DESIGN AND ANALYSIS OF NEW COOPERATIVE RELAYING NETWORKS FOR ENHANCING PHYSICAL LAYER SECURITY

BY

AHMED HASSAN ABD EL-MALEK

A Dissertation Presented to the
DEANSHIP OF GRADUATE STUDIES

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS
DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the
Requirements for the Degree of

DOCTOR OF PHILOSOPHY
In

ELECTRICAL ENGINEERING

DECEMBER 2015

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS
DHAHRAN 31261, SAUDI ARABIA

DEANSHIP OF GRADUATE STUDIES

This thesis, written by **AHMED HASSAN ABD EL-MALEK** under the direction of his thesis adviser and approved by his thesis committee, has been presented to and accepted by the Dean of Graduate Studies, in partial fulfillment of the requirements for the degree of **DOCTOR OF PHILOSOPHY IN ELECTRICAL ENGINEERING.**

Dissertation Committee

Dr. Salam A. Zummo (Adviser)

Dr. M.-S. Alouini (Member)

23.2.2016

Dr. Shokri Selim (Member)

azzedine zerguine

Dr. Azzedine Zerguine (Member)

Dr. Ali Muqaibel (Member)

Dr. Ali A. Al-Shaikhi
Department Chairman

Dr. Salam A. Zummo
Dean of Graduate Studies

7/3/16

Date

© Ahmed H. Abd El-Malek
December 2015

To My Parents, Sister and Brother

ACKNOWLEDGMENTS

Firstly, Praise be to Allah, Lord of the Worlds, for the good health and wellbeing that were necessary to complete this dissertation.

I would like to express my sincere gratitude to my advisor Prof. Salam Zummo for the continuous support of my Ph.D. study and related research, for his excellent guidance, patience, caring and motivation. His thoughtful comments and criticisms have driven me substantially to achieve more significant contributions.

I am deeply grateful to the committee members of my dissertation Prof. Mohamed-Slim Alouini, Prof. Shokri Selim, Prof. Azzedine Zerguine, and Dr. Ali Muqaibel for their constructive comments, suggestions, and support.

My sincere thanks also go to Dr. Fawaz Al-Qahtani and Dr. Anas Salhab, who give me a chance to collaborate with them and provide me with the necessary knowledge and experience to continue my dissertation work. Without their valuable support, it would not be possible to conduct this research.

I would also like to thank my parents, my sisters, and brother. They were always supporting me and encouraging me with their best wishes.

Finally, I would like to express my thanks to my Electrical Engineering Department and my KFUPM for their friendly support and cooperation.

TABLE OF CONTENTS

ACKNOWLEDGMENTS **v**

LIST OF FIGURES **xi**

LIST OF ACRONYMS **xvii**

ABSTRACT **xx**

ABSTRACT (ARABIC) **xxiii**

CHAPTER 1 INTRODUCTION **1**

1.1 Motivation 1

1.2 Background 6

1.2.1 MIMO Systems 9

1.2.2 Cooperative Networks 11

1.2.3 Cognitive Radio Networks 15

1.2.4 Multiuser Relay Networks 15

1.2.5 Free Space Optical Communications 17

1.3 Dissertation Contributions 20

1.4 Dissertation Outline 23

CHAPTER 2 A BANDWIDTH EFFICIENT COGNITIVE RADIO WITH TWO-PATH AMPLIFY -AND-FORWARD RELAYING **26**

2.1 Introduction 26

2.2 Literature Review 28
2.3 System Model 31
2.4 Power Allocation for BER Minimization 35
    2.4.1 Optimal Power Allocation 37
    2.4.2 Suboptimal Power Allocation 38
2.5 Power Allocation for Rate Maximization 39
2.6 Scenario I: Physical Layer Security under SU Jamming 39
2.7 Scenario II: Physical Layer Security Scheme under Secondary User Transmission Awareness 43
2.8 Complexity Analysis 47
2.9 Numerical Results 48
2.10 Conclusion 55
2.11 List of Publications 57

CHAPTER 3 BANDWIDTH EFFICIENT SCHEMES FOR COOPERATIVE TWO-WAY COGNITIVE RELAYING NETWORKS 59
3.1 Introduction 59
3.2 Literature Review 61
3.3 System and Channel Models 67
    3.3.1 Multiple Access (MA) Phase 69
    3.3.2 Broadcasting (BC) Phase 70
    3.3.3 SINR Statistics of Cooperative TWR-AF Network 80
3.4 Performance Analysis 82
    3.4.1 SU Network Performance Analysis 82
    3.4.2 PU Network Performance Analysis with All Participant (AP) Scheme 85
    3.4.3 PU Network Performance Analysis with RS Scheme 89
    3.4.4 PU Network Performance Analysis with RE Scheme 93
3.5 Power Allocation for SEP Minimization 97

3.5.1 AP Scheme 97
3.5.2 RS Scheme 98
3.5.3 RE Scheme 99
3.6 Power Allocation for SUM Rate Maximization 100
3.6.1 AP Scheme 101
3.6.2 RS Scheme 102
3.6.3 RE Scheme 103
3.7 Physical Layer Security Approach 104
3.7.1 Scenario I: Cooperative Beamforming (CB) 104
3.7.2 Scenario II: Relay and Jamming (R-J) 107
3.8 Numerical Results 109
3.9 Conclusion 118
3.10 List of Publications 119

CHAPTER 4 MULTIUSER SIMO MIXED RF/FSO RELAY NETWORKS 124

4.1 Introduction 124
4.2 Literature Review 126
4.3 System and Channel Models 134
4.3.1 System Model 135
4.3.2 Channel Model 138
4.4 Performance Analysis 139
4.4.1 Outage Probability 139
4.4.2 Asymptotic Outage Probability 142
4.4.3 Average Symbol Error Probability 146
4.4.4 Ergodic Channel Capacity 147
4.4.5 Power Allocation 149
4.5 Physical Layer Security Approach 152
4.5.1 Security Analysis 152

4.5.2 Cooperative Jamming Model for Enhancing Physical Layer Security . . . 159
4.6 Numerical Results . . . 166
4.7 Conclusion . . . 177
4.8 List of Publications . . . 179

CHAPTER 5 MULTIUSER MIXED RF/FSO RELAY NETWORKS IN THE PRESENCE OF RF INTERFERENCE 181
5.1 Introduction . . . 181
5.2 Literature Review . . . 183
5.3 System and Channel Models . . . 189
  5.3.1 System Model . . . 190
  5.3.2 Channel Model . . . 193
5.4 Performance Analysis . . . 194
  5.4.1 Exact Outage Probability . . . 194
  5.4.2 Asymptotic Outage Probability . . . 196
  5.4.3 Power Allocation . . . 201
5.5 Physical Layer Security Approach . . . 203
  5.5.1 Security Analysis . . . 204
  5.5.2 Cooperative Jamming Model for Enhancing Physical Layer Security . . . 208
5.6 Simulation and Numerical Results . . . 213
5.7 Conclusion . . . 224
5.8 List of Publications . . . 226

CHAPTER 6 CONCLUSIONS AND FUTURE RESEARCH 227
6.1 Summary of Contributions . . . 227
6.2 Future Research . . . 231
6.3 List of Publications . . . 232

APPENDICES 235

CHAPTER A APPENDIX FOR CHAPTER 2 **236**

A.1 Proof $\mathbf{H}_{\mathsf{D}}$ is a full rank matrix 236

BIBLIOGRAPHY **240**

VITAE **260**

LIST OF FIGURES

2.1 Cognitive radio network with two-path AF relaying scheme. . . . 32

2.2 Cooperative cognitive radio network with two-path AF relaying scheme with multiple passive eavesdroppers. 40

2.3 BER performance comparison between FIC algorithm and the proposed algorithm using (ICD/MLD) in Rayleigh fading channels. . 49

2.4 BER performance of PU and SU employing different power allocation criteria (solid line: simulation, dashed line: analytical). . . . 50

2.5 Comparison in terms of achievable average rate between the proposed model and the two-path FIC scheme for different scenarios.(solid line: with direct link, dashed line: without direct link). . 51

2.6 Secrecy rate of scenario I of the proposed model with multiple eavesdroppers. 52

2.7 A comparison between scenario I and scenario II of the proposed model in terms of secrecy rate against the number of eavesdroppers M with SNR = 10 dB (solid line: with direct link, dashed line: with no direct link). 53

2.8 Secrecy rate for scenario II of the proposed model with multiple eavesdroppers and different values of eavesdropper channel variance σ_{g}^2. 54

2.9 A comparison between scenario I and scenario II of the proposed model in terms of secrecy outage probability against M. 55

2.10 BER performance of scenario I of the proposed model with different number of eavesdroppers. 56

2.11 BER performance of scenario II of the proposed model with single eavesdropper node and different values of eavesdropper channel variance σ_{g}^2. 57

3.1 Multiple access phase of the proposed cooperative TWR-AF relaying scheme. 68
3.2 Broadcasting phase of the proposed cooperative TWR-AF relaying scheme. 70
3.3 ASEP comparison between the proposed cooperative cognitive TWR-AF schemes and the conventional one. 110
3.4 The SEP performance of SU network for different SU transmission power $P_A = \mathcal{P} = 0.33P_{\mathsf{s}}$ and $0.75P_{\mathsf{s}}$. 111
3.5 Outage probability comparison between the proposed cooperative cognitive TWR-AF schemes and the conventional TWR-AF model. 112
3.6 PU network achievable rate comparison between the proposed cooperative cognitive TWR-AF schemes and the conventional TWR-AF scheme. 113
3.7 The PU SEP performance of the proposed AP scheme against the amplification factor λ_{ap} for different SER sum ratio, i.e., $m_1 : m_2 = 1 : 1$ and $1 : 5$ at SNR = 30 dB. 114
3.8 The PU SEP performances of the proposed RS and RE schemes against the amplification factor $\lambda_{\mathsf{rs}} = \lambda_{\mathsf{re}} = \lambda$ for different SER sum ratio, i.e., $m_1 : m_2 = 1 : 1$ and $1 : 5$ at SNR = 30 dB. 115
3.9 PU network achievable rate of the proposed AP scheme against the amplification factor λ_{ap} for SNR $= 15, 20$ and 25 dB. 120
3.10 PU network achievable rate of the proposed RE and RS schemes against the amplification factor $\lambda_{\mathsf{rs}} = \lambda_{\mathsf{re}} = \lambda$ for SNR $= 15, 20$ and 25 dB. 120
3.11 Secrecy sum rate of the proposed CB scenario for different values of optimal amplification factor $\lambda_{\mathsf{ap}}^{\mathrm{opt}} = 0.5P_{\mathsf{s}}, 0.75P_{\mathsf{s}}$ and $0.95P_{\mathsf{s}}$. . 121

3.12 Secrecy sum rate of the proposed RJ scenario for different values of required amplification factor $\lambda_Q = 0.5\lambda_{\mathsf{rs}}^{\text{opt}}, 0.7\lambda_{\mathsf{rs}}^{\text{opt}}$ and $0.9\lambda_{\mathsf{rs}}^{\text{opt}}$. . 121
3.13 SRT analysis comparison between the proposed AP scheme with CB technique and the conventional TWR-AF. 122
3.14 SRT analysis for the proposed RS scheme with RJ technique with different required amplification factor $\lambda_Q = 0.99\lambda_{\mathsf{rs}}^{\text{opt}}, 0.97\lambda_{\mathsf{rs}}^{\text{opt}}$ and $0.95\lambda_{\mathsf{rs}}^{\text{opt}}$. 122
3.15 Comparison between the line search method and the proposed power allocation solution in (3.84) in terms of the optimal solutions ($\lambda_{\mathsf{ap}}^{\text{opt}}$) for AP scheme. 123
3.16 Comparison between the line search method and the proposed power allocation solution in (3.84) in terms of the optimal solutions ($\lambda_{\mathsf{rs}}^{\text{opt}}$) for RS scheme. 123

4.1 Dual-hop MU-SIMO mixed RF/FSO relay network with opportunistic scheduling and multiple antenna eavesdropper. 134
4.2 Outage probabilities for both MRC and SC schemes versus SNR of the considered system with opportunistic scheduling and different number of users K. 167
4.3 Outage probabilities for both MRC and SC schemes versus SNR of the considered system with opportunistic scheduling and different values of Nakagami-m parameter m_u. 168
4.4 Average symbol error probabilities for both MRC and SC schemes versus SNR of the considered system with opportunistic scheduling and different atmospheric turbulence conditions. 169
4.5 Average symbol error probabilities for both MRC and SC schemes versus SNR of the considered system with opportunistic scheduling and different types of optical detection schemes r. 170

4.6 Ergodic capacities for both MRC and SC schemes versus SNR of the considered system with opportunistic scheduling and different values of pointing error ζ. 171

4.7 Ergodic capacities for both MRC and SC schemes versus SNR of the considered system with opportunistic scheduling and different values of N_{r}. 172

4.8 Optimal power allocation for MRC scheme versus number of users K for different atmospheric turbulence conditions α and β. 173

4.9 Intercept probability of MRC scheme of the considered system with opportunistic scheduling and different number of eavesdropper antennas N_e. 174

4.10 SRT analysis for MRC scheme of the considered system with opportunistic scheduling and different number of users K. 175

4.11 Intercept Probability for MRC scheme versus number relay antennas N_{r} of the considered system with opportunistic scheduling and different values of outage probability P_{out}. 176

4.12 The impact of optimal power allocation on the secrecy performance for MRC scheme of the considered system with opportunistic scheduling and different number of relay antennas N_{r}. 177

4.13 The impact of optimal power allocation on the SRT analysis for SC scheme of the considered system with opportunistic scheduling and different atmospheric turbulence conditions α and β. 178

4.14 Intercept probability for MRC scheme of the considered system with opportunistic scheduling with different value of jamming power P_{J}. 179

4.15 CJ model intercept probability for SC scheme versus SNR of the considered system with opportunistic scheduling and different values of outage probability P_{out}. 180

5.1 Dual-hop MU-SIMO mixed RF/FSO relay network with opportunistic scheduling and multi-antenna eavesdropper. 190

5.2 Outage probability versus SNR of the considered system with opportunistic scheduling and different number of users K at weak atmospheric turbulence conditions $\alpha = 10.764, \beta = 9.247$. 214

5.3 Outage probability versus SNR of the considered system with opportunistic scheduling and different number of users K at strong atmospheric turbulence conditions $\alpha = 5.084, \beta = 3.416$. 215

5.4 Outage probability versus SNR of the considered system with opportunistic scheduling and different number of co-channel interferers I_{R} at the relay in different atmospheric turbulence conditions α and β. 216

5.5 Outage probability versus SNR of the considered system with opportunistic scheduling and different values of Nakagami-m parameters m_k and $m_{I_{\mathrm{R}}}$ in different atmospheric turbulence conditions α and β. 217

5.6 Optimal power allocation for the considered system with opportunistic scheduling versus number of users K for different atmospheric turbulence conditions α and β. 218

5.7 Optimal power allocation for the considered system with opportunistic scheduling versus SNR for different values of I_{R}. 219

5.8 Optimal power allocation for the considered system with opportunistic scheduling versus SNR for different atmospheric turbulence conditions α and β. 220

5.9 Intercept probability versus SNR of of the considered system with opportunistic scheduling and power allocation for different number of users K. 221

5.10 Intercept probability versus SNR of the considered system with opportunistic scheduling and power allocation for different values of I_{R}. 222

5.11 Intercept probability versus SNR of the considered system with opportunistic scheduling and power allocation for different number of co-channel interferers I_{E} at the eavesdropper. 223
5.12 The impact of different CJ scenarios on the SRT analysis of the considered system with opportunistic scheduling. 224
5.13 The impact of different AP CJ scenario on the SRT analysis of the considered system with opportunistic scheduling for different atmospheric turbulence conditions. 225

LIST OF ACRONYMS

AF	Amplify-and-Forward
AP	All Participant
AN	Artificial Noise
AWGN	Additive White Gaussian Noise
BC	Broadcasting
BER	Bit Error Rate
CB	Cooperative Beamforming
CF	Compress-and-Forward
CJ	Cooperative Jamming
CR	Cognitive Radio
CCI	Co-Channel Interference
CDF	Cumulative Distribution Function
CRN	Cognitive Relay Networks
CSI	Channel-State Information
DF	Decode-and-Forward
DT	Direct Transmission
e2e	End-to-End

FIC	Full Interference Cancellation
FSO	Free Space Optics
ICD	Inverse Channel Detector
i.i.d.	Independent and Identical Distribution
i.ni.d.	Independent and Non-Identical Distribution
IRI	Inter-Relay Interference
JMLD	Joint Maximum Likelihood Detection
LOS	Line-of-Sight
LPD	Low Probability of Detection
LPI	Low Probability of Intercept
MA	Multiple Access
MU	Multi-User
MLD	Maximum Likelihood Detection
MRC	Maximal-Ratio Combining
MRN	Multiuser Relay Networks
MRT	Maximum-Ratio Transmission
MIMO	Multiple Input Multiple Output
OSTBC	Orthogonal Space Time Block Code
PU	Primary User
pdf	Probability Density Function
PHY	Physical Layer
PIC	Partial Interference Cancellation
RE	Relay Elimination

RF	Radio Frequency
RS	Relay Selection
R-J	Relay-and-Jam
SC	Selection Combining
SU	Secondary User
SEP	Symbol Error Probability
SER	Symbol Error Rate
SNR	Signal-to-Noise Ratio
SRT	Security Reliability Trade-off
SINR	Signal-to-Interference Plus Noise Ratio
SIMO	Single Input Multiple Output
TAS	Transmit Antenna Selection
TWR	Two-Way Relaying

THESIS ABSTRACT

NAME:	Ahmed Hassan Abd El-Malek
TITLE OF STUDY:	Design and Analysis of New Cooperative Relaying Networks for Enhancing Physical Layer Security
MAJOR FIELD:	Electrical Engineering
DATE OF DEGREE:	December 2015

The advantages of wireless communication networks such as mobility, flexibility and installation simplicity nominated these networks to be a backbone of most of the people business and social activities. Despite these advantages and due to the nature of the wireless medium, one of the major problems in wireless networks is the security of the shared information over the network. As wireless communication networks are rapidly included in many daily activities resulting in a growing security concern, this security interest inspired researchers in the area of wireless network security to proposed new communication models with high data transmission security and to present a recent new security approach known as physical layer security approach.

Therefore, free space optical communications are presented as an effective se-

cure means of transferring data at high rates over short distances. Free space optical communication offers the potential of broadband communication capacity, as they operate on unlicensed optical beams, and therefore represent a cost-effective alternative and/or complement to their radio frequency counterparts.

Moreover, physical layer security is increasingly recognized as a potentially powerful means of ensuring secure communication over publicly accessible wireless networks. The main concept of physical layer security is to ensure that the wiretap channel of an eavesdropper is a degraded version of the main authorised channel. This increases the security of the wireless networks and that is highly applicable to emerging wireless systems.

In the area of cooperative cognitive radio, we propose two new bandwidth efficient cooperative cognitive radio systems which enable cooperation between the primary user system and the secondary user system. The goals of these newly proposed systems are to enhance the wireless network bandwidth efficiency, minimize the total error probability, and maximize the total sum-rate of the system. Then, we propose new cooperative scenarios to enhance the physical layer security performance against eavesdropping attacks. The results show that the proposed models enhance the spectral efficiency, improve the system error performance and increase the total achievable sum rate. In addition, the proposed models enhance the secrecy performance of primary networks against eavesdropping attacks.

In the area of mixed RF/FSO networks, we investigate performance of multiuser single-input-multiple-output mixed RF/FSO systems for different diversity *combining techniques employed by a multi-antenna relay node. Then, we propose power allocation model with the help cooperative jamming technique to enhance the physical layer security of the considered systems by utilizing the selected worst user based on the authorized relay selection. Finally, we study the impact of non-identical co-channel interference signals on the security reliability trade-off analysis of multiuser mixed RF/FSO networks. Then, we employ the cooperative jamming technique to enhance the system secrecy performance against eavesdropping attack. The results show that the proposed mixed RF/FSO networks increase the ergodic capacity and enhances the secrecy performance against eavesdropping attacks.*

ملخّص

منذ نهاية القرن الماضي، اعتبرت شبكات الإتصالات اللاسلكية واحدة من أفضل أدوات تحسين الإنتاجية و الإبداع. قدمت هذة الشبكات مجموعة من المزايا أهمها الحركية و المرونة وسهولة التركيب والاستخدام مما رشّحها لتصبح عموداً فقريّا لمعظم الأنشطة الرسمية و الإجتماعية. و لكن و على الرغم من كل هذه المزايا ، و نظرا لطبيعة قنوات الإتصال اللاسلكية ، تظلّ حماية المعلومات المتداولة عبر شبكات الإتصالات اللاسلكية واحدة من المشاكل الرئيسة لهذه الشبكات. و نتيجة لإندماج شبكات الإتصالات اللاسلكية سريعاً فى مختلف الأنشطة اليومية ، زاد القلق من قدرة هذه الشبكات على حماية المعلومات. هذا القلق المتزايد في الآونة الأخيرة ألهم الباحثين فى مجال حماية شبكات الإتصالات اللاسلكية لتقديم نهج أمني جديد يعرف بأمن الطبقة المادية.(Physical layer)

تم تعريف أمن الطبقة المادية على نحو متزايد على أنه وسيلة قوية لضمان إتصال آمن عبر شبكات الإتصالات اللاسلكية فى ظلّ تزايد الشكوك حول قدرة نظم التشفير التقليدية على توفير الحماية اللازمة نتيجة للتحسن الكبير فى أداء الحوسبة. يقوم مفهوم الحماية فى هذا النهج الجديد على ضمان أنّ قناة التنّصت هى نسخة متدهورة من القناة الرئيسة مما يزيد من أمن الشبكات اللاسلكية. مما يجعل هذا النهج الجديد فى الحماية ملائما جداً لشبكات الاتصالات اللاسلكية المدمجة الحديثة. نتج عن ذلك تقديم أطروحة عمل تهدف إلى تصميم و دراسة كيفية حماية أنظمة الإتصال الإدراكية اللاسلكية و التي يتم فيها تقاسم الطيف اللاسلكي بين نوعين من المستخدمين هما المستخدم الرئيسي و المستخدم الثانوي. ستنفّذ هذه الدراسة على نوعين من الإتصالات الإدراكية مقسمة على حسب قدرة المستخدمين (الرئيسي و الثانوي) على التعاون.

تشجّع شبكات الإتصال الإدراكية التعاونية التعاون بين المستخدم الرئيسي والمستخدم الثانوي. المزايا الرئيسية لهذا التعاون تتمثل في زيادة معدل البيانات الإجمالي للنظام ، و رفع كفاءة الاشغال في النطاق الترددي وتحسين معدل السريّة. سيتم دراسة تحسين الأمن من خلال التعاون فى الطبقة المادية عبر قنوات خبوْ مختلفة ، و حيث تكون نقاط الإتصال المرخصة مجهزة بهوائي واحد أو أكثر و في وجود متنصت واحد أو أكثر مجهز بهوائي واحد أو أكثر تحت ظروف التشغيل التي ثبت في الماضي أن أنها تؤثر على أمن الشبكة.

من ناحية أخرى، تعتبر الإتصالات الضوئية أو البصرية في الفراغ وسيلة فعّالة لنقل المعلومات بسرعات عالية و لمسافات قصيرة. لقد تمّ تقديم هذا النوع من الإتصالات من أجل التغلّب على مشكلة "الميل الأخير" في الشبكات اللاسلكية و التي تتمثّل بالإنخفاض في سرعة نقل المعلومات للمستخدمين كما يحدث في بعض أنظمة الإتصالات بسبب ظاهرة التلاشي – الناتجة عن وصول الإشارة للمستقبل من خلال عدّة مسارات و بأطوار مختلفة و التي تؤدّي إلى ضرر كبير بجودة الإشارة – على سبيل المثال. في مثل هذه الأنظمة ، يتم نقل المعلومات أو الإشارات بين مرسل ومستقبل ضوئيان موجودان ، مثلاً ، على سطح بنايتين متقابلتين على بعد بضع مئات من الأمتار. هذا البعد بين المرسل و المستقبل يمكن أن يشكّل تحدٍّ فعليّ في عمليّة نقل الإشارات في أنظمة الإتصالات العاديّة و لكن ليس بالنسبة لمثيلاتها من أنظمة الإتصال الضوئي في الفراغ.

بصفتها قادرة على نقل المعلومات بسرعة الإتصالات ذات الطيف العريض (و التي بدورها تقود لنقل معلومات بسرعات عالية جداً) ، و حيث أنّها تعمل على ترددات طيف غير مُرَخّصة ، تمثّل الإتصالات الضوئية في الفراغ بديل أو مكمّل قليل التكلفة لإتصالات التردد الراديوي. و لأنّ الموجات الضوئيّة غير مملوكة لشركات تزويد الخدمة ، إستخدامها مجّاني و بدون لكميّة المعلومات المنقولة. بالإضافة إلى ذلك ، ميّزاتها مثل الأمن المرتفع ، المرونة ، سرعة الإنتشار ، و عدم تعرّضها للتداخل كما في إنظمة التردد الراديوي ، جعلت منها مرغوبة الإستخدام في حالات الطوارىء و التطبيقات العسكرية. إلى جانب الإتصالات الضوئية في الفراغ ، تمّ تقديم تقنية أو شبكات المرحّلات للتغلّب على مشكلة التلاشي في شبكات الإتصال اللاسلكية من خلال تزويد النظام بنسخ متعدّدة من الإشارات المُرسلة بشكل مدروس. بالإضافة إلى ذلك ، تمتاز شبكات المرحّلات بقدرتها على زيادة مدى وصول

الإشارة ، تحسينها لكفاءة إستخدام القدرة ، تحسينها لسعة النظام. وسيلة أخرى لتحسين آداء أنظمة الإتصالات اللاسلكية هي تنظيم وصول المستخدمين لمصادر النظام و عملية نقل معلوماتهم.

نقدّم في هذا البحث بعض السيناريوهات الجديدة و الفعّالة لشبكات الإتصال الإدراكية التعاونية وكذلك لشبكات المرحّلات المدمجة من نوع تردد راديوي/تردد إتصال بصري في الفراغ وذلك من أجل دراسة أمن الطبقة المادية وتحسين الأداء المقدم من هذه الشبكات لتعزيز الأداء الأمنى. حيث يقدم البحث فى البداية طرق جديدة ومبتكرة للتعاون بين المستخدم الأساسى و الثانوى من أجل تعزيز أمن الطبقة المادية مع السماح للمستخدم الثانوى باستخدام الطيف الترددى فى نفس الوقت. ومن ثم يتجه البحث لدراسة مدى سرية المعلومات التى يمكن أن تقدمها شبكات المرحّلات المدمجة من نوع تردد راديوي/تردد إتصال بصري في الفراغ وذلك من خلال دراسة أداء هذه الشبكات فى حالة التعرض لهجوم من متنصت واحد أو عدة متنصيتين.

ولقد أثبتت الدراسة أنه يمكت تحسين معامل السرية و الأمان فى الطبقة المادية باستخدام تلك النماذج المبتكرة فى البحث. حيث أشارت المعادلات والمحاكاة باستخدام الحاسوب تحسن فى أداء الشبكات المقترحة من وجهة نظر الفاعلية و الأمان.

CHAPTER 1

INTRODUCTION

1.1 Motivation

Although wireless communication networks play an essential role in many daily life activities nowadays, their capability to provide a secure data sharing is still questionable. Because of the broadcasting characteristics of wireless communication networks, the security issues against jamming and eavesdropping attacks are still open topics for research and development. Additionally, the exponential increase in wireless network users demand with the frequency spectrum limitations leads to propose new wireless networks schemes. These new schemes allow cooperation, spectrum sharing between different network users and mixed transmission technologies to fulfill customer needs. These merged networks with different subscribers increase the concerns about wireless network security.

Inspired by what is mentioned above, a new secrecy approach denoted by physical layer (PHY) security has been recently presented [1]. The concept of the PHY security states that a secure transmission can be guaranteed as long as the wiretap channel is worse than the main channel. Hence, this approach aims to help the authorized users to securely transmit their data in the presence of eavesdroppers by employing all available network resources to assure that the wiretap channel is of sufficiently a poor quality. In order to establish a secure wireless transmission, the authorized users employ all available channel state information (CSI) of the main channel as well as the wiretap channel. Subsequent efforts explored the effect of different network resources such as power allocation, multiple antennas, beamforming, and artificial noise in enhancing the randomness of wireless channel to make the main channel status always better than the wiretap channel.

Due to the size limitations of mobile sets, the advantages of multiple-input-multiple-output (MIMO) such as increasing the diversity order, the coding gain and improving the network security are not fully utilized in practical wireless networks. Maximum-ratio transmission (MRT) is one of the multiple antennas techniques that has received a great attention because of its significant performance compared to other MIMO diversity techniques. The MRT technique can achieve a full diversity gain and an array gain due to the utilization of feedback information. However, the design and operation of the conventional maximal ratio combining (MRC) face many challenges, such as 1) the increase in processing complexity due to the user of multiple RF chains, 2) the amplification in power consumption due to the use of all deployed antennas, and 3) the sensitivity to erroneous estimation of CSI.

Therefore, the use of transmit antenna selection (TAS) can be a suitable low-complexity scheme, that can achieve the same diversity gain, and relatively less array gain. Moreover, the cooperative networks were proposed to overcome these size limitations and construct virtual MIMO networks that enable wireless networks to gain all the benefits that are mentioned earlier. The main concept of cooperative networks is that having relays in wireless networks results in enhancing the network performance and gaining the MIMO advantages. In addition, the existence of these friendly relays encourages employing them in more efficient PHY security scenarios that enhance wireless network security against eavesdropping. The relay nodes take place in many PHY security schemes in which they might do their original role improving the received signal at the intended receivers, or they might work differently as friendly jammers or cooperative beamformers. Joint beamforming and artificial noise generating relays have been studied recently using the art of optimization and game theory methods.

One of the recent challenges facing network security is the spectrum sharing networks known as cognitive radio (CR) networks. CR networks are presented as a promising solution to the limited frequency spectrum problem. They divide the users into two main categories: primary users (PUs) and secondary users (SUs). Based on that, the PU network might allow the SU network to share the spectrum under certain interference limitations, or the SU network might sense the spectrum to find a free time-slot for its transmission. To enhance CR networks performance, the concept of cooperative networks is implemented to gain their previously mentioned advantages. These cooperative CR networks create security challenges that emphasize the importance of having the PHY security scenarios in such networks. The concept of CR changed the nature of how relay nodes are arranged. Instead of using passive relay nodes, which only apply a certain protocol on the received data, CR employs SU nodes with a dual mission relaying PU data and transmitting their data. In contrast, instead of sending a non-informative jamming signal to jam the eavesdropper nodes, the SU transmitter can send its data, with this jamming signal preventing access by an eavesdropper.

Recently, free space optical (FSO) communications provide an efficient solution in overcoming the problem of last mile communication in wireless communication systems. In particular, the communicating nodes employ optical or laser beams to send the information data through the free space instead of radio frequency (RF) channels. FSO systems have enormous advantages over the existing wireless networks such as: lower interference footprint, low cost deployment, and higher bandwidth. One of the most important advantages of FSO systems is their ability to provide a high secure transmission because of the concentrated and narrow laser beam between the optical transmitter and receiver which makes the ability for intercepting the optical transmission very limited. Moreover, the specific nature of light beams limits the intercept ability of any nearby eavesdroppers which could try to overhear the communication between the transmitter and receiver. A good probability of interception may exist when a part of the beam radiation is reflected by small particles. This may make the communication beam detectable by the eavesdropper which is not in the line-of-sight (LOS) of the communicating peers. However, the amount of power received by the eavesdropper will be considerably smaller, compared to an equivalent RF scenario.

Although the FSO communications provide numerous advantages over other RF wireless counterparts, the problems of atmospheric turbulence, and misalignment between the optical pairs limit the coverage area to be less than a kilometer. Recently, the new mixed RF/FSO relay networks have provided a successful solution for the coverage limitation problems of the FSO systems as well as it reduce the need for the very limited RF resources. The operations of mixed RF/FSO relay networks take place over two links which are the RF link and the FSO link.

Based on the secrecy advantages of the FSO link over the RF link, the mixed RF/FSO networks enhances the network secrecy performance against eavesdroppers compared to their wireless networks counterparts. This secrecy advantages besides the other aforementioned advantages encourage us to study the reliability analysis of such networks as well as their secrecy performance in different networks setups and for different eavesdropping attack strategies.

Motivated by the aforementioned discussion, we propose to enhance PHY security in wireless networks in two different models, namely, cooperative CR models and mixed RF/FSO models in the presence of multiple passive eavesdroppers. Then, several new CR models are proposed in this work. In cooperative CR models, the SU network cooperates with the PU network via suitable relaying protocol to improve the bandwidth efficiency and as a result, the secrecy performance. Whereas, in mixed RF/FSO relay networks, the security advantage of FSO communication is employed in enhancing PHY security. In these mixed networks, the communications are held over two hops, namely, RF hop and FSO hop. First, we study the reliability performance of the new proposed networks in terms of the outage probability, the error probability, the achievable rate , and the ergodic capacity. Then, we investigate the secrecy performance of these proposed networks against different eavesdropping attacks in terms of the secrecy capacity, and the intercept probability. Finally, we provide the security reliability trade-off analysis of the proposed models.

The rest of this chapter is organized as follows. Section 1.2 reviews the literature on the area of PHY security for different wireless network models. Section 1.3 explains the dissertation contributions. Finally, the dissertation outline is given in Section 1.4.

1.2 Background

PHY security has been considered as a necessary strategy to increase secrecy in wireless communication networks considering the broadcast nature of radio frequency channels which causes security susceptibilities [1]. The state of art behind PHY security is to employ the spatial and temporal characteristics of wireless medium for enhancing networks security [2]. Any public wireless communication system can be divided into authorized and unauthorized nodes. Due to the broadcasting nature of wireless transmission, an authorized (legitimate) communication may suffer from jamming where unauthorized transmitters try to degrade the signal at the front end of the intended receiver, or, on the other hand, they may suffer from eavesdroppers which are unauthorized receivers (wire-trappers) trying to attack the transmission and extract information. An early study on this research topic showed that, in wiretap channels, a perfect secrecy can be achieved when the main channel conditions is better than the wiretap channel conditions [3]. The basic concept about PHY security is to use the available amount of CSI and noise to mitigate the amount of information that the eavesdropper can extract. The difficulty of PHY security designs depends on the amount of information available for both legitimate (authorized) and eavesdropper systems about each other. This information includes the transmission protocol, the transmission power and CSI, the active or passive eavesdropper, the number of eavesdroppers and the number of antennas equipped in each node [4, 5]. The goal of PHY security is to provide the authorized system with a secure wireless communication without any need for using an encryption key. The literature showed that there exist some codes for the wiretap channel that guarantee both low error probabilities and a certain degree of security [6, 2, 7, 8, 9, 10].

The work presented by Wyner for single antenna wiretapped channel was generalized in [11], where authors derived a single letter characterization of the achievable rates for discrete memoryless channels of two receiver broadcast. The type II wiretap channel was presented in [12] in which authors showed that a secure communication can be guaranteed with a characterization value which represents the subset of the legitimate user coded bits the eavesdropper can access a noiseless main communication channel.

Wiretap channels under fading environment have been studied in [6], where the authors obtained the outage probability then defined the secrecy capacity in terms of outage probability. A complete characterization of the maximum transmission rate at which the eavesdropper can not decode the data was provided. The results showed that a perfect secure transmission can be possible even if the wiretap channel has an average signal-to-noise-ratio (SNR) higher than the main channel link. For the same average SNR, the outage secrecy capacity performance of a wireless channel could be worse than the secrecy capacity of a Gaussian wiretap channel. Under the assumption of slow fading wiretap channel, the authors in [13, 14] derived the secrecy capacity with complete CSI. The results showed that the secrecy capacity can be achievable with Gaussian random codes and optimal power adaptation. The work was extended in [15], in which the authors assumed fast Rayleigh fading over wiretap channel with AWGN. The results showed that a positive secrecy capacity can be obtained with Gaussian random code, artificial noise (AN) injection, and power allocation. Same results were valid even when the main channel gain is arbitrarily worse than the wiretapper's average channel gain. Authors in [16] considered the case where no or partial side information about the eavesdropper CSI is available at the legitimate nodes denoted by compound wiretap channels.

1.2.1 MIMO Systems

Enhancing PHY security of wireless channels by using the spatial-temporal characteristics of MIMO systems was investigated in [17]. The authors designed a complete CSI transmission techniques which can achieve either a low probability of detection, or a low probability of intercept with a different amount of CSI available at an eavesdropper. The wiretap channel with MIMO technology was examined in [18] where authors obtained the secrecy capacity for a model which includes legitimate nodes with double antennas and a single antenna eavesdropper. The results showed that using the beamforming technique can be optimal for this channel with no preprocessing of information. The work in [19] considered the problem of computing the perfect secure capacity of multiple antenna channels based on a generalization of the wiretap channel to a MIMO broadcast wiretap channel.

The concept of using AN technique was proposed in [20, 21]. A multiple antennas transmitter or a single antenna transmitter with amplify repeaters tried to degrade the wiretap channel by generating an AN at the same time they tried to minimize the impact of this AN at the legitimate destination. The AN technique was used in [22, 23] to aid the MIMO transmitter beamforming scheme. An additional secrecy capacity gain can be achieved by jointly optimizing the AN transmit covariance matrix with the MIMO beamforming covariance matrix. The optimal power allocation based on MIMO beamforming, precoding and AN generation was studied in [24] for cooperative and non-cooperative networks. The authors in [25] used an optimal power allocation strategy with beamforming and AN techniques in multiple-input-single-output (MISO) network in order to define a protected zone around the legitimate transmitter and achieve a high probability of secrecy. The works in [26, 27, 28] studied the design of robust beamforming techniques with the aid of AN varies according to the amount of CSI available for both authorized and unauthorized networks as well as the state of the eavesdropper (i.e., active or passive).

The perfect secrecy capacity was proved to be the difference between the two mutual information, the one of the legitimate user minus the one of the eavesdropper. For the practical case of passive eavesdropper, the work in [9] studied the secrecy performance when MRC scheme was employed at both authorized and unauthorized nodes. The previous work was extended in [8] in which the secrecy outage probability was investigated when the eavesdropper node applies both MRC and selection combining (SC) schemes.

The works in [29, 30] derived the secrecy performance metrics of TAS scheme under different fading channels. The authors in [29] analyzed the PHY security of multiple transmitter antennas communication system using TAS criterion with single antenna destination in the presence of multi-antennas eavesdropper node. The secrecy outage probability were investigated and closed-form expressions were derived. Results showed that the authorized node equipped with multiple antennas could enhance the PHY security performance. In [31, 30], the PHY security performance of TAS with different diversity combining methods were studied.

Closed-form expressions for the exact and the asymptotic secrecy outage probability were derived and they demonstrated that the maximum secrecy outage diversity gain could be achieved.

The work proposed in [32] studied the secrecy performance of the wiretap channel with TAS at the transmitter and MRC at the receiver and eavesdropper in the presence of multiple correlated antennas. Therefore, exact and asymptotic outage probabilities were derived in closed-form expressions. It was shown that when the main channel has low SNR values, the system is more secure if the antenna correlation at the eavesdroppers is higher than that at the authorized destination. Whereas, at medium to high SNR values, increasing the antenna correlation at the receiver has a remarkable effect on the secrecy performance than the correlation at the eavesdropper.

1.2.2 Cooperative Networks

Cooperative communications where the main communication nodes are served by relays has gained high attention in PHY security research. Due to the different roles that these relay nodes can play in order to increase the main network secrecy capacity, cooperative communications have become a very attractive topic for research [33]. The secrecy capacity in the presence of a single eavesdropper and with the help of a relay node was studied in [34], where a secrecy performance comparison was held between different relaying protocols (i.e., Amplify-and-Forward (AF), decode-and-forward (DF), and compress-and-forward (CF)) and direct transmission (DT). The works in [35] examined the two main relaying protocols, namely, DF and AF when there are more than one relay in cooperating with the legitimate system. The main goal was to maximize the secrecy capacity by choosing the optimal beamforming weight at each relay. A secrecy rate performance comparison between the cooperative beam-forming and cooperative jamming was introduced. Due to noise amplification at AF relays, the secure capacity maximization problem is very difficult to be optimally solved. Authors in [36] proposed a new suboptimal beamforming scheme by recasting the maximization problem as a two level optimization problem using semidefinite relaxation and one-dimensional search techniques in the presence of multiple eavesdroppers. In [37], where a new PHY security scheme was proposed in which a relay out of two relays is opportunistically selected to enhance the secrecy performance against eavesdropping attack. In particular, one DF relay is selected to assist the source in delivering its data to the receiver. At the same time, the second relay jams the eavesdropper nodes. This work was extended in [38], authors proposed a new scheme in which the destination is jamming the eavesdropper with no additional interference at the existing relays. Then, the selected relay retransmits the decoded source signal. Simultaneously, the source cooperates with a particular relay to jam the eavesdropper without affecting the authorized transmission at the destination. The results showed that although the eavesdropper had a complete CSI, the system was able to achieve a non-zero secrecy capacity.

The works in [39, 40] proposed a new cooperative jamming (CJ) technique with noise forwarding strategy known as “Deaf cooperation” in which the full duplex relay transmits dummy codewords in order to confuse the eavesdropper nodes independently. An Optimal power solution was obtained and the achievable secrecy rate was derived. The results showed that even the CSI of eavesdropper channel is not available, the proposed algorithm can achieve a non-zero secrecy capacity. The cooperative secure transmission with beamforming aid in the presence of multiple eavesdropper with AF relay was introduced in [36]. The work proposed to beamforming schemes that are secrecy rate maximization beamforming and null-space beamforming. The authors in [41] investigated the multiple antennas AF relay - eavesdropper channel with imperfect CSI. Beamforming technique was used by the relay in different wiretap channel models. A comparison between optimal rank-1, match-and-forward and zero-forcing beamformers are held. Results show that the optimal zero-forcing beamformer may outperforms the match-and-forward beamformer over Rician fading while they have the same performance for the deterministic uncertainty channels.

The CJ technique with a set of relays was investigated in [42], where a number of AF relays are divided optimally between AF relays and cooperative jammers with imperfect CSI. Optimal weights for relays beamforming were obtained. Another joint optimization problem including the beamforming weights and the power of the jammers was solved. The problem of relay selection was investigated in [43] where multiple DF relays help the legitimate system against multiple eavesdropping attack. Closed-form expression for the intercept probability was derived for different transmission schemes. The results showed that exploiting multiple relays in cooperation networks improves the PHY security. The work was generalized in [44], where multiple AF and DF relays were considered in the presence of multiple eavesdroppers. Increasing the number of cooperative DF relays with opportunistic relay selection scheme was shown to vanish the secrecy outage probability as shown in [45].

The problem of relay nodes mobility was investigated in [46], where the multi-antenna relays were moving. Optimal positions and jamming weights for the relays were obtained and a novel decentralized relays mobility control was presented. The results showed that the consideration of relays mobility could save relays transmitting power and reduce the total number of relays needed for secure communication. The impact of limited feedback of side channel information from the intended receiver was examined in [47], while the effect of delay CSI feedback on relay selection was presented in [48].

A new scheme was proposed in [49], that considered a two hop DF relay network with a single eavesdropper. The proposed scheme used the legitimated source and destination nodes to generate an AN while they were idle. The proposed work defined two types of cooperative jamming models, namely, full CJ and partial CJ. The results showed that both models improve the system secrecy capacity but in the case of passive eavesdropper, the full CJ model outperforms the partial CJ model. In case of single hop networks, the works in [50, 51] proposed a full duplex legitimated destination node that has the ability to transmit a jamming signal and receive the secret message simultaneously.

1.2.3 Cognitive Radio Networks

CR networks provide improvements in bandwidth efficiency of wireless networks with the current fixed spectrum regulation policy by intelligently sharing the spectrum resources [52]. The work in [53] analyzed the interaction between SUs and eavesdroppers in the presence of multiple PUs. Game theoretic techniques were used to obtain the equilibrium point between the SUs and eavesdroppers in a non-cooperative game. A novel algorithm was proposed to select a secure channel which was shown to improved the secrecy capacity of SU network. The cooperation between a PU network and a SU network was discussed in [54]. The SU network helps the PU network to improve its secrecy capacity by jamming the eavesdropper within a certain power. As a reward, the PU allows for more interference from the SU network or gives the SU network a portion of the time to use it for its own transmission. The CJ and cooperation beamforming techniques were applied to cooperative CRN in [33, Ch.4], which were shown to improve the PU network secrecy capacity.

1.2.4 Multiuser Relay Networks

The performance of multiuser (MU) relays networks (MRNs) in which the system consists of a source, an AF relay and multiple destinations was investigated in [55]. Closed-form expressions for the outage probability over generalized Nakagami-m

fading channels were derived. The unbalanced hops model was studied under the effect of dissimilar per-hop fading parameters and/or dissimilar per-hop averaged faded SNRs. Because of ignoring the direct links between the source and the destinations and the half duplex nature of the relay node, the obtained diversity order and spectral efficiency were not satisfactory. The symbol error rate (SER) of the same model was studied and presented in [56]. The authors in [57] studied the opportunistic direct links in a MU cooperative network with a DF relaying. They proposed that the relaying transmission can be avoided as long as the selected direct link is sufficiently good, satisfying the spectrum efficiency requirements which improve the spectral efficiency.

All the aforementioned MU cooperative network works were under the assumption of single antenna nodes. The impact of multiple correlated antennas on the performance of MU scheduling for CSI-assisted and fixed gain AF relaying was investigated in [58]. The MRN was considered with a single source of multiple correlated antennas communicating with a selected destination node from a set of multi-destinations with a single antenna via a dual correlated antenna AF relay node. Results investigated the outage probability and SER of the considered system where closed-form expressions were derived. The work indicated that although the multiple antennas enhance the network overall performance, the correlation between antennas degrades the performance. Diversity order and ergodic capacity were analyzed. The work has been extended in [59] in which MRN with multiple correlated antennas considered. The work derived closed-form expressions for the system outage probability, SER and the ergodic capacity. The work findings showed that increasing of the correlation harms the system performance but for point-to-multipoint links, the increase of antenna correlation was shown to provide capacity improvement.

Recently, the work in [60] studied the performance of MU and multi-relay CRNs, in which multiple SU relays help the SU source to transmit its data to multiple SU destinations, which existed closed to a single PU destination. Closed-form expressions for outage probabilities were derived for both AF and DF relaying schemes. The asymptotic analysis showed that the diversity order of the system is not affected by the interference constraint and equals to the sum of the relay and destination nodes.

1.2.5 Free Space Optical Communications

With the rapid growth in the number of users of wireless systems and huge demand on the amount of data rates such systems are expected to carry, FSO communication has arisen as an effective means of transferring data at high rates over short distances [61]. The FSO communications transmit the data between an optical transmitter and a receiver, which can be separated by a less than one kilometer distance. The signals propagate between the communicating points - termed nodes - through the atmosphere along a beam of light. FSO offers the advantages of broadband communication capacity, being cost-effective, secure and easy to set up [62]. These features of FSO communication systems potentially make them possible to solve the current issues that traditional RF communication systems are facing, such as high cost and excessive use of the spectrum [63].

Recently, sophisticated schemes for MU access and scheduling on expanded RF bands have been receiving much interest from academic and research communities. The accommodation of more users per a unit resource and time has been proposed through various PHY and MAC layer designs. Among these designs, spectrum-sharing have been shown to improve the spectral efficiency in wireless networks [66]. More spatial MIMO techniques can provide substantial benefits through exploiting space domain and using advanced signal processing techniques. With the emerging use of FSO and RF bands to support future expansion of wireless networks in terms of coverage, capacity, and reliability, the development of new MU access and scheduling schemes become very critical. These schemes require new approaches of modeling and analysis that are different from the RF-alone scenarios.

Based on aforementioned discussion, a number of issues was experienced to be employed in actual communications systems which leads to investigate various scenarios to obtain the ideal setup. One scenario with significant potential for efficient communications is the use of mixed RF/FSO relay networks. In this scenario, multiple users with RF capabilities can be multiplexed into a single FSO link via a relay node for a dual-hop case [67, 68]. More specifically, this scenario involves connecting multiple users with a relay (which could be a building) using wireless channels and then an FSO link is connecting between the relay and the destination (which could be another building). This type of connection, in which a high-speed FSO link is used, aims to seal the gap between the backbone network and the last-mile access networks [69], which is a particular issue in developing countries where there might be a poor fiber optic or connecting infrastructure. Alternatively, an FSO transmitter and a receiver can be easily installed on high buildings to connect the last mile by having the users communicate using their RF networks, leaving the last mile to be covered by the FSO communication. One of the key ideas that can be studied in relation to this scenario is the scheduling among users, as will be further discussed in the coming chapters.

Another important area of research is the dual-hop parallel FSO relaying, in which a source node communicates with a destination node with the help of multiple relays. As shown in the literature review, a system of all-optical links was previously proposed and investigated [70], where all the nodes communicate over FSO links. Another important scenario arising from this system and could also be considered is the dual-hop FSO/RF scenario. This relaying scenario could be seen in all-optical relay networks when the second hop FSO links suffer from bad weather conditions, such as strong fog. In such conditions, the second hop communications could be conducted over RF links as a backup for the FSO links. Moreover, the FSO first hop might be utilized to serve multiple base stations (BSs) or users at the same time through providing high data rate of multiple RF links.

1.3 Dissertation Contributions

Based on the aforementioned discussions, the dissertation contributions can be divided into two main parts, which are the cooperative CR networks and the mixed RF/FSO networks. Generally, the work investigates the reliability performance metrics of new system models in both areas such as the outage probability, the symbol error probability (SEP), the maximum achievable rate and the ergodic capacity. Then, the work studies the secrecy performance of these new systems against eavesdropping attacks as follows:

- In the area of cooperative CR networks, we propose a new model based on the well-known two-path AF scheme. Upon sharing CSI between PU and SU networks, the proposed model can enhance the bandwidth efficiency. We obtain the optimal SU transmission power and amplification factor values to minimize the total sum of the proposed model probability of error. Then, we find the total sum rate of the proposed cooperative CR model over Rayleigh fading environment and compare it with the existing cooperative models. Moreover, we design new PHY security schemes to enhance the secrecy performance against single/multiple passive eavesdroppers. Then, we find the secrecy capacity performance as well as the secrecy outage probability of the proposed schemes as a function of the SU transmission power and amplification factors.

- In the area of cooperative CR networks, we propose a new cooperative two-way AF model with three different schemes of cooperation. Based on applied cooperative scheme, the bandwidth efficiency is shown to enhance with different values. We derive closed-form expressions for the system outage probability, the SEP and the maximum achievable rate in Rayleigh fading environment. Then, we obtain the optimal SU transmission power and amplification factor values to minimize the total sum SEP of the proposed model. Hence, we find the optimal power values needed to maximize the total sum rate of the proposed cooperative model. For the three proposed cooperative schemes, we compare the derived reliability performance metrics with the existing conventional two-way AF relaying model. Moreover, we investigate the secrecy performance of the new proposed model against eavesdropping attack for two different scenarios based on the selected cooperative scheme.

- In the area of mixed RF/FSO networks, we investigate the reliability performance of dual-hop MU single-input-multiple-output (SIMO) mixed RF/FSO networks in which a multiple antennas relay node selects the best user among a set of single antenna users during the RF hop, then, the relay applies the AF protocol on the received data and retransmits it to the optical receiver over the FSO hop. We also study the proposed system performance under two different diversity combining schemes which are MRC and SC. Hence, we derive closed-form expressions for the system reliability performance metrics such as the outage probability, the SEP and the ergodic capacity in Nakagami-m/Gamma-Gamma environments. Based on the asymptotic outage probability and FSO atmospheric conditions, we obtain a new optimal RF power formula which is tested against different diversity orders and atmospheric channel conditions. Moreover, we investigate the system secrecy performance against multiple antennas passive eavesdropper attack. Furthermore, system intercept probability is derived. In addition, we proposed a PHY security model to improve system security.

- In the area of mixed RF/FSO networks, we investigate the impact of co-channel interference (CCI) signals on the reliability performance of dual-hop MU mixed RF/FSO networks in which a relay node with a single antenna selects the best user among a set of single antenna users during the first hop, then, the relay applies the AF protocol on the received data and retransmits it to the optical receiver during the second hop. We derive closed-form expression for the system outage probability in Nakagami-m/Gamma-Gamma environments. Based on the asymptotic outage probability, the interference power and the FSO atmospheric conditions, we obtain a new optimal RF power formula which is tested against different diversity orders, different number of CCI signals and atmospheric channel conditions. Moreover, we investigate the system secrecy performance against a passive eavesdropper attack. The eavesdropper is also assumed to suffer from a number of non-identical CCI signals. Hence, we derive a closed-form expression for the system intercept probability. In addition, we propose a PHY security model to enhance the system secrecy performance.

1.4 Dissertation Outline

In Chapter 2, we propose a new cooperative CR model which employs the two-path AF scheme. The proposed model encourages the PU networks to cooperate with the SU network, which enhances the PU diversity order. On the other hand, SU network makes use of the inter-relay-interference (IRI) problem in this two-path AF scheme to transmit its data. Moreover, the proposed model is showed to enhance the security performance of the PU network in the presence of eavesdroppers. Optimal power allocation values are obtained for the SU transmission power and amplification factors to enhance the proposed model probability of error performance and its secrecy performance.

In Chapter 3, we propose a new cooperative two-way AF relaying cognitive network in which the SU network pairs (i.e., the source and destination) serve as two extra relay nodes to help the co-existing PU two-way AF relaying network. For this model, we propose three different schemes for cooperation between the PU network and the SU network namely, the all participant scheme, the relay selection scheme and the relay elimination scheme. For all proposed schemes, we derive the system performance metrics which are the outage probability, the SEP and the maximum achievable rate. Power allocation optimization problems are formulated to obtain the optimal power values which minimize the total sum SEP. Also, other problems to maximize the maximum sum rate are proposed. Then, the PHY security performance of the proposed model is investigated against eavesdropping attacks for two different scenarios, namely, the cooperative beamforming scenario and the relay-jamming scenario. New power allocation optimization problems are formulated to find the optimal power values which maximize the system secrecy capacity in the presence of a passive eavesdropper for both scenarios.

In Chapter 4, we propose a new MU SIMO mixed RF/FSO relay networks in which the selected best user among a set users transmits its data to an AF relay node over an RF link of Nakagami-m fading distribution during the first hop, then, the relay retransmits the received data to the destination over an FSO link of Gamma-Gamma distribution. Closed-form expressions for different system reliability metrics are derived. To get more insights on the system key parameters, we derive asymptotic formulas for the outage probability. Then, optimal RF transmission power is proposed based on the asymptotic outage probability formulas, the number of users, the number of antennas and the FSO link conditions. Moreover, the secrecy performance of the considered model is investigated in the presence of a single passive eavesdropper equipped with multiple antennas. Therefore, we derive the system intercept probability which is further simplified to its asymptotic formula. In addition, we enhance the system secrecy performance of the considered model by applying a CJ model for which we derive a new intercept probability closed-form expressions and its corresponding asymptotic formula.

In Chapter 5, we study the impact of non-identical CCI on the security and reliability analysis of MU mixed RF/FSO networks. The RF/FSO links are assumed to follow Nakagami-m/Gamma-Gamma channels distributions. In this model, we consider that both the authorized nodes (i.e., the users and relay) and the eavesdropper suffer from non-identical CCI signals. We derive closed-form expression for the system outage probability. At high SNR values, we simplify the outage probability expression to a less sophisticated asymptotic formula. Based on the asymptotic formula, a new RF power allocation formula is proposed that is dependent on the number of users, the Nakagami-m parameter, the CCI signals and the FSO link conditions. Hence, the secrecy performance is investigated by obtaining the system intercept probability. To enhance the system secrecy performance, we propose a new PHY security model based on a CJ technique.

Finally, in Chapter 6, we briefly summarize the main conclusions of the dissertation and point out some possible future research directions.

CHAPTER 2

A BANDWIDTH EFFICIENT COGNITIVE RADIO WITH TWO-PATH AMPLIFY -AND-FORWARD RELAYING

2.1 Introduction

In this chapter, we introduce a new CR system employing the two-path AF relaying scheme. In the proposed system, the primary user (PU) transmitter cooperates with the secondary user (SU) transmitter and receiver to relay PU data to the PU destination. The proposed algorithm makes use of the inter-relay interference (IRI) between the two relay nodes to transmit SU data and minimize their IRI effect on the PU destination. Two optimization problems are formulated to find optimal power allocation between SU transmission and relaying amplifying factors: one to minimize the probability of error and the other one to maximize the average achievable rate. Moreover, the improvement in PU network PHY security against multiple passive eavesdroppers is studied in two different scenarios. Optimization problems are formulated to find the optimal power allocation solutions that maximize PU secrecy rate in terms of SU transmission power, AF amplification factors. Lagrangian multipliers method is used to obtain the optimal solutions. Numerical results show that the proposed algorithm outperforms the single data transmission and existing two-path relaying scheme. In addition, the PU network achieves diversity order of 3 when maximum likelihood decoder (MLD) is used, whereas SU network achieves diversity order of 2. In addition, the new cooperative CR model can achieve a non-zero secrecy rate even if the wiretap channel conditions are better than the main channel conditions.

The rest of this chapter is organized as follows: Section 2.2 reviews related literature. Section 2.3 introduces the proposed system model. Section 2.4 formulates BER minimization optimization problem. Rate maximization optimization problem is presented in Section 2.5. Section 2.6 presents the design of the PHY security model based on SU jamming transmission. Section 2.7 illustrates the design of the PHY security model under the SU transmission awareness. Section 2.8 presents the complexity analysis of the proposed model. Section 2.9 discusses the numerical results. Finally, Section 2.10 concludes the work.

2.2 Literature Review

Two-path relaying has been recently considered as an attractive wireless communication scheme to improve the spectral efficiency and performance of half-duplex cooperative networks. The two-path relaying scheme consists of a source node S, a destination D and two relay nodes R_{A} and R_{B}. Transmission time slots are divided between the two relays, i.e., while one relay is receiving the source data, the other relay forwards the previous data received during the previous time slot to D [71, 72]. The two-path relaying scheme needs $N+1$ time slots to transmit N data symbols from S to D. In order to increase bandwidth efficiency of $N/(N+1)$, N should be sufficiently large. In [73, 74], the two-path relaying scheme was used to relay data from a source S to a destination D using one of the two famous relaying protocols, namely, AF and DF. Due to the simultaneous transmission from S to relay nodes R_{A} and R_{B}, inter-relay interference (IRI) appears and degrades the system performance. Partial interference cancellation (PIC) [73] and full interference cancellation (FIC) [74] were proposed to mitigate the IRI effect at the destination D.

To overcome spectrum scarcity problem, CR is presented as an efficient technology. In [75], cooperative relaying was applied in CR, by allowing the SU to operate as a relay node for the PU. Then, the PU rewards the SU by allowing higher interference threshold if the SU operates in an underlay CR mode, or by allocating a time slot to the SU to transmit his data in an overlay CR mode. Power allocation scheme and time division criteria have been developed for this model. The disadvantage of the proposed model in [75] is that the PU has to wait the SU for two time slots, the first slot is used to relay PU data, and the second slot is used to transmit SU data, resulting in large delay and lower bandwidth efficiency.

PHY security has been considered as a necessary strategy to enhance secrecy in wireless communication networks due to the broadcast nature of the wireless medium and the resulting security susceptibilities [1]. The secrecy capacity was studied in [34] in the presence of a single eavesdropper and with the help of a relay node where a secrecy performance comparison was held between different relaying protocols (i.e., AF, DF, CF and DT). The authors in [35] examined the DF and AF relaying protocols in the presence of more than one relay in cooperation with the legitimate user. The main goal was to maximize the secrecy capacity by choosing the optimal beamforming weights at each relay. A secrecy rate performance comparison between the cooperative beam-forming and cooperative jamming was introduced. Due to noise amplification at the AF relays, the secure capacity maximization problem becomes very difficult to be optimally solved. In [37], a new scheme was proposed to enable an opportunistic selection of two relay nodes for the goal of increasing the security against eavesdropping attack. The first relay operates in the conventional mode by assisting the source to deliver its data to its destination via a DF strategy. The second relay is used to create intentional interference at the eavesdroppers. The proposed selection technique jointly protects the authorized destination against interference and eavesdropping by jamming the reception of the eavesdropper.

Recently, the cooperation between PU and SU networks has been investigated in [76]. Two scenarios have been studied based on the knowledge of the PU message at SU nodes. For each scenario, three optimization problems have been formulated: the maximization of the PU rate, the maximization of the SU rate and the maximization of the SU transmission power. For some special cases, closed-form expressions have been obtained and the cooperation between PU and SU networks has been analyzed using a game theoretic approach using the Stackelberg game. The work in [77] studied the impact of untrusted SU nodes on the cooperation between PU and SU networks

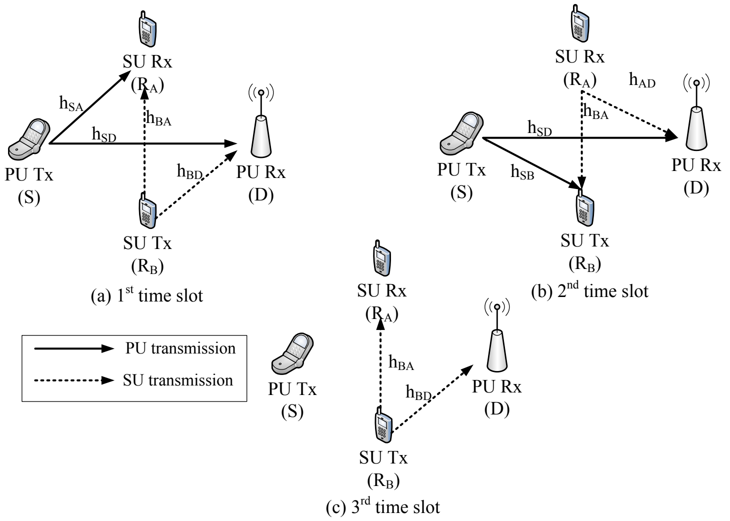
In this chapter, we present a new cooperative CR model by employing the two-path relaying in a cooperative CR relay network. As shown in Figure 2.1, nodes S and D represent the PU network, whereas nodes R_A and R_B represent the SU network. At the same time, R_A and R_B help the PU network in conducting its transmission using two-path AF relaying as will be explained later. As a reward, the PU system allows SU system (R_A and R_B) to transmit its data simultaneously through the proposed protocol described in Section 2.3.

The main challenge is to control SU transmission power and amplifying factors of the two relays in order to minimize the probability of error at both PU and SU destinations. To this end, we formulate an optimization problem to minimize the proposed system BER in terms of the SU transmission power and the two relays amplifying factors. The Lagrangian multipliers method is used to find the optimal values to minimize the exact probability of error of the PU system under constraints on available power budget. A sub-optimal power allocation is obtained by minimizing the asymptotic probability of error of PU system resulting in lower complexity optimization. Another optimization problem is formulated to maximize the average achievable rate based on the same parameters and constraints used in the minimization problem. Then, we investigate the secrecy performance of the proposed model in the presence of multiple passive eavesdroppers. The contribution of this work is to design efficient PHY security models against multiple passive eavesdroppers that are located close to the PU destination. Two different scenarios are investigated based on if the eavesdroppers are aware of SU transmission or not.

The proposed model needs three time slots to transmit two PU symbols and one SU symbol resulting in achieving a unity bandwidth efficiency. Simulation results show that the proposed model achieves a diversity order of 3 for the PU system and a diversity order of 2 for the SU system. Moreover, the proposed scenarios are shown to achieve a non-zero secrecy rate against large number of multiple passive eavesdroppers M even if the wiretap channel condition is better than the main channel.

2.3 System Model

Figure 2.1 shows the operation of the proposed protocol that enables the transmission of two PU symbols and one SU symbol in three time slots.



(a) 1st time slot

(b) 2nd time slot

(c) 3rd time slot

Figure 2.1: Cognitive radio network with two-path AF relaying scheme.

The channel gain between S and D is denoted by h_{SD}, and the channel gains between S and R$_{\mathsf{A}}$ and R$_{\mathsf{B}}$ are denoted by h_{SA} and h_{SB}, respectively with an average channel gain of v_{S}^2. The channel gains between R$_{\mathsf{A}}$ and R$_{\mathsf{B}}$ are h_{AB} and h_{BA}, respectively with average channel gain v_{R}^2. The two relay nodes R$_{\mathsf{A}}$ and R$_{\mathsf{B}}$ have channel gains to the destination node given by h_{AD} and h_{BD}, respectively with an average of v_{D}^2. For notational simplicity, all the channels are assumed to be independent and identically distributed (i.i.d.) flat Rayleigh fading channels. AF protocol is applied by both relays since it is less complex and more flexible in handling IRI than DF protocol [74].

In the first time slot, S transmits the algebraic subtraction of two successive modulated signals denoted by s_1 and s_2 with a total power of P_{s}. At the same time R_B transmits its data b_1 with power P_{B} which interferes with PU data at R$_{\mathsf{A}}$ and D. During the first time slot, the received signals at D and R$_{\mathsf{A}}$ are, respectively given by

$$y_{\mathsf{D}}^{(1)} = \sqrt{\frac{P_{\mathsf{s}}}{2}} h_{\mathsf{SD}}(s_1 - s_2) + \sqrt{P_{\mathsf{B}}} h_{\mathsf{BD}} b_1 + w_{\mathsf{D}}^{(1)}, \tag{2.1}$$

$$y_{\mathsf{A}}^{(1)} = \sqrt{\frac{P_{\mathsf{s}}}{2}} h_{\mathsf{SA}}(s_1 - s_2) + \sqrt{P_{\mathsf{B}}} h_{\mathsf{BA}} b_1 + w_{\mathsf{A}}^{(1)}, \tag{2.2}$$

where w_{D} and w_{A} are additive white Gaussian noise (AWGN) samples with zero-mean and variance σ^2. Then, S transmits the second symbol s_2 with a total power of P_{s} during the second time slot to R$_{\mathsf{B}}$ and D, while R$_{\mathsf{A}}$ transmits the previous received data after applying AF protocol. The received signals at D and R$_{\mathsf{B}}$ during the second time slot are, respectively given by

$$y_{\mathsf{D}}^{(2)} = \sqrt{P_{\mathsf{s}}} h_{\mathsf{SD}} s_2 + h_{\mathsf{AD}} \beta_{\mathsf{A}} y_{\mathsf{A}}^{(1)} + w_{\mathsf{D}}^{(2)}, \tag{2.3}$$

$$y_{\mathsf{B}}^{(2)} = \sqrt{P_{\mathsf{s}}} h_{\mathsf{SB}} s_2 + h_{\mathsf{AB}} \beta_{\mathsf{A}} y_{\mathsf{A}}^{(1)} + w_{\mathsf{B}}^{(2)}, \tag{2.4}$$

where w_{B} is an AWGN sample with zero-mean and variance σ^2. Assuming R_{A} retransmits the data with power $P_{\mathsf{R_A}} = \lambda_{\mathsf{A}} P_{\mathsf{s}}$, then the normalized amplification factor is defined as $\beta_{\mathsf{A}}^2 = \frac{P_{\mathsf{R_A}}}{E|y_{\mathsf{A}}^{(1)}|^2} = \frac{\lambda_{\mathsf{A}} P_{\mathsf{s}}}{v_{\mathsf{S}}^2 P_{\mathsf{s}} + v_{\mathsf{R}}^2 P_{\mathsf{B}} + \sigma^2}$. During the third time slot, S is idle while R$_{\mathsf{B}}$ transmits the received signal after removing the interfered SU data b_1 and adding a new fresh version of it but with negative sign, i.e., $-b_1$ with power P_{B}. Under the assumption of knowing CSI by all relay nodes and destinations, the received signal at D and R$_{\mathsf{A}}$ during the third time slot are, respectively given by

$$y_{\mathsf{D}}^{(3)} = h_{\mathsf{BD}}\beta_{\mathsf{B}}(y_{\mathsf{B}}^{(2)} - b_1') - \sqrt{P_{\mathsf{B}}}h_{\mathsf{BD}}b_1 + w_{\mathsf{D}}^{(3)}, \tag{2.5}$$

$$y_{\mathsf{A}}^{(3)} = h_{\mathsf{BA}}\beta_{\mathsf{B}}(y_{\mathsf{B}}^{(2)} - b_1') - \sqrt{P_{\mathsf{B}}}h_{\mathsf{BA}}b_1 + w_{\mathsf{A}}^{(3)}, \tag{2.6}$$

where b_1' is the modified image of SU data b_1 such that $b_1' = \beta_{\mathsf{A}}h_{\mathsf{AB}}h_{\mathsf{BA}}b_1$. Assuming that R_{B} transmits the received signal with power $P_{\mathrm{R}_{\mathsf{B}}} = \lambda_{\mathsf{B}}P_{\mathsf{s}}$, then the normalized amplifying factor is defined as $\beta_{\mathsf{B}}^2 = \frac{P_{\mathrm{R}_{\mathsf{B}}}}{E|y_{\mathsf{B}}^{(2)}|^2} = \frac{\lambda_{\mathsf{B}}P_{\mathsf{s}}}{v_{\mathsf{S}}^2P_{\mathsf{s}}+\lambda_{\mathsf{A}}v_{\mathsf{R}}^2P_{\mathsf{s}}+\sigma^2}$. From the above equations and the presence of two receivers in this model, the matrix model for the 3-slot system at D can be written as

$$\mathbf{y}_{\mathsf{D}} = \mathbf{H}_{\mathsf{D}}\mathbf{x}_{\mathsf{s}} + \mathbf{w}_{\mathsf{D}}', \tag{2.7}$$

where $\mathbf{y}_{\mathsf{D}} = \left[y_{\mathsf{D}}^{(1)}, y_{\mathsf{D}}^{(2)}, y_{\mathsf{D}}^{(3)}\right]^T$, $\mathbf{x}_{\mathsf{s}} = \left[\sqrt{P_{\mathsf{s}}}s_1, \sqrt{P_{\mathsf{s}}}s_2, \sqrt{P_{\mathsf{B}}}b_1\right]^T$,

$$\mathbf{H}_{\mathsf{D}} = \begin{bmatrix} \sqrt{\frac{1}{2}}h_{\mathsf{SD}} & -\sqrt{\frac{1}{2}}h_{\mathsf{SD}} & h_{\mathsf{BD}} \\ \sqrt{\frac{1}{2}}\alpha_{\mathsf{A}} & h_{\mathsf{SD}} - \sqrt{\frac{1}{2}}\alpha_{\mathsf{A}} & \beta_{\mathsf{A}}h_{\mathsf{AD}}h_{\mathsf{BA}} \\ \sqrt{\frac{1}{2}}\beta_{\mathsf{B}}h_{\mathsf{BD}}\alpha_{\mathsf{A}}' & \beta_{\mathsf{B}}h_{\mathsf{BD}}(h_{\mathsf{SD}} - \sqrt{\frac{1}{2}}\alpha_{\mathsf{A}}') & -h_{\mathsf{BD}} \end{bmatrix}, \tag{2.8}$$

and the noise vector at D is given by

$$\mathbf{w}_{\mathsf{D}}' = \begin{bmatrix} w_{\mathsf{D}}^{(1)} \\ w_{\mathsf{D}}^{(2)} + \beta_{\mathsf{A}}h_{\mathsf{AD}}w_{\mathsf{A}}^{(1)} \\ w_{D}^{(3)} + h_{\mathsf{BD}}\beta_{\mathsf{B}}(w_{\mathsf{B}}^{(2)} + h_{\mathsf{AB}}\beta_{\mathsf{A}}w_{\mathsf{A}}^{(1)}) \end{bmatrix}, \tag{2.9}$$

where $\alpha_{\mathsf{A}} = \beta_{\mathsf{A}} h_{\mathsf{AD}} h_{\mathsf{SA}}$ and $\alpha'_{\mathsf{A}} = \beta_{\mathsf{A}} h_{\mathsf{AB}} h_{\mathsf{SA}}$. For the SU system, the received signals of the receiver R_{A} can be expressed as

$$\mathbf{y}_{\mathsf{A}} = \mathbf{H}_{\mathsf{A}} \mathbf{x}_{\mathsf{s}} + \mathbf{w}'_{\mathsf{A}}, \tag{2.10}$$

where $\mathbf{y}_{\mathsf{A}} = \left[y_{\mathsf{A}}^{(1)}, y_{\mathsf{A}}^{(3)}\right]^T$, $\mathbf{x}_{\mathsf{s}} = \left[\sqrt{P_{\mathsf{s}}}s_1, \sqrt{P_{\mathsf{s}}}s_2, \sqrt{P_{\mathsf{B}}}b_1\right]^T$,

$$\mathbf{H}_{\mathsf{A}} = \begin{bmatrix} \sqrt{\frac{1}{2}} h_{\mathsf{SA}} & -\sqrt{\frac{1}{2}} h_{\mathsf{SA}} & h_{\mathsf{BA}} \\ \sqrt{\frac{1}{2}} \beta_{\mathsf{B}} h_{\mathsf{BA}} \alpha'_{\mathsf{A}} & \beta_{\mathsf{B}} h_{\mathsf{BA}} (h_{\mathsf{SD}} - \sqrt{\frac{1}{2}} \alpha'_{\mathsf{A}}) & -h_{\mathsf{BA}} \end{bmatrix}, \tag{2.11}$$

and the noise vector at R_{A} is given by

$$\mathbf{w}'_{\mathsf{A}} = \left[w_{\mathsf{A}}^{(1)}, w_{\mathsf{A}}^{(2)} + h_{\mathsf{BA}} \beta_{\mathsf{B}} (w_{\mathsf{B}}^{(2)} + h_{\mathsf{AB}} \beta_{\mathsf{A}} w_{\mathsf{A}}^{(1)})\right]^T. \tag{2.12}$$

In case there is no direct link between S and D or the direct link is too weak, the same equations and expressions are valid with setting $h_{\mathsf{SD}} = 0$.

