Power Optimized Relay Selection and Jamming for Security Enhancement in Cooperative Networks

A Thesis

Submitted by

Shemi P M

Reg. No. 4861

for the award of the degree of

Doctor of Philosophy

Division of Electronics Engineering
School of Engineering
Cochin University of Science and Technology
Kochi, India

December 2019

....dedicated to my parents

School of Engineering
Cochin University of Science and Technology
Kochi, India

Dr. Jibukumar M. G. Ph: +91 9497683331
Professor Email: jibukumar@cusat.ac.in

Certificate

This is to certify that the thesis entitled **Power Optimized Relay Selection and Jamming for Security Enhancement in Cooperative Networks** submitted by Ms. Shemi P M to the Cochin University of Science and Technology for the award of the degree of Doctor of Philosophy is a bonafide record of research work carried out by her under my supervision and guidance at the Division of Electronics Engineering, School of Engineering, Cochin University of Science and Technology, Kochi. The contents of this thesis, in full or in parts, have not been submitted to any other University or Institute for the award of any degree or diploma.

I further certify that the corrections and modifications suggested by the audience during the pre-synopsis seminar and recommended by the Doctoral Committee have been incorporated in the thesis.

Place: Kochi
Date : 11.12.2019

Dr. Jibukumar M G
Research Guide

DECLARATION

I hereby declare that the work presented in the thesis entitled **Power Optimized Relay Selection and Jamming for Security Enhancement in Cooperative Networks** is based on the original research work carried out by me under the supervision and guidance of Dr. Jibukumar M G, Professor, Division of Electronics Engineering, School of Engineering, Cochin University of Science and Technology for the award of degree of Doctor of Philosophy with Cochin University of Science and Technology. I further declare that the contents of this thesis in full or in parts have not been submitted to any other University or Institute for the award of any degree or diploma.

Place: Kochi **Shemi P M**

Date: 11.12.2019

ACKNOWLEDGEMENTS

First of all, I bow before THE ALMIGHTY for all the blessings. Only with His blessings, I could bring all my efforts to a successful completion.

I would like to express my sincere gratitude to my supervisor, Dr. Jibukumar M G, Professor, Division of Electronics Engineering, School of Engineering, Cochin University of Science and Technology, for his valuable guidance, scholarly inputs and consistent encouragement I received throughout the research work. Without his help the thesis could have never been completed. He has always made himself available to clarify my doubts despite his busy schedules and I consider it as a great opportunity to do my doctoral programme under his guidance and to learn from his research expertise.

I would like to extend my gratitude to Dr. Abdulla P, my Doctoral Committee member, Dr. M. R. Radhakrishna Panicker, Principal, School of Engineering and Dr. Beena K S, Dean, Faculty of Engineering for their support and guidance during the course of the work. I would like to thank all the faculty members and staff of Division of Electronics Engineering, School of Engineering for their support and help during my research.

I also extend my sincere thanks to Dr. A. Biju, Principal, M E S College Maramapally for his constant encouragement and support. Gratitude is also extended to all the management committee members of M E S College Marampally.

I am grateful to my friend and mentor, Dr. Sabu M K, Professor and Head, Department of Computer Applications, Cochin University of Science and Technology for his countless and selfless help since the very first day I joined research till the day of final thesis submission. With his guidance, I have always felt confident enough to overcome any difficulty I faced during my research.

I would like to make a special mention of the selfless support and guidance I received from my colleagues Dr. Raphika P M and Dr. Jasmine P M during my study. I gained a lot from them through their scholarly interactions at various points of my research programme. I thank all my colleagues of Department of Electronics, MES College Marampally for their unconditional support during my research.

I am grateful to Dr. Bindu P and Mr. Biju K S for their valuable contributions and timely help. I remember with gratitude the help and contributions from my co-researchers, Mr. Premkumar C V, Ms. Sethu Lakshmi P, Ms. Nivea Kesav, Ms. Tripti C. and Ms. Shamla B and M Tech Scholars Ms. Neenu V S and Ms. Roshan Anna John. I would like to thank all of them for making my hours of work in the lab enjoyable with their endless companionship and help as well.

I would like to thank my friends Ms. Jaseena K U, Ms. Baby A K, and Ms. Shabana Basheer who have contributed their support, ideas and time towards the successful completion of this work.

I am extremely grateful to the University Grants Commission for giving me the opportunity to do the research by availing the faculty development programme.

I would like to express my utmost gratitude to my parents, sister and brother for their love and support, which have been a source of great comfort and energy throughout my study.

I am very much indebted to my husband Dr. Ali M A and my children Nashik, Nihala and Nahla for their spirit of love, patience and encouragement which gave me the courage to persevere.

Shemi P M

ABSTRACT

Secure transmission is a fundamental concern in wireless communications. Wireless communication systems are particularly vulnerable to security attacks because of the inherent openness of the transmission medium. Physical layer security (PLS) has recently become an emerging technique to complement and significantly improve the communication security of wireless networks. Compared to cryptographic approaches, PLS is a fundamentally different paradigm where secrecy is achieved by exploiting the physical layer properties of the communication system, such as thermal noise, interference and the time-varying nature of fading channels. Different from the upper layer security, secret key is not needed in physical layer security; resulting in low complexity, low energy cost, which makes it more suitable for wireless systems.

Cooperative communication based on relaying nodes has been considered as a promising technique to enhance the PLS performance against eavesdropping. Among the proposed PLS solutions; cooperative relaying, cooperative jamming and a combination of these two techniques have recently attracted research interest. In this thesis, physical layer attacks of the cooperative communication systems are studied and security enhancement techniques using cooperative relaying and jamming schemes are investigated. Since multiple relays consume system resources and power in cooperative relaying, it is important to select one relay among the available candidates to maximize the cooperation benefits. Various relay selection techniques available in the literature are analysed and the thesis proposed a novel relay selection scheme based on the probability of path selection criterion of Ant Colony Optimization algorithm. This method helps to analyse the secrecy performance in three wireless scenarios namely traditional, fading and path loss models.

Although relay selection improves resource utilization, it will not always guarantee perfect secrecy as the secrecy will be degraded with poor legitimate channel conditions. To overcome this problem, the thesis proposed two jamming schemes, *i)* source and relay based jamming (SRBJ), which uses two independent jamming signals and *ii)* source based jamming scheme (SBJ) with single jamming signal in order to degrade the eavesdropper. The complexity with SRBJ scheme is reduced in SBJ. The thesis also proposed a source based jamming scheme to enhance the secrecy of practical wireless networks consisting of multiple untrusted relays with external eavesdroppers.

In cooperative jamming, the system performance is highly dependent on both the jamming strategy as well as the jamming power level. If the power allocated to jamming signal is too low, the received signal at the eavesdropper cannot be degraded sufficiently. On the other hand, if the jamming power is too high, the received signal at the destination will be degraded. Thus, it is essential to assign optimal power to the jamming signals. Hence an optimal power allocation (OPA) based on gradient-free optimization method namely; Nelder-Mead algorithm is proposed to derive the optimal power allocation factors for the jamming scheme, which overcomes the problems with conventional gradient-based optimization methods. The performance as well as the complexity of the proposed OPA based schemes/algorithm is evaluated through simulations using MATLAB and R Programming. The results revealed a significant performance improvement over other transmission schemes and optimization methods.

Keywords: physical layer security, secrecy capacity, amplify-and-forward, Ant Colony Optimization, Nelder-Mead algorithm, optimal power allocation.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

ACO	Ant Colony Optimization
AF	Amplify-and-Forward
AN	Artificial Noise
BRS	Best Relay Selection
CC	Coded Cooperation
CDI	Channel Distribution Information
CF	Compress-and-Forward
CJ	Cooperative Jamming
CN	Complex Noise
CR	Cooperative Relaying
CSI	Channel State Information
DBJ	Destination Based Jamming
DF	Decode-and-Forward
DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service
ECSI	Eavesdropper Channel State Information
EPA	Equal power allocation
ES	Exhaustive Search
ESR	Ergodic Secrecy Rate
ESSR	Ergodic Secrecy Sum Rate
GB	Gradient Based
IAF	Incremental Amplify-and-Forward
ICSI	Instantaneous Channel State Information
IDF	Incremental Decode-and-Forward

LAN	Local Area Networks
MAC	Medium Access Control
MER	Main-to-Eavesdropper Ratio
MIMO	Multiple-Input Multiple- Output
MR	Multiple Relays
MRC	Maximal Ratio Combining
NF	Noise-Forwarding
NM	Nelder Mead algorithm
OFDMA	Orthogonal Frequency-Division Multiple Access
OPA	Optimal Power Allocation
ORS	Optimal Relay Selection
PA	Power Allocation
PLS	Physical Layer Security
PRS	Partial Relay Selection
QoS	Quality of Service
RS	Relay Selection
SC	Selection Combining
SBJ	Source Based Jamming
SCSI	Statistical Channel State Information
SNR	Signal-to-Noise Ratio
SOP	Secrecy Outage Probability
SR	Secrecy Rate
SRBJ	Source and Relay Based Jamming
TDMA	Time Division Multiple Access
UT	Untrusted
WC	Worst Case

NOTATIONS

P	Total transmit power
P_s	Source power
P_r	Relay power
G	Channel gain
h	Fading coefficients
R_s	Secrecy rate
σ^2	Noise variance
a, a_s, a_r	Power allocation factors
x_s	Information from the source
n_z	Jamming signal
n_i	Additive noise at i^{th} node
G_o	Carrier wavelength
d_{ij}	Distance between nodes i and j
d_o	Reference distance
L	Path loss coefficient
g	Amplification factor (AF)
y_i	Received signal at i^{th} node
γ	Signal-to-noise ratio
R_i	Transmission rate at i^{th} node
$\hat{x}_s$	Decoded signal
N	Number of relay nodes
δ	Step size in exhaustive search algorithm
m	Number of iterations in exhaustive search algorithm
B	Bandwidth
C_s	Secrecy capacity
Cm	Channel capacity of main link

C_w	Channel capacity of wiretap link
E {.}	Expectation of a function
α & β	Relevance parameters in ACO algorithm
$\tau_{i,j}$	Amount of pheromone on edge *i, j* (ACO algorithm)
η	Heuristic information between *i* and *j* (ACO algorithm)
$P_{i,j}$	Probability of signal transmitted from *i* to *j*
ρ	*Reflection parameter* (NM algorithm)
ψ	*Expansion parameter* (NM algorithm)
ε	*Contraction* parameter (NM algorithm)
γ	*Shrinking parameter* (NM algorithm)
$\overline{x}$	Centroid
Δ	Simplex (NM algorithm)
n	Number of variables to be optimized in NM algorithm

Chapter 1
Introduction

1.1 Motivation

In present communication scenario, security and privacy of data being transmitted is critical due to the broadcast nature of wireless medium. Traditionally, the issue of information security has been primarily addressed at the upper layers of the protocol stack (e.g., the network layer) using cryptographic algorithms. However, there are several significant challenges for cryptographic approaches in wireless networks, like, complexity and security issues in key distribution and management, complex encryption and decryption algorithms etc. As a result, physical layer security emerges as an alternative means to achieve perfect transmission secrecy in wireless networks. Different from the upper layer security, secret key is not needed in physical layer security; resulting in low complexity, low energy cost, which makes it more suitable for wireless systems.

