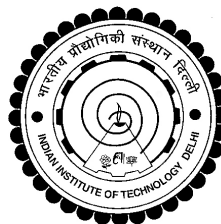


**RESOURCE ALLOCATION FOR SECURE OFDMA
WITH
UNTRUSTED USERS**

RAVIKANT SAINI



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

©Indian Institute of Technology Delhi (IITD), New Delhi, 2016

**RESOURCE ALLOCATION FOR SECURE OFDMA
WITH
UNTRUSTED USERS**

by

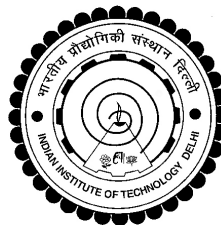
RAVIKANT SAINI

*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 incapacibilities, 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	v
List of Tables	vii
List of Symbols	ix
1 Introduction	1
1.1 Background	1
1.2 Secure Rate Definition	2
1.3 Motivation and Scope of the Dissertation	4
1.3.1 Motivation	4
1.3.2 Scope	5
1.3.3 Problem Definition	5
1.4 Organization	5
2 Literature Survey	7
2.1 Introduction	7
2.2 Trusted Users and External Eavesdropper	8
2.2.1 Single Source-Destination Pair	8
2.2.2 Single Source-Destination Pair with Helpers	9
2.2.3 Multiuser Scenario	11
2.3 Untrusted Users	12
2.4 Research Gap and Motivation	14
2.4.1 Broadcast Communication with Jammer	14
2.4.2 Cooperative Communication with Relay	14
2.5 Summary	15

3	Secure Sum Rate Maximization with Friendly Jammer	17
3.1	Introduction	17
3.1.1	Contribution	17
3.1.2	Chapter Organization	18
3.2	System Model	18
3.3	Resource Allocation Problem	20
3.4	Subcarrier Allocation at Source	21
3.5	Subcarrier Allocation at Jammer, and Jammer Power Bounds	22
3.5.1	Selective Jamming for Secure Rate Improvement	23
3.5.2	SNR Reordering	27
3.5.3	Constrained Jamming to Avoid SNR Reordering	27
3.6	Joint Optimization of Source and Jammer Power	29
3.6.1	Solution of Subproblem-1	31
3.6.2	Solution of Subproblem-2	32
3.6.3	Convergence of Joint Power Allocation	34
3.7	Solution with Reduced Complexity for Sum Rate Maximization	36
3.8	Complexity Analysis	38
3.9	Asymptotic Analysis for Sum Rate Maximization	38
3.9.1	Asymptotic Bounds	40
3.10	Results and Discussion	41
3.10.1	Effect of Jammer Location	42
3.10.2	Effect of Source Power Variation	42
3.10.3	Effect of Jammer Power Variation	44
3.10.4	Performance Variation with Number of Users	45
3.11	Summary	46
4	Max-min Fair Resource Allocation with Friendly Jammer	47
4.1	Introduction	47
4.1.1	Contribution	47
4.1.2	Chapter Organization	48
4.2	Max-min Fair Resource Allocation for Secure OFDMA	49
4.3	Subcarrier Snatching	50
4.4	Proposed Modified Max-min Fairness Scheme	53
4.4.1	Proactively Fair Jammer Power Allocation (PFA)	55

4.4.2	On-demand Jammer Power Allocation (ODA)	55
4.5	Max-min Fairness with Reduced Complexity	57
4.6	Complexity Analysis	58
4.7	Asymptotic Bound for Proposed Max-min Fairness	59
4.8	Results and Discussion	60
4.8.1	Effect of Source Power Variation	60
4.8.2	Effect of Jammer Power Variation	61
4.9	Summary	62
5	Resource Allocation in Cooperative Communication with DF Relay	63
5.1	Introduction	63
5.1.1	Contribution	63
5.1.2	Chapter Organization	64
5.2	System Model	64
5.3	Sum Rate Maximization	65
5.3.1	Subcarrier Allocation	66
5.3.2	Power Allocation	67
5.3.3	Analytical and Graphical Interpretation	71
5.4	Sum Power Minimization	73
5.4.1	User-Level Sum Power Minimization	74
5.5	Subcarrier Pairing	75
5.5.1	Optimal Subcarrier Pairing	75
5.5.2	Sum Rate Maximization	77
5.5.3	Sum Power Minimization	78
5.6	Results and Discussion	78
5.7	Summary	80
6	Conclusion and Future Works	81
6.1	Concluding Remarks	81
6.2	Future Works	82
	Bibliography	84
	Publications	93
	Biodata of the Author	95

List of Figures

1.1	Wiretap channel	2
2.1	Single source-destination pair with external eavesdropper.	9
2.2	Multiple trusted users with external eavesdropper.	11
2.3	Multiple untrusted users.	13
3.1	Broadcast secure OFDMA communication system with untrusted users and a friendly jammer	19
3.2	Secure rate versus source power at various jammer locations with jammer power $P_J/\sigma^2 = 0$ dB.	42
3.3	Secure rate and fairness performance versus source power at $P_{J1}/\sigma^2 =$ 0 dB and $P_{J2}/\sigma^2 = 6$ dB. ‘Rate-ub’: rate upper bound; ‘Fairness-ub’: fairness upper bound.	43
3.4	Secure rate and fairness performance versus jammer power at $P_{S1}/\sigma^2 =$ 12 dB and $P_{S2}/\sigma^2 = 15$ dB.	44
3.5	Secure rate versus number of users M at $P_J/\sigma^2 = 6$ dB, and $P_{S1}/\sigma^2 = 12$ dB and $P_{S2}/\sigma^2 = 15$ dB.	45
4.1	Fairness and secure rate versus source power at $P_{J1}/\sigma^2 = 12$ dB and $P_{J2}/\sigma^2 = 18$ dB.	61
4.2	Fairness and secure rate versus jammer power at $P_S/\sigma^2 = 15$ dB.	62
5.1	DF relay assisted cooperative secure OFDMA communication system with untrusted users	64
5.2	Graphical interpretation of optimal power allocation.	72
5.3	Sum secure rate versus source power.	79
5.4	Sum power per user versus minimum support rate.	80

List of Tables

3.1	Source-users channel gains $ h_{m,n} $	26
3.2	Jammer-users channel gains $ g_{m,n} $	26
3.3	Users' SNRs and secure rate $R_{s_{3,2}}$ versus P_{j_2}	26
3.4	Users' SNRs and secure rate $R_{s_{1,3}}$ versus P_{j_3}	28
3.5	Coefficients of the non linear equation (3.25)	33
4.1	Source-users channel gains $ h_{m,n} $	52
4.2	Jammer-users channel gains $ g_{m,n} $	52
4.3	Complexity comparison of proposed Max-min algorithms	59

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 j th constraint in i th 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 i th user channel coefficient on subcarrier n
$g_{i,n}$	Jammer to i th user channel coefficient on subcarrier n
$h_{i,n}$	Source to i th 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
$P_{j_n}^*$	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 m th 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 variable 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