2.4 Power Allocation for BER Minimization

In this section, optimal and sub-optimal power allocation problems are presented to minimize the probability of error of both PU and SU networks. Since different images of the data symbols are sent during different time slots creating a virtual MIMO network, maximum likelihood detector (MLD) can be used by the PU and SU systems to detect their data. MLD is the optimal detector in terms of minimizing the probability of error [78]. The MLD estimates the symbol vector $\hat{\mathbf{x}}_{\mathsf{s}}$ that gives the minimum Euclidean distance metric at D and R$_{\mathsf{A}}$, independently. The Euclidean distance metrics can be expressed [79] for D and R$_{\mathsf{A}}$, respectively as

$$\mu_{\mathsf{D}} = \|\mathbf{y}_{\mathsf{D}} - \mathbf{H}_{\mathsf{D}}\mathbf{x}_{\mathsf{s}}\|^2 = \sum_{l=1}^{L=3} |y_{\mathsf{D}}^{(l)} - \mathbf{h}_{\mathsf{D}}^{(l)}\mathbf{x}_{\mathsf{s}}|^2, \tag{2.13}$$

$$\mu_{\mathsf{A}} = \|\mathbf{y}_{\mathsf{A}} - \mathbf{H}_{\mathsf{A}}\mathbf{x}_{\mathsf{s}}\|^2 = \sum_{l=1}^{L=2} |y_{\mathsf{A}}^{(l)} - \mathbf{h}_{\mathsf{A}}^{(l)}\mathbf{x}_{\mathsf{s}}|^2, \tag{2.14}$$

where $\mathbf{h}_{\mathsf{D}}^{(l)}$ and $\mathbf{h}_{\mathsf{A}}^{(l)}$ denote the l-th row of $\mathbf{H}_{\mathsf{D}}$ and $\mathbf{H}_{\mathsf{A}}$, respectively. The MLD computational complexity depends on number of points in the signal constellation and number of transmitters which are three nodes in this system, namely S, R$_{\mathsf{A}}$ and R$_{\mathsf{B}}$. The pairwise-error probability is defined as the probability that the MLD chooses the erroneous data vector $c_i = (c_{i1}, c_{i2}, c_{i3})$ instead of the transmitted data vector $c_j = (c_{j1}, c_{j2}, c_{j3})$, where the data symbols c_{im} and c_{jm} are for the m-th user. Based on the derivations presented in [80, 81, 79], the union bound of the probability of error for m-th user is given by

$$P_{s_m} \leq \sum_{i} \prod_{l=1}^{L} \frac{1}{(1 + r_{sm,ijl})}, \tag{2.15}$$

where i includes all the indexes of vectors in c_i that differ in their m-th position from the transmitted vector c_j, $m = 1, 2$ and 3. The number of independent paths L takes the value of 3 for PU system and $L = 2$ for SU system. The term $r_{sm,ijl}$

is given by [79, eq:(9)]

$$r_{sm,ijl} = a_{s_m,ijl}\Gamma_{s_m,jl}\sqrt{(a_{s_m,ijl}\Gamma_{s_m,jl})^2 + 2(a_{s_m,ijl}\Gamma_{s_m,jl})} + 1, \tag{2.16}$$

where $a_{s_m,ijl} = \| d_i - d_j \|^2 / 2E_{sl}$, E_{sl} is the symbol energy per branch and $\Gamma_{s_m,jl} = E_{sl}/N_0$ is the average symbol SNR per diversity branch as shown in [79, eq:(10)].

2.4.1 Optimal Power Allocation

In this part, we formulate a power allocation problem which minimizes the BER sum for both PU and SU networks of the proposed system by controlling the SU transmission power P_{B} and the two relays amplifying factors β_{A} and β_{B}. The goal is to find the values of those parameters that minimize the overall BER. The BER is a function of the SNR and it can be expressed for a given channel state as [82] $P_{\mathsf{b}}(e) = f(P_{\mathsf{B}}, \lambda_{\mathsf{A}}, \lambda_{\mathsf{B}})$, where $f(.)$ is a function determined based on the type of the modulation scheme and detection method. In this problem, $f(.)$ equals the probability of error given in (2.15). Then, an optimization problem has been formulated in which the target function can be minimizing the PU BER only or minimizing the total sum BER of the PU and SU. Such that

$$\begin{aligned} &\text{minimize} \;\; f(P_{\mathsf{B}}, \lambda_{\mathsf{A}}, \lambda_{\mathsf{B}}) \\ &\text{subject to: } P_{\mathsf{B}} + \lambda_{\mathsf{B}} P_{\mathsf{s}} \le \overline{\mathbf{P}}_{\mathsf{B}}, \\ &\qquad 2P_{\mathsf{B}} + \lambda_{\mathsf{A}} P_{\mathsf{s}} + \lambda_{\mathsf{B}} P_{\mathsf{s}} \le \overline{\mathbf{P}}_{\mathsf{total}}. \end{aligned} \tag{2.17}$$

To find the optimal values for P_{B}, λ_{A} and λ_{B}, Lagrangian multipliers method with the two power constraints in (2.17) is used [83]. The Lagrangian function $\mathcal{J}(.)$ can be expressed as

$$\begin{aligned}\mathcal{J}\left(P_{\mathsf{B}}, \lambda_{\mathsf{A}}, \lambda_{\mathsf{B}}\right) = f\left(P_{\mathsf{B}}, \lambda_{\mathsf{A}}, \lambda_{\mathsf{B}}\right) &+ \Lambda_1\left(P_{\mathsf{B}} + \lambda_{\mathsf{B}} P_{\mathsf{s}} - \overline{\mathbf{P}}_{\mathsf{B}}\right) \\ &+ \Lambda_2\left(2P_{\mathsf{B}} + \lambda_{\mathsf{A}} P_{\mathsf{s}} + \lambda_{\mathsf{B}} P_{\mathsf{s}} - \overline{\mathbf{P}}_{\mathsf{total}}\right), \end{aligned} \tag{2.18}$$

where Λ_1 and Λ_2 denote the Lagrangian multipliers. Since finding a closed-form solution for the BER function in (2.15) is difficult, hence, the optimal power allocation solution has been found in an iterative manner.

2.4.2 Suboptimal Power Allocation

A less sophisticated approach for power allocation optimization is to minimize the asymptotic union bound of the probability of error instead of the exact one in (2.15). This results in a less complex optimization problem and yields an approximate power allocation that works well in high SNR regions. In high SNR regions, the expression in (2.15) can be reduced to [79]

$$P_{s_m,\mathrm{asym}} \le \sum_i \prod_{l=1}^{L} r_{s_m,ijl}^{-1}. \tag{2.19}$$

Applying the same discussion in Section 2.4.1 provides the suboptimal power allocation solution.

2.5 Power Allocation for Rate Maximization

In this section, the average achievable rate of the proposed system is discussed. The average achievable rate for the proposed model can be obtained by

$$R_{\mathsf{D}} = \frac{1}{3}\mathrm{E}\left\{\log\left[\det\left(\mathbf{I} + \frac{\mathbf{H}_{\mathsf{D}}\mathbf{H}_{\mathsf{D}}^{*}}{\mathrm{E}\left[\mathbf{w}_{\mathsf{D}}'\mathbf{w}_{\mathsf{D}}'^{*}\right]}\right)\right]\right\}. \tag{2.20}$$

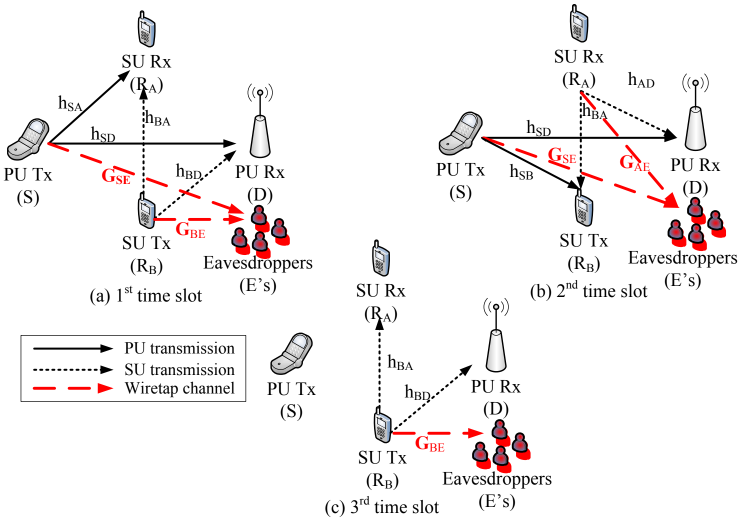
It is clear that the average achievable rate is a function of P_{B}, λ_{A} and λ_{B}. The goal is to find the optimal values of these parameters which maximize the average achievable rate. In this case, $g(P_{\mathsf{B}}, \lambda_{\mathsf{A}}, \lambda_{\mathsf{B}})$ equals the average achievable rate given by (2.20). Then, the optimization problem can be formulated such that:

$$\begin{aligned} &\text{maximize } \; g(P_{\mathsf{B}}, \lambda_{\mathsf{A}}, \lambda_{\mathsf{B}}) \\ &\text{subject to: } P_{\mathsf{B}} + \lambda_{\mathsf{B}} P_{\mathsf{s}} \leq \overline{\mathbf{P}}_{\mathsf{B}}, \\ &\qquad 2P_{\mathsf{B}} + \lambda_{\mathsf{A}} P_{\mathsf{s}} + \lambda_{\mathsf{B}} P_{\mathsf{s}} \leq \overline{\mathbf{P}}_{\mathsf{total}}. \end{aligned} \tag{2.21}$$

Following the same steps in Section 2.4.1 in solving (2.17), the optimal solution for rate maximization can be obtained.

2.6 Scenario I: Physical Layer Security under SU Jamming

In this scenario, it is assumed that the eavesdroppers know about the cooperation between PU and SU networks in the transmission of PU data but they do not



(a) 1st time slot

(b) 2nd time slot

(c) 3rd time slot

Figure 2.2: Cooperative cognitive radio network with two-path AF relaying scheme with multiple passive eavesdroppers.

know about the simultaneous transmission of PU and SU data. In another way, the eavesdroppers are assumed to be attacking the PU transmission only and ignoring SU data. In this case, the eavesdroppers treat the interference from SU transmission as a noise and hence can be treated as a jamming signal on the eavesdroppers. The model in which the eavesdroppers are unaware of the simultaneous transmission is similar to the relay - jamming model known as (R-J) cooperation scheme [37].

Consider the presence of M passive eavesdropping nodes. In addition, the each of the eavesdroppers is assumed to be equipped with a single antenna with no cooperation between them. This is more practical and allow them to avoid being detected. The M eavesdroppers attack the PU system and treat the SU data transmission as noise resulting in an R-J model [33]. We denote the channels between the nodes S, $\mathsf{R_A}$, $\mathsf{R_B}$ and the m-th eavesdropper by $g_{\mathsf{SE_m}}$, $g_{\mathsf{AE_m}}$ and $g_{\mathsf{BE_m}}$, respectively. The channel coefficients are assumed to be independent and identical random variable and to follow Rayleigh fading distribution (i.i.d) with zero mean and variance v_{g}^2. Then according to the considered model in Section 2.3, the matrix model at the m-th eavesdropper after three-time slots is given by

$$\mathbf{y}_{\mathsf{E_m}} = \mathbf{G}_{\mathsf{E_m}}\mathbf{x}_{\mathsf{s}} + b_1\mathbf{G}_{\mathsf{J_m}} + \mathbf{w}_{\mathsf{E_m}}, \tag{2.22}$$

where $\mathbf{y}_{\mathsf{E}} = \left[y_{\mathsf{E}}^{(1)}, y_{\mathsf{E}}^{(2)}, y_{\mathsf{E}}^{(3)}\right]^T$, $\mathbf{x}_{\mathsf{s}} = [s_1, s_2]^T$,

$$\mathbf{G}_{\mathsf{E_m}} = \begin{bmatrix} \sqrt{\frac{P_{\mathsf{s}}}{2}}g_{\mathsf{SE_m}} & -\sqrt{\frac{P_{\mathsf{s}}}{2}}g_{\mathsf{SE_m}} \\ \sqrt{\frac{P_{\mathsf{s}}}{2}}\alpha_{\mathsf{E_m}} & \sqrt{P_{\mathsf{s}}}g_{\mathsf{SE_m}} - \sqrt{\frac{P_{\mathsf{s}}}{2}}\alpha_{\mathsf{E_m}} \\ \sqrt{\frac{P_{\mathsf{s}}}{2}}\beta_{\mathsf{B}}g_{\mathsf{BE_m}}\alpha'_{\mathsf{A}} & \beta_{\mathsf{B}}g_{\mathsf{BE_m}}(\sqrt{P_{\mathsf{s}}}h_{\mathsf{SD}} - \sqrt{\frac{P_{\mathsf{s}}}{2}}\alpha'_{\mathsf{A}}) \end{bmatrix}, \tag{2.23}$$

$$\mathbf{G}_{\mathsf{J_m}} = \left[\sqrt{P_{\mathsf{B}}}g_{\mathsf{BE_m}}, \sqrt{P_{\mathsf{B}}}\beta_{\mathsf{A}}h_{\mathsf{BA}}g_{\mathsf{AE_m}}, -\sqrt{P_{\mathsf{B}}}g_{\mathsf{BE}}\right]^T, \tag{2.24}$$

$$\mathbf{w}_{\mathsf{E_m}} = \begin{bmatrix} w_{\mathsf{E_m}}^{(1)} \\ w_{\mathsf{E_m}}^{(2)} + \beta_{\mathsf{A}}g_{\mathsf{AE_m}}w_{\mathsf{A}}^{(1)} \\ w_{\mathsf{E_m}}^{(3)} + g_{\mathsf{BE_m}}\beta_{\mathsf{B}}(w_{\mathsf{B}}^{(2)} + h_{\mathsf{AB}}\beta_{\mathsf{A}}w_{\mathsf{A}}^{(1)}) \end{bmatrix}, \tag{2.25}$$

where $\alpha_{\mathsf{E}} = \beta_{\mathsf{A}}g_{\mathsf{AE_m}}h_{\mathsf{SA}}$. In case there is no direct link between S and E or the direct link is too weak, the same equations and expressions are valid with setting $g_{\mathsf{SE_m}} = 0$ for $\mathsf{m} \in \{1, ..., M\}$. The average data rate for the proposed model at the

m-th eavesdropper can be obtained by

$$R_{\mathsf{E_m}} = \frac{1}{3}\mathrm{E}\left\{\log\left[\det\left(\mathbf{I} + \frac{\mathbf{G}_{\mathsf{E_m}}\mathbf{G}^*_{\mathsf{E_m}}}{\mathrm{E}\left[\mathbf{w}'_{\mathsf{E_m}}\mathbf{w}'^*_{\mathsf{E_m}}\right]}\right)\right]\right\}, \tag{2.26}$$

where $\mathbf{w}'_{\mathsf{E}}$ is the sum of jamming signal and noise and it is given by

$$\mathbf{w}'_{\mathsf{E_m}} = b_1\mathbf{G}_{\mathsf{J_m}} + \mathbf{w}_{\mathsf{E_m}}. \tag{2.27}$$

Then, the achievable secrecy rate for non-cooperative eavesdropping nodes can be obtained by

$$\begin{aligned} R_{\mathsf{S}} &= \min_{\mathsf{m}\in M}\left\{R_{\mathsf{D}} - R_{\mathsf{E_m}}\right\} \\ &= \min_{\mathsf{m}\in M}\left\{\frac{1}{3}\mathrm{E}\left\{\log\left[\frac{\det\left(\mathbf{I} + \frac{\mathbf{H}_{\mathsf{D}}\mathbf{H}^*_{\mathsf{D}}}{\mathrm{E}\left[\mathbf{w}_{\mathsf{D}}\mathbf{w}^*_{\mathsf{D}}\right]}\right)}{\det\left(\mathbf{I} + \frac{\mathbf{G}_{\mathsf{E_m}}\mathbf{G}^*_{\mathsf{E_m}}}{\mathrm{E}\left[\mathbf{w}'_{\mathsf{E_m}}\mathbf{w}'^*_{\mathsf{E_m}}\right]}\right)}\right]\right\}\right\}. \end{aligned} \tag{2.28}$$

It is clear that R_{S} is always greater than zero as long as P_{B} does not equal zero. A power allocation problem is presented to maximize the secrecy rate $R_{\mathsf{S}} = f(P_{\mathsf{B}}, \lambda_{\mathsf{A}}, \lambda_{\mathsf{B}})$ such as

$$\begin{aligned} &\text{maximize} \;\; f(P_{\mathsf{B}}, \lambda_{\mathsf{A}}, \lambda_{\mathsf{B}}) \\ &\text{subject to: } P_{\mathsf{B}} + \lambda_{\mathsf{B}}P_{\mathsf{s}} \le \bar{\mathbf{P}}_{\mathsf{B}}, \\ &\qquad 2P_{\mathsf{B}} + \lambda_{\mathsf{A}}P_{\mathsf{s}} + \lambda_{\mathsf{B}}P_{\mathsf{s}} \le \bar{\mathbf{P}}_{\mathsf{total}}. \end{aligned} \tag{2.29}$$

To find the optimal values for P_{B}, λ_{A} and λ_{B}, Lagrangian multipliers method [83] with the two power constraints in (2.29) is used. The Lagrangian function $\mathcal{J}(.)$ can be expressed as

$$\begin{aligned}\mathcal{J}\left(P_{\mathsf{B}},\lambda_{\mathsf{A}},\lambda_{\mathsf{B}}\right) &= f\left(P_{\mathsf{B}},\lambda_{\mathsf{A}},\lambda_{\mathsf{B}}\right)+\Lambda_1\left(P_{\mathsf{B}}+\lambda_{\mathsf{B}}P_{\mathsf{s}}-\bar{\mathbf{P}}_B\right)\\ &\quad+\Lambda_2\left(2P_{\mathsf{B}}+\lambda_{\mathsf{A}}P_{\mathsf{s}}+\lambda_{\mathsf{B}}P_{\mathsf{s}}-\bar{\mathbf{P}}_{\mathsf{total}}\right), \qquad (2.30)\end{aligned}$$

where Λ_1 and Λ_2 denote Lagrangian multipliers. Since finding a closed-form solution for the secrecy rate function, the optimal power allocation solution has been obtained iteratively.

2.7 Scenario II: Physical Layer Security Scheme under Secondary User Transmission Awareness

In this section, we consider the worst case for a secure transmission in which the eavesdroppers have all the information about the cooperation between the PU network and SU network including SU simultaneous transmission. In this scenario, it is assumed that the eavesdroppers know the channel coefficients between all the system nodes, as well as the transmission power and relays amplification factors. In this case, the SU transmission is no more treated as a jamming signal as the eavesdroppers try to detect and decode all transmitted symbols. Hence, the R-J cooperative scheme is no more applicable for increasing transmission secrecy.

Regarding the proposed model, the common use of beam-forming criteria in many works in the literature does not apply for two reasons. Firstly, the individual transmission of each node and different data transmission during simultaneous broadcasting is considered. Secondly, each node is assumed to be equipped with a single antenna. Since the PU transmitter S subtracts the two successive data symbols before transmission during the first-time slot, that could be considered as a kind of network coding done by S. Then, we design a weighted network coding at S by the multiplying the two symbols s_1 and s_2 by μ_1 and μ_2, respectively. Although the eavesdroppers have all the information about the proposed model, the source messages are always confidential. Then, the eavesdroppers have no information about the messages, or the weight of each message s_1 and s_2 in the transmitted combination message. The goal is to find the optimal values of μ_1 and μ_2 which maximize the secrecy rate R_{S}.

In this scenario, at the m-th eavesdropper, the received signals are given by

$$\mathbf{y}_{\mathsf{E}} = \mathbf{G}_{\mathsf{E_m}}\mathbf{x}_{\mathsf{s}} + \boldsymbol{\Delta}\mathbf{G}_{\mathsf{m}}\mathbf{x}_{\mathsf{s}} + \mathbf{w}_{\mathsf{E_m}}, \tag{2.31}$$

where $\mathbf{y}_{\mathsf{E_m}} = \left[y^{(1)}_{\mathsf{E_m}}, y^{(2)}_{\mathsf{E_m}}, y^{(3)}_{\mathsf{E_m}}\right]^T$, $\mathbf{x}_{\mathsf{s}} = [s_1, s_2, b_1]^T$, ΔG_{m} is given by (2.32), and

$$\begin{aligned}
\mathbf{\Delta G}_{\mathsf{m}} &= \mathbf{G}^{\text{Actual}}_{\mathsf{E_m}} - \mathbf{G}_{\mathsf{E_m}} \\
&= \begin{bmatrix}
\sqrt{\mu_1 \frac{P_{\mathsf{s}}}{2}} g_{\mathsf{SE_m}} & -\sqrt{\mu_2 \frac{P_{\mathsf{s}}}{2}} g_{\mathsf{SE_m}} & \sqrt{P_{\mathsf{B}}} g_{\mathsf{BE_m}} \\
\sqrt{\mu_1 \frac{P_{\mathsf{s}}}{2}} \alpha_{\mathsf{E_m}} & \sqrt{P_{\mathsf{s}}} g_{\mathsf{SE_m}} - \sqrt{\mu_2 \frac{P_{\mathsf{s}}}{2}} \alpha_{\mathsf{E_m}} & \sqrt{P_{\mathsf{B}}} \beta_{\mathsf{A}} g_{\mathsf{AE_m}} h_{\mathsf{BA}} \\
\sqrt{\mu_1 \frac{P_{\mathsf{s}}}{2}} \beta_{\mathsf{B}} g_{\mathsf{BE_m}} \alpha'_{\mathsf{A}} & \beta_{\mathsf{B}} g_{\mathsf{BE_m}} \left(\sqrt{P_{\mathsf{s}}} h_{\mathsf{SD}} - \sqrt{\mu_2 \frac{P_{\mathsf{s}}}{2}} \alpha'_{\mathsf{A}}\right) & -\sqrt{P_{\mathsf{B}}} g_{\mathsf{BE_m}}
\end{bmatrix} \\
&- \begin{bmatrix}
\sqrt{\mu_{1\mathsf{e_m}} \frac{P_{\mathsf{s}}}{2}} g_{\mathsf{SE_m}} & -\sqrt{\mu_{2\mathsf{e_m}} \frac{P_{\mathsf{s}}}{2}} g_{\mathsf{SE_m}} & \sqrt{P_{\mathsf{B}}} h_{\mathsf{BE_m}} \\
\sqrt{\mu_{1\mathsf{e_m}} \frac{P_{\mathsf{s}}}{2}} \alpha_{\mathsf{E_m}} & \sqrt{P_{\mathsf{s}}} g_{\mathsf{SE_m}} - \sqrt{\mu_{2\mathsf{e_m}} \frac{P_{\mathsf{s}}}{2}} \alpha_{\mathsf{E_m}} & \sqrt{P_{\mathsf{B}}} \beta_{\mathsf{A}} g_{\mathsf{AE}} h_{\mathsf{BA}} \\
\sqrt{\mu_{1\mathsf{e_m}} \frac{P_{\mathsf{s}}}{2}} \beta_{\mathsf{B}} g_{\mathsf{BE_m}} \alpha'_{\mathsf{A}} & \beta_{\mathsf{B}} g_{\mathsf{BE_m}} \left(\sqrt{P_{\mathsf{s}}} h_{\mathsf{SD}} - \sqrt{\mu_{2\mathsf{e_m}} \frac{P_{\mathsf{s}}}{2}} \alpha'_{\mathsf{A}}\right) & -\sqrt{P_{\mathsf{B}}} g_{\mathsf{BE_m}}
\end{bmatrix},
\end{aligned} \tag{2.32}$$

$$\mathbf{w}_{\mathsf{E_m}} = \begin{bmatrix}
w^{(1)}_{\mathsf{E_m}} \\
w^{(2)}_{\mathsf{E_m}} + \beta_{\mathsf{A}} g_{\mathsf{AE_m}} w^{(1)}_{\mathsf{A}} \\
w^{(3)}_{\mathsf{E_m}} + g_{\mathsf{BE_m}} \beta_{\mathsf{B}} (w^{(2)}_{\mathsf{B}} + h_{\mathsf{AB}} \beta_{\mathsf{A}} w^{(1)}_{\mathsf{A}})
\end{bmatrix}. \tag{2.33}$$

In case there is no direct link between S and E or the direct link is too weak, the same equations and expressions are valid with setting $g_{\mathsf{SE_m}} = 0$ for $\mathsf{m} \in \{1, ..., M\}$.

The average data rate for the proposed model at E_{m} is given by (2.26), where

$$\mathbf{w}'_{\mathsf{E_m}} = \mathbf{\Delta G}_{\mathsf{m}} \mathbf{x}_{\mathsf{s}} + \mathbf{w}_{\mathsf{E_m}}. \tag{2.34}$$

In this scenario, the legitimated nodes agree to follow a certain transmission codebook in terms of μ_1 and μ_2. During the full transmission period that consists of three-time slots, the PU source S chooses a particular value from the codebook for μ_2 and its corresponding value of μ_1 for transmission. The main goal is to randomize the data at the eavesdropper node in order to maximize the secrecy rate. The selection criteria for μ_1 and μ_2 is given by

1. $\mu_1 + \mu_2 = 2$
2. Since the SU receiver depends only on two time slots to detect its data; then the PU data should be available in both transmission slots in order to minimize the SU BER. As a result and by referring to channel matrix $\mathbf{H}_{\mathsf{D}}$, it is clear that $0 < \mu_2 < \frac{|h_{\mathsf{SD}}|^2}{\alpha_{\mathsf{A}}^2}$.

In another way, the eavesdroppers are assumed to give equal weights for both PU symbols. Then, an optimization problem is formulated to maximize the secrecy rate $R_{\mathsf{S}} = g\left(\mu_1, \mu_2\right)$ such as

$$\begin{aligned} &\text{maximize} \;\; g(\mu_1, \mu_2) \\ &\text{subject to } \mu_1 + \mu_2 = 2 \;\&\; 0 < \mu_2 < \frac{|h_{\mathsf{SD}}|^2}{\alpha_{\mathsf{A}}^2}. \end{aligned} \tag{2.35}$$

The Lagrangian algorithm expressed in Section 2.6 is followed to obtain optimal values for μ_1 and μ_2. Note that, the complexity of the proposed algorithm can be in the number of steepest descent algorithm iterations needed to converge which is dependent of its step size.

2.8 Complexity Analysis

In this part, the complexity analysis of the proposed model is presented. The proposed model can initially set to enhance the PU secrecy performance with no need for any extra procedures or friendly nodes. Therefore, the proposed model achieves a non-zero secrecy capacity with the same complexity analysis of the joint multiuser MLD detection process. For the joint multiuser MLD decoder, the joint detection of P users each with a modulation size of Q symbols transmitted in three time slots has a number of operations equals to $3Q^P$. Hence, this joint multiuser MLD decoder has a complexity of order $O(Q^P)$. It is clear that the complexity of the joint multiuser MLD decoder increases exponentially with P. However, This complexity can be reduced by using suboptimal joint decoders such as multiuser detection maximum likelihood sphere decoders in [84]. The complexity of the proposed sphere decoder in [84] is a polynomial function of the number of users P and is independent of the modulation size Q. On the other hand, the proposed model is compared to the conventional two-path AF relaying networks with full interference cancellation (FIC) algorithm in [74]. For a frame of length N symbols, the FIC model needs $N+1$ time slots to transmit the whole frame resulting in a bandwidth efficiency equals to $N/(N+1)$. The FIC algorithm has three methods for detection; namely, forward detection, backward detection and maximum ratio combining detection. The total number of operations needed for detection in FIC model equals to $2N+1$ for forward/ backward detection. While for MRC detection, the number of operations equals to $4N+2$. It can be noted that the complexity analysis of the FIC model is of order $O(N)$. However, the number of frames N should be relatively high to achieve a unity bandwidth efficiency resulting in increasing network delay. Moreover, the linearity of the FIC detection methods kills any diversity gain that might be obtained from the inter-relay interference phenomena.

2.9 Numerical Results

Numerical examples are presented to verify the performance of proposed scheme. Since the proposed scheme transmits 3 data symbols in 3 time slots with bandwidth efficiency equals to 1, the simulations of FIC algorithm [74] were generated with 64 symbols per frame to result in almost a unity bandwidth efficiency. For a fair comparison with the FIC model in [74], the total power budget is set to be the same as that used in [74] for three successive transmissions, i.e., $4P_{\mathsf{s}}$. Since the proposed model has no control on the PU source power, then $2P_{\mathsf{s}}$ is excluded from the total power budget such as $\overline{\mathbf{P}}_{\mathsf{total}} = \lambda_{\mathsf{A}}P_{\mathsf{s}} + \lambda_{\mathsf{B}}P_{\mathsf{s}} + 2P_{\mathsf{B}} = 2P_{\mathsf{s}}$. The power budget for R_{B} ($\overline{\mathbf{P}}_{\mathsf{B}}$) is defined as the maximum power allowed at R_{B} for both data relaying and SU data transmission during a single transmission, then $\overline{\mathbf{P}}_{\mathsf{B}} \geq \lambda_{\mathsf{B}}P_{\mathsf{s}} + P_{\mathsf{B}}$. The steepest decent algorithm was employed to find the solution in an iterative manner with a step size given by $\mu(i) = \rho \min_{k:(P_{\mathsf{B}}(i+1),\lambda_{\mathsf{A}}(i+1),\lambda_{\mathsf{B}}(i+1))\leq 0} \tilde{\mu}_k(i)$, where ρ is a positive scaling factor smaller than 1, and $\tilde{\mu}_k(i)$ is the updated step-size with $k = 1, 2$ and 3 for P_{B}, λ_{A} and λ_{B}, respectively.

Figure 2.3 shows a comparison between different transmission schemes that

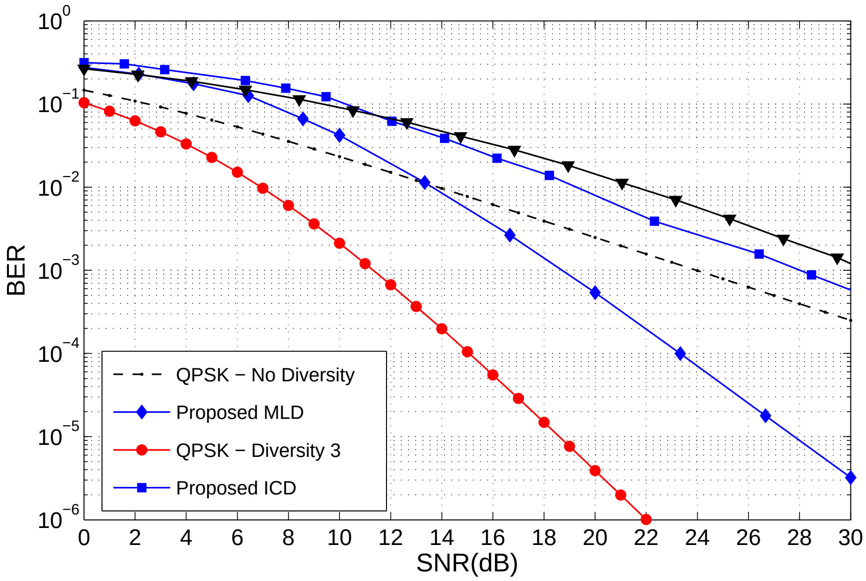


Figure 2.3: BER performance comparison between FIC algorithm and the proposed algorithm using (ICD/MLD) in Rayleigh fading channels.

the PU can use to transmit its data over a Rayleigh fading channel. The used modulation scheme is QPSK. It is clear from this figure that the proposed scheme with MLD detector outperforms the two-path relaying with FIC in [74]. The proposed scheme with ICD detector yields a poor performance in comparison with MLD as it depends on linear operations with low computational complexity. Although the matrix $\mathbf{H}_{\mathsf{D}}$ is a full rank matrix of 3 resulting in a full PU diversity order of 3, Figure 2.3 shows that the MLD performance is slightly less than 3. Because of the channel model matrix of the proposed system at D (i.e., $\mathbf{H}_{\mathsf{D}}$) has some repeated entries such as h_{SD} and h_{BD}. In addition, the products of two channel coefficients in $\mathbf{H}_{\mathsf{D}}$ lead to a different fading distribution. Thus, the differences in the channel model causes the loss of diversity compared to classical MIMO.

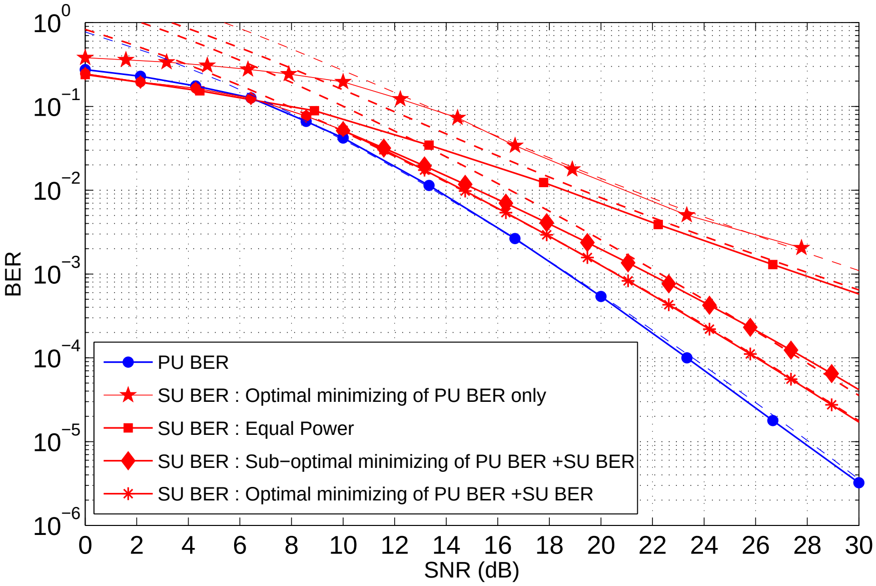


Figure 2.4: BER performance of PU and SU employing different power allocation criteria (solid line: simulation, dashed line: analytical).

Figure 2.4 introduces the effect of different optimization target functions where the PU performance does not change due to the presence of a direct link while there is a huge improvement in the SU performance depending on the target function. Figure 2.4 compares the SU performance under optimal power allocation ($P_{\mathsf{B}} = 0.812$, $\lambda_{\mathsf{A}} = 1$, $\lambda_{\mathsf{B}} = 0.188$) and suboptimal power allocation ($P_{\mathsf{B}} = 0.612$, $\lambda_{\mathsf{A}} = 1$, $\lambda_{\mathsf{B}} = 0.336$) versus equal power allocation schemes.

A comparison between the proposed model and the FIC model [74] in terms of average achievable rate is presented in Figure 2.5. In the presence of a direct link between S and D, results show that the proposed model achieves higher data rate than FIC until on SNR value of 20 dB both models tend to achieve the same average rate. While in the absence of direct link scenario, the proposed model outperforms the FIC algorithm in terms of average achievable rate. The proposed

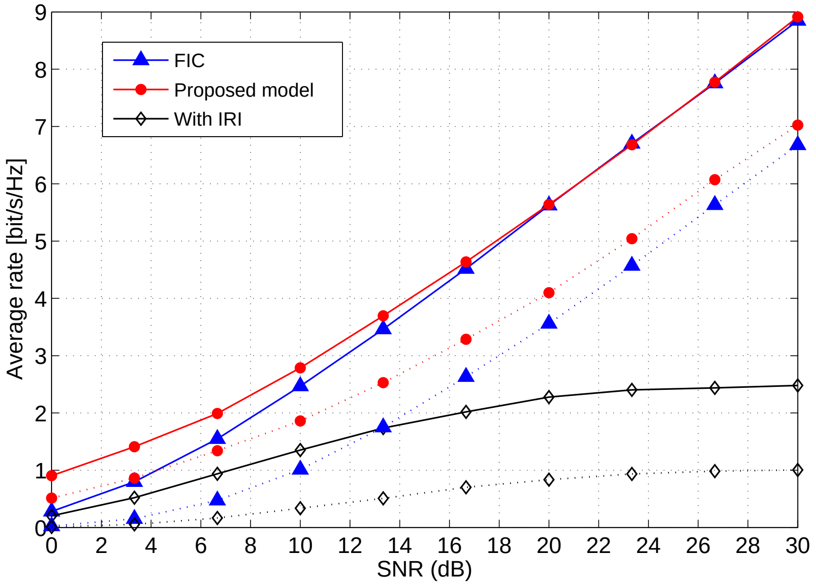


Figure 2.5: Comparison in terms of achievable average rate between the proposed model and the two-path FIC scheme for different scenarios.(solid line: with direct link, dashed line: without direct link).

model provides higher data rate based on the joint detection of PU and SU data.

The secrecy rate of the proposed model under the R-J assumption is presented in Figure 2.6 with different number of eavesdropping nodes. In this case, the optimization problem for secrecy rate maximization has been solved for $M = 3$, and the optimal values obtained have been tested against a higher number of eavesdroppers. It is clear that the proposed model provides a non-zero secrecy rate even if the number of eavesdropping nodes becomes greater than the number of eavesdropping nodes used in the optimization problem. This proves the effectiveness of the proposed model to face any increase in the number of eavesdroppers.

The effect of increasing the number of eavesdroppers M on the secrecy rate is investigated in Figure 2.7. For scenario I, results show that the secrecy rate decreases as the number of eavesdroppers increases with and without the presence

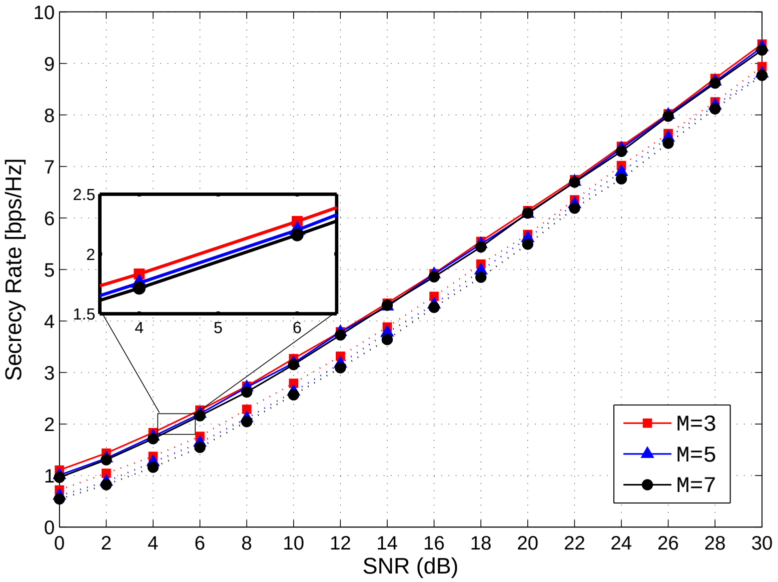


Figure 2.6: Secrecy rate of scenario I of the proposed model with multiple eavesdroppers.

of a direct link between S and E's. They also show that increasing M effects the direct link secrecy rate more than no direct link secrecy rate which can be since the eavesdroppers with a direct link get the advantage form diversity by receiving two copies of the data instead of once copy in the case of no direct link. In addition, this figure demonstrates that the secrecy rate of scenario II decreases as M increases for both direct link and no direct link cases. Results show that scenario II can achieve a non-zero secrecy rate as long as $M \leq 14$ eavesdropping nodes.

The secrecy rate of the proposed model under the assumptions of SU transmission awareness (i.e., scenario II) is investigated in Figure 2.8 against different eavesdropper channel conditions σ_{g}^2. Results show that the secrecy rate decreases as σ_{g}^2 increases which are expected due to the CSI of wiretap channel becomes bet-

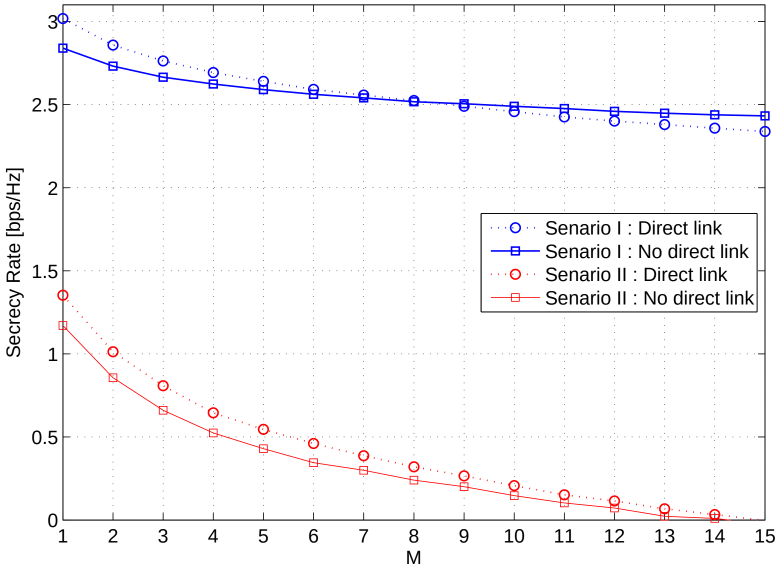


Figure 2.7: A comparison between scenario I and scenario II of the proposed model in terms of secrecy rate against the number of eavesdroppers M with SNR = 10 dB (solid line: with direct link, dashed line: with no direct link).

ter than the main channel. Moreover, this figure shows that the proposed model is still able to achieve non-zero secrecy rate at medium and high SNR regions.

The secrecy outage probability introduced in Figure 2.9 is the probability that the instantaneous secrecy rate becomes less than zero. Results show that increasing the number of eavesdroppers M increases the probability of secrecy outage, as expected. In addition, the secrecy performance of scenario I outperforms scenario II since the amount of information available for the eavesdroppers in scenario II is much higher than that of scenario I.

The proposed model BER performance with the R-J scheme is studied in Figure 2.10. Results show that the PU BER is affected by the existence of the direct link. Also, findings show that the eavesdropper BER is almost around 0.45 with no direct link between the PU source S and the eavesdroppers (i.e.,

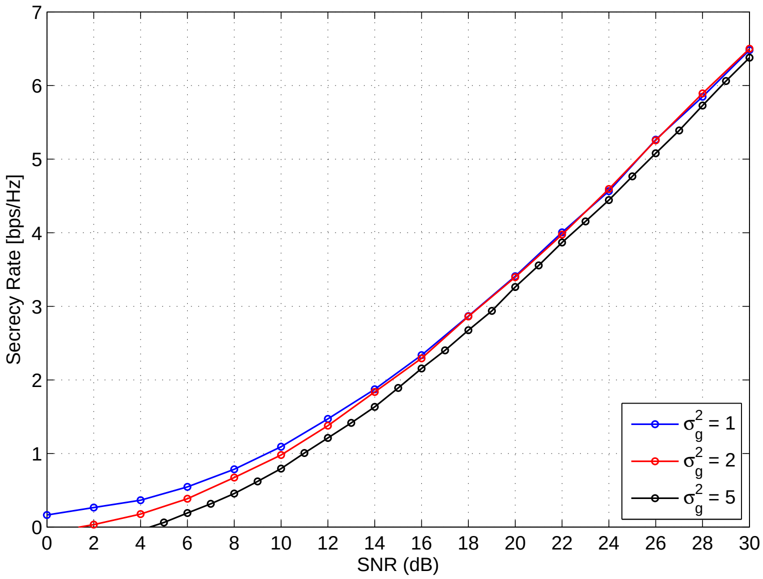


Figure 2.8: Secrecy rate for scenario II of the proposed model with multiple eavesdroppers and different values of eavesdropper channel variance σ_{g}^2.

$g_{\mathsf{SE_m}} = 0$). Furthermore, it can be seen from this figure that increasing the number of eavesdroppers slightly improves their BER performance, as expected.

The proposed model BER performance with SU transmission awareness is studied in Figure 2.11 for different values of wiretap channel variance. Results show that the eavesdropper BER performance becomes worst as the wiretap channel variance is higher due to the increase in the jamming channel matrix coefficients. These coefficients depend on the wiretap channel coefficients (i.e., $g_{\mathsf{SE_m}}$, $g_{\mathsf{AE_m}}$ and $g_{\mathsf{BE_m}}$). Since the secrecy rate maximization problem is a function in μ_1 and μ_2, the SU transmission power and relaying amplification factors are set to be equal in this case.

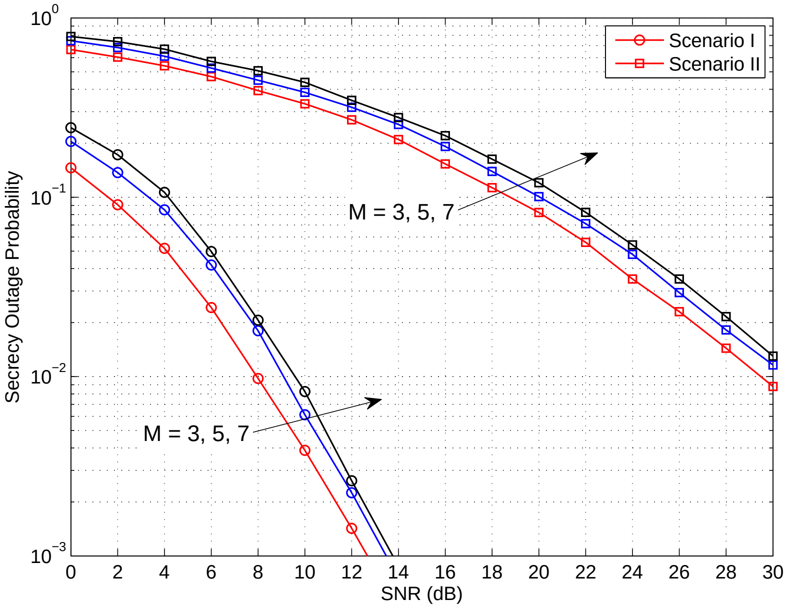


Figure 2.9: A comparison between scenario I and scenario II of the proposed model in terms of secrecy outage probability against M.

2.10 Conclusion

In this chapter, the two relay nodes in A two-path AF relaying scheme were allowed to act as a complete secondary system beside their role as relay nodes for the PU system. The goal was to fully utilize the channel bandwidth by using the IRI between the two relays to transmit the SU data. Two optimization problems were formulated to minimize the proposed system BER and to maximize the average achievable rate in terms of SU transmission power and the two amplifying factors of relays. Moreover, the cooperative CR with two-path AF relaying was investigated from the PHY security point of view. The considered model was shown to enhance the PHY security of the PU network against multiple passive eavesdroppers. Two optimization problems were formulated to maximize the

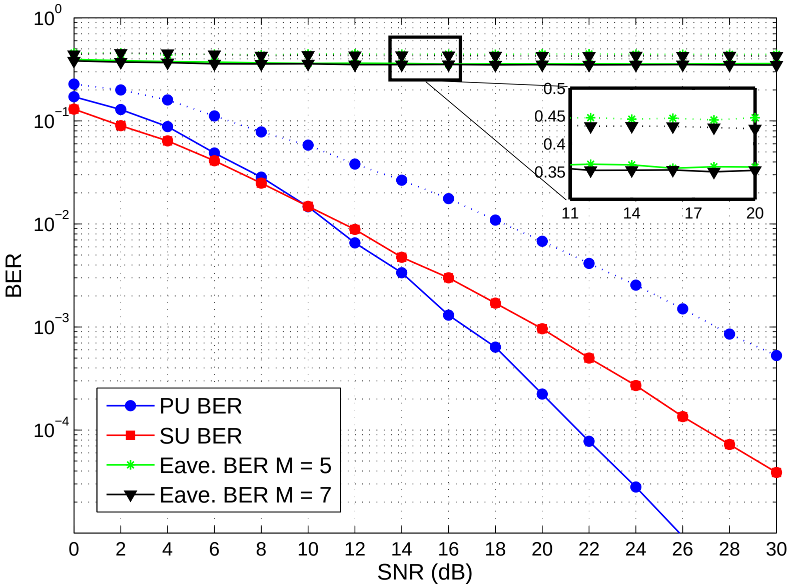


Figure 2.10: BER performance of scenario I of the proposed model with different number of eavesdroppers.

secrecy rate based on the SU transmission power, the two amplifying factors under SU transmission awareness or ignorance. Results showed that the PU and SU systems achieve diversity orders of 3 and 2, respectively with no additional complexity at the receivers. It was shown also that employing different power allocation schemes do not change the performance of the PU system, but rather has a noticeable impact on the SU system performance. Finally, the proposed model was shown to achieve higher data rate than the two-path relay model proposed in [74]. In addition, results illustrated that the considered model can achieve a non-zero secrecy rate in the presence of multiple eavesdroppers even if the CSI of the wiretap channel is better than the main channel.

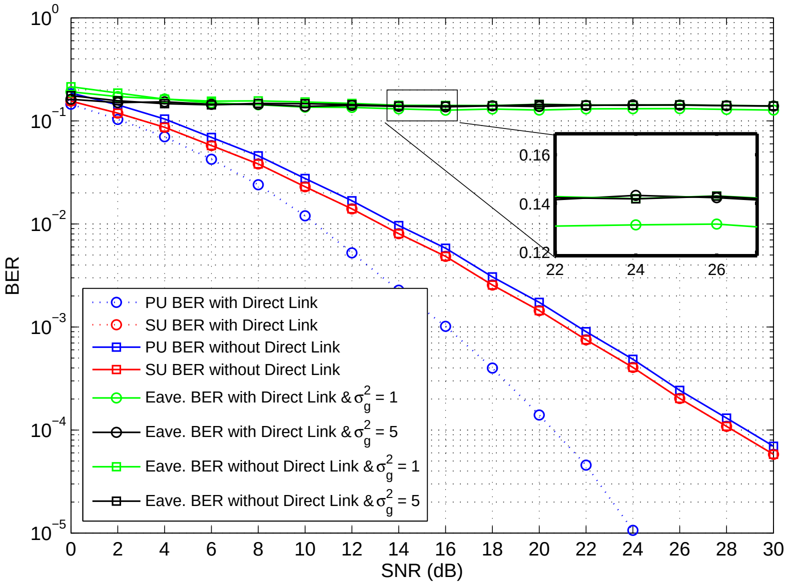


Figure 2.11: BER performance of scenario II of the proposed model with single eavesdropper node and different values of eavesdropper channel variance σ_g^2.

2.11 List of Publications

- **Ahmed H. Abd El-Malek** and Salam A. Zummo, ″A bandwidth Efficient Cognitive Radio with Two-Path Amplify-and-Forward Relaying,″ IEEE Wireless Commun. Lett., vol. 4, no. 1, pp. 6669, February 2015.

- **Ahmed H. Abd El-Malek** and Salam A. Zummo, ″Cooperative Cognitive Radio Model for Enhancing Physical Layer Security in Two-Path Amplify-and-Forward Relaying Networks,″ Accepted in the IEEE Global Commun. Conf. (GLOBECOM15), San Diego, CA, USA, December 2015.

- **Ahmed H. Abd El-Malek** and Salam A. Zummo, ″ Two-Path Amplify-and-Forward Relaying Method for Bandwidth Efficient Cognitive Radios,″ U.S. Patent and Trademark Office (USPTO), Patent Number: US 9136925, Issued, September 2015.

CHAPTER 3

BANDWIDTH EFFICIENT SCHEMES FOR COOPERATIVE TWO-WAY COGNITIVE RELAYING NETWORKS

3.1 Introduction

In this chapter, new cooperative two-way cognitive relaying schemes are proposed. In these models, a PU network consisting of two PU sources communicate with each other via a single AF relay. In addition, a SU source transmits its data to a SU destination via the same PU relay node. To mitigate the SU interference caused to PU network, the PU network considers the SU network pairs as two additional relay nodes helping the original PU relay node in improving the PU network performance. As a reward for its cooperation, the PU network allows the SU network to communicate simultaneously via the PU relay node using DF protocol. The proposed system allows the transmission of four PU symbols and one SU symbol in four/three-time slots resulting in a bandwidth efficiency of 1.25/1.67 based on the applied cooperative scheme, respectively. Two power allocation optimization problems are formulated; the first problem minimizes the weighted sum of the average SEP of both PU and SU systems, whereas the second problem maximizes the total achievable sum rate of the PU and SU networks. Lagrangian multiplier method is used to find the optimal solutions for both problems under the constraint of maximum allowable power budget. In addition, the work investigates how the proposed models improve PU PHY security performance against a single passive eavesdropper with the help of cooperative beamforming and RJ techniques.

Results show that the error performance of the proposed four-time slots cooperative schemes outperforms the conventional two-way relaying networks with AF protocol (i.e., currently existing models). Moreover, findings illustrate that the total achievable sum rate of the proposed cooperative schemes is higher than the total achievable rate of the conventional two-way model. From secrecy point of view, the proposed model achieves a non-zero secrecy rate which improves PU system security against eavesdropping attacks.

The rest of this chapter is organized as follows. Section 3.2 reviews related literature. Section 3.3 introduces the system and channel models. Section 3.4 provides the asymptotic error probability and achievable rate of the SU network. Exact and asymptotic closed-form expressions for the outage and SEP of the PU network as well as the PU achievable rate are derived in this section. Section 3.5 introduces the power allocation optimization problems that minimize the weighted sum of error probabilities of PU and SU networks for different cooperative schemes. The power allocation optimization problems for rate maximization in different cooperative schemes are presented in Section 3.6. Section 3.7 investigates the secrecy performance of the proposed cooperative schemes under two different scenarios based on the applied scheme. Numerical results and discussions are provided in Section 3.8. Finally, Section 3.9 presents some concluding remarks.

3.2 Literature Review

Two-way relay (TWR) communications are considered as promising transmission schemes to increase network throughput and improve spectrum utilization efficiency, especially for half-duplex communication models [73]. The operation of TWR model can be done over two phases; namely, multiple access (MA) phase in which the two sources transmit their data and broadcasting (BC) phase in which the relay node re-transmits the previously received data. When AF and DF relaying protocols are employed, two resulting TWR systems become known as two-phase and three-phase TWR schemes, respectively. In the two-phase scheme, the AF relaying protocol is applied where two symbols are transmitted in two-time slots (one for MA phase and one for BC phase). On the other hand, the DF relaying protocol is applied in the three-phase scheme where two symbols are transmitted in three-time slots (two for MA phase and one for BC phase) [65, 64]. Although the two-phase scheme achieves a better spectral efficiency than the three-phase scheme, the performance of the later outperforms that of the two-phase scheme.

The performance of TWR scheme with various transmission protocols and network coding schemes was investigated and analyzed in [85, 86, 87]. The effect of CCI on the performance of two-way relaying with AF protocol (TWR-AF) scheme was investigated in [88] assuming Rayleigh fading environment and in [89] assuming Nakagami-m fading environment. Closed-form expressions for outage probability and SEP were derived. Results showed that increasing the number of interfering nodes and their powers degrades the system performance dramatically.

The performance of TWR-AF scheme with multiple relay nodes was explored in [90, 91]. In [90], the authors applied the max-min criterion to employ a simpler relay selection (RS) algorithm. Results showed that the RS algorithm outperforms the all-relay participation (AP) model as the re-transmission power is concentrated in the best selected relay instead of being equally distributed among all the relays. The performance of TWR-AF scheme with and without RS was discussed in [91]. Closed-form expressions for outage probability and SEP were derived using moment generating function.

CR networks are recently considered as an effective solution to enhance bandwidth efficiency. Among the most common CR paradigms are the underlay and overlay models [52, 92]. Underlay CR paradigm allows the SU to share the spectrum with the PU at the same time under peak interference constraint to guarantee reliable communication between the PUs. As a payback for allowing the SU network to use the spectrum of the PU network, the SU network pairs (i.e., transmitter and receiver) may cooperate with the PU network in relaying the PU data, resulting in increasing PU network diversity and improving its performance. As a reward, the PU network may allow more interference power level or may dedicate a certain time slot for SU transmission [75].

The use of cooperative relaying in CR networks has been discussed in [75], in which the SU transmitter works as a relay node for the PU network which rewards the SU network by allowing a higher interference threshold if the SU works in the underlay CR mode, or by allocating a time slot to the SU node if it works in the overlay CR mode. Power allocation scheme and time division criteria have been developed for this model. The disadvantage of the proposed model in [75] is that the PU has to wait the SU for two-time slots: the first one is used to relay PU data, whereas the second slot is used to transmit SU data. Of course, this increases PU network delay and decreases its bandwidth efficiency.

PHY security is an efficient strategy to enhance secrecy in wireless communication networks due to the broadcast nature of the wireless medium and the resulting security susceptibilities [1]. The secrecy capacity was studied in [34] in the presence of a single eavesdropper and with the help of a relay node where a secrecy performance comparison was conducted between different relaying protocols (i.e. AF, DF, compress-and-forward (CF) and direct transmission (DT)). The authors in [35] examined the DF and AF relaying protocols in the presence of more than one relay in cooperation with the legitimate user. The main goal was to maximize the secrecy capacity by choosing the optimal beam-forming weights at each relay. In [37], a new PHY security scheme was proposed to enable an opportunistic selection of two relay nodes for the goal of increasing the security against eavesdropping attack. The first relay operates in a conventional mode by assisting the source to deliver its data to its destination via a DF strategy, whereas, the second relay is used to create intentional interference at the eavesdroppers. The proposed selection technique jointly protects the authorized destination against interference and eavesdropping by jamming the reception of the eavesdropper. The new approach was analyzed under different complexity requirements based on instantaneous and average knowledge of the eavesdropper channels. The work in [37] was extended in [38], in which a new scheme was proposed to enable the destination to jam the eavesdropper without creating interference at the relay during the first time slot. In the second slot, one optimally selected relay retransmits the decoded source signal to the destination, and at the same time, that particular relay cooperates with the source to jam the eavesdropper without creating interference at the destination.

Recently, the cooperation between PU and SU networks has been proposed in [76]. Two scenarios have been studied based on the knowledge of the PU message at the SU node. For each scenario, three optimization problems have been formulated: the maximization of the PU rate, the maximization of the SU rate and the maximization of the SU transmission power. For some special cases, closed-form optimal solutions have been obtained and the cooperation between PU and SU networks has been analyzed using a game theoretic approach using the Stackelberg game. In [77], an optimization problem was formulated such that the SU transmission power is distributed in order to achieve a maximum SU data rate while resulting in the highest PU secrecy rate.

Based on the aforementioned work, we can observe the impact of CR networks in enhancing wireless systems spectral efficiency. However, the non-cooperative CR networks where the SU networks do not cooperate with the PU networks might suffer from a very low allowable PU interference limit resulting in reducing SU transmission power. In addition, the SU receivers might suffer from PU interference which degrades the SU system performance specially, with low allowable SU transmission power. Therefore, cooperative CR networks might provide solutions to these problems where the cooperation between PU and SU networks could guarantee some remarkable benefits for both networks in terms of performance and or PHY security. Inspired by the advantages of cooperative CR models, this work proposed a bandwidth efficient cooperative TWR-AF scheme. The proposed system consists of a PU TWR-AF network with a single relay in the presence of SU source and destination. The SU source communicates with the SU destination through the PU relay under the assumption of no direct link and using a DF protocol. The PU relay may reward the SU network by relaying its data if the SU nodes serve as relay nodes for the PU network. The SU network aims to transmit simultaneously with the PU network which causes co-channel interference at the relay nodes. Two different cooperative models are proposed; namely, relay selection (RS) scheme and relay elimination (RE) scheme. More details on how the proposed models work are provided in Section 3.3.

The effect of SU interference is mitigated by controlling the SU transmission and relaying powers as well as the PU relaying powers. The key contribution is to control the transmission and relaying power levels at all relay nodes (i.e., PU node and the SU pairs) to achieve a minimum SEP at both cooperative networks. To do so, we formulate an optimization problem to minimize average SEP of both cooperative networks in terms of the power levels at relaying nodes. Lagrangian multiplier method is used to find the optimal values of power levels to minimize the total SEP of the proposed cooperative system under power budget constraints at each relay node as well as total power budget constraint. In addition, another power allocation problem is formulated to maximize the total achievable sum rate of both PU and SU networks in terms of transmission and relying power levels under the same constraint of total power budget. Finally, the PHY security of the proposed cooperative TWR-AF model is investigated based on the relay-and-jamming (R-J) scenario.

The main contribution of this chapter is the proposing of new cooperative TWR-AF cognitive schemes in which the SU network cooperates with PU network in relaying the PU data. As a reward for its cooperation, the SU source is allowed to use the PU relay node to transmit SU data to the SU destination. The new proposed schemes achieve a better bandwidth efficiency compared to conventional TWR-AF network presented in [88]. Closed-form mathematical formulas are derived for the performance metrics of the two cooperative schemes. Finally, the work investigates the three different proposed cooperative schemes from the PHY security viewpoint by showing that the new schemes can achieve a non-zero secrecy rate in the presence of a single passive eavesdropper.

3.3 System and Channel Models

In this section, the proposed TWR-AF model consists of two PU nodes X and Y communicate with each other via a PU relay R in the presence of SU transmitter A and SU receiver B. It is assumed that all the nodes are equipped with a single antenna and operated in half-duplex mode. Since there is no direct link between the SU source A and the SU destination B, the SU source A might ask the PU relay R to transmit the SU data to the destination B. The PU network might agree to help the SU network as a reward for the SU network cooperation when it serves as two extra relays for the PU transmission. The proposed system is presented for two different transmission schemes namely; RS and RE schemes. In both schemes, the channel coefficient between X and R is denoted by g_{XR}, and the channel coefficients between X and A and B are denoted by g_{XA} and g_{XB}, respectively with an average of γ_{g}. Similarly, the channel coefficients between Y

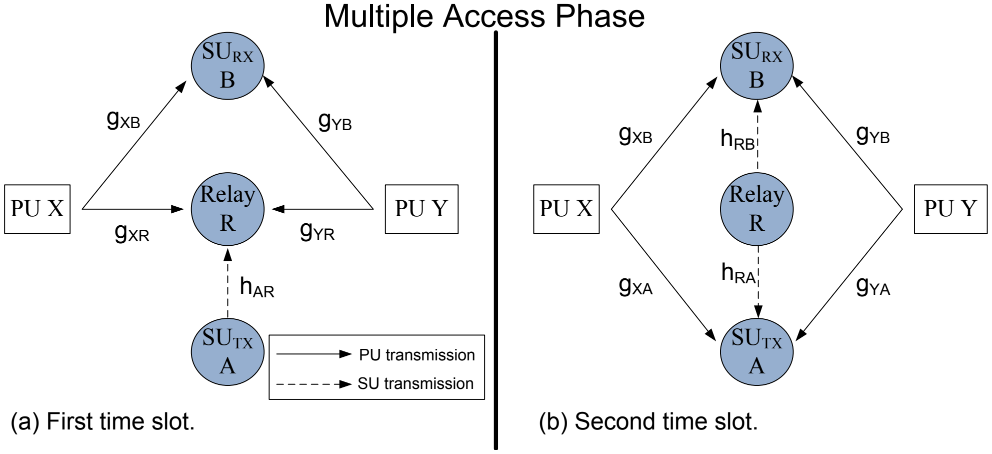


Figure 3.1: Multiple access phase of the proposed cooperative TWR-AF relaying scheme.

and R, A and B are denoted by g_{YR}, g_{YA} and g_{YB}, respectively with an average of γ_{g}. The channel coefficient between A and R is h_{AR} with an average of γ_{h}. Finally, the channel coefficient between R and B is h_{RB} with an average of γ_{h}. It is important to clarify that due to the half-duplex communication mode and the simultaneous transmission of both PU nodes, there is no direct link between the PU nodes (i.e., X and Y). For notational simplicity, all the channels are assumed to be i.i.d. and to follow Rayleigh fading distribution. During PU transmission, AF protocol is applied by the three relays since it is less complex and more flexible in handling interference than DF protocol [74]. While for SU transmission, DF protocol is applied by the PU relay node R in order to reduce the effect of SU transmission interference at the PU receivers. The communications of the proposed scheme take place over two phases (i.e., MA and BC). These two phases for both cooperative schemes are discussed in details as follows:

3.3.1 Multiple Access (MA) Phase

For both cooperative schemes, the MA phase is identical as shown in Figure 3.1. During the first time slot, PU sources X and Y transmit their modulated symbols denoted by x_1 and y_1 with transmission powers of P_{X} and P_{Y}, respectively. At the same time, SU source A transmits its data a_1 with a transmission power P_{A} which interferes with PU data at R. Since there is no direct link between the SU network pairs A and B, the SU receiver B receives the PU transmissions with no interference. Then, the received signals at R and B are, respectively given by

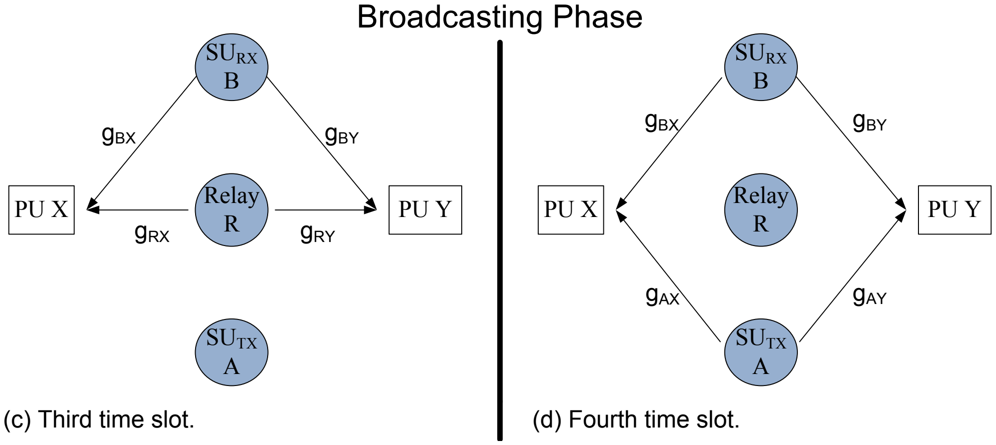
$$z_{\mathsf{R}}^{(1)} = \sqrt{P_{\mathsf{X}}} g_{\mathsf{XR}} x_1 + \sqrt{P_{\mathsf{Y}}} g_{\mathsf{YR}} y_1 + \sqrt{P_{\mathsf{A}}} h_{\mathsf{AR}} a_1 + w_{\mathsf{R}}^{(1)}, \tag{3.1}$$

$$z_{\mathsf{B}}^{(1)} = \sqrt{P_{\mathsf{X}}} g_{\mathsf{XB}} x_1 + \sqrt{P_{\mathsf{Y}}} g_{\mathsf{YB}} y_1 + w_{\mathsf{B}}^{(1)}, \tag{3.2}$$

where w_{R} and w_{B} are AWGN samples with zero-mean and variance σ_0^2.