Diversity techniques in wireless communication systems are exploited to increase the transmission reliability and wireless security. Several diversity approaches like multiple-input multiple-output (MIMO), multiuser and cooperative diversity techniques to improve wireless physical layer security are available in the literature (L. Dong *et al.*, 2010; F. Oggier and B. Hassibi, 2011; L. Fan *et al.*, 2014; Y. Zou *et al.*, 2015). The MIMO and multiuser diversity techniques are generally applicable to various cellular and WiFi networks, since they typically consist of multiple users, and, such

devices are equipped with multiple antennas. On the other hand, the cooperative diversity mechanism is applicable to some advanced cellular and WiFi networks that have adopted the relay architecture, such as the Long Term Evolution Advanced system (LTE-A) and IEEE 802.16j/m, where relay stations are introduced to assist wireless data transmission (Y. Zou et al., 2015).

Multiuser diversity techniques employ user scheduling in multiuser wireless channels which allows the base station to select high quality channel users to transmit information. Orthogonal multiple access mechanisms such as orthogonal frequency-division multiple access (OFDMA) and time-division multiple access (TDMA) are used for information transmission (Y. Zou *et al.*, 2015). In MIMO systems, multiple antennas are used at the transceiver which increases data rate and reliability of the wireless link. However, using multiple co-located antennas cause degradation in the system Quality of service (QoS) due to correlation between them. Also, due to size, cost, or hardware limitations, small handheld wireless devices may not be able to support multiple antennas. To overcome the above drawback, cooperative communication has been introduced to exploit the benefit of MIMO in a distributed manner. Security enhancement exploiting cooperative diversity techniques are addressed in the thesis.

The ultimate aim of the cooperative communication is to transmit the signal from source to destination securely against the attacks of eavesdropper. To secure and protect the confidentiality of data being transmitted, physical layer security offers cooperative diversity solutions like cooperative relaying and jamming schemes.

Cooperative relaying protocol increases the main channel capacity whereas jamming techniques degrade the wiretap channel capacity. In either case the secrecy of the cooperative wireless network is enhanced. In cooperative relaying scheme, the total energy-efficiency is limited since the relays consume the system resources and power. It is therefore important to select one relay among the available candidates to maximize the cooperation benefits. Relay selection techniques can overcome the inefficient spectral usage of cooperative relays.

Although relay selection scheme improves the resource utilization, it will not always guarantee perfect secrecy as the secrecy will be degraded with poor legitimate channel conditions. Cooperative jamming is an alternative to this problem. In cooperative jamming scheme, the power allocated to the jamming signal should be high enough to interrupt the received signal at the eavesdropper; however allocating too much power on the jamming signal can degrade the signal quality at the destination. Thus, it is essential to assign optimal power to the jamming signals so as to maximize the secrecy rate (L. Dong *et al.*, 2010). Literature review has thus revealed the necessity of low complexity power optimized model for cooperative wireless networks using cooperative relaying and jamming schemes.

1.2 Research Objectives

The aim of the research is to develop a power optimized cooperative network model that enhances the privacy concepts of physical layer security. The following specific objectives are identified to achieve the aim.

i. To comprehensively study the physical layer security of cooperative communication systems in terms of security attacks. To investigate the existing security enhancement techniques in wireless cooperative communication systems - various cooperative relaying and jamming protocols, power optimization algorithms for secrecy rate maximization etc. and to address the merits and demerits of the current schemes.

ii. To provide a power optimized solution for two-hop cooperative networks which resolves the limitations of conventional cooperative relaying and jamming schemes.

iii. To develop a low complex and power optimized secrecy enhancement solution via relay selection and different jamming techniques for two-hop cooperative networks where power consumption and complexity considerations are well noted.

iv. To validate the performance of the optimized model through analytical modelling and simulations.

1.3 Thesis Contributions

Major contributions of the thesis based on the proposed physical layer security enhancement solutions for cooperative communication systems are stated below.

- A novel relay selection technique based on the probability of path selection criterion of Ant Colony Optimization algorithm is proposed for two-hop amplify-and-forward and decode-and-forward cooperative relaying networks and a performance comparison is formulated. Unlike conventional relay selection

techniques, the proposed method helps to analyse the secrecy performance in three wireless scenarios namely traditional, fading and path loss models; considering the channel gain and fading coefficients defining the channels separately. Analysis is carried out for the two relay selection schemes namely best relay selection (BRS) and partial relay selection (PRS). The performance based on secrecy rate (R_s) is evaluated for $\boldsymbol{N}$ trusted relays distributed randomly between the source and destination and for different eavesdropper position. The performance comparison of optimal power allocation (OPA) based on gradient method and exhaustive search algorithms and equal power allocation (EPA) strategies are also studied. The impact of number of relaying nodes on the secrecy is also evaluated. Numerical results show the merits of the proposed relay selection scheme in terms of secrecy rate in different wireless scenarios as compared to traditional schemes.

- Relay selection techniques will not always guarantee perfect secrecy because the secrecy rate will reduce or even drop to zero when the legitimate channel conditions are poor or when the eavesdroppers appear near to source. To overcome this problem, two jamming schemes are proposed. While using jamming signals, powers should be allocated optimally. So, an optimal power allocation scheme based on Nelder-Mead algorithm is proposed for an amplify-and-forward cooperative network with multiple trusted relays employing source and relay based jamming scheme (SRBJ); and secrecy performance in traditional, path loss and fading model wireless scenarios are

analysed. The source and relay based jamming scheme uses two different jamming signals at the source and selected relay in order to degrade the eavesdropper. The performance of the proposed power optimization algorithm is compared with gradient-based and three-dimensional exhaustive search algorithms and its complexity analysis is also carried out. The conventional AF scheme and the secrecy performance with EPA strategy are also derived for comparison. The effect of relay location on secrecy is also examined for both schemes and the impact of single and multiple relays on secrecy are also evaluated. It is observed from the numerical results that the proposed optimization algorithm provides better performance compared with other optimization methods and also with conventional transmission schemes. But the limitations of this model are *i)* the complexity in generating and processing two jamming signals and *ii)* with the nature of the relays; the jamming signal from the source can be removed only if the relays are considered trusted.

- The problems with SRBJ scheme can be overcome by employing cooperative jamming scheme with single jamming signal and by considering multiple trusted and untrusted relaying strategies. In heterogeneous networks or in practical scenarios, the assistance of the intermediate relaying node is essential to convey a confidential message. In such cases, the relays may not be authenticated and have a lower security clearance in the network; hence it is not trusted with the information it is relaying. Untrusted relays can be observed as

beneficial nodes as well as potential eavesdroppers. So, to reduce the power consumption and complexity with source and relay based jamming scheme, a source based jamming (SBJ) that uses single jamming signal is proposed. Scenario with multiple trusted amplify-and-forward relays is addressed in chapter 5 and that with untrusted relays is addressed in chapter 6. In both cases, power optimization for maximizing the secrecy is done by using Nelder-Mead algorithm. The relay selection which uses ACO path probability criterion helps the secrecy performance analysis in there wireless scenarios. Gradient-based and two-dimensional exhaustive search algorithms for power optimization are derived for comparison. Numerical results reveal that the proposed OPA schemes show better performance compared with other optimization methods, conventional transmission schemes and EPA strategy.

1.4 Thesis Outline

The thesis is organized as follows:

Chapter 2 presents a review of literature on physical layer security strategies where various diversity techniques like cooperative relaying protocols, relay selection schemes, cooperative jamming techniques are reviewed. Cooperative networks with trusted and untrusted relaying schemes with power allocation problems are also presented.

Chapter 3 presents a novel relay selection algorithm for secrecy enhancement in two-hop cooperative wireless networks. The system

model is addressed in this chapter. Partial relay selection and best relay selection analysis in three wireless scenarios namely traditional, fading and path loss models, employing AF and DF transmission protocols are presented. Traditional PRS and BRS schemes are used as benchmark schemes for comparison. The performance comparison of OPA based on gradient method and exhaustive search algorithms and EPA strategies are also studied. The simulation results supporting the proposed scheme are also provided.

Chapter 4 presents the power optimized source and relay based jamming scheme for security enhancement in amplify-and-forward relaying network. The OPA factors for secrecy rate maximization are derived using Nelder-Mead algorithm and its complexity analysis is also presented. Simulation results are presented to compare the performance of the proposed scheme with conventional AF, direct transmission without and with jamming schemes, and EPA schemes and also with other optimization methods.

Chapter 5 presents a power optimized source based jamming (SBJ) for trusted amplify-and-forward relaying scheme. Nelder-Mead algorithm is used for power optimization. The benchmark schemes used for comparison are SRBJ, conventional AF, direct transmission scheme without and with jamming and also with gradient-based optimization and exhaustive search algorithms. The simulation results illustrate the performance comparison with different benchmark schemes.

Chapter 6 presents a power optimized source based jamming scheme

for a cooperative network with multiple untrusted amplify-and-forward relays and an external eavesdropper. Performance comparison of the proposed scheme with worst-case untrusted scenario, EPA strategy and other optimization methods are presented. Finally, simulation results are presented which validate the theoretical contributions.

Chapter 7 concludes with the key information addressed in all the chapters of the thesis. In addition, a brief discussion on the possible extensions of the work is presented as well.

Chapter 2
Literature Review

2.1 Physical Layer Security

Secure transmission is a fundamental concern in wireless communications. The concept of information theoretic security has been introduced by C. E. Shannon (1949), where cryptographic protocols have been implemented to provide security in the upper layers (e.g., the network layer), based on the assumption of an error-free link in the physical layer. In wireless scenarios, the distribution and management of secret key in cryptographic algorithms is expensive as well as vulnerable to attacks (B. Schneier, 1998). Wireless systems are mostly vulnerable to attacks because of the openness of the transmission medium. Physical layer security (PLS) has recently become an emerging technique to complement and significantly improve the security of wireless networks. Compared to cryptographic approaches, in PLS, secrecy is achieved by using the physical layer characteristics of the wireless channel, such as thermal noise, interference and the time-varying nature of fading channels.

The concept of PLS was introduced by A. D. Wyner (1975), where a discrete memory-less wiretap channel in the presence of an eavesdropper was examined and he found out that a perfectly secure communication could be attained if the wiretap channel is degraded. The results of Wyner's work were later extended to Gaussian wiretap channel (S. K. Leung-Yan-Cheong and M. E. Hellman, 1978), where secrecy capacity, the difference between the channel capacities of the

main and wiretap channels is developed. It has been proved that perfect secrecy is achieved if the secrecy capacity is positive; i.e., the transmission from source to destination can be perfectly secure when the main channel capacity is greater than the wiretap channel capacity. If the secrecy capacity falls below zero, the transmission becomes insecure and the eavesdropper can succeed in capturing the source transmission. In (I Csiszar and J Korner, 1978; Liang Y *et al.*, 2008), the secrecy capacity of the Gaussian wiretap channel was extended to signal transmission over the broadcast and wireless fading channels respectively. However, in wireless communications, secrecy capacity is severely degraded due to the fading effect.

A systematic overview of the basic concepts, recent advancements, and open issues in providing communication security at the physical layer is presented in (Xiangyun Zhou *et al.*, 2013). It also introduces the key concepts, design issues, and solutions to PLS in single-user and multi-user communication systems as well as large-scale wireless networks. In (Raef Bassily *et al.*, 2013), a summary of the recent advances in the area of wireless PLS is given, that guarantees confidentiality by using cooperative techniques unique to the wireless medium.

2.2 Wireless Security Requirements

In wireless networks, owing to the broadcast nature of the wireless medium, the information exchanged among legitimate users is vulnerable to various threats. Secure wireless communications should satisfy certain requirements like authenticity, confidentiality, integrity, and availability (C. S. R. Murthy and B. S. Manoj, 2004), in

order to protect the wireless transmissions against security attacks. These are detailed as follows:

2.2.1 Authenticity

Authenticity refers to the true identity of a network node in order to distinguish authorized users from unauthorized users. In wireless networks, a pair of communicating nodes should first perform mutual authentication before establishing a communication link (Y. Jiang *et al.*, 2006). A network node is equipped with a wireless network interface card and has a unique media access control (MAC) address, which can be used for authentication purposes.

