n	Dummy vriable to handle $\min$ function
U^a	Set of active users in the system
v	Indicator for a minimum rate user

w	Sent message at source in wiretap channel model
w'	Received estimate at destination in wiretap channel model
w_m	Priority weight of user m
w'_n	Priority weight of the user m mapped over its subcarrier n
x	Indicator for subcarrier in set $\mathcal{J}_0$
y	Indicator for subcarrier in set $\mathcal{J}_1$
$x^{(n)}$	Input to the main channel in wiretap channel model
$y^{(n)}, z^{(n)}$	Output of the main channel channel and the wiretap channel, respectively
x_n, y_n, z_n	Coefficients of the quadratic equation in P_{j_n}
α_n, β_n	Internal parameters in jammer power threshold calculation
$\gamma_{m,n}$	SNR of user m over subcarrier n without jammer power
$\gamma'_{m,n}$	SNR of user m over subcarrier n with jammer power
λ, μ	Lagrange multipliers for power constraints
$\zeta_n, \theta_n, \tau_n$	Lagrange multipliers
ρ_n	Internal parameter in quadratic equation in P_{r_n}
δ	A small positive number
Δ_n	Discriminant of the quadratic in P_{j_n}
σ^2	AWGN noise variance
$\pi_{m,n}$	Subcarrier allocation indicator at source
π_{j_n}	Subcarrier allocation indicator at jammer
ξ	Step size in PD procedure for updating λ
η, ν, κ	Internal parameters used for defining function f