During the second time slot, PU sources X and Y transmit their second PU symbols x_2 and y_2 with transmission powers of P_{X} and P_{Y}, respectively to A and B. Simultaneously, the relay R jointly decodes the previously received SU data symbol $\widehat{a}_1$ and re-transmits it to the SU receiver B with a transmission power P_{R}. Then, the received signals at A and B are given by

$$z_{\mathsf{A}}^{(2)} = \sqrt{P_{\mathsf{X}}} g_{\mathsf{XA}} x_2 + \sqrt{P_{\mathsf{Y}}} g_{\mathsf{YA}} y_2 + \sqrt{P_{\mathsf{R}}} h_{\mathsf{RA}} \widehat{a}_1 + w_{\mathsf{A}}^{(2)}, \tag{3.3}$$



(c) Third time slot.

(d) Fourth time slot.

Figure 3.2: Broadcasting phase of the proposed cooperative TWR-AF relaying scheme.

$$z_{\mathsf{B}}^{(2)} = \sqrt{P_{\mathsf{X}}} g_{\mathsf{XB}} x_2 + \sqrt{P_{\mathsf{Y}}} g_{\mathsf{YB}} y_2 + \sqrt{P_{\mathsf{R}}} h_{\mathsf{RB}} \widehat{a}_1 + w_{\mathsf{B}}^{(2)}, \tag{3.4}$$

where w_{A} and w_{B} are AWGN samples with zero-mean and variance σ_0^2. By the end of the MA phase, the SU transmission is completed. The SU receiver B decodes the transmitted symbol $\widehat{a}_1$ from R which is denoted by $\widehat{\widehat{a}}_1$.

3.3.2 Broadcasting (BC) Phase

For the BC phase, the two cooperative schemes operate differentially. In the RS scheme, the best relay is selected to re-transmit the PU data via min-max criterion [90] for a two-time slots BC phase. Whereas the RE scheme eliminates the worst relay among all the three relays for a single time slot BC phase. Hence, the cooperative TWR-AF model with RS scheme transmits five data symbols (i.e., four PU symbols and one SU symbol) in four-time slots achieving a bandwidth efficiency of 1.25. On the other hand, the cooperative TWR-AF model with

RE scheme transmits the same five data symbols in three-time slots achieving a bandwidth efficiency of 1.67. The BC phase for both RS and RE scheme is described as follows:

3.3.2.1 AP Scheme

The BC phase operations for the AP scheme is introduced in Figure 3.2. During the third time slot, PU and SU sources are idle while R transmits the received signal after trying to remove the interfered SU data a_1 by subtracting the decoded SU symbol at R (i.e., $\widehat{a}_1$) from the received signal $z_{\mathsf{R}}^{(1)}$. On the other hand, the SU receiver B decodes the interfered SU data during the second time slot and applies AF protocol to the remaining signal. Under the assumption of knowing CSI by all relay nodes and destinations, the received signals at X and Y during the third time slot are given by

$$z_{\mathsf{X}}^{(3)} = g_{\mathsf{RX}}\beta_{\mathsf{R}}\left(z_{\mathsf{R}}^{(1)} - \sqrt{P_{\mathsf{A}}}h_{\mathsf{AR}}\widehat{a}_1\right) + g_{\mathsf{BX}}\beta_{\mathsf{B}_2}\left(z_{\mathsf{B}}^{(2)} - \sqrt{P_{\mathsf{R}}}h_{\mathsf{RB}}\widehat{\widehat{a}}_1\right) + w_{\mathsf{X}}^{(3)}, \tag{3.5}$$

$$z_{\mathsf{Y}}^{(3)} = g_{\mathsf{RY}}\beta_{\mathsf{R}}\left(z_{\mathsf{R}}^{(1)} - \sqrt{P_{\mathsf{A}}}h_{\mathsf{AR}}\widehat{a}_1\right) + g_{\mathsf{BY}}\beta_{\mathsf{B}_2}\left(z_{\mathsf{B}}^{(2)} - \sqrt{P_{\mathsf{R}}}h_{\mathsf{RB}}\widehat{\widehat{a}}_1\right) + w_{\mathsf{Y}}^{(3)} \tag{3.6}$$

where w_{X} and w_{Y} are AWGN samples with zero-mean and variance σ_0^2. The normalized amplification coefficient at R and B are given by $\beta_{\mathsf{R}}^2 = \frac{\lambda_R}{z_{\mathsf{R}}^{(1)}}$ and $\beta_{\mathsf{B}_2}^2 = \frac{\lambda_{B_2}}{z_{\mathsf{B}}^{(2)}}$, respectively.

During the fourth time slot, PU sources and the PU relay node (i.e., X, Y and R) are idle while the SU nodes A and B re-transmit the previously received PU data. Using orthogonal space time block code (OSTBC) technique, The SU source

A performs a self-interference cancellation for its own data a_1 from the received signal during second time slot (i.e., Z_{A}^{2}), then applies AF protocol to the resultant signal before re-transmitting it to both PU destinations X and Y. On the other hand, the SU destination B applies AF protocol to the previously received signal during the first time slot (i.e., Z_{B}^{2}) before re-transmitting to PU destinations X and Y. The received signals at both PU destinations X and Y during the fourth time slot are given by

$$z_{\mathsf{X}}^{(4)} = g_{\mathsf{BX}}\beta_{\mathsf{B}_1}\left(z_{\mathsf{B}}^{(1)}\right)^{*} - g_{\mathsf{AX}}\beta_{\mathsf{A}}\left(z_{\mathsf{A}}^{(2)} - \sqrt{P_{\mathsf{R}}}h_{\mathsf{RA}}a_1\right)^{*} + w_{\mathsf{X}}^{(4)}, \tag{3.7}$$

$$z_{\mathsf{Y}}^{(4)} = g_{\mathsf{BY}}\beta_{\mathsf{B}_1}\left(z_{\mathsf{B}}^{(1)}\right)^{*} - g_{\mathsf{AY}}\beta_{\mathsf{A}}\left(z_{\mathsf{A}}^{(2)} - \sqrt{P_{\mathsf{R}}}h_{\mathsf{RA}}a_1\right)^{*} + w_{\mathsf{Y}}^{(4)}, \tag{3.8}$$

where w_{X} and w_{Y} are AWGN samples with zero-mean and variance σ_0^2. The normalized amplification coefficients at A and B are given by $\beta_{\mathsf{A}}^2 = \frac{\lambda_A}{z_{\mathsf{A}}^{(2)}}$ and $\beta_{\mathsf{B}_1}^2 = \frac{\lambda_{B_1}}{z_{\mathsf{B}}^{(1)}}$, respectively.

After the completion of the proposed system phases, the PU nodes apply self-interference cancellation on their received signals to remove their own data before decoding process. Then, the received signals at both X and Y during the third time slot after self-interference cancellation are given by

$$\tilde{z}_{\mathsf{X}}^{(3)} = z_{\mathsf{X}}^{(3)} - \sqrt{P_{\mathsf{X}}}g_{\mathsf{XR}}x_1 - \sqrt{P_{\mathsf{X}}}g_{\mathsf{XB}}x_2, \tag{3.9}$$

$$\tilde{z}_{\mathsf{Y}}^{(3)} = z_{\mathsf{Y}}^{(3)} - \sqrt{P_{\mathsf{Y}}}g_{\mathsf{YR}}y_1 - \sqrt{P_{\mathsf{Y}}}g_{\mathsf{YB}}y_2. \tag{3.10}$$

Following the same above-mentioned discussion, the received signals at both X

and Y during the fourth time slot after self-interference cancellation are given by

$$\widetilde{z}_{\mathsf{X}}^{(4)} = z_{\mathsf{X}}^{(4)} - \left(\sqrt{P_{\mathsf{X}}} g_{\mathsf{XB}} x_1\right)^* + \left(\sqrt{P_{\mathsf{X}}} g_{\mathsf{XA}} x_2\right)^*, \tag{3.11}$$

$$\widetilde{z}_{\mathsf{Y}}^{(4)} = z_{\mathsf{Y}}^{(4)} - \left(\sqrt{P_{\mathsf{Y}}} g_{\mathsf{YB}} y_1\right)^* + \left(\sqrt{P_{\mathsf{Y}}} g_{\mathsf{YA}} y_2\right)^*. \tag{3.12}$$

From the previous equations and the presence of two PU destinations in this model, the matrix model for the proposed system at PU node X can be written as

$$\widetilde{\mathbf{z}}_{\mathsf{X}} = \mathbf{G}_{\mathsf{X}} \mathbf{y} + \widetilde{\mathbf{w}}_{\mathsf{X}}, \tag{3.13}$$

where $\widetilde{\mathbf{z}}_{\mathsf{X}} = \left[\widetilde{z}_{\mathsf{X}}^{(3)}, \widetilde{z}_{\mathsf{X}}^{(4)*}\right]^T$, $\mathbf{y} = [y_1, y_2]^T$, the channel matrix $\mathbf{G}_{\mathsf{X}}$ is given by

$$\mathbf{G}_{\mathsf{X}} = \begin{bmatrix} \beta_{\mathsf{R}} g_{\mathsf{RX}} g_{\mathsf{YR}} & \beta_{\mathsf{B}_2} g_{\mathsf{BX}} g_{\mathsf{YB}} \\ \beta_{\mathsf{B}_1} g_{\mathsf{BX}}^* g_{\mathsf{YB}} & -\beta_{\mathsf{A}} g_{\mathsf{AX}}^* g_{\mathsf{YA}} \end{bmatrix}, \tag{3.14}$$

and the noise vector at X is given by

$$\widetilde{\mathbf{w}}_{\mathsf{X}} = \begin{bmatrix} \beta_{\mathsf{R}} g_{\mathsf{RX}} \left(\sqrt{P_{\mathsf{A}}} h_{\mathsf{AR}} \left(a_1 - \widehat{a}_1\right) + w_{\mathsf{R}}^{(1)}\right) + \beta_{\mathsf{B}_2} g_{\mathsf{BX}} \left(\sqrt{P_{\mathsf{R}}} h_{\mathsf{RB}} \left(\widehat{a}_1 - \widehat{\widehat{a}}_1\right) + w_{\mathsf{B}}^{(2)}\right) + w_{\mathsf{X}}^{(3)} \\ \beta_{\mathsf{B}_1} g_{\mathsf{BX}} w_{\mathsf{B}}^{(1)*} - \beta_{\mathsf{A}} g_{\mathsf{AX}} \left(\sqrt{P_{\mathsf{R}}} h_{\mathsf{RA}} \left(\widehat{a}_1 - a_1\right) + w_{\mathsf{A}}^{(2)}\right)^* + w_{\mathsf{X}}^{(4)} \end{bmatrix}. \tag{3.15}$$

Similarly, the matrix model for the proposed system at PU node Y can be written as

$$\widetilde{\mathbf{z}}_{\mathsf{Y}} = \mathbf{G}_{\mathsf{Y}}\mathbf{x} + \widetilde{\mathbf{w}}_{\mathsf{Y}}, \tag{3.16}$$

where $\widetilde{\mathbf{z}}_{\mathsf{Y}} = \left[\widetilde{z}_{\mathsf{Y}}^{(3)}, \widetilde{z}_{\mathsf{Y}}^{(4)*}\right]^T$, $\mathbf{y} = [x_1, x_2]^T$, the channel matrix $\mathbf{G}_{\mathsf{Y}}$ is given by

$$\mathbf{G}_{\mathsf{Y}} = \begin{bmatrix} \beta_{\mathsf{R}} g_{\mathsf{RY}} g_{\mathsf{XR}} & \beta_{\mathsf{B}_2} g_{\mathsf{BY}} g_{\mathsf{XB}} \\ \beta_{\mathsf{B}_1} g_{\mathsf{BY}}^{*} g_{\mathsf{XB}} & -\beta_{\mathsf{A}} g_{\mathsf{AY}}^{*} g_{\mathsf{XA}} \end{bmatrix}, \tag{3.17}$$

and the noise vector at Y is given by

$$\widetilde{\mathbf{w}}_{\mathsf{Y}} = \\ \begin{bmatrix} \beta_{\mathsf{R}} g_{\mathsf{RY}} \left(\sqrt{P_{\mathsf{A}}} h_{\mathsf{AR}} \left(a_1 - \widehat{a}_1\right) + w_{\mathsf{R}}^{(1)}\right) + \beta_{\mathsf{B}_2} g_{\mathsf{BY}} \left(\sqrt{P_{\mathsf{R}}} h_{\mathsf{RB}} \left(\widehat{a}_1 - \widehat{\widehat{a}}_1\right) + w_{\mathsf{B}}^{(2)}\right) + w_{\mathsf{Y}}^{(3)} \\ \beta_{\mathsf{B}_1} g_{\mathsf{BY}} w_{\mathsf{B}}^{(1)*} - \beta_{\mathsf{A}} g_{\mathsf{AY}} \left(\sqrt{P_{\mathsf{R}}} h_{\mathsf{RA}} \left(\widehat{a}_1 - a_1\right) + w_{\mathsf{A}}^{(2)}\right)^{*} + w_{\mathsf{Y}}^{(4)} \end{bmatrix}. \tag{3.18}$$

3.3.2.2 RS Scheme

In this scheme, the min-max relay selection algorithm in [90] is used to find the best relay during the BC phase. Since the two PU data pairs (i.e., (x_1, y_1) and (x_2, y_2)) are available at two different relays (i.e., (x_1, y_1) at (R, B) and (x_2, y_2) at (A, B)). Then, during the third time slot, and after removing the interfered SU data symbol via joint detection, the best relay is selected between the nodes R and B to re-transmit PU first symbols (i.e., (x_1, y_1)) using the min-max selection criterion presented in [90]. Hence, the received signals at X and Y are, respectively given by

$$z_{\mathsf{X}}^{(3)} = \begin{cases} g_{\mathsf{RX}}\beta_{\mathsf{R}}\left(z_{\mathsf{R}}^{(1)} - \sqrt{P_{\mathsf{A}}}h_{\mathsf{AR}}\widehat{a}_1\right) + w_{\mathsf{X}}^{(3)}, & \text{if} \quad \min\left(\left|g_{\mathsf{RX}}\right|^2, \left|g_{\mathsf{RY}}\right|^2\right) > \min\left(\left|g_{\mathsf{BX}}\right|^2, \left|g_{\mathsf{BY}}\right|^2\right) \\ g_{\mathsf{BX}}\beta_{\mathsf{B}_1} z_{\mathsf{B}}^{(1)} + w_{\mathsf{X}}^{(3)}, & \text{if} \quad \min\left(\left|g_{\mathsf{RX}}\right|^2, \left|g_{\mathsf{RY}}\right|^2\right) < \min\left(\left|g_{\mathsf{BX}}\right|^2, \left|g_{\mathsf{BY}}\right|^2\right) \end{cases}, \tag{3.19}$$

$$z_{\mathsf{Y}}^{(3)} = \begin{cases} g_{\mathsf{RY}}\beta_{\mathsf{R}}\left(z_{\mathsf{R}}^{(1)} - \sqrt{P_{\mathsf{A}}}h_{\mathsf{AR}}\widehat{a}_1\right) + w_{\mathsf{Y}}^{(3)}, & \text{if} \quad \min\left(\left|g_{\mathsf{RX}}\right|^2, \left|g_{\mathsf{RY}}\right|^2\right) > \min\left(\left|g_{\mathsf{BX}}\right|^2, \left|g_{\mathsf{BY}}\right|^2\right) \\ g_{\mathsf{BY}}\beta_{\mathsf{B}_1} z_{\mathsf{B}}^{(1)} + w_{\mathsf{Y}}^{(3)}, & \text{if} \quad \min\left(\left|g_{\mathsf{RX}}\right|^2, \left|g_{\mathsf{RY}}\right|^2\right) < \min\left(\left|g_{\mathsf{BX}}\right|^2, \left|g_{\mathsf{BY}}\right|^2\right) \end{cases}, \tag{3.20}$$

where $\beta_{\mathsf{R}} = \frac{\lambda_{\mathsf{R}} P_{\mathsf{s}}}{z_{\mathsf{R}}^{(1)}}$, $\beta_{\mathsf{B}_1} = \frac{\lambda_{\mathsf{B}_1} P_{\mathsf{s}}}{z_{\mathsf{B}}^{(1)}}$, $w_{\mathsf{X}}^{(3)}$ and $w_{\mathsf{Y}}^{(3)}$ denote the AWGN samples at PU nodes X and Y, respectively during the third time slot. After applying self-interference cancellation at each PU node, the received signals at PU nodes X and Y are, respectively given by

$$\widetilde{z}_{\mathsf{X}}^{(3)} = \begin{cases} z_{\mathsf{X}}^{(3)} - \sqrt{P_{\mathsf{X}}} g_{\mathsf{XR}} x_1, & \text{if} \quad \min\left(\left|g_{\mathsf{RX}}\right|^2, \left|g_{\mathsf{RY}}\right|^2\right) > \min\left(\left|g_{\mathsf{BX}}\right|^2, \left|g_{\mathsf{BY}}\right|^2\right) \\ z_{\mathsf{X}}^{(3)} - \sqrt{P_{\mathsf{X}}} g_{\mathsf{XB}} x_1, & \text{if} \quad \min\left(\left|g_{\mathsf{RX}}\right|^2, \left|g_{\mathsf{RY}}\right|^2\right) < \min\left(\left|g_{\mathsf{BX}}\right|^2, \left|g_{\mathsf{BY}}\right|^2\right) \end{cases}, \tag{3.21}$$

$$\widetilde{z}_{\mathsf{Y}}^{(3)} = \begin{cases} z_{\mathsf{Y}}^{(3)} - \sqrt{P_{\mathsf{Y}}} g_{\mathsf{YR}} y_1, & \text{if} \quad \min\left(|g_{\mathsf{RX}}|^2, |g_{\mathsf{RY}}|^2\right) > \min\left(|g_{\mathsf{BX}}|^2, |g_{\mathsf{BY}}|^2\right) \\ z_{\mathsf{Y}}^{(3)} - \sqrt{P_{\mathsf{Y}}} g_{\mathsf{YB}} y_1, & \text{if} \quad \min\left(|g_{\mathsf{RX}}|^2, |g_{\mathsf{RY}}|^2\right) < \min\left(|g_{\mathsf{BX}}|^2, |g_{\mathsf{BY}}|^2\right) \end{cases}, \tag{3.22}$$

which can be, respectively represented as

$$\widetilde{z}_{\mathsf{X}}^{(3)} = \sqrt{P_{\mathsf{Y}}} g_{\mathsf{iX}} \beta_{\mathsf{i}} g_{\mathsf{Yi}} y_1 + \widetilde{w}_{\mathsf{Xi}}^{(3)}, \tag{3.23}$$

$$\widetilde{z}_{\mathsf{Y}}^{(3)} = \sqrt{P_{\mathsf{X}}} g_{\mathsf{iY}} \beta_{\mathsf{i}} g_{\mathsf{Xi}} x_1 + \widetilde{w}_{\mathsf{Yi}}^{(3)}, \tag{3.24}$$

where $\mathsf{i} \in \{\mathsf{R}, \mathsf{B}\}$ represents the selected relay between R and B. While $\widetilde{w}_{\mathsf{Xi}}^{(3)}$ and $\widetilde{w}_{\mathsf{Yi}}^{(3)}$ denote the AWGN samples at X and Y, respectively in addition to the SU interference signal due to incorrect decoding at relays.

Similarly, during the fourth time slot, the min-max criterion is applied to select the best relay between A and B to re-transmit PU second symbols (i.e., (x_2, y_2)). Hence, the received signals at X and Y are, respectively given by

$$z_{\mathsf{X}}^{(4)} = \begin{cases} g_{\mathsf{AX}} \beta_{\mathsf{A}} \left(z_{\mathsf{A}}^{(2)} - \sqrt{P_{\mathsf{R}}} h_{\mathsf{RA}} a_1\right) + w_{\mathsf{X}}^{(4)}, & \text{if} \quad \min\left(|g_{\mathsf{AX}}|^2, |g_{\mathsf{AY}}|^2\right) > \min\left(|g_{\mathsf{BX}}|^2, |g_{\mathsf{BY}}|^2\right) \\ g_{\mathsf{BX}} \beta_{\mathsf{B}_2} \left(z_{\mathsf{B}}^{(2)} - \sqrt{P_{\mathsf{R}}} h_{\mathsf{RB}} \widehat{\widehat{a}}_1\right) + w_{\mathsf{X}}^{(4)}, & \text{if} \quad \min\left(|g_{\mathsf{AX}}|^2, |g_{\mathsf{AY}}|^2\right) < \min\left(|g_{\mathsf{BX}}|^2, |g_{\mathsf{BY}}|^2\right) \end{cases}, \tag{3.25}$$

$$z_{\mathsf{Y}}^{(4)} = \left\{ \begin{array}{ll} g_{\mathsf{AY}}\beta_{\mathsf{A}}\left(z_{\mathsf{A}}^{(2)} - \sqrt{P_{\mathsf{R}}}h_{\mathsf{RA}}a_1\right) + w_{\mathsf{Y}}^{(4)}, & \text{if} \quad \min\left(|g_{\mathsf{AX}}|^2, |g_{\mathsf{AY}}|^2\right) > \min\left(|g_{\mathsf{BX}}|^2, |g_{\mathsf{BY}}|^2\right) \\ g_{\mathsf{BY}}\beta_{\mathsf{B}_2}\left(z_{\mathsf{B}}^{(2)} - \sqrt{P_{\mathsf{R}}}h_{\mathsf{RB}}\widehat{\widehat{a}}_1\right) + w_{\mathsf{Y}}^{(4)}, & \text{if} \quad \min\left(|g_{\mathsf{AX}}|^2, |g_{\mathsf{AY}}|^2\right) < \min\left(|g_{\mathsf{BX}}|^2, |g_{\mathsf{BY}}|^2\right) \end{array} \right., \tag{3.26}$$

where $\beta_{\mathsf{A}} = \frac{\lambda_{\mathsf{A}} P_{\mathsf{s}}}{z_{\mathsf{A}}^{(2)}}$, $\beta_{\mathsf{B}_2} = \frac{\lambda_{\mathsf{B}_2} P_{\mathsf{s}}}{z_{\mathsf{B}}^{(2)}}$, $w_{\mathsf{X}}^{(4)}$ and $w_{\mathsf{Y}}^{(4)}$ denote the AWGN samples at PU nodes X and Y, respectively during the fourth time slot. After applying self-interference cancellation at each PU node, the received signals at X and Y are, respectively given by

$$\widetilde{z}_{\mathsf{X}}^{(4)} = \left\{ \begin{array}{ll} z_{\mathsf{X}}^{(4)} - \sqrt{P_{\mathsf{X}}}g_{\mathsf{XA}}x_2, & \text{if} \quad \min\left(|g_{\mathsf{AX}}|^2, |g_{\mathsf{AY}}|^2\right) > \min\left(|g_{\mathsf{BX}}|^2, |g_{\mathsf{BY}}|^2\right) \\ z_{\mathsf{X}}^{(4)} - \sqrt{P_{\mathsf{X}}}g_{\mathsf{XB}}x_2, & \text{if} \quad \min\left(|g_{\mathsf{AX}}|^2, |g_{\mathsf{AY}}|^2\right) < \min\left(|g_{\mathsf{BX}}|^2, |g_{\mathsf{BY}}|^2\right) \end{array} \right., \tag{3.27}$$

$$\widetilde{z}_{\mathsf{Y}}^{(4)} = \left\{ \begin{array}{ll} z_{\mathsf{Y}}^{(4)} - \sqrt{P_{\mathsf{Y}}}g_{\mathsf{YA}}y_2, & \text{if} \quad \min\left(|g_{\mathsf{AX}}|^2, |g_{\mathsf{AY}}|^2\right) > \min\left(|g_{\mathsf{BX}}|^2, |g_{\mathsf{BY}}|^2\right) \\ z_{\mathsf{Y}}^{(4)} - \sqrt{P_{\mathsf{Y}}}g_{\mathsf{YB}}y_2, & \text{if} \quad \min\left(|g_{\mathsf{AX}}|^2, |g_{\mathsf{AY}}|^2\right) < \min\left(|g_{\mathsf{BX}}|^2, |g_{\mathsf{BY}}|^2\right) \end{array} \right., \tag{3.28}$$

which can be, respectively represented as

$$\widetilde{z}_{\mathsf{X}}^{(4)} = \sqrt{P_{\mathsf{Y}}}g_{\mathsf{jX}}\beta_{\mathsf{j}}g_{\mathsf{Yj}}y_2 + \widetilde{w}_{\mathsf{Xj}}^{(4)}, \tag{3.29}$$

$$\widetilde{z}_{\mathsf{Y}}^{(4)} = \sqrt{P_{\mathsf{X}}}g_{\mathsf{jY}}\beta_{\mathsf{j}}g_{\mathsf{Xj}}x_2 + \widetilde{w}_{\mathsf{Yj}}^{(4)}, \tag{3.30}$$

where $\mathsf{j} \in \{\mathsf{A}, \mathsf{B}\}$ represents the selected relay between A and B. While $\widetilde{w}_{\mathsf{Xj}}^{(4)}$ and $\widetilde{w}_{\mathsf{Yj}}^{(4)}$ denote the AWGN samples at X and Y, respectively in addition to the SU interference signal due to incorrect decoding at relays.

3.3.2.3 RE Scheme

In this scheme, the worst relay among the three relays (i.e., R, A and B) is eliminated during the BC phase. Since each one of PU symbols is available at two of the three relays, the elimination of the worst relay will not cause any data loss. Then, the other two relays re-transmit their previously received PU symbols simultaneously. Noted that, the two relays transmissions should be different than each other. In order to understand RE scheme, we give the following example. For instance, after the MA phase, the PU data symbols (x_1, y_1) are available at the two relays R and B during the first time slot. Whereas, the PU data symbols (x_2, y_2) are available at the two relays A and B. If the eliminated relay was A, relay R would re-transmit PU symbols (x_1, y_1), while relay B would re-transmit PU symbols (x_2, y_2), simultaneously. Hence, the received signals at X and Y during the third time slots are, respectively given by

$$z_{\mathsf{X}}^{(3)} = \begin{cases} g_{\mathsf{RX}}\beta_{\mathsf{R}}\left(z_{\mathsf{R}}^{(1)} - \sqrt{P_{\mathsf{A}}}h_{\mathsf{AR}}\widehat{a}_1\right) + g_{\mathsf{BX}}\beta_{\mathsf{B}_2}\left(z_{\mathsf{B}}^{(2)} - \sqrt{P_{\mathsf{R}}}h_{\mathsf{RB}}\widehat{\widehat{a}}_1\right) + w_{\mathsf{X}}^{(3)}, & \text{if} \quad A \text{ is the worst} \\ g_{\mathsf{RX}}\beta_{\mathsf{R}}\left(z_{\mathsf{R}}^{(1)} - \sqrt{P_{\mathsf{A}}}h_{\mathsf{AR}}\widehat{a}_1\right) + g_{\mathsf{AX}}\beta_{\mathsf{A}}\left(z_{\mathsf{A}}^{(2)} - \sqrt{P_{\mathsf{R}}}h_{\mathsf{RA}}a_1\right) + w_{\mathsf{X}}^{(3)}, & \text{if} \quad B \text{ is the worst} \\ g_{\mathsf{BX}}\beta_{\mathsf{B}_1}z_{\mathsf{B}}^{(1)} + g_{\mathsf{AX}}\beta_{\mathsf{A}}\left(z_{\mathsf{A}}^{(2)} - \sqrt{P_{\mathsf{R}}}h_{\mathsf{RA}}a_1\right) + w_{\mathsf{X}}^{(3)}, & \text{if} \quad R \text{ is the worst} \end{cases}, \tag{3.31}$$

$$
z_{\mathsf{Y}}^{(3)} =
$$

$$
\begin{cases} g_{\mathsf{RY}}\beta_{\mathsf{R}}\left(z_{\mathsf{R}}^{(1)} - \sqrt{P_{\mathsf{A}}}h_{\mathsf{AR}}\widehat{a}_1\right) + g_{\mathsf{By}}\beta_{\mathsf{B}_2}\left(z_{\mathsf{B}}^{(2)} - \sqrt{P_{\mathsf{R}}}h_{\mathsf{RB}}\widehat{\widehat{a}}_1\right) + w_{\mathsf{Y}}^{(3)}, & \text{if} \quad A \text{ is the worst} \\ g_{\mathsf{RY}}\beta_{\mathsf{R}}\left(z_{\mathsf{R}}^{(1)} - \sqrt{P_{\mathsf{A}}}h_{\mathsf{AR}}\widehat{a}_1\right) + g_{\mathsf{AY}}\beta_{\mathsf{A}}\left(z_{\mathsf{A}}^{(2)} - \sqrt{P_{\mathsf{R}}}h_{\mathsf{RA}}a_1\right) + w_{\mathsf{Y}}^{(3)}, & \text{if} \quad B \text{ is the worst} \\ g_{\mathsf{BY}}\beta_{\mathsf{B}_1}z_{\mathsf{B}}^{(1)} + g_{\mathsf{AY}}\beta_{\mathsf{A}}\left(z_{\mathsf{A}}^{(2)} - \sqrt{P_{\mathsf{R}}}h_{\mathsf{RA}}a_1\right) + w_{\mathsf{Y}}^{(3)}, & \text{if} \quad R \text{ is the worst} \end{cases},
\tag{3.32}
$$

Then, the received signals at X and Y after applying self-interference cancellation are, respectively given by

$$
\widetilde{z}_{\mathsf{X}}^{(3)} = \begin{cases} z_{\mathsf{X}}^{(3)} - \sqrt{P_{\mathsf{X}}}g_{\mathsf{XR}}x_1 - \sqrt{P_{\mathsf{X}}}g_{\mathsf{XB}}x_2, & \text{if} \quad A \text{ is the worst} \\ z_{\mathsf{X}}^{(3)} - \sqrt{P_{\mathsf{X}}}g_{\mathsf{XR}}x_1 - \sqrt{P_{\mathsf{X}}}g_{\mathsf{XA}}x_2, & \text{if} \quad B \text{ is the worst} \\ z_{\mathsf{X}}^{(3)} - \sqrt{P_{\mathsf{X}}}g_{\mathsf{XB}}x_1 - \sqrt{P_{\mathsf{X}}}g_{\mathsf{XA}}x_2, & \text{if} \quad R \text{ is the worst} \end{cases},
\tag{3.33}
$$

$$
\widetilde{z}_{\mathsf{Y}}^{(3)} = \begin{cases} z_{\mathsf{Y}}^{(3)} - \sqrt{P_{\mathsf{Y}}}g_{\mathsf{YR}}y_1 - \sqrt{P_{\mathsf{Y}}}g_{\mathsf{YB}}y_2, & \text{if} \quad A \text{ is the worst} \\ z_{\mathsf{Y}}^{(3)} - \sqrt{P_{\mathsf{Y}}}g_{\mathsf{YR}}y_1 - \sqrt{P_{\mathsf{Y}}}g_{\mathsf{YA}}y_2, & \text{if} \quad B \text{ is the worst} \\ z_{\mathsf{Y}}^{(3)} - \sqrt{P_{\mathsf{Y}}}g_{\mathsf{YB}}y_1 - \sqrt{P_{\mathsf{Y}}}g_{\mathsf{YA}}y_2, & \text{if} \quad R \text{ is the worst} \end{cases},
\tag{3.34}
$$

which can be, respectively represented as

$$
\widetilde{z}_{\mathsf{X}}^{(3)} = \mathbf{g}_{\mathsf{ij}}\mathbf{y} + \widetilde{w}_{\mathsf{Xij}}^{(3)},
\tag{3.35}
$$

$$
\widetilde{z}_{\mathsf{Y}}^{(3)} = \mathbf{g}_{\mathsf{ij}}\mathbf{x} + \widetilde{w}_{\mathsf{Yij}}^{(3)},
\tag{3.36}
$$

where $\mathsf{i} \in \{\mathsf{R}, \mathsf{B}\}$ and $\mathsf{j} \in \{\mathsf{A}, \mathsf{B}\}$ represent the selected two relays among R, A and B. While $\widetilde{w}^{(3)}_{\mathsf{Xij}}$ and $\widetilde{w}^{(3)}_{\mathsf{Yij}}$ denote the AWGN samples at X and Y, respectively in addition to the SU interference signal due to incorrect decoding at relays.

3.3.3 SINR Statistics of Cooperative TWR-AF Network

In this part, a simplified mathematical formulas are presented which will be used to obtain a more mathematically tractable expressions for the proposed model in different cooperative schemes. Firstly, the channels between the PU sources (i.e., X and Y) and all the relays (i.e., R, A and B) are assumed to follow i.i.d. Rayleigh fading distribution. Then, the CDF of $|g_{\mathsf{ij}}|^2$ is given by

$$F_{|g_{\mathsf{ij}}|^2}(z) = 1 - \exp\left(\frac{-z}{P_{\mathsf{i}}\gamma_{\mathsf{g}}}\right), \tag{3.37}$$

where γ_{g} denotes the channel gain average $\gamma_{\mathsf{g}} = \mathbf{E}(|g_{\mathsf{ij}}|^2)$ for $\mathsf{i} \in \{X, Y\}, \mathsf{j} \in \{R, A, B\}$, and P_{i} denotes the transmission power per PU. Then, for a single relay transmission, a tight upper bound on the equivalent signal-to-interference and noise ratio (SINR) at the PU node is given by [88]

$$\gamma_{\mathsf{i}} \leq \min\left(\frac{P_{\mathsf{i}}|g_{\mathsf{ij}}|^2}{I_{\mathsf{j}} + 2}, \lambda_{\mathsf{j}} P_{\mathsf{i}} |g_{\mathsf{ji}}|^2\right), \tag{3.38}$$

where $\mathsf{i} \in \{X, Y\}, \mathsf{j} \in \{R, A, B\}$, the interference at relay nodes due to detection error in SU transmission is denoted by $I_{\mathsf{j}} = P_{I_{\mathsf{j}}}|h_{\mathsf{jk}}|$ with $\mathsf{k} \in \{R, A, B\}$, where $P_{I_{\mathsf{j}}}$ denotes the interfering power and $|h_{\mathsf{jk}}|$ denotes the channel gain coefficients between relay nodes. Based on the analysis derived in [88], the CDF of the upper bounded SINR (γ_{i}) is given by

$$F_{\gamma_{\mathsf{i}}}^{(L)}(\gamma) = 1 - \alpha^{L} \exp\left(-\beta\gamma\right), \tag{3.39}$$

where $\beta = \left[\frac{2}{P_{\mathsf{i}}\gamma_{\mathsf{g}}} + \frac{1}{\lambda_{\mathsf{j}} P_{\mathsf{i}}\gamma_{g}}\right]$, $\alpha = \frac{\mu}{\gamma+\mu}$, $\mu = \frac{P_{\mathsf{i}}\gamma_{\mathsf{g}}}{P_{I_{\mathsf{j}}}\gamma_{\mathsf{h}}}$, and $\mathsf{i} \in \{x, y\}$, $\mathsf{j} \in \{R, A, B\}$. Note that L denotes the number of interfering signals at each relay node caused by detection error of SU symbol. Hence, L can take two values $L = 0$ for no interference (i.e., correct detection of SU symbol at the corresponding relay node), and $L = 1$ for interference (i.e., error in detection of SU symbol at the corresponding relay node). All channel coefficients are assumed to follow i.i.d. Rayleigh fading distribution. Then, the SINR CDFs of PU nodes X and Y are identical (i.e., $F_{\gamma_{\mathsf{x}}}^{(L)} = F_{\gamma_{\mathsf{y}}}^{(L)}$). Differentiating (3.39) w.r.t. γ to obtain the pdf of γ_{i}, such as

$$f_{\gamma_{\mathsf{i}}}^{(L)}(\gamma) = \left[\frac{L/\mu}{\gamma+\mu} + \beta\right]\left(\frac{\mu}{\gamma+\mu}\right)^{L} \exp\left(-\beta\gamma\right). \tag{3.40}$$

For high SNR regimes, the SINR CDF can be simplified using Taylor's series resulting in an asymptotic expression given by

$$F_{\gamma_{\mathsf{i}}}^{(L),\infty} = \left(\beta + \frac{L}{\mu}\right)\gamma + o(\gamma), \tag{3.41}$$

where $o(\gamma)$ represents the terms with higher order of γ. Hence, the asymptotic CDF expression in (3.41) provides a simpler mathematical formula which can be useful in achieving different important system parameters such as diversity order and coding gain.

Next, the above-mentioned expressions are used to derive closed-form expressions for the performance metrics of the proposed cooperative TWR-AF model with different cooperative schemes.

3.4 Performance Analysis

In this section, we investigate the proposed model performance metrics for both PU and SU networks in terms of outage probability, SEP and achievable rate. This section is divided into two parts; the first part studies the SU performance in terms of asymptotic SEP and maximum achievable rate, and the second part presents the PU performance for RS and RE schemes.

3.4.1 SU Network Performance Analysis

In this part, and for tractable analysis, the SU asymptotic SEP closed-form expression is derived based on the work presented in [67]. Then, the SU achievable rate is obtained based on the chosen applied scheme from the three proposed cooperative schemes (i.e., AP, RS and RE).

3.4.1.1 Asymptotic SU SEP

The SU data symbol is jointly detected with the others two PU data symbols via a multiuser joint detection process. The joint maximum likelihood detection (JMLD) algorithm is used to extract the SU symbol from the received signals at both PU relay node R and the SU destination B after the first two-time slots, such as

$$\widetilde{\mathbf{u}}_{\mathsf{R}} = \arg\max_{\mathbf{u}_{\mathsf{R}}} \left| z_{\mathsf{R}}^{(1)} - \mathbf{h}_{\mathsf{R}}^{*}\mathbf{u}_{\mathsf{R}} \right|^{2}, \tag{3.42}$$

$$\widetilde{\mathbf{u}}_{\mathsf{B}} = \arg\max_{\mathbf{u}_{\mathsf{B}}} \left| z_{\mathsf{B}}^{(2)} - \mathbf{h}_{\mathsf{B}}^{*}\mathbf{u}_{\mathsf{B}} \right|^{2}, \tag{3.43}$$

where $\mathbf{u}_{\mathsf{R}} = \left[\sqrt{P_{\mathsf{X}}}x_1, \sqrt{P_{\mathsf{Y}}}y_1, \sqrt{P_{\mathsf{A}}}a_1\right]^*$ is the symbols vector at R and $\mathbf{h}_{\mathsf{R}} = [g_{\mathsf{XR}}, g_{\mathsf{YR}}, h_{\mathsf{AR}}]^*$ is the channel coefficients vector. Similarly, $\mathbf{u}_{\mathsf{B}} = \left[\sqrt{P_{\mathsf{X}}}x_2, \sqrt{P_{\mathsf{Y}}}y_2, \sqrt{P_{\mathsf{R}}}\widehat{a}_1\right]^*$ denotes the data symbols vector at B and the channel vector at B is given by $\mathbf{h}_{\mathsf{B}} = [g_{\mathsf{XB}}, g_{\mathsf{YB}}, h_{\mathsf{RB}}]^*$.

Then, for the first hop between A and R, the SEP of JMLD of the SU symbol in Rayleigh fading environment follows an asymptotic upper bound (UB) expression which is given by [67]

$$\mathrm{SEP}_{\mathrm{SU}}^{(1)} = \frac{M_{\mathrm{P}}^2}{2}\, q\!\left(\frac{3\mathrm{SNR}_{\mathrm{SU}}^{(1)}}{M_{\mathrm{S}}-1}\right) \approx \frac{(M_{\mathrm{S}}-1)\, M_{\mathrm{P}}^2}{6\mathrm{SNR}_{\mathrm{SU}}^{(1)}} = \rho_1, \tag{3.44}$$

where M_{S} and M_{P} denote the number of SU and PU constellation symbols, respectively, $\mathrm{SNR}_{\mathrm{SU}}^{(1)}$ denotes the SU SNR in the first hop, and the function $q(a) = 1 - \sqrt{\frac{a/2}{1+a/2}}$. To gain more insights, an approximated expression for $q(a)$ function can be derived using the Taylor expansion of $q(a)$ around $\frac{1}{a} = 0$ resulting in $q(a) \approx \frac{1}{a}$ for large values of a. In the special case of $(M_{\mathrm{S}}, M_{\mathrm{P}}) = (4, 4)$, the upper bound expression becomes

$$\mathrm{SEP}_{\mathrm{SU}}^{(1)} \approx \frac{8}{\mathrm{SNR}_{\mathrm{SU}}^{(1)}}. \tag{3.45}$$

Similarly, for the second hop between R and B, the SEP is given by

$$\mathrm{SEP}_{\mathrm{SU}}^{(2)} = \frac{M_{\mathrm{P}}^{2}}{2}\, q\left(\frac{3\mathrm{SNR}_{\mathrm{SU}}^{(2)}}{M_{\mathrm{S}}-1}\right) \approx \frac{\left(M_{\mathrm{S}}-1\right) M_{\mathrm{P}}^{2}}{6\mathrm{SNR}_{\mathrm{SU}}^{(2)}} = \rho_2, \tag{3.46}$$

where $\mathrm{SNR}_{\mathrm{SU}}^{(2)}$ denotes the SU SNR in the second hop. Then, the total asymptotic SU SEP at the SU destination B can be approximated to be

$$\mathrm{SEP}_{\mathrm{SU}} \approx \mathrm{SEP}_{\mathrm{SU}}^{(1)} + \mathrm{SEP}_{\mathrm{SU}}^{(2)} = \rho_1 + \rho_2. \tag{3.47}$$

For simplicity and without loss of generality, the SU transmission powers at both SU source A and the PU relay R are assumed to be identical (i.e., $P_{\mathsf{A}} = P_{\mathsf{R}} = \mathcal{P}$). Under the consideration of i.i.d. channels during the two hops of SU network, equal SU SEP per hop is obtained, such as

$$\mathrm{SEP}_{\mathrm{SU}} \approx \mathrm{SEP}_{\mathrm{SU}}^{(1)} + \mathrm{SEP}_{\mathrm{SU}}^{(2)} = \rho + \rho = 2\rho. \tag{3.48}$$

3.4.1.2 SU Achievable Rate

In this part, a closed-form expression for SU achievable rate is obtained. Similarly, under the assumption of $P_{\mathsf{A}} = P_{\mathsf{R}} = \mathcal{P}$, the SU network can transmit a single SU data symbol every four-time slots in the case of RS scheme. Then, the

SU network achievable rate is given by

$$\mathcal{R}_{\mathrm{SU}}^{\mathrm{AP/RS}} = \frac{1}{4}\log_2\left(1 + \frac{\mathcal{P}\gamma_{\mathsf{h}}}{\sigma_0^2}\right). \tag{3.49}$$

On the other hand, the SU network can transmit a single SU data symbol every three-time slots in the case of RE scheme. Then, the SU network achievable rate is given by

$$\mathcal{R}_{\mathrm{SU}}^{\mathrm{RE}} = \frac{1}{3}\log_2\left(1 + \frac{\mathcal{P}\gamma_{\mathsf{h}}}{\sigma_0^2}\right). \tag{3.50}$$

The SU SEP performance depends on number of signal constellation symbols for both PU and SU networks, as well as the available SU transmission power at both A and R. It is clear that the SU SEP performance is independent of the applied cooperative transmission scheme (i.e., AP, RS and RE schemes); whereas the SU achievable rate depends on the applied cooperative scheme.

In the following, the key performance metrics of the PU network such outage probability, SEP and maximum achievable rate are investigated. The analytical expressions are derived for the proposed cooperative schemes.

3.4.2 PU Network Performance Analysis with All Participant (AP) Scheme

In this part, the PU performance metrics of the PU network under AP cooperative scheme are derived. As shown in Section 3.3, the AP scheme creates a virtual single-input-multiple-output (SIMO) transmission with space-time characteristics. In the following, closed-form expression for exact and asymptotic outage probability are derived. Then, these new formulas are used to obtain closed-form expressions for exact and asymptotic SEP, as well as achievable rate.

3.4.2.1 Outage Probability

The outage probability is an important performance indicator which can be defined as the probability that the end-to-end SNR falls below a given threshold γ. Again, for simplicity without loss of generality, all AF relaying factors are assumed to be identical (i.e., $\lambda_{\mathsf{R}} = \lambda_{\mathsf{A}} = \lambda_{\mathsf{B}_1} = \lambda_{\mathsf{B}_2} = \lambda_{\mathsf{ap}}$), and consider constant SU transmission power over the two hops (i.e., $P_{\mathsf{A}} = P_{\mathsf{R}} = \mathcal{P}_{\mathsf{ap}}$). Then, for AP scheme, the PU outage probability can be evaluated by

$$P_{\mathrm{AP}}\left(\gamma\right) = \left(1-\rho\right)^2 F_{\gamma_{\mathsf{x}}}^{(0)}\left(\gamma\right) F_{\gamma_{\mathsf{x}}}^{(0)}\left(\gamma\right) + \rho\left(1-\rho\right) F_{\gamma_{\mathsf{x}}}^{(0)}\left(\gamma\right) F_{\gamma_{\mathsf{x}}}^{(1)}\left(\gamma\right) + \rho F_{\gamma_{\mathsf{x}}}^{(1)}\left(\gamma\right) F_{\gamma_{\mathsf{x}}}^{(1)}\left(\gamma\right) \tag{3.51}$$

where $F_{\gamma_{\mathsf{x}}}^{(L)}\left(\gamma\right)$ is the CDF of γ_{x} with L interfering signals at relays node given by (3.39). Hence, the exact outage probability of the PU cooperative TWR-AF model with AP scheme is upper bounded by

$$\begin{aligned} P_{\mathrm{AP}}\left(\gamma\right) = & \left(1-\rho\right)^2 \left[1-\exp\left(-\beta_{\mathsf{ap}}\gamma\right)\right]^2 + \rho\left(1-\rho\right)\left[1-\exp\left(-\beta_{\mathsf{ap}}\gamma\right)\right] \\ & \times\left[1-\alpha_{\mathsf{ap}}\exp\left(-\beta_{\mathsf{ap}}\gamma\right)\right] + \rho\left[1-\alpha_{\mathsf{ap}}\exp\left(-\beta_{\mathsf{ap}}\gamma\right)\right)^2 \end{aligned} \tag{3.52}$$

where $\beta_{\mathsf{ap}} = \left(\frac{1}{\lambda_{\mathsf{ap}} P_{\mathsf{s}} \gamma_{\mathsf{g}}} + \frac{2}{P_{\mathsf{s}} \gamma_{\mathsf{g}}}\right)$, $\alpha_{\mathsf{ap}} = \frac{\mu_{\mathsf{ap}}}{\gamma + \mu_{\mathsf{ap}}}$, and $\mu_{\mathsf{ap}} = \frac{P_{\mathsf{s}} \gamma_{\mathsf{g}}}{\mathcal{P}_{\mathsf{ap}} \gamma_{\mathsf{h}}}$.

For high SNR values, the asymptotic outage probability of the cooperative TWR-AF model with AP scheme is given by

$$P_{\mathrm{AP}}^{\infty}(\gamma) = (1-\rho)^2 \beta_{\mathsf{ap}}^2 \gamma^2 + \rho (1-\rho) \beta_{\mathsf{ap}} (\beta_{\mathsf{ap}} + \mu_{\mathsf{ap}}) \gamma^2 + \rho (\beta_{\mathsf{ap}} + \mu_{\mathsf{ap}})^2 \gamma^2. \quad (3.53)$$

In the following, the exact and asymptotic AP outage probability closed-form expressions are employed to obtain both exact and asymptotic PU SEP formulas for AP scheme.

3.4.2.2 Average SEP

In this section, closed-form expressions for exact and asymptotic SEP for both AP and RS schemes are derived. The average SEP admits the following expression

$$\begin{aligned} \mathrm{SEP} &= \frac{M_{\mathrm{P}}^2}{2} \int_0^{\infty} a_{\mathrm{mod}} Q\left(\sqrt{2 b_{\mathrm{mod}} \gamma}\right) f_{\gamma}(\gamma) d\gamma \\ &= \frac{M_{\mathrm{P}}^2}{2} \times \frac{a_{\mathrm{mod}} \sqrt{b_{\mathrm{mod}}}}{2\sqrt{\pi}} \int_0^{\infty} \frac{\exp(-b_{\mathrm{mod}} \gamma)}{\gamma^{1/2}} P_{\mathsf{out}}(\gamma) d\gamma, \end{aligned} \quad (3.54)$$

where $Q(\cdot)$ is the Gaussian-Q function, a_{mod} and b_{mod} are modulation specific constants. Due to the joint detection of the PU symbols at the destinations an error constant $\frac{M_{\mathrm{P}}^2}{2}$ is presented similar to the SU JMLD shown in Section 3.4.1. Hence, the exact SEP of the PU cooperative TWR-AF model with AP scheme is upper bounded by

$$\begin{aligned}\mathrm{SEP}_{\mathrm{AP}} =&\frac{M_{\mathrm{P}} a_{\mathrm{mod}} \sqrt{b_{\mathrm{mod}}}}{4\sqrt{\pi}} \Bigg[\sqrt{\frac{\pi}{b_{\mathrm{mod}}}} - \left(2-3\rho-\rho^2\right)\sqrt{\frac{\pi}{b_{\mathrm{mod}}+\beta_{\mathsf{ap}}}} - \left(3\rho-\rho^2\right)\mu_{\mathsf{ap}} \\ &\times\sqrt{\pi\left(b_{\mathrm{mod}}+\beta_{\mathsf{ap}}\right)}\Phi\left(1,\frac{3}{2},\mu_{\mathsf{ap}}\left(b_{\mathrm{mod}}+\beta_{\mathsf{ap}}\right)\right) + \left(1-\rho\right)^2\sqrt{\frac{\pi}{b_{\mathrm{mod}}+2\beta_{\mathsf{ap}}}} \\ &+\rho\left(1-\rho\right)\mu_{\mathsf{ap}}\sqrt{\pi\left(b_{\mathrm{mod}}+2\beta_{\mathsf{ap}}\right)}\Phi\left(1,\frac{3}{2},\mu_{\mathsf{ap}}\left(b_{\mathrm{mod}}+2\beta_{\mathsf{ap}}\right)\right) \\ &+\rho\mu_{\mathsf{ap}}^2\sqrt{\pi\left(b_{\mathrm{mod}}+2\beta_{\mathsf{ap}}\right)^3}\;\Phi\left(2,\frac{5}{2},\mu_{\mathsf{ap}}\left(b_{\mathrm{mod}}+2\beta_{\mathsf{ap}}\right)\right)\Bigg] \end{aligned} \tag{3.55}$$

Similarly, the asymptotic SEP can be derived by substituting (3.53) in (3.54), hence, the asymptotic SEP of the PU cooperative TWR-AF model with AP scheme is upper bounded by

$$\begin{aligned}\mathrm{SEP}_{\mathrm{AP}}^{\infty} =&\frac{3M_{\mathrm{P}} a_{\mathrm{mod}}}{8b_{\mathrm{mod}}}\left[\left(1-\rho\right)^2\beta_{\mathsf{ap}}^2 + \rho\left(1-\rho\right)\beta_{\mathsf{ap}}\left(\beta_{\mathsf{ap}}+\mu_{\mathsf{ap}}\right) + \rho\left(\beta_{\mathsf{ap}}+\mu_{\mathsf{ap}}\right)^2\right] \\ =&\frac{3M_{\mathrm{P}} a_{\mathrm{mod}}}{8b_{\mathrm{mod}}}\Bigg[\left(1-\rho\right)^2\left(\frac{1}{\lambda_{\mathsf{ap}}P_{\mathsf{s}}\gamma_{\mathsf{g}}}+\frac{2}{P_{\mathsf{s}}\gamma_{\mathsf{g}}}\right)^2 + \rho\left(1-\rho\right)\left(\frac{1}{\lambda_{\mathsf{ap}}P_{\mathsf{s}}\gamma_{\mathsf{g}}}+\frac{2}{P_{\mathsf{s}}\gamma_{\mathsf{g}}}\right) \\ &\times\left(\frac{1}{\lambda_{\mathsf{ap}}P_{\mathsf{s}}\gamma_{\mathsf{g}}}+\frac{2+\mathcal{P}_{\mathsf{ap}}\gamma_{\mathsf{h}}}{P_{\mathsf{s}}\gamma_{\mathsf{g}}}\right) + \rho\left(\frac{1}{\lambda_{\mathsf{ap}}P_{\mathsf{s}}\gamma_{\mathsf{g}}}+\frac{2+\mathcal{P}_{\mathsf{ap}}\gamma_{\mathsf{h}}}{P_{\mathsf{s}}\gamma_{\mathsf{g}}}\right)^2\Bigg] \end{aligned} \tag{3.56}$$

3.4.2.3 Achievable Rate

The achievable rate represents the maximum achievable rate under which the system can recover the error in transmitted data. For the cooperative TWR with AP scheme, the achievable rate is given by [88]

$$\mathcal{R}_{\mathrm{PU}}^{\mathrm{AP}} = \mathrm{E}\left[\log_2\left(1+\gamma_{\mathrm{AP}}\right)\right]. \tag{3.57}$$

Since this exact expression cannot be obtained in a closed-form formula, Jensen's inequality is used to obtain an approximated expression. Hence, the achievable rate of the cooperative TWR-AF model with AP scheme is upper bounded by

$$\mathcal{R}_{\mathrm{PU}}^{\mathrm{AP}} \leq \log_2\left(1+\mathrm{E}\left[\gamma_{\mathrm{AP}}\right]\right) \tag{3.58}$$

where $\mathrm{E}\left[\gamma_{\mathrm{AP}}\right]$ can be evaluated using the obtained outage probability formula in (3.52) for AP scheme, such as

$$\begin{aligned}
\mathrm{E}\left[\gamma_{\mathrm{AP}}\right] &= \int_0^{\infty}\left(1-P_{\mathrm{AP}}(\gamma)\right) d\gamma \\
&= \frac{\left(3-4\rho+\rho^2\right)}{2\beta_{\mathsf{ap}}}+\left(3\rho-\rho^2\right)\mu_{\mathsf{ap}}\ \Phi\left(1,1,\beta_{\mathsf{ap}}\mu_{\mathsf{ap}}\right)-\rho\left(1-\rho\right)\mu_{\mathsf{ap}} \\
&\quad \times\Phi\left(1,1,2\beta_{\mathsf{ap}}\mu_{\mathsf{ap}}\right)-\rho\mu_{\mathsf{ap}}\ \Phi\left(1,0,2\beta_{\mathsf{ap}}\mu_{\mathsf{ap}}\right)
\end{aligned} \tag{3.59}$$

3.4.3 PU Network Performance Analysis with RS Scheme

In this part, closed-form expressions for RS scheme performance metrics are derived. In the proposed RS scheme, the min-max selection criterion is used to select the best relay among the two available relays per time slot. Firstly, the pdf and CDF of the min-max criterion are derived to be used then in obtaining the analytical closed-form expressions for the RS scheme performance metrics. Based on the analysis given in [90], the pdf of opportunistic RS scheme is given by

$$f_{\mathrm{RS}}(z) = N f_{\gamma_{\mathsf{x}}^{\min}}(z) F_{\gamma_{\mathsf{x}}^{\min}}^{N-1}(z) = 2N f_{\gamma_{\mathsf{x}}}(z) \left(1 - F_{\gamma_{\mathsf{x}}}(z)\right) \left[1 - \left(1 - F_{\gamma_{\mathsf{x}}}(z)\right)^2\right]^{N-1}, \tag{3.60}$$

where N denotes the total number of relays, $f_{\gamma_{\mathsf{x}}^{\min}}(z) = 2 f_{\gamma_{\mathsf{x}}}(z)\left(1 - F_{\gamma_{\mathsf{x}}}(z)\right)$, and $F_{\gamma_{\mathsf{x}}^{\min}}(z) = 1 - \left(1 - F_{\gamma_{\mathsf{x}}}(z)\right)^2$. In this model, substituting $N = 2$ results in

$$f_{\mathrm{RS}}^{(L)}(z) = 2 f_{\gamma_{\mathsf{x}}^{\min}}^{(L)}(z) F_{\gamma_{\mathsf{x}}^{\min}}^{(L)}(z) = 4 f_{\gamma_{\mathsf{x}}}^{(L)}(z) \left(1 - F_{\gamma_{\mathsf{x}}}^{(L)}(z)\right) \left[1 - \left(1 - F_{\gamma_{\mathsf{x}}}^{(L)}(z)\right)^2\right], \tag{3.61}$$

where $L \in \{0, 1\}$ is the number of interfering signals due to error detection at relay nodes. Then, the CDF of RS scheme can be obtained by

$$F_{\mathrm{RS}}^{(L)}(Z) = \int_0^Z f_{\mathrm{RS}}^{(L)}(z)\, dz. \tag{3.62}$$

Based on the value of $L \in \{0, 1\}$, we obtained two CDFs, respectively given by

$$F_{\mathrm{RS}}^{(0)}(Z) = \int_0^Z f_{\mathrm{RS}}^{(0)}(z)\, dz = 1 - 2\exp\left(-2\beta_{\mathsf{rs}} Z\right) + \exp\left(-4\beta_{\mathsf{rs}} Z\right), \tag{3.63}$$

$$\begin{aligned} F_{\mathrm{RS}}^{(1)}(Z) &= \int_0^Z f_{\mathrm{RS}}^{(1)}(z)\, dz \\ &= 1 - 2\frac{\mu_{\mathsf{rs}}^2}{\left(Z + \mu_{\mathsf{rs}}\right)^2} \exp\left(-2\beta_{\mathsf{rs}} Z\right) + \frac{\mu_{\mathsf{rs}}^4}{\left(Z + \mu_{\mathsf{rs}}\right)^4} \exp\left(-4\beta_{\mathsf{rs}} Z\right), \end{aligned} \tag{3.64}$$

where $\beta_{\mathsf{rs}} = \left(\frac{1}{\lambda_{\mathsf{rs}} P_{\mathsf{s}} \gamma_{\mathsf{g}}} + \frac{2}{P_{\mathsf{s}} \gamma_{\mathsf{g}}}\right)$, and $\mu_{\mathsf{rs}} = \frac{P_{\mathsf{s}} \gamma_{\mathsf{g}}}{\mathcal{P}_{\mathsf{rs}} \gamma_{\mathsf{h}}}$.

3.4.3.1 Outage Probability

Based on previous discussion, the PU network outage probability under RS scheme is given by

$$P_{\mathrm{RS}}\left(\gamma_{\mathrm{out}}\right) = \left(1-\rho\right) F_{\mathrm{RS}}^{(0)}\left(\gamma_{\mathrm{out}}\right) + \rho F_{\mathrm{RS}}^{(1)}\left(\gamma_{\mathrm{out}}\right), \tag{3.65}$$

where γ_{out} is a predetermined outage threshold value. Then, the substitution of (3.63) and (3.64) in (3.65) provides the exact and asymptotic outage probabilities under RS schemes which are summarized as follows. The exact outage probability of PU cooperative TWR-AF model with RS scheme is upper bounded by

$$\begin{aligned} P_{\mathrm{RS}}\left(\gamma_{\mathrm{out}}\right) =& \left(1-\rho\right)\left[1 - 2\exp\left(-2\beta_{\mathsf{rs}}\gamma_{\mathrm{out}}\right) + \exp\left(-4\beta_{\mathsf{rs}}\gamma_{\mathrm{out}}\right)\right] \\ &+ \rho\left[1 - \frac{2\mu_{\mathsf{rs}}^{2}\exp\left(-2\beta_{\mathsf{rs}}\gamma_{\mathrm{out}}\right)}{\left(\gamma_{\mathrm{out}}+\mu_{\mathsf{rs}}\right)^{2}} + \frac{\mu_{\mathsf{rs}}^{4}\exp\left(-4\beta_{\mathsf{rs}}\gamma_{\mathrm{out}}\right)}{\left(\gamma_{\mathrm{out}}+\mu_{\mathsf{rs}}\right)^{4}}\right]. \end{aligned} \tag{3.66}$$

At high SNR values, the asymptotic outage probability of PU cooperative TWR-AF model with RS scheme is upper bounded by

$$\begin{aligned} P_{\mathrm{RS}}^{\infty}\left(\gamma_{\mathrm{out}}\right) =& 4\left(1-\rho\right)\left[\beta_{\mathsf{rs}}^{2}\gamma_{\mathrm{out}}^{2} - \beta_{\mathsf{rs}}^{3}\gamma_{\mathrm{out}}^{3} + \frac{1}{4}\beta_{\mathsf{rs}}^{4}\gamma_{\mathrm{out}}^{4}\right] \\ &+ 4\rho\left[\left(\beta_{\mathsf{rs}}+\mu_{\mathsf{rs}}\right)^{2}\gamma_{\mathrm{out}}^{2} - \left(\beta_{\mathsf{rs}}+\mu_{\mathsf{rs}}\right)_{\mathsf{rs}}^{3}\gamma_{\mathrm{out}}^{3} + \frac{1}{4}\left(\beta_{\mathsf{rs}}+\mu_{\mathsf{rs}}\right)_{\mathsf{rs}}^{4}\gamma_{\mathrm{out}}^{4}\right] \\ &\approx 2\left(1-\rho\right)\left(\frac{1}{\lambda_{\mathsf{rs}}P_{\mathsf{s}}\gamma_{\mathsf{g}}} + \frac{2}{P_{\mathsf{s}}\gamma_{\mathsf{g}}}\right)^{2}\gamma_{\mathrm{out}}^{2} + 2\rho\left(\frac{1}{\lambda_{\mathsf{rs}}P_{\mathsf{s}}\gamma_{\mathsf{g}}} + \frac{2+\mathcal{P}_{\mathsf{rs}}\gamma_{\mathsf{h}}}{P_{\mathsf{s}}\gamma_{\mathsf{g}}}\right)^{2}\gamma_{\mathrm{out}}^{2}. \end{aligned} \tag{3.67}$$

In the following, the exact and asymptotic outage probability closed-form expressions are employed to obtain both exact and asymptotic PU SEP formulas for RS scheme.

3.4.3.2 Average SEP

Similar to AP scheme, the substitution of the RS outage probability (3.66) in (3.54) gives the PU SEP exact closed-form expression are provided as follows. The exact SEP of PU cooperative TWR-AF model with RS scheme is upper bounded by

$$\begin{aligned}\mathrm{SEP}_{\mathrm{RS}} = \frac{a_{\mathrm{mod}}\sqrt{b_{\mathrm{mod}}}}{2\sqrt{\pi}} \Bigg[& \sqrt{\frac{\pi}{b_{\mathrm{mod}}}} - 2\left(1-\rho\right)\sqrt{\frac{\pi}{b_{\mathrm{mod}}+2\beta_{\mathsf{rs}}}} + \left(1-\rho\right)\sqrt{\frac{\pi}{b_{\mathrm{mod}}+4\beta_{\mathsf{rs}}}} \\ & -2\sqrt{\pi}\rho\mu_{\mathsf{rs}}^{2}\left(b_{\mathrm{mod}}+2\beta_{\mathsf{rs}}\right)^{3/2}\Phi\left(2,2.5,\left(b_{\mathrm{mod}}+2\beta_{\mathsf{rs}}\right)\mu_{\mathsf{rs}}\right) \\ & +\sqrt{\pi}\rho\mu_{\mathsf{rs}}^{4}\left(b_{\mathrm{mod}}+4\beta_{\mathsf{rs}}\right)^{7/2}\Phi\left(4,4.5,\left(b_{\mathrm{mod}}+4\beta_{\mathsf{rs}}\right)\mu_{\mathsf{rs}}\right)\Bigg].\end{aligned} \tag{3.68}$$

For high SNR values, the asymptotic SEP of PU cooperative TWR-AF model with RS scheme is upper bounded by

$$\begin{aligned}\mathrm{SEP}_{\mathrm{RS}}^{\infty}\left(\gamma\right) &\approx \frac{3a_{\mathrm{mod}}}{2b_{\mathrm{mod}}}\left[\left(1-\rho\right)\beta_{\mathsf{rs}}^{2}+\rho\left(\beta_{\mathsf{rs}}+\mu_{\mathsf{rs}}\right)^{2}\right] \\ &\approx \frac{3a_{\mathrm{mod}}}{2b_{\mathrm{mod}}}\left[\left(1-\rho\right)\left(\frac{1}{\lambda_{\mathsf{rs}}P_{\mathsf{s}}\gamma_{\mathsf{g}}}+\frac{2}{P_{\mathsf{s}}\gamma_{\mathsf{g}}}\right)^{2}+\rho\left(\frac{1}{\lambda_{\mathsf{rs}}P_{\mathsf{s}}\gamma_{\mathsf{g}}}+\frac{2+\mathcal{P}_{\mathsf{rs}}\gamma_{\mathsf{h}}}{P_{\mathsf{s}}\gamma_{\mathsf{g}}}\right)^{2}\right].\end{aligned} \tag{3.69}$$

3.4.3.3 Achievable Rate

For the PU cooperative TWR-AF with RS scheme, the achievable rate is given by [88]

$$\mathcal{R}_{\mathrm{PU}}^{\mathrm{RS}} = \mathrm{E}\left[\log_2\left(1+\gamma_{\mathrm{RS}}\right)\right]. \tag{3.70}$$

Again, the rate in (3.70) cannot be obtained in a closed-form mathematical formula. Hence, the achievable rate of PU cooperative TWR-AF model with RS scheme is upper bounded by

$$\mathcal{R}_{\mathrm{PU}}^{\mathrm{RS}} \leq \log_2\left(1+\mathrm{E}\left[\gamma_{\mathrm{RS}}\right]\right), \tag{3.71}$$

where $\mathrm{E}\left[\gamma_{\mathrm{RS}}\right]$ can be evaluated using the obtained outage probability formulas in (3.66) for RS scheme, such as

$$\begin{aligned} \mathrm{E}\left[\gamma_{\mathrm{RS}}\right] &= \int_0^\infty \left(1-P_{\mathrm{RS}}\left(\gamma\right)\right) d\gamma \\ &= \frac{3\left(1-\rho\right)}{4\beta_{\mathsf{rs}}} + 4\rho\mu_{\mathsf{rs}}^2\beta_{\mathsf{rs}}\ \Phi(2,2,2\beta_{\mathsf{rs}}\mu_{\mathsf{rs}}) - 64\rho\mu_{\mathsf{rs}}^4\beta^3\ \Phi(4,4,4\beta_{\mathsf{rs}}\mu_{\mathsf{rs}}). \end{aligned} \tag{3.72}$$

3.4.4 PU Network Performance Analysis with RE Scheme

In this part, the performance analysis for RE scheme is presented. The worst relay link among all the available links is eliminated from the BC phase. Then, based on the analysis of selecting the N-th worst relay among K relays presented in [93], the CDF of the N-th order statistic is given by

$$F_{\gamma_{N,K}}(\gamma) = \sum_{i=N}^{K} \binom{K}{i} \left[F_{\gamma_k}(\gamma)\right]^i \left[1 - F_{\gamma_k}(\gamma)\right]^{K-i}. \tag{3.73}$$

Given that $N = 1$ and $N = K$ correspond to the worst and the best relay selections, respectively. Since the RE scheme selects the worst relay for elimination, then the above CDF in (3.73)is valid for our case with $N = 1$ and $K = 3$. Hence, the resulting CDF is given by

$$F_{\text{RE}}^{(L)}(\gamma) = \frac{1}{2}\left(F_{\gamma_{2,3}}^{(L)}(\gamma) + F_{\gamma_{3,3}}^{(L)}(\gamma)\right) = \frac{1}{2}\left[F_{\gamma_{\times}}^{(L)}(\gamma)\right]^2 \left[3 - F_{\gamma_{\times}}^{(L)}(\gamma)\right]. \tag{3.74}$$

Then, the resultant RE scheme CDF is used to derive closed-form mathematical formulas for the system probability of outage, SEP and achievable rate.