2.2.2 Confidentiality

Confidentiality refers to limiting the data access to intended users only, while preventing the information disclosure to unauthorized entities (W. Stalling, 2010). Primarily, cryptography and encryption techniques have been utilized in upper layers of protocol stack to provide confidentiality. Recently, PLS has emerged as a means of protecting the confidentiality of wireless transmission against eavesdropping attacks.

2.2.3 Integrity

Data integrity is to ensure that the received data has not been altered or modified during data transmission. It is significantly important to detect any alternation or manipulation in the data packets with the least amount of latency and false alarm rate. Man in the middle attacks may target the data integrity as they overhear the communication and they may set up new communication routes and

insert corrupted packets (AJ Menezes et al., 1996).

2.2.4 Availability

Availability is ensuring that legitimate entities can access the network and have a robust communication (Yis Shiu et al., 2011). For instance, denial of service (DoS) and distributed denial of service (DDoS) attacks may target the availability of a network which occupies the network resources and this result in DoS for authorized nodes.

2.3 Security Attacks in Wireless Communication System

The most common attacks in wireless networks can be classified into two categories: passive and active (W. Stalling, 2010). Passive attacks do not disrupt network operation; instead the adversary steals transmitted information from wireless channels. Eavesdropping and traffic analysis are the two types of passive attacks. For the case of active attacks the adversary significantly interferes with normal network operations and tries to alter the network data. Active attacks include DoS attacks, masquerade attacks, replay attacks, information disclosure and message modification attacks (Yi S Shiu et al., 2011).

2.3.1 Passive Attacks

Eavesdropping

An eavesdropping attack is an intrusion where someone tries to steal information that computers, smartphones, or other devices transmit over a network. An email message, telephonic conversation, or a transferred file may contain confidential information and it is necessary to secure the data so as to prevent the eavesdroppers from

learning the contents of these transmissions. Encryption is the most common technique for protecting the important information. Though eavesdropper can intercept the transmitted signal it cannot obtain any critical information from the encrypted data.

Traffic analysis

Traffic analysis is used to determine the locations and identities of the communicating parties by intercepting and examining the transmitted messages. The traffic information may be useful for tracking communication patterns of any two parties.

2.3.2 Active Attacks

DoS attacks

A DoS attack is an adversary's attempt to use the resources available to its legitimate users. An adversary can use jamming signals thereby, disrupting the communications to make the attacked nodes suffer from DoS in a specific region (C. S. R. Murthy and B. S. Manoj, 2004).

Masquerade attacks

Masquerade attack takes place when an intruder pretends to be a legitimate user and misleads the authentication system. The authentication sequences can be captured, and therefore an invalid user can obtain privileges to access information illegally.

Message modification

Message modification refers to an attack in which an attacker alters the data by performing additions or deletions to the communication content.

Information disclosure

A compromised node can act as an information leaker by deliberately

disclosing the confidential information to unauthorized nodes.

Replay attacks

It involves the passive capture of a message and its subsequent transmission to produce an authorized effect.

2.4 Diversity for Physical Layer Security

Diversity is a communication technique where the transmitted signal travels through various independent paths and thus making the probability that all the wireless paths are in fade negligible. It is an effective way to tackle fading and improve reliability. In (Y Zou *et al.*, 2015), various diversity techniques to improve wireless PLS, namely multiple-input multiple-output (MIMO), multiuser and cooperative diversities are presented.

MIMO is an antenna technology for wireless communications in which multiple antennas are used at both the source and destination. It has been shown that MIMO technique has a great potential to enhance the security of wireless data transmissions (A. Khisti and G. W. Wornell, 2008a; A. Khisti and G. W. Wornell, 2008b; S. A. A. Fakoorian and A. Lee Swindlehurst, 2013). The secrecy capacity of a multiple-input, single-output, multi eavesdropper (MISOME) wiretap channel has been investigated in (A. Khisti and G. W. Wornell, 2008a), and the optimal solutions for the MIMO Gaussian wiretap channel are addressed in (A. Khisti and G. W. Wornell, 2008b; S. A. A. Fakoorian and A. Lee Swindlehurst, 2013). Also, due to size, cost, or hardware limitations, small handheld wireless devices may not be able to support multiple antennas. As a result, cooperative communication has been considered as a practical solution for

providing secure transmission for such devices.

Cooperative diversity is obtained when relay nodes are used for transmitting the signals. A cooperative wireless network shown in Fig. 2.1 comprises of a source S, *N* relays and a destination D in the presence of an eavesdropper E. Here the relays are exploited to assist the signal transmission from source to destination. The source node transmits independent signals to the relay and destination nodes. The destination node thus receives signal from the source and the retransmitted signal from the relay nodes. With the help of relaying node the quality of the signal received at the destination can be improved (Y Zou *et al.*, 2015). Cooperative diversity technology is a promising solution for the high data-rate coverage required in future cellular and ad-hoc wireless communications systems. In a cooperative scenario ensuring secure communication becomes more complex, since more nodes are involved.

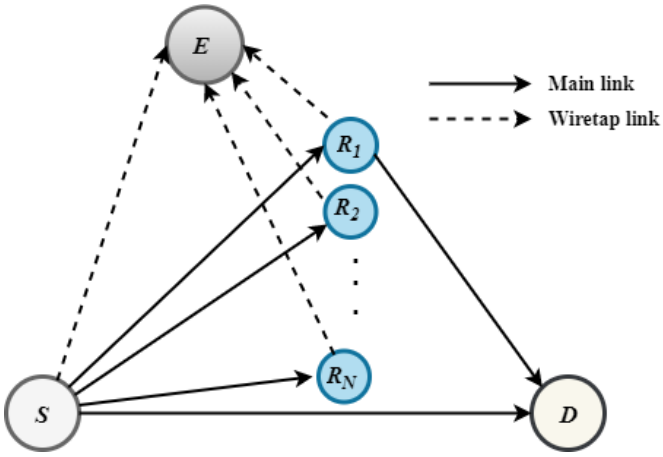


Fig. 2.1 Cooperative diversity system with *N* relays in the presence of an eavesdropper

2.5 Cooperative Communication

Cooperative communication has emerged as a promising method for mitigating wireless channel fading and improving reliability of wireless networks. Nodes in cooperative communication help each other with information transmission by exploiting the broadcast nature of wireless communication (J. N. Laneman *et al.*, 2004; A. Ibrahim *et al.*, 2008). In a cooperative transmission scheme, neighboring nodes are exploited as relay nodes, in which they cooperate with the source-destination pair to deliver multiple copies of the information through independent fading channels to the destination. Fig. 2.2 illustrates a simple cooperative communication system where two nodes (one source node and one relay node) communicate with the destination node (Fatemeh Mansourkiaie and M H Ahmed, 2015).

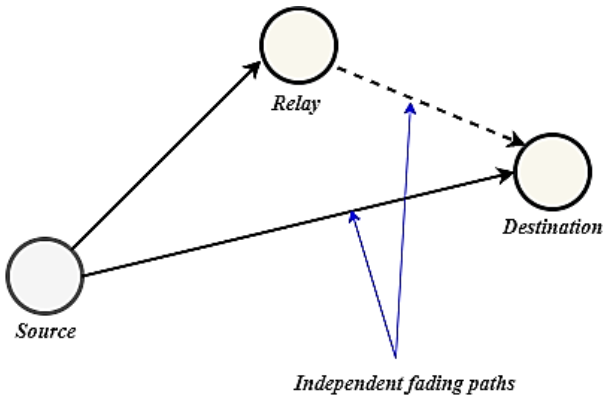


Fig. 2.2 Cooperative communication system with single relay

Each node has one antenna and does not have spatial diversity individually. However, the relay node can overhear and receive the

data, and it can forward the data to the destination node. This generates spatial diversity as the fading paths are statistically independent. Combining multiple copies of the same signal at the destination node in cooperative communication system leads to several advantages, which includes better signal quality, reduced transmission power, better coverage, and higher capacity (A. Nosratinia *et al.*, 2004; R. Madan *et al.*, 2008; W. Zhuang and M. Ismail, 2012).

Cooperative communication at the physical layer involves *i)* cooperative and relaying schemes; *ii)* the transmission power allocation for each node to satisfy the QoS requirements of the network; and *iii)* the relay selection schemes of the network (Fatemeh Mansourkiaie, and M H Ahmed, 2015). The idea of cooperative communication was introduced by E. C. Van der Meulen (1971). Meulen constructed a three-terminal relay channel and derived upper and lower bounds on its channel capacity. The capacity of the cooperative relay channel was investigated in (T. M. Cover and A. A. El Gamal, 1979), where two cooperation protocols namely decode-and-forward and compress-and-forward (CF) were proposed. The relaying techniques used by cooperating relay nodes vary in their performance, implementation complexity, and signal processing. (J N Laneman *et al.*, 2004) introduced a number of relaying techniques that combat fading: *(i)* fixed relaying schemes such as decode-and-forward (DF) or amplify-and forward (AF) and *(ii)* adaptive relaying schemes such as selection relaying and incremental relaying techniques; and performance characterizations of these protocols are presented in terms of outage probabilities in the high SNR regime.

The main benefit of applying cooperative communications in wireless networks is to achieve diversity gains, without the need of maintaining multiple antennas at each user. Moreover, spectral efficiency is still guaranteed by employing adaptive relay selection techniques. The cooperation in wireless system offers several advantages that include performance gain, balanced QoS, higher spatial diversity, higher throughput/lower delay, lower transmitted power, reduced costs due to infrastructure-less deployment etc. Some of the demerits of cooperative relaying include complex scheduling, increased overhead, increased interference, extra traffic etc. (M. Dohler, Y. Li, 2010).

2.6 Cooperation Protocols

Different cooperative transmission schemes have been proposed to achieve cooperative diversity gains and spectral efficiency in (J N Laneman *et al.*, 2004), of which the commonly used fixed transmission protocols in cooperative communication system namely, amplify-and-forward and decode-and-forward schemes are described below.

2.6.1 Amplify-and-Forward (AF)

In AF scheme, each relay receives a noisy version of the signal transmitted by the source. The relay then amplifies this noisy version and forwards it towards the destination. The destination combines the information sent by the relay/s and the source and estimates the transmitted signal. Independent faded version of the signal can be used for correlation, to accurately detect and estimate the message signal.

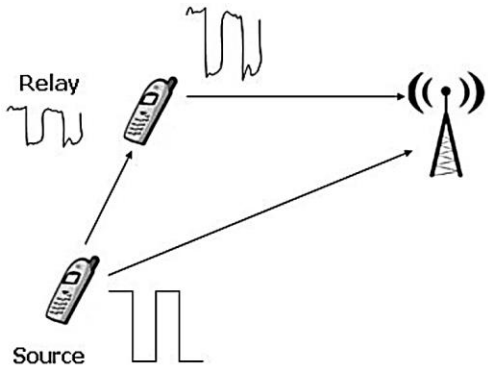


Fig. 2.3 Amplify-and-forward transmission scheme

2.6.2 Decode-and-Forward (DF)

Here, the relay node decodes the received signal, re-encode it and then retransmit it to the destination. The decoded signal at the relay may be incorrect because of approximate errors in the received signal. The diversity of the system with DF relaying protocol is one because the performance of the system is limited by the weakest link from source to relay and source to destination.