3.4.4.1 Outage Probability

Based on previous discussion, the PU network outage probability under RE scheme is upper bounded by

$$P_{\text{RE}}(\gamma_{\text{out}}) = (1 - \rho) F_{\text{RE}}^{(0)}(\gamma_{\text{out}}) + \rho F_{\text{RE}}^{(1)}(\gamma_{\text{out}}), \tag{3.75}$$

where $F_{\text{RE}}^{(0)}(\gamma_{\text{out}}) = \frac{1}{2}\left[F_{\gamma_{\times}}^{(0)}(\gamma_{\text{out}})\right]^2\left[3 - F_{\gamma_{\times}}^{(0)}(\gamma_{\text{out}})\right]$ denotes the case of no interference, while $F_{\text{RE}}^{(1)}(\gamma_{\text{out}}) = \frac{1}{2}\left[F_{\gamma_{\times}}^{(1)}(\gamma_{\text{out}})\right]^2\left[3 - F_{\gamma_{\times}}^{(1)}(\gamma_{\text{out}})\right]$ denotes the case of interference. Substituting these CDFs in (3.75) results in the RE scheme outage probability. Hence, the exact outage probability of PU cooperative TWR-AF model with RE scheme is upper bounded by

$$
\begin{aligned}
P_{\mathrm{RE}}\left(\gamma_{\mathrm{out}}\right) &= \left(1-\rho\right) F_{\mathrm{RE}}^{(0)}\left(\gamma_{\mathrm{out}}\right) + \rho F_{\mathrm{RE}}^{(1)}\left(\gamma_{\mathrm{out}}\right) \\
&= \frac{\left(1-\rho\right)}{2}\left[F_{\gamma_{\mathsf{x}}}^{(0)}\left(\gamma_{\mathrm{out}}\right)\right]^{2}\left[3-F_{\gamma_{\mathsf{x}}}^{(0)}\left(\gamma_{\mathrm{out}}\right)\right] + \frac{\rho}{2}\left[F_{\gamma_{\mathsf{x}}}^{(1)}\left(\gamma_{\mathrm{out}}\right)\right]^{2}\left[3-F_{\gamma_{\mathsf{x}}}^{(1)}\left(\gamma_{\mathrm{out}}\right)\right] \\
&= 1-\frac{3}{2}\left(1-\rho+\rho\alpha_{\mathsf{re}}\right)\exp\left(-\beta_{\mathsf{re}}\gamma_{\mathrm{out}}\right) + \frac{1}{2}\left(1-\rho+\rho\alpha_{\mathsf{re}}^{3}\right)\exp\left(-3\beta_{\mathsf{re}}\gamma_{\mathrm{out}}\right),
\end{aligned}
\tag{3.76}
$$

where $\beta_{\mathsf{re}} = \left(\frac{1}{\lambda_{\mathsf{re}} P_{\mathsf{s}}\gamma_{\mathsf{g}}} + \frac{2}{P_{\mathsf{s}}\gamma_{\mathsf{g}}}\right)$, $\alpha_{\mathsf{re}} = \frac{\mu_{\mathsf{re}}}{\gamma+\mu_{\mathsf{re}}}$, and $\mu_{\mathsf{re}} = \frac{P_{\mathsf{s}}\gamma_{\mathsf{g}}}{\mathcal{P}_{\mathsf{re}}\gamma_{\mathsf{h}}}$.

For high SNR values, the asymptotic outage probability of PU cooperative TWR-AF model with RE scheme is given by

$$
\begin{aligned}
P_{\mathrm{RE}}^{\infty}\left(\gamma_{\mathrm{out}}\right) &= \left(1-\rho\right) F_{\mathrm{RE}}^{(0),\infty}\left(\gamma_{\mathrm{out}}\right) + \rho F_{\mathrm{RE}}^{(1),\infty}\left(\gamma_{\mathrm{out}}\right) \\
&= \frac{\left(1-\rho\right)}{2}\beta_{\mathsf{re}}^{2}\gamma_{\mathrm{out}}^{2}\left[3-\beta_{\mathsf{re}}\gamma_{\mathrm{out}}\right] + \frac{\rho}{2}\left(\beta_{\mathsf{re}}+\mu_{\mathsf{re}}\right)^{2}\gamma_{\mathrm{out}}^{2}\left[3-\left(\beta_{\mathsf{re}}+\mu_{\mathsf{re}}\right)\gamma_{\mathrm{out}}\right].
\end{aligned}
\tag{3.77}
$$

3.4.4.2 Average SEP

In this part, an exact closed-form expression for PU SEP under RE cooperative scheme is derived. Then, this new formula is simplified for high SNR regions. The substitution of the RE outage probability (3.76) in (3.54) provides the exact SEP of PU cooperative TWR-AF model with RE scheme which is upper bounded by

$$\begin{aligned}\mathrm{SEP}_{\mathrm{RE}} =& \frac{M_{\mathrm{P}}^2}{2} \times \frac{a_{\mathrm{mod}}\sqrt{b_{\mathrm{mod}}}}{2\sqrt{\pi}} \Bigg[\sqrt{\frac{\pi}{b_{\mathrm{mod}}}} - \frac{3\left(1-\rho\right)}{2}\sqrt{\frac{\pi}{b_{\mathrm{mod}}+\beta_{\mathsf{re}}}} - \frac{3}{2}\sqrt{\pi}\rho\mu_{\mathsf{re}}\left(b_{\mathrm{mod}}+\beta_{\mathsf{re}}\right)^{1/2} \\ & \times\Phi\left(1, 1.5, \left(b_{\mathrm{mod}}+\beta_{\mathsf{re}}\right)\mu_{\mathsf{re}}\right) + \frac{\left(1-\rho\right)}{2}\sqrt{\frac{\pi}{b_{\mathrm{mod}}+3\beta_{\mathsf{re}}}} + \frac{1}{2}\sqrt{\pi}\rho\mu_{\mathsf{re}}^3\left(b_{\mathrm{mod}}+\beta_{\mathsf{re}}\right)^{5/2} \\ & \times\Phi\left(3, 3.5, \left(b_{\mathrm{mod}}+\beta_{\mathsf{re}}\right)\mu_{\mathsf{re}}\right)\Bigg], \qquad (3.78)\end{aligned}$$

where $\frac{M_{\mathrm{P}}^2}{2}$ is an error constant due to JMLD and depends on PU symbols signal constellation M_{P} has been previously discussed in Section 3.4.1.

For high SNR values, the asymptotic SEP of PU cooperative TWR-AF model with RE scheme is upper bounded by

$$\mathrm{SEP}_{\mathrm{RE}}^{\infty}\left(\gamma\right) \approx \frac{M_{\mathrm{P}}^2}{2} \times \frac{3a_{\mathrm{mod}}}{2b_{\mathrm{mod}}}\left[\frac{\left(1-\rho\right)}{2}\beta_{\mathsf{re}}^2\left(3-\beta_{\mathsf{re}}\right) + \frac{\rho}{2}\left(\beta_{\mathsf{re}}+\mu_{\mathsf{re}}\right)^2\left[3-\left(\beta_{\mathsf{re}}+\mu_{\mathsf{re}}\right)\right]\right]. \tag{3.79}$$

3.4.4.3 Achievable Rate

In this part and following the same previously mentioned steps, the achievable rate of PU cooperative TWR-AF model with RE scheme is upper bounded by

$$\mathcal{R}_{\mathrm{PU}}^{\mathrm{RE}} \leq \frac{4}{3}\log_2\left(1+\mathrm{E}\left[\gamma_{\mathrm{RE}}\right]\right), \tag{3.80}$$

where $\mathrm{E}\left[\gamma_{\mathrm{RE}}\right]$ is given by

$$\mathrm{E}\left[\gamma_{\mathrm{RE}}\right] = \frac{4\left(1-\rho\right)}{3\beta_{\mathsf{re}}} + \frac{3}{2}\rho\mu_{\mathsf{re}}\Phi\left(1, 1, \beta_{\mathsf{re}}\mu_{\mathsf{re}}\right) + \frac{27}{2}\rho\mu_{\mathsf{re}}^3\beta_{\mathsf{re}}^3\Phi\left(3, 4, 3\beta_{\mathsf{re}}\mu_{\mathsf{re}}\right). \tag{3.81}$$

3.5 Power Allocation for SEP Minimization

In this section, power allocation optimization problems are formulated to minimize the weighted sum SEP of PU and SU networks of the proposed cooperative schemes by controlling the SU transmission power (i.e., P_{A} and P_{R}) and the relays amplifying factors (i.e., λ_{A}, λ_{R}, λ_{B_1}, and λ_{B_2}). The goal is to find the optimal values of these parameters to minimize the total SEP. For simplicity and without loss of generality, the PU and SU asymptotic ASEPs are considered in the studied case.

3.5.1 AP Scheme

In this section, we formulate a power allocation optimization problem is obtained to minimize the weighted sum SEP of both cooperative networks of the proposed system by controlling the SU transmission power (i.e., P_{A} and P_{R}) and the relays amplifying factors (i.e., λ_{A}, λ_{R}, λ_{B_1}, and λ_{B_2}). The goal is to find the optimal values to minimize the overall SEP. Hence, the optimization problem is given by

$$\begin{aligned} &\text{minimize } \; m_1 \, \mathrm{SEP}_{\mathrm{PU}}^{\infty} + m_2 \, \mathrm{SEP}_{\mathrm{SU}}^{\infty} \\ &\text{subject to: } 2\mathcal{P}_{\mathsf{ap}} + 4\lambda_{\mathsf{ap}} \leq \overline{\mathbf{P}}_{\mathsf{total}}. \end{aligned} \tag{3.82}$$

where m_1 and m_2 denote the weights of both PU and SU ASEPs in the total SEP sum. $\mathcal{P}_{\mathsf{ap}} = P_{\mathsf{A}} = P_{\mathsf{R}}$, $\lambda_{\mathsf{ap}} = \lambda_j$ and $j \in \{\mathsf{A}, \mathsf{R}, \mathsf{B}_1, \mathsf{B}_2\}$. The total available power budget for the proposed TWR-AF model is denoted by $\overline{\mathbf{P}}_{\mathsf{total}}$. Lagrangian multipliers method [83] with the power constraint in (3.82) is used. The Lagrangian function $\mathcal{J}(.)$ can be expressed as

$$\mathcal{J}\left(P_i, \lambda_j\right) = m_1 \mathrm{SEP}_{\mathrm{PU}}^{\infty} + \mathrm{m}_2 \mathrm{SEP}_{\mathrm{SU}}^{\infty} + \Lambda_1 \left(2\mathcal{P}_{\mathsf{ap}} + 4\lambda_{\mathsf{ap}} - \overline{\mathbf{P}}_{\mathsf{total}}\right), \tag{3.83}$$

where Λ_1 denotes the Lagrangian multipliers. Hence, the optimal amplification factor $\lambda_{\mathsf{ap}}^{\mathrm{opt}}$ is the real positive solution of the fifth order equation which is given by

$$\begin{aligned}
&384\left(\frac{P_s}{\sigma_0^2}\right)^2 \gamma_{\mathsf{h}}^2 m_1 x^5 - 192\overline{\mathbf{P}}_{\mathsf{total}}\left(\frac{P_s}{\sigma_0^2}\right)^2 \gamma_{\mathsf{h}}^2 m_1 x^4 \\
&+\left(24\overline{\mathbf{P}}_{\mathsf{total}}^2\left(\frac{P_s}{\sigma_0^2}\right)^2 \gamma_{\mathsf{h}}^2 - 128\left(\frac{P_s}{\sigma_0^2}\right)^2 \gamma_{\mathsf{g}}^2 \frac{m_2}{m_1} + 672\frac{P_s}{\sigma_0^2}\gamma_{\mathsf{h}} + 1536\right) m_1 x^3 \\
&+\left(-336\frac{P_s}{\sigma_0^2}\gamma_{\mathsf{h}}\overline{\mathbf{P}}_{\mathsf{total}} + 48\mathrm{SNR}\gamma_{\mathsf{h}} + 1536\right) m_1 x^2 \\
&+\left(42\frac{P_s}{\sigma_0^2}\gamma_{\mathsf{h}}\overline{\mathbf{P}}_{\mathsf{total}}^2 - 24\frac{P_s}{\sigma_0^2}\gamma_{\mathsf{h}}\overline{\mathbf{P}}_{\mathsf{total}} - 192\overline{\mathbf{P}}_{\mathsf{total}}\right) m_1 x + 3\frac{P_s}{\sigma_0^2}\gamma_{\mathsf{h}}\overline{\mathbf{P}}_{\mathsf{total}}^2 m_1 = 0
\end{aligned} \tag{3.84}$$

3.5.2 RS Scheme

For RS scheme, all the amplifying powers go to the selected best relay. Hence, for RS scheme, we can formulate the optimization problem such as

$$\begin{gathered}
\text{minimize } \; m_1 \ \mathrm{SEP}_{\mathrm{PU}}^{\infty} + m_2 \ \mathrm{SEP}_{\mathrm{SU}}^{\infty} \\
\text{subject to: } 2\mathcal{P}_{\mathsf{rs}} + 2\lambda_{\mathsf{rs}} \leq \overline{\mathbf{P}}_{\mathsf{total}}.
\end{gathered} \tag{3.85}$$

where m_1 and m_2 denote the weights of both PU and SU ASEPs in the total SEP sum, respectively. We assume $\mathcal{P}_{\mathsf{rs}} = P_{\mathsf{A}} = P_{\mathsf{R}}$, $\lambda_{\mathsf{rs}} = \lambda_j$ and $j = \mathsf{A}, \mathsf{R}, \mathsf{B}_1$ and B_2. The total available power budget for the proposed TWR-AF model is denoted by $\overline{\mathbf{P}}_{\mathsf{total}}$. Lagrangian multipliers method [83] with the power constraint in (3.85) is used. The Lagrangian function $\mathcal{J}(.)$ can be expressed as

$$\mathcal{J}\left(P_i, \lambda_j\right) = m_1 \mathrm{SEP}_{\mathrm{PU}}^{\infty} + \mathrm{m}_2 \mathrm{SEP}_{\mathrm{SU}}^{\infty} + \Lambda_1 \left(2\mathcal{P}_{\mathsf{rs}} + 4\lambda_{\mathsf{rs}} - \overline{\mathbf{P}}_{\mathsf{total}}\right), \tag{3.86}$$

where Λ_1 denotes the Lagrangian multipliers. Hence, the optimal $\lambda_{\mathsf{rs}}^{\mathrm{opt}}$ is the real positive solution of a fifth order equation which is given by

$$\begin{aligned} &48\frac{P_s}{\sigma_0^2}\gamma_{\mathsf{h}}^2 m_1 x^5 - 48\frac{P_s}{\sigma_0^2}\overline{\mathbf{P}}_{\mathsf{total}}\gamma_{\mathsf{h}}^2 m_1 x^4 + (12\overline{\mathbf{P}}_{\mathsf{total}}^2\frac{P_s}{\sigma_0^2}\gamma_{\mathsf{h}}^2 - 64\frac{P_s}{\sigma_0^2}\gamma_{\mathsf{g}}^2\frac{m_2}{m_1} + 120\gamma_{\mathsf{h}})m_1 x^3 \\ &+ (-120\overline{\mathbf{P}}_{\mathsf{total}} + 12)\gamma_{\mathsf{h}} m_1 x^2 + (30\overline{\mathbf{P}}_{\mathsf{total}} - 12)\overline{\mathbf{P}}_{\mathsf{total}}\gamma_{\mathsf{h}} m_1 x + 3\overline{\mathbf{P}}_{\mathsf{total}}^2\gamma_{\mathsf{h}} m_1 = 0. \end{aligned} \tag{3.87}$$

3.5.3 RE Scheme

For RE scheme, all the amplifying powers are distributed on the two best selected relays. Hence, the optimization problem for RE model can be formulated as

$$\begin{aligned} &\text{minimize } \ m_1 \ \mathrm{SEP}_{\mathrm{PU}}^{\infty} + m_2 \ \mathrm{SEP}_{\mathrm{SU}}^{\infty} \\ &\text{subject to: } 2\mathcal{P}_{\mathsf{re}} + 2\lambda_{\mathsf{re}} \leq \overline{\mathbf{P}}_{\mathsf{total}}. \end{aligned} \tag{3.88}$$

Following the previously-mentioned procedure in solving (3.85) results in the optimal $\lambda_{\mathsf{re}}^{\mathrm{opt}}$ real positive solution of a seventh order equation which is given by

$$\begin{aligned}
&64\frac{P_s}{\sigma_0^2}\gamma_{\mathsf{h}}^3 m_1 x^7 + 96\frac{P_s}{\sigma_0^2}\gamma_{\mathsf{h}}^2 m_1\left(\frac{P_s}{\sigma_0^2}\gamma_{\mathsf{g}} - \overline{\mathbf{P}}_{\mathsf{total}}\frac{P_s}{\sigma_0^2}\gamma_{\mathsf{h}} - 2\right)x^6\\
&+ 48\overline{\mathbf{P}}_{\mathsf{total}}\frac{P_s}{\sigma_0^2}\gamma_{\mathsf{h}}^2 m_1\left(\overline{\mathbf{P}}_{\mathsf{total}}\frac{P_s}{\sigma_0^2}\gamma_{\mathsf{h}} - 2\frac{P_s}{\sigma_0^2}\gamma_{\mathsf{g}} + 4\right)x^5 + 8\frac{P_s}{\sigma_0^2}\gamma_{\mathsf{h}} m_1\\
&\times\left(3\overline{\mathbf{P}}_{\mathsf{total}}^2\frac{P_s}{\sigma_0^2}\gamma_{\mathsf{h}}\gamma_{\mathsf{g}} - \overline{\mathbf{P}}_{\mathsf{total}}^3\frac{P_s}{\sigma_0^2}\gamma_{\mathsf{h}}^2 - 6\overline{\mathbf{P}}_{\mathsf{total}}^2\gamma_{\mathsf{h}} - 16\frac{P_s}{\sigma_0^2}\gamma_{\mathsf{g}}^3\frac{m_2}{m_1} - 6\overline{\mathbf{P}}_{\mathsf{total}}\gamma_{\mathsf{h}} + 30\gamma_{\mathsf{g}} - \frac{54}{\frac{P_s}{\sigma_0^2}}\right)x^4\\
&+ 24\frac{P_s}{\sigma_0^2}\gamma_{\mathsf{h}} m_1\left(2\overline{\mathbf{P}}_{\mathsf{total}}^2\gamma_{\mathsf{h}} - 10\overline{\mathbf{P}}_{\mathsf{total}}\gamma_{\mathsf{g}} + \gamma_{\mathsf{g}} + \frac{18\overline{\mathbf{P}}_{\mathsf{total}} - 10}{\frac{P_s}{\sigma_0^2}}\right)x^3\\
&+ 12\overline{\mathbf{P}}_{\mathsf{total}}\frac{P_s}{\sigma_0^2}\gamma_{\mathsf{h}} m_1\left(5\overline{\mathbf{P}}_{\mathsf{total}}\gamma_{\mathsf{g}} - \overline{\mathbf{P}}_{\mathsf{total}}^2\gamma_{\mathsf{h}} - 2\gamma_{\mathsf{g}} - \frac{9\overline{\mathbf{P}}_{\mathsf{total}}}{\frac{P_s}{\sigma_0^2}} + \frac{20}{\frac{P_s}{\sigma_0^2}} - \frac{1}{\overline{\mathbf{P}}_{\mathsf{total}}\frac{P_s}{\sigma_0^2}}\right)x^2\\
&+ 6\overline{\mathbf{P}}_{\mathsf{total}}\gamma_{\mathsf{h}} m_1\left(\overline{\mathbf{P}}_{\mathsf{total}}\frac{P_s}{\sigma_0^2}\gamma_{\mathsf{g}} - 10\overline{\mathbf{P}}_{\mathsf{total}} + 2\right)x - 3\overline{\mathbf{P}}_{\mathsf{total}}^2\gamma_{\mathsf{h}} m_1 = 0. \qquad (3.89)
\end{aligned}$$

3.6 Power Allocation for SUM Rate Maximization

In this section, the power allocation optimization problems for maximizing the average achievable sum rate of the proposed system are formulated. Similar to SEP optimization case, the average achievable sum rate is a function of SU transmission powers (i.e., P_{A} and P_{R}) and the relays amplifying factors (i.e., λ_{A}, λ_{R}, λ_{B_1}, and λ_{B_2}). The goal is to find the optimal values which maximize the weighted sum of the average achievable sum rate.

3.6.1 AP Scheme

In this section, the power allocation optimization problem for maximizing the average achievable sum rate of the proposed system was formulated. Similar to SEP section, The average achievable sum rate is a function of SU transmission power (i.e., P_{A} and P_{R}) and the three relays amplifying factors (i.e., λ_{A}, λ_{R}, λ_{B_1}, and λ_{B_2}). The goal is to find the optimal values which maximize the average achievable sum rate. Hence, the optimization problem has been formulated such that:

$$\begin{aligned} &\text{maximize } \ m_1\mathcal{R}_{\text{PU}} + m_2\mathcal{R}_{\text{SU}} \\ &\text{subject to: } 2\mathcal{P}_{\mathsf{ap}} + 4\lambda_{\mathsf{ap}} \leq \overline{\mathbf{P}}_{\mathsf{total}}. \end{aligned} \tag{3.90}$$

For simplicity at high SNR region, the achievable rate at PU network is approximated using the formula given by

$$\Phi\left(a, b, z\right) \approx z^{-a} \tag{3.91}$$

which simplifies $\mathcal{R}_{\text{PU}}$ in (3.58) for AP scheme to be

$$\mathcal{R}_{\text{PU}}^{\text{AP}} \approx \frac{3}{2\beta_{\mathsf{ap}}} \tag{3.92}$$

Following the same steps in the previous Section in solving (3.82), the optimal solution for rate maximization is obtained such that for AP scheme, the optimal amplifying factor $\lambda_{\text{opt}}^{\text{AP}}$ is

$$\lambda_{\text{opt}}^{\text{AP}} = \frac{\sqrt{6\gamma_{\mathsf{g}}\gamma_{\mathsf{h}}m_1m_2}}{4\gamma_{\mathsf{h}}m_2} - \frac{1}{2} \qquad , \text{for} \qquad \frac{2}{3} < \frac{m_1\gamma_{\mathsf{g}}}{m_2\gamma_{\mathsf{h}}} < \frac{\left(\overline{\mathbf{P}}_{\mathsf{total}} + 2\right)^2}{6} \tag{3.93}$$

Hence, the optimal SU transmission power $\mathcal{P}_{\mathsf{ap}}$ is given by

$$\mathcal{P}_{\mathsf{ap}}^{\text{opt}} = \frac{1}{2}\left(\overline{\mathbf{P}}_{\mathsf{total}} - 4\lambda_{\mathsf{ap}}^{\text{opt}}\right). \tag{3.94}$$

3.6.2 RS Scheme

For RS scheme, the amplifying factors are assigned to the best selected relay. Hence, the optimization problem can be formulated as

$$\begin{aligned} &\text{maximize } \ m_1\mathcal{R}_{\text{PU}}^{\text{RS}} + m_2\mathcal{R}_{\text{SU}}^{\text{RS}} \\ &\text{subject to: } 2\mathcal{P}_{\mathsf{rs}} + 2\lambda_{\mathsf{rs}} \leq \overline{\mathbf{P}}_{\mathsf{total}}. \end{aligned} \tag{3.95}$$

For simplicity at high SNR region, the achievable rate at PU network is approximated using the formula given by

$$\Phi\left(a, b, z\right) \approx z^{-a}, \tag{3.96}$$

which simplifies $\mathcal{R}_{\text{PU}}$ in (3.71) for RS scheme to be

$$\mathcal{R}_{\text{PU}}^{\text{RS}} \approx \frac{3}{4\beta_{\mathsf{rs}}}. \tag{3.97}$$

Following the same steps in the previous section, the optimal amplifying factor $\lambda_{\mathsf{rs}}^{\mathrm{opt}}$ for rate maximization in RS scheme is given by

$$\lambda_{\mathsf{rs}}^{\mathrm{opt}} = \frac{\sqrt{3\gamma_{\mathsf{g}}\gamma_{\mathsf{h}}m_1m_2}}{2\gamma_{\mathsf{h}}m_2} - \frac{1}{2}, \qquad \text{for} \qquad \frac{1}{3} < \frac{m_1\gamma_{\mathsf{g}}}{m_2\gamma_{\mathsf{h}}} < \frac{\left(\overline{\mathbf{P}}_{\mathsf{total}} + 1\right)^2}{3}. \tag{3.98}$$

Then, the optimal SU transmission power $\mathcal{P}_{\mathsf{rs}}$ is given by

$$\mathcal{P}_{\mathsf{rs}}^{\mathrm{opt}} = \frac{1}{2}\left(\overline{\mathbf{P}}_{\mathsf{total}} - 2\lambda_{\mathsf{rs}}^{\mathrm{opt}}\right). \tag{3.99}$$

3.6.3 RE Scheme

For RE scheme, the amplifying factors are distributed on the best two selected relays. Hence, the optimization problem can be formulated as

$$\begin{aligned} &\text{maximize } \; m_1\mathcal{R}_{\mathrm{PU}}^{\mathrm{RE}} + m_2\mathcal{R}_{\mathrm{SU}}^{\mathrm{RE}} \\ &\text{subject to: } 2\mathcal{P}_{\mathsf{re}} + 2\lambda_{\mathsf{re}} \leq \overline{\mathbf{P}}_{\mathsf{total}}. \end{aligned} \tag{3.100}$$

Again for simplicity, the asymptotic rate equation is obtained by

$$\mathcal{R}_{\mathrm{PU}}^{\mathrm{RE}} \approx \frac{4}{3\beta_{\mathsf{re}}}. \tag{3.101}$$

Similarly, the optimal amplifying factor $\lambda_{\mathsf{re}}^{\mathrm{opt}}$ in RE scheme is given by

$$\lambda_{\mathsf{re}}^{\mathrm{opt}} = \frac{\sqrt{\gamma_{\mathsf{g}}\gamma_{\mathsf{h}}m_1m_2}}{\gamma_{\mathsf{h}}m_2} - \frac{1}{2}, \qquad \text{for} \qquad \frac{1}{4} < \frac{m_1\gamma_{\mathsf{g}}}{m_2\gamma_{\mathsf{h}}} < \left(\overline{\mathbf{P}}_{\mathsf{total}} + \frac{1}{2}\right)^2. \tag{3.102}$$

Then, the optimal SU transmission power $\mathcal{P}_{\mathsf{re}}$ is given by

$$\mathcal{P}_{\mathsf{re}}^{\mathrm{opt}} = \frac{1}{2}\left(\overline{\mathbf{P}}_{\mathsf{total}} - 2\lambda_{\mathsf{re}}^{\mathrm{opt}}\right). \tag{3.103}$$

3.7 Physical Layer Security Approach

In this section, the secrecy performance of the proposed model is investigated in the present of a single eavesdropper. Assume that the eavesdropper knows about the cooperation between PU and SU networks to transmit the PU data. The following discussion presents two PHY layer security scenarios based on the cooperation schemes used between PU and SU networks (i.e., AP or RS schemes). In the case of AP scheme, the relay nodes apply a cooperative beamforming (CB) scenario. While in the case of RS scheme, the Relay and Jamming (R-J) scenario is applied. Both scenarios are discussed as follows:

3.7.1 Scenario I: Cooperative Beamforming (CB)

In this scenario, Both PU and SU networks agree to apply AP cooperation scheme discussed in Section 3.3.2 which employs all relay nodes in PU transmission during the broadcasting phase. Hence, the CB scenario is applicable to enhance secrecy performance of PU network in the present of a single eavesdropper attacking PU network transmission. In this scenario, each relay broadcasts a weighted version of PU data received during MA phase.

During the BC phase, each relay node re-transmits a weighted version of the previously received PU message to maximize the total SNR received at each PU destination node (i.e., X and Y) such that

$$\widetilde{\mathbf{z}}_{\mathsf{X}} = \mathbf{g}_{\mathsf{X}}^{*}\mathbf{v}\mathbf{g}_{\mathsf{Y}}y + \widetilde{w}_{\mathsf{X}}, \tag{3.104}$$

$$\widetilde{\mathbf{z}}_{\mathsf{Y}} = \mathbf{g}_{\mathsf{Y}}^{*}\mathbf{v}\mathbf{g}_{\mathsf{X}}x + \widetilde{w}_{\mathsf{Y}}, \tag{3.105}$$

where $\mathbf{v}$ is 2×1 matrix of the weights v_1 and v_2. Then, the received signal at E is given by

$$\widetilde{\mathbf{z}}_{\mathsf{E}} = \mathbf{f}_{\mathsf{E}}^{*}\mathbf{v}\mathbf{g}_{\mathsf{X}}x + \mathbf{f}_{\mathsf{E}}^{*}\mathbf{v}\mathbf{g}_{\mathsf{Y}}y + \widetilde{w}_{\mathsf{E}}. \tag{3.106}$$

Hence, the total achievable rate for PU network is given by

$$\mathcal{R}_{\text{PU}} = \frac{1}{2}\log_2\left(1 + \frac{P_s\mathbf{g}_{\mathsf{Y}}^{T}\mathbf{V}\mathbf{g}_{\mathsf{X}}\mathbf{g}_{\mathsf{X}}^{H}\mathbf{V}^{H}\mathbf{g}_{\mathsf{Y}}^{*}}{\left(\mathbf{g}_{\mathsf{Y}}^{T}\mathbf{V}\mathbf{V}^{H}\mathbf{g}_{\mathsf{Y}}^{*} + 1\right)\sigma^2}\right) + \frac{1}{2}\log_2\left(1 + \frac{P_s\mathbf{g}_{\mathsf{X}}^{T}\mathbf{V}\mathbf{g}_{\mathsf{Y}}\mathbf{g}_{\mathsf{Y}}^{H}\mathbf{V}^{H}\mathbf{g}_{\mathsf{X}}^{*}}{\left(\mathbf{g}_{\mathsf{X}}^{T}\mathbf{V}\mathbf{V}^{H}\mathbf{g}_{\mathsf{X}}^{*} + 1\right)\sigma^2}\right) \tag{3.107}$$

On the other hand, the achievable rate at the eavesdropper E is given by

$$\mathcal{R}_{\text{E}} = \frac{1}{2}\log_2\left(1 + \frac{P_s\left|f_{\mathsf{XE}}\right|^2 + P_s\left|f_{\mathsf{YE}}\right|^2}{\mathcal{P}\left|f_{\mathsf{AE}}\right|^2 + \sigma^2} + \frac{P_s\mathbf{g}_{\mathsf{X}}^{T}\mathbf{V}\mathbf{f}_{\mathsf{E}}\mathbf{f}_{\mathsf{E}}^{H}\mathbf{V}^{H}\mathbf{g}_{\mathsf{X}}^{*} + P_s\mathbf{g}_{\mathsf{Y}}^{T}\mathbf{V}\mathbf{f}_{\mathsf{E}}\mathbf{f}_{\mathsf{E}}^{H}\mathbf{V}^{H}\mathbf{g}_{\mathsf{Y}}^{*}}{\left(\mathbf{g}_{\mathsf{X}}^{T}\mathbf{V}\mathbf{V}^{H}\mathbf{g}_{\mathsf{X}}^{*} + \mathbf{g}_{\mathsf{Y}}^{T}\mathbf{V}\mathbf{V}^{H}\mathbf{g}_{\mathsf{Y}}^{*} + 1\right)\sigma^2}\right) \tag{3.108}$$

The goal in this scenario is to find the optimal weights which guarantees a positive secrecy rate $\mathcal{R}_S$ at both PU destinations nodes which is given by

$$\begin{aligned}\mathcal{R}_S &= [\mathcal{R}_{\text{PU}} - \mathcal{R}_{\mathsf{E}}]^+\\ &= \frac{1}{2}\left[\log_2\left(1+\frac{P_s\mathbf{g}_{\mathsf{Y}}^T\mathbf{V}\mathbf{g}_{\mathsf{X}}\mathbf{g}_{\mathsf{X}}^H\mathbf{V}^H\mathbf{g}_{\mathsf{Y}}^*}{\left(\mathbf{g}_{\mathsf{Y}}^T\mathbf{V}\mathbf{V}^H\mathbf{g}_{\mathsf{Y}}^*+1\right)\sigma^2}\right)+\log_2\left(1+\frac{P_s\mathbf{g}_{\mathsf{X}}^T\mathbf{V}\mathbf{g}_{\mathsf{Y}}\mathbf{g}_{\mathsf{Y}}^H\mathbf{V}^H\mathbf{g}_{\mathsf{X}}^*}{\left(\mathbf{g}_{\mathsf{X}}^T\mathbf{V}\mathbf{V}^H\mathbf{g}_{\mathsf{X}}^*+1\right)\sigma^2}\right)\right.\\ &\left.-\log_2\left(1+\frac{P_s\left|f_{\mathsf{XE}}\right|^2+P_s\left|f_{\mathsf{YE}}\right|^2}{\mathcal{P}\left|f_{\mathsf{AE}}\right|^2+\sigma^2}+\frac{P_s\mathbf{g}_{\mathsf{X}}^T\mathbf{V}\mathbf{f}_{\mathsf{E}}\mathbf{f}_{\mathsf{E}}^H\mathbf{V}^H\mathbf{g}_{\mathsf{X}}^*+P_s\mathbf{g}_{\mathsf{Y}}^T\mathbf{V}\mathbf{f}_{\mathsf{E}}\mathbf{f}_{\mathsf{E}}^H\mathbf{V}^H\mathbf{g}_{\mathsf{Y}}^*}{\left(\mathbf{g}_{\mathsf{X}}^T\mathbf{V}\mathbf{V}^H\mathbf{g}_{\mathsf{X}}^*+\mathbf{g}_{\mathsf{Y}}^T\mathbf{V}\mathbf{V}^H\mathbf{g}_{\mathsf{Y}}^*+1\right)\sigma^2}\right)\right]^+\end{aligned} \tag{3.109}$$

Since the eavesdropper's CSI is assumed to be unavailable at each of the proposed system nodes, an optimization problem is formulated to find the optimal weights which maximize the total achievable rate at each of PU nodes such as

$$\begin{aligned}&\text{maximize } \ \mathcal{R}_{\text{PU}}\\ &\text{subject to: } \mathbf{V}\mathbf{V}^H = 2\lambda_{\mathsf{ap}}^{\text{opt}}\end{aligned} \tag{3.110}$$

$$v_1^2 = \frac{2\left(\sqrt{\frac{1}{|g_{\mathsf{iY}}|^2|g_{\mathsf{jY}}|^2}+\frac{1}{|g_{\mathsf{iX}}|^2|g_{\mathsf{jX}}|^2}+\frac{1}{|g_{\mathsf{iY}}|^2|g_{\mathsf{jX}}|^2}+\frac{1}{|g_{\mathsf{jY}}|^2|g_{\mathsf{iX}}|^2}}-\frac{1}{|g_{\mathsf{iY}}|^2}-\frac{1}{|g_{\mathsf{iX}}|^2}\right)}{\frac{1}{|g_{\mathsf{iY}}|^2}+\frac{1}{|g_{\mathsf{jY}}|^2}+\frac{1}{|g_{\mathsf{iX}}|^2}+\frac{1}{|g_{\mathsf{jY}}|^2}}\lambda_{\mathsf{ap}}^{\text{opt}} \tag{3.111}$$

Hence, the value of v_2^2 is given by

$$v_2^2 = 2\lambda_{\mathsf{ap}}^{\text{opt}} - v_1^2 \tag{3.112}$$

3.7.2 Scenario II: Relay and Jamming (R-J)

In this scenario, the cooperation is applied between PU and SU network as discussed in Section 3.3.2 which employs the relay node with the best channel conditions to broadcast PU messages received during MA phase while the other relay keeps idle. Hence, the R-J scenario is suitable to enhance secrecy performance of PU network against a single passive eavesdropper attack. During the BC phase, while the selected relay re-transmits the previously received message, the second two relays transmit a friendly jamming signals with a certain power P_{J} to harm the wiretap channel and confuse the eavesdropper. The key assumption made here is that the sources have perfect knowledge of the jamming signals transmitted by the friendly jammer node. Then, the jamming signal harms only the wiretap channel. Hence, E receives the following signals

$$z_{\mathsf{E}}^{(3)} = f_{\mathsf{i}^*\mathsf{E}}\beta_{\mathsf{i}^*} z_{\mathsf{i}^*}^{(1)} + \sum_{\mathsf{i}\neq\mathsf{i}^*} \sqrt{P_{\mathrm{J}_\mathsf{i}}} f_{\mathsf{iE}} s_{\mathrm{J}_\mathsf{i}} + w_{\mathsf{E}}^{(3)}, \tag{3.113}$$

$$z_{\mathsf{E}}^{(4)} = f_{\mathsf{i}^*\mathsf{E}}\beta_{\mathsf{i}^*} z_{\mathsf{i}^*}^{(2)} + \sum_{\mathsf{i}\neq\mathsf{i}^*} \sqrt{P_{\mathrm{J}_\mathsf{i}}} f_{\mathsf{iE}} s_{\mathrm{J}_\mathsf{i}} + w_{\mathsf{E}}^{(4)}, \tag{3.114}$$

where $\mathsf{i} \in \{\mathrm{A}, \mathrm{B}, \mathrm{R}\}$, i^* denotes the index of selected relay and $\mathsf{i} \neq \mathsf{i}^*$ denotes the friendly jammers such that $\mathsf{i}^* \in \{\mathrm{R}, \mathrm{B}\}$ during the third time slot, whereas $\mathsf{i}^* \in \{\mathrm{A}, \mathrm{B}\}$ during the fourth time slot, $f_{\mathsf{i}^*\mathsf{E}}$ denotes the channel coefficient between the i^*-th selected relay and E, $f_{\mathsf{iE}}, \mathsf{i} \neq \mathsf{i}^*$ denotes the channel coefficient between the unselected relays (i.e., friendly jammers) and E, $P_{\mathrm{J}_\mathsf{i}}$ denotes the jamming power, and w_{E} denotes the AWGN sample at E with zero mean and variance σ_0^2. Hence, the maximum achievable rate at E can be expressed as

$$\mathcal{R}_{\mathsf{E}} = \frac{1}{2}\log_2\left(1 + \frac{P_s\beta_{\mathsf{i}^*}|g_{\mathsf{Xi}^*}|^2|f_{\mathsf{i}^*\mathsf{E}}|^2 + P_s\beta_{\mathsf{i}^*}|g_{\mathsf{Yi}^*}|^2|f_{\mathsf{i}^*\mathsf{E}}|^2}{\left(1+\beta_{\mathsf{i}^*}|f_{\mathsf{i}^*\mathsf{E}}|^2\right)\sigma^2 + \sum_{\mathsf{i}\neq\mathsf{i}^*} P_{\mathrm{J}_\mathsf{i}}|f_{\mathsf{iE}}|^2}\right). \tag{3.115}$$

Then, the secrecy rate of the proposed model with RS scheme at each PU node (i.e., X and Y) is given by

$$\begin{aligned}\mathcal{R}_S &= \left[\mathcal{R}_{\mathrm{PU}} - \mathcal{R}_{\mathsf{E}}\right]^+ \\ &= \frac{1}{2}\Bigg[\log_2\left(1 + \frac{P_s\beta_{\mathsf{i}^*}|g_{\mathsf{i}^*\mathsf{X}}|^4}{\left(1+\beta_{\mathsf{i}^*}|g_{\mathsf{i}^*\mathsf{X}}|^2\right)\sigma^2}\right) + \log_2\left(1 + \frac{P_s\beta_{\mathsf{i}^*}|g_{\mathsf{i}^*\mathsf{Y}}|^4}{\left(1+\beta_{\mathsf{i}^*}|g_{\mathsf{i}^*\mathsf{Y}}|^2\right)\sigma^2}\right) \\ &\quad - \log_2\left(1 + \frac{P_s\beta_{\mathsf{i}^*}|g_{\mathsf{Xi}^*}|^2|f_{\mathsf{i}^*\mathsf{E}}|^2 + P_s\beta_{\mathsf{i}^*}|g_{\mathsf{Yi}^*}|^2|f_{\mathsf{i}^*\mathsf{E}}|^2}{\left(1+\beta_{\mathsf{i}^*}|f_{\mathsf{i}^*\mathsf{E}}|^2\right)\sigma^2 + \sum_{\mathsf{i}\neq\mathsf{i}^*} P_{\mathrm{J}_\mathsf{i}}|f_{\mathsf{iE}}|^2}\right)\Bigg]^+, \end{aligned} \tag{3.116}$$

where $[.]^+$ represents $\max(.,0)$. It is clear that $\mathcal{R}_S$ depends on the amount of available jamming powers $P_{\mathrm{J}_\mathsf{i}}$. Hence, increasing the jamming powers increases the secrecy capacity $\mathcal{R}_S$ but on the other hand, it harms PU network achievable rate as the total amount of power available to the PU network is limited to $\lambda_{\mathsf{rs}}^{\mathrm{opt}}$. To solve this problem, the PU network adjusts a certain required rate $\mathcal{R}_Q$ such that $\mathcal{R}_Q < \mathcal{R}_{\mathrm{PU}}^{\mathrm{RS,max}}$. Then, the optimal amplification factor λ_Q can be obtained such as

$$\begin{aligned} &\text{Minimize } \lambda_Q \\ &\text{subject to: } \mathcal{R}_{\mathrm{PU}} = \mathcal{R}_Q < \mathcal{R}_{\mathrm{PU}}^{\mathrm{RS,max}} \\ &\qquad \sum_{\mathsf{i}\neq\mathsf{i}^*} P_{\mathrm{J}_\mathsf{i}} + \lambda_Q = \lambda_{\mathsf{rs}}^{\mathrm{opt}}. \end{aligned} \tag{3.117}$$

Following the same steps in solving (3.85) in the previous section , the optimal value is given by

$$\lambda_Q = \frac{1}{\frac{3P_{\mathrm{s}}\gamma_{\mathrm{g}}}{4\mathcal{R}_Q} - 2}. \tag{3.118}$$

3.8 Numerical Results

Numerical examples are presented to verify the performance of the proposed schemes. The proposed AP and RS cooperative schemes transmit five data symbols in four-time slots with a bandwidth efficiency of 1.25. On the other hand, the proposed RE cooperative scheme transmits five data symbols in three-time slots resulting in a bandwidth efficiency of 1.67. Whereas, the conventional TWR-AF proposed in [88] transmits two data symbols in two-time slots with a bandwidth efficiency of 1. The proposed system performance is compared with the conventional TWR-AF model in [88] and for a fair comparison, the total power budget of the proposed cooperative schemes is set to be the same as the power budget in [88].

A SEP performance comparison between the different proposed cooperative schemes and the conventional TWR-AF is presented in Figure 3.3. At low SNR values, results show that both AP and RS cooperative schemes provide a SEP performance similar to the conventional TWR-AF model. As the SNR goes higher, the RS scheme outperforms the AP cooperative scheme and the conventional TWR-AF scheme. Although the SEP performance of the AP scheme becomes a

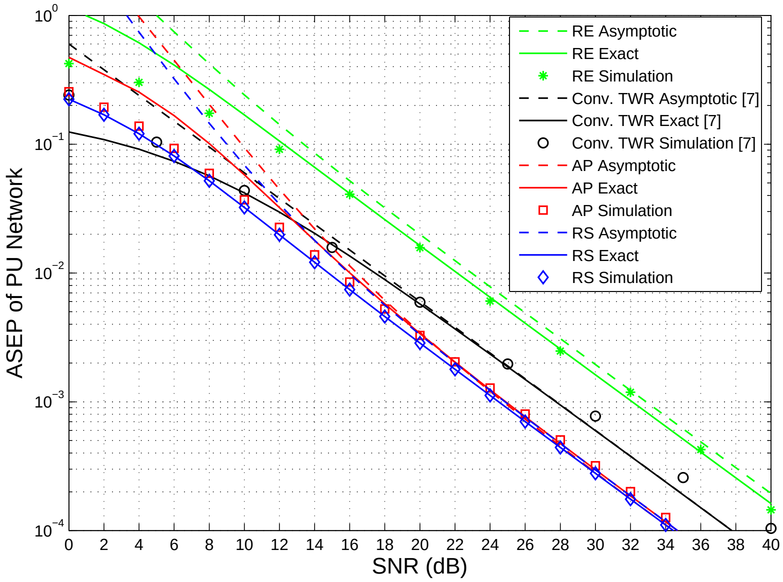


Figure 3.3: ASEP comparison between the proposed cooperative cognitive TWR-AF schemes and the conventional one.

bit worse than the RS scheme, the AP scheme still outperforms the conventional TWR-AF model. This advantage of the proposed AP and RS schemes encourages the PU system to cooperate with the SU network. It is important to clarify that the RS scheme enhances the SEP performance more than the AP scheme because of the concentration of the transmission power at the selected best relay instead of the equal transmission power distribution used in the AP scheme. On the other hand, it is clear that the proposed RE scheme provides the worst SEP performance. This is because the proposed RE model depends on choosing the best two relays out of three relays to transmit two different pairs of data (i.e., (x_1, y_1) and (x_2, y_2)), this harms the SEP performance of this scheme due to joint detection used at each PU node.

The SU SEP performance is presented in Figure 3.4 where the SU SEP is

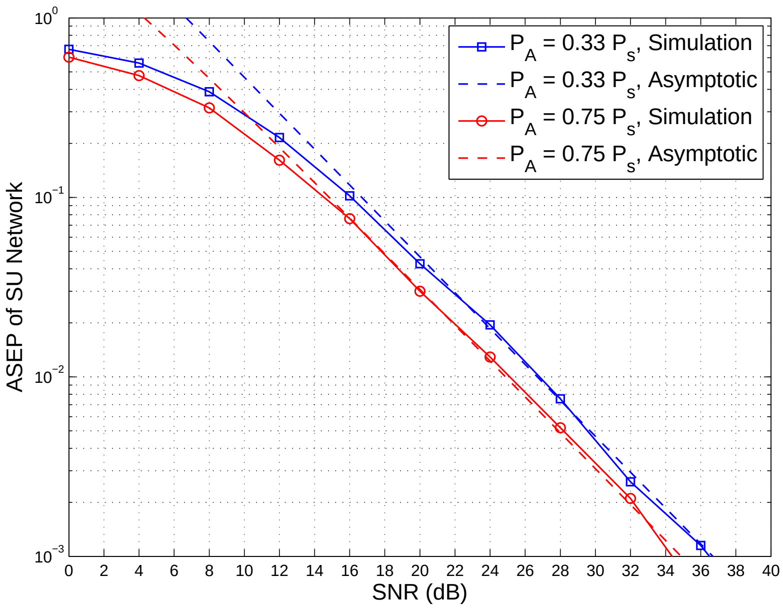


Figure 3.4: The SEP performance of SU network for different SU transmission power $P_A = \mathcal{P} = 0.33P_{\mathsf{s}}$ and $0.75P_{\mathsf{s}}$.

studied against different values of SU transmission power $P_{\mathsf{A}} = P_{\mathsf{R}} = \mathcal{P}$. It can be seen from this figure that the SU SEP performance is improved with increasing the SU transmission power, as expected. Moreover, the asymptotic formulas are shown to match with simulation results at medium-to-high SNR values which verifies the ability of these asymptotic formulas to represent the SU SEP performance in all derived mathematical expressions through this work.

The outage probability performance of different cooperative schemes is studied in Figure 3.5. We can see that the RS scheme provides the worst outage performance compared to the other two proposed schemes. These results could be confusing in comparison with the SEP performance of each scheme presented in Figure 3.3. But this confusion can be clarified as the PU receivers at RE scheme utilize a JMLD process to detect both transmitted PU symbols simulta-

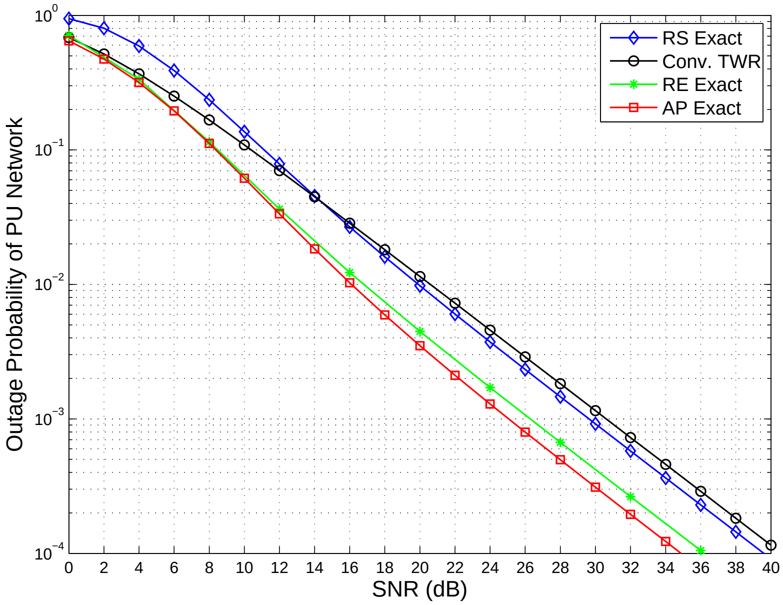


Figure 3.5: Outage probability comparison between the proposed cooperative cognitive TWR-AF schemes and the conventional TWR-AF model.

neously. On the other hand, the PU receivers utilize MLD process in the case of RS scheme. Then, the joint detection of two PU symbols clearly degrades the system performance.

Figure 3.6 presents a comparison between the proposed models and the conventional TWR-AF network from the PU maximum achievable rate point of view. It can be seen that the RE scheme provides the best achievable rate since it transmits a complete five data symbols (i.e., four PU symbols + one SU symbol) in three-time slots resulting in a bandwidth efficiency of 1.67. On the other hand, AP and RS schemes achieve a bandwidth efficiency of 1.25, and the conventional TWR-AF model achieves a bandwidth efficiency of 1. Hence, this considerable rate performance improvement of the proposed RE scheme encourages the authors to study its performance as an alternative scheme which could be efficient

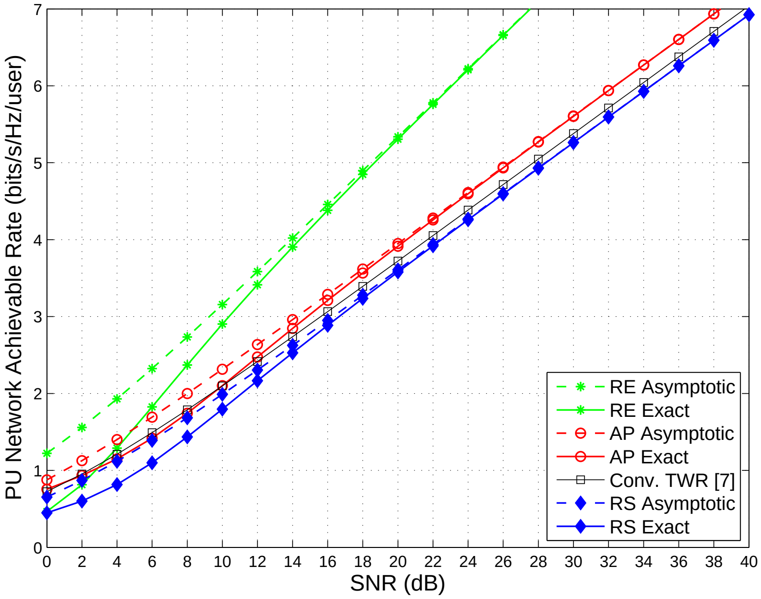


Figure 3.6: PU network achievable rate comparison between the proposed cooperative cognitive TWR-AF schemes and the conventional TWR-AF scheme.

in network applications of high data rate and acceptable low SEP performance. In addition, the RS model provides the worst rate performance as the RS scheme depends only on one relay node in transmitting its data which could be interfered by the resultant SU detection error signal. It is important to clarify that although the PU rate of the proposed RS scheme is worse than that of the conventional TWR-AF model, the total achievable sum rate of the RS scheme (i.e., the PU network and the SU network) is higher than the total achievable sum rate of the TWR-AF model (i.e., the PU network only).

The AP SEP performance against the relay amplification factor λ_{ap} is presented in Figure 3.7 with SNR = 30 dB. It is clear that the PU SER is a convex function w.r.t. λ_{ap}. Hence, a unique optimal value $\lambda_{\mathsf{ap}}^{\mathrm{opt}}$ exists. Results clarify the effect of the weighted sum of PU and SU SEPs (i.e., $m_1 : m_2$) on the proposed

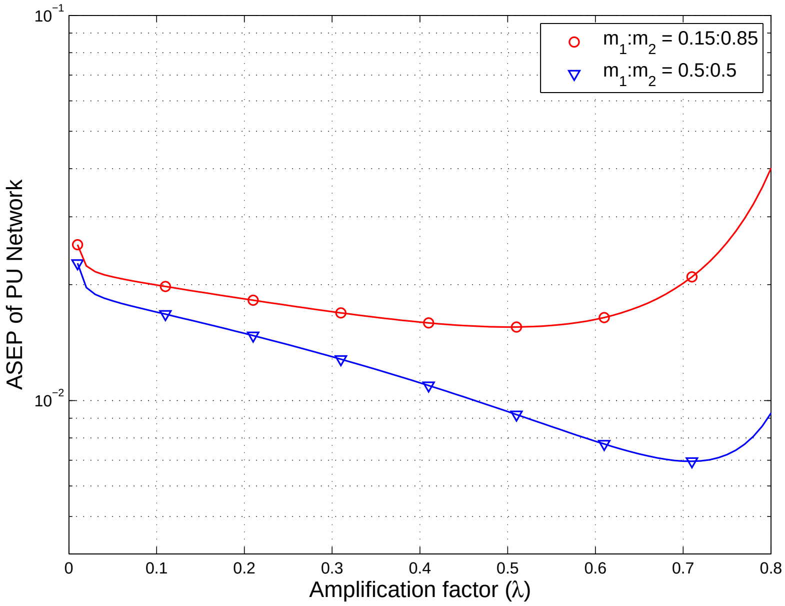


Figure 3.7: The PU SEP performance of the proposed AP scheme against the amplification factor λ_{ap} for different SER sum ratio, i.e., $m_1 : m_2 = 1 : 1$ and $1 : 5$ at SNR $= 30$ dB.

system performance. It is clear that the optimal value $\lambda_{\mathsf{ap}}^{\mathrm{opt}}$ is affected by the values of m_1 and m_2 resulting in enhancing or degrading the PU SEP performance.

The SEP performance of both RS and RE schemes against their relay amplification factors λ_{rs} and λ_{re} is introduced in Figure 3.8 with SNR $= 30$ dB. It can be seen that the SEP performances of both RS and RE schemes are affected by the weights ratio $m_1 : m_2$. Moreover, we can see that the RS scheme outperforms the RE scheme for all values of λ. Also, the RS scheme is more sensitive to the ratio $m_1 : m_2$ than the RE scheme, because of its operation nature. This weight ratio sensitivity could be clearly observed based on the changing on the optimal amplify factor corresponding to the change in the weight ratios (i.e., $m_1 : m_2$). For the RS model, it can be noticed that the optimal amplifying factor $\lambda_{\mathsf{rs}}^{\mathrm{opt}}$ has

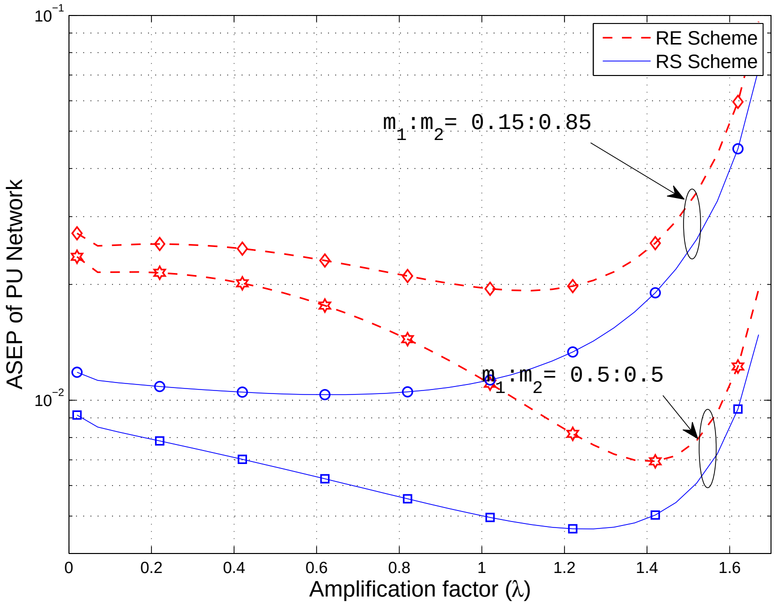


Figure 3.8: The PU SEP performances of the proposed RS and RE schemes against the amplification factor $\lambda_{\mathsf{rs}} = \lambda_{\mathsf{re}} = \lambda$ for different SER sum ratio, i.e., $m_1 : m_2 = 1 : 1$ and $1 : 5$ at SNR $= 30$ dB.

been shifted to the left from the value of $1.2P_{\mathsf{s}}$ with $m_1 : m_2 = 0.5 : 0.5$ to a new value of $0.4P_{\mathsf{s}}$ with $m_1 : m_2 = 0.15 : 0.85$ resulting in a difference of $0.8P_{\mathsf{s}}$. Whereas, for the RE model, the optimal amplifying factor $\lambda_{\mathsf{re}}^{\mathrm{opt}}$ has been shifted to the left from the value of $1.4P_{\mathsf{s}}$ with $m_1 : m_2 = 0.5 : 0.5$ to a new value of $1P_{\mathsf{s}}$ with $m_1 : m_2 = 0.15 : 0.85$ resulting in a difference of $0.4P_{\mathsf{s}}$. Hence, it is clear that the RS model is more sensitive to the weight ratio more than the RE model.

The AP rate performance against λ_{ap} is presented in Figure 3.9. It is clear that the AP rate is a concave function w.r.tλ_{ap} resulting in an optimal value $\lambda_{\mathsf{ap}}^{\mathrm{opt}}$. Results demonstrate that $\lambda_{\mathsf{ap}}^{\mathrm{opt}}$ is almost a constant value for different SNR values.

Similarly, the RS and RE achievable rate performance against $\lambda_{\mathsf{rs}} = \lambda_{\mathsf{re}} = \lambda$ is presented in Figure 3.10. Both RS and RE achievable rates are concave functions w.r.t. λ resulting in a unique optimal values $\lambda_{\mathsf{rs}}^{\mathrm{opt}}$ and $\lambda_{\mathsf{re}}^{\mathrm{opt}}$. From the achievable rate viewpoint, results show that the RE scheme always outperforms the RS scheme for all values of λ and under different SNR conditions.

The PHY security performance of the proposed scenarios is presented in Figure 3.11 and Figure 3.12. The secrecy performance of Scenario I: CB approach is presented in Figure 3.11. Since the CB approach is applicable with the AP scheme, then, results show the effect $\lambda_{\mathsf{ap}}^{\mathrm{opt}}$ on the secrecy performance. It is clear that increasing $\lambda_{\mathsf{ap}}^{\mathrm{opt}}$ enhances the secrecy performance but it might be limited to a certain maximum value based on the allowable SU transmission power $\mathcal{P}_{\mathsf{ap}}$. Moreover, results show that the AP scheme can achieve a non-zero secrecy rate in the presence of a single passive eavesdropper.

The secrecy performance of R-J approach is studied in Figure 3.12. The R-J PHY security model is applicable to RS and RE schemes as there is at least one idle relay during each data transmission. This unselected/eliminated relay is used as a friendly jammer at the eavesdropper. It is obvious that the R-J approach with RS scheme can achieve a non-zero secrecy rate in the presence of a single passive eavesdropper.

Recently, the security reliability trade-off analysis has been presented as an efficient method to study the penalty that the communication systems should pay from their reliability performance to enhance their secrecy performance [94]. The security reliability trade-off analysis of the proposed cooperative TWR-AF model is discussed in Figure 3.13 and Figure 3.14 in which the system intercept probability represents the system secrecy performance and the system outage probability represents the system reliability performance. The system intercept probability is defined as the probability that the wiretap channel rate exceeds a predefined threshold.

The SRT analysis of AP cooperative scheme with CB technique is presented in Figure 3.13 and compared to the SRT analysis of the conventional TWR-AF model in [88]. It can be noticed that for the same outage probability value the intercept probability of the AP scheme is smaller than that of the conventional TWR-AF model. As a result, the AP scheme with CB technique enhances the system secrecy performance over the conventional TWR-AF model which provides another motivation for the PU network to cooperate with the SU network.

The SRT analysis of the RJ scenario is presented in Figure 3.14 with different values of λ_Q. Results show that increasing λ_Q increases the intercept probability and degrades the system secrecy performance. This is because increasing λ_Q decreases the remaining power for jamming which enhances the wiretap channel conditions and results in increasing the system intercept probability.

The optimal solution of the proposed power allocation problem in Section 3.5 is compared to the optimal power values obtained using line search optimization method as shown in Figure 3.15 and Figure 3.16 for both AP and RS schemes, respectively. The results show that the optimal solutions of the proposed power allocation problems match the optimal power values obtained by the line search method at the high SNR values. This can be explained as the proposed power allocation problems are formulated to obtained the optimal values which minimize the asymptotic SEP. Since the asymptotic SEPs match the exact SEP at the high SNR values, the optimal power allocations solutions should be matched at the high SNR values.

3.9 Conclusion

In this chapter, a new cooperative TWR-AF model was proposed under different cooperation schemes, namely, AP, RS and RE schemes. Exact and asymptotic closed-form expressions for PU and SU performance metrics were derived including outage probability, average SEP, and maximum achievable rate. Moreover, PHY security approach was proposed to enhance PU network secrecy performance via a relay and jamming scenario. Results showed that the proposed model can achieve a bandwidth efficiency of 1.25 with AP and RS cooperative schemes, whereas it can achieve a bandwidth efficiency of 1.67 with RE cooperative scheme. In addition, findings illustrated that the AP and RS schemes achieve a SEP performance similar to the conventional TWR-AF model at low SNR region, while they outperform the conventional model at high SNR regions. The secrecy performance of the proposed cooperative schemes was investigated under two different scenarios where the cooperative beamforming and relay and jamming techniques were employed. Finally, results showed that the proposed cooperative schemes provide a non-zero secrecy rate in the presence of a single passive eavesdropper which enhances the secrecy performance of the PU networks.

3.10 List of Publications

- **Ahmed H. Abd El-Malek** and Salam A. Zummo, ″A Cooperative Model for Enhancing Spectral Efficiency in Two-Way Amplify-and-Forward Relaying Networks,″ Accepted in IEEE 82nd Veh. Technol. Conf. (VTC-Fall'15), Boston, USA, September 2015.
- **Ahmed H. Abd El-Malek**, Anas M. Salhab and Salam A. Zummo, ″Enhancing Spectral Efficiency in Cooperative Cognitive Two-Way Amplify-and-Forward Relaying Networks, ″ Accepted in IEEE Wireless Commun. and Networking Conf. (WCNC'16), Doha, Qatar, April 2016.
- **Ahmed H. Abd El-Malek** and Salam A. Zummo, ″ Bandwidth Efficient Cooperative Two-Way Amplify-and- Forward Relaying Method,″ U.S. Patent and Trademark Office (USPTO), Docket Number: 37000.28, Disclosed.
- **Ahmed H. Abd El-Malek**, Anas M. Salhab and Salam A. Zummo, ″ A New Bandwidth Efficient Relay Selection/Elimination Scheme in Cooperative Two-Way Cognitive Relaying Networks,″ Submitted to IEEE Trans. Veh. Tech. .

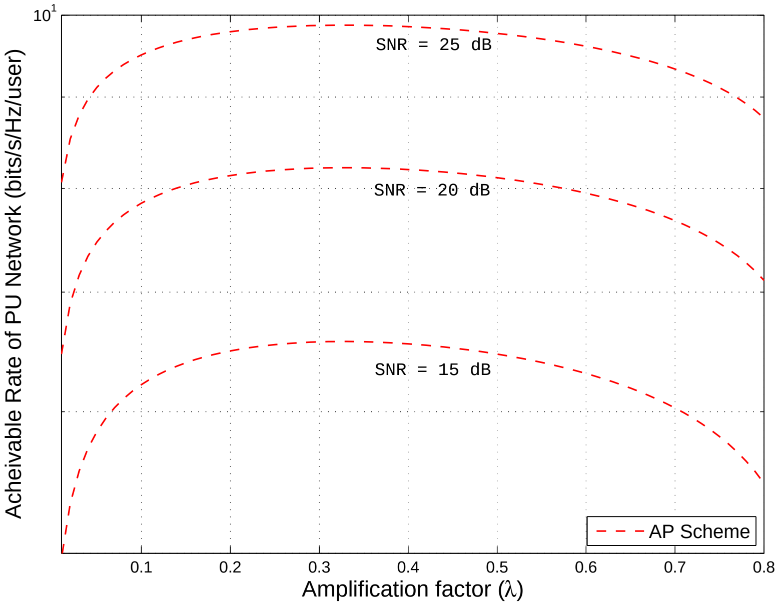


Figure 3.9: PU network achievable rate of the proposed AP scheme against the amplification factor λ_{ap} for $\text{SNR} = 15, 20$ and 25 dB.

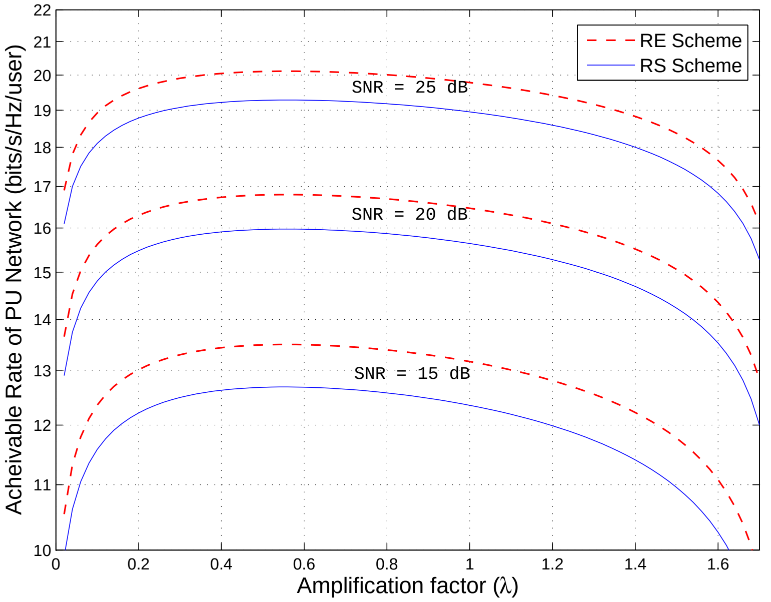


Figure 3.10: PU network achievable rate of the proposed RE and RS schemes against the amplification factor $\lambda_{\mathsf{rs}} = \lambda_{\mathsf{re}} = \lambda$ for $\text{SNR} = 15, 20$ and 25 dB.

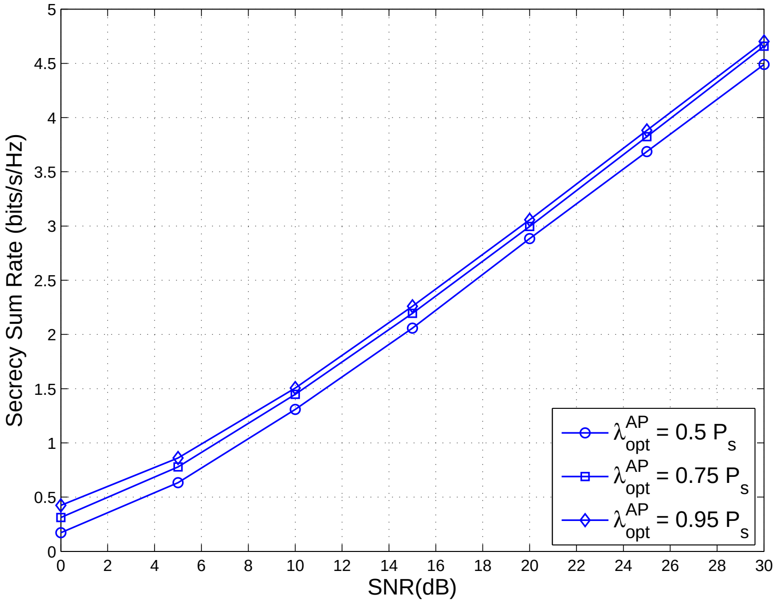


Figure 3.11: Secrecy sum rate of the proposed CB scenario for different values of optimal amplification factor $\lambda_{\mathsf{ap}}^{\mathrm{opt}} = 0.5P_{\mathsf{s}}, 0.75P_{\mathsf{s}}$ and $0.95P_{\mathsf{s}}$.

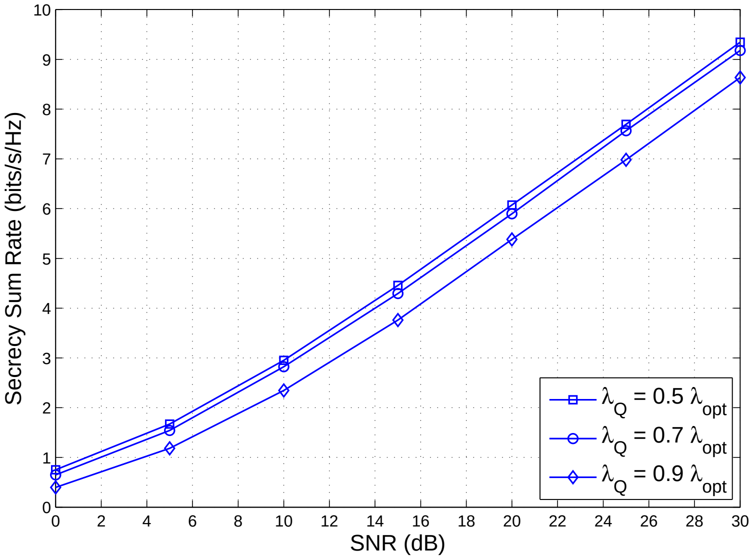


Figure 3.12: Secrecy sum rate of the proposed RJ scenario for different values of required amplification factor $\lambda_Q = 0.5\lambda_{\mathsf{rs}}^{\mathrm{opt}}, 0.7\lambda_{\mathsf{rs}}^{\mathrm{opt}}$ and $0.9\lambda_{\mathsf{rs}}^{\mathrm{opt}}$.

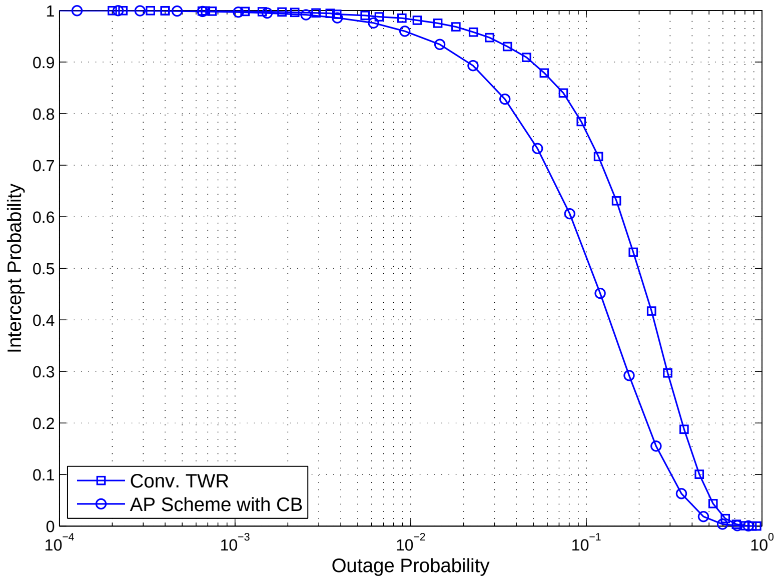


Figure 3.13: SRT analysis comparison between the proposed AP scheme with CB technique and the conventional TWR-AF.

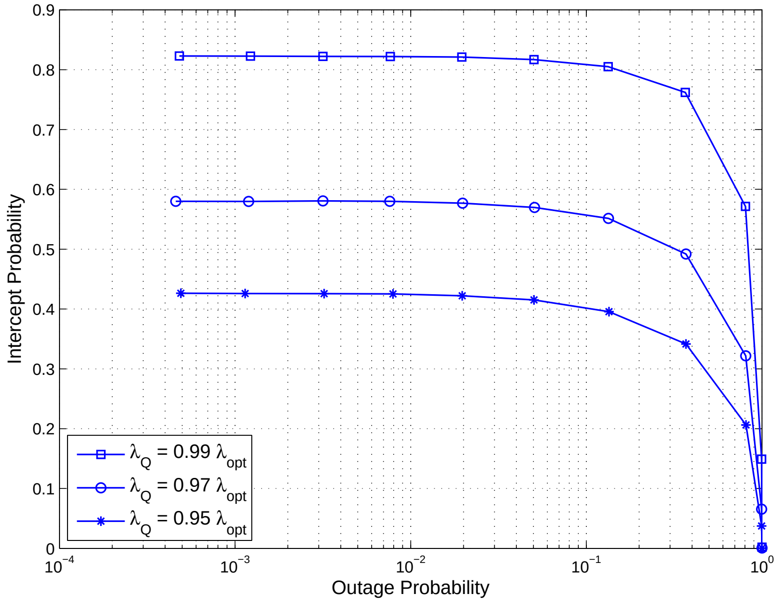


Figure 3.14: SRT analysis for the proposed RS scheme with RJ technique with different required amplification factor $\lambda_Q = 0.99\lambda_{\mathsf{rs}}^{\mathrm{opt}}, 0.97\lambda_{\mathsf{rs}}^{\mathrm{opt}}$ and $0.95\lambda_{\mathsf{rs}}^{\mathrm{opt}}$.

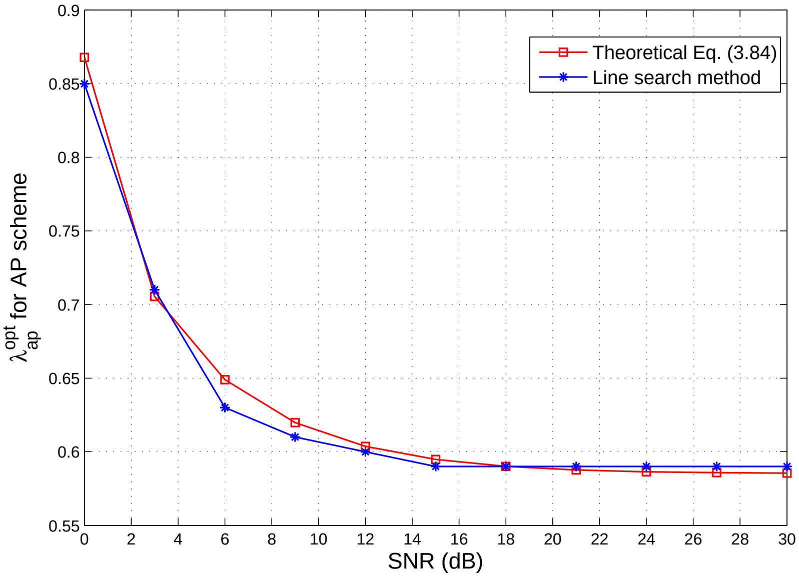


Figure 3.15: Comparison between the line search method and the proposed power allocation solution in (3.84) in terms of the optimal solutions ($\lambda_{\mathsf{ap}}^{\mathrm{opt}}$) for AP scheme.

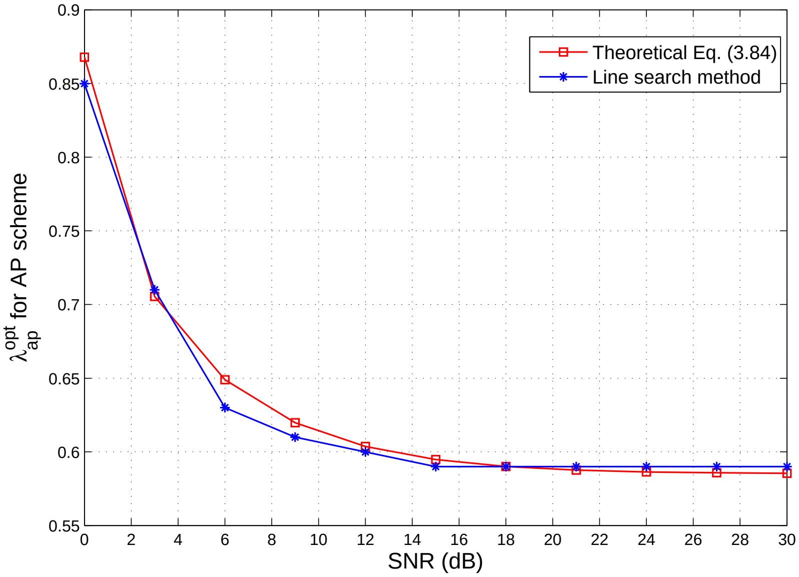


Figure 3.16: Comparison between the line search method and the proposed power allocation solution in (3.84) in terms of the optimal solutions ($\lambda_{\mathsf{rs}}^{\mathrm{opt}}$) for RS scheme.

CHAPTER 4

MULTIUSER SIMO MIXED RF/FSO RELAY NETWORKS

4.1 Introduction

In this chapter, the performance of MU single-input-multiple-output (SIMO) mixed RF/FSO relaying network with user opportunistic scheduling is investigated. The considered system includes multiple users, one AF relay, one destination and a multiple-antenna eavesdropper. The users communicate with the multiple antenna relay node over RF links, whereas, the relay communicates with the optical destination over an FSO link. Both MRC and SC schemes are used at the relay to combine the signal received from the best user on different antennas. We assume that the RF channels are following Nakagami-m distribution, and the FSO channel is following Gamma-Gamma fading distribution in the presence of pointing error (jitter fading). In particular, we derived closed-form expressions for the outage probability, average SEP and ergodic channel capacity. Furthermore, the system performance is studied at high SNR regime where the diversity order and coding gain are derived and analyzed. Using the asymptotic results, the power of the best selected user is determined to minimize the system outage probability under the dominant RF or FSO link. Then, the considered system secrecy performance is investigated where the intercept probability is derived. For enhancing PHY security of the considered system, we propose a new CJ model in which the worst user is selected by the authorized system to jam the existing eavesdropper. Numerical results and simulations are generated to validate the newly derived mathematical formulas. Results show that under strong turbulence conditions, the system performance is shown to be limited by the performance of the FSO link and the diversity order is determined by the minimum value of the turbulence fading and pointing error parameters. Whereas, the RF channels dominate the system overall performance in the case of weak atmospheric turbulence conditions, and the considered system diversity order depends on the Nakagami-m fading parameter, N_{r} and K. Furthermore, for the special case of identical users' channels, the system achieves a maximum diversity order. Finally, results show the effectiveness of the proposed power allocation strategy in enhancing the system secrecy performance against possible eavesdropper attacks.

The rest of this chapter is organized as follows. Section 4.2 reviews the literature. Section 4.3 presents the system and channel models. Section 4.4 evaluates the reliability performance metrics. Section 4.5 studies the PHY security performance analysis with optimal power allocation. Numerical results and simulated are presented and discussed in Section 4.6. Finally, Section 4.7 concludes the work contributions.

4.2 Literature Review

Recently, One of the most efficient solution for the problem of RF wireless spectrum scarcity has been considered to be FSO communications [61]. As the FSO communication systems operate on unlicensed optical beams, these systems present an alternative way for data transmission by employing optical transmitter and receiver which are separated by a few hundreds of meters. Moreover, the advantages of FSO communication such as quick deployment, high security, solidity to RF CCI, and flexibility have made FSO communications attractive for emergencies and military purpose [62].

Beside the FSO communications, cooperative networks, in which the main communication nodes are served by relays, have gained significant attention as an promising solution for multipath fading problem in the area wireless networks [64, 65]. The cooperative communication networks have the ability to enhance the performance of wireless network by increasing the diversity order, enhancing the coding gain, extending the coverage area and reducing the required transmission power. One of the main obstacles in FSO communications is the atmospheric turbulence condition. These phenomena significantly degrades the performance of FSO systems and limits the coverage distance to few hundred of meters [67].

To overcome these performance limitations, the mixed RF/FSO relaying schemes have been presented as effective methods which can handle these difficulties. In such networks, the communications take place over two hops (RF and FSO). In the first hop, the relay received the source message over an RF link, while the relay node communicates with the receiver over an optical link (FSO link). Capitalizing the concept of RF MU multiplexing, the mixed RF/FSO network was presented in [68]. Hence, the mixed RF/FSO system can be considered as a practical model for several applications such as cellular networks where the relay station helps multiple mobile nodes by forwarding the data to the base station, and indoor femtocell networks where the relay serves multiple users as an access point which forwards the data to the macro base station.

A lot of research can be found in literature on discussed the performance of FSO relaying networks which employed a single relay in their transmissions as shown in [95, 96, 97, 98]. Following the literature, different distribution models were proposed to represent the FSO links such as the log-normal fading model , the Gamma-Gamma fading model, and the Malaga fading model. The work in [95, 97] investigated the performance of FSO relay networks over weak turbulence fading channels with log-normal distribution. In particular, the impact of the direct link between the source and destination on the outage performance of FSO relaying networks with AF and DF relaying protocols was studied in [95]. On the other hand, the work in [96, 98] investigated the performance of FSO relay networks over Gamma-Gamma fading channels. In Particular, closed-form expressions were derived for the outage probability and SEP of bidirectional FSO relay networks in [96]. The impact of jitter fading was combined with the induced-turbulence fading and represented by a new distribution which used in studying the performance of mixed RF/FSO networks in [68].

Recently, the research has been investigated the performance of MU scheduling in FSO relaying network. In [99], the outage probability, bit error rate and channel capacity of mixed RF/FSO relay network with MU and DF relaying were studied and mathematical formulas were obtained. In the studied system, a single selected user communicates with the relay node over an RF link and, then, the relay retransmits the previously received source data to the destination over a Gamma-Gamma fading distributed FSO channel with pointing errors. The presence of multiple users was not exploited in the last two studies since increasing the number of users does not increase the system diversity gain. The work in [100] studied reliability performance metrics in terms of outage probability and error probability for a MU mixed RF/FSO relay network with vertical-bell laboratories layered space-time technique and DF relaying. Exact and asymptotic formulas were obtained for the outage probability and SEP over Gamma-Gamma fading channels with pointing errors. Various MU pair scheduling schemes were presented in [101] for dual-hop bidirectional FSO single relay networks. Under log-normal fading channels, exact closed-form expressions were derived for the outage probability taking into account the impact of path loss.

The basic principle of PHY security is to use the available CSI and noise to mitigate the amount of information that the eavesdropper can extract, with the aim of providing the authorized system with secure communication without the need for an encryption key. Effective PHY security design depends on legitimate (authorized) systems obtaining information about the eavesdropper system, whereas, security is compromised when the reverse occurs. This information includes the transmission protocols, transmission power and CSI, whether the eavesdroppers are active or passive, number of eavesdroppers and number of antennas with which each node is equipped [4, 5].

Because of the line of sight nature of FSO channels, the FSO systems are considered to be very high secure systems. However, the PHY security of FSO systems was investigated in [102], which studied the secrecy performance of a single hop FSO system consisting of a single optical transmitter and receiver in the presence of a single passive eavesdropper (i.e., eavesdropper CSI is unavailable). Results showed that the eavesdropper can harm the FSO system secrecy performance if it is able to physically locate near to either the authorized transmitter or receiver, and the eavesdropper is able to intercept the authorized transmission without affecting the amount of received power at the optical receiver. Since the authors in [102] stated that they failed to imagine the way an eavesdropper should look like to be able to physically intercept the authorized transmission, the practicality of the proposed model becomes questionable. In relevant to what is mentioned above, the FSO systems could be assumed to be highly secured systems as mentioned in [1].

Due to the broadcasting nature of the wireless 1RF networks, an eavesdropper can easily attack the authorized transmission with no need to be physically closed to any of the authorized RF transmitter or receiver. Therefore, we can clearly say that in mixed RF/FSO networks, the RF link is the weak link from the secrecy performance viewpoint. Hence, PHY security is considered as a necessary means for increasing secrecy in wireless communication networks. The main principle employed through this strategy is to take advantage of the spatial-temporal characteristics of wireless channels in achieving secure data transmission [2].

The secrecy performance of MU wireless networks were investigated in different system models in the literature [103, 104, 105, 106, 107]. The work in [103] studied the secrecy performance of MU uplink wiretap networks where multiple users communicate with a base station in the presence of multiple eavesdroppers. The work proposed that the base station would select a certain user based on a pre-determined threshold that is related to the channel gains of the eavesdroppers. Results showed that the proposed sub-optimal user scheduling could guarantee a secure transmission without harming the optimal network throughput. Then, the work has been extended in [104] which studied the secrecy performance of MU downlink wiretap networks with opportunistic scheduling where the base station communicates with multiple users in the presence of asymmetrically located eavesdroppers. Closed-form expression for the secrecy throughput and secrecy outage probability were derived. Results illustrated that the proposed scheduling achieves a secrecy diversity order equals to the number of users. The works in

[105, 106, 107] investigated the impact of MU scheduling and relay selection on the secrecy performance of CR networks. Results showed that increasing the number of authorized nodes improves the secrecy performance of the system.

For enhancing PHY security in wireless networks, CJ model was proposed in [37] with opportunistic selection of two relay nodes. This scheme operates as follows: the first relay regularly assists the legitimate transmitter to deliver its data to the intended receiver using the DF protocol. Simultaneously, the second relay creates intentional interference at the eavesdropper nodes. The proposed selection technique protects the legitimate user receiver against interference and eavesdropping, in addition to jamming the eavesdropper reception. Results showed that the hybrid method for switching between jamming and non-jamming cases enhances the secrecy capacity based on the CSI of wiretap channel. A CJ model with a set of relays was investigated in [42], wherein the AF relays were optimally divided into AF relays and cooperative jammers with imperfect CSI. The optimal weights for relay beamforming were obtained. Another joint optimization problem, including the beamforming weights and the power of the jammers, was solved. The authors in [38] proposed a new scheme in which the destination jams the eavesdropper nodes without creating any interference problems at the relay node. In the second time slot of communication, the relay, which is optimally selected, starts to retransmit the decoded source signal, and at the same time, cooperates with the legitimate source to efficiently harm the eavesdropper channel without creating interference at the destination. Results showed that although the eavesdropper has a complete CSI, a non-zero secrecy capacity can be achieved which enhances PHY securities of wireless communications network over the worst case for secure data transmission.

Based on the aforementioned discussion, we can conclude that the security and reliability performances of dual-hop MU SIMO mixed RF/FSO relay networks with user scheduling have not been addressed yet. In such scheme, the relay selects the best user with the highest SNR to conduct its transmission over an RF link. Then, the relay retransmits the received signal to the optical receiver over an FSO link. In this chapter, we introduce the opportunistic scheduling to select the best user among multiple users in dual-hop mixed RF/FSO relay networks with AF relaying. Uplink transmission is considered where multiple users communicate with one AF relay node through RF links and the relay communicates with one destination node through an FSO link in the presence of a single passive eavesdropper with multiple antennas. The RF/FSO links are assumed to follow Nakagami-m/Gamma-Gamma fading models, respectively with the effect of pointing errors. The work contributions can be summarized as follows. Firstly, the impact of multiple antennas relaying and opportunistic user selection on the system performance of MU-SIMO mixed RF/FSO networks with AF relaying is investigated over Nakagami-m/Gamma-Gamma fading channels. In particular, for the use of multiple-antenna technique at the relay node, we study two different diversity combining models (MRC and SC). In particular, we obtain the end-to-end (e2e) SNRs for both adopted combining schemes. Then, new exact closed-form expressions for the outage probability, ASPE and ergodic capacity are derived. Moreover, asymptotic closed-form expressions for the outage probability are derived under two different cases of atmospheric turbulence conditions of the FSO link. These newly derived asymptotic expressions are used to investigate the impact of the key system parameters such as the strength of atmospheric turbulence, number of users, and number of antennas at the relay.

Secondly, we investigate the key system parameters using the asymptotic results of the outage probability clearly determines the dominant link between the RF and FSO links in the cosidered system performance. Based on that dominant link, we propose a new power allocation formula which optimally obtains the required RF transmission power.

Thirdly, the secrecy performance of the adopted MU-SIMO mixed RF/FSO network is investigated in the presence of a single passive RF eavesdropper equipped with multiple antennas. In particular, we study the secrecy performance of the RF link against eavesdropping attack. For a more practical scenario, we assume the eavesdropper is passive (CSI is unavailable) with multiple antennas. Then, closed-form expressions for the intercept probability are derived for the two proposed combining schemes (i.e., MRC and SC). Moreover, asymptotic expressions for the system intercept probability are obtained to investigate the key parameters affecting the secrecy performance.

Finally, in order to enhance RF secrecy performance, we propose a new CJ model where the worst user selected by the relay serves as a friendly jammer and

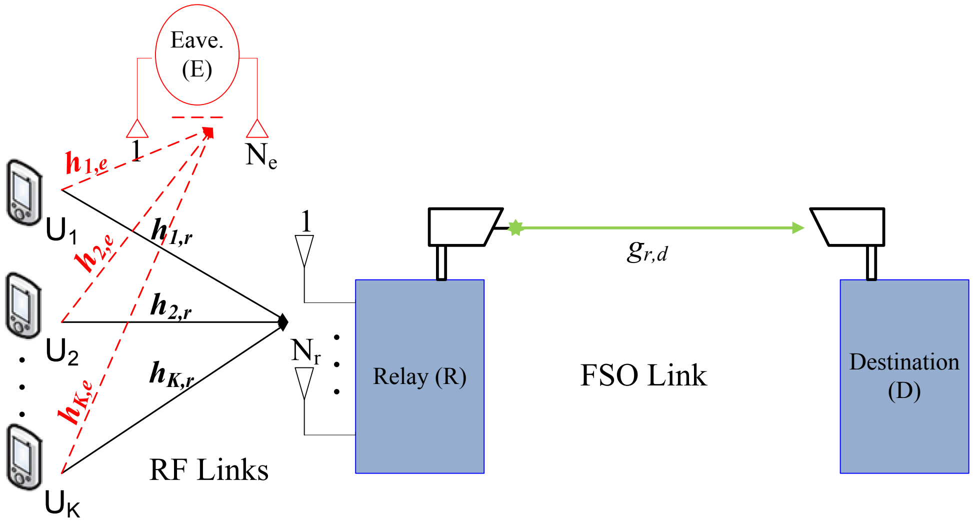


Figure 4.1: Dual-hop MU-SIMO mixed RF/FSO relay network with opportunistic scheduling and multiple antenna eavesdropper.

transmits a jamming signal which is known to the authorized system nodes. Hence, new closed-form expressions for the intercept probability are derived. Then, asymptotic expressions are obtained to study the impact of jamming power on the system secrecy performance. With the help of the asymptotic outage probability formulas, a power allocation problem is formulated to enhance the CJ model secrecy performance.

4.3 System and Channel Models

This section consists of two parts. Firstly, we introduce some preliminary discussions on the considered system model. Secondly, we present a brief discussion on channel models.

4.3.1 System Model

As shown in Figure 4.1, we consider a dual-hop MU-SIMO mixed RF/FSO relay network consisted of K users U_k $(k = 1, \ldots, K)$ each equipped with a single antenna, an AF relay R having N_{r} uncorrelated antennas from one side and with a single photo-aperture transmitter from the other side, and one destination D with single photo detector. The K users communicate with the destination D via the AF relay R with no direct link between the users and D. The users communicate with the relay node through RF links, whereas the relay communicates with the destination through an FSO link. The operations of the considered half-duplex communication model take place over two phases: RF phase (selected user $\mathrm{U}_{\mathrm{Sel}} \rightarrow$ R) and FSO phase (R $\rightarrow$ D). In the RF phase, the received signal at R through the n-th antenna from the k-th user is given by

$$y_{k,n,\mathsf{r}} = \sqrt{P_k} h_{k,n,\mathsf{r}} x_k + w_{\mathsf{r}}, \tag{4.1}$$

where $h_{k,n,\mathsf{r}}$ is the link channel coefficient between the k-th user (U_k) and the n-th antenna at R, x_k denotes the k-th user transmitted data with $\mathbb{E}\{|x_k|^2\} = 1$, $w_{\mathsf{r}} \sim \mathcal{CN}(0, N_0)$ is an AWGN sample at R. Based on (4.1), the SNR observed at the n-th antenna of R can be expressed as

$$\gamma_{k,n,\mathsf{r}} = \frac{P_k}{N_0} |h_{k,n,\mathsf{r}}|^2. \tag{4.2}$$

Hence, the combined SNR of the $\mathrm{U}_k \rightarrow \mathrm{R}$ link for two important schemes can be written as

$$\gamma_{k,\mathsf{r}} \triangleq \begin{cases} \frac{P_k}{N_0}\|\mathbf{h}_{k,\mathsf{r}}\|^2 = \sum_{n=1}^{N_\mathsf{r}} \gamma_{k,n,\mathsf{r}}, & \text{for MRC} \\ \max\limits_{1 \le n \le N_\mathsf{r}} \frac{P_k}{N_0}|h_{k,n,\mathsf{r}}|^2 = \max\{\gamma_{k,1,\mathsf{r}}, \gamma_{k,2,\mathsf{r}}, \ldots, \gamma_{k,N_\mathsf{r},\mathsf{r}}\}, & \text{for SC} \end{cases}. \tag{4.3}$$

The user selection algorithm implements the opportunistic scheduling based on the $\mathrm{U}_k \rightarrow \mathrm{R}$ link. Herein, the user with the largest $\gamma_{k,\mathsf{r}}$ is selected among other users to communicate with R during the RF phase. Hence, the best user is selected such as

$$\gamma_{\mathrm{Sel},\mathsf{r}} \triangleq \begin{cases} \max\limits_{1 \le k \le K} \frac{P_k}{N_0}\|\mathbf{h}_{k,\mathsf{r}}\|^2, & \text{for MRC} \\ \max\limits_{\substack{1 \le k \le K \\ 1 \le n \le N_\mathsf{r}}} \frac{P_k}{N_0}|h_{k,n,\mathsf{r}}|^2, & \text{for SC} \end{cases}. \tag{4.4}$$

In the FSO phase, an amplified version of the selected user message $y_{\mathrm{Sel},\mathsf{r}}$ is forwarded over the optical link. Hence, at D, the received signal is given by

$$y_{\mathsf{r},\mathsf{d}} = g_{\mathsf{r},\mathsf{d}}\mathsf{G}y_{\mathrm{Sel},\mathsf{r}} + w_\mathsf{d}, \tag{4.5}$$

where $g_{\mathsf{r},\mathsf{d}}$ is the link channel coefficient between the R and D, G is the relay gain chosen as [108], $\mathsf{G} = \sqrt{\frac{P_\mathsf{r}}{P_{\mathrm{Sel}}|h_{\mathrm{Sel},\mathsf{r}}|^2 + N_0}}$, and $w_\mathsf{d} \sim \mathcal{CN}(0, N_0)$ is an AWGN sample at D. Manipulate (4.5) after the substitution with the value of G, the e2e SNR at the destination is given by

$$\gamma_{\mathrm{Sel},\mathsf{D}} = \frac{\gamma_{\mathrm{Sel},\mathsf{r}}\widetilde{\gamma}_{\mathsf{r},\mathsf{d}}}{\gamma_{\mathrm{Sel},\mathsf{r}} + \widetilde{\gamma}_{\mathsf{r},\mathsf{d}} + 1}, \tag{4.6}$$

where $\widetilde{\gamma}_{\mathsf{r},\mathsf{d}}$ is the SNR of the FSO hop that is related to the channel coefficient of the selected user, say user U_k, which is defined as $g_{\mathsf{r},\mathsf{d},k}$ (i.e., $g_{\mathsf{r},\mathsf{d},k}$ is the FSO channel coefficient due to U_k), through the conditional result

$$\widetilde{\gamma}_{\mathsf{r},\mathsf{d}} = \gamma_{\mathsf{r},\mathsf{d},k} \triangleq \frac{P_{\mathsf{r}}}{N_0}|g_{\mathsf{r},\mathsf{d},k}|^2, \text{ if } \gamma_{\mathrm{Sel},\mathsf{r}} = \gamma_{k,\mathsf{r}}, \tag{4.7}$$

where the condition that $\gamma_{\mathrm{Sel},\mathsf{r}} = \gamma_{k,\mathsf{r}}$ has probability of occurrence that is given by

$$\Pr\{\gamma_{\mathrm{Sel},\mathsf{r}} = \gamma_{k,\mathsf{r}}\} = \Pr\{\gamma_{k,\mathsf{r}} > \max_{\substack{1\leq i\leq K \\ i\neq k}} \gamma_{i,\mathsf{r}}\}. \tag{4.8}$$

The SNR in (4.6) can be upper bounded using the approximation (e.g., [68], [99]) $\gamma_{\mathrm{Sel},\mathsf{D}} \cong \min\{\gamma_{\mathrm{Sel},\mathsf{r}}, \widetilde{\gamma}_{\mathsf{r},\mathsf{d}}\}$.

Then, the user that has the largest e2e SNR is selected, which gives

$$\gamma_{\mathrm{Sel},\mathsf{D}} = \max\{\gamma_{1,\mathsf{D}}, \gamma_{2,\mathsf{D}}, \ldots, \gamma_{K,\mathsf{D}}\}. \tag{4.9}$$

4.3.2 Channel Model

For RF links, the channel coefficients $h_{k,n,\mathsf{r}}$, for $k = 1, 2, \ldots, K$ and $n = 1, 2, \ldots, N_{\mathsf{r}}$, are assumed to follow Nakagami-m fading model and hence, the CDF of the k-th user's (U_k) SNR with MRC at R is given by

$$\begin{aligned} F_{\mathrm{RF}}(x) &= F_{\gamma_{k,\mathsf{r}}}(x) \\ &= 1 - \sum_{p=0}^{m_k N_{\mathsf{r}}-1} \frac{(m_k \lambda_{k,\mathsf{r}} x)^p}{p!} \exp\left(-m_k \lambda_{k,\mathsf{r}} x\right), \end{aligned} \tag{4.10}$$

where $\lambda_{k,\mathsf{r}} = 1/\bar{\gamma}_{k,\mathsf{r}}$ with $\bar{\gamma}_{k,\mathsf{r}} = \frac{P_k}{N_0}\mathbb{E}\{\|\mathbf{h}_{k,\mathsf{r}}\|^2\} = \frac{P_k}{N_0}\Omega_{k,\mathsf{r}}$. While, the CDF of the k-th user SNR with SC at R is given by

$$\begin{aligned} F_{\mathrm{RF}}(x) &= F_{\gamma_{k,n,\mathsf{r}}}(x) \\ &= \left[1 - \sum_{p=0}^{m_k-1} \frac{(m_k \lambda_{k,\mathsf{r}} x)^p}{p!} \exp\left(-m_k \lambda_{k,\mathsf{r}} x\right)\right]^{N_{\mathsf{r}}} \\ &= \sum_{j=0}^{N_{\mathsf{r}}} \binom{N_{\mathsf{r}}}{j} (-1)^j \widetilde{\sum}_{p_{k,1},p_{k,2},\ldots,p_{k,j}}^{m_k-1} \frac{(m_k \lambda_{k,\mathsf{r}} \gamma)^{\sum_{n=1}^{j} p_{k,n}}}{\prod_{t=1}^{j} p_{k,t}!} \exp\left(-j m_k \lambda_{k,\mathsf{r}} \gamma\right), \end{aligned} \tag{4.11}$$

where $\widetilde{\sum}_{p_{k,1},p_{k,2},\ldots,p_{k,j}}^{m_k-1}$ denotes a short-hand notation for $\sum_{p_{k,1}}^{m_k-1} \sum_{p_{k,2}}^{m_k-1} \cdots \sum_{p_{k,j}}^{m_k-1}$, $\lambda_{k,\mathsf{r}} = 1/\bar{\gamma}_{k,\mathsf{r}}$ with $\bar{\gamma}_{k,\mathsf{r}} = \frac{P_k}{N_0}\mathbb{E}\{|h_{k,\mathsf{r}}|^2\} = \frac{P_k}{N_0}\Omega_{k,\mathsf{r}}$.

Furthermore, assuming Gamma-Gamma fading model with the effect pointing errors, the SNR pdf of the FSO link for U_k is given by [68]

$$f_{\gamma_{\mathsf{r},\mathsf{d},k}}(\gamma) = \frac{\zeta_k^2}{r_k \gamma \Gamma(\alpha_k)\Gamma(\beta_k)} \mathrm{G}_{1,3}^{3,0}\left[\alpha_k \beta_k \left(\lambda_{\mathsf{r},\mathsf{d},k}\gamma\right)^{\frac{1}{r_k}} \middle| \begin{matrix} \zeta_k^2+1 \\ \zeta_k^2, \alpha_k, \beta_k \end{matrix}\right], \tag{4.12}$$

where ζ_k is the ratio between the equivalent beam radius at the receiver and the pointing error displacement standard deviation (jitter) at the receiver (i.e., the FSO link is pointing error free as $\zeta_k \to \infty$). The type of detection is determined based on the value of r_k where heterodyne detection is represented by $r_k = 1$, and the intensity modulation (IM)/ direct detection is represented by $r_k = 2$. The fading severity of atmospheric turbulence conditions are determined by the values of α_k and β_k where high values represent weak turbulence. $\Gamma(.)$ is the Gamma function as defined in [109, Eq. (8.310)], $\lambda_{\mathsf{r},\mathsf{d},k} = 1/\bar{\gamma}_{\mathsf{r},\mathsf{d},k}$ with $\bar{\gamma}_{\mathsf{r},\mathsf{d},k} = \frac{P_{\mathsf{r}}}{N_0}\mathbb{E}\{|g_{\mathsf{r},\mathsf{d},k}|^2\} = \frac{P_{\mathsf{r}}}{N_0}\mu_{\mathsf{r},\mathsf{d},k}$, and G(.) is the Meijer G-function as defined by [109, Eq. (9.301)].

4.4 Performance Analysis

This section presents the outage probability, ASEP and the ergodic capacity assuming exact channel information. Based on the aforementioned SNR bound, exact mathematical formulas are derived for these performance measures when the multi-antenna relay node utilizes two diversity combining techniques (i.e., MRC and SC).

4.4.1 Outage Probability

An outage event occurs when the SNR at D goes below a predetermined outage threshold γ_{out}. Hence, the outage probability is given by $P_{\mathsf{out}} = \Pr\left[\gamma_{\mathrm{Sel},\mathsf{D}} \leq \gamma_{\mathsf{out}}\right]$, $\gamma_{\mathsf{out}} = \left(2^{2\mathcal{R}} - 1\right)$ and $\mathcal{R}$ denotes the spectral efficiency. Then, the CDF of $\gamma_{\mathrm{Sel},\mathsf{D}}$

can be written as [110]

$$F_{\gamma_{\text{Sel,D}}}(\gamma) = F_{\gamma_{\text{Sel,r}}}(\gamma) + F_{\widetilde{\gamma}_{\mathsf{r,d}}}(\gamma) - F_{\gamma_{\text{Sel,r}}}(\gamma) F_{\widetilde{\gamma}_{\mathsf{r,d}}}(\gamma), \tag{4.13}$$

where $F_{\gamma_{\text{Sel,r}}}(\gamma)$ and $F_{\widetilde{\gamma}_{\mathsf{r,d}}}(\gamma)$ are the CDFs of first hop and second hop SNRs, respectively. Using the opportunistic scheduling, the CDF $F_{\gamma_{\text{Sel,r}}}(\gamma)$ is given by

$$F_{\gamma_{\text{Sel,r}}}(\gamma) = \prod_{k=1}^{K} F_{\gamma_{k,\mathsf{r}}}(\gamma), \tag{4.14}$$

where $F_{\gamma_{k,\mathsf{r}}}(\gamma)$ is the CDF of the SNR of the k-th user which depends on the combining technique utilized by R as follows:

4.4.1.1 MRC Scheme

In this scheme, the relay node R combines all received signals at relay antennas. Hence, substituting MRC scheme CDF $F_{\gamma_{k,\mathsf{r}}}(\gamma)$ given by (4.10) in (4.14) and applying the identity

$$\prod_{k=1}^{K} (1 - q_k) = \sum_{k=0}^{K} \frac{(-1)^k}{k!} \sum_{n_1,\ldots,n_k}^{K} \prod_{t=1}^{k} q_{n_t}, \tag{4.15}$$

with $\sum_{n_1,\ldots,n_k}^{K}$ being a short- hand notation for $\sum\limits_{\substack{n_1=\ldots=n_k=1 \\ n_1\neq\ldots\neq n_k}} \!\!\ldots\sum$, (4.14) can be rewritten as

$$F_{\gamma_{\text{Sel,r}}}(\gamma) = \sum_{k=0}^{K} \frac{(-1)^k}{k!} \sum_{n_1,\ldots,n_k}^{K} \sum_{q=0}^{\sum_{t=1}^{k} m_t N_{\mathsf{r}} - 1} \Xi_q \gamma^q \exp\left(-\lambda_{\text{tot}} \gamma\right), \tag{4.16}$$

where $\Xi_q = \sum_{|s_t|=q} \frac{(m_t \lambda_{t,r})^{p_t}}{p_t!}$, and $\lambda_{\text{tot}} = \sum_{t=1}^{k} m_t \lambda_{t,\mathsf{r}}$.

Hence, by integrating (4.12), the CDF $F_{\widetilde{\gamma}_{\mathsf{r,d}}}(\gamma)$ is given by

$$F_{\widetilde{\gamma}_{\mathsf{r,d}}}(\gamma) = \int_0^\gamma f_{\widetilde{\gamma}_{\mathsf{r,d}}}(t)dt = A\mathrm{G}_{r+1,3r+1}^{3r,1}\left[\frac{B}{\bar{\gamma}_{\mathsf{r,d}}}\gamma\middle|_{\chi_2,0}^{1,\chi_1}\right], \tag{4.17}$$

where $A = \frac{r^{\alpha+\beta-2}\zeta^2}{(2\pi)^{r-1}\Gamma(\alpha)\Gamma(\beta)}$, $B = \frac{(\alpha\beta)^r}{r^{2r}}$, $\chi_1 = \frac{\zeta^2+1}{r}, \ldots, \frac{\zeta^2+1}{r}$ comprises of r terms, and $\chi_2 = \frac{\zeta^2}{r}, \ldots, \frac{\zeta^2+r-1}{r}$,

$\frac{\alpha}{r}, \ldots, \frac{\alpha+r-1}{r}, \frac{\beta}{r}, \ldots, \frac{\beta+r-1}{r}$ consists of $3r$ terms. Hence, the substitution of (4.16) and (4.17) in (4.13) yields to

$$\begin{aligned} F_{\gamma_{\mathsf{D}}}(\gamma) = & \sum_{k=0}^{K} \frac{(-1)^k}{k!} \sum_{n_1,\ldots,n_k}^{K} \sum_{q=0}^{\sum_{t=1}^{k} m_t n_{\mathsf{R}}-1} \Xi_q \gamma^q \exp\left(-\lambda_{\text{tot}}\gamma\right) \\ & \times \left\{1 - A\mathrm{G}_{r+1,3r+1}^{3r,1}\left[\frac{B}{\bar{\gamma}_{\mathsf{r,d}}}\gamma\middle|_{\chi_2,0}^{1,\chi_1}\right]\right\} + A\mathrm{G}_{r+1,3r+1}^{3r,1}\left[\frac{B}{\bar{\gamma}_{\mathsf{r,d}}}\gamma\middle|_{\chi_2,0}^{1,\chi_1}\right]. \end{aligned} \tag{4.18}$$

Then, we can obtain the closed-form expression for the system outage probability by replacing γ with γ_{out} in (5.15).

4.4.1.2 SC Scheme

In this scheme, the relay node R selects the received signals with the maximum SNR at the front-end of relay antennas. Hence, substituting MRC scheme CDF

$F_{\gamma_{k,\mathsf{r}}}(\gamma)$ given by (4.11) in (4.14) yields

$$\begin{aligned} F_{\gamma_{\mathrm{Sel},\mathsf{r}}}(\gamma) &= \prod_{k=1}^{K}\left[\sum_{j=0}^{N_{\mathsf{r}}}\binom{N_{\mathsf{r}}}{j}(-1)^{j}\widetilde{\sum}_{p_{k,1},p_{k,2},\ldots,p_{k,j}}^{m_k-1}\frac{(m_k\lambda_{k,\mathsf{r}}\gamma)^{\sum_{n=1}^{j}p_{k,n}}}{\prod_{t=1}^{j}p_{k,t}!}\exp\left(-jm_k\lambda_{k,\mathsf{r}}\gamma\right)\right] \\ &= \sum_{j=0}^{N_{\mathsf{r}}}\binom{N_{\mathsf{r}}}{j}(-1)^{j}\widetilde{\sum}_{p_{1,1},\ldots,p_{1,j}}^{m_1-1}\cdots\widetilde{\sum}_{p_{K,1},\ldots,p_{K,j}}^{m_K-1}\Upsilon_{\delta}\gamma^{\delta}\exp\left(-\lambda_{\mathrm{tot},\delta}\gamma\right), \end{aligned} \tag{4.19}$$

where $\delta = \sum_{k=1}^{K}\sum_{n=1}^{j}p_{k,n}$, $\Upsilon_{\delta} = \prod_{k=1}^{K}\frac{(m_k\lambda_{k,\mathsf{r}})^{\sum_{n=1}^{j}p_{k,n}}}{\prod_{t=1}^{j}p_{k,t}!}$ and $\lambda_{\mathrm{tot},\delta} = \sum_{|\sum_{k=1}^{K}\sum_{n=1}^{j}p_{k,n}=\delta|}jm_k\lambda_{k,\mathsf{r}}$. Substituting (4.19) in (4.13) and after some simplifications, we get

$$\begin{aligned} F_{\gamma_{\mathsf{D}}}(\gamma) = &\sum_{j=0}^{N_{\mathsf{r}}}\binom{N_{\mathsf{r}}}{j}(-1)^{j}\widetilde{\sum}_{p_{1,1},\ldots,p_{1,j}}^{m_1-1}\cdots\widetilde{\sum}_{p_{K,1},\ldots,p_{K,j}}^{m_K-1}\Upsilon_{v}\gamma^{\delta}\exp\left(-\lambda_{\mathrm{tot},v}\gamma\right)\Bigg\{1 \\ &- A\mathrm{G}_{r+1,3r+1}^{3r,1}\left[\frac{B}{\bar{\gamma}_{\mathsf{r,d}}}\gamma\middle|\begin{smallmatrix}1,\chi_1\\ \chi_2,0\end{smallmatrix}\right]\Bigg\} + A\mathrm{G}_{r+1,3r+1}^{3r,1}\left[\frac{B}{\bar{\gamma}_{\mathsf{r,d}}}\gamma\middle|\begin{smallmatrix}1,\chi_1\\ \chi_2,0\end{smallmatrix}\right]. \end{aligned} \tag{4.20}$$

Substituting γ by γ_{out} in (4.20), we can directly obtain the closed-form expression for the outage probability.

4.4.2 Asymptotic Outage Probability

Revealing more insights on various system parameters on the system performance, a less sophisticated asymptotic expressions for the outage probability are derived and analyzed.

For high SNR regime, the outage probability is simplified to its asymptotic formula which can be written as $P_{\mathsf{out}} \simeq (G_{\mathsf{c}}\mathrm{SNR})^{-G_{\mathsf{d}}}$, where G_{c} denotes the coding gain of the system and G_{d} is the diversity order of the system [111]. Hence, as $\bar{\gamma}_{k,\mathsf{r}} \to \infty$, the CDF expressions of the RF link SNR with MRC and SC techniques at R in (4.16) and (4.19), respectively are simplified to their asymptotic expressions such as

$$F^{\infty}_{\gamma_{\text{Sel},\mathsf{r}}}(\gamma) = \begin{cases} \prod_{k=1}^{K} \frac{m_k^{m_k N_{\mathsf{r}}}}{(m_k N_{\mathsf{r}})!} \left(\lambda_{k,\mathsf{r}}\gamma\right)^{m_k N_{\mathsf{r}}}, & \text{for MRC} \\ \prod_{k=1}^{K} \frac{m_k^{m_k N_{\mathsf{r}}}}{(m_k!)^{N_{\mathsf{r}}}} \left(\lambda_{k,\mathsf{r}}\gamma\right)^{m_k N_{\mathsf{r}}}, & \text{for SC} \end{cases}. \tag{4.21}$$

For further simplification, the users could be assumed to have identical channels ($\lambda_{1,\mathsf{r}} = \lambda_{2,\mathsf{r}} = \cdots = \lambda_{K,\mathsf{r}} = \lambda_{u,\mathsf{r}}$) and ($m_1 = m_2 = \cdots = m_K = m_u$). For the identical case, the CDF in (4.21) simplifies to

$$F^{\infty}_{\gamma_{\text{Sel},\mathsf{r}}}(\gamma) = \begin{cases} \left[\frac{m_u^{m_u N_{\mathsf{r}}}}{(m_u N_{\mathsf{r}})!}\right]^{K} \left(\lambda_{u,\mathsf{r}}\gamma\right)^{m_u N_{\mathsf{r}} K}, & \text{for MRC} \\ \left[\frac{m_u^{m_u N_{\mathsf{r}}}}{(m_u!)^{N_{\mathsf{r}}}}\right]^{K} \left(\lambda_{u,\mathsf{r}}\gamma\right)^{m_u N_{\mathsf{r}} K}, & \text{for SC} \end{cases}. \tag{4.22}$$

For the FSO link, we have two different cases:

Case 1: Weak Turbulence

For large values of α and β, as $\bar{\gamma}_{\mathsf{r,d}} \to \infty$, $F_{\tilde{\gamma}_{\mathsf{r,d}}}(\gamma)$ is simplified to [109, Eq. (9.303)]

$$F^{\infty}_{\tilde{\gamma}_{\mathsf{r,d}}}(\gamma) \simeq \frac{AB\gamma}{\bar{\gamma}_{\mathsf{r,d}}}. \tag{4.23}$$

For high SNR values, the CDF in (4.13) can be simplified to values to be

$$F^{\infty}_{\gamma_{\mathsf{D}}}(\gamma) \simeq F^{\infty}_{\gamma_{\text{Sel},\mathsf{r}}}(\gamma) + F^{\infty}_{\tilde{\gamma}_{\mathsf{r,d}}}(\gamma), \tag{4.24}$$

Noting that, we can ignore the term $-F_{\gamma_{\mathrm{Sel,r}}}(\gamma)F_{\widetilde{\gamma}_{\mathsf{r,d}}}(\gamma)$ in (4.13) for high SNR values.

Upon substituting $F_{\gamma_{u,\mathsf{r}}}(\gamma)$ in (4.21) and then substituting the resulting CDF and (4.23) in (4.24), we get

$$F_{\gamma_{\mathsf{D}}}^{\infty}(\gamma) \simeq \begin{cases} \prod_{k=1}^{K} \frac{m_k^{m_k N_{\mathsf{r}}}}{(m_k N_{\mathsf{r}})!} \left(\lambda_{k,\mathsf{r}}\gamma\right)^{m_k N_{\mathsf{r}}} + \frac{AB\gamma}{\bar{\gamma}_{\mathsf{r,d}}}, & \text{for MRC} \\ \prod_{k=1}^{K} \frac{m_k^{m_k N_{\mathsf{r}}}}{(m_k!)^{N_{\mathsf{r}}}} \left(\lambda_{k,\mathsf{r}}\gamma\right)^{m_k N_{\mathsf{r}}} + \frac{AB\gamma}{\bar{\gamma}_{\mathsf{r,d}}}, & \text{for SC} \end{cases}. \tag{4.25}$$

Hence, the asymptotic outage probability is given by

$$P_{\mathsf{out}}^{\infty} = \begin{cases} \prod_{k=1}^{K} \frac{m_k^{m_k N_{\mathsf{r}}}}{(m_k N_{\mathsf{r}})!} \left(\lambda_{k,\mathsf{r}}\gamma_{\mathsf{out}}\right)^{m_k N_{\mathsf{r}}} + \frac{AB\gamma_{\mathsf{out}}}{\bar{\gamma}_{\mathsf{r,d}}}, & \text{for MRC} \\ \prod_{k=1}^{K} \frac{m_k^{m_k N_{\mathsf{r}}}}{(m_k!)^{N_{\mathsf{r}}}} \left(\lambda_{k,\mathsf{r}}\gamma_{\mathsf{out}}\right)^{m_k N_{\mathsf{r}}} + \frac{AB\gamma_{\mathsf{out}}}{\bar{\gamma}_{\mathsf{r,d}}}, & \text{for SC} \end{cases}. \tag{4.26}$$

Based on (4.26), it can be noticed that the considered system at weak turbulence conditions might have two cases of dominant term; namely, RF dominant and FSO dominant. In the case of RF dominant (i.e., $F_{\gamma_{\mathrm{Sel,r}}}^{\infty}(\gamma) >> F_{\widetilde{\gamma}_{\mathsf{r,d}}}^{\infty}(\gamma)$, $F_{\widetilde{\gamma}_{\mathsf{r,d}}}^{\infty}(\gamma) \approx 0.01F_{\gamma_{\mathrm{Sel,r}}}^{\infty}(\gamma)$), the considered system achieves a diversity order of $m_u N_{\mathsf{r}} K$ with identical users. Also, the system coding gain is affected by the values of Nakagami-m fading parameter, number of relay antennas N_{r} and γ_{out}. Hence, increasing the values of m_u, N_{r} and/or K provides a remarkable improvement in the diversity gain of the RF link and this may lead to the case where the FSO link becomes the dominant term. In this case (i.e., the FSO dominant) where $F_{\widetilde{\gamma}_{\mathsf{r,d}}}^{\infty}(\gamma) >> F_{\gamma_{\mathrm{Sel,r}}}^{\infty}(\gamma)$ (i.e., $F_{\gamma_{\mathrm{Sel,r}}}^{\infty}(\gamma) \approx 0.01F_{\widetilde{\gamma}_{\mathsf{r,d}}}^{\infty}(\gamma)$), the overall performance becomes a function of the FSO link parameters which depends on the laser transmission power, receiver detector type and the noise level at the destination. Although the FSO link suffers from a weak turbulence conditions, keeping increasing the diversity gain of the RF link might limit the adopted system performance to the FSO link performance. This remark will be used in solving the power allocation problem in Section. 4.4.5.

<u>**Case 2:**</u> Strong Turbulence

For small values of α and β, from [112, Eq. (07.34.06.0006.01)], if $z \to \infty$, the Meijer G-function has the following series representation

$$\mathrm{G}_{p,q}^{m,n}\left[z\middle|\begin{smallmatrix}a_1,\ldots,a_p\\ b_1,\ldots,b_q\end{smallmatrix}\right]=\sum_{k=1}^{m}\frac{\prod_{j=1,j\neq k}^{m}\Gamma(b_j-b_k)\prod_{j=1}^{n}\Gamma(1-a_j+b_k)}{\prod_{j=n+1}^{p}\Gamma(a_j-b_k)\prod_{j=m+1}^{q}\Gamma(1-b_j+b_k)}z^{b_k}(1+o(z)), \tag{4.27}$$

where $p \leq q$ is required. Here, we use the same approach that was used in [113] in writing the outage probability for this case. Defining $v/r = \min\{\zeta^2, \alpha, \beta\}$, the CDF of second hop SNR $F_{\tilde{\gamma}_{\mathsf{r,d}}}(\gamma)$ can be easily seen to simplify to

$$F_{\tilde{\gamma}_{\mathsf{r,d}}}^{\infty}(\gamma) \simeq \Lambda\left(\frac{\gamma}{\bar{\gamma}_{\mathsf{r,d}}}\right)^{\frac{\nu}{r}}, \tag{4.28}$$

where Λ is constant. Hence, the asymptotic CDF of the considered system is given by

$$F_{\gamma_{\mathsf{D}}}(\gamma) \simeq \begin{cases} \prod_{k=1}^{K}\frac{m_k^{m_k N_{\mathsf{r}}}}{(m_k N_{\mathsf{r}})!}\left(\lambda_{k,\mathsf{r}}\gamma\right)^{m_k N_{\mathsf{r}}}+\Lambda\left(\frac{\gamma}{\bar{\gamma}_{\mathsf{r,d}}}\right)^{\frac{\nu}{r}}, & \text{for MRC}\\ \prod_{k=1}^{K}\frac{m_k^{m_k N_{\mathsf{r}}}}{(m_k!)^{N_{\mathsf{r}}}}\left(\lambda_{k,\mathsf{r}}\gamma\right)^{m_k N_{\mathsf{r}}}+\Lambda\left(\frac{\gamma}{\bar{\gamma}_{\mathsf{r,d}}}\right)^{\frac{\nu}{r}}, & \text{for SC}\end{cases}. \tag{4.29}$$

Then, the asymptotic outage probability for this case can be written at high SNR values as

$$P_{\mathsf{out}}^{\infty}=\begin{cases}\prod_{k=1}^{K}\frac{m_k^{m_k N_{\mathsf{r}}}}{(m_k N_{\mathsf{r}})!}\left(\lambda_{k,\mathsf{r}}\gamma_{\mathsf{out}}\right)^{m_k N_{\mathsf{r}}}+\Lambda\left(\frac{\gamma_{\mathsf{out}}}{\bar{\gamma}_{\mathsf{r,d}}}\right)^{\frac{\nu}{r}}, & \text{for MRC}\\ \prod_{k=1}^{K}\frac{m_k^{m_k N_{\mathsf{r}}}}{(m_k!)^{N_{\mathsf{r}}}}\left(\lambda_{k,\mathsf{r}}\gamma_{\mathsf{out}}\right)^{m_k N_{\mathsf{r}}}+\Lambda\left(\frac{\gamma_{\mathsf{out}}}{\bar{\gamma}_{\mathsf{r,d}}}\right)^{\frac{\nu}{r}}, & \text{for SC}\end{cases}. \quad (4.30)$$

For the case of strong turbulence conditions, and based on (4.30), the diversity order of the considered system is limited to $\min\{\zeta^2/2, \alpha/2, \beta/2, m_u N_{\mathsf{r}} K\}$. This result shows that the worst channel link between the RF and FSO links limits the system diversity order. For large values of RF link parameters (i.e., m_u, N_{r} and K), and under strong turbulence conditions and pointing errors, the FSO link will dominate the overall performance. Moreover, the impact of RF channels and number of users on the overall performance could be neglected. This remark will be used in obtaining the optimal RF transmission power needed under strong turbulence conditions in Section. 4.4.5.

4.4.3 Average Symbol Error Probability

From [114], it can be shown that the ASEP is given by

$$\text{ASEP}=\frac{a\sqrt{b}}{2\sqrt{\pi}}\int_0^{\infty}\frac{\exp\left(-b\gamma\right)}{\sqrt{\gamma}}F_{\gamma_{\text{Sel,D}}}(\gamma)d\gamma, \quad (4.31)$$

where a and b are modulation specific parameters.

4.4.3.1 MRC Scheme

Upon substituting (5.15) in (4.31) and with the help of [109, Eq. (7.813.1)] and [109, Eq. (3.381.4)], we get

$$\begin{aligned}\text{ASEP} =& \frac{a\sqrt{b}}{2\sqrt{\pi}}\left[\sum_{k=0}^{K}\frac{(-1)^k}{k!}\sum_{n_1,\ldots,n_k}^{K}\sum_{q=0}^{\sum_{t=1}^{k}m_t N_{\mathsf{r}}-1}\Xi_q(b+\lambda_{\text{tot}})^{-\left(q+\frac{1}{2}\right)}\left\{\Gamma\left(q+\frac{1}{2}\right)\right.\right.\\ &\left.\left.- A\mathrm{G}_{r+2,3r+1}^{3r,2}\left[\frac{B}{(b+\lambda_{\text{tot}})\bar{\gamma}_{\mathsf{r,d}}}\middle|\begin{matrix}q+\frac{1}{2},1,\chi_1\\ \chi_2,0\end{matrix}\right]\right\} + Ab^{-\frac{1}{2}}\mathrm{G}_{r+2,3r+1}^{3r,2}\left[\frac{B}{b\bar{\gamma}_{\mathsf{r,d}}}\middle|\begin{matrix}\frac{1}{2},1,\chi_1\\ \chi_2,0\end{matrix}\right]\right].\end{aligned} \tag{4.32}$$

4.4.3.2 SC Scheme

Similarly, substituting (4.20) in (4.31) yields to

$$\begin{aligned}\text{ASEP} = \frac{a\sqrt{b}}{2\sqrt{\pi}}&\left[\sum_{j=0}^{N_{\mathsf{r}}}\binom{N_{\mathsf{r}}}{j}(-1)^j\widetilde{\sum}_{p_{1,1},\ldots,p_{1,j}}^{m_1-1}\cdots\widetilde{\sum}_{p_{K,1},\ldots,p_{K,j}}^{m_K-1}\Upsilon_\delta(b+\lambda_{\text{tot},\delta})^{-\left(\delta+\frac{1}{2}\right)}\times\right.\\ &\left.\left\{\Gamma\left(\delta+\frac{1}{2}\right) - A\mathrm{G}_{r+2,3r+1}^{3r,2}\left[\frac{B}{(b+\lambda_{\text{tot},\delta})\bar{\gamma}_{\mathsf{r,d}}}\middle|\begin{matrix}\delta+\frac{1}{2},1,\chi_1\\ \chi_2,0\end{matrix}\right]\right\} + Ab^{-\frac{1}{2}}\mathrm{G}_{r+2,3r+1}^{3r,2}\left[\frac{B}{b\bar{\gamma}_{\mathsf{r,d}}}\middle|\begin{matrix}\frac{1}{2},1,\chi_1\\ \chi_2,0\end{matrix}\right]\right].\end{aligned} \tag{4.33}$$

4.4.4 Ergodic Channel Capacity

Based on the derived CDF formulas of $\gamma_{\text{Sel},\mathsf{D}}$, the ergodic capacity could be evaluated by

$$C = \frac{1}{2\ln(2)}\int_0^\infty \frac{1 - F_{\gamma_{\text{Sel},\mathsf{D}}}(\gamma)}{1+\gamma}d\gamma \tag{4.34}$$

4.4.4.1 MRC Scheme

Upon substituting (5.15) in (4.34) and using $(1+\gamma)^{-1} = \mathrm{G}_{1,1}^{1,1}\left[\gamma\middle|\begin{smallmatrix}0\\0\end{smallmatrix}\right]$ in integrals which include Meijer G-function, we get

$$\begin{aligned}C =&\frac{1}{2\ln(2)}\left\{\sum_{k=0}^{K}\frac{(-1)^{k+1}}{k!}\sum_{n_1,\ldots,n_k}^{K}\sum_{q=0}^{\sum_{t=1}^{k}m_tN_{\mathsf{r}}-1}\left[\Xi_q\int_0^\infty(1+\gamma)^{-1}\gamma_q\exp\left(-\lambda_{\mathrm{tot}}\gamma\right)d\gamma\right.\right.\\&\left.+A\Xi_q\int_0^\infty\gamma^q\exp\left(-\lambda_{\mathrm{tot}}\gamma\right)\mathrm{G}_{1,1}^{1,1}\left[\gamma\middle|\begin{smallmatrix}0\\0\end{smallmatrix}\right]\mathrm{G}_{r,3r}^{3r,0}\left[\frac{B}{\bar{\gamma}_{\mathsf{r,d}}}\gamma\middle|\begin{smallmatrix}\chi_1\\\chi_2\end{smallmatrix}\right]d\gamma\right]\\&\left.+A\int_0^\infty\mathrm{G}_{1,1}^{1,1}\left[\gamma\middle|\begin{smallmatrix}0\\0\end{smallmatrix}\right]\mathrm{G}_{r,3r}^{3r,0}\left[\frac{B}{\bar{\gamma}_{\mathsf{r,d}}}\gamma\middle|\begin{smallmatrix}\chi_1\\\chi_2\end{smallmatrix}\right]d\gamma\right\}.\end{aligned}\tag{4.35}$$

The first integral can be obtained with the help of [109, Eq. (9.211.4)], while, we could evaluate the other two integrals using Meijer G-function integral properties [112, Eq. (07.34.21.0011.01)] and [112, Eq. (07.34.21.0081.01)]. Hence, the ergodic capacity of the considered system is given by

$$\begin{aligned}C =&\frac{1}{2\ln(2)}\left\{\sum_{k=0}^{K}\frac{(-1)^{k+1}}{k!}\sum_{n_1,\ldots,n_k}^{K}\sum_{q=0}^{\sum_{t=1}^{k}m_tN_{\mathsf{r}}-1}\Xi_q\left[q!\Psi(q+1,q+1,\lambda_{\mathrm{tot}})\right.\right.\\&\left.\left.-A\mathrm{G}_{1,0:1,1:r+1,3r+1}^{0,1:1,1:3r,1}\left[\frac{1}{\lambda_{\mathrm{tot}}},\frac{B\lambda_{\mathrm{tot}}}{\bar{\gamma}_{\mathsf{r,d}}}\middle|\begin{smallmatrix}1\\-\end{smallmatrix}\middle|\begin{smallmatrix}0\\0\end{smallmatrix}\middle|\begin{smallmatrix}q+1,\chi_1\\\chi_2,0\end{smallmatrix}\right]\right]+A\mathrm{G}_{r+2,3r+2}^{3r+1,2}\left[\frac{B}{\bar{\gamma}_{\mathsf{r,d}}}\middle|\begin{smallmatrix}1,0,\chi_1\\\chi_2,0,0\end{smallmatrix}\right]\right\},\end{aligned}\tag{4.36}$$

where $\mathrm{G}\left[Z_1,Z_2\middle|.\middle|.\middle|.\right]$ denotes the extended generalized bivariate Meijer G-function.

4.4.4.2 SC Scheme

Similarly, substituting (4.20) in (4.34) results in

$$\begin{aligned} C =&\frac{1}{2\ln(2)}\left\{\sum_{j=0}^{N_{\mathsf{R}}}\binom{N_{\mathsf{R}}}{j}(-1)^{j}\widetilde{\sum}_{p_{1,1},\dots,p_{1,j}}^{m_1-1}\dots\widetilde{\sum}_{p_{K,1},\dots,p_{K,j}}^{m_K-1}\Upsilon_{\delta}\left[\delta!\Psi(\delta+1,\delta+1,\lambda_{\text{tot},\delta})\right.\right. \\ &\left.\left.-A\mathrm{G}_{1,0:1,1:r+1,3r+1}^{0,1:1,1:3r,1}\left[\frac{1}{\lambda_{\text{tot},\delta}},\frac{B\lambda_{\text{tot},\delta}}{\bar{\gamma}_{\mathsf{r,d}}}\middle|\begin{matrix}1\\-\end{matrix}\middle|\begin{matrix}0\\0\end{matrix}\middle|\begin{matrix}\delta+1,\chi_1\\\chi_2,0\end{matrix}\right]\right]+A\mathrm{G}_{r+2,3r+2}^{3r+1,2}\left[\frac{B}{\bar{\gamma}_{\mathsf{r,d}}}\middle|\begin{matrix}1,0,\chi_1\\\chi_2,0,0\end{matrix}\right]\right\}. \end{aligned} \tag{4.37}$$

It is important to mention that the above-derived closed-form expressions of ergodic capacity (4.36) and (4.37) are exact expressions for the case of heterodyne detection model (i.e., $r = 1$), whereas, these expressions are considered as lower bounds for the case of IM/DD detection model (i.e., $r = 2$) as given in [115, Eq. (26)].

4.4.5 Power Allocation

In this part, we propose a new power allocation solution for the RF transmission power of the K users (i.e., P_k). As we remarked in Section 4.4.2, the performance of the FSO link could be limited due to the atmospheric (weak strong) turbulence. In addition, the FSO link performance might be limited due to the limited FSO transmission power (the power of the laser beam) because of safety regulation and eye protection. Hence, the performance of the considered system might be limited to the FSO link performance since the overall system performance of the considered system is always dominated by the worse link between the two links (i.e., RF and FSO links). As a result, we explaine two different scenarios of performance dominant cases (i.e., RF and FSO case). Therefore, the considered system might not be able to get the benefits of both diversity and coding gains provided by the MU RF links (the FSO dominant case). Whereas, the considered system might be able to fully utilize the diversity and coding gain improvements in the RF links (the RF dominant case).

As a result, allowing the selected best user $\mathrm{U_{Sel}}$ to transmit with it maximum transmission power P_{T} might be inefficient and a waste of power resources as there is no additional improvements in the considered system overall performance when the conditions of the FSO link are worse than the RF link (i.e., FSO dominant case). Whereas, in the case of RF dominant term, the selected best user $\mathrm{U_{Sel}}$ should transmit with its maximum transmission power P_{T} to enhance the system overall performance. Hence, we can say that the optimal RF transmission power of the selected best user P_k^{opt} is given by

$$P_k^{\mathsf{opt}} = \min\left(P_{\mathsf{T}}, P_{\mathsf{req}}\right), \tag{4.38}$$

where P_{req} is the minimum required RF transmission power which guarantees that the FSO link is still the dominant term in the total system outage probability. Under the two cases of atmospheric turbulence conditions of the FSO link, we have the following:

Case 1: Weak Turbulence

In this case, determining the dominant term between the RF and FSO links depends on both RF and FSO main parameters as increasing the number of relay antennas N_{r} and number of users K could change the dominant term form the RF to the FSO term. In order to overcome this problem and from our observations, we notice that the dominant outage term is the term which is larger than or equal to 100 times the other term. For example, the FSO outage term is the dominant term when $F_{\tilde{\gamma}_{\mathsf{r,d}}}(\gamma) \geq 100 \times F_{\gamma_{\mathrm{Sel},\mathsf{r}}}(\gamma)$, and vice versa.

For simplicity and without loss of generality, the asymptotic outage probability expressions derived in Section 4.4.2 are used to obtain mathematically tractable solutions. For weak turbulence case with FSO dominant term, the optimal transmission power is given by

$$\begin{aligned} &\min \ P_{\mathsf{req}} \\ &\text{Subject to: } F^{\infty}_{\gamma_{\mathrm{Sel},\mathsf{r}}}(\gamma) \approx 0.01 F^{\infty}_{\tilde{\gamma}_{\mathsf{r,d}}}(\gamma). \end{aligned} \tag{4.39}$$

Under the assumption of identical users channels with equal transmission powers, the optimal value is given by

$$P_{\mathsf{req}} = \begin{cases} \frac{N_0 m_u \gamma_{\mathsf{out}}}{\Omega_{u,r}((m_u N_{\mathsf{r}})!)^{m_u N_{\mathsf{r}}}} \left(\frac{0.01 A B \gamma_{\mathsf{out}}}{\bar{\gamma}_{\mathsf{r,d}}}\right)^{\frac{-1}{m_u N_{\mathsf{r}} K}}, & \text{for MRC} \\ \frac{N_0 m_u \gamma_{\mathsf{out}}}{\Omega_{u,r}((m_u N_{\mathsf{r}})!)^{m_u}} \left(\frac{0.01 A B \gamma_{\mathsf{out}}}{\bar{\gamma}_{\mathsf{r,d}}}\right)^{\frac{-1}{m_u N_{\mathsf{r}} K}}, & \text{for SC} \end{cases}. \tag{4.40}$$

While for the weak turbulence with RF dominant case, the selected best user will transmit with maximum transmission power P_{T}.

<u>Case 2:</u> Strong Turbulence

Similarly, under the assumption of identical users channels with equal transmission powers, the optimal value is given by

$$P_{\mathsf{req}} = \begin{cases} \frac{N_0 m_u \gamma_{\mathsf{out}}}{\Omega_{u,r}((m_u N_{\mathsf{r}})!)^{m_u N_{\mathsf{r}}}} \left(\frac{0.01 \Lambda \gamma_{\mathsf{out}}^{\nu/r}}{\bar{\gamma}_{\mathsf{r,d}}^{\nu/r}} \right)^{\frac{-1}{m_u N_{\mathsf{r}} K}}, & \text{for MRC} \\ \frac{N_0 m_u \gamma_{\mathsf{out}}}{\Omega_{u,r}((m_u N_{\mathsf{r}})!)^{m_u}} \left(\frac{0.01 \Lambda \gamma_{\mathsf{out}}^{\nu/r}}{\bar{\gamma}_{\mathsf{r,d}}^{\nu/r}} \right)^{\frac{-1}{m_u N_{\mathsf{r}} K}}, & \text{for SC} \end{cases}. \qquad (4.41)$$

4.5 Physical Layer Security Approach

In this section, the secrecy performance of the considered system is studied under the eavesdropper attacking. Since the FSO link has the advantage of high security level, the work is concentrating on studying the secrecy performance of the RF link. This section is divided into two parts, the first part introduce the RF link security analysis, and the second part proposed a new CJ model based on the worst user selection.

4.5.1 Security Analysis

4.5.1.1 System Intercept Probability

In this part, the secrecy performance of the considered system is investigated in the presence of a single passive eavesdropper (E) equipped with multiple antennas N_{e}. For a practical scenario, the CSI of the eavesdropper is assumed to be unavailable and the eavesdropper is assumed to be located randomly between the K users and the relay node R. Since the eavesdropper is passive, its wiretap channel CSI is unavailable at the legitimate K users and relay. For a fair secrecy performance study, the passive eavesdropper is assumed to be equipped with multiple antennas.