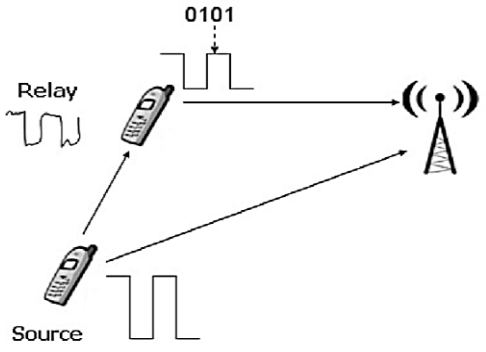


Fig. 2.4 Decode-and-forward transmission scheme

AF and DF are the commonly used transmission protocols in cooperative communication system. AF is the simplest protocol, but it suffers from the noise amplification problem which can degrade the signal quality, particularly at low SNR. Though performance of DF is comparatively better than AF, hardware complexity is more in DF because of decoding and encoding needed at the relay nodes. DF also suffers from the error propagation problem which may occur if the relay incorrectly detects/decodes a message and forwards this incorrect information to the destination, which can diminish the performance of the system.

2.7 Cooperative Relaying

Cooperative relaying schemes overcome the wireless channel impairments and also ensure secure communications under the wireless environments (L Lai and H El Gamal, 2008; L Dong *et al.,* 2010; J Li *et al.,*2011;V N Q Bao and N L Trung 2012). The typical four-terminal relay eavesdropper channel is introduced in (L Lai and H El Gamal, 2008), where different cooperation strategies namely, noise-forwarding (NF), CF and AF are discussed and the corresponding achievable performance bounds are also derived. L Lai and H El Gamal (2008) show that even if the source-destination information rate is zero a positive secrecy can be achieved if the relay is closer to the destination than to eavesdropper. Several cooperative relaying schemes with AF and DF protocols are proposed for improving the security of wireless communications in (L Dong *et al.,* 2010; J Li *et al.,* 2011).

In (V N Q Bao and N L Trung 2012), a dual-hop cooperative multi-

relay system model is designed to optimize the achievable secrecy rate (SR) or the total transmit power. When multiple relays are used for transmission, the system requires multiple orthogonal channel resources for source and relay transmissions which reduces the system spectral efficiency. At the destination, these signals need to be combined by Maximal Ratio Combining (MRC) which further increases the hardware complexity. This inefficient spectral utilization of cooperative relays as well as the complexity can be overcome by relay selection techniques. By selecting the best relay among a set of relays, only one relay participates in the cooperation and thereby full diversity can be achieved with low overhead (A. Bletsas *et al.*, 2006; Y. Zhao *et al.*, 2007). Thus, relay selection algorithms help in reducing the computational complexity during the signal processing operation of wireless networks (CMK Swain and Susmita Das, 2018).

2.7.1 Relay Selection (RS)

Relay selection plays an important role in cooperative communication as it contributes to the diversity gain. Since the relays consume system resources and power, the total energy-efficiency of the relaying techniques may be limited. It is therefore important to select a relay among available candidates to maximize the cooperation benefits for the user or for the whole system (Lin Z *et al.*, 2006). Relay selection is widely studied in previous works. A Nosratinia and T E Hunter (2006) show that relay selection techniques can capture maximum diversity in the number of cooperating nodes, while each node only knows its own receive channel state. (R Madan *et al.*, 2008) selects relays by minimizing the total power consumption.

Relay selection can be of proactive and reactive types. *Proactive* relay selection occurs when the selection is performed before the source transmission whereas *reactive type* is the selection carried out after the source transmission. Even though RS process consumes both energy and time, it must be performed frequently in order to exploit the diversity of a better channel in presence of mobility or in highly dynamical environments. The number of relays also plays an important role since this factor contributes to the dynamism of the network and directly corresponds to the diversity order of the system. For example, a scheme where one fixed relay is used, achieves a diversity order of two. If N relays are used, the diversity order becomes N+1 (Y Zou *et al.*, 2015).

The *opportunistic relaying* proposed in (A. Bletsas *et al.*, 2006), selects a single relay among a set of relays based on *i)* which relay provides the best end-to-end path between source and destination and *ii)* instantaneous channel state information (ICSI). In (A. Bletsas *et al.*, 2007), opportunistic relaying schemes with DF and AF strategies, without global CSI at each relay or at a central controller are implemented. This reduces the required cooperation overhead. In (I. Krikidis *et al.*, 2009a), max-min relay selection is considered in an interference-limited AF cooperative network. The outage probability and average channel capacity for the case with best relay selection (BRS) technique in a dual-hop DF multi-relay cooperative system are derived (S. Ikki and M. Ahmed, 2010).

Based on the knowledge of the ICSI or the statistical channel state information (SCSI) of all the links, the problem of RS is mostly

solved for the following three cases.

i) Optimal relay selection (ORS) is implemented when all the ICSI is known

ii) Traditional relay selection is implemented when all except relay-eavesdropper ICSI is known. Traditional relay selection measures main channel capacity only.

iii) Suboptimal relay selection is performed when all but relay-eavesdropper ICSI and relay-eavesdropper SCSI are known.

For the dual-hop multiple DF relay system in (I. Krikidis, 2010), secrecy outage probability (SOP) is derived for all the above three selection schemes, assuming high SNR where all the relay nodes successfully decode the source transmission. In (Y. Zou *et al.*, 2013), closed-form intercept probability expressions for optimal and traditional relay selection schemes are derived using DF and AF protocols in dual-hop multi-relay system. Instead of single eavesdropper, the effect of optimal and traditional relay selection are studied in a dual hop multiple DF relay system with multiple eavesdropper, where probability of non-zero achievable secrecy rate, SOP and achievable SR are derived (V. N. Q. Bao *et al.*, 2013).

In (H Moharrer, A Olfat, 2014), a simple joint relay selection and beamforming method, by assuming certain fixed maximum allowable power for each node in a two-hop multi-relay DF network is investigated. SOP of dual-hop AF relay system with single eavesdropper is investigated in (A. Jindal *et al.*, 2014a; A. Jindal *et al.*, 2014b). In (A. Jindal *et al.*, 2014a), an ORS method based on SOP is proposed which does not require any ICSI measurement. In

(A. Jindal *et al.*, 2014b), RS is considered when ICSI of the eavesdropper is not available. Whenever RS problem is considered for secrecy in cooperative DF relaying, perfect decoding is assumed at each relay in the high SNR scenario. By doing so, the effects of the quality of the first hop link is neglected which actually can affect the rate of the particular branch to the destination and the secrecy rate. Without considering the high SNR setup on the relays that they correctly decode the messages; Chinmoy Kundu *et al.* (2015) derived the non-zero secrecy capacity in a multiple DF relay scenario. The authors in (Fawaz S *et al.*, 2015) consider only a set of relays that successfully decode the message; relays can decode the message only if the SNR at them meet a predetermined threshold.

In (Tong Li et al., 2015), the impact of relay selection and MRC on the physical layer security of DF relaying based cooperative communications systems is studied. The impact of the main-to-eavesdropper ratio (MER) on the legitimate receiver of DF based cooperative networks is analyzed, and the closed from expressions for SOP and the average secrecy channel capacity over Rayleigh fading channels, have been derived. In (Chinmoy Kundu *et al.*, 2016), three relay selection schemes that depend on the ICSI and SCSI knowledge, namely traditional, improved traditional and optimal are proposed to enhance the SOP using threshold-selection DF relays. The authors derived the closed-form SOP and secrecy outage assuming direct links from source to destination and source to eavesdropper. It is found that the diversity of SOP of all strategies increases with the number of relays. In (Jianrong Bao *et al.*, 2017), an incremental selection hybrid decode-amplify-forward scheme for

two-hop single relay systems and a RS strategy based on the hybrid decode-amplify-and-forward scheme for multi-relay systems along with an optimized power allocation (PA) method are proposed. The optimal relay location for maximizing the gain of the proposed algorithm is also designed.

In (CMK Swain and Susmita Das, 2018), the performance of a conventional AF/DF assisted IEEE 802.16j multi-relay WiMAX network employing threshold based harmonic mean and threshold based max-min of SNR RS algorithms are studied. They also analyzed the diversity combining techniques like MRC and SC at the receiver. In (Long Yang *et al.*, 2017), an *adaptive eavesdropper is* selected to perform eavesdropping or jamming based on the eavesdropping channel quality. The authors presented ORS schemes that minimize the SOP for three cases of eavesdropper channel state information (ECSI) availability (full ECSI, partial ECSI and statistical ECSI). The research work of (S Abdulhadi *et al.*, 2012) presents a survey of the distributed relay selection schemes for adhoc cooperative wireless networks.

To optimize the secrecy rate, in most of the works mentioned above, the ICSIs of the eavesdroppers are assumed to be available. However, considering the eavesdroppers are passive, the ICSIs are difficult to obtain in practice. Therefore, the security schemes with only the channel distribution information (CDI) of the eavesdropper are investigated. Assuming that the CDI of the eavesdropper is independent and identical Rayleigh distribution, an *opportunistic relay chatting* scheme was proposed in (Z. Ding *et al.*, 2011), where a

best cooperative node is chosen as the relay to forward the confidential information while the other nodes send jamming signals to cover the data transmission. The idea has been generalized to a two-way AF network in (Z. Ding *et al.*, 2012). In both (Z. Ding *et al.*, 2011; Z. Ding *et al.*, 2012), the CSIs of the legitimate links from the source to the relay node, and from the relay node to the destination are assumed to be perfect.

Various relay selection techniques available in the literature are analysed and the thesis proposed a novel relay selection scheme based on the probability of path selection criterion of Ant Colony Optimization algorithm. In the existing relay selection schemes, the relay selection is carried out for a single wireless scenario where channel gain and/or fading are taken in to account. Here, unlike the conventional relay selection schemes, the channel gain (G) and fading coefficients (h) defining a wireless channel (M. Dohler, Y. Li, 2010) are considered separately. This gives the flexibility to choose the best relay in different wireless scenarios like traditional, path loss and fading models; depending on the significance of channel parameters G and h. AF and DF transmission protocols are used.

2.8 Cooperative Jamming

Although RS techniques improve the resource utilization, it will not always guarantee perfect secrecy as the secrecy will be degraded with poor legitimate channel conditions. Cooperative jamming is an alternative to this problem. The jamming signals in cooperative jamming can create interference at the eavesdropper; thereby reducing the SNR at the eavesdropper which improves secrecy. The

power allocated to the jamming signal should be high enough to interrupt the received signal at the eavesdropper; however allocating too much power on the jamming signal can degrade the signal quality at the destination. Thus, it is essential to assign optimal power to the jamming signals so as to maximize the secrecy rate. CJ can be implemented by the networks nodes, i.e., source, relay or destination; or two of the nodes, i.e., source and destination or source and relay to transmit the jamming signals. Accordingly, it can be of destination based jamming (DBJ), source based jamming (SBJ), friendly jammer based jamming and hybrid jamming. Among the various CJ methods, DBJ can be easily implemented because the destination can perform self-interference cancellation from its prior information of the jamming signal (Lu Lv *et al.*, 2017).

2.8.1 Destination based jamming

In DBJ, the destination node sends jamming signal to degrade the eavesdropper. The idea of DBJ to achieve a positive secrecy rate is proposed in (J Huang *et al.*, 2013). The problem of secure transmission in two-hop AF networks with an untrusted relay using DBJ technique is studied in (Ali Kuhestani and Abbas Mohammadi, 2016). (L Wang *et al.*, 2014) presented OPA in the presence of a single untrusted relay. In (Ali Kuhestani *et al.*, 2018a), the authors proposed a joint relay selection and power allocation scheme for a cooperative network, where a multiple antenna source communicates with a single-antenna destination in the presence of single antenna untrusted relays and single antenna passive eavesdroppers; for non-colluding and colluding eavesdropper cases. On the basis of the DBJ scheme, the impact of relay selection on secrecy capacity is analysed

in (L. Sun *et al.*, 2012; L. Sun *et al.*, 2015). Furthermore, combining jamming power allocation strategy with the DBJ scheme, significant secrecy capacity improvement is attained (L Wang *et al.*, 2014).

An OPA strategy with DBJ, considering the hardware imperfections is proposed for a cooperative network that comprises of a source, a destination, and an untrusted AF relay and the results indicate that OPA together with the hardware design considerably improves the secrecy (Ali Kuhestani *et al.*, 2018c). (Ali Kuhestani and Abbas Mohammadi, 2016) studied the problem of secure transmission in two-hop AF systems with an untrusted relay by using DBJ scheme; where the destination sends an intended jamming signal to the relay. Based on OPA strategy, the closed-form expressions for the outage probability and ESR are derived for three cases. In the two cases, either of the source or the destination node is equipped with large-scale antennas and in the third case, both of them are equipped with large scale antenna arrays. Numerical results showed that the OPA scheme significantly improves the power efficiency in comparison with EPA strategy

2.8.2 Source based jamming

In SBJ scheme, the source node transmits the jamming signal along with the information in order to degrade the wiretap channel. The problem of secure transmission in two-hop AF networks with an untrusted relay using SBJ by exploiting the direct link is studied in (Lu Lv *et al.*, 2017). Considering a total power budget, a power allocation strategy for allocating powers between the source and relay as well as the information and jamming signals is proposed and the

secrecy performance evaluation is done based on the ESC and SOP metrics. In (A Mabrouk *et al.*, 2017), a secure adaptive relaying scheme to improve security in energy efficient cooperative untrusted relay networks is proposed. Here, the authors investigated a trade-off between energy consumption and PLS in a wireless powered communication network consisting of one source-destination pair and multiple AF untrusted relays.

2.8.3 Friendly jammer based jamming

In (I Krikidis *et al.*, 2009b), the authors proposed to select one relay as an actual relay to deliver the desired message to the destination and another relay as a helper to degrade the eavesdropper's link. S. Goel and R. Negi (2008) and G Zheng *et al.* (2011), presented the use of multiple relays to play the role of jammer and not to send the desired message. The null-space cooperative jamming that generates interference orthogonal to the real signals in a single antenna system is presented in (S. Goel and R. Negi, 2008). It is found that the null-space jamming though being simple and effective is not good for secrecy rate maximization. Cooperative jamming to increase the PLS of a wiretap fading channel via distributed relays is studied in (G Zheng *et al.*, 2011), where each relay transmits a weighted jamming signal to degrade the eavesdropper's signal and the optimization of collaborative relay weights in maximizing the secrecy rate with individual power constraints is addressed. In (L Dong *et al.*, 2011), a four terminal two hop DF relay network with a jamming scheme is introduced, in which the message and jamming signal are transmitted by the source and relay without considering the direct link.

2.8.4 Hybrid jamming

In hybrid jamming, two of the nodes are used for sending the jamming signals. An approach that the source and the relay exploit some of their available power to transmit jamming signals to create interference at the eavesdropper in a four-terminal AF relay network is investigated in (A. Li *et al.*, 2015), where direct links are considered. In (Nan Run Zhou *et al.*, 2015) , the secrecy capacity and the optimal power distribution for a two-hop AF relaying system in two scenarios where artificial noise added by the source and the relay nodes are studied. In (A. Li *et al.*, 2017), an AN-aided jamming strategy is exploited to improve the secrecy rate of a two-way AF relay network in the presence of an eavesdropper, employing PA at the source and relay.

2.9 Hybrid Relaying and Jamming

To further improve the security, hybrid beamforming/opportunistic relaying and jamming schemes have been proposed for both one and two-way relay networks in (H. M. Wang *et al.*, 2018a; H. M. Wang *et al.*, 2018b; C. Wang *et al.*, 2015), where both two phases of the cooperative transmissions will be under protection. For all the above works only a single source-destination pair is considered. A hybrid cooperative beamforming and jamming approach was investigated in (H. M. Wang *et al.*, 2018b) to enhance the wireless secrecy capacity, where partial relay nodes are allowed to assist the source transmission to the legitimate destination with the aid of distributed beamforming, while the remaining relay nodes are used to transmit artificial noise (AN) to confuse the eavesdropper.

In (H. M. Wang *et al.*, 2018a), a *joint* cooperative beamforming and jamming scheme to enhance the PLS of an AF based relay network is proposed, where a part of intermediate nodes adopt distributed beamforming while others jam the eavesdropper simultaneously. Since the ICSI of the eavesdropper is not known, a cooperative AN transmission based secrecy strategy subjected to the individual power constraint at each node is proposed. The beamformer weights and power allocation are obtained by solving a second-order convex cone programming together with a linear programming problem. In (C. Wang *et al.*, 2015), an opportunistic relaying with jamming scheme is proposed for securing a two-hop DF trusted relay network, where sequential parametric convex approximation algorithm is used for OPA and ESR maximization, assuming the CDI of the eavesdropper is known. The authors in (Dan Deng *et al.*, 2017) investigate the secure communications of multiuser untrusted AF relay networks considering direct links where one user is selected with the help of an untrusted relay. The direct link between source and destination cannot be utilised in the DBJ schemes, which means that the flexibility offered by cooperation is not fully exploited. Better secrecy performance can be achieved if the power of source and relay is efficiently allocated according to the channel knowledge. Only the power between information and jamming signals is allocated in (L Wang *et al.*, 2014), which may not make full use of the power resource. In (Nan Run Zhou *et al.*, 2015), a multiple relay node communication system using AF scheme with one eavesdropper is discussed, where there is no direct link between source and destination and relay nodes are equipped with single antenna

cooperating to transmit the received signals. The secrecy capacity and the optimal power distribution are studied in two scenarios, AN added by the transmitter and AN added by the cooperative relay nodes. The results show that it is better to distribute more power to the available signals if the main channel is better, while more power to AN if the wiretap channel is better. The sub-optimal power distribution can attain close performance compared with the optimal power distribution strategy but with substantially reduced computational complexity.

Three categories of relay and jammer selection schemes namely selection schemes without jamming, selection schemes with conventional jamming and selection schemes with controlled jamming were proposed in (Doaa H. Ibrahim *et al.*, 2015), to improve the PLS of two-way DF cooperative networks. The selection process is analyzed in single eavesdropper model and multiple cooperating and non-cooperating eavesdropper models. The obtained results show that the selection schemes with jamming outperform the schemes without jamming when the intermediate nodes are distributed dispersedly between sources and eavesdropper nodes. However, when the intermediate nodes cluster gets close to one of the sources, they are not superior any more due to the strong interference on the destination nodes. Therefore, a hybrid scheme which switches between selection schemes with jamming and schemes without jamming is introduced to overcome the negative effects of interference. In (H Hui *et al.*, 2015), a **s**ecure relay and jammer selection for PLS is studied in a wireless network with multiple intermediate nodes and eavesdroppers, where each intermediate node

either helps to forward messages as a relay, or broadcasts noise as a jammer. A closed-form expression for the SOP is derived for two relay and jammer selection methods.

In (Sarbani Ghose *et al.*, 2016), SOP and ESR is obtained in closed-form for a dual-hop, DF relay system with MRC and SC diversity combining at the eavesdropper. A pre-defined SNR threshold is considered for the relay to be able to decode or retransmit. Performance analysis is carried out when CSI is known at the transmitter and CSI is unknown at the transmitter. Asymptotic analysis of SOP is presented. The authors show that the direct link has a significant impact on system secrecy. It is found that secrecy performances are the best if the relay is always able to decode correctly. They also found that knowledge of CSI helps to achieve better secrecy at lower rate. In (W Wang *et al.*, 2016a), a generalized relay and jammer selection scheme is proposed to improve the security in a cooperative relay network. The expression of the SOP, with the assumption that global CSI of the legitimate receiver and SCSI of the eavesdropper are available, has been derived and both the power allocation factor and the number of relay nodes have been jointly optimized to minimize the SOP. It has been shown that the proposed multi-relay selection scheme outperforms the conventional single-relay selection scheme without additional overhead.

2.10 Trusted and Untrusted Relays

Relays can be considered as trusted or untrusted in cooperative networks. In trusted scenario, secure communication between source and destination occurs with the help of relays even in the presence of

eavesdroppers. But in practice, it is likely to come across public ad hoc networks where relays used for connectivity may not be authenticated. In such cases, secrecy of the information transmitted via relay nodes need to be protected, despite the fact that the relay is a cooperating node. Since the relays are not trusted with the information it is relaying (X. He and A. Yener, A, 2009; X. He and A. Yener, 2010); they are considered untrusted. Even in the absence of external eavesdroppers, secrecy cannot be guaranteed in untrusted networks.

2.10.1 Trusted Relays

In trusted relay scenarios, the source is supported by a single or multiple trustworthy relays to transmit confidential information to destination in the presence of a passive eavesdropper, in addition to the legitimate parties. The trusted relays can be fully exploited to enhance security significantly (LJ Rodriguez *et al.*, 2015). Several strategies to improve security have been addressed before. One among them is the relaying strategy where the relay nodes help in transmission by simply relaying information between the legitimate nodes depending on one-way (OW) and two-way (TW) relay protocols, based on how the information flow. In OW relaying, a source communicates to a destination node with the help of relays in a unidirectional fashion i.e., from source to destination. In TW relaying, two nodes exchange data and information flows in a bidirectional manner. When only one relay is available, the conventional AF or DF techniques are used along with OW or TW relay protocols. On the other hand, when multiple relays are available, distributed beamforming is the most common relaying

approach where, multiple relays transmit the noisy version of the received signal for AF relays or a weighted version of the decoded signal for DF relays.

2.10.2 Untrusted Relays

In cooperative networks consisting of one or multiple untrusted relay nodes, the source-destination pair needs to keep the information confidential from the relays, while relays are used for transmitting information. Examples of such networks include networks belonging to a government or a financial institution or adhoc networks, where the relay nodes have different level of security clearance. (X. He and A. Yener, 2010) appears to be the first work dealing with untrusted relaying scheme, which focuses on secrecy capacity. By considering a three-node model with a source, a destination and an untrusted relay, it was demonstrated that the untrusted relay can be beneficial for some specific relaying topologies. Specifically, when there is an orthogonal link in the second hop from the relay to the destination, higher secrecy rate would be obtained when relay is considered as an eavesdropper as well as a helper rather than considering eavesdropper only. AF and CF relaying protocols can be used for untrusted relaying schemes, whereas DF is not suitable since it requires the relay to decode the message from its observation. On the other hand, when the source and relay transmit to the destination via a multiple access channel, while there is an orthogonal link from source to relay, the secrecy capacity is equal to zero (L. Sun *et al.*, 2015). In (Nan Run Zhou *et al.*, 2014), a comparison between one-way and two-way half-duplex AF relaying schemes with an untrusted relay is studied in terms of their secrecy rates and it is found that with equal transmit

power at the two relaying protocols, the two-way relaying scheme has better performance compared to one-way relaying protocol under high SNR regime.

The results in (X. He and A. Yener, 2010) have been extended to multi-antenna structures in (C. Jeong *et al.*, 2012), where all the nodes are equipped with multiple antennas. In particular, by jointly optimizing the source beamforming vector and the relay beamforming matrix, the cooperative scheme achieves a better secrecy rate than the non-cooperative scheme. However, the proposed beamforming scheme can only be applied to AF relaying. It has been proved that by adopting CJ in the network containing trusted/untrusted relays with/without external eavesdroppers; it can have a good impact on secrecy performance compared to those which do not have any secrecy scheme.