Hence, in the RF phase, the received signal at E through the i-th antenna from the k-th user is given by

$$y_{k,i,\mathsf{e}} = \sqrt{P_k} h_{k,i,\mathsf{e}} x_k + w_{\mathsf{e}}, \tag{4.42}$$

where $h_{k,i,\mathsf{e}}$ is the wiretap channel coefficient between the k-th user (U_k) and the i-th antenna at E, $w_{\mathsf{e}} \sim \mathcal{CN}(0, N_0)$ is an AWGN sample at E. Using (4.42), the SNR observed at the i-th antenna of E can be expressed as

$$\gamma_{k,i,\mathsf{e}} = \frac{P_k}{N_0} |h_{k,i,\mathsf{e}}|^2. \tag{4.43}$$

Since the eavesdropper E applies MRC technique, the combined SNR of the U_k → E link can be written as

$$\gamma_{k,\mathsf{e}} \triangleq \frac{P_k}{N_0} \|\mathbf{h}_{k,\mathsf{e}}\|^2 = \sum_{i=1}^{N_{\mathsf{e}}} \gamma_{k,i,\mathsf{e}}. \tag{4.44}$$

According to Shannon's theorem, the capacity of wiretap channel (i.e., $\mathrm{U}_k - \mathrm{E}$ link) is given by

$$C_{k,\mathsf{e}} = \log_2 \left(1 + \frac{P_k}{N_0} \|\mathbf{h}_{k,\mathsf{e}}\|^2 \right). \tag{4.45}$$

Hence, the intercept probability represents the probability that the wiretap channel capacity is higher than $\mathcal{R}$, such as

$$P_{\mathrm{int}}^{(k)} = \Pr(C_{k,\mathsf{e}} > \mathcal{R}). \tag{4.46}$$

Similarly, the substitution of $C_{k,\mathsf{e}}$ from (5.33) in (4.46) leads to

$$\begin{aligned} P_{\mathrm{int}}^{(k)} &= \Pr\left(\log_2\left(1 + \frac{P_k}{N_0}\|\mathbf{h}_{k,\mathsf{e}}\|^2\right) > \mathcal{R}\right) \\ &= \Pr\left(\frac{P_k}{N_0}\|\mathbf{h}_{k,\mathsf{e}}\|^2 > \delta\right), \end{aligned} \tag{4.47}$$

where δ is a predetermined outage threshold defined by $2^{\mathcal{R}} - 1$. Based on the aforementioned discussion on the considered model analysis, the wiretap channel is the channel between the selected best user $\mathrm{U}_{\mathrm{Sel}}$ and the eavesdropper E. Hence, the wiretap channel capacity can be expressed as

$$\begin{aligned} P_{\mathrm{int}}^{\mathrm{Sel}} &= \Pr\left(\log_2\left(1 + \frac{P_{\mathrm{Sel}}}{N_0}\|\mathbf{h}_{\mathrm{Sel},\mathsf{e}}\|^2\right) > \mathcal{R}\right) = \Pr\left(\frac{P_{\mathrm{Sel}}}{N_0}\|\mathbf{h}_{\mathrm{Sel},\mathsf{e}}\|^2 > \delta\right) \\ &= \sum_{k=1}^{K} \Pr\left(\mathrm{U}_k = \mathrm{U}_{\mathrm{Sel}}\right) \Pr\left(\frac{P_k}{N_0}\|\mathbf{h}_{k,\mathsf{e}}\|^2 > \delta\right), \end{aligned} \tag{4.48}$$

where $\mathbf{h}_{\mathrm{Sel},\mathsf{e}}$ is the wiretap channel coefficient vector between the selected best user ($\mathrm{U}_{\mathrm{Sel}}$) and the N_{e} antennas at E, and P_{Sel} is the transmission power of the selected best user. The term $\Pr\left(\mathrm{U}_k = \mathrm{U}_{\mathrm{Sel}}\right)$ denotes the event that the k-th user is the selected user $\mathrm{U}_{\mathrm{Sel}}$ by the authorized relay R. Noting that, this probability depends on the combining technique applied by R (i.e., MRC or SC) such as

$$\Pr\left(\mathrm{U}_k = \mathrm{U}_{\mathrm{Sel}}\right) = \begin{cases} \Pr\left(\max\limits_{j\in\{K-k\}} \|\mathbf{h}_{j,\mathsf{r}}\|^2 < \|\mathbf{h}_{k,\mathsf{r}}\|^2\right), & \text{for MRC} \\ \Pr\left(\max\limits_{\substack{j\in\{K-k\} \\ 1<i<N_{\mathsf{r}}}} |h_{j,i,\mathsf{r}}|^2 < |h_{k,\mathsf{r}}|^2\right), & \text{for SC} \end{cases}. \tag{4.49}$$

On the other hand, the eavesdropper E is assumed to apply a MRC technique to maximize the total SNR of the received signal. Hence, the term $\Pr\left(\frac{P_k}{N_0}\|\mathbf{h}_{k,\mathsf{e}}\|^2 > \delta\right)$ in (4.48) is given by

$$\begin{aligned} \Pr\left(\frac{P_k}{N_0}\|\mathbf{h}_{k,\mathsf{e}}\|^2 > \delta\right) &= 1 - \Pr\left(\frac{P_k}{N_0}\|\mathbf{h}_{k,\mathsf{e}}\|^2 < \delta\right) \\ &= \sum_{l=0}^{m_k N_{\mathsf{e}}-1} \frac{\left(m_k \lambda_{k,\mathsf{e}} \delta\right)^l}{l!} \exp\left(-m_k \lambda_{k,\mathsf{e}} \delta\right), \end{aligned} \tag{4.50}$$

Then, at high SNR values (i.e., $\gamma_{k,\mathsf{e}} \to \infty$), the intercept probability expression can be simplified to

$$\begin{aligned} \overset{\infty}{\Pr}\left(\frac{P_k}{N_0}\|\mathbf{h}_{k,\mathsf{e}}\|^2 > \delta\right) &= 1 - \overset{\infty}{\Pr}\left(\frac{P_k}{N_0}\|\mathbf{h}_{k,\mathsf{e}}\|^2 < \delta\right) \\ &= 1 - \frac{\left(m_k \lambda_{k,\mathsf{e}} \delta\right)^{m_k N_{\mathsf{e}}}}{(m_k N_{\mathsf{e}})!}. \end{aligned} \tag{4.51}$$

Therefore, based on the formulas presented in (4.48), (4.49) and (4.50), we have two different PHY security models as follows:

In this model, the secrecy performance of the considered system is investigated when the authorized relay R performs the MRC technique and the eavesdropper E performs the MRC technique. Hence, the intercept probability for the MRC/MRC model is given by

$$P_{\text{int}}^{\text{Sel,MRC}} = \sum_{k=1}^{K} \Pr\left(\max_{j \in \{K-k\}} \|\mathbf{h}_{j,\mathsf{r}}\|^2 < \|\mathbf{h}_{k,\mathsf{r}}\|^2 \right) \Pr\left(\frac{P_k}{N_0} \|\mathbf{h}_{k,\mathsf{e}}\|^2 > \delta \right), \tag{4.52}$$

where the probability of the best user selection is given by

$$\begin{aligned}
&\Pr\left(\max_{j \in \{K-k\}} \|\mathbf{h}_{j,\mathsf{r}}\|^2 < \|\mathbf{h}_{k,\mathsf{r}}\|^2 \right) = \int_0^\infty \prod_{j \in K-k} F_{\|\mathbf{h}_{j,\mathsf{r}}\|^2}(x) f_{\|\mathbf{h}_{k,\mathsf{r}}\|^2}(x) dx \\
&= \int_0^\infty \prod_{j \in K-k} \left[1 - \sum_{p=0}^{m_j N_\mathsf{r}-1} \frac{(m_j N_\mathsf{r} x)^p}{p!} \exp(-m_j N_\mathsf{r} x) \right] \frac{(m_k \lambda_{k,\mathsf{r}})^{m_k N_\mathsf{r}}}{(m_k N_\mathsf{r} - 1)!} \frac{\exp(-m_k \lambda_{k,\mathsf{r}} x)}{x^{1-m_k N_\mathsf{r}}} dx \\
&= \sum_{j=0}^{K-1} \frac{(-1)^j}{j!} \sum_{\substack{n_1,\ldots,n_K \\ n_j \neq n_k}}^{K-1} \sum_{q_j=0}^{\sum_{t_j=1}^{j} m_{t_j} N_\mathsf{r} - 1} \Xi_{q_j} \frac{(m_k \lambda_{k,\mathsf{r}})^{m_k N_\mathsf{r}}}{(m_k N_\mathsf{r} - 1)!} \int_0^\infty \frac{\exp\left(-(\lambda_{\text{tot}_j} + m_k \lambda_{k,\mathsf{r}}) x\right)}{x^{1-q_j-m_k N_\mathsf{r}}} dx \\
&= \sum_{j=0}^{K-1} \frac{(-1)^j}{j!} \sum_{\substack{n_1,\ldots,n_K \\ n_j \neq n_k}}^{K-1} \sum_{q_j=0}^{\sum_{t_j=1}^{j} m_{t_j} N_\mathsf{r} - 1} \Xi_{q_j} \frac{(m_k \lambda_{k,\mathsf{r}})^{m_k N_\mathsf{r}}}{(m_k N_\mathsf{r} - 1)!} \frac{\Gamma(q_j + m_k N_\mathsf{r})}{(\lambda_{\text{tot}_j} + m_k \lambda_{k,\mathsf{r}})^{(q_j + m_k N_\mathsf{r})}}.
\end{aligned} \tag{4.53}$$

In this model, the secrecy performance of the adopted system is investigated when the authorized relay R performs the SC technique and the eavesdropper E performs the MRC technique. Hence, the intercept probability for the SC/MRC model is given by

$$P_{\text{int}}^{\text{Sel,SC}} = \sum_{k=1}^{K} \Pr\left(\max_{\substack{j \in \{K-k\} \\ 1<i<N_\mathsf{r}}} |h_{j,i,\mathsf{r}}|^2 < |h_{k,\mathsf{r}}|^2 \right) \Pr\left(\frac{P_k}{N_0} \|\mathbf{h}_{k,\mathsf{e}}\|^2 > \delta \right), \tag{4.54}$$

where the probability of best user selection is given by

$$\begin{aligned}
&\Pr\left(\max_{\substack{j\in\{K-k\}\\ 1<i<N_{\mathsf{r}}}} |h_{j,i,\mathsf{r}}|^2 < |h_{k,\mathsf{r}}|^2\right) = \int_0^\infty \prod_{j\in K-k} F_{\|\mathbf{h}_{j,\mathsf{r}}\|^2}(x) f_{\|\mathbf{h}_{k,\mathsf{r}}\|^2}(x)dx \\
&= \sum_{i=0}^{N_{\mathsf{R}}} \binom{N_{\mathsf{R}}}{i} (-1)^i \widetilde{\sum}_{p_{1,1},\ldots,p_{1,i}}^{m_1-1} \ldots, j\neq k, \ldots \widetilde{\sum}_{p_{K,1},\ldots,p_{K,i}}^{m_K-1} \Upsilon_{j,\Delta_j} \\
&\times \frac{(m_k\lambda_{k,\mathsf{r}})^{m_k N_{\mathsf{r}}}}{(m_k N_{\mathsf{r}}-1)!} (\lambda_{\mathrm{tot}_{j},\Delta_j} + m_k\lambda_{k,\mathsf{r}})^{-(\Delta_j + m_k N_{\mathsf{r}})} \Gamma(\Delta_j + m_k N_{\mathsf{r}}). \qquad (4.55)
\end{aligned}$$

4.5.1.2 Impact of RF Power Allocation on Secrecy Performance

In this part, we investigate the impact of the proposed RF transmission power relation in Section 4.4.5 on the PHY security of the considered system. The relation in (4.38) states that the optimal RF transmission power depends on the dominant link between the RF and FSO links. To emphasize the importance of the power allocation relation (4.38), consider a single user $K = 1$ which transmits its data with a maximum transmission power P_{T_1} in the presence of a passive eavesdropper equipped with N_{e} antennas. Hence, the intercept probability of the single user is given by

$$\Pr\left(\frac{P_k}{N_0}\|\mathbf{h}_{k,\mathsf{e}}\|^2 > \delta\right) = \sum_{l=0}^{m_1 N_{\mathsf{e}}-1} \frac{(m_1\lambda_{1,\mathsf{e}}\delta)^l}{l!} \exp\left(-m_1\lambda_{1,\mathsf{e}}\delta\right), \qquad (4.56)$$

Then, at high SNR values (i.e., $\gamma_{k,\mathsf{e}} \to \infty$), the intercept probability expression can be simplified to

$$\begin{aligned}\overset{\infty}{\Pr}\left(\frac{P_1}{N_0}\|\mathbf{h}_{1,\mathsf{e}}\|^2 > \delta\right) &= 1 - \frac{(m_1\lambda_{1,\mathsf{e}}\delta)^{m_1 N_\mathsf{e}}}{(m_1 N_\mathsf{e})!} \\ &= 1 - \frac{(m_1\delta)^{m_1 N_\mathsf{e}}}{(m_1 N_\mathsf{e})!}\left(\frac{N_0}{P_{\mathsf{T}_1}\Omega_{1,\mathsf{e}}}\right)^{m_1 N_\mathsf{e}}. \qquad (4.57)\end{aligned}$$

It is clear from (4.57) that the intercept probability depends on the value of the RF transmission power (P_{T_1}). It is obvious that increasing P_{T_1} harms the system security by increasing the probability of intercept. Whereas, decreasing P_{T_1} decreases the intercept probability and enhances the system secrecy performance. On the other hand, decreasing P_{T_1} increases the system RF outage probability and harms the system reliability performance. This contradiction between the system secrecy performance represented by the intercept probability and the system reliability performance represented by the outage probability is known as security-reliability trade-off (SRT) analysis. This trade-off analysis depends on the value of P_{T_1} which emphasizes the importance of our power allocation relation in (4.38). Since the optimal RF transmission power depends on the dominant link between the two system links (i.e., RF and FSO link), we have the following two cases:

Case (1): FSO link is dominant

In this case, increasing P_{T_1} does not enhance the system outage performance because of the dominant FSO link. Therefore, it would be more practical to transmit with a reduced value P_{req} which is less than P_{T_1}. As a result, the secrecy performance of the considered system will be improved without harming the system outage performance.

Case (2): RF link is dominant

In this case, the RF link dominates the system outage performance, hence, the user has to transmit with its maximum power P_{T_1}. Although reducing the RF transmission power improves the secrecy performance, it also increases the system outage probability. Therefore, we present a CJ model to enhance system secrecy performance in the next part.

4.5.2 Cooperative Jamming Model for Enhancing Physical Layer Security

4.5.2.1 System Intercept Probability

In this part, we employ CJ technique to enhance the system secrecy performance. To do that, a friendly jamming signal which is known to R is employed which can be canceled at R by subtraction [116]. Since the considered system selects the best user among all the K users, the rest $K-1$ users will be idle during the selected best user transmission. Therefore, the proposed CJ model selects the worst $\mathrm{U}_k - \mathrm{R}$ link among the remaining $K-1$ users to broadcast the prior known jamming signal at R to jam E. The worst relay is selected to reduce any interference caused by the jammer in the case of imperfect CSI. Hence, in the RF phase, the received signal at E through the i-th antenna from the k-th user can be expressed as

$$y_{k,i,\mathsf{e}} = \sqrt{P_k} h_{k,i,\mathsf{e}} x_k + \sqrt{P_\mathrm{J}} h_{\mathrm{J},i,\mathsf{e}} x_\mathrm{J} + w_\mathsf{e}, \tag{4.58}$$

where $h_{\mathrm{J},i,\mathsf{e}}$ is the channel coefficient between the jamming user ($\mathrm{U_J}$) and the i-th antenna at E and x_J is the transmitted jamming signal from $\mathrm{U_J}$ with $\mathbb{E}\{|x_\mathrm{J}|^2\} = 1$. Using (4.58), the SNR observed at the i-th antenna of E can be expressed as

$$\gamma_{k,i,\mathsf{e}} = \frac{P_k |h_{k,i,\mathsf{e}}|^2}{P_\mathrm{J} |h_{\mathrm{J},i,\mathsf{e}}|^2 + N_0}. \tag{4.59}$$

Since the eavesdropper E applies MRC technique, the combined SNR of the U_k → E link can be written as

$$\gamma_{k,\mathsf{e}} \triangleq \frac{P_k \|\mathbf{h}_{k,\mathsf{e}}\|^2}{P_\mathrm{J} \|\mathbf{h}_{\mathrm{J},\mathsf{e}}\|^2 + N_0} = \sum_{i=1}^{N_\mathsf{e}} \gamma_{k,i,\mathsf{e}}. \tag{4.60}$$

According to Shannon's theorem, the capacity of wiretap channel (i.e., $\mathrm{U}_k - \mathrm{E}$ link) is given by

$$C_{k,\mathsf{e}} = \log_2 \left(1 + \frac{P_k \|\mathbf{h}_{k,\mathsf{e}}\|^2}{P_\mathrm{J} \|\mathbf{h}_{\mathrm{J},\mathsf{e}}\|^2 + N_0} \right). \tag{4.61}$$

Again, the intercept probability represents the probability that the wiretap channel capacity is higher than $\mathcal{R}$, such as

$$P_\mathrm{int}^{(k)} = \Pr(C_{k,\mathsf{e}} > \mathcal{R}). \tag{4.62}$$

Similarly, the substitution of $C_{k,\mathsf{e}}$ from (4.61) in (4.62) leads to

$$\begin{aligned} P_{\text{int}}^{(k)} &= \Pr\left(\log_2\left(1+\frac{P_k\|\mathbf{h}_{k,\mathsf{e}}\|^2}{P_{\text{J}}\|\mathbf{h}_{\text{J},\mathsf{e}}\|^2+N_0}\right)>\mathcal{R}\right) \\ &= \Pr\left(\frac{P_k\|\mathbf{h}_{k,\mathsf{e}}\|^2}{P_{\text{J}}\|\mathbf{h}_{\text{J},\mathsf{e}}\|^2+N_0}>\delta\right), \end{aligned} \tag{4.63}$$

Using CJ, the eavesdropper E will be suffering from a jamming signal transmitted by the worst selected user (U_J), hence, the wiretap channel capacity can be expressed as

$$\begin{aligned} P_{\text{int}}^{\text{Sel}} &= \Pr\left(\log_2\left(1+\frac{P_{\text{Sel}}\|\mathbf{h}_{\text{Sel},\mathsf{e}}\|^2}{P_{\text{J}}\|\mathbf{h}_{\text{J},\mathsf{e}}\|^2+N_0}\right)>\mathcal{R}\right) = \Pr\left(\frac{P_{\text{Sel}}\|\mathbf{h}_{\text{Sel},\mathsf{e}}\|^2}{P_{\text{J}}\|\mathbf{h}_{\text{J},\mathsf{e}}\|^2+N_0}>\delta\right) \\ &= \sum_{k=1}^{K}\Pr\left(\text{U}_k=\text{U}_{\text{Sel}}\right)\left[\sum_{t\in\{K-k\}}\Pr\left(\text{U}_t=\text{U}_{\text{J}}\right)\Pr\left(\frac{P_k\|\mathbf{h}_{k,\mathsf{e}}\|^2}{P_J\|\mathbf{h}_{\text{t},\mathsf{e}}\|^2+N_0}>\delta\right)\right]. \end{aligned} \tag{4.64}$$

The results in (4.64) is similar to (4.48) with the new term $\Pr\left(\text{U}_t=\text{U}_{\text{J}}\right)$ denotes the event that the t-th user is the selected worst user (i.e., jamming user U_J) by the authorized relay R. Noting that, this probability depends on the combining technique applied by R (i.e., MRC or SC) such as

$$\Pr\left(\text{U}_t=\text{U}_{\text{J}}\right)=\begin{cases}\Pr\left(\min\limits_{j\in\{K-k-t\}}\|\mathbf{h}_{j,\mathsf{r}}\|^2>\|\mathbf{h}_{t,\mathsf{r}}\|^2\right), & \text{for MRC}\\ \Pr\left(\min\limits_{\substack{j\in\{K-k-t\}\\ 1<i<N_{\mathsf{r}}}}|h_{j,i,\mathsf{r}}|^2>|h_{t,\mathsf{r}}|^2\right), & \text{for SC}\end{cases}. \tag{4.65}$$

On the other hand, the eavesdropper E is assumed to apply a MRC technique to maximize the total SNR of the received signal in the presence of a jamming signal with a power of P_J. Hence, the term $\Pr\left(\frac{P_k\|\mathbf{h}_{k,\mathsf{e}}\|^2}{P_J\|\mathbf{h}_{\mathrm{t},\mathsf{e}}\|^2+N_0} > \delta\right)$ in (4.64) is given by

$$\Pr\left(\frac{P_k\|\mathbf{h}_{k,\mathsf{e}}\|^2}{P_J\|\mathbf{h}_{\mathrm{t},\mathsf{e}}\|^2+N_0} > \delta\right) = 1 - \Pr\left(\frac{P_k\|\mathbf{h}_{k,\mathsf{e}}\|^2}{P_J\|\mathbf{h}_{\mathrm{t},\mathsf{e}}\|^2+N_0} < \delta\right)$$
$$= 1 - \sum_{l=0}^{m_k N_\mathsf{e}-1} \frac{(m_k\lambda_{k,\mathsf{e}}\delta)^l \exp\left(-m_k\lambda_{k,\mathsf{e}}\delta\right)}{l!(m_t\lambda_{t,\mathsf{e}})^{-m_t N_\mathsf{e}}} \Phi\left(m_t N_\mathsf{e}, 1+p+m_t N_\mathsf{e}; m_k\lambda_{k,\mathsf{e}}\delta + m_t\lambda_{t,\mathsf{e}}\right), \tag{4.66}$$

where $\Phi(a,b;c)$ is the confluent hupergeometric function defined by [109, Eq. 9.210.1]. At high SNR values (i.e., $\gamma_{k,\mathsf{e}} \to \infty$), the intercept probability can be simplified to be

$$\overset{\infty}{\Pr}\left(\frac{P_k}{N_0}\|\mathbf{h}_{k,\mathsf{e}}\|^2 > \delta\right) = 1 - \overset{\infty}{\Pr}\left(\frac{P_k}{N_0}\|\mathbf{h}_{k,\mathsf{e}}\|^2 < \delta\right)$$
$$= 1 - \frac{(m_k\lambda_{k,\mathsf{e}}\delta)^{m_k N_\mathsf{e}}}{(m_k N_\mathsf{e})!(m_t\lambda_{t,\mathsf{e}})^{-m_t N_\mathsf{e}}} \Phi\left(m_t N_\mathsf{e}, 1+(m_t+m_k)N_\mathsf{e}; m_t\lambda_{t,\mathsf{e}}\right). \tag{4.67}$$

Therefore, based on the formulas presented in (4.48), (4.49) and (4.50), we have two different PHY security models as follows:

In this model, the secrecy performance of the considered system is investigated when both the authorized relay R and the eavesdropper E perform the MRC technique. Hence, the intercept probability for the MRC/MRC model is given by

$$P_{\mathrm{int}}^{\mathrm{Sel,MRC}} = \sum_{k=1}^{K} \Pr\left(\max_{j\in\{K-k\}} \|\mathbf{h}_{j,\mathsf{r}}\|^2 < \|\mathbf{h}_{k,\mathsf{r}}\|^2\right) \Pr\left(\min_{j\in\{K-k-t\}} \|\mathbf{h}_{j,\mathsf{r}}\|^2 > \|\mathbf{h}_{t,\mathsf{r}}\|^2\right)$$
$$\times \Pr\left(\frac{P_k}{N_0}\|\mathbf{h}_{k,\mathsf{e}}\|^2 > \delta\right), \tag{4.68}$$

where the probability of worst user selection is given by

$$\Pr\left(\min_{j\in\{K-k-t\}} \|\mathbf{h}_{j,\mathsf{r}}\|^2 > \|\mathbf{h}_{t,\mathsf{r}}\|^2\right) = 1 - \int_0^\infty \prod_{j\in\{K-k-t\}} \left[1 - F_{\|\mathbf{h}_{j,\mathsf{r}}\|^2}(x)\right] f_{\|\mathbf{h}_{t,\mathsf{r}}\|^2}(x)dx \tag{4.69}$$

In this model, the secrecy performance of the considered system is investigated when the authorized relay R performs the SC technique and the eavesdropper E performs the MRC technique. Hence, the intercept probability for the SC/MRC model is given by

$$\begin{aligned} P_{\text{int}}^{\text{Sel,SC}} = \sum_{k=1}^{K} \Pr\left(\max_{\substack{j\in\{K-k\}\\ 1<i<N_{\mathsf{r}}}} |h_{j,i,\mathsf{r}}|^2 < |h_{k,\mathsf{r}}|^2\right) \Pr\left(\min_{\substack{j\in\{K-k-t\}\\ 1<i<N_{\mathsf{r}}}} |h_{j,i,\mathsf{r}}|^2 > |h_{t,\mathsf{r}}|^2\right) \\ \times \Pr\left(\frac{P_k}{N_0}\|\mathbf{h}_{k,\mathsf{e}}\|^2 > \delta\right), \end{aligned} \tag{4.70}$$

where the probability of the worst user selection is given by

$$\Pr\left(\min_{\substack{j\in\{K-k-t\}\\ 1<i<N_{\mathsf{r}}}} |h_{j,i,\mathsf{r}}|^2 > |h_{t,\mathsf{r}}|^2\right) = 1 - \int_0^\infty \prod_{j\in\{K-k-t\}} \left[1 - F_{\|\mathbf{h}_{j,\mathsf{r}}\|^2}(x)\right] f_{\|\mathbf{h}_{t,\mathsf{r}}\|^2}(x)dx \tag{4.71}$$

4.5.2.2 Power Allocation for PHY Security Enhancement

In this part, a power allocation optimization problem is formulated to enhance the CJ model PHY security performance. The power allocation problem here aims to find the optimal transmission and jamming powers which achieve a certain outage probability performance ($P_{\text{out,Req.}}^{\text{CJ}}$) for the CJ PHY security model. For a fair comparison between the secrecy performance of the proposed CJ model and the secrecy performance considered MU SIMO RF/FSO system without CJ, the total power for transmission and jamming is set to be equal to the maximum user transmission power P_{T} (i.e., $P_{\mathsf{T}} = P_{\text{Req.}} + P_{\text{J}}$).

Based on the above-mentioned discussion, the outage performance of the CJ model is similar to the performance of the normal RF/FSO model since the authorized destination is assumed to know the jamming signal. Hence, the outage probabilities of both models are identical. For simplicity, the asymptotic outage probability is used to obtain the optimal transmission powers. Again, since the outage probability of the considered system with CJ model depends on the dominant link between the two RF and FSO links, we have two different cases:

Case (1): FSO link is dominant

In this case, the optimal power allocation formula which is presented in Section. 4.4.2 is valid. The the transmission RF power is set to be P_{req} and the jamming power is given by $P_{\text{J}} = P_{\mathsf{T}} - P_{\text{req}}$. It is important to emphasize that the CJ model enhances the system secrecy performance in two ways. Firstly, the CJ model decreases the RF transmission power to P_{req} without harming the system outage probability. Secondly, the deducted power from the RF transmission is used as a jamming power P_{J} is used by the friendly jammer node (i.e., the selected worst user) to enhance the system secrecy performance.

Case (2): RF link is dominant

In this case, the RF link dominates the system outage performance. Hence, the user has to transmit with its maximum power P_{T}. Therefore, another power allocation problem is formulated to find the optimal power value P_k^* which set the RF/FSO system with CJ model outage probability to a certain required value ($P_{\text{out,Req.}}^{\text{CJ}}$). Then, the remaining power is allocated for CJ to improve the PHY security of the system. The optimization problem can be formulated such as

$$\begin{aligned} &\text{Minimize } \; P_k \\ &\text{subject to: } P_{\text{out}}^{\infty,\text{CJ}} = P_{\text{out,Req.}}^{\infty,\text{CJ}} > P_{\text{out,Min.}}^{\infty,\text{CJ}} \\ &\qquad\qquad P_k + P_{\text{J}} = P_{\mathsf{T}}, \end{aligned} \tag{4.72}$$

where $P_{\text{out,Req.}}^{\infty,\text{CJ}}$ is a predetermined required asymptotic RF outage probability which cannot exceed the minimum outage probability $P_{\text{out,Min.}}^{\infty,\text{CJ}}$ achieved by the system when the total power P_{T} is used for transmission only. Hence the optimal power P_k^* is given by

$$P_k^* = \begin{cases} \left[\prod_{k=1}^{K} \frac{\left(m_k N_0 \Omega_{k,N_{\mathsf{r}}}^{-1} \gamma_{\mathsf{out}}\right)^{m_k N_{\mathsf{r}}}}{(m_k N_{\mathsf{r}})! P_{\text{out,Req.}}^{\infty,\text{CJ}}}\right]^{\frac{1}{\sum_{k=1}^{K} m_k N_{\mathsf{r}}}}, & \text{for MRC} \\ \left[\prod_{k=1}^{K} \frac{\left(m_k N_0 \Omega_{k,N_{\mathsf{r}}}^{-1} \gamma_{\mathsf{out}}\right)^{m_k N_{\mathsf{r}}}}{m_k! P_{\text{out,Req.}}^{\infty,\text{CJ}}}\right]^{\frac{1}{\sum_{k=1}^{K} m_k N_{\mathsf{r}}}}, & \text{for SC} \end{cases}. \tag{4.73}$$

Under the assumption of identical users channels with equal transmission powers, the optimal value is given by

$$P_k^* = \begin{cases} \frac{N_0 m_u \gamma_{\mathsf{out}}}{\Omega_{u,r}((m_u N_{\mathsf{r}})!)^{m_u N_{\mathsf{r}}}} \left(P_{\text{out,Req.}}^{\infty,\text{CJ}}\right)^{\frac{-1}{m_u N_{\mathsf{r}} K}}, & \text{for MRC} \\ \frac{N_0 m_u \gamma_{\mathsf{out}}}{\Omega_{u,r}((m_u N_{\mathsf{r}})!)^{m_u}} \left(P_{\text{out,Req.}}^{\infty,\text{CJ}}\right)^{\frac{-1}{m_u N_{\mathsf{r}} K}}, & \text{for SC} \end{cases}. \tag{4.74}$$

Hence, the jamming power is given by

$$P_{\mathrm{J}} = P_{\mathsf{T}} - P_k^*. \tag{4.75}$$

4.6 Numerical Results

Numerical examples and Monte-Carlo simulations are generated to validate the reliability of the newly derived exact and asymptotic expressions via comparison. Numerical examples are provided to show the effect of cooperative jamming, number of users, power optimization, number of antennas at the relay, turbulence fading parameters and pointing error on the system performance. The used modulation scheme is assumed to be binary phased shift keying (BPSK), and 10^6 iterations have been run in generating the simulation results.

The impact of K on the system outage performance is investigated in Figure 4.2. For combining schemes, results show that increasing the K increases the system diversity order. Moreover, it is clear that the outage performance of MRC scheme outperforms the SC scheme as the average SNR of selected user in the MRC scheme (all antennas are considered in the selection process) is larger than that in the SC scheme (one antenna is considered in the selection process). This performance gap between the two combining schemes becomes smaller with high number of users since keeping increasing number of users reaches the point where the FSO link becomes dominating the system performance rather the RF link.

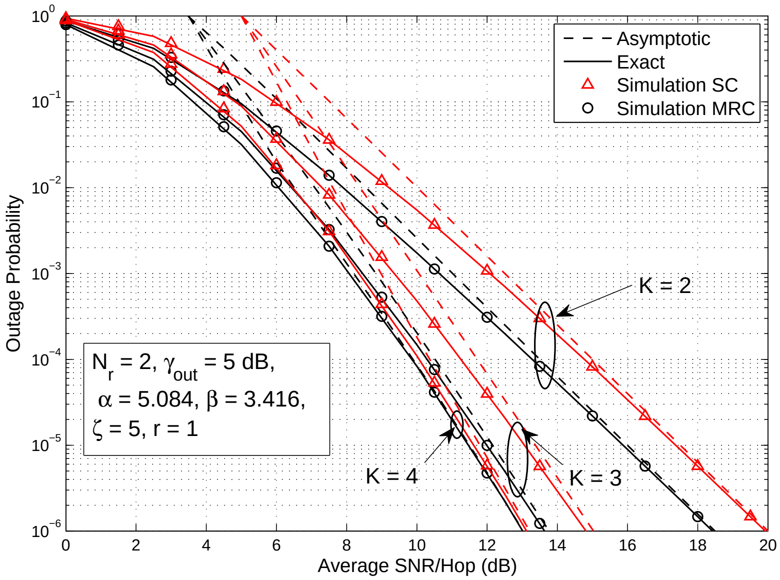


Figure 4.2: Outage probabilities for both MRC and SC schemes versus SNR of the considered system with opportunistic scheduling and different number of users K.

This fact is clearly shown in the asymptotic results. Also, it is important to mention that both MRC and SC schemes achieve the same diversity gain but the MRC has a better coding gain compared to SC scheme.

Another parameter which affects the system outage performance is the Nakagami-m fading parameter represented by m_u and it is studied in Figure 4.3. For both combining schemes, results show that increasing m_u enhances the system reliability by increasing its diversity order. Again, the impact of m_u on the system performance is also limited by the FSO link conditions.

Figure 4.4 shows how the FSO link atmospheric turbulence conditions, represented by α and β, could harm the considered system performance. It can be notice that decreasing α and β (i.e., stronger turbulence conditions) leads to the situation where the FSO link dominants the system performance which may kill

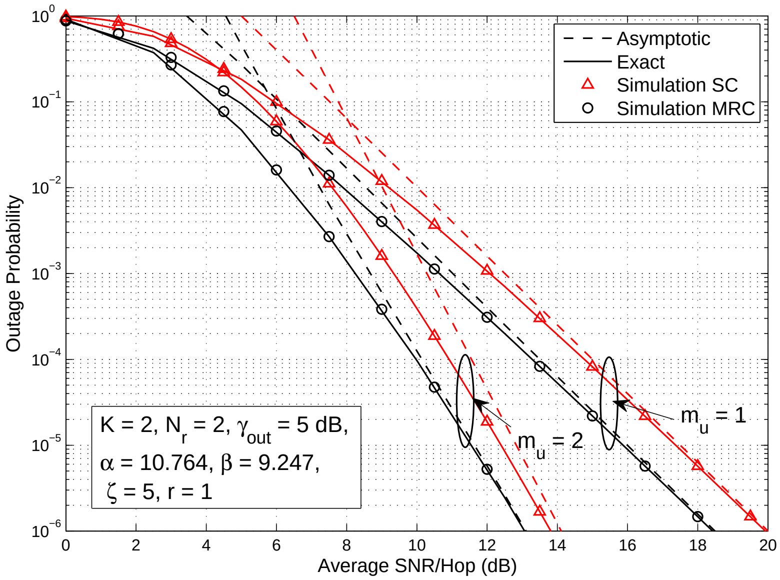


Figure 4.3: Outage probabilities for both MRC and SC schemes versus SNR of the considered system with opportunistic scheduling and different values of Nakagami-m parameter m_u.

any improvements in the system performance coming from the RF link. For fixed values of K, m_k and N_r (i.e., RF link diversity gain is fixed), it can be noticed that the considered system diversity order is directly affected by the FSO link conditions. Moreover, it is clear that at strong turbulence, there is no performance gain for MRC scheme over the SC scheme. Whereas, keeping increasing α and β reduces the fading severity of FSO links and results in a remarkable improvement in the MRC scheme performance over the SC scheme performance.

The average symbol error probability performances of both heterodyne detection (i.e., $r = 1$) and IM/DD detection (i.e., $r = 2$) schemes are presented in Figure 4.5. Results show that the performance of heterodyne detection mode outperforms the IM/DD mode , as expected. This performance gain is achieved with a complexity plenty.

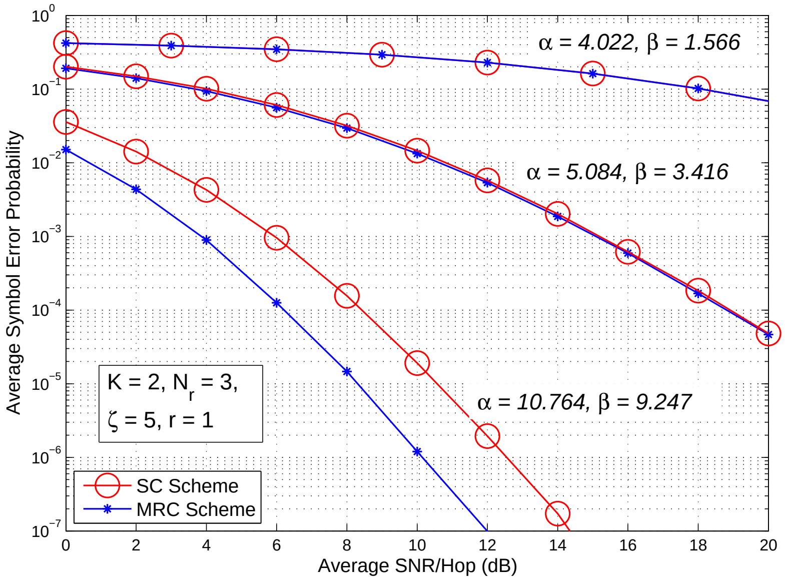


Figure 4.4: Average symbol error probabilities for both MRC and SC schemes versus SNR of the considered system with opportunistic scheduling and different atmospheric turbulence conditions.

The effect of pointing error (i.e., ζ) on the considered system ergodic capacity is investigated in Figure 4.6. It is clear that increasing ζ improves the system ergodic capacity. Moreover, results illustrate that the MRC scheme can achieve a higher system ergodic capacity than the SC scheme, as expected. This gain in system capacity due to using MRC scheme becomes smaller as ζ keeps increasing.

The effect of relay antennas N_{r} on the system ergodic capacity is studied in Figure 4.7 under weak turbulence conditions. It is clear that increasing N_{r} increases the system ergodic capacity. In addition, it can be noticed that increasing N_{r} has a significant improvement on the ergodic capacity performance of the MRC scheme compared to SC scheme, as expected.

The optimal power allocation formula which was provided in (4.38) is validated in Figure 4.8. Under different FSO turbulence conditions, the formula is

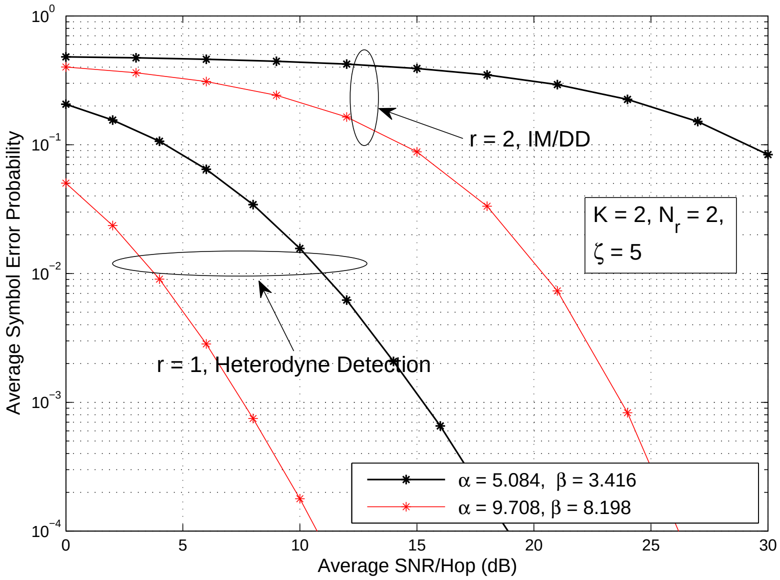


Figure 4.5: Average symbol error probabilities for both MRC and SC schemes versus SNR of the considered system with opportunistic scheduling and different types of optical detection schemes r.

investigated for different number of users K. As long as the RF link dominates the system performance, the selected user transmits with maximum power $P_{\mathsf{T}} = 1$ (i.e., normalized). Once the FSO link dominates the performance, the proposed optimal power allocation formula obtains the required user transmission power P^{opt} which guarantees the best RF link performance (RF outage $= 0.01$ FSO outage) and saves the rest of the power as there will be no performance improvement due to increasing it. As shown in this figure, for the case of strong turbulence ($\alpha = 4.022, \beta = 1.566$), it can be noticed that the selected user transmits with P_{T} as long as $K \leq 2$. As K becomes > 2, the FSO link becomes the dominant link and the selected user transmits with a power less than P_{T} with no wasted power. On the other hand, for the case of weak turbulence ($\alpha = 21.589, \beta = 19.821$), it can be noticed that the selected user transmits with P_{T} as long as $K \leq 4$ as in this

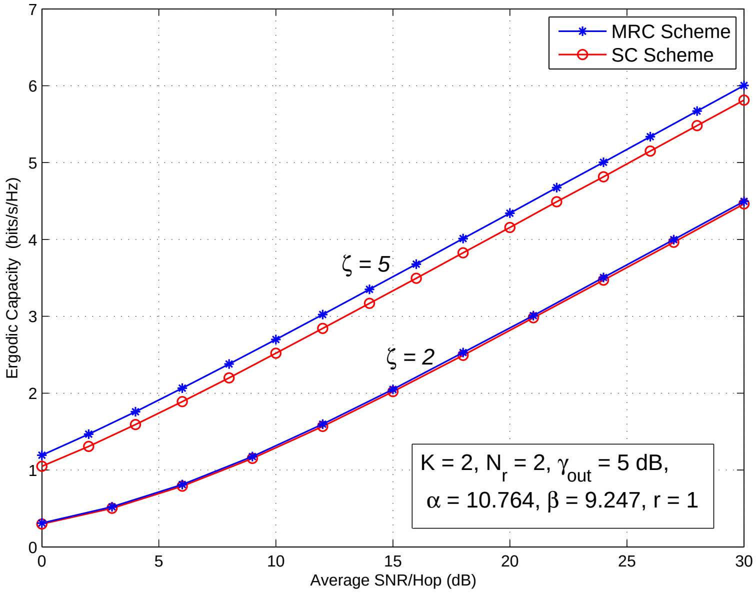


Figure 4.6: Ergodic capacities for both MRC and SC schemes versus SNR of the considered system with opportunistic scheduling and different values of pointing error ζ.

case, the FSO link needs more users in order to dominate the system performance.

The secrecy performance of the considered system with MRC scheme is studied in Figure 4.9 for different number of eavesdropper antennas N_e. Results show that increasing N_e improves the eavesdropper intercept probability and degrades the system security. This is because increasing N_e increases the number of links between the eavesdropper and the selected user which improves the total e2e SNR value at the eavesdropper and results in increasing the intercept probability.

The SRT analysis of the considered system in presented in Figure 4.10 where the trade-off relation between the system outage probability and intercept probability is investigated. Results show that increasing the number of users K improves the system security performance against a multiple-antenna eavesdropper attack.

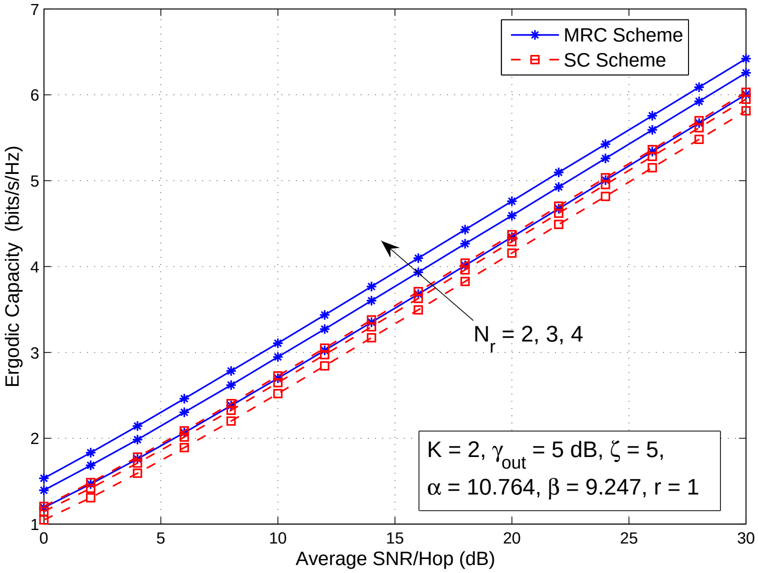


Figure 4.7: Ergodic capacities for both MRC and SC schemes versus SNR of the considered system with opportunistic scheduling and different values of N_{r}.

This is because increasing K increases the system diversity order which results in decreasing the needed transmission power to achieve the same outage probability value. Hence, the system intercept probability decreases and enhances the security performance.

The effect of number of relay antennas N_{r} on the system secrecy performance is illustrated in Figure 4.11. It is clear from this figure that increasing N_{r} under a certain outage probability performance decreases the system intercept probability and enhances the system secrecy performance. This improvement in the system secrecy performance can be explained by the fact that increasing the number of relay antennas decreases the needed transmission power to achieve the same outage performance resulting in enhancing the system secrecy performance. It is obvious also that increasing the required outage probability from 10^{-1} to 10^{-3}

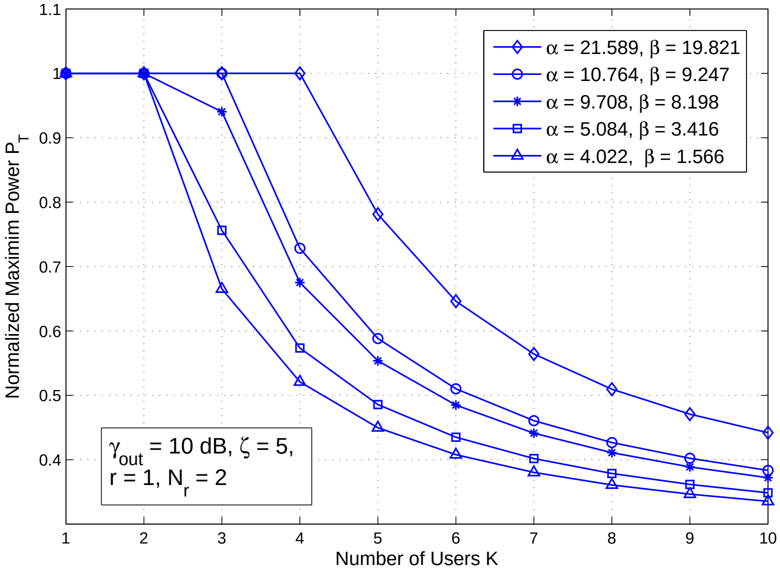


Figure 4.8: Optimal power allocation for MRC scheme versus number of users K for different atmospheric turbulence conditions α and β.

harms the system secrecy performance as in this case the selected best user needs to pump more transmission power to achieve a better outage performance which results in increasing the system intercept probability.

The impact of optimal power allocation on the secrecy performance is investigated in Figure 4.12. As previously mentioned, the selected user transmits with maximum transmission power P_{T} as long as the RF link is dominant. This maximum power transmission gives an advantage for the eavesdropper to overhear the authorized transmission. Once the FSO link dominates the system performance, there is no need for the selected user to transmit with maximum power. Hence, the optimal PA obtains the needed transmission value which depends on the system diversity order and the FSO link conditions. With this power allocation scheme, reducing the selected user transmission power harms the intercept

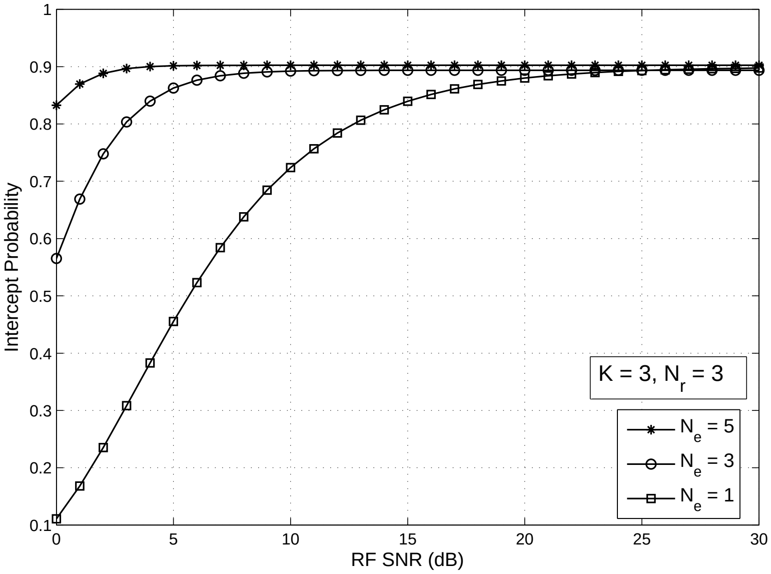


Figure 4.9: Intercept probability of MRC scheme of the considered system with opportunistic scheduling and different number of eavesdropper antennas N_e.

probability without affecting the system outage performance. In this figure, it is shown that increasing N_{r} with applying power allocation outperforms the secrecy performance without no power allocation.

Figure 4.13 studies the impact of the proposed power allocation scheme on the SRT analysis of the considered system. Results show that the proposed power allocation formula has a significant impact on the system secrecy performance in different FSO link conditions. It can be noticed that when the system applies the optimal power allocation scheme, the SRT curve moves downwards. This is because the power allocation scheme allows the selected user to reduce its transmission power to a certain value that keeps the same system outage performance. Whereas, this power reduction degrades the system intercept probability which results in enhancing system secrecy performance. Therefore, for the same value of

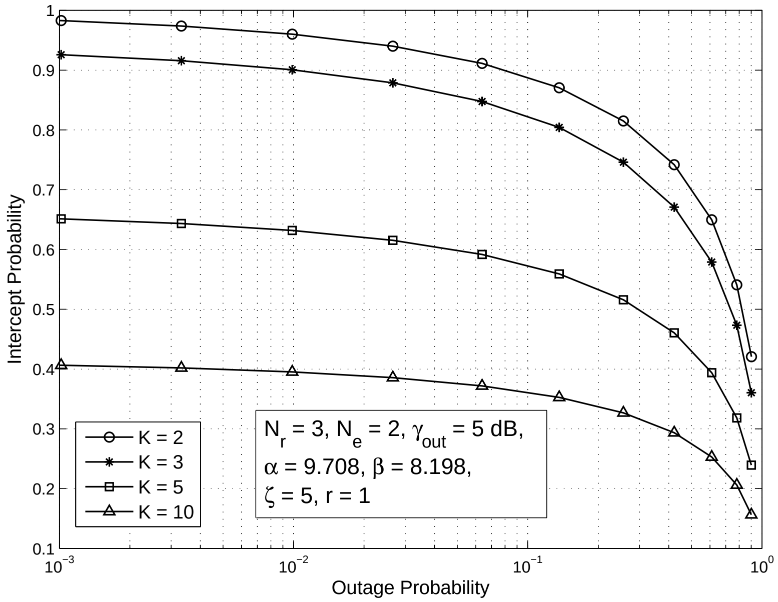


Figure 4.10: SRT analysis for MRC scheme of the considered system with opportunistic scheduling and different number of users K.

outage probability the power allocation scheme achieves a smaller intercept probability compared to no power allocation case. Moreover, as mentioned before, the atmospheric turbulence conditions α and β are two main parameters which affect the value of the optimal transmission power. Hence, it is clear that the optimal power value of the weak turbulence case is higher than the optimal value of the strong turbulence case. As a result, the secrecy performance of the strong turbulence case outperforms the secrecy performance of the weak turbulence case.

The intercept probability for the proposed CJ model versus SNR for different values of jamming power P_{J} is discussed in Figure 4.14. Results show that increasing P_{J} decreases the system intercept probability and improves its secrecy performance, as expected.

The CJ model performance is investigated for different values of outage per-

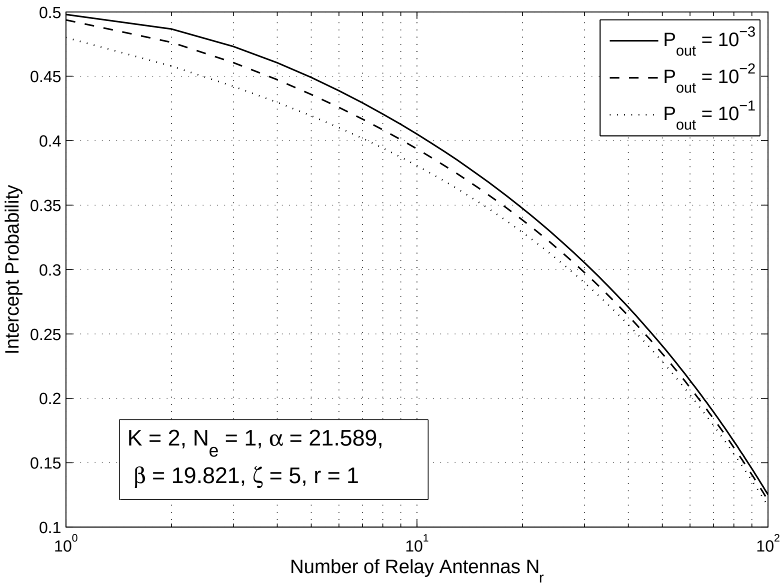


Figure 4.11: Intercept Probability for MRC scheme versus number relay antennas N_r of the considered system with opportunistic scheduling and different values of outage probability P_out.

formance in Figure 4.15. Results demonstrate that increasing the needed outage probability values decreases the system intercept probability and enhances the secrecy performance for two reasons. First, high outage probability performance requires less transmission power from the selected user which reduces the system intercept probability. Second, this reduction in the required transmission power increases the jamming power P_J resulting in a further enhancement in the system secrecy performance.

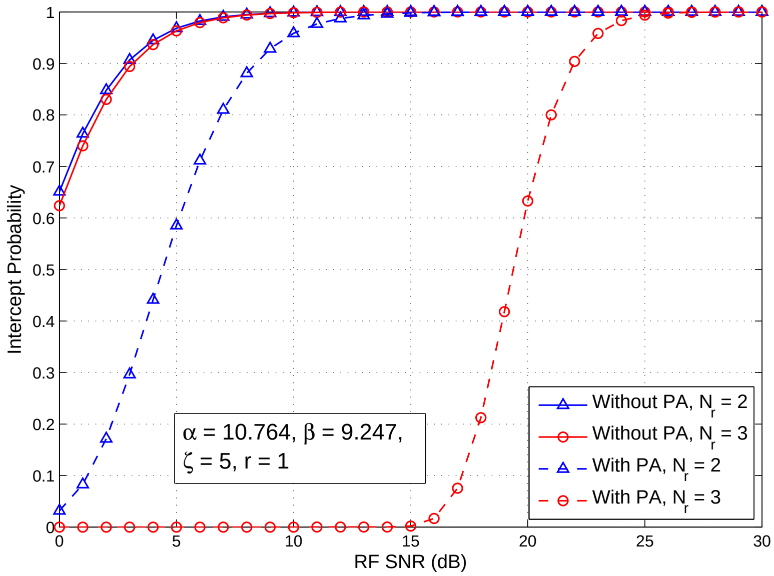


Figure 4.12: The impact of optimal power allocation on the secrecy performance for MRC scheme of the considered system with opportunistic scheduling and different number of relay antennas N_r.

4.7 Conclusion

In this chapter, we studied the performance of dual-hop MU SIMO mixed RF/FSO relay network with opportunistic scheduling and two different diversity combing schemes (MRC and SC). Closed-from expressions were derived for the outage probability, ASEP and ergodic capacity assuming Nakagami-m/Gamma-Gamma fading distributions for the RF/FSO links with the consideration of pointing errors. For high SNR values, closed-form expressions for the asymptotic outage probability were derived and used in obtaining optimal power allocation solutions. Moreover, the secrecy performance of the considered system against a multiple-antenna eavesdropper attack was investigated and the system intercept probability formula was derived. To enhance the secrecy performance of the con-

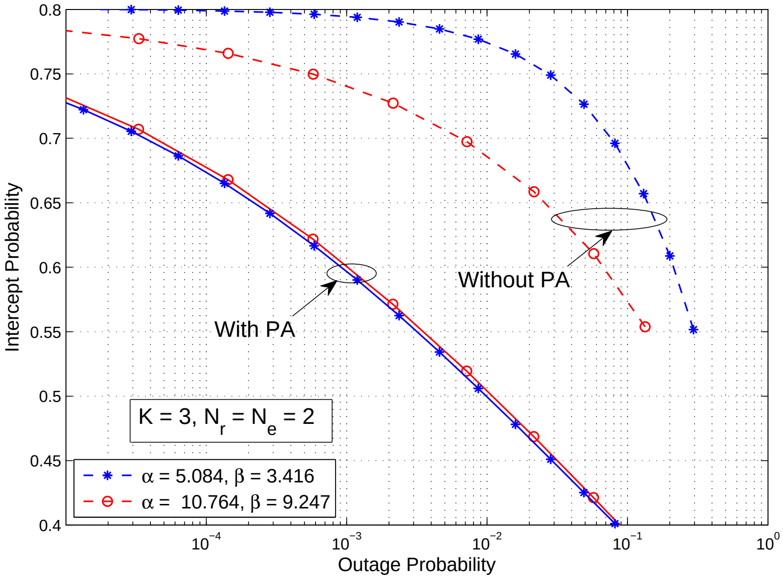


Figure 4.13: The impact of optimal power allocation on the SRT analysis for SC scheme of the considered system with opportunistic scheduling and different atmospheric turbulence conditions α and β.

sidered system, a new cooperative model which employs the selected worst user by the authorized relay to serve as a friendly jammer was proposed. Also, closed-form expressions for the intercept probability of CJ model were derived. The findings demonstrated that under weak atmospheric turbulence conditions, RF links dominate the system overall performance resulting in achieving a full diversity order of $m_k N_{\mathrm{r}} K$. In the case of strong atmospheric turbulence conditions, the FSO link dominates the system performance which limits the diversity order to the minimum value of the turbulence fading and pointing error parameters. Moreover, power allocation formula was shown to provide a significant improvement in the secrecy performance of the considered system. Finally, the proposed CJ model was shown to enhance the system performance, especially for the RF dominant case.

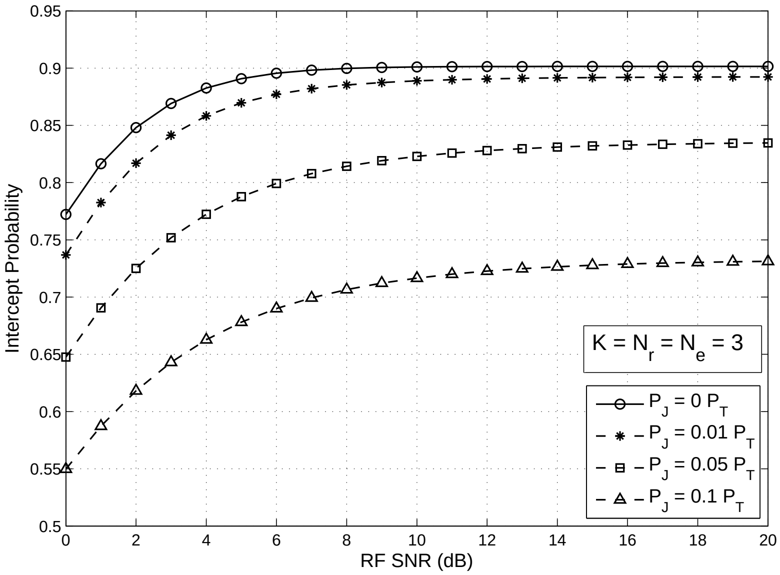


Figure 4.14: Intercept probability for MRC scheme of the considered system with opportunistic scheduling with different value of jamming power P_{J}.

4.8 List of Publications

- **Ahmed H. Abd El-Malek**, Anas M. Salhab and Salam A. Zummo, ″Security-Reliability Analysis and Power Allocation in Multiuser SIMO Mixed RF/FSO Relay Networks, ″ Accepted in IEEE Wireless Commun. and Networking Conf. (WCNC'16), Doha, Qatar, April 2016.
- **Ahmed H. Abd El-Malek**, Anas M. Salhab, Salam A. Zummo and Mohamed-Slim Alouini ″Security and Reliability Analysis of Diversity Combining Technqiues in SIMO Mixed RF/FSO with Multiple Users., ″ to be submitted to the second workshop on Optical Wireless Commun., IEEE Int'l

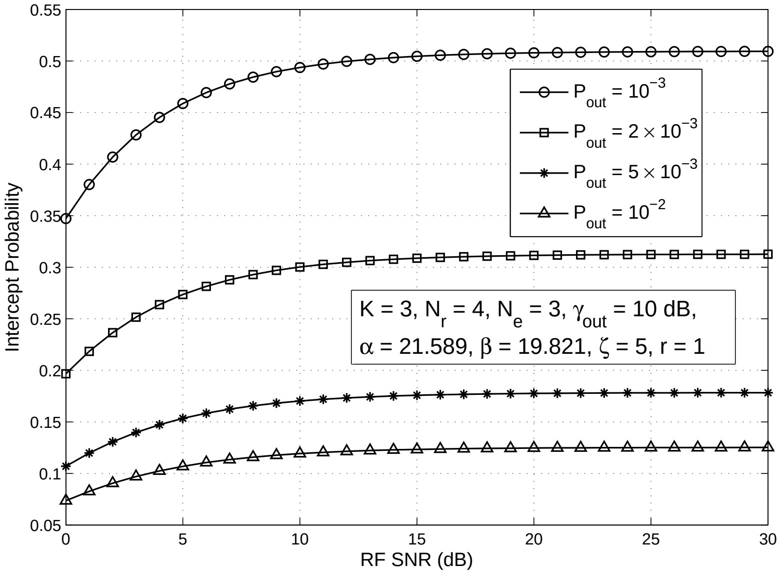


Figure 4.15: CJ model intercept probability for SC scheme versus SNR of the considered system with opportunistic scheduling and different values of outage probability P_{out}.

Conf. on Commun.(ICC'16), Kuala Lumpur, Malaysia, May 2016.

- **Ahmed H. Abd El-Malek**, Anas M. Salhab, Salam A. Zummo and Mohamed-Slim Alouini ″ Security-Reliability Trade-off Analysis for Multiuser SIMO Mixed RF/FSO Relay Networks with Opportunistic User Scheduling,″ to be submitted to IEEE Trans. Wireless Commun..

CHAPTER 5

MULTIUSER MIXED RF/FSO RELAY NETWORKS IN THE PRESENCE OF RF INTERFERENCE

5.1 Introduction

In this chapter, the impact of RF co-channel interference (CCI) on the performance of MU mixed RF/FSO relay network with opportunistic user scheduling is investigated. The considered system includes multiple users, one AF relay, one destination and an eavesdropper. In particular, the SRT analysis is investigated for the considered system in the presence of CCI. We assume that the RF channels are following Nakagami-m distribution, and the FSO channel is following Gamma-Gamma fading distribution in the presence of jitter fading. On the other hand, the RF interference channels are assumed to be independent but non-identically distributed (i.ni.d). Firstly, we investigate the system probability of outage. Then, an asymptotic expression for the outage probability is obtained at the high signal-tointerference-and-noise ratio (SINR) region to get more insights on the system performance key parameters. Moreover, based on asymptotic probability of outage, the optimal transmission power in two different cases based on the atmospheric turbulence conditions. Secondly, the secrecy performance of the considered system is studied in the presence of CCI at both authorized relay and unauthorized eavesdropper. Exact closed-form expression for the intercept probability of the considered system is derived and then simplified to an asymptotic formula. Moreover, the impact of the proposed power allocation formula on the system secrecy performance is investigated under two atmospheric turbulence conditions. Finally, the PHY security performance of the considered MU mixed RF/FSO model is enhanced using two different CJ models. For this purpose, we investigate the intercept probability of the CJ models in the presence of interference over Nakagami-m fading channels. Using the derived asymptotic expression for outage probability, another power allocation optimization problem is formulated and solved to find the optimal transmission and jamming powers needed to enhance the system security. Numerical and simulation results are presented to support the derived mathematical formulas to clarify the main contributions of the work.

The findings of this chapter show that although CCI increases the system outage probability, it might improve the system secrecy performance. Moreover, in the case of weak turbulence conditions, the RF channels dominate the overall performance, and the considered system diversity order depends on the Nakagami-m fading parameter, number of relay antennas and the number of users. Furthermore, for the special case of identical users' channels, the system achieves a maximum diversity order. In the case of strong turbulence conditions, the FSO link dominates the overall performance which limits the system diversity order to the minimum value of the turbulence fading and pointing error parameters. Finally, results show the effectiveness of the proposed power allocation strategy in enhancing the system secrecy performance against possible eavesdropper attacks.

The rest of this chapter is organized as follows. Section 5.2 reviews the literature. Section 5.3 presents the system and channel models. The performance analysis is evaluated in Section 5.4. Section 5.5 provides the PHY security performance analysis with optimal power allocation. Numerical results and simulations are presented and discussed in Section 5.6. Finally, Section 5.7 concludes the work contributions.

5.2 Literature Review

FSO communication systems employ light beams or laser technologies to enhance the wireless network connectivity by providing high data rates. The FSO system provides some benefits over the radio frequency (RF) systems, such as license free operation, low power, high security, simple installation and larger bandwidth. Moreover, the communication operations of the FSO systems depends on the LOS communication between the optical transmitter and receiver which limits the effect of RF interference on the system performance of such systems [61]. Due to the above-mentioned advantages, the FSO systems have been employed in many applications such as in last mile access point in cellular networks and indoor femtocell networks [117].

Although the FSO systems provide efficient solutions for many of RF networks problems such as spectrum sacristy, interference, and security, the performance of FSO system is showed to be limited to some main parameters which are the atmospheric turbulence conditions, the limited laser beam power and pointing errors. The pointing errors are caused by the dynamic misalignment between the optical transmitter and receiver. These aforementioned parameters degrade the performance of the FSO systems and limit their coverage area. Therefore, the mixed RF/FSO relaying networks have been presented as promising communication models which gather the advantages of both RF and FSO network besides the advantages of cooperative communication networks [101]. The mixed RF/FSO networks are dual-hop networks in which the communications take place over an RF channel in the first hop and over an FSO channel in the second hop. These mixed networks enhance the capacity of wireless networks by multiplexing a large number of RF users through a single FSO link [64, 65].

The performance of mixed RF/FSO networks with AF relaying was investigated in [96]. The outage performance of the mixed RF/FSO network was studied in [118] in Rayleigh/Gamma-Gamma channels models. The work was extended in [68] where the outage performance, error probability and ergodic capacity were investigated. Furthermore, the work in [68] investigated the impact of the pointing errors on the system performance. Recently, the general Malaga distribution over the FSO link was used in the analysis of system performance [119] instead of Gamma-Gamma distribution.

One of the advantages of FSO system over the RF systems is their rigidity to RF interference. Due to the mixed communication nature of the RF/FSO network, the co-channel interference would degrade the system performance of the RF links. The impact of CCI on the reliability performance of different RF wireless systems was investigated in [120, 121]. The impact CCI on the system performance of cooperative communications network with AF relaying protocol was studied in [120]. Closed-form expressions for outage and error probabilities were derived for both identical and non-identical channels between the intended nodes. Moreover, the interference channels were assumed to follow identical distribution. Results showed that the system performance is limited by the interference level. The impact non-identical interfering signals on the N-th order best selected relay in dual hop cooperative networks over Rayleigh fading environment was studied in [121]. Close-form expression for exact outage probability was derived. Revealing more insights on the reliability performance, close-form expressions for asymptotic outage probability were derived. Results showed that the system diversity order linearly increases with the number of relays and linearly decreases with the order of the selected relay. Moreover, results illustrated that the system is still able to achieve full diversity order in the presence of finite number of interferes with finite powers.

The LOS nature of FSO systems provides high security against eavesdropping attacks. However, the secrecy performance of a single hop FSO system was investigated in [102]. Although the results showed that the eavesdropper which is nearly located to either the authorized optical transmitter or receiver can harm the FSO system secrecy performance, the disability of splitting the optical transmitted data without affecting its power makes the practicality of the considered security model questionable. On the other hand, the secrecy performance of RF networks was shown to be affected by any eavesdropping attack due to the broadcasting nature of the RF channels. Hence, the RF link might be the weaker link in the mixed RF/FSO network from the secrecy performance viewpoint. Therefore, several PHY security models were proposed and employed along with different RF network models to enhance the secrecy performance against eavesdroppers. The main function of PHY security models is to make use of the available system resources such as spatial-temporal channel characteristics [12], multiple antennas [19], cooperative relays and jammers [122, 41] and beamforming [123] to enhance the main channel conditions against the wiretap channel conditions.

The secrecy performance of multiuser wireless networks were investigated in different system models in the literature [103, 104]. The work in [103] studied the secrecy performance of multiuser uplink wiretap networks where multiple users communicate with a base station in the presence of multiple eavesdroppers. The work proposed that the base station would select a certain user based on a predetermined threshold that is related to the channel gains of the eavesdroppers. Results showed that the proposed sub-optimal user scheduling could guarantee a secure transmission without harming the optimal network throughput. Then, the work has been extended in [104] which studied the secrecy performance of multiuser downlink wiretap networks with opportunistic scheduling where the base station communicates with multiple users in the presence of asymmetrically located eavesdroppers. Closed-form expressions for the secrecy throughput and secrecy outage probability were derived. CJ is another approach to implement cooperation for wireless communications with secrecy constraints [124]. Similar to the artificial noise (AN) scheme, in CJ, the friendly jammers transmit jamming signals (noise) while the source is transmitting the information signal [125].

Recently, the effect of CCI on the secrecy performance of cooperative wireless networks was investigated in [126]. The authors presented optimal and suboptimal relay selection methods for enhancing the secrecy performance of interference-limited cooperative networks with DF relays. In particular, the work concentrated on enhancing the secrecy performance in the cooperative phase (i.e., the second phase of communications) under the assumption of identical interferers only at the destination and the eavesdropper. The relays were assumed to operate in interference-free conditions. The work presented closed-form expressions for the secrecy outage probability and the probability of non-zero secrecy capacity. Although the work in [126] studied the impact of CCI over the second phase of cooperative networks communications, it neglected the impact of CCI over the first phase of cooperative networks communications by assuming interference-free relays which limited the obtained results to a special case of interference-limited networks. The results showed that the presence of CCI might improve or degrade the system secrecy performance. However, the work did not propose any security enhancement scenarios which can improve the secrecy performance when the presence of CCI is harmful.

Based on the above-mentioned discussion, we notice that the impact of CCI on the system reliability performance of MU mixed RF/FSO networks has not been addressed yet. Moreover, the secrecy performance of the considered MU mixed RF/FSO system in the presence of passive eavesdropper and the existence of CCI at both the authorized system and eavesdropper has not been studied yet. Therefore, the main contributions of this work can be summarized as follows. First, the impact of non-identical CCI on the reliability performance of authorized MU mixed RF/FSO system is investigated. Exact closed-form expression for the outage probability of the considered system is derived assuming Nakagami-m/Gamma-Gamma fading channels distribution. Then, asymptotic expressions for the outage probability of the considered system are derived under different conditions of atmospheric channel conditions at the high SNR regime. The obtained asymptotic expressions are used to obtain the optimal RF transmission power based on the diversity order and atmospheric channel conditions. Second, the secrecy performance of the considered system in the presence of single passive eavesdropper is investigated under the existence of non-identical CCI at both authorized system and eavesdropper. Exact closed-form expression for the intercept probability of the considered system is derived, then, it is simplified to a less sophisticated asymptotic expression. The impact of the obtained optimal RF power expression on the secrecy performance is studied. Third, the work employs the CJ technique in the considered system to increase system security in the presence of CCI. To do so, a power allocation optimization problem is formulated to find the optimal transmission and jamming powers needed by the considered model to enhance authorized network PHY security in the presence of a passive eavesdropper. Hence, closed-form expressions of these powers are obtained. Since obtaining closed-form expressions for the security-reliability trade-off (SRT) analysis of the MU mixed RF/FSO model is very complicated, the trade-off analysis is investigated numerically in Section 5.6.

5.3 System and Channel Models

In this section, firstly, some preliminary discussions on the considered system model is presented. Then, a brief discussion on the channel models is introduced.