2.11 Power Allocation

In cooperative networks employing relaying and jamming schemes, power requirement always depend on the position of relays and eavesdropper. Power should be properly allocated between the source and relay; and between the information and jamming signals. Prior studies have revealed that, for transmission, the system requires less source power when a relay close to source is selected and more source power when a relay near to destination is selected. If the relay at the centre of the network is selected as is the case with best relay position, such that source-relay and relay-destination distances are the same, then the source and relay require almost same power. The system will not be secure if the eavesdropper appears near to source,

as it can easily get the information; therefore more source power is needed to overcome the insecurity.The jamming signals in cooperative jamming technique can create interference at the eavesdropper; which reduces the SNR at the eavesdropper and improves secrecy. The power allocated to the jamming signal should be high enough to interrupt the received signal at the eavesdropper; however allocating too much power to the jamming signal can degrade the signal quality at the destination. Thus, it is essential to assign optimum power to the jamming signals so as to maximize the secrecy rate (L Dong *et al.*, 2010). Power allocation (PA) has thus become an important parameter that must be optimized while dealing with the secrecy performance of cooperative networks employing cooperative relaying or jamming or both. OPA for secure communication in cooperative relay networks employing trusted and untrusted relaying schemes; energy efficient cooperative relay networks etc. have been studied. A survey of optimization approaches for wireless PLS is conducted in (Dong Wang *et al.*, 2018), which discusses various topics on PLS designs, the performance metrics and different categories of optimization problems adopted in security designs, the impacts of CSI on optimization and design etc.

OPA strategy normally adopts gradient-based optimization methods like derivative test to maximize the secrecy rate. But, gradient-based methods have problems with noisy and discontinuous functions, non-differentiable functions and/or constraints, mixed variable functions or functions of large dimensionality. Since the secrecy rate is a non-linear function of three/two independent variables depending on the type of jamming scheme used; it may be difficult to find the partial

derivatives of the function at all relay positions so as to do the gradient-based optimization for maximizing the secrecy. So, to overcome the problems with gradient method, a gradient free method known as Nelder Mead algorithm (J.A. Nelder and R. Mead, 1965) is used.

2.12 Secrecy Capacity

The fundamental metric of secrecy is termed as secrecy capacity, which is the maximum achievable secrecy rate of the system. It indicates the maximum transmission rate from source to desired destination while eavesdropper is not able to access transmitted data. The secrecy capacity *Cs* is formulated as (M Bloch et al., 2011),

$$C_s = [C_m - C_w]^+ \tag{2.1}$$

where C_m is the capacity of the main channel and C_w denotes the capacity of the wiretap channel. A positive secrecy capacity is needed for secure transmission. Shannon-Hartley theorem (R.V L Hartley, 1928) defines the channel capacity as the maximum of information that can be transmitted and is related to the bandwidth (*B*) and signal to noise ratio (*SNR*).

$$C = B \log_2 (1+SNR) \tag{2.2}$$

Thus, the capacity of the main channel is given by

$$\mathrm{C_m} = \frac{1}{2}\log_2 (1+\gamma_\mathrm{m}) \tag{2.3}$$

Likewise, the capacity of the wiretap channel is given by

$$\mathrm{C_w} = \frac{1}{2}\log_2 (1+\gamma_\mathrm{w}) \tag{2.4}$$

In cooperative communication, signal transmission involves two

phases. The ½ in the capacity equations denotes that two time slots are used for information transfer. γ_m and γ_w denote the instantaneous SNR received at the intended and the unintended receivers respectively. The notion of secrecy capacity can be explained in a way that if the maximum of information transmitted in the legitimate channel is higher than the maximum of information transmitted in the wiretap channel; the eavesdropper can never receive enough information to break through the legitimate transmission. This is called as *Perfect Secrecy*. Note that if $\gamma_m > \gamma_w$ legitimate receiver can receive more information and the transmission is secured. Otherwise, if $\gamma_m < \gamma_w$ the transmission is unsecured and C_s will become negative. The unsecured situation has no secrecy capacity therefore C_s under such condition is defined as zero.

$$C_s = \begin{cases} \frac{1}{2}\log_2(1+\gamma_m) - \frac{1}{2}\log_2(1+\gamma_w), & \gamma_m > \gamma_w \\ 0, & \gamma_m < \gamma_w \end{cases} \quad (2.5)$$

Therefore, based on equation (2.1), it can be said that increasing the received SNR of the main link or decreasing the received SNR of the wiretap link result in improving the secrecy capacity. Accordingly, security of the communication system has been investigated considering instantaneous SNR of the legitimate and illegitimate links to examine under which conditions positive secrecy capacity is achievable.

2.13 Chapter Summary

In this chapter, literature survey on various PLS techniques for enhancing secrecy in wireless networks is conducted. The extensive

literature review illustrates the current status of the diversity solutions of PLS that include cooperative relaying, relay selection and jamming schemes. Different relaying protocols available in the literature are summarized.

In the first part on cooperative relaying, various relay selection techniques available in the literature are analysed, the key design issues for improving the secrecy have been identified, and the potential applications of cooperative communications with relay selection in general cooperative wireless networks is discussed. By considering the probability of path selection criterion of Ant Colony Optimization algorithm for relay selection, the proposed method helps to analyse the secrecy performance in different wireless scenarios like traditional, path loss and fading models. AF and DF transmission protocols are used and a performance comparison among them is formulated.

In the second part, various cooperative jamming schemes to enhance the system secrecy have been reviewed. The definition of secrecy capacity to achieve positive secrecy of the system is derived. The problem of power allocation for secrecy rate maximization for the case of trusted and untrusted relaying schemes is studied. The issues with traditional gradient-based power optimization method are addressed and the thesis proposed a gradient-free power optimization algorithm for two jamming schemes - a source and relay based jamming and source based jamming schemes. The performance as well as the complexity of the proposed schemes/algorithm is evaluated through simulations using MATLAB and R Programming.

Chapter 3

Relay Selection for Secrecy Enhancement in Cooperative Networks

3.1 Introduction

Cooperative communication using relaying nodes has been considered as a promising technique for increasing the physical layer security of wireless systems against eavesdropping (L Lai and H El Gamal, 2008) In addition to that; relaying can improve the network coverage and diversity without using multiple antennas (J. N. Laneman *et al*., 2004). An important performance parameter of PLS is the secrecy rate, which quantifies the maximum rate of transmission at which the eavesdropper cannot decode any of the information from the transmitting node. Achievable secrecy rate is given by the difference of the information rates of the main channel and that of the wiretap channel (A. D. Wyner, 1975). A positive secrecy rate is to be guaranteed for secure communication and that can be achieved only if the main channel is better than the wiretap channel. We cannot always ensure perfect secrecy even when the wiretap channel is less noisy than the main channel. Cooperative relaying, an effective method to combat multipath fading that enhances the security of wireless communications is proposed to overcome this situation.

In a cooperative communication system, intermediate nodes are utilized as relays to forward the data from source to destination over independent wireless channels. With multiple relays the main channel

capacity can be significantly increased by using cooperative beamforming. But the drawback is, with multiple relays, the system requires multiple orthogonal channel resources for the source and relay transmissions, which reduces the system spectral efficiency. At the destination, these signals need to be combined by MRC which further increases the hardware complexity. This inefficient spectral utilization of cooperative relays as well as the complexity can be overcome by relay selection techniques. By selecting the best relay among a set of relays, only one relay participates in the cooperation and thereby full diversity can be achieved with low overhead and complexity (A. Bletsas *et al.,* 2006; Y. Zhao *et al.,* 2007; CMK Swain and Susmita Das, 2018). Because of the ease of implementation, fixed relays are a low cost and low complexity solution to meet the requirement of high data rate communication far from the base station.

In this chapter, a novel relay selection scheme is devised to enhance the secrecy of dual-hop AF and DF cooperative relay networks and a performance comparison is formulated. The probability of path selection criterion of Ant Colony Optimization algorithm is used for selecting the relay with high end-to-end SNR, which is explained in Section 3.4. Here, unlike the conventional relay selection schemes, the channel gain (G) and fading coefficients (h) defining a wireless channel (M. Dohler, Y. Li, 2010) are treated separately. This gives the flexibility to choose the best relay in different wireless scenarios like traditional, path loss and fading models; depending on the significance of channel gain and fading coefficients. In the existing relay selection schemes, the relay selection is carried out for a single

wireless scenario where channel gain and/or fading are taken in to account. In most of the prior works, *(i)* the relays form a cluster at the center of the network model *(ii)* the eavesdropper appears only in the coverage area of relays and *(iii)* the direct link between source and destination (S-D) is not considered. However, due to broadcast nature of wireless medium, the direct link between source and destination is likely to exist and the eavesdropper may appear anywhere in the system and can tap signals from both the direct and relayed path.

A practical and general scenario where (i) the channels suffer from independent non-identical Rayleigh fading; *(ii)* the direct links between the source-destination and source-eavesdropper are available; and (*iii)* relay nodes randomly distributed between the source and destination; is considered. Accordingly, we analyzed the secrecy performance in three different cases, when *(i)* both channel gain and fading coefficients are significant as in the case of a traditional wireless scenario *(ii)* only fading coefficients h are significant as in a fading model and *(iii)* only channel gain G is significant as in a path loss model. Analysis is carried out for the two relay selection schemes namely best relay selection (BRS) and partial relay selection (PRS). The performance based on secrecy rate (R_s); is evaluated for $\boldsymbol{N}$ trusted relays distributed dispersedly between the source and destination and for different eavesdropper position. Traditional BRS and PRS schemes are used as benchmark schemes for comparison (A. Bletsas *et al.*, 2006; W Wang *et al.*, 2016a; I. Krikidis *et al.*, 2008). The performance comparison of OPA based on gradient method and exhaustive search algorithms and equal power

allocation (EPA) strategies are also studied. The impact of number of relaying nodes on the secrecy is also evaluated. Numerical results show the merits of the proposed relay selection scheme in terms of secrecy rate in different wireless scenarios as compared to traditional schemes.

The algorithm finds application in wireless networks employing centralized relay system such as wireless mobile networks, wireless LAN, wireless network structure for rural areas etc. In wireless mobile networks, both channel gain and fading are considered; in wireless LAN, only fading is considered as distance between the nodes is almost fixed whereas in wireless network structure for rural areas, distance is one of the key factors driving system design and performance.

3.2 System Model

The system model is shown in Fig. 3.1, where a source S communicates with a destination D via N randomly distributed intermediate relay nodes with a passive eavesdropper E. For notational convenience, the relays are represented by $R = \{R_k \mid k=1, 2, \ldots, N\}$ and are assumed to be trusted. The eavesdropper is a passive attacker, whose aim is to interpret the source information without modifying it. All the nodes are equipped with single omnidirectional antenna and the relays operate in half-duplex mode. The direct link between source and destination is used so as to exploit the benefits of cooperation A time-division multiple-access protocol (TDMA) is assumed; hence complete transmission of information takes place in two time slots. The solid and dashed lines in the figure represent the

main link and wiretap link respectively. The channels are assumed to be independent and modeled as Rayleigh fading. The channel coefficients remain constant within the process of one signal transmission. Due to Rayleigh fading, all channel gains are exponentially distributed and the additive noise at each receiver is characterized by a Gaussian random variable with zero mean and variance σ^2, i.e., CN (0, σ^2). The total transmit power of the system is taken as P. Since the transmission channels for all the relays are orthogonal, the signal can be separated at the destination without any interference. MRC is employed at the destination for AF and at the eavesdropper for both AF and DF, as they get two independent copies of the message from the direct and relayed paths. .

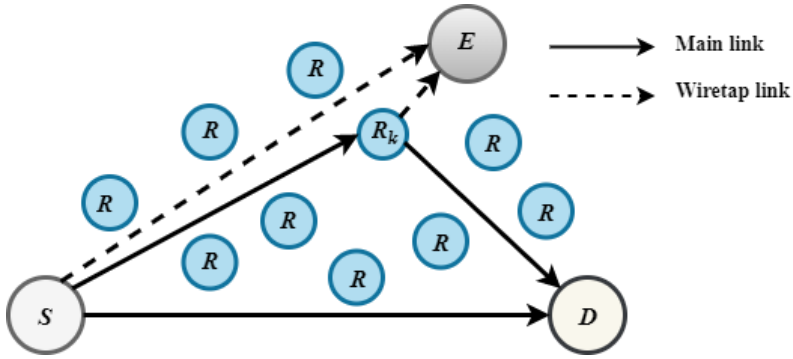


Fig. 3.1 System Model

The same system model is used for the analysis of works in Chapters 4 and 5

3.3 Transmission Scheme

The signal transmission is divided into broadcast phase and relaying phase. During the broadcast phase, the signal x_s from the source is

broadcasted to N relays as well as to destination; and during the second phase of transmission, the selected relay forwards the received signal to destination. Let $P_s = aP$ and $P_r = (1\text{-}a)\ P$ be the power allocated at the source (P_s) and relay (P_r); where $a \in (0, 1)$ indicates the power allocation factor and P is the total transmit power. For EPA, a is taken as 0.5, so that equal power is allocated to source and relay. The signal received at the k^{th} relay, destination, and eavesdropper during the first phase can be expressed in terms of channel gain and fading coefficients (M. Dohler, Y. Li, 2010), as

$$y_{SR_k} = \sqrt{aP} G_{SR_k} h_{SR_k} x_s + n_{R_k} \tag{3.1}$$

$$y_{SD} = \sqrt{aP} G_{SD} h_{SD} x_s + n_{D_1} \tag{3.2}$$

$$y_{SE} = \sqrt{aP} G_{SE} h_{SE} x_s + n_{E_1} \tag{3.3}$$

where $\mathbf{E}\{|x_s|^2\}=1$; n_{R_k}, n_{D_1}, n_{E_1} are the additive noises at the corresponding nodes respectively.

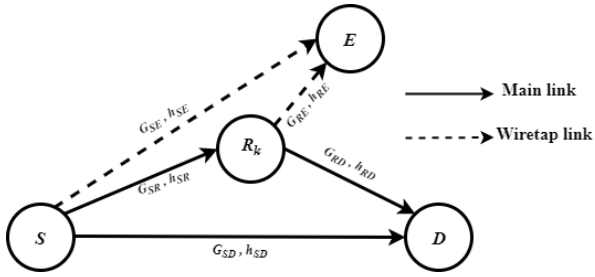
The channel gain G_{ij} between nodes i and j is expressed as

$$G_{ij} = G_o \left(\frac{d_{ij}}{d_o} \right)^{-L/2} \tag{3.4}$$

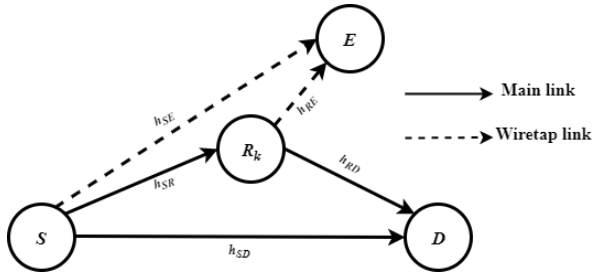
where G_o is a constant depending on the carrier wavelength, d_{ij} is the distance between nodes i and j, d_o is a reference distance, L is the path loss coefficient whose values vary in the range $2 \leq L \leq 6$. The channel gain G_{ij} is set to $(d_{ij})^{-L/2}$, assuming the other parameters as 1 for simplicity. Considering a passive eavesdropper whose CSI is not available; a relay selection method is adopted based on the probability of path selection of ACO which is explained in Section

3.4. Once the relay is selected, the selected relay uses AF or DF protocol to forward the signal to destination. Notice that, in both AF and DF relaying transmission, the source signal is transmitted twice from the source and relay, since the direct link between the source and destination is assumed.

The channel coefficients for the proposed and conventional models are shown in Fig. 3.2 *a* and *b* respectively. In the proposed model, the channel is defined by two parameters namely channel gain (*G*) and fading coefficients (*h*) (M. Dohler, Y. Li, 2010); whereas in conventional models, the channel gain or fading or the combined effect of channel gain and fading are considered as a single entity.



(a)



(b)

Fig. 3.2 Channel coefficients of *a) proposed model b) conventional model* with the selected relay

3.3.1 Amplify-and-Forward (AF)

During the relaying phase of transmission, the signal received from the source is amplified by the selected relay and then forwarded to destination. The signal received at the destination and eavesdropper is expressed as

$$y_{R_kD} = \sqrt{aP} G_{SR_k} h_{SR_k} G_{R_kD} h_{R_kD} g x_s + G_{R_kD} h_{R_kD} g n_{R_k} + n_{D_2} \tag{3.5}$$

$$y_{R_kE} = \sqrt{aP} G_{SR_k} h_{SR_k} G_{R_kE} h_{R_kE} g x_s + G_{R_kE} h_{R_kE} g n_{R_k} + n_{E_2} \tag{3.6}$$

where n_{D_2} and n_{E_2} are the additive noises at the corresponding nodes and g is the amplification factor at the selected relay given by

$$g = \sqrt{\frac{(1-a)P}{\left|G_{SR_k} h_{SR_k}\right|^2 aP + {\sigma_R}^2}} \tag{3.7}$$

The overall SNR at the destination and eavesdropper applying MRC is

$$\begin{aligned} \gamma_{D_{AF}} &= \left|G_{SD} h_{SD}\right|^2 \left(\frac{aP}{{\sigma_D}^2}\right) + \frac{g^2 \left|G_{SR_k} h_{SR_k}\right|^2 \left|G_{R_kD} h_{R_kD}\right|^2 aP}{g^2 \left|G_{R_kD} h_{R_kD}\right|^2 {\sigma_R}^2 + {\sigma_D}^2} \\ &= a\gamma_{SD} + \frac{a(1-a)\gamma_{SR_k}\gamma_{R_kD}}{1 + a\gamma_{SR_k} + (1-a)\gamma_{R_kD}} \end{aligned} \tag{3.8}$$

$$\gamma_{E_{AF}} = \left|G_{SE} h_{SE}\right|^2 \left(\frac{aP}{{\sigma_E}^2}\right) + \frac{g^2 \left|G_{SR_k} h_{SR_k}\right|^2 \left|G_{R_kE} h_{R_kE}\right|^2 aP}{g^2 \left|G_{R_kE} h_{R_kE}\right|^2 {\sigma_R}^2 + {\sigma_E}^2}$$

$$= a\gamma_{SE} + \frac{a(1-a)\gamma_{SR_k}\gamma_{R_kE}}{1 + a\gamma_{SR_k} + (1-a)\gamma_{R_kE}} \tag{3.9}$$

where γ indicates the signal to noise ratio (SNR). γ_{SR_k}, γ_{SD} and γ_{R_kD} are the instantaneous SNR in the source-relay, source-destination and relay-destination channels respectively. Mathematically, the instantaneous SNR between the two nodes is obtained as follows:

$$\gamma_{ij} = P\frac{\left|G_{ij}h_{ij_k}\right|^2}{\sigma_j^{\ 2}} \tag{3.10}$$

where i and j indicate the transmitting and receiving nodes respectively. We assume for simplicity that all the additive noise variances during the first and second phases are equal. Therefore, the transmission rate at the destination and eavesdropper are

$$R_{D_{AF}} = \frac{1}{2}\log_2\left(1+a\gamma_{SD}+\frac{a(1-a)\gamma_{SR_k}\gamma_{R_kD}}{1+a\gamma_{SR_k}+(1-a)\gamma_{R_kD}}\right) \tag{3.11}$$

$$R_{E_{AF}} = \frac{1}{2}\log_2\left(1+a\gamma_{SE}+\frac{a(1-a)\gamma_{SR_k}\gamma_{R_kE}}{1+a\gamma_{SR_k}+(1-a)\gamma_{R_kE}}\right) \tag{3.12}$$

3.3.2 Decode-and-Forward (DF)

In the conventional DF protocol, the relays try to decode their received signal from the source. The best relay is then selected prior to the second phase of transmission. In the relaying phase of transmission, the selected relay re-encodes the decoded signal $\hat{x}_s$ and forwards it to destination with power P_r = (1-a) P. The received signal at the destination and eavesdropper is thus given by

$$y_{R_kD} = \sqrt{(1-a)P}G_{R_kD}h_{R_kD}\hat{x}_s + n_{D_2} \tag{3.13}$$

$$y_{R_kE} = \sqrt{(1-a)P}G_{R_kE}h_{R_kE}\hat{x}_s + n_{E_2} \tag{3.14}$$

Here, the relay is selected based on good channel properties and it produces less decoding errors compared to others, hence $\hat{x}_S \approx x_S$. So we take the assumption that the relay completely decodes the message. In the DF relaying transmission, the mutual information between the source and the destination is limited by that of the weakest link between S-R_k and the combined channel from S-D and R_k-D (K. J. Rayliu *et al.,* 2009). The combined effect of S-D and R_k-D is considered because of the presence of direct link between source and destination. The achievable rate at the destination of DF relaying transmission can be written with the help of Eq. (4.21) in (K. J. Rayliu *et al.*, 2009).

$$R_{D_{DF}} = \frac{1}{2}\min\left\{\log_2\left(1+a\gamma_{SR_k}\right), \log_2\left(1+a\gamma_{SD}+(1-a)\gamma_{R_kD}\right)\right\} \qquad (3.15)$$

Meanwhile, the eavesdropper can overhear the transmission from R_k to destination. Since eavesdropper gets two chances to intercept the message from the source and the relay, MRC is done to improve SNR (W Wang *et al.*, 2016a). Assuming that the relay nodes use the same signal as the source in the first phase, the achievable rate at the eavesdropper is obtained by using Eq. (9) in (W Wang *et al.*, 2016a).

$$R_{E_{DF}} = \frac{1}{2}\log_2\left(1+a\gamma_{SE}+(1-a)\gamma_{R_kE}\right) \qquad (3.16)$$

where γ_{SE} and γ_{R_kE} are the instantaneous SNR in the source-eavesdropper and relay-eavesdropper channels obtained by (3.10).

3.4 Relay Selection Algorithm

3.4.1 Proposed relay selection algorithm

In our work, the probability of path selection of Ant Colony

Optimization (ACO) algorithm is used for selecting the best relay. ACO is a very popular algorithm used for finding optimal paths based on the behaviour of ants searching for food. Ants communicate with each other using a volatile chemical substance known as pheromones. They lay pheromone while they travel; i.e., their movement is controlled by pheromone, which will evaporate over time. The movement of ants can be interpreted as signal flow in the wireless scenario.

The two stages in the ACO algorithm are (Xin-She Yang *et al.*, 2013) are as follows.

i) the probability of selecting a route and

ii) the evaporation rate of the pheromone.

The first stage is for finding the route and the second stage is for the optimization part. Of the two stages in the ACO solution, we are concentrating only on the first part of finding the probability of a route.