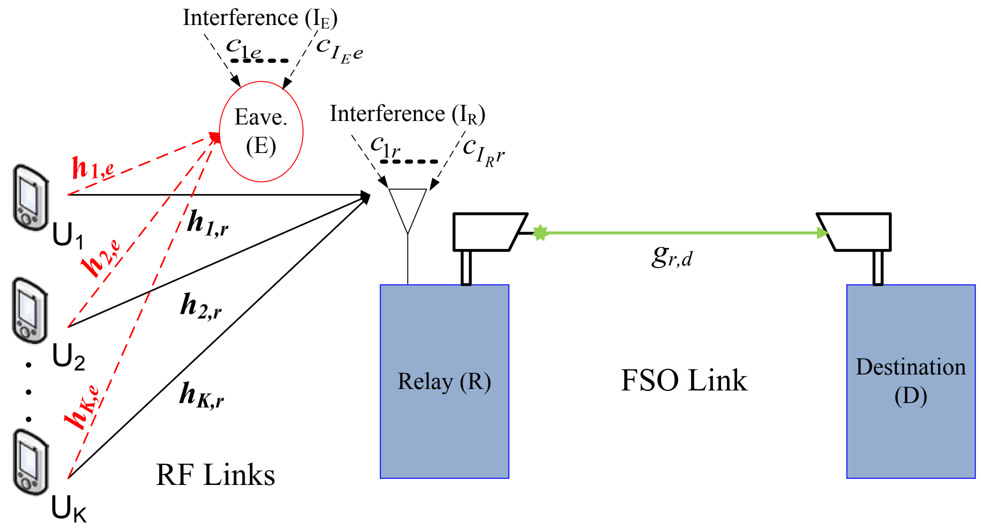


Figure 5.1: Dual-hop MU-SIMO mixed RF/FSO relay network with opportunistic scheduling and multi-antenna eavesdropper.

5.3.1 System Model

As shown in Figure 5.1, The considered system model is a dual-hop MU mixed RF/FSO relay network which consists of K users U_k $(k = 1, \ldots, K)$, equipped with a single antenna each, an AF relay R equipped with a single antenna from one side and a single photo-aperture transmitter from the other side, and one destination D with a single photo detector. The K users communicate with the destination D via the AF relay R with no direct link between the users and D because of the direct link suffers from high fading severity or the destination node is not equipped with RF antennas. Moreover, the communication operates in a half-duplex mode. Hence, the communications take place over two phases, namely, RF phase (where the selected best user communicate with the relay node over RF channel) and FSO phase (where the relay communicates with the destination over optical link). Moreover, the RF links between the K users and the relay are assumed to suffer from a number of non-identical interfering signals (I_{R}) at the front end of the relay antenna which degrades the performance of the considered system RF link. In the RF phase, the received signal at R from the k-th user in the presence of I_{R} interferers can be expressed as

$$y_{k,\mathsf{r}} = \sqrt{P_k} h_{k,\mathsf{r}} x_k + \sum_{i_{\mathsf{r}}=1}^{I_{\mathrm{R}}} \sqrt{P_{i_{\mathsf{r}}}} c_{i_{\mathsf{r}},\mathsf{r}} x_{i_{\mathsf{r}}} + w_{\mathsf{r}}, \tag{5.1}$$

where $h_{k,\mathsf{r}}$ is the RF link channel coefficient between the k-th user (U_k) and R, x_k is the transmitted symbol from U_k with $\mathbb{E}\{|x_k|^2\} = 1$ and transmitted power P_k, $c_{i_{\mathsf{r}},\mathsf{r}}$ is the RF link channel coefficient between the i_{r}-th interferer and R, $x_{i_{\mathsf{r}}}$ denotes the i_{r}-th interference symbol with $\mathbb{E}\{|x_{i_{\mathsf{r}}}|^2\} = 1$ and transmitted power $P_{i_{\mathsf{r}}}$, $w_{\mathsf{r}} \sim \mathcal{CN}(0, N_0)$ is an AWGN sample at R. Based on (5.1), the SINR observed at R can be expressed as

$$\gamma_{k,\mathsf{r}} = \frac{P_k |h_{k,\mathsf{r}}|^2}{\sum_{i_{\mathsf{r}}=1}^{I_{\mathrm{R}}} P_{i_{\mathsf{r}}} |c_{i_{\mathsf{r}},\mathsf{r}}|^2 + N_0}. \tag{5.2}$$

The user selection algorithm implements the opportunistic scheduling based on the $\mathrm{U}_k \rightarrow$ R link. Herein, the user with the largest $\gamma_{k,\mathsf{r}}$ is selected as the best user to communicate R over RF channels such as

$$\gamma_{\mathrm{Sel},\mathsf{r}} \triangleq \frac{\max\limits_{1 \leq k \leq K} [P_k |h_{k,\mathsf{r}}|^2]}{\sum_{i_{\mathsf{r}}=1}^{I_{\mathrm{R}}} P_{i_{\mathsf{r}}} |c_{i_{\mathsf{r}},\mathsf{r}}|^2 + N_0}. \tag{5.3}$$

In the FSO phase, the relay R amplifies the received message $y_{\mathrm{Sel},\mathsf{r}}$ and retransmits to the destination D. Hence, the received signal at D is given by

$$y_{\mathsf{r},\mathsf{d}} = g_{\mathsf{r},\mathsf{d}} \mathsf{G} y_{\mathrm{Sel},\mathsf{r}} + w_{\mathsf{d}}, \tag{5.4}$$

where $g_{\mathsf{r},\mathsf{d}}$ is the link channel coefficient between R and D, G is the relay gain chosen as [108], $\mathsf{G} = \sqrt{\frac{P_{\mathsf{r}}}{P_{\mathrm{Sel}}|h_{\mathrm{Sel},\mathsf{r}}|^2 + \sum_{i_{\mathsf{r}}=1}^{I_{\mathrm{R}}} P_{i_{\mathsf{r}}}|c_{i_{\mathsf{r}},\mathsf{r}}|^2 + N_0}}$ and $w_{\mathsf{d}} \sim \mathcal{CN}(0, N_0)$ is an AWGN sample at D. Upon substituting the value of G in (5.4) and with some simple manipulations, the e2e SNR at D is given by

$$\gamma_{\mathrm{Sel},\mathsf{D}} = \frac{\gamma_{\mathrm{Sel},\mathsf{r}} \widetilde{\gamma}_{\mathsf{r},\mathsf{d}}}{\gamma_{\mathrm{Sel},\mathsf{r}} + \widetilde{\gamma}_{\mathsf{r},\mathsf{d}} + 1}, \tag{5.5}$$

where $\widetilde{\gamma}_{\mathsf{r},\mathsf{d}}$ is the SNR of the FSO hop that is related to the channel coefficient $g_{\mathsf{r},\mathsf{d}}$ of the R → D link. Hence, $\widetilde{\gamma}_{\mathsf{r},\mathsf{d}}$ can be expressed as

$$\widetilde{\gamma}_{\mathsf{r},\mathsf{d}} \triangleq \frac{P_{\mathsf{r}}}{N_0} |g_{\mathsf{r},\mathsf{d}}|^2. \tag{5.6}$$

The SNR in (5.5) can be upper bounded using the approximation (e.g., [68], [99]) $\gamma_{\mathrm{Sel},\mathsf{D}} \cong \min\{\gamma_{\mathrm{Sel},\mathsf{r}}, \widetilde{\gamma}_{\mathsf{r},\mathsf{d}}\}$. Then, the user that has the largest e2e SNR is selected, which gives

$$\gamma_{\mathrm{Sel},\mathsf{D}} = \max\{\gamma_{1,\mathsf{D}}, \gamma_{2,\mathsf{D}}, \ldots, \gamma_{K,\mathsf{D}}\}. \tag{5.7}$$

5.3.2 Channel Model

For RF links, the channel coefficients $h_{k,\mathsf{r}}$, for $k = 1, 2, \ldots, K$, are assumed to follow Nakagami-m fading distribution, then the CDF of the k-th user's (U_k) SNR at R is given by

$$F_{\gamma_{k,\mathsf{r}}}(x) = 1 - \sum_{p=0}^{m_k-1} \frac{(m_k \lambda_{k,\mathsf{r}} x)^p}{p!} \exp\left(-m_k \lambda_{k,\mathsf{r}} x\right), \tag{5.8}$$

where $\lambda_{k,\mathsf{r}} = 1/\bar{\gamma}_{k,\mathsf{r}}$ with $\bar{\gamma}_{k,\mathsf{r}} = \frac{P_k}{N_0}\mathbb{E}\{|h_{k,\mathsf{r}}|^2\} = \frac{P_k}{N_0}\Omega_{k,\mathsf{r}}$.

Moreover, the RF link is assumed to suffer from I_{R} of interfering signals which are assumed to be independent but not necessarily identically distributed (i.ni.d) Nakagami-m random variables with parameters $m_{i_{\mathsf{r}}}$ and $\Omega_{i_{\mathsf{r}},r}$. Hence, the pdf of the total interference at R is given as [127]

$$f_{|c_{i,r}|^2}(y) = \left[\prod_{i_{\mathsf{r}}}^{I_{\mathrm{R}}} (m_{i_{\mathsf{r}}}\lambda_{i_{\mathsf{r}},\mathsf{r}})^{m_{i_{\mathsf{r}}}}\right] \sum_{i_{\mathsf{r}}}^{I_{\mathrm{R}}} \sum_{j=1}^{m_{i_{\mathsf{r}}}} \frac{\beta_{i_{\mathsf{r}}}^{j-1} y^{m_{i_{\mathsf{r}}}-j}}{(m_{i_{\mathsf{r}}}-j)!(j-1)!} \exp(-m_{i_{\mathsf{r}}}\lambda_{i_{\mathsf{r}},\mathsf{r}} y), \tag{5.9}$$

where

$$\beta_{i_{\mathsf{r}}}^{j-1} = \frac{d^{j-1}}{ds^{j-1}} \left[\prod_{\substack{v \neq i_{\mathsf{r}} \\ v=1}}^{I_{\mathrm{R}}} (m_v \lambda_{v,\mathsf{r}} + s)^{m_v}\right]\Bigg|_{s=-m_{i_{\mathsf{r}}}\lambda_{i_{\mathsf{r}},\mathsf{r}}}. \tag{5.10}$$

For the optical link, the FSO link is assumed to follow Gamma-Gamma fading distribution with pointing errors as discussed in Section 4.3.2.

5.4 Performance Analysis

In this section, the system outage performance is investigated. Based on the aforementioned SNR bound, exact closed-form expression of the outage probability is derived. Then, for high SNR values, the exact closed-form expression of the outage probability is simplified to a mathematical formula for the asymptotic outage probability.

5.4.1 Exact Outage Probability

An outage event occurs when the SNR at D goes below a predetermined outage threshold γ_{out}. Hence, the outage probability is given by $P_{\mathsf{out}} = \Pr\left[\gamma_{\mathrm{Sel},\mathsf{D}} \leq \gamma_{\mathsf{out}}\right]$, $\gamma_{\mathsf{out}} = \left(2^{2\mathcal{R}} - 1\right)$ and $\mathcal{R}$ denotes the spectral efficiency. Then, the CDF of $\gamma_{\mathrm{Sel},\mathsf{D}}$ can is given by [110]

$$F_{\gamma_{\mathrm{Sel},\mathsf{D}}}(\gamma) = F_{\gamma_{\mathrm{Sel},\mathsf{r}}}(\gamma) + F_{\widetilde{\gamma}_{\mathsf{r},\mathsf{d}}}(\gamma) - F_{\gamma_{\mathrm{Sel},\mathsf{r}}}(\gamma)F_{\widetilde{\gamma}_{\mathsf{r},\mathsf{d}}}(\gamma), \tag{5.11}$$

where $F_{\gamma_{\mathrm{Sel},\mathsf{r}}}(\gamma)$ and $F_{\widetilde{\gamma}_{\mathsf{r},\mathsf{d}}}(\gamma)$ are the CDFs of first hop SINR and the second hop SNR, respectively. Using the opportunistic scheduling in (5.3), the CDF $F_{\gamma_{\mathrm{Sel},\mathsf{r}}}(\gamma)$ can be written as

$$F_{\gamma_{\mathrm{Sel},\mathsf{r}}}(\gamma) = \int_{1}^{\infty} f_Y(y) \left[\prod_{k=1}^{K} F_{\gamma_{k,\mathsf{r}}}(\gamma y)\right] dy, \tag{5.12}$$

where $F_{\gamma_{k,\mathsf{r}}}(\gamma y)$ is the CDF of the SNR of the k-th user given in (5.8), and $f_Y(y)$ is the pdf of the interference power at R given in (5.9). Hence, substituting (5.8) and (5.9) in (5.12) and applying the identity

$$\prod_{k=1}^{K}(1-q_k)=\sum_{k=0}^{K}\frac{(-1)^k}{k!}\sum_{n_1,\ldots,n_k}^{K}\prod_{t=1}^{k}q_{n_t}, \tag{5.13}$$

with $\sum_{n_1,\ldots,n_k}^{K}$ being a short- hand notation for $\sum\limits_{\substack{n_1=\ldots=n_k=1\\ n_1\neq\ldots\neq n_k}}\ldots\sum$, (5.12) can be rewritten as

$$\begin{aligned}
F_{\gamma_{\mathrm{Sel,r}}}(\gamma) &= \left[\prod_{i_{\mathsf{r}}}^{I_{\mathrm{R}}}(m_{i_{\mathsf{r}}}\lambda_{i_{\mathsf{r}},\mathsf{r}})^{m_{i_{\mathsf{r}}}}\right]\sum_{k=0}^{K}\frac{(-1)^k}{k!}\sum_{n_1,\ldots,n_k}^{K}\sum_{q=0}^{\sum_{t=1}^{k}m_t-1}\sum_{i_{\mathsf{r}}}^{I_{\mathrm{R}}}\sum_{j=1}^{m_{i_{\mathsf{r}}}}\frac{\Xi_q\gamma^q\beta_{i_{\mathsf{r}}}^{j-1}}{(m_{i_{\mathsf{r}}}-j)!(j-1)!} \\
&\quad\times\exp(m_{i_{\mathsf{r}}}\lambda_{i_{\mathsf{r}},\mathsf{r}})\int_{1}^{\infty}(\gamma y)^q(y-1)^{m_{i_{\mathsf{r}}}-1}\exp\left(-(\lambda_{\mathrm{tot}}\gamma+m_{i_{\mathsf{r}}}\lambda_{i_{\mathsf{r}},\mathsf{r}})y\right)dy \\
&= \left[\prod_{i_{\mathsf{r}}}^{I_{\mathrm{R}}}(m_{i_{\mathsf{r}}}\lambda_{i_{\mathsf{r}},\mathsf{r}})^{m_{i_{\mathsf{r}}}}\right]\sum_{k=0}^{K}\frac{(-1)^k}{k!}\sum_{n_1,\ldots,n_k}^{K}\sum_{q=0}^{\sum_{t=1}^{k}m_t-1}\sum_{i_{\mathsf{r}}}^{I_{\mathrm{R}}}\sum_{j=1}^{m_{i_{\mathsf{r}}}}\frac{\Xi_q\gamma^q\beta_{i_{\mathsf{r}}}^{j-1}}{(m_{i_{\mathsf{r}}}-j)!(j-1)!} \\
&\quad\times\exp(-\lambda_{\mathrm{tot}}\gamma)\Gamma(m_{i_{\mathsf{r}}})\Phi(m_{i_{\mathsf{r}}},m_{i_{\mathsf{r}}}+q+1;\lambda_{\mathrm{tot}}\gamma+m_{i_{\mathsf{r}}}\lambda_{i_{\mathsf{r}},\mathsf{r}}),
\end{aligned} \tag{5.14}$$

where $\Xi_q=\sum_{|s_t|=q}\frac{(m_t\lambda_{t,\mathsf{r}})^{p_t}}{p_t!}$, and $\lambda_{\mathrm{tot}}=\sum_{t=1}^{k}m_t\lambda_{t,\mathsf{r}}$.

Upon substituting (5.14) and (4.17) in (5.11) and after some simplifications, we get

$$\begin{aligned}
F_{\gamma_{\mathsf{D}}}(\gamma) &= \left[\prod_{i_{\mathsf{r}}}^{I_{\mathrm{R}}}(m_{i_{\mathsf{r}}}\lambda_{i_{\mathsf{r}},\mathsf{r}})^{m_{i_{\mathsf{r}}}}\right]\sum_{k=0}^{K}\frac{(-1)^k}{k!}\sum_{n_1,\ldots,n_k}^{K}\sum_{q=0}^{\sum_{t=1}^{k}m_t-1}\sum_{i_{\mathsf{r}}}^{I_{\mathrm{R}}}\sum_{j=1}^{m_{i_{\mathsf{r}}}}\frac{\Xi_q\gamma^q\beta_{i_{\mathsf{r}}}^{j-1}}{(m_{i_{\mathsf{r}}}-j)!(j-1)!} \\
&\times\exp(-\lambda_{\mathrm{tot}}\gamma)\Gamma(m_{i_{\mathsf{r}}}-j+1)\Phi(m_{i_{\mathsf{r}}}-j+1,m_{i_{\mathsf{r}}}+q-j+2;\lambda_{\mathrm{tot}}\gamma+m_{i_{\mathsf{r}}}\lambda_{i_{\mathsf{r}},\mathsf{r}}) \\
&\times\left\{1-A\mathrm{G}_{r+1,3r+1}^{3r,1}\left[\frac{B}{\bar{\gamma}_{\mathsf{r,d}}}\gamma\middle|\begin{matrix}1,\chi_1\\ \chi_2,0\end{matrix}\right]\right\}+A\mathrm{G}_{r+1,3r+1}^{3r,1}\left[\frac{B}{\bar{\gamma}_{\mathsf{r,d}}}\gamma\middle|\begin{matrix}1,\chi_1\\ \chi_2,0\end{matrix}\right].
\end{aligned} \tag{5.15}$$

Finally, we obtain the system outage probability by replacing γ by γ_{out} in (5.15).

5.4.2 Asymptotic Outage Probability

To get more insights about the considered system performance to determine the key parameters which affect the system performance, a simpler asymptotic expressions for the outage probability are derived and analyzed.

At high SNR values, the outage probability can be expressed as $P_{\mathsf{out}} \simeq (G_{\mathsf{c}}\mathrm{SNR})^{-G_{\mathsf{d}}}$, where G_{c} denotes the coding gain of the system and G_{d} is the diversity order of the system [111].

Hence, the CDF expression of the k-th user in (5.8) can be simplified to be

$$F^{\infty}_{\gamma_{k,\mathsf{r}}}(x) = \frac{(m_k \lambda_{k,\mathsf{r}} x)^{m_k}}{m_k!} \tag{5.16}$$

Substituting (5.16) in (5.12) yields to

$$\begin{aligned} F^{\infty}_{\gamma_{\mathrm{Sel},\mathsf{r}}}(\gamma) = {} & \left[\prod_{i_{\mathsf{r}}}^{I_{\mathrm{R}}} (m_{i_{\mathsf{r}}} \lambda_{i_{\mathsf{r}},\mathsf{r}})^{m_{i_{\mathsf{r}}}}\right] \left[\prod_{k=1}^{K} \frac{(m_k \lambda_{k,\mathsf{r}})^{m_k}}{m_k!}\right] \gamma^{\sum_{k=1}^{K} m_k} \sum_{i_{\mathsf{r}}}^{I_{\mathrm{R}}} \sum_{j=1}^{m_{i_{\mathsf{r}}}} \frac{\beta_{i_{\mathsf{r}}}^{j-1}}{(m_{i_{\mathsf{r}}} - j)!(j-1)!} \\ & \times \Gamma(m_{i_{\mathsf{r}}} - j + 1)\ \Phi\!\left(m_{i_{\mathsf{r}}} - j + 1, m_{i_{\mathsf{r}}} + \sum_{k=1}^{K} m_k - j + 2; \lambda_{\mathrm{tot}}\gamma + m_{i_{\mathsf{r}}} \lambda_{i_{\mathsf{r}},\mathsf{r}}\right). \end{aligned} \tag{5.17}$$

For further simplification, the users could be assumed to have identical channels $(\lambda_{1,\mathsf{r}} = \lambda_{2,\mathsf{r}} = \cdots = \lambda_{K,\mathsf{r}} = \lambda_{u,\mathsf{r}})$ and $(m_1 = m_2 = \cdots = m_K = m_u)$. For the identical case, the CDF in (5.17) simplifies to

$$F^{\infty}_{\gamma_{\mathrm{Sel,r}}}(\gamma) = \left[\prod_{i_{\mathsf{r}}}^{I_{\mathrm{R}}} (m_{i_{\mathsf{r}}} \lambda_{i_{\mathsf{r}},\mathsf{r}})^{m_{i_{\mathsf{r}}}}\right] \left(\frac{(m_u \lambda_{u,\mathsf{r}})^{m_u}}{m_u!}\right)^{K} \gamma^{m_u K} \sum_{i_{\mathsf{r}}}^{I_{\mathrm{R}}} \sum_{j=1}^{m_{i_{\mathsf{r}}}} \frac{\beta_{i_{\mathsf{r}}}^{j-1}}{(m_{i_{\mathsf{r}}} - j)!(j-1)!}$$

$$\times \Gamma(m_{i_{\mathsf{r}}} - j + 1)\ \Phi(m_{i_{\mathsf{r}}} - j + 1, m_{i_{\mathsf{r}}} + m_u K - j + 2; \lambda_{\mathrm{tot}} \gamma + m_{i_{\mathsf{r}}} \lambda_{i_{\mathsf{r}},\mathsf{r}}) . \tag{5.18}$$

On the other hand, the FSO link may have two different cases based on the atmospheric turbulence conditions as follows:

Case 1: Weak Turbulence

Herein, the FSO link is assumed to suffer from a weak turbulence conditions which are represented by large values of α and β in (4.17). Then, as $\bar{\gamma}_{\mathsf{r,d}} \to \infty$, the CDF of the second hop (FSO link) SNR $F_{\tilde{\gamma}_{\mathsf{r,d}}}(\gamma)$ can be simplified to [109, Eq. (9.303)]

$$F^{\infty}_{\tilde{\gamma}_{\mathsf{r,d}}}(\gamma) \simeq \frac{AB\gamma}{\bar{\gamma}_{\mathsf{r,d}}}. \tag{5.19}$$

For high SNR values, the CDF in (5.11) can be simplified to be

$$F^{\infty}_{\gamma_{\mathsf{D}}}(\gamma) \simeq F^{\infty}_{\gamma_{\mathrm{Sel,r}}}(\gamma) + F^{\infty}_{\tilde{\gamma}_{\mathsf{r,d}}}(\gamma), \tag{5.20}$$

Upon substituting (5.17) and (5.19) in (5.20), we get

$$F_{\gamma_{\mathsf{D}}}^{\infty}(\gamma) \simeq \left[\prod_{i_{\mathsf{r}}}^{I_{\mathrm{R}}} (m_{i_{\mathsf{r}}}\lambda_{i_{\mathsf{r}},\mathsf{r}})^{m_{i_{\mathsf{r}}}}\right] \left[\prod_{k=1}^{K} \frac{(m_k \lambda_{k,\mathsf{r}})^{m_k}}{m_k!}\right] \gamma^{\sum_{k=1}^{K} m_k} \sum_{i_{\mathsf{r}}}^{I_{\mathrm{R}}} \sum_{j=1}^{m_{i_{\mathsf{r}}}} \frac{\beta_{i_{\mathsf{r}}}^{j-1}}{(m_{i_{\mathsf{r}}}-j)!(j-1)!}$$
$$\times\, \Gamma(m_{i_{\mathsf{r}}}-j+1)\ \Phi\Bigg(m_{i_{\mathsf{r}}}-j+1, m_{i_{\mathsf{r}}}+\sum_{k=1}^{K} m_k - j + 2; \lambda_{\mathrm{tot}}\gamma + m_{i_{\mathsf{r}}}\lambda_{i_{\mathsf{r}},\mathsf{r}}\Bigg) + \frac{AB\gamma}{\bar{\gamma}_{\mathsf{r},\mathsf{d}}}. \tag{5.21}$$

For the case of identical users, the resultant asymptotic expression in (5.21) can be further simplified to

$$F_{\gamma_{\mathsf{D}}}^{\infty}(\gamma) \simeq \left[\prod_{i_{\mathsf{r}}}^{I_{\mathrm{R}}} (m_{i_{\mathsf{r}}}\lambda_{i_{\mathsf{r}},\mathsf{r}})^{m_{i_{\mathsf{r}}}}\right] \left(\frac{(m_u \lambda_{u,\mathsf{r}})^{m_u}}{m_u!}\right)^{K} \gamma^{m_u K} \sum_{i_{\mathsf{r}}}^{I_{\mathrm{R}}} \sum_{j=1}^{m_{i_{\mathsf{r}}}} \frac{\beta_{i_{\mathsf{r}}}^{j-1}}{(m_{i_{\mathsf{r}}}-j)!(j-1)!}$$
$$\times\, \Gamma(m_{i_{\mathsf{r}}}-j+1)\ \Phi(m_{i_{\mathsf{r}}}-j+1, m_{i_{\mathsf{r}}}+m_u K - j + 2; \lambda_{\mathrm{tot}}\gamma + m_{i_{\mathsf{r}}}\lambda_{i_{\mathsf{r}},\mathsf{r}}) + \frac{AB\gamma}{\bar{\gamma}_{\mathsf{r},\mathsf{d}}}. \tag{5.22}$$

Hence, the asymptotic probability of outage can be obtained from (5.21) or (5.22) by replacing γ by γ_{out}. It can be seen from (5.21) that the outage performance of the considered system might be dominated by either the RF link or the FSO link based on key system parameters such as numer of users K, Nakagami-m parameter m_k, number of RF CCI signals I_{R},atmospheric turbulence conditions α and β resulting in having two main cases of dominant term; namely, RF dominant and FSO dominant. In the case of RF dominant (i.e., $F_{\gamma_{\mathrm{Sel},\mathsf{r}}}^{\infty}(\gamma) >> F_{\widetilde{\gamma}_{\mathsf{r},\mathsf{d}}}^{\infty}(\gamma)$), the considered system can achieve a diversity order of $m_u K$ in the case of identical users and a coding gain which depends on Nakagami-m fading parameter, number of CCI signals, interferers powers and γ_{out}. However, the case of RF dominant is sensitive to the RF diversity order. Therefore, increasing the number of users K and the Nakagami-m parameter m_k might change the dominant link from the RF link to the FSO link. In this case (i.e., the FSO dominant) where $F^{\infty}_{\tilde{\gamma}_{\mathsf{r,d}}}(\gamma) >> F^{\infty}_{\gamma_{\mathrm{Sel},\mathsf{r}}}(\gamma)$, the considered system performance becomes a function of the FSO link parameters which depends on the laser transmission power, receiver detector type and the noise level at the destination.

Herein, the FSO link is assumed to suffer from a strong atmospheric turbulence conditions which are represented by small values of α and β in (4.17). From [112, Eq. (07.34.06.0006.01)], if $z \to \infty$, the Meijer G-function has the following series representation

$$\mathrm{G}^{m,n}_{p,q}\left[z\middle|\begin{matrix}a_1,\ldots,a_p\\ b_1,\ldots,b_q\end{matrix}\right] = \sum_{k=1}^{m} \frac{\prod_{j=1,j\neq k}^{m}\Gamma(b_j-b_k)\prod_{j=1}^{n}\Gamma(1-a_j+b_k)}{\prod_{j=n+1}^{p}\Gamma(a_j-b_k)\prod_{j=m+1}^{q}\Gamma(1-b_j+b_k)} z^{b_k}(1+o(z)), \tag{5.23}$$

where $p \leq q$ is required. Here, we use the same approach that was used in [113] in writing the outage probability for this case. Defining $\nu = \min\{\zeta^2, \alpha, \beta\}$ and $\bar{\gamma}_{\mathsf{r,d}} \to \infty$, $F_{\tilde{\gamma}_{\mathsf{r,d}}}(\gamma)$ can be simplified to

$$F^{\infty}_{\tilde{\gamma}_{\mathsf{r,d}}}(\gamma) \simeq \Lambda \left(\frac{\gamma}{\bar{\gamma}_{\mathsf{r,d}}}\right)^{\frac{\nu}{r}}, \tag{5.24}$$

where Λ is constant. Hence, the asymptotic CDF of the considered system is given by

$$F^{\infty}_{\gamma_{\mathsf{D}}}(\gamma) \simeq \left[\prod_{i_{\mathsf{r}}}^{I_{\mathrm{R}}} (m_{i_{\mathsf{r}}}\lambda_{i_{\mathsf{r}},\mathsf{r}})^{m_{i_{\mathsf{r}}}}\right] \left[\prod_{k=1}^{K} \frac{(m_k\lambda_{k,\mathsf{r}})^{m_k}}{m_k!}\right] \gamma^{\sum_{k=1}^{K} m_k} \sum_{i_{\mathsf{r}}}^{I_{\mathrm{R}}} \sum_{j=1}^{m_{i_{\mathsf{r}}}} \frac{\beta_{i_{\mathsf{r}}}^{j-1}\Gamma(m_{i_{\mathsf{r}}}-j+1)}{(m_{i_{\mathsf{r}}}-j)!(j-1)!}$$
$$\times\ \Phi\left(m_{i_{\mathsf{r}}}-j+1, m_{i_{\mathsf{r}}}+\sum_{k=1}^{K} m_k - j+2; \lambda_{\mathrm{tot}}\gamma + m_{i_{\mathsf{r}}}\lambda_{i_{\mathsf{r}},\mathsf{r}}\right) + \Lambda\left(\frac{\gamma}{\bar{\gamma}_{\mathsf{r},\mathsf{d}}}\right)^{\frac{\nu}{r}}. \quad (5.25)$$

For the case of identical users, the resultant asymptotic expression in (5.25) can be further simplified to

$$F^{\infty}_{\gamma_{\mathsf{D}}}(\gamma) \simeq \left[\prod_{i_{\mathsf{r}}}^{I_{\mathrm{R}}} (m_{i_{\mathsf{r}}}\lambda_{i_{\mathsf{r}},\mathsf{r}})^{m_{i_{\mathsf{r}}}}\right] \left(\frac{(m_u\lambda_{u,\mathsf{r}})^{m_u}}{m_u!}\right)^{K} \gamma^{m_u K} \sum_{i_{\mathsf{r}}}^{I_{\mathrm{R}}} \sum_{j=1}^{m_{i_{\mathsf{r}}}} \frac{\beta_{i_{\mathsf{r}}}^{j-1}\Gamma(m_{i_{\mathsf{r}}}-j+1)}{(m_{i_{\mathsf{r}}}-j)!(j-1)!}$$
$$\times\ \Phi(m_{i_{\mathsf{r}}}-j+1, m_{i_{\mathsf{r}}}+m_u K - j+2; \lambda_{\mathrm{tot}}\gamma + m_{i_{\mathsf{r}}}\lambda_{i_{\mathsf{r}},\mathsf{r}}) + \Lambda\left(\frac{\gamma}{\bar{\gamma}_{\mathsf{r},\mathsf{d}}}\right)^{\frac{\nu}{r}}. \quad (5.26)$$

Then, the asymptotic probability of outage can be obtained from (5.25) or (5.26) by replacing γ by γ_{out}. From (5.25), it can be notice that the diversity order in the case of strong turbulence equals to $\min\{\nu/r, m_u N_{\mathsf{r}} K\}$. This result shows how diversity order depends on the worst link between the RF and FSO links. For large values of RF link parameters (i.e., m_u and K), and under sever turbulence conditions and pointing errors, the FSO link will dominate the system performance. This remark will be used in obtaining the optimal RF transmission power needed under strong turbulence conditions in Section. 5.4.3.

5.4.3 Power Allocation

In this section, a new power allocation solution is proposed for the RF transmission power of the K users (i.e., P_k) in the presence of CCI. As we remarked in Section 5.4.2, the performance of the FSO link could be limited due to the atmospheric (weak or strong) turbulence and the limited FSO transmission power (the power of the laser beam) due to safety regulation and eye protection. As a result, the FSO link performance might become the worse link and dominate the considered system performance. Therefore, in the case of FSO dominant, the considered system does not attain the benefits of both diversity and coding gains provided by the multiuser RF link. Whereas, in the case of RF dominant, the considered system might be able to fully utilize the diversity and coding gain improvements.

Based on previously discussion, in the case of FSO dominant, it would be inefficient and waste of power resources if the selected best user $\mathrm{U}_{\mathrm{Sel}}$ is allowed to transmit with its maximum transmission power P_{T} as there is no additional improvements are gained in the considered system overall performance. Whereas, in the case of RF dominant, the overall system performance will attain its maximum diversity order and coding gain if the selected best user $\mathrm{U}_{\mathrm{Sel}}$ transmits with its maximum transmission power P_{T}. Hence, based on the dominant link, the optimal RF transmission power of the selected best user P_k^{opt} is given by

$$P_k^{\mathsf{opt}} = \min\left(P_{\mathsf{T}}, P_{\mathsf{req}}\right), \tag{5.27}$$

where P_{req} is the minimum required RF transmission power which guarantees that the FSO link is still the dominant term in the total system outage probability. Under the two cases of atmospheric turbulence conditions of the FSO link, we have the following:

Case 1: Weak Turbulence

In this case, the dominant term alternates between the RF and FSO links based on the main system parameters including K, m_k, I_{R}, α and β. In order to overcome this problem and from our observations, we consider that the dominant outage term is greater than or equal to 100 times the other term. For example, the FSO outage term is the dominant term when $F_{\widetilde{\gamma}_{\mathsf{r,d}}}(\gamma) \geq 100 \times F_{\gamma_{\mathrm{Sel},\mathsf{r}}}(\gamma)$, and vice versa.

For simplicity and without loss of generality, the asymptotic outage probability expressions derived in Section 5.4.2 are used to obtain mathematically tractable solutions. For weak turbulence case with FSO dominant term, the optimal transmission power is given by

$$\begin{aligned} &\min \;\; P_{\mathsf{req}} \\ &\text{Subject to: } F^{\infty}_{\gamma_{\mathrm{Sel},\mathsf{r}}}(\gamma) \approx 0.01 F^{\infty}_{\widetilde{\gamma}_{\mathsf{r,d}}}(\gamma). \end{aligned} \tag{5.28}$$

Under the assumption of identical users channels with equal transmission powers, the optimal value is given by

$$\begin{aligned} P_{\mathsf{req}} = \frac{m_u \gamma}{\Omega_{u,\mathsf{r}} (m_u!)^{\frac{1}{m_u}}} & \Bigg[\Bigg(\prod_{i_{\mathsf{r}}}^{I_{\mathrm{R}}} (m_{i_{\mathsf{r}}} \lambda_{i_{\mathsf{r}},\mathsf{r}})^{m_{i_{\mathsf{r}}}} \Bigg) \sum_{i_{\mathsf{r}}}^{I_{\mathrm{R}}} \sum_{j=1}^{m_{i_{\mathsf{r}}}} \frac{\beta_{i_{\mathsf{r}}}^{j-1} \Gamma(m_{i_{\mathsf{r}}} - j + 1)}{(m_{i_{\mathsf{r}}} - j)!(j-1)!} \\ \times \;\; & \Phi(m_{i_{\mathsf{r}}} - j + 1, m_{i_{\mathsf{r}}} + m_u K - j + 2; \lambda_{\mathrm{tot}} \gamma + m_{i_{\mathsf{r}}} \lambda_{i_{\mathsf{r}},\mathsf{r}}) \, \frac{100 \bar{\gamma}_{\mathsf{r,d}}}{A B \gamma} \Bigg]^{\frac{1}{K m_u}}. \end{aligned} \tag{5.29}$$

While for the weak turbulence with RF dominant case, the selected best user will transmit with maximum transmission power P_{T}.

Case 2: Strong Turbulence

Similarly, under the assumption of identical users channels with equal transmission powers, the optimal value is given by

$$\begin{aligned} P_{\mathsf{req}} = \frac{m_u\gamma}{\Omega_{u,\mathsf{r}}(m_u!)^{\frac{1}{m_u}}} & \Bigg[\Bigg(\prod_{i_{\mathsf{r}}}^{I_{\mathrm{R}}}(m_{i_{\mathsf{r}}}\lambda_{i_{\mathsf{r}},\mathsf{r}})^{m_{i_{\mathsf{r}}}}\Bigg)\sum_{i_{\mathsf{r}}}^{I_{\mathrm{R}}}\sum_{j=1}^{m_{i_{\mathsf{r}}}}\frac{\beta_{i_{\mathsf{r}}}^{j-1}}{(m_{i_{\mathsf{r}}}-j)!(j-1)!}\Gamma(m_{i_{\mathsf{r}}}-j+1) \\ & \times\ \Phi(m_{i_{\mathsf{r}}}-j+1, m_{i_{\mathsf{r}}}+m_uK-j+2; \lambda_{\mathrm{tot}}\gamma+m_{i_{\mathsf{r}}}\lambda_{i_{\mathsf{r}},\mathsf{r}})\,\Lambda^{-1}\left(\frac{\gamma}{100\bar{\gamma}_{\mathsf{r,d}}}\right)^{\frac{-\nu}{r}}\Bigg]^{\frac{1}{Km_u}}. \end{aligned} \tag{5.30}$$

5.5 Physical Layer Security Approach

In this section, the PHY security analysis of the considered MU mixed RF/FSO system is studied in the presence of CCI and under an eavesdropper attack. Since the FSO link has the advantage of high security level, the work is concentrating on studying the impact of CCI on the secrecy performance of the RF link. This section is divided into two parts, the first part introduces the RF link security analysis in the presence of CCI, and the second part proposes a new CJ model based on the worst user selection.

5.5.1 Security Analysis

5.5.1.1 System Intercept Probability

In this part, the secrecy performance of the considered system is investigated in the presence of a single passive eavesdropper (E) which is located randomly between the K users and the relay node R. Since the eavesdropper is passive, its wiretap channel CSI is unavailable at the legitimate K users and relay. The passive eavesdropper is assumed to suffer from I_{E} i.ni.d. CCI signals. Hence, in the RF phase, the k-th user received signal at E is given by

$$y_{k,\mathsf{e}} = \sqrt{P_k} h_{k,i,\mathsf{e}} x_k + \sum_{i_{\mathsf{e}}=1}^{I_{\mathrm{E}}} \sqrt{P_{i_{\mathsf{e}}}} c_{i_{\mathsf{e}},\mathsf{e}} x_{i_{\mathsf{e}}} + w_{\mathsf{e}}, \tag{5.31}$$

where $h_{k,\mathsf{e}}$ is the wiretap channel coefficient between the k-th user (U_k) and the eavesdropper E, x_k is the transmitted symbol from U_k with $\mathbb{E}\{|x_k|^2\} = P_k$, $c_{i_{\mathsf{e}},\mathsf{e}}$ is the RF link channel coefficient between the i_{e}-th interferer and E, $x_{i_{\mathsf{e}}}$ denotes the i_{e}-th interference symbol $\mathbb{E}\{|x_{i_{\mathsf{e}}}|^2\} = 1$ and transmitted power $P_{i_{\mathsf{e}}}$, $w_{\mathsf{e}} \sim \mathcal{CN}(0, N_0)$ is an AWGN sample at E. Using (5.31), the SNR of the k-th user observed at E can be expressed as

$$\gamma_{k,\mathsf{e}} = \frac{P_k |h_{k,\mathsf{e}}|^2}{\sum_{i_{\mathsf{e}}=1}^{I_{\mathrm{E}}} P_{i_{\mathsf{e}}} |c_{i_{\mathsf{e}},\mathsf{e}}|^2 + N_0}. \tag{5.32}$$

According to Shannon's theorem, the capacity of wiretap channel (i.e., $\mathrm{U}_k - \mathrm{E}$ link) is given by

$$C_{k,\mathsf{e}} = \log_2\left(1 + \frac{P_k|h_{k,\mathsf{e}}|^2}{\sum_{i_{\mathsf{e}}=1}^{I_{\mathrm{E}}} P_{i_{\mathsf{e}}}|c_{i_{\mathsf{e}},\mathsf{e}}|^2 + N_0}\right). \tag{5.33}$$

Hence, the intercept probability represents the probability that the wiretap channel capacity is higher than $\mathcal{R}$, such as

$$\begin{aligned}
P_{\mathrm{int}}^{(k)} &= \Pr(C_{k,\mathsf{e}} > \mathcal{R}) \\
&= \Pr\left[\log_2\left(1 + \frac{P_k|h_{k,\mathsf{e}}|^2}{\sum_{i_{\mathsf{e}}=1}^{I_{\mathrm{E}}} P_{i_{\mathsf{e}}}|c_{i_{\mathsf{e}},\mathsf{e}}|^2 + N_0}\right) > \mathcal{R}\right] \\
&= \Pr\left[\frac{P_k|h_{k,\mathsf{e}}|^2}{\sum_{i_{\mathsf{e}}=1}^{I_{\mathrm{E}}} P_{i_{\mathsf{e}}}|c_{i_{\mathsf{e}},\mathsf{e}}|^2 + N_0} > \delta\right] \\
&= \sum_{p=0}^{m_k-1} \frac{(m_k\lambda_{k,\mathsf{r}}\delta)^p}{p!} \left[\prod_{i_{\mathsf{e}}=1}^{I_{\mathrm{E}}} (m_{i_{\mathsf{e}}}\lambda_{i_{\mathsf{e}},\mathsf{e}})^{m_{i_{\mathsf{e}}}}\right] \sum_{i_{\mathsf{e}}=1}^{I_{\mathrm{E}}} \sum_{j=1}^{m_{i_{\mathsf{e}}}} \frac{(m_{i_{\mathsf{e}}}-1)!\beta_{i_{\mathsf{e}}}^{j-1}}{(m_{i_{\mathsf{e}}}-j)!(j-1)!} \exp(-m_k\lambda_{k,\mathsf{e}}\delta) \\
&\quad \times \Gamma(m_{i_{\mathsf{e}}}-j+1)\Phi(m_{i_{\mathsf{e}}}-j+1, m_{i_{\mathsf{e}}}+p-j+2; m_{i_{\mathsf{e}}\lambda_{i_{\mathsf{e}},\mathsf{e}}} + m_k\lambda_{k,\mathsf{e}}\delta)
\end{aligned} \tag{5.34}$$

where δ is a predetermined outage threshold defined by $2^{\mathcal{R}}-1$. The previously derived expression can be simplified at high SINR values to an asymptotic intercept probability expression which is a less sophisticated formula given by

$$\begin{aligned}
P_{\mathrm{int}}^{\infty,(k)} &= 1 - \frac{(m_k\lambda_{k,\mathsf{r}}\delta)^{m_k}}{m_k!} \left[\prod_{i_{\mathsf{e}}=1}^{I_{\mathrm{E}}} (m_{i_{\mathsf{e}}}\lambda_{i_{\mathsf{e}},\mathsf{e}})^{m_{i_{\mathsf{e}}}}\right] \sum_{i_{\mathsf{e}}=1}^{I_{\mathrm{E}}} \sum_{j=1}^{m_{i_{\mathsf{e}}}} \frac{(m_{i_{\mathsf{e}}}-1)!\beta_{i_{\mathsf{e}}}^{j-1}}{(m_{i_{\mathsf{e}}}-j)!(j-1)!} \\
&\quad \times \Gamma(m_{i_{\mathsf{e}}}-j+1)\Phi(m_{i_{\mathsf{e}}}-j+1, m_{i_{\mathsf{e}}}+m_k-j+2; m_{i_{\mathsf{e}}}\lambda_{i_{\mathsf{e}},\mathsf{e}})
\end{aligned} \tag{5.35}$$

After best user selection, the wiretap channel would be the channel between the selected best user $\mathrm{U}_{\mathrm{Sel}}$ and the eavesdropper E. Hence, the wiretap channel capacity for the selected best user is given by

$$\begin{aligned}
P_{\mathrm{int}}^{\mathrm{Sel}} &= \Pr\left[\log_2\left(1+\frac{P_{\mathrm{Sel}}|h_{\mathrm{Sel},\mathsf{e}}|^2}{\sum_{i_{\mathsf{e}}=1}^{I_{\mathrm{E}}} P_{i_{\mathsf{e}}}|c_{i_{\mathsf{e}},\mathsf{e}}|^2+N_0}\right) > \mathcal{R}\right] \\
&= \Pr\left[\frac{P_{\mathrm{Sel}}|h_{\mathrm{Sel},\mathsf{e}}|^2}{\sum_{i_{\mathsf{e}}=1}^{I_{\mathrm{E}}} P_{i_{\mathsf{e}}}|c_{i_{\mathsf{e}},\mathsf{e}}|^2+N_0} > \delta\right] \\
&= \sum_{k=1}^{K} \Pr\left(\mathrm{U}_k = \mathrm{U}_{\mathrm{Sel}}\right) \Pr\left[\frac{P_k|h_{k,\mathsf{e}}|^2}{\sum_{i_{\mathsf{e}}=1}^{I_{\mathrm{E}}} P_{i_{\mathsf{e}}}|c_{i_{\mathsf{e}},\mathsf{e}}|^2+N_0} > \delta\right],
\end{aligned} \tag{5.36}$$

where $h_{\mathrm{Sel},\mathsf{e}}$ denotes the wiretap channel coefficient between the selected best user ($\mathrm{U}_{\mathrm{Sel}}$) and E, and P_{Sel} is the transmission power of the selected best user. The term $\Pr\left(\mathrm{U}_k = \mathrm{U}_{\mathrm{Sel}}\right)$ denotes the event that the k-th user is the selected user $\mathrm{U}_{\mathrm{Sel}}$ by the authorized relay R which is given by

$$\begin{aligned}
&\Pr\left(\mathrm{U}_k = \mathrm{U}_{\mathrm{Sel}}\right) = \Pr\left(\max_{j\in\{K-k\}} |h_{j,\mathsf{r}}|^2 < |h_{k,\mathsf{r}}|^2\right) = \int_0^\infty \prod_{j\in\{K-k\}} F_{\|\mathbf{h}_{j,\mathsf{r}}\|^2}(x) f_{\|\mathbf{h}_{k,\mathsf{r}}\|^2}(x)dx \\
&= \int_0^\infty \prod_{j\in\{K-k\}} \left[1-\sum_{p=0}^{m_j-1}\frac{(m_j x)^p}{p!}\exp(-m_j x)\right] \frac{(m_k\lambda_{k,\mathsf{r}})^{m_k}}{(m_k-1)!}\frac{\exp(-m_k\lambda_{k,\mathsf{r}}x)}{x^{1-m_k}}dx \\
&= \sum_{j=0}^{K-1}\frac{(-1)^j}{j!}\sum_{\substack{n_1,\ldots,n_K\\ n_j\neq n_k}}^{K-1}\sum_{q_j=0}^{\sum_{t_j=1}^{j} m_{t_j}-1} \Xi_{q_j}\frac{(m_k\lambda_{k,\mathsf{r}})^{m_k}}{(m_k-1)!}\int_0^\infty \frac{\exp\left(-(\lambda_{\mathrm{tot}_j}+m_k\lambda_{k,\mathsf{r}})x\right)}{x^{1-q_j-m_k}}dx \\
&= \sum_{j=0}^{K-1}\frac{(-1)^j}{j!}\sum_{\substack{n_1,\ldots,n_K\\ n_j\neq n_k}}^{K-1}\sum_{q_j=0}^{\sum_{t_j=1}^{j} m_{t_j}-1} \Xi_{q_j}\frac{(m_k\lambda_{k,\mathsf{r}})^{m_k}}{(m_k-1)!}(\lambda_{\mathrm{tot}_j}+m_k\lambda_{k,\mathsf{r}})^{-(q_j+m_k)}\Gamma(q_j+m_k)
\end{aligned} \tag{5.37}$$

Then, the intercept probability of the selected best user can be obtained by substituting (5.34) and (5.37) in (5.36).

5.5.1.2 Impact of RF Power Allocation on SRT Analysis

Based on the previous discussion in Section 5.4 and this section, it is obvious that increasing the selected user transmission power P_k increases the intercept probability and degrades the system secrecy performance and vice versa. On the other hand, decreasing P_k increases the system RF outage probability which degrades the system reliability performance. Therefore, it is clear that SRT analysis of the considered system depends on the value of P_k resulting in increasing the demands to find an optimal P_k value which maintains the system secrecy performance without harming the system outage performance. Hence, the presented power allocation formula in (5.27) might obtain the required optimal RF transmission power value. Since (5.27) depends on the dominant link between the two system links (i.e., RF and FSO link), we have the following two cases:

Case (1): FSO link is dominant

In this case, the FSO link dominates the system performance. As a result, increasing P_k will not enhance the system outage performance, and it would be more practical to apply the formula in (5.27) to obtain the reduced optimal value P_{req} which is less than the maximum transmission power P_{T}. Hence, the intercept probability of the considered system will be decreased without harming the system outage performance.

Case (2): RF link is dominant

In this case, the user has to transmit with its maximum power P_{T} as the RF link dominates the system outage performance. Although reducing the RF transmission power improves the secrecy performance, it also increases the system outage probability. Therefore, the present formula in (5.27) fails to obtain an optimal power value less than P_{T}. As a result, we propose a CJ model which enhances system secrecy performance in the next part.

5.5.2 Cooperative Jamming Model for Enhancing Physical Layer Security

5.5.2.1 System Intercept Probability

In this part, we employ CJ technique to enhance the system secrecy performance. To do that, a friendly jamming signal which is known to R is employed which can be canceled at R by subtraction [116]. Since the considered system selects the best user among all the K users, the rest $K-1$ users will be idle during the selected best user transmission. Therefore, the proposed CJ model selects the worst $\mathrm{U}_k - \mathrm{R}$ link among the remaining $K-1$ users to broadcast the prior known jamming signal at R to jam E. The worst relay is selected to reduce any interference caused by the jammer in the case of imperfect CSI. Hence, in the RF phase, the k-th user received signal at E is given by

$$y_{k,\mathsf{e}} = \sqrt{P_k} h_{k,\mathsf{e}} x_k + \sum_{i_{\mathsf{e}}=1}^{I_{\mathrm{E}}} \sqrt{P_{i_{\mathsf{e}}}} c_{i_{\mathsf{e}},\mathsf{e}} x_{i_{\mathsf{e}}} + \sum_{\mathrm{J}} \sqrt{\frac{P_{\mathrm{J}}}{\mathrm{J}}} h_{\mathrm{J},\mathsf{e}} x_{\mathrm{J}} + w_{\mathsf{e}}, \tag{5.38}$$

where $\mathrm{J} = 1$ denotes that the CJ would be the selected worst user by R, and $\mathrm{J} \in \{K-k\}$ denotes that the cooperative jammers would be all authorized users except the k-th user. $h_{\mathrm{J},\mathsf{e}}$ is the channel coefficients between the cooperative jammer (U_{J})

and E, x_{J} is the transmitted jamming signal from $\mathrm{U_J}$ with $\mathbb{E}\{|x_{\mathrm{J}}|^2\} = 1$, and P_{J} is the total available power for CJ which would be transmitted by a single jammer node or equally divided between the all $\{K-k\}$ CJ nodes. Using (5.38), the SINR of the k-th user observed at E can be expressed as

$$\gamma_{k,\mathsf{e}} = \frac{P_k|h_{k,\mathsf{e}}|^2}{\sum_{i_{\mathsf{e}}=1}^{I_{\mathrm{E}}} P_{i_{\mathsf{e}}}|c_{i_{\mathsf{e}},\mathsf{e}}|^2 + \sum_{\mathrm{J}} \frac{P_{\mathrm{J}}}{\mathrm{J}}|h_{\mathrm{J},\mathsf{e}}|^2 + N_0}. \tag{5.39}$$

Again, according to Shannon's theorem, the capacity of wiretap channel (i.e., $\mathrm{U}_k - \mathrm{E}$ link) is given by

$$C_{k,\mathsf{e}} = \log_2\left(1 + \frac{P_k|h_{k,\mathsf{e}}|^2}{\sum_{i_{\mathsf{e}}=1}^{I_{\mathrm{E}}} P_{i_{\mathsf{e}}}|c_{i_{\mathsf{e}},\mathsf{e}}|^2 + \sum_{\mathrm{J}} \frac{P_{\mathrm{J}}}{\mathrm{J}}|h_{\mathrm{J},\mathsf{e}}|^2 + N_0}\right). \tag{5.40}$$

Again, the intercept probability represents the probability that the wiretap channel capacity is higher than $\mathcal{R}$, such as

$$\begin{aligned}
P_{\text{int}}^{(k)} &= \Pr(C_{k,\mathsf{e}} > \mathcal{R}) \\
&= \Pr\left[\log_2\left(1 + \frac{P_k|h_{k,\mathsf{e}}|^2}{\sum_{i_{\mathsf{e}}=1}^{I_{\mathrm{E}}} P_{i_{\mathsf{e}}}|c_{i_{\mathsf{e}},\mathsf{e}}|^2 + \sum_{\mathrm{J}} \frac{P_{\mathrm{J}}}{\mathrm{J}}|h_{\mathrm{J},\mathsf{e}}|^2 + N_0}\right) > \mathcal{R}\right] \\
&= \Pr\left[\frac{P_k|h_{k,\mathsf{e}}|^2}{\sum_{i_{\mathsf{e}}=1}^{I_{\mathrm{E}}} P_{i_{\mathsf{e}}}|c_{i_{\mathsf{e}},\mathsf{e}}|^2 + \sum_{\mathrm{J}} \frac{P_{\mathrm{J}}}{\mathrm{J}}|h_{\mathrm{J},\mathsf{e}}|^2 + N_0} > \delta\right] \\
&= \sum_{p=0}^{m_k-1} \frac{(m_k\lambda_{k,\mathsf{r}}\delta)^p}{p!} \left[\prod_{n=1}^{N}(m_n\lambda_{n,\mathsf{e}})^{m_n}\right] \sum_{n=1}^{N}\sum_{j=1}^{m_n} \frac{(m_n-1)!\beta_n^{j-1}}{(m_n-j)!(j-1)!} \exp(-m_k\lambda_{k,\mathsf{e}}\delta) \\
&\quad \times \Gamma(m_n-j+1)\Phi(m_n-j+1, m_n+p-j+2; m_{n\lambda_{n,\mathsf{e}}} + m_k\lambda_{k,\mathsf{e}}\delta),
\end{aligned} \tag{5.41}$$

where $N = I_{\mathrm{E}} + \mathrm{J}$ represents the number of non-identical CCI signals at E plus the number of CJ signals J. Based on the applied CJ model N is given by

$$N = \begin{cases} I_{\mathrm{E}} + K - 1, & \text{for all participant (AP) CJ} \\ I_{\mathrm{E}} + 1, & \text{for a selected worst user CJ} \end{cases} . \tag{5.42}$$

Similarly, the asymptotic intercept probability expression for both CJ models is given by

$$P_{\mathrm{int}}^{\infty,(k)} = 1 - \frac{(m_k \lambda_{k,\mathsf{r}} \delta)^{m_k}}{m_k!} \left[\prod_{n=1}^{N} (m_n \lambda_{n,\mathsf{e}})^{m_n} \right] \sum_{n=1}^{I_{\mathrm{E}}} \sum_{j=1}^{m_n} \frac{(m_n - 1)! \beta_n^{j-1}}{(m_n - j)!(j-1)!}$$

$$\times \Gamma(m_n - j + 1) \Phi(m_n - j + 1, m_n + m_k - j + 2; m_n \lambda_{n,\mathsf{e}}). \tag{5.43}$$

Using CJ models, the eavesdropper E is suffering from extra jamming signals transmitted either by the selected worst user ($\mathrm{U_J}$) or all remaining $K - 1$ users (all participant CJ). Based on the two different CJ model, the wiretap channel capacity can be expressed as

$$P_{\mathrm{int}}^{\mathrm{Sel}} = \Pr \left[\frac{P_{\mathrm{Sel}} |h_{\mathrm{Sel},\mathsf{e}}|^2}{\sum_{i_{\mathsf{e}}=1}^{I_{\mathrm{E}}} P_{i_{\mathsf{e}}} |c_{i_{\mathsf{e}},\mathsf{e}}|^2 + \sum_{\mathrm{J}} \frac{P_{\mathrm{J}}}{\mathrm{J}} |h_{\mathrm{J},\mathsf{e}}|^2 + N_0} > \delta \right]$$

$$= \begin{cases} \sum\limits_{k=1}^{K} \Pr\left(\mathrm{U}_k = \mathrm{U_{Sel}}\right) \Pr\left(\frac{P_k \|\mathbf{h}_{k,\mathsf{e}}\|^2}{\sum_{i_{\mathsf{e}}=1}^{I_{\mathrm{E}}} P_{i_{\mathsf{e}}} |c_{i_{\mathsf{e}},\mathsf{e}}|^2 + \sum_{\mathrm{J}} \frac{P_{\mathrm{J}}}{\mathrm{J}} |h_{\mathrm{J},\mathsf{e}}|^2 + N_0} > \delta \right), & \mathrm{J} \in \{K - k\} \\ \sum\limits_{k=1}^{K} \Pr\left(\mathrm{U}_k = \mathrm{U_{Sel}}\right) & \\ \times \left[\sum\limits_{t \in \{K-k\}} \Pr\left(\mathrm{U}_t = \mathrm{U_J}\right) \Pr\left(\frac{P_k \|\mathbf{h}_{k,\mathsf{e}}\|^2}{\sum_{i_{\mathsf{e}}=1}^{I_{\mathrm{E}}} P_{i_{\mathsf{e}}} |c_{i_{\mathsf{e}},\mathsf{e}}|^2 + \sum_{\mathrm{J}} \frac{P_{\mathrm{J}}}{\mathrm{J}} |h_{\mathrm{J},\mathsf{e}}|^2 + N_0} > \delta \right) \right], & \mathrm{J} = 1 \end{cases} . \tag{5.44}$$

The results in (5.44) is similar to (5.36) with the new term $\Pr\left(\mathrm{U}_t = \mathrm{U}_\mathrm{J}\right)$ denotes the event that the t-th user is the selected worst user (i.e., jamming user U_J) by the authorized relay R which is given by

$$\begin{aligned}\Pr\left(\mathrm{U}_t = \mathrm{U}_\mathrm{J}\right) &= \Pr\left(\min_{q\in\{K-k-t\}} |h_{q,\mathrm{r}}|^2 > |h_{t,\mathrm{r}}|^2\right) \\ &= 1 - \int_0^\infty \prod_{q\in\{K-k-t\}} \left[1 - F_{|\mathbf{h}_{q,\mathrm{r}}|^2}(x)\right] f_{|\mathbf{h}_{t,\mathrm{r}}|^2}(x)dx. \qquad (5.45)\end{aligned}$$

5.5.2.2 Power Allocation for PHY Security Enhancement

In this part, a power allocation optimization problem is formulated to enhance the CJ model PHY security performance. The power allocation problem here aims to find the optimal transmission and jamming powers which achieve a certain outage probability performance ($P^{\mathrm{CJ}}_{\mathrm{out,Req.}}$) for the CJ PHY security model. For a fair comparison between the secrecy performance of the proposed CJ model and the secrecy performance of the considered MU mixed RF/FSO system without CJ, the total power for transmission and jamming is set to be equal to the maximum user transmission power P_T (i.e., $P_\mathsf{T} = P_{\mathrm{Req.}} + P_\mathrm{J}$).

Based on the above-mentioned discussion, the outage performance of the CJ model is similar to the performance of the normal RF/FSO model since the authorized destination is assumed to know the jamming signal. Hence, the outage probabilities of both models are identical. For simplicity, the asymptotic outage probability is used to obtain the optimal transmission powers. Again, since the outage probability of the considered system with CJ model depends on the dominant link between the two RF and FSO links, we have two different cases:

Case (1): FSO link is dominant

In this case, the optimal power allocation formula which is presented in Section. 5.4.2 is valid. The the transmission RF power is set to be P_{req} and the jamming power is given by $P_{\mathrm{J}} = P_{\mathsf{T}} - P_{\mathrm{req}}$. It is important to emphasize that the CJ model enhances the system secrecy performance in two ways. Firstly, the CJ model decreases the RF transmission power to P_{req} without harming the system outage probability. Secondly, the deducted power from the RF transmission is used as a jamming power P_{J} is used by the friendly jammer node (i.e., the selected worst user) to enhance the system secrecy performance.

Case (2): RF link is dominant

In this case, the RF link dominates the system outage performance. Hence, the user has to transmit with its maximum power P_{T}. Therefore, another power allocation problem is formulated to find the optimal power value P_k^* which set the RF/FSO system with CJ model outage probability to a certain required value ($P_{\mathrm{out,Req.}}^{\mathrm{CJ}}$). Then, the remaining power is allocated for CJ to enhance the system security. The optimization problem can be formulated such as

$$\begin{aligned} &\text{Minimize } \; P_k \\ &\text{subject to: } P_{\mathrm{out}}^{\infty,\mathrm{CJ}} = P_{\mathrm{out,Req.}}^{\infty,\mathrm{CJ}} > P_{\mathrm{out,Min.}}^{\infty,\mathrm{CJ}}, \\ &\qquad P_k + P_{\mathrm{J}} = P_{\mathsf{T}}, \end{aligned} \tag{5.46}$$

where $P_{\mathrm{out,Req.}}^{\infty,\mathrm{CJ}}$ is a predetermined required asymptotic RF outage probability which cannot exceed the minimum outage probability $P_{\text{out,Min.}}^{\infty,\text{CJ}}$ achieved by the system when the total power P_{T} is used for transmission only. Under the assumption of identical users channels with equal transmission powers, the optimal value is given by

$$P_k^* = \frac{m_u \gamma}{\Omega_{u,\text{r}}(m_u!)^{\frac{1}{m_u}}} \left[\left(\prod_{i_{\text{r}}}^{I_{\text{R}}} (m_{i_{\text{r}}} \lambda_{i_{\text{r}},\text{r}})^{m_{i_{\text{r}}}} \right) \sum_{i_{\text{r}}}^{I_{\text{R}}} \sum_{j=1}^{m_{i_{\text{r}}}} \frac{\beta_{i_{\text{r}}}^{j-1}}{(m_{i_{\text{r}}} - j)!(j-1)!} \Gamma(m_{i_{\text{r}}} - j + 1) \right.$$
$$\left. \times \ \Phi(m_{i_{\text{r}}} - j + 1, m_{i_{\text{r}}} + m_u K - j + 2; \lambda_{\text{tot}} \gamma + m_{i_{\text{r}}} \lambda_{i_{\text{r}},\text{r}}) \frac{1}{P_{\text{out,Req.}}^{\infty,\text{CJ}}} \right]^{\frac{1}{K m_u}}. \tag{5.47}$$

Hence, the jamming power is given by

$$P_{\text{J}} = P_{\mathsf{T}} - P_k^*. \tag{5.48}$$

5.6 Simulation and Numerical Results

In this section, numerical results obtained by using the above-derived expressions are presented together with Monte-Carlo simulations. The effects of some key system parameters on the overall system performance are investigated such as number of users K, atmospheric channel conditions, interference power, number of interference signals, power optimization and CJ. In all simulations unless mentioned otherwise, we assume the interference power P_{I} is scaling with SNR and the number of interfering signals at both relay and eavesdropper equals 3. The

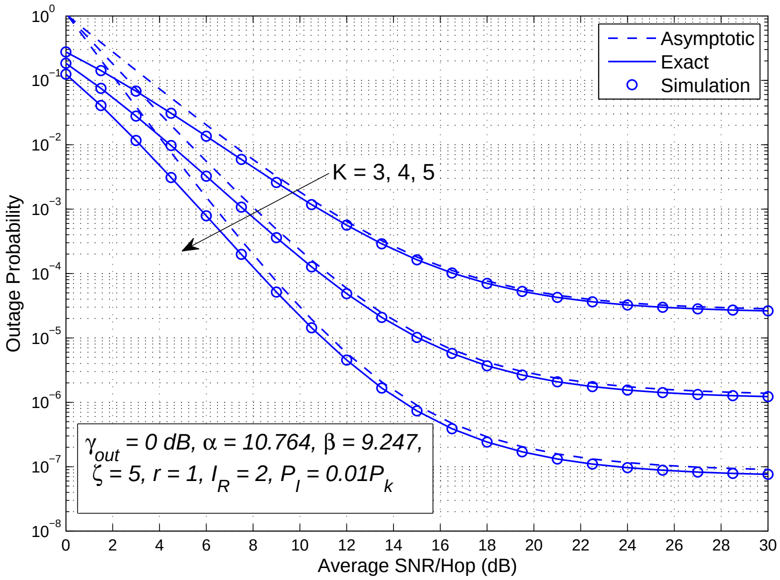


Figure 5.2: Outage probability versus SNR of the considered system with opportunistic scheduling and different number of users K at weak atmospheric turbulence conditions $\alpha = 10.764, \beta = 9.247$.

channel gains between the K users and the relay are randomized with means $\Omega_{k,\mathrm{r}} = 10$ dB. Similarly, the channel gains between the K users and the eavesdropper E are randomized with means $\Omega_{k,\mathrm{e}} = 7$ dB. Moreover, the CCI links at all authorized/unauthorized nodes are randomized with a mean value of 3 dB.

The outage performance of the considered system for different number of users K is investigated in Figure 5.2. It is clear that increasing K increases the system diversity gain and enhances the system outage performance. The effect of CCI signals on the system outage performance can be notice clearly at high SNR values where increasing the SNR value does not enhance the system outage performance. Results show that the exact analytical expression matches both asymptotic and simulations results which validate the derived closed-form expressions. It is important to clarify that under weak turbulence the outage performance of

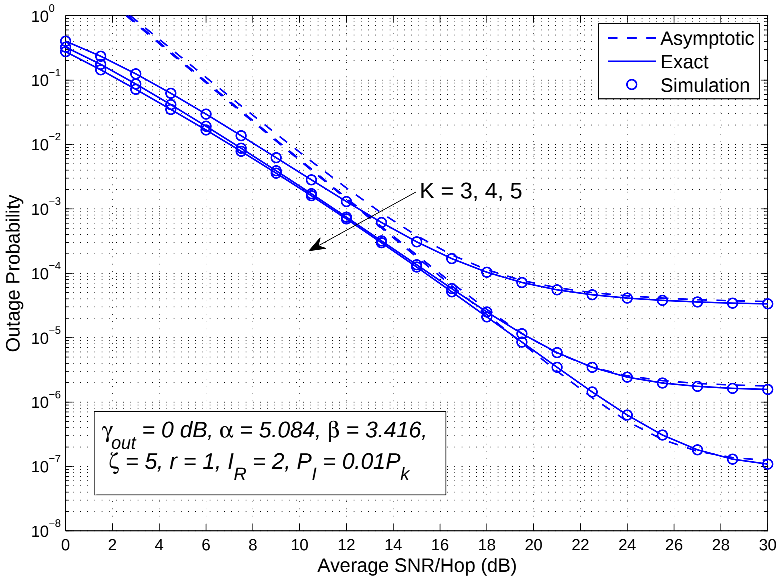


Figure 5.3: Outage probability versus SNR of the considered system with opportunistic scheduling and different number of users K at strong atmospheric turbulence conditions $\alpha = 5.084, \beta = 3.416$.

the considered system is limited to the RF link conditions, hence, we can see that increasing K provides a remarkable improvement on the system performance. On the other hand, Figure 5.3 shows how strong atmospheric turbulence conditions could limit the system outage performance. In this figure, at low SNR values, although increasing K improves the system outage performance, the outage performance improvement becomes very small with higher number of K at low to medium SNR values. This is because after a certain value of users the system performance becomes limited by the FSO link performance which is independent of the number of users. Hence, at low to medium SNR values, increasing K would have no effect on the system performance. Whereas, at high SNR values increasing K pushes down the outage performance floor caused by the CCI signals which improves the system outage performance.

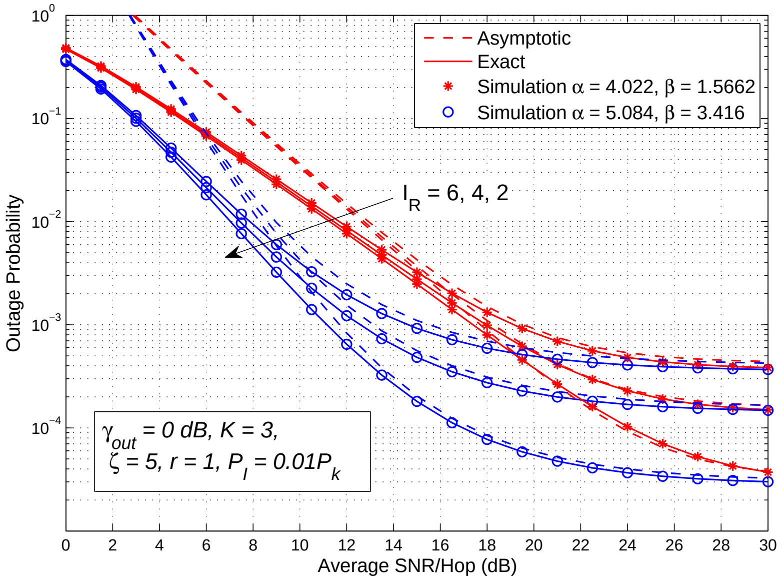


Figure 5.4: Outage probability versus SNR of the considered system with opportunistic scheduling and different number of co-channel interferers I_{R} at the relay in different atmospheric turbulence conditions α and β.

The impact of the number of CCI signals I_{R} on the system outage performance is investigated in Figure 5.4. It is clear that increasing I_{R} increases the system outage probability as expected. At low to medium SNR values, it is clear that increasing the number of interferers has a very limited impact on the system outage for the case of strong atmospheric turbulence conditions (i.e., $\alpha = 4.022, \beta = 1.566$), while increasing the number of interferers has a remarkable impact on the system outage performance under weaker turbulence conditions (i.e., $\alpha = 5.084, \beta = 3.416$). On the other hand, at high SNR values, increasing I_{R} harms the system reliability by increasing its outage performance under the two cases of atmospheric turbulence conditions. Again, a noise floor appears in this figure as the interference power is assumed to be scaled with SNR.

The effect of Nakagami-m parameters m_k and $m_{I_{\mathrm{R}}}$ on the system outage perfor-

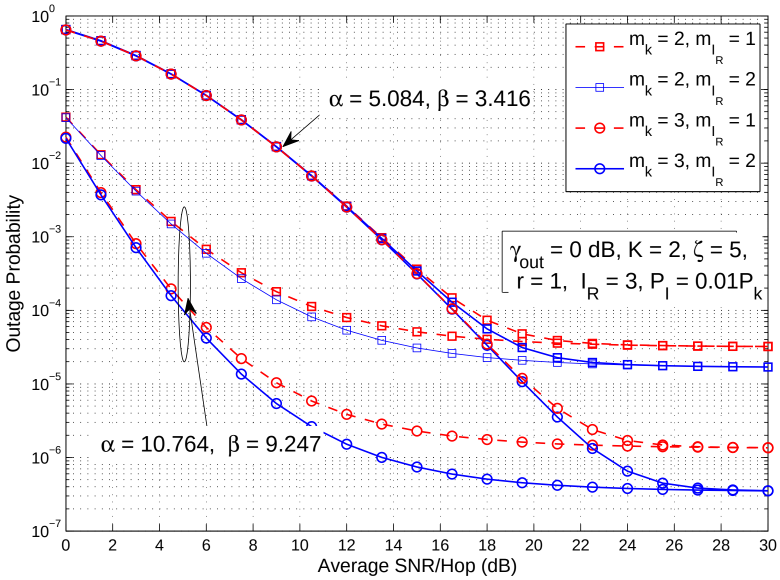


Figure 5.5: Outage probability versus SNR of the considered system with opportunistic scheduling and different values of Nakagami-m parameters m_k and $m_{I_{\mathrm{R}}}$ in different atmospheric turbulence conditions α and β.

mance is studied in Figure 5.5 under different conditions of atmospheric turbulence conditions. At weak turbulence conditions, it is clear that increasing m_k enhances the system outage performance. Moreover, at strong turbulence conditions, it can be noticed that increasing m_k has no impact on the system outage performance at low to medium SNR values since the system performance is limited by the FSO link performance. At high SNR values and under both turbulence conditions, it can be noticed that increasing m_k enhances the system outage performance by pushing down the performance floor. On the other hand, results show that increasing $m_{I_{\mathrm{R}}}$ enhances the system outage performance which matches the results obtained in [128].

The proposed optimal power allocation formula is investigated in Figure 5.6 against different number of users K and under different FSO turbulence condi-

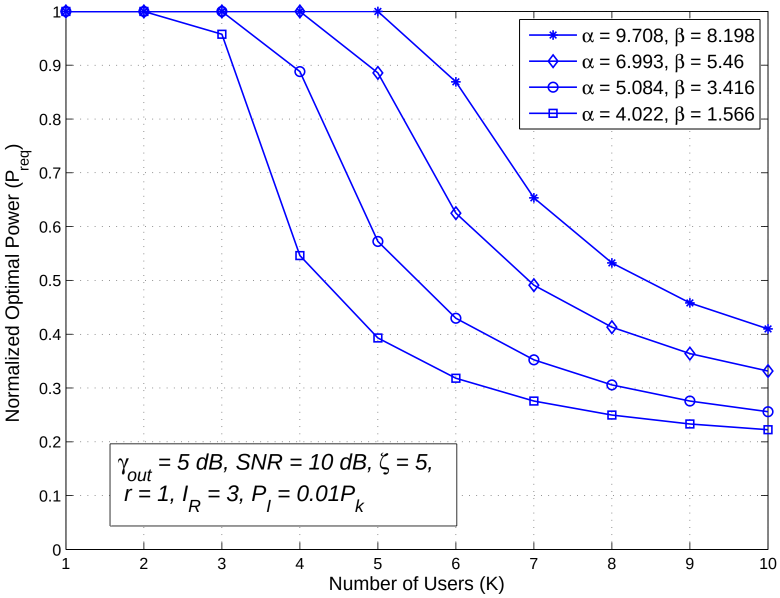


Figure 5.6: Optimal power allocation for the considered system with opportunistic scheduling versus number of users K for different atmospheric turbulence conditions α and β.

tions. As long as the RF link dominates the considered system performance, the selected user transmits with maximum power $P_{\mathsf{T}} = 1$ (i.e., normalized). Once the FSO link dominates the considered system performance, the proposed optimal power allocation formula obtains the required user transmission power P^{opt} which guarantees the best RF link performance (RF outage $=$ 0.01 FSO outage) and saves the rest of the power as there will be no performance improvement due to increasing it. As shown in this figure, for the case of strong turbulence $(\alpha = 4.022, \beta = 1.566$), it can be noticed that the selected user transmits with P_{T} as long as $K \leq 3$. As K becomes > 3, the FSO link becomes the dominant link and the selected user transmits with a power less than P_{T} with no wasted power. On the other hand, for the case of weak turbulence $(\alpha = 9.708, \beta = 8.198)$, it can

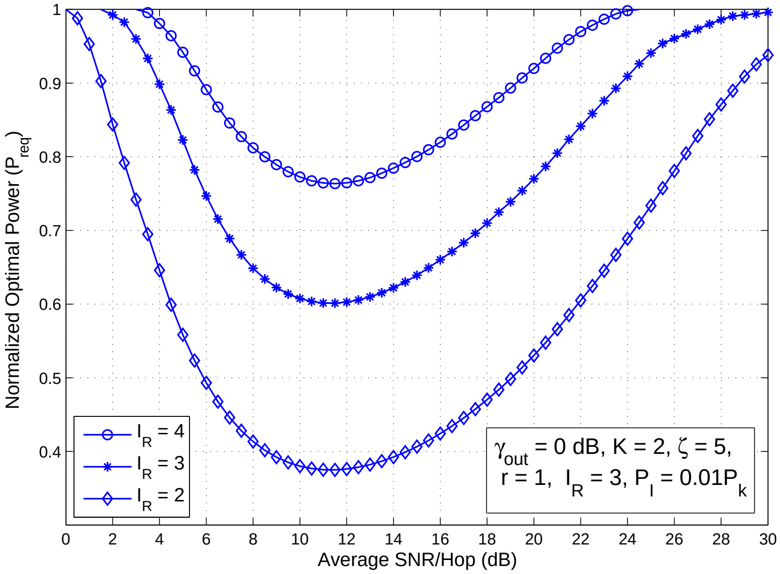


Figure 5.7: Optimal power allocation for the considered system with opportunistic scheduling versus SNR for different values of I_{R}.

be noticed that the selected user transmits with P_{T} as long as $K \leq 5$ as in this case, the FSO link needs more users in order to dominate the system performance.

The impact of the number of CCI signals I_{R} on the proposed power allocation formula is presented in Figure 5.7. In general, it can be observed that the as SNR increases the optimal required power decreases till SNR = 11 dB, then the optimal needed power starts to increase again till it reaches one at high values of SNR. Results show that increasing the number of interferers requires a higher optimal power value to maintain the relation between the RF link and FSO link which explains that the minimum value of the normalized optimal power goes from 0.4 to 0.8 when increasing I_{R} from 2 to 4 under fixed atmospheric turbulence conditions.

To investigate the impact of atmospheric channel conditions on the proposed power allocation formula, Figure 5.8 presents the normalized optimal power values

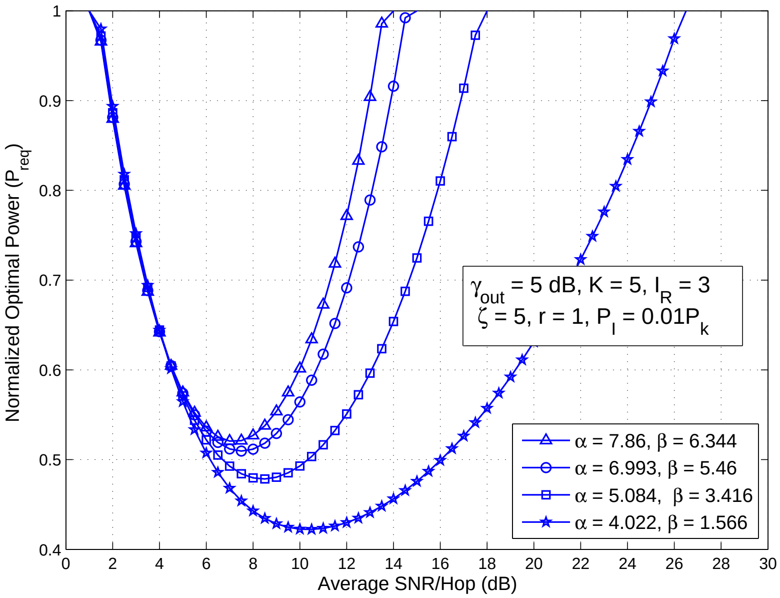


Figure 5.8: Optimal power allocation for the considered system with opportunistic scheduling versus SNR for different atmospheric turbulence conditions α and β.

against SNR under different values of α and β. Results show that increasing the values of α and β decreases the SNR range in which the power allocation formula could be effective. Moreover, the value of the needed optimal power increases with better atmospheric turbulence conditions in order to maintain the relation between the RF link and FSO link.

The secrecy performance of the considered model is studied in Figure 5.9 in terms of intercept probability. Results show that increasing the number of users K decreases the intercept probability which enhances the system secrecy performance. Moreover, the impact of the proposed power allocation formula on the system secrecy performance is investigated and compared to the case without applying power allocation formula. It can be noticed that at low SNR values both cases (i.e., with and without power allocation) provide the same intercept prob-

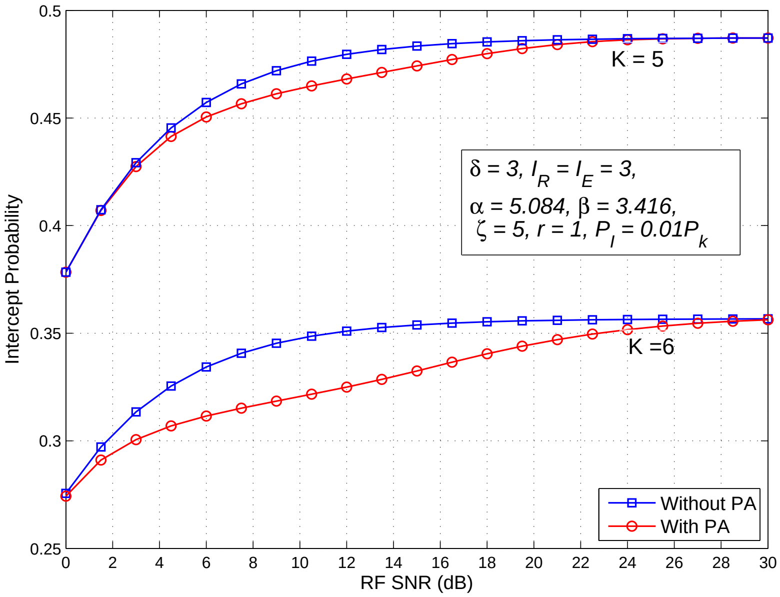


Figure 5.9: Intercept probability versus SNR of of the considered system with opportunistic scheduling and power allocation for different number of users K.

ability. At medium SNR values, the case with power allocation outperform the other case and enhances the system secrecy performance since the needed optimal power becomes less than the total available power P_T. At high SNR values, the CCI signals at the relay affects the optimal power and forces the user to transmit with its maximum power P_T resulting in increasing the intercept probability the case with power allocation to match intercept probability of the case without power allocation which harming the system secrecy performance. Under the same atmospheric turbulence conditions, it can be observed that increasing the number of users K increases the secrecy performance gap between the case with power allocation and the case without power allocation.

The impact of interference power at the relay on the system secrecy performance is investigated in Figure 5.10. Results compared between the secrecy per-

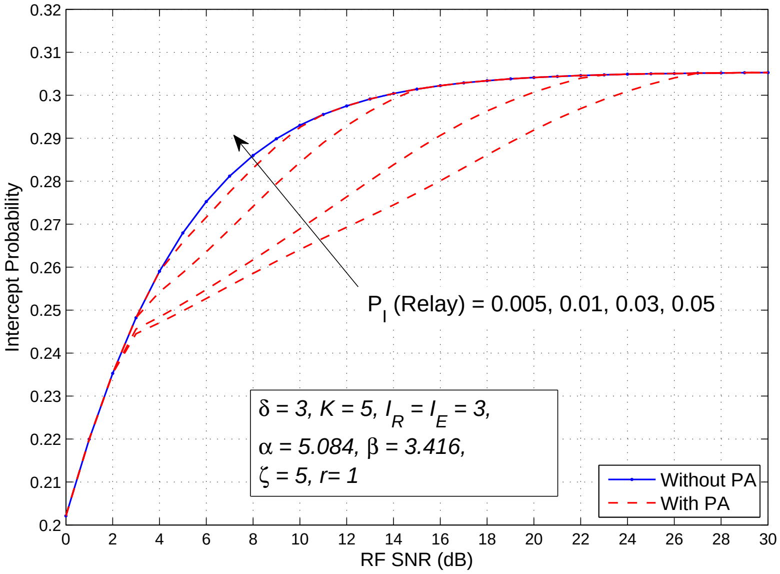


Figure 5.10: Intercept probability versus SNR of the considered system with opportunistic scheduling and power allocation for different values of I_{R}.

formance of the considered model with and without power allocation. When the considered system does not apply power allocation formula, the system intercept probability would be not affected by the interference power at the relay since the authorized user keeps transmitting with its maximum power P_{T}. On the other hand, when the considered system applies the power allocation formula, the system intercept probability decreases which enhances the system secrecy performance. However, the secrecy performance gab between the two cases is controlled by the amount of interference power at the relay. It is clear that increasing the interference power at the relay causes the user to transmit with a higher power resulting in increasing the system intercept probability and harming the secrecy performance.

On the other hand, the impact of interference power at the eavesdropper on the

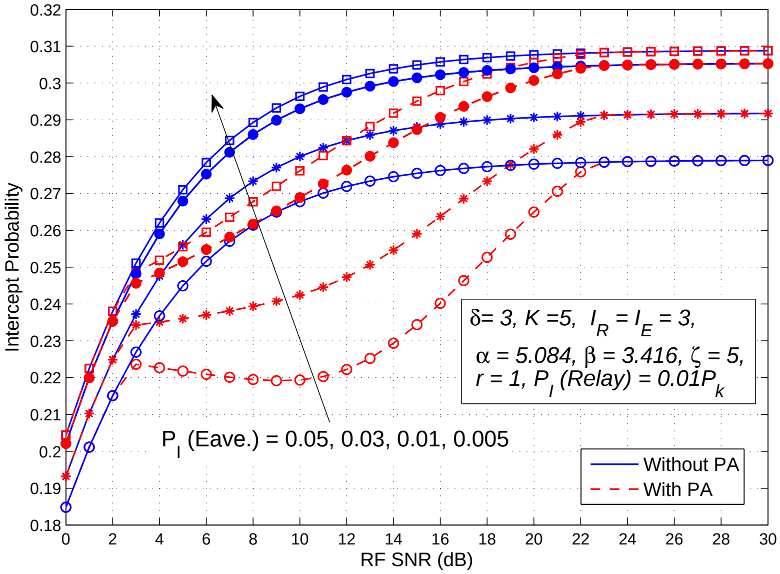


Figure 5.11: Intercept probability versus SNR of the considered system with opportunistic scheduling and power allocation for different number of co-channel interferers I_{E} at the eavesdropper.

system secrecy performance is studied in Figure 5.11. It is obvious that increasing the interference power at the eavesdropper reduces the intercept probability and enhances the system secrecy performance as shown in the figure. Moreover, if the interference power at the eavesdropper keeps increasing, the secrecy performance of the considered model with power allocation achieves a remarkable improvements in terms of secrecy performance compared to the case without power allocation. This can be explained as the eavesdropper will suffer from low transmitted power from the selected user besides the interference power which already has a significant impact on the intercept probability.

The SRT analysis of the considered system in different CJ scenarios is investigated in Figure 5.12. Results show that the AP scenario achieves the best secrecy performance among all scenarios. However, the selected jammer scenario could

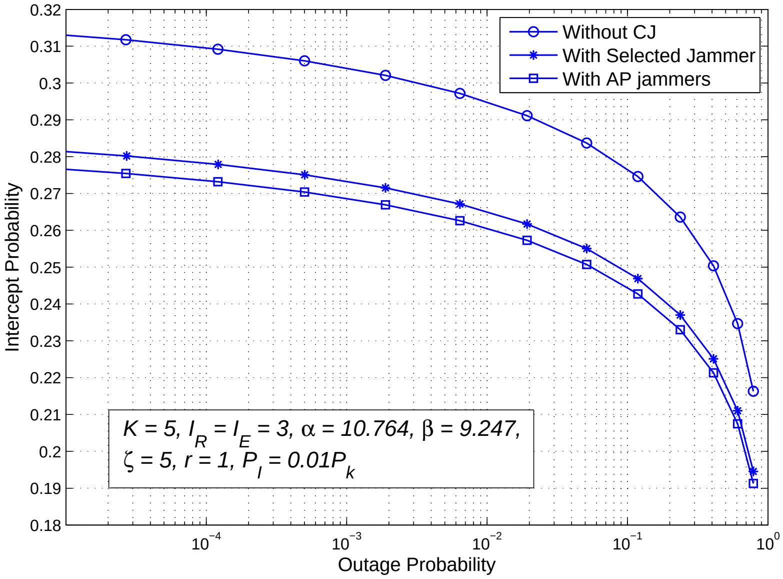


Figure 5.12: The impact of different CJ scenarios on the SRT analysis of the considered system with opportunistic scheduling.

achieve a secrecy performance which is closed to the AP scenario and better that the scenario without CJ. This significant performance of the selected jammer scenario makes it an alternative solution in the case where the AP scenario is not applicable.

Figure 5.13 studies the impact of CJ model on the SRT analysis of the considered system in different FSO link conditions. Results show that the CJ model achieves a better secrecy performance without affecting the system reliability performance.

5.7 Conclusion

This chapter investigated the impact of non-idential CCI on the security and reliability performance metrics of MU mixed RF/FSO relay network with opportunis-

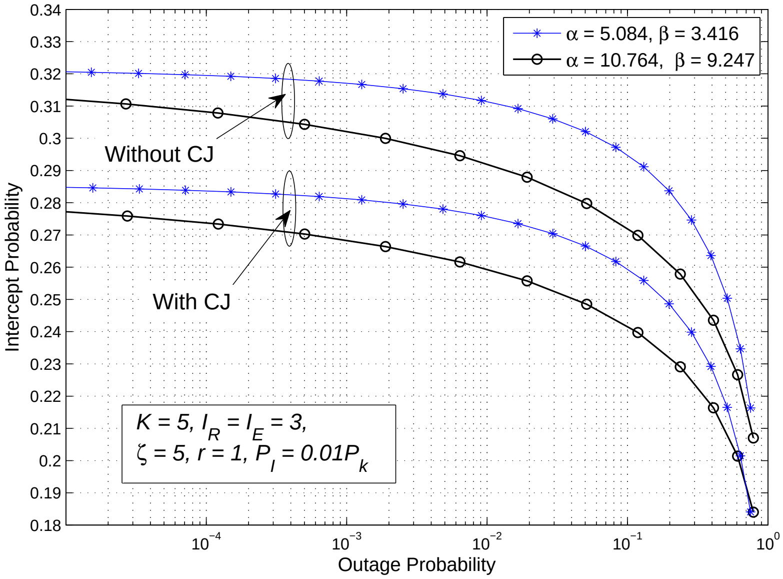


Figure 5.13: The impact of different AP CJ scenario on the SRT analysis of the considered system with opportunistic scheduling for different atmospheric turbulence conditions.

tic scheduling. We considered that the RF/FSO links are following Nakagami-m/Gamma-Gamma fading distributions with jitter effect. Then, new mathematical formula was derived for the exact outage probability. For high SNR values, closed-form expressions for the asymptotic outage probability were derived and used in obtaining optimal power allocation solutions. Moreover, the PHY security of the system against a single passive eavesdropper attack was investigated and the system intercept probability formula was derived in the presence of non-identical co-channel interference. To enhance the secrecy performance, a new cooperative model which employs the selected worst user by the authorized relay to serve as a friendly jammer was proposed. Also, closed-form expressions for the intercept probability of two different CJ models were derived. Findings of this chapter illustrated the RF links dominated the system performance in the case of weak turbulence conditions and the system achieves the full diversity order of $m_k K$. On the other hand, the FSO link dominated the system performance in the case of strong turbulence conditions which limits the diversity order of the system. Moreover, power allocation formula was shown to provide a significant improvement in the secrecy performance of the considered system. Finally, the proposed CJ model was shown to enhance the system performance, especially for the RF dominant case.

5.8 List of Publications

- **Ahmed H. Abd El-Malek**, Anas M. Salhab and Salam A. Zummo, ″ Security-Reliability Trade-off Analysis and Power Allocation in Multiuser Mixed RF/FSO Relay Networks in the presence of interference,″ to be submitted.

CHAPTER 6

CONCLUSIONS AND FUTURE RESEARCH

In this chapter, we summarize and discuss the main contributions of this dissertation and suggest some possible future research directions.

6.1 Summary of Contributions

The dissertation work covered two main areas in cooperative relay networks which are the area of cooperative cognitive radio networks and the area of mixed RF/FSO relaying networks. In both considered areas, we proposed new models and investigated their reliability performance metrics such as outage probability, SEP, achievable rate and ergdoic capacity. Moreover, we studied the secrecy performance of the considered models against eavesdropping attacks.

In the area of cooperative CR networks, we proposed two new models which are the cooperative two-path AF relaying CR model and the cooperative two-way

AF relaying CR model. In the two-path AF relaying CR model, we proposed a new system in which the SU pairs serves as the two relaying nodes for the PU network. This new model achieves a bandwidth efficient equals to 1 with PU diversity order of 3 and SU diversity order of 2. The error probability performance of this proposed model outperforms the other existing models performances. On the other hand, this proposed model achieves the highest total achievable sum rate compared to other existing models. Moreover, the secrecy performance of the considered two-path AF relaying CR model was investigated against passive eavesdropping attacks. We studied the secrecy performance under to different scenarios based on the knowledge of the eavesdropper about the SU transmission. Results show that the proposed model enhances the PU network PHY security against single/multiple passive eavesdroppers which might encourage the PU network to cooperate with the SU networks.

The second proposed model was the cooperative two-way AF relaying CR model, in which the PU networks might allow the SU network to use the single PU relay in their transmission if the SU pairs agree to relay the PU data between the two PU nodes. For this cooperative model, we proposed three different schemes for cooperation namely, AP scheme, RS scheme and RE scheme. For all proposed schemes, we derived closed-form expressions for the outage probability, SEP and maximum achievable rate. Then, the derived closed-form expressions were simplified to simpler asymptotic formulas at high SNR values. Based on the obtained asymptotic expressions, we formulated power allocation optimization problems to find the optimal power need to minimize the weighted sum SEPs or to maximize the weighted sum achievable rates. The findings show that the system achieves a bandwidth efficiency equals to 1.25/1.67 based on the selected cooperative scheme. Moreover, the secrecy performance of the proposed model was investigated in the presence of passive eavesdropper. Two different techniques which are cooperative beamforming and relay-and-jamming techniques were used to enhance the proposed system secrecy performance.

In the area of mixed RF/FSO relaying networks, we investigated the performance of MU-SIMO mixed RF/FSO networks with MRC/SC diversity combining technique over Nakagami-m/Gamma-Gamma fading channels. We derived closed-form expressions for the system outage probability, SEP and ergodic capacity. Hence, for high SNR values, the outage probability expression was simplified to its asymptotic expressions. Based on the obtained asymptotic expression, we proposed a new RF power allocation formula which was tested under different atmospheric turbulence conditions. The findings showed that the considered model can achieve a diversity order of $m_k K N_\mathsf{r}$. The performance of considered model with MRC technique outperforms the performance of the considered model with SC technique especially at weak turbulence conditions. Moreover, the system secrecy performance was studied in the presence of multiple antennas passive eavesdropper. Closed-form expressions for the system intercept probability were derived for different cased of diversity combining techniques applied by the authorized relay. The impact of the proposed RF power allocation formula on the system secrecy performance was investigated. Finally, cooperative jamming technique was proposed to enhance the system secrecy performance. Results showed that the proposed power allocation formula enhances the system secrecy performance especially at strong turbulence conditions. The proposed cooperative jamming techniques provided a remarkable improvement in the system secrecy performance.

Furthermore, in the area of mixed RF/FSO relaying networks, we investigated the impact of non-identical co-channel interference on the performance of a MU mixed RF/FSO networks over Nakagami-m/Gamma-Gamma fading channels. First, we investigated the impact of interfering signals on the system outage performance by obtaining closed-form expression for the system outage probability in the presence of interference. Hence, we obtained asymptotic outage probability formula at high SNR values. We proposed a new RF power allocation formula based on the derived asymptotic outage formula. Second, we studied the impact of interfering signals on the system secrecy performance. We assumed that both authorized and unauthorized nodes suffering from non-identical interference. Closed-form expression for the system intercept probability was derived and then simplified to its asymptotic formula at high SNR values. The impact of the obtained power allocation formula on the system secrecy performance was investigated in the presence of interference. Finally, we enhanced the system secrecy performance by applying cooperative jamming technique. Results showed that although the system reliability performance might be harmed by the co-channel interference, the system secrecy performance might be improved because of the existence of interference. Moreover, the proposed power allocation formula enhances the system secrecy performance against eavesdroppers especially at strong turbulence conditions. The proposed cooperative jamming models were shown to improve the considered system secrecy performance.

6.2 Future Research

In the above-mentioned proposed works, we studied the secrecy performance of different systems in the presence of a passive eavesdropper. Although, the case of the passive eavesdropper is considered as the worst case of eavesdropping attack due to the unavailability of wiretap channels CSI, we may also need to consider the case of active eavesdroppers where the eavesdroppers communicate with each others. For the case of active eavesdroppers, the authorized system nodes have full or partial wiretap channels CSI which would change the way of authorized communication setups. The available wiretap channels CSI might change the relay selection model, antenna selection mode, the beamforming technique and the selected friendly jammer.

Recently, the area of device-to-device (D2D) communications attracts a lot of research work. In this area, D2D communications enable devices to communicate directly with each other without routing the data paths through a network infrastructure (i.e., base stations). Hence, D2D communications enhances the wireless network bandwidth efficiency. In addition, D2D communications can also enhance the wireless networks energy efficiency, reduce the network delay, and provide a higher throughput. Therefore, the work proposed in the area of cooperative CR models can be extended to enhance the work in the area of D2D communications. Moreover, the PHY security models proposed in this work can be employed in the area of D2D communication to enhance their secrecy performance.

In addition, the work in the area of mixed RF/FSO networks can be extended to the area of CR networks which would enhance the system spectral efficiency and reduced the interference of the SU network on the PU networks. The CR mixed RF/FSO links can highly increase the throughput of the SU networks by multiuser multiplexing. Moreover, the mixed RF/FSO system can enhance the SU secrecy performance because of the LOS nature of the FSO links.

6.3 List of Publications

- **Ahmed H. Abd El-Malek**, Fawaz Al-Qahtani, Salam A. Zummo, and Hussein Alnuweiri, ″TAS/MRC in Cognitive Relay Networks over Rayleigh Fading Channels with Correlated Antennas,″ in Proc. IEEE Int'l Conf. on Commun., (ICC14), Sydney, Australia, June 2014.

- **Ahmed H. Abd El-Malek**, Fawaz Al-Qahtani, Salam A. Zummo, and Hussein Alnuweiri, ″Cognitive Multiuser MIMO in Spectrum Sharing Environment with Antenna Correlation over Nakagami-m Fading,″ in Proc. IEEE Veh. Technol. Conf. (VTC-Fall'14), Vancouver, BC, Canada, September 2014.

- **Ahmed H. Abd El-Malek**, Fawaz Al-Qahtani, Salam A. Zummo, and Hussein Alnuweiri, ″MIMO Multiuser Cognitive Relay Network in Spectrum Sharing Environment with Antenna Correlation over Rayleigh Fading Channels,″ in Proc. IEEE Wireless Commun. and Networking Conf. (WCNC'15), New Orleans, LA, USA, March 2015.

- **Ahmed H. Abd El-Malek**, Fawaz Al-Qahtani, Trung Q. Duong, Salam A. Zummo, and Hussein Alnuweiri,″MIMO Cognitive Relay Networks with Correlated Antennas over Rayleigh Fading Channels,″ IEEE Trans. Veh. Technol., accepted, June 2015.

- **Ahmed H. Abd El-Malek**, Fawaz Al-Qahtani, Salam A. Zummo, and Hussein Alnuweiri, ″Transmit Antenna Selection of Correlated MIMO Multiuser Cognitive Radio Networks in Nakagami-m Fading Channels,″ Accepted in Wireless Commun. and Mobile Computing, Wiley, January 2016.

- **Ahmed H. Abd El-Malek**, Fawaz Al-Qahtani, Salam A. Zummo, and Hussein Alnuweiri, ″Underlay Spectrum Sharing Relay Correlated MIMO Networks with Transmit Antenna Selection,″ Under second round of review in Wireless personal commun., Springer.

- **Ahmed H. Abd El-Malek**, Anas M. Salhab and Salam A. Zummo, ″Optimal Power Allocation for Enhancing Physical Layer Security in Opportunistic Relay Networks in the Presence of Co-Channel Interference,″ in Proc. IEEE Global Commun. Conf. (GLOBECOM15), San Diego, CA, USA, December 2015.

- **Ahmed H. Abd El-Malek**, Anas M. Salhab, Salam A. Zummo and Mohamed-Slim Alouini, ″Cooperative Jamming Technique for Enhancing Physical Layer Security in Opportunistic Relay Networks in the Presence of Interference,″ to be submitted to IEEE Trans. Veh. Technol..

APPENDICES

APPENDIX A

APPENDIX FOR CHAPTER 2

A.1 Proof $\mathbf{H}_{\mathsf{D}}$ is a full rank matrix

In this appendix, we showed that the channel matrix $\mathbf{H}_{\mathsf{D}}$ is a full rank matrix of rank 3. Based on eq.(8) in the revised manuscript, the matrix at node D is given by

$$\mathbf{H}_{\mathsf{D}} = \begin{bmatrix} \sqrt{\frac{1}{2}} h_{\mathsf{SD}} & -\sqrt{\frac{1}{2}} h_{\mathsf{SD}} & h_{\mathsf{BD}} \\ \sqrt{\frac{1}{2}} \alpha_{\mathsf{A}} & h_{\mathsf{SD}} - \sqrt{\frac{1}{2}} \alpha_{\mathsf{A}} & \beta_{\mathsf{A}} h_{\mathsf{AD}} h_{\mathsf{BA}} \\ \sqrt{\frac{1}{2}} \beta_{\mathsf{B}} h_{\mathsf{BD}} \alpha'_{\mathsf{A}} & \beta_{\mathsf{B}} h_{\mathsf{BD}} (h_{\mathsf{SD}} - \sqrt{\frac{1}{2}} \alpha'_{\mathsf{A}}) & -h_{\mathsf{BD}} \end{bmatrix}, \tag{A.1}$$

where $\alpha_{\mathsf{A}} = \beta_{\mathsf{A}} h_{\mathsf{AD}} h_{\mathsf{SA}}$ and $\alpha'_{\mathsf{A}} = \beta_{\mathsf{A}} h_{\mathsf{AB}} h_{\mathsf{SA}}$. Then, to prove that the matrix $\mathbf{H}_{\mathsf{D}}$ is a full rank matrix, we need to show that $\mathbf{H}_{\mathsf{D}} \times \mathbf{x} = \mathbf{0}$, if and only if $\mathbf{x} = \mathbf{0}$, where $\mathbf{x} = [x_1, x_2, x_3]^T$ and $\mathbf{0}$ is a 3×1 zero column vector.

For simplicity and without losing generality, consider the average channel gains of all the channels (i.e. $v_{\mathsf{S}}^2, v_{\mathsf{R}}^2$ and v_{D}^2,) equal 1. Then

$$\mathbf{H}_{\mathsf{D}} = \begin{bmatrix} \sqrt{\frac{1}{2}} & -\sqrt{\frac{1}{2}} & 1 \\ \sqrt{\frac{1}{2}}\beta_{\mathsf{A}} & 1-\sqrt{\frac{1}{2}}\beta_{\mathsf{A}} & \beta_{\mathsf{A}} \\ \sqrt{\frac{1}{2}}\beta_{\mathsf{B}}\beta_{\mathsf{A}} & \beta_{\mathsf{B}}-\sqrt{\frac{1}{2}}\beta_{\mathsf{A}} & -1 \end{bmatrix}, \tag{A.2}$$

and

$$\begin{bmatrix} \sqrt{\frac{1}{2}} & -\sqrt{\frac{1}{2}} & 1 \\ \sqrt{\frac{1}{2}}\beta_{\mathsf{A}} & 1-\sqrt{\frac{1}{2}}\beta_{\mathsf{A}} & \beta_{\mathsf{A}} \\ \sqrt{\frac{1}{2}}\beta_{\mathsf{B}}\beta_{\mathsf{A}} & \beta_{\mathsf{B}}-\sqrt{\frac{1}{2}}\beta_{\mathsf{A}} & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \mathbf{0}. \tag{A.3}$$

Then, applying Gaussian elimination method as following:

i. Eliminating x_1 from the second row of $\mathbf{H}_{\mathsf{D}}$ by adding $-\beta_{\mathsf{A}} \times r_1$ to r_2: $\{-\beta_{\mathsf{A}} \times r_1 + r_2 \rightarrow r_2\}$.

$$\begin{bmatrix} \sqrt{\frac{1}{2}} & -\sqrt{\frac{1}{2}} & 1 \\ 0 & 1 & 0 \\ \sqrt{\frac{1}{2}}\beta_{\mathsf{B}}\beta_{\mathsf{A}} & \beta_{\mathsf{B}}-\sqrt{\frac{1}{2}}\beta_{\mathsf{A}} & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \mathbf{0}. \tag{A.4}$$

ii. Eliminating x_1 from the third row of $\mathbf{H}_{\mathsf{D}}$ by adding $-\beta_{\mathsf{A}}\beta_{\mathsf{B}} \times r_1$ to r_3:

$\{-\beta_{\mathsf{A}}\beta_{\mathsf{B}} \times r_1 + r_3 \rightarrow r_3\}$

$$\begin{bmatrix} \sqrt{\frac{1}{2}} & -\sqrt{\frac{1}{2}} & 1 \\ 0 & 1 & 0 \\ 0 & \beta_{\mathsf{B}} & -1-\beta_{\mathsf{A}}\beta_{\mathsf{B}} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \mathbf{0}. \tag{A.5}$$

iii. Eliminating x_2 from the third row of $\mathbf{H}_{\mathsf{D}}$ by adding $\sqrt{2}\beta_{\mathsf{B}} \times r_2$ to r_3: $\left\{+\sqrt{2}\beta_{\mathsf{B}} \times r_2 + r_3 \rightarrow r_3\right\}$

$$\begin{bmatrix} \sqrt{\frac{1}{2}} & -\sqrt{\frac{1}{2}} & 1 \\ 0 & 1 & 0 \\ 0 & 0 & -1-\beta_{\mathsf{A}}\beta_{\mathsf{B}}+\sqrt{2}\beta_{\mathsf{B}} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \mathbf{0}. \tag{A.6}$$

From (A.6), it can be easily noticed that $x_2 = 0$, and

$$\left(-1-\beta_{\mathsf{A}}\beta_{\mathsf{B}}+\sqrt{2}\beta_{\mathsf{B}}\right) x_3 = 0 \tag{A.7}$$

which leads to

$$\beta_{\mathsf{B}} = \frac{1}{\sqrt{2}-\beta_{\mathsf{A}}} \qquad \text{or} \qquad x_3 = 0 \tag{A.8}$$

First, we notice that β_{B} can reach ∞ if $\beta_{\mathsf{A}} = \sqrt{2}$. But since $\beta_{\mathsf{A}} \leq 1 < \sqrt{(2)}$, then β_{B} cannot reach ∞.

Second, we check if $\beta_{\mathsf{B}} = \frac{1}{\sqrt{2}-\beta_{\mathsf{A}}}$, starting from

$$\beta_{\mathsf{B}} = \sqrt{\frac{\lambda_{\mathsf{B}}}{1 + \lambda_{\mathsf{A}} + \sigma^2}}, \tag{A.9}$$

and assuming noise-free $\sigma^2 = 0$, then

$$\beta_{\mathsf{B}} = \sqrt{\frac{\lambda_{\mathsf{B}}}{1 + \lambda_{\mathsf{A}}}} \qquad \text{and} \qquad \beta_{\mathsf{A}} = \sqrt{\frac{\lambda_{\mathsf{A}}}{1 + P_{\mathsf{B}}}}. \tag{A.10}$$

Since $P_{\mathsf{B}} = 1 - \lambda_B$, then $\lambda_{\mathsf{A}} = \beta_{\mathsf{A}}^2(2 - \lambda_{\mathsf{B}})$ and

$$\beta_{\mathsf{B}} = \sqrt{\frac{\lambda_{\mathsf{B}}}{1 + \beta_{\mathsf{A}}^2(2 - \lambda_{\mathsf{B}})}} = \sqrt{\frac{1}{\frac{1}{\lambda_{\mathsf{B}}} + \beta_{\mathsf{A}}^2(\frac{2}{\lambda_{\mathsf{B}}} - 1)}} \neq \frac{1}{\sqrt{2} - \beta_{\mathsf{A}}} \tag{A.11}$$

Finally, it can be noted that $x_3 = 0$ is the only solution to (A.8) and as a result from (A.6), $x_1 = 0$. Since the vector $\mathbf{x} = 0$, the channel matrix $\mathbf{H}_{\mathsf{D}}$ is concluded to be a full rank matrix. ■

Following the same procedures, it can easily proof that the SU channel matrix $\mathbf{H}_{\mathsf{A}}$ is a full rank matrix of rank 2.

Bibliography

[1] Yi-Sheng Shiu, Shih-Yu Chang, Hsiao-Chun Wu, S.C.-H. Huang, and Hsiao-Hwa Chen. Physical layer security in wireless networks: a tutorial. *IEEE Wireless Commun.*, 18(2):66–74, 2011.

[2] M. Bloch, J. Barros, M. R D Rodrigues, and S.W. McLaughlin. Wireless information-theoretic security. *IEEE Trans. Inf. Theory*, 54(6):2515–2534, 2008.

[3] A. D. Wyner. The wire-tap channel. *Bell Syst. Tech. J.*, 54(8):1355–1387, 1975.

[4] Tie Liu and S. Shamai. A note on the secrecy capacity of the multiple-antenna wiretap channel. *IEEE Trans. Inf. Theory*, 55(6):2547–2553, June 2009.

[5] A. Chorti, S.M. Perlaza, Zhu Han, and H.V. Poor. Physical layer security in wireless networks with passive and active eavesdroppers. In *Global Communications Conference (GLOBECOM), 2012 IEEE*, pages 4868–4873, Dec 2012.

[6] J. Barros and M. R D Rodrigues. Secrecy capacity of wireless channels. In *Proc. IEEE Int. Symp. on Inform. Theory*, pages 356–360, 2006.

[7] A. Khisti and Gregory W. Wornell. Secure transmission with multiple antennas part ii: The mimome wiretap channel. *IEEE Trans. Inf. Theory*, 56(11):5515–5532, 2010.

[8] V.U. Prabhu and M.R.D. Rodrigues. On wireless channels with M -antenna eavesdroppers: Characterization of the outage probability and ϵ - outage secrecy capacity. *IEEE Trans. Inf. Forens. Security*, 6(3):853–860, 2011.

[9] Fangming He, Hong Man, and Wei Wang. Maximal ratio diversity combining enhanced security. *IEEE Commun. Lett.*, 15(5):509–511, 2011.

[10] S. Bashar, Zhi Ding, and G.Y. Li. On secrecy of codebook-based transmission beamforming under receiver limited feedback. *IEEE Trans. Wireless Commun.*, 10(4):1212–1223, 2011.

[11] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24(3):339–348, May 1978.

[12] L.H. Ozarow and A.D. Wyner. Wire-tap channel ii. In Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, editors, *Advances in Cryptology*, volume 209 of *Lecture Notes in Computer Science*, pages 33–50. Springer Berlin Heidelberg, 1985.

[13] Yingbin Liang, H.V. Poor, and S. Shamai. Secure communication over fading channels. *IEEE Trans. Inf. Theory*, 54(6):2470–2492, June 2008.

[14] Praveen Kumar Gopala, Lifeng Lai, and H. El-Gamal. On the secrecy capacity of fading channels. *IEEE Trans. Inf. Theory*, 54(10):4687–4698, Oct 2008.

[15] Zang Li, R. Yates, and W. Trappe. Secret communication with a fading eavesdropper channel. In *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*, pages 1296–1300, June 2007.

[16] Liang Yingbin, Kramer Gerhard, Poor H Vincent, and Shlomo Shamai. Compound wiretap channels. *EURASIP J. on Wireless Commun. and Networking*, 2009, 2009.

[17] A.O. Hero. Secure space-time communication. *IEEE Trans. Inf. Theory*, 49(12):3235–3249, Dec 2003.

[18] S. Shafiee, Nan Liu, and Sennur Ulukus. Towards the secrecy capacity of the gaussian mimo wire-tap channel: The 2-2-1 channel. *IEEE Trans. Inf. Theory*, 55(9):4033–4039, Sept 2009.

[19] F. Oggier and B. Hassibi. The secrecy capacity of the mimo wiretap channel. *IEEE Trans. Inf. Theory*, 57(8):4961–4972, 2011.

[20] R. Negi and S. Goel. Secret communication using artificial noise. In *Vehicular Technology Conference, 2005. VTC-2005-Fall. 2005 IEEE 62nd*, volume 3, pages 1906–1910, Sept 2005.

[21] S. Goel and R. Negi. Guaranteeing secrecy using artificial noise. *IEEE Trans. Wireless Commun.*, 7(6):2180–2189, June 2008.

[22] Qiang Li and Wing-Kin Ma. Spatially selective artificial-noise aided transmit optimization for miso multi-eves secrecy rate maximization. *IEEE Trans. Signal Process.*, 61(10):2704–2717, May 2013.

[23] Pin-Hsun Lin, Szu-Hsiang Lai, Shih-Chun Lin, and Hsuan-Jung Su. On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels. *IEEE J. Sel. Areas Commun.*, 31(9):1728–1740, September 2013.

[24] Y.-W.P. Hong, Pang-Chang Lan, and C.-C.J. Kuo. Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches. *IEEE Signal Process. Mag.*, 30(5):29–40, Sept 2013.

[25] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami. Phy layer security based on protected zone and artificial noise. *IEEE Signal Process. Lett.*, 20(5):487–490, May 2013.

[26] A. Mukherjee and A.L. Swindlehurst. Robust beamforming for security in mimo wiretap channels with imperfect csi. *IEEE Trans. Signal Process.*, 59(1):351–361, Jan 2011.

[27] S. Gerbracht, C. Scheunert, and E.A. Jorswieck. Secrecy outage in miso systems with partial channel information. *IEEE Trans. Inf. Forens. Security*, 7(2):704–716, April 2012.

[28] M.R. Bloch and J.N. Laneman. Exploiting partial channel state information for secrecy over wireless channels. *IEEE J. Sel. Areas Commun.*, 31(9):1840–1849, September 2013.

[29] H. Alves, R.D. Souza, M. Debbah, and M. Bennis. Performance of transmit antenna selection physical layer security schemes. *IEEE Signal Process. Lett.*, 19(6):372–375, 2012.

[30] Nan Yang, P.L. Yeoh, M. Elkashlan, R. Schober, and I.B. Collings. Transmit antenna selection for security enhancement in mimo wiretap channels. *IEEE Trans. Commun.*, 61(1):144–154, 2013.

[31] N. Yang, P. Yeoh, M. Elkashlan, R. Schober, and J. Yuan. Mimo wiretap channels: Secure transmission using transmit antenna selection and receive generalized selection combining, 2013.

[32] Nan Yang, H.A. Suraweera, I.B. Collings, and Chau Yuen. Physical layer security of tas/mrc with antenna correlation. *IEEE Trans. Inf. Forens. Security*, 8(1):254–259, 2013.

[33] Ning Zhang and Jon W. Mark. *Security-aware Cooperation in Cognitive Radio Networks.* Springer Briefs in Computer Science. Springer, 2014.

[34] M. Yuksel and E. Erkip. Secure communication with a relay helping the wire-tapper. In *Proc. IEEE Inform. Theory Workshop (ITW)*, pages 595–600, Tahoe City, CA, September 2007.

[35] Lun Dong, Zhu Han, A.P. Petropulu, and H.V. Poor. Improving wireless physical layer security via cooperating relays. *IEEE Trans. Signal Process.*, 58(3):1875–1888, March 2010.

[36] Ye Yang, Qiang Li, Wing-Kin Ma, Jianhua Ge, and P. C. Ching. Cooperative secure beamforming for af relay networks with multiple eavesdroppers. *IEEE Signal Process. Lett.*, 20(1):35–38, Jan 2013.

[37] I. Krikidis, J.S. Thompson, and S. McLaughlin. Relay selection for secure cooperative networks with jamming. *IEEE Trans. Wireless Commun.*, 8(10):5003–5011, October 2009.

[38] Yupeng Liu, Jiangyuan Li, and A.P. Petropulu. Destination assisted cooperative jamming for wireless physical-layer security. *IEEE Trans. Inf. Forens. Security*, 8(4):682–694, April 2013.

[39] R. Bassily and S. Ulukus. Deaf cooperation for secrecy with multiple antennas at the helper. *IEEE Trans. Inf. Forens. Security*, 7(6):1855–1864, Dec 2012.

[40] R. Bassily and S. Ulukus. Deaf cooperation and relay selection strategies for secure communication in multiple relay networks. *IEEE Trans. Signal Process.*, 61(6):1544–1554, March 2013.

[41] Hui-Ming Wang, Miao Luo, Xiang-Gen Xia, and Qinye Yin. Joint cooperative beamforming and jamming to secure af relay systems with individual

power constraint and no eavesdropper's csi. *IEEE Signal Process. Lett.*, 20(1):39–42, Jan 2013.

[42] S. Vishwakarma and A. Chockalingam. Amplify-and-forward relay beamforming for secrecy with cooperative jamming and imperfect csi. In *Communications (ICC), 2013 IEEE International Conference on*, pages 3047–3052, June 2013.

[43] Yulong Zou, Xianbin Wang, and Weiming Shen. Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack. In *Communications (ICC), 2013 IEEE International Conference on*, pages 2183–2187, June 2013.

[44] Yulong Zou, Xianbin Wang, and Weiming Shen. Optimal relay selection for physical-layer security in cooperative wireless networks. *IEEE J. Sel. Areas Commun.*, 31(10):2099–2111, October 2013.

[45] L. Hanzo, X. Wang, W. Shen, and Y. Zou. Security versus reliability analysis of opportunistic relaying. *IEEE Trans. Veh. Technol.*, PP(99):1–1, 2013.

[46] D.S. Kalogerias, N. Chatzipanagiotis, M.M. Zavlanos, and A.P. Petropulu. Mobile jammers for secrecy rate maximization in cooperative networks. In *Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on*, pages 2901–2905, May 2013.

[47] Minyan Pei, A.L. Swindlehurst, Dongtang Ma, and Jibo Wei. Adaptive limited feedback for miso wiretap channels with cooperative jamming. *IEEE Trans. Signal Process.*, 62(4):993–1004, Feb 2014.

[48] Nien-En Wu and Hsueh-Jyh Li. Effect of feedback delay on secure cooperative networks with joint relay and jammer selection. *IEEE Wireless Commun. Lett.*, 2(4):415–418, August 2013.

[49] Jing Huang and A.L. Swindlehurst. Cooperative jamming for secure communications in mimo relay networks. *IEEE Trans. Signal Process.*, 59(10):4871–4884, Oct 2011.

[50] Wei Li, M. Ghogho, Bin Chen, and Chunlin Xiong. Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis. *IEEE Commun. Lett.*, 16(10):1628–1631, October 2012.

[51] Gan Zheng, I. Krikidis, Jiangyuan Li, A.P. Petropulu, and B. Ottersten. Improving physical layer secrecy using full-duplex jamming receivers. *IEEE Trans. Signal Process.*, 61(20):4962–4974, Oct 2013.

[52] A. Goldsmith, S.A. Jafar, I. Maric, and S. Srinivasa. Breaking spectrum gridlock with cognitive radios: An information theoretic perspective. *Proceedings of the IEEE*, 97(5):894–914, May 2009.

[53] A. Houjeij, W. Saad, and T. Bascar. A game-theoretic view on the physical layer security of cognitive radio networks. In *Communications (ICC), 2013 IEEE International Conference on*, pages 2095–2099, June 2013.

[54] I. Stanojev and A. Yener. Improving secrecy rate via spectrum leasing for friendly jamming. *IEEE Trans. Wireless Commun.*, 12(1):134–145, January 2013.

[55] Nan Yang, M. Elkashlan, and Jinhong Yuan. Outage probability of multiuser relay networks in nakagami- m fading channels. *IEEE Trans. Veh. Technol.*, 59(5):2120–2132, 2010.

[56] Nan Yang, M. Elkashlan, and Jinhong Yuan. Symbol error rate of wireless multiuser relay networks in nakagami-m fading channels. In *Communications (ICC), 2010 IEEE International Conference on*, pages 1–5, May 2010.

[57] Haiyang Ding, Jianhua Ge, D.B. da Costa, and Yi Guo. Spectrally efficient diversity exploitation schemes for downlink cooperative cellular networks. *IEEE Trans. Veh. Technol.*, 61(1):386–393, Jan 2012.

[58] N.S. Ferdinand and N. Rajatheva. Multi-user scheduling in af relay network with antenna correlation. In *Vehicular Technology Conference (VTC Spring), 2011 IEEE 73rd*, pages 1–5, 2011.

[59] N.S. Ferdinand, N. Rajatheva, and M. Latva-aho. Effect of antenna correlation on the performance of mimo multi-user dual hop relay network. In *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, pages 332–337, 2011.

[60] F.R.V. Guimaraes, D.B. da Costa, T.A. Tsiftsis, C.C. Cavalcante, and G.K. Karagiannidis. Multiuser and multirelay cognitive radio networks under

spectrum-sharing constraints. *IEEE Trans. Veh. Technol.*, 63(1):433–439, 2014.

[61] D. Kedar and S. Arnon. Urban optical wireless communication networks: the main challenges and possible solutions. *IEEE Commun. Mag.*, 42(5):S2–S7, May 2004.

[62] N.D. Chatzidiamantis, H.G. Sandalidis, G.K. Karagiannidis, and M. Matthaiou. Inverse gaussian modeling of turbulence-induced fading in free-space optical systems. *J. Lightw. Technol.*, 29(10):1590–1596, May 2011.

[63] W.O. Popoola and Z. Ghassemlooy. Bpsk subcarrier intensity modulated free-space optical communications in atmospheric turbulence. *J. Lightw. Technol.*, 27(8):967–973, April 2009.

[64] J.N. Laneman, D.N.C. Tse, and Gregory W. Wornell. Cooperative diversity in wireless networks: Efficient protocols and outage behavior. *IEEE Trans. Inf. Theory*, 50(12):3062–3080, December 2004.

[65] A. Sendonaris, E. Erkip, and B. Aazhang. User cooperation diversity. part i. system description. *IEEE Trans. Commun.*, 51(11):1927–1938, November 2003.

[66] Simon Haykin. Cognitive radio: brain-empowered wireless communications. *IEEE J. Sel. Areas Commun.*, 23(2):201–220, February 2005.

[67] Eunju Lee, Jaedon Park, Dongsoo Han, and Giwan Yoon. Performance analysis of the asymmetric dual-hop relay transmission with mixed rf/fso links. *IEEE Photonics Technol. Lett.*, 23(21):1642–1644, November 2011.

[68] I.S. Ansari, F. Yilmaz, and M.-S. Alouini. Impact of pointing errors on the performance of mixed rf/fso dual-hop transmission systems. *IEEE Wireless Commun. Lett.*, 2(3):351–354, June 2013.

[69] N. Saquib, S.R. Sakib, A. Saha, and M. Hussain. Free space optical connectivity for last mile solution in bangladesh. In *in Proc. Intl Conf. on Education Technol. and Computer (ICETC)*, volume 2, pages 484–487, Shanghai, China, June 2010.

[70] N.D. Chatzidiamantis, D.S. Michalopoulos, E.E. Kriezis, G.K. Karagiannidis, and R. Schober. Relay selection in relay-assisted free space optical systems. In *in Proc. IEEE Global Commun. Conf. (Globecom)*, pages 1–6, Houston, USA, December 2011.

[71] T. Oechtering and A. Sezgin. A new cooperative transmission scheme using the space-time delay code. In *Smart Antennas, 2004. ITG Workshop on*, pages 41–48, 2004.

[72] A. Ribeiro, Xiaodong Cai, and G.B. Giannakis. Opportunistic multipath for bandwidth-efficient cooperative networking. In *Acoustics, Speech, and Signal Processing, 2004. Proceedings. (ICASSP '04). IEEE International Conference on*, volume 4, pages iv–549–iv–552 vol.4, 2004.

[73] B. Rankov and A. Wittneben. Spectral efficient protocols for half-duplex fading relay channels. *IEEE J. Sel. Areas Commun.*, 25(2):379–389, 2007.

[74] Chunbo Luo, Yu Gong, and Fuchun Zheng. Full interference cancellation for two-path relay cooperative networks. *IEEE Trans. Veh. Technol.*, 60(1):343–347, 2011.

[75] Feng Li, Xuezhi Tan, and Li Wang. Power scheme and time-division bargaining for cooperative transmission in cognitive radio. *Wiley Wireless Commun. and Mobile Computing*, 15(2):379388, February 2015.

[76] Frédéric Gabry, Nan Li, Nicolas Schrammar, Maksym Girnyk, L Rasmussen, and Mikael Skoglund. On the optimization of the secondary transmitter's strategy in cognitive radio channels with secrecy. *IEEE J. Sel. Areas Commun.*, 32(3):451–463, March 2014.

[77] Hyoungsuk Jeon, Steven W. McLaughlin, Il-Min Kim, and Jeongseok Ha. Secure communications with untrusted secondary nodes in cognitive radio networks. *IEEE Trans. Wireless Commun.*, 13(4):1790–1805, April 2014.

[78] J.G. Proakis and M. Salehi. *Digital Communications*. McGraw-Hill Int. ed. McGraw-Hill Higher Educ., 2008.

[79] Xu Zhu and R.D. Murch. Performance analysis of maximum likelihood detection in a mimo antenna system. *IEEE Trans. Commun.*, 50(2):187–191, 2002.

[80] S.J. Grant and J.K. Cavers. Performance enhancement through joint detection of cochannel signals using diversity arrays. *IEEE Trans. Commun.*, 46(8):1038–1049, 1998.

[81] S.J. Grant and J.K. Cavers. Further analytical results on the joint detection of cochannel signals using diversity arrays. *IEEE Trans. Commun.*, 48(11):1788–1792, 2000.

[82] Chang Soon Park and Kwang-Bok Lee. Transmit power allocation for ber performance improvement in multicarrier systems. *IEEE Trans. Commun.*, 52(10):1658–1663, 2004.

[83] D.G. Luenberger and Y. Ye. *Linear and Nonlinear Programming*. Int. Series in Operations Research & Manage. Sci. Springer, 2008.

[84] L. Brunel. Multiuser detection techniques using maximum likelihood sphere decoding in multicarrier cdma systems. *IEEE Trans. Wireless Commun.*, 3(3):949–957, May 2004.

[85] Jung-Bin Kim and Dongwoo Kim. Comparison of two snr-based feedback schemes in multiuser dual-hop amplify-and-forward relaying networks. *IEEE Commun. Lett.*, 12(8):557–559, 2008.

[86] Raymond H.Y. Louie, Yonghui Li, and B. Vucetic. Practical physical layer network coding for two-way relay channels: performance analysis and comparison. *IEEE Trans. Wireless Commun.*, 9(2):764–777, February 2010.

[87] T.J. Oechtering and H. Boche. Optimal time-division for bidirectional relaying using superposition encoding. *IEEE Commun. Lett.*, 12(4):265–267, April 2008.

[88] S.S. Ikki and S. Aissa. Performance analysis of two-way amplify-and-forward relaying in the presence of co-channel interferences. *IEEE Trans. Commun.*, 60(4):933–939, April 2012.

[89] E. Soleimani-Nasab, M. Matthaiou, M. Ardebilipour, and G.K. Karagiannidis. Two-way af relaying in the presence of co-channel interference. *IEEE Trans. Commun.*, 61(8):3156–3169, August 2013.

[90] Lingyang Song. Relay selection for two-way relaying with amplify-and-forward protocols. *IEEE Trans. Veh. Technol.*, 60(4):1954–1959, May 2011.

[91] Weiping Liu and Liang Yang. Performance analysis for two-way relaying networks with and without relay selection. *Wireless Personal Communications*, 75(4):2485–2494, 2014.

[92] Ian F. Akyildiz, Won-Yeol Lee, Mehmet C. Vuran, and Shantidev Mohanty. Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Elsevier J. Comput. Networks*, 50:2127–2159, 2006.

[93] L. Yang, K. Qaraqe, E. Serpedin, and X. Gao. Performance analysis of two-way relaying networks with the n-th worst relay selection over various fading channels. *IEEE Trans. Veh. Technol.*, 64(7):3321–3327, July 2015.

[94] Yulong Zou, Xianbin Wang, Weiming Shen, and L. Hanzo. Security versus reliability analysis of opportunistic relaying. *IEEE Trans. Veh. Technol.*, 63(6):2653–2661, July 2014.

[95] M. Karimi and M. Nasiri-Kenari. Outage analysis of relay-assisted free-space optical communications. *IET Commun.*, 4(12):1423–1432, August 2010.

[96] P. Puri, P. Garg, and M. Aggarwal. Outage and error rate analysis of network-coded coherent twr-fso systems. *IEEE Photonics Technol. Lett.*, 26(18):1797–1800, September 2014.

[97] M.A. Kashani, M.M. Rad, M. Safari, and M. Uysal. All-optical amplify-and-forward relaying system for atmospheric channels. *IEEE Commun. Lett.*, 16(10):1684–1687, October 2012.

[98] M.R. Bhatnagar. Performance analysis of decode-and-forward relaying in gamma-gamma fading channels. *IEEE Photonics Technol. Lett.*, 24(7):545–547, April 2012.

[99] I.S. Ansari, F. Yilmaz, and M.-S. Alouini. On the performance of mixed rf/fso variable gain dual-hop transmission systems with pointing errors. In *Proc. IEEE Veh. Tech. Conf. (VTC'13-Fall)*, pages 1–5, Las Vegas, USA, 2-5 September 2013.

[100] N.I. Miridakis, M. Matthaiou, and G.K. Karagiannidis. Multiuser relaying over mixed rf/fso links. *IEEE Trans. Commun.*, 62(5):1634–1645, May 2014.

[101] P. Puri, P. Garg, M. Aggarwal, and P.K. Sharma. Multiple user pair scheduling in bi-directional single relay assisted fso systems. In *Proc. IEEE Int'l Conf. on Commun. (ICC)*, pages 3401–3405, Sydney, Australia, 10-14 June 2014.

[102] F.J. Lopez-Martinez, G. Gomez, and J.M. Garrido-Balsells. Physical-layer security in free-space optical communications. *IEEE Photonics J.*, 7(2):1–14, April 2015.

[103] Hu Jin, Won-Yong Shin, and Bang Chul Jung. On the multi-user diversity with secrecy in uplink wiretap networks. *IEEE Commun. Lett.*, 17(9):1778–1781, September 2013.

[104] Xin Ge, Peiran Wu, Hu Jin, and Victor C.M. Leung. Secrecy analysis of multiuser downlink wiretap networks with opportunistic scheduling. In *Communications (ICC), 2015 IEEE International Conference on*, pages 7370–7375, June 2015.

[105] Yulong Zou, Xianbin Wang, and Weiming Shen. Physical-layer security with multiuser scheduling in cognitive radio networks. *IEEE Trans. Commun.*, 61(12):5103–5113, December 2013.

[106] Yulong Zou, Xuelong Li, and Ying-Chang Liang. Secrecy outage and diversity analysis of cognitive radio systems. *IEEE J. Sel. Areas Commun.*, 32(11):2222–2236, November 2014.

[107] Yulong Zou, B. Champagne, Wei-Ping Zhu, and L. Hanzo. Relay-selection improves the security-reliability trade-off in cognitive radio systems. *IEEE Trans. Commun.*, 63(1):215–228, January 2015.

[108] M.O. Hasna and M.-S. Alouini. End-to-end performance of transmission systems with relays over rayleigh-fading channels. *IEEE Trans. Wireless Commun.*, 2(6):1126–1131, November 2003.

[109] I. S. Gradshteyn and I. M. Ryzhik. *Table of Integrals, Series and Products.* San Diego, CA: Academic, 2000.

[110] S.S. Ikki and S. Aissa. A study of optimization problem for amplify-and-forward relaying over weibull fading channels with multiple antennas. *IEEE Commun. Lett.*, 15(11):1148–1151, November 2011.

[111] M. K. Simon and M.-S. Alouini. *Digital Communication over Fading Channels.* Wiley, 2nd ed. edition, 20005.

[112] *The Wolfram functions site.* 2013.

[113] Liang Yang, Xiqi Gao, and M.-S. Alouini. Performance analysis of relay-assisted all-optical fso networks over strong atmospheric turbulence channels with pointing errors. *J. Lightw. Technol.*, 32(23):4613–4620, December 2014.

[114] M.R. McKay, A.J. Grant, and I.B. Collings. Performance analysis of mimo-mrc in double-correlated rayleigh environments. *IEEE Trans. Commun.*, 55(3):497–507, March 2007.

[115] A. Lapidoth, S.M. Moser, and M.A. Wigger. On the capacity of free-space optical intensity channels. *IEEE Trans. Inf. Theory*, 55(10):4449–4461, October 2009.

[116] Hang Long, Wei Xiang, Jing Wang, Yueying Zhang, and Wenbo Wang. Cooperative jamming and power allocation with untrusty two-way relay nodes. *IET Commun.*, 8(13):2290–2297, September 2014.

[117] G.T. Djordjevic, M.I. Petkovic, A.M. Cvetkovic, and G.K. Karagiannidis. Mixed rf/fso relaying with outdated channel state information. *IEEE J. Sel. Areas Commun.*, PP(99):1–1, 2015.

[118] Jemin Lee, Hano Wang, J.G. Andrews, and Daesik Hong. Outage probability of cognitive relay networks with interference constraints. *IEEE Trans. Wireless Commun.*, 10(2):390–395, 2011.

[119] José María Garrido-Balsells, Antonio Jurado-Navas, José Francisco Paris, Miguel Castillo-Vázquez, and Antonio Puerta-Notario. General analytical expressions for the bit error rate of atmospheric optical communication systems: erratum. *Opt. Lett.*, 39(20):5896–5896, Oct 2014.

[120] S.S. Ikki and S. Aissa. Performance analysis of dual-hop relaying systems in the presence of co-channel interference. In *Proc. IEEE Global Telecom. Conf. (GLOBECOM 2010),*, pages 1–5, Dec 2010.

[121] A.M. Salhab, F. Al-Qahtani, S.A. Zummo, and H. Alnuweiri. Outage analysis of n^{th}-best df relay systems in the presence of cci over rayleigh fading channels. *IEEE Commun. Lett.*, 17(4):697–700, April 2013.

[122] Ling Tang, Xiaowen Gong, Jianhui Wu, and Junshan Zhang. Secure wireless communications via cooperative relaying and jamming. In *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, pages 849–853, Dec 2011.

[123] Xiyuan Wang, Kun Wang, and Xian-Da Zhang. Secure relay beamforming with imperfect channel side information. *IEEE Trans. Veh. Technol.*, 62(5):2140–2155, Jun 2013.

[124] Xiangyun Zhou, Meixia Tao, and R.A. Kennedy. Cooperative jamming for secrecy in decentralized wireless networks. In *Communications (ICC), 2012 IEEE International Conference on*, pages 2339–2344, June 2012.

[125] Bo Wang, Pengcheng Mu, and Zongze Li. Secrecy rate maximization with artificial-noise-aided beamforming for miso wiretap channels under secrecy outage constraint. *IEEE Commun. Lett.*, 19(1):18–21, January 2015.

[126] Tran Trung Duy, T.Q. Duong, Tu Lam Thanh, and Vo Nguyen Quoc Bao. Secrecy performance analysis with relay selection methods under impact of co-channel interference. *IET Commun.*, 9(11):1427–1435, 2015.

[127] A.A. Abu-Dayya and N.C. Beaulieu. Outage probabilities of cellular mobile radio systems with multiple nakagami interferers. *IEEE Trans. Veh. Technol.*, 40(4):757–768, November 1991.

[128] FawazS AI-Qahtani, Caijun Zhong, KhalidA Qaraqe, Hussein AInuweiri, and Tharm Ratnarajah. Performance analysis of fixed-gain af dual-hop relaying systems over nakagami-m fading channels in the presence of interference. *EURASIP J. Wireless Comm. and Networking*, 2011(1), 2011.

Vitae

- Name: Ahmed Hassan Abd El-Malek
- Nationality: Egyptian
- Date of Birth: June 10, 1985
- Email: *ahmedhassan@kfupm.edu.sa*
- Permenant Address: Alexandria, Egypt.
- Education:
  - M.Sc. in Electrical Engineering, November 2010, Alexandria University, Alexandria, Egypt

    Thesis Title: New Trends in Space Time Error Correcting Codes

    Major: Communications.
  - B.Sc. in Electrical Engineering (Distinction with degree of Honor), June 2007, Alexandria University, Alexandria, Egypt

    Major: Communication and Electronics.

- Publications:

Refereed Journal Publications

  - **Ahmed H. Abd El-Malek** and Salam A. Zummo, ″A bandwidth Efficient Cognitive Radio with Two-Path Amplify-and-Forward Relaying,″ IEEE Wireless Commun. Lett., vol. 4, no. 1, pp. 6669, February 2015.
  - **Ahmed H. Abd El-Malek**, Fawaz Al-Qahtani, Trung Q. Duong, Salam A. Zummo, and Hussein Alnuweiri,″MIMO Cognitive Relay Networks with Correlated Antennas over Rayleigh Fading Channels,″ IEEE Trans. Veh. Technol., accepted, June 2015.
  - **Ahmed H. Abd El-Malek**, Fawaz Al-Qahtani, Salam A. Zummo, and Hussein Alnuweiri, ″Transmit Antenna Selection of Correlated MIMO Multiuser Cognitive Radio Networks in Nakagami-m Fading Channels,″ Accepted in Wireless Commun. and Mobile Computing, Wiley, January 2016.

Refereed Conference Publications

  - **Ahmed H. Abd El-Malek**, Anas M. Salhab, Salam A. Zummo and Mohamed-Slim Alouini ″Security and Reliability Analysis of Diversity Combining Technqiues in SIMO Mixed RF/FSO with Multiple Users., ″ Accepted in the workshop on wireless physical layer security, IEEE Int'l Conf. on Commun.(ICC'16), Kuala Lumpur, Malaysia, May 2016.
  - **Ahmed H. Abd El-Malek**, Anas M. Salhab and Salam A. Zummo,

″Enhancing Spectral Efficiency in Cooperative Cognitive Two-Way Amplify-and-Forward Relaying Networks, ″ Accepted in IEEE Wireless Commun. and Networking Conf. (WCNC'16), Doha, Qatar, April 2016.

– **Ahmed H. Abd El-Malek** and Salam A. Zummo, ″Cooperative Cognitive Radio Model for Enhancing Physical Layer Security in Two-Path Amplify-and-Forward Relaying Networks,″ in Proc. IEEE Global. Commun. Conf. (GLOBECOM15), San Diego, CA, USA, December 2015.

– **Ahmed H. Abd El-Malek**, Anas M. Salhab and Salam A. Zummo, ″Optimal Power Allocation for Enhancing Physical Layer Security in Opportunistic Relay Networks in the Presence of Co-Channel Interference,″ in Proc. IEEE Global Commun. Conf. (GLOBECOM15), San Diego, CA, USA, December 2015.

– **Ahmed H. Abd El-Malek** and Salam A. Zummo, ″A Cooperative Model for Enhancing Spectral Efficiency in Two-Way Amplify-and-Forward Relaying Networks,″ Accepted in IEEE 82nd Veh. Technol. Conf. (VTC-Fall'15), Boston, USA, September 2015.

– **Ahmed H. Abd El-Malek**, Fawaz Al-Qahtani, Salam A. Zummo, and Hussein Alnuweiri, ″MIMO Multiuser Cognitive Relay Network in Spectrum Sharing Environment with Antenna Correlation over Rayleigh Fading Channels,″ in Proc. IEEE Wireless Commun. and

Networking Conf. (WCNC'15), New Orleans, LA, USA, March 2015.

- **Ahmed H. Abd El-Malek**, Fawaz Al-Qahtani, Salam A. Zummo, and Hussein Alnuweiri, ″Cognitive Multiuser MIMO in Spectrum Sharing Environment with Antenna Correlation over Nakagami-m Fading,″ in Proc. IEEE Veh. Technol. Conf. (VTC-Fall'14), Vancouver, BC, Canada, September 2014.
- **Ahmed H. Abd El-Malek**, Fawaz Al-Qahtani, Salam A. Zummo, and Hussein Alnuweiri, ″TAS/MRC in Cognitive Relay Networks over Rayleigh Fading Channels with Correlated Antennas,″ in Proc. IEEE Int'l Conf. on Commun., (ICC14), Sydney, Australia, June 2014.