Path probability selection

According to the probability of path selection of ACO, considering an ant launched from a certain node (say i), a number of choices (set of nodes A= $\{j_1, j_2, \ldots, j_N\}$) are there to select an intermediate node to reach the destination in wireless scenario; an ant will move from node i to node $j \in$ A with probability (Marco Dorigo and Thomas Stutzle, 2006).

$$p_{i,j} = \frac{\tau_{i,j}^{\alpha} \eta_{i,j}^{\beta}}{\sum_{j} \tau_{i,j}^{\alpha} \eta_{i,j}^{\beta}} \tag{3.17}$$

where

- $\tau_{i,j}$ is the amount of pheromone (traces) on edge i, j
- $\eta_{i,j}$ is the desirability of edge i, j (typically $\eta_{i,j} = 1/d_{ij}$), which gives the heuristic information between the nodes i and j.
- α and β are non-negative numbers called the relevance parameters that control the influence of $\tau_{i,j}$ and $\eta_{i,j}$ respectively.

Owing to the suitability of the algorithm in the current wireless scenario, the probability function is adopted for finding the best relay. For applying the path probability function of ACO algorithm, we need to have two independent parameters defining the wireless channel. Here, the channel gain (G) and fading coefficients (h) of a wireless channel are considered separately (M. Dohler, Y. Li, 2010). For path probability calculation in the proposed approach, h and G are mapped to $\tau$and η respectively.

For the proposed algorithm, for each relay path from source to destination, two probabilities are calculated; one for the path from the source to relay and another for the path from relay to destination and this will make up a total of N probability pairs. Accordingly, the probability of a signal transmitted from source to k^{th} relay and that from k^{th} relay to destination are given by

$$p_{S,R_k} = \frac{G_{SR_k}^{\alpha} h_{SR_k}^{\beta}}{\sum_{k=1}^{N} G_{SR_k}^{\alpha} h_{SR_k}^{\beta}} \tag{3.18}$$

$$p_{R_k,D} = \frac{G_{R_kD}^{\alpha} h_{R_kD}^{\beta}}{\sum_{k=1}^{N} G_{R_kD}^{\alpha} h_{R_kD}^{\beta}} \tag{3.19}$$

According to the probability function, the best relay is selected based on the significance of channel gain and fading coefficients; i.e., by choosing different values for the relevance parameters. The relevance parameters α and β determine the relative influence of G and h respectively. G_{ij} is dependent on d_{ij}, where d_{ij} is the distance between nodes i and j. If $\alpha = 0$, only h is taken into account whereas if $\beta = 0$, only G is considered for selecting the path. If both α and β are non-zero values and equal, both G and h are given equal preference whereas if they are not equal, G or h is given importance depending on whether $\alpha > \beta$ or $\beta > \alpha$ respectively. The path selection process is explained in Table 3.1.

Table 3.1 Path selection process of ACO

Relevance parameters	**Channel parameters considered for path selection**
$\alpha = 0$	Only h
$\beta = 0$	Only G
$\alpha = \beta$ & $\alpha, \beta > 0$	Both G and h with equal preference
$\alpha \neq \beta$; $\alpha > \beta$	G is given priority
$\alpha \neq \beta$; $\alpha < \beta$	h is given priority

3.4.2 Traditional Relay Selection Schemes

Relay selection techniques can be categorized into two types, i.e., partial relay selection (PRS) and best relay selection (BRS). Both the source to relay and relay to destination signal-to-noise ratios are considered for BRS; whereas, that of only the source to relay is considered for PRS. These schemes select only the best relay from

multiple relaying candidates to cooperate with a communication link, which improves the spectral efficiency. We have considered these two relay selection schemes for the analysis. The proposed algorithm is applied to both to find the best relay in each scheme. A comparison between the proposed and traditional relay selection schemes is also studied.

Partial Relay Selection (PRS)

The first-hop CSI is used to select the best relay in the PRS scheme (I. Krikidis *et al.*, 2008). In the proposed scheme, the relay that gives the maximum source to relay probability $p_{S,Rk}$ is selected whereas in the traditional scheme, the one that gives the maximum instantaneous SNR in source to relay link is selected as best relays. Mathematically they are expressed as follows:

$$\text{Relay}_{PRS}^{P} = \arg\max_{k \in R} \left(p_{S,R_k} \right) \tag{3.20}$$

$$\text{Relay}_{PRS}^{T} = \arg\max_{k \in R} \left(\gamma_{SR_k} \right) \tag{3.21}$$

where γ_{SR_k} is the instantaneous SNR at the k^{th} relay and is determined by (3.10). For both proposed and traditional AF and DF protocols, same expressions are used for finding the best relay in PRS scheme.

Best Relay Selection (BRS)

In the BRS scheme, the relay that gives the best end-to-end SNR is chosen as the best relay, i.e.

$$\text{Best Relay (traditional)} = \arg\max_{k} \left(\gamma_D \right) \tag{3.22}$$

where γ_D is the SNR at the legitimate destination.

3.4.3 Relay Selection for AF Scheme

In the proposed AF scheme, the best probability pair $p_{S,Rk}$ and $p_{Rk,D}$ from the N pairs gives the best relay and is obtained by taking the harmonic mean as

$$\text{Best Relay}_{AF}^{P} = \arg\max_{k \in R} \left(\frac{p_{S,R_k} p_{R_k,D}}{p_{S,R_k} + p_{R_k,D}} \right) \tag{3.23}$$

For the traditional AF scheme, best relay depends on the instantaneous SNRs of source to relay and relay to destination links as Eq. (2) in (A. Bletsas *et al.*, 2006) and it is expressed as

$$\text{Best Relay}_{AF}^{T} = \arg\max_{k \in R} \left(\frac{\gamma_{SR_k} \gamma_{R_k D}}{\gamma_{SR_k} + \gamma_{R_k D}} \right) \tag{3.24}$$

The more representative measure in this context is the harmonic mean as the probabilities depend on the time-varying characteristics of the fading channels.

3.4.4 Relay Selection for DF Scheme

In DF protocol, the end-to-end transmission is in failure if one of the two hops is corrupted. In the BRS scheme, the relay that maximizes the capacity of DF relaying transmission is observed as the best relay (W Wang *et al.*, 2016a). In the proposed BRS scheme, the best relay is selected based on the probabilities $p_{S,Rk}$ and $p_{Rk,D.}$ whereas in the traditional scheme, the best relay depends on the instantaneous SNR of source-relay and relay-destination links. Mathematically the best relays are selected as follows:

$$\text{Best Relay}_{DF}^{P} = \arg\max_{k \in R} \min\left(p_{S,R_k} , p_{R_k,D} \right) \tag{3.25}$$

$$\text{Best Relay}_{DF}^{T} = \arg\max_{k \in R} \min\left(\gamma_{SR_k}, \gamma_{R_k D}\right) \tag{3.26}$$

where the instantaneous SNRs in the source-destination and relay-destination channels are determined by (3.10). The max-min criterion is chosen as an efficient best relay selection metric as it is simple and the implementation complexity is less since it does not involve any computational operations.

3.5 Performance Analysis

3.5.1 Secrecy Rate

The secrecy metric used for performance evaluation is the secrecy rate R_s, and is defined as the maximum rate of transmission at which an eavesdropper cannot decode any of the information from the transmitting node. The instantaneous secrecy rate is given by M. Bloch *et al.* (2008);

$$R_s = \left(R_D - R_E\right)^+ = \left[\frac{1}{2}\log_2\left(1+\gamma_D\right) - \frac{1}{2}\log_2\left(1+\gamma_E\right)\right]^+ \tag{3.27}$$

where $[x]^+ = \max\{0, x\}$;

i.e., $[x]^+ = x$ if $x > 0$ and

$= 0$ if $x \leq 0$

R_D and R_E represent the achieved transmission rates at the destination and eavesdropper nodes respectively. If we can guarantee a positive secrecy rate by proper power allocation at the nodes, the secrecy rate becomes (Ali Kuhestani and Abbas Mohammadi, 2016)

$$R_s = \frac{1}{2}\log_2\left(1+\gamma_D\right) - \frac{1}{2}\log_2\left(1+\gamma_E\right) \tag{3.28}$$

Amplify-and-Forward

The secrecy rate of AF scheme with proposed relay selection is obtained by substituting (3.11) and (3.12) in (3.27) as

$$R_{s_{AF}}(a) = \left[\frac{1}{2}\log_2\left(1+a\gamma_{SD}+\frac{a(1-a)\gamma_{SR_k}\gamma_{R_kD}}{1+a\gamma_{SR_k}+(1-a)\gamma_{R_kD}}\right)-\frac{1}{2}\log_2\left(1+a\gamma_{SE}+\frac{a(1-a)\gamma_{SR_k}\gamma_{R_kE}}{1+a\gamma_{SR_k}+(1-a)\gamma_{R_kE}}\right)\right]^+ \quad (3.29)$$

Decode-and-Forward

For DF transmission scheme, the secrecy rate is obtained by substituting (3.15) and (3.16) in (3.27) and is therefore expressed as

$$R_{s_{DF}} = \left[\frac{1}{2}\min\left\{\log_2\left(1+a\gamma_{SR_k}\right),\log_2\left(1+a\gamma_{SD}+(1-a)\gamma_{R_kD}\right)\right\}-\frac{1}{2}\log_2\left(1+a\gamma_{SE}+(1-a)\gamma_{R_kE}\right)\right]^+ \quad (3.30)$$

3.5.2 Optimal Power Allocation

For achieving maximum secrecy, we need to optimize the power allocation factor '*a'* in the secrecy rates given in (3.29) and (3.30). The secrecy rate maximization is done by gradient-based method and exhaustive search algorithm.

Gradient-Based Method (GB)

In the gradient-based method of optimization, the problem of secrecy rate maximization can be done by means of differentiation i.e., to findthe optimum value of '*a*' that gives the maximum secrecy rate.

$$Max\ achievable\ rate = \arg\max_{a}\left(R_s\right) \quad (3.31)$$

The computational complexity of gradient method of optimization is found to be *O (n*); where *n* is the size of the input variable (Coello C.A.C., 2018).

Steps to compute the derivative function

In the gradient-based method of optimization, the secrecy rate maximization can be done by means of derivative test. Derivative test uses the derivatives of the function to locate the critical points and determine whether each point is a local maximum, a local minimum or a saddle point. It also gives information about the concavity of a function.

i. Find the derivative of the function R_s, $\frac{dR_s}{da}$

ii. Solve for all a that satisfies the equation, $\frac{dR_s}{da}$ =0; to find the critical points, i.e., the points at which the function may have maximum or minimum.

iii. Find the second derivative of R_s; $\frac{d^2R_s}{da^2}$ at critical points. This gives a set of values. The critical point at which the second derivative yields negative value is the optimum value and the value of secrecy rate at that point gives maximum secrecy rate.

The optimization for equations (3.29) and (3.30) is carried out by Matlab simulation.

For the case of DF, the SNR at destination is calculated first, by taking the minimum of SNR at the relay and that at the destination. Then it is applied in the secrecy rate equation (3.30) and then derivative tests are performed to find the optimum value. The results of optimal power allocation factor and maximum secrecy rate are presented in Table 3.3.

Exhaustive Search Method (ES)

The algorithm that tries every possible solution of an objective function is known as exhaustive search. It is the simplest of all search methods. This method evaluates the objective function at a predetermined number of equally spaced points δ. After finding the function values for all the possible combinations of dependent variables, the maximum function value is identified and the parameters that provide the maximum function value are considered as optimal values. Although exhaustive search is conceptually simple and often effective, such an approach to problem solving is sometimes considered inelegant (J Nievergelt, 2000). The computational complexity of exhaustive search algorithm is found to be $O(2^n)$.

3.6 Numerical Results and Analysis

In this section, the results based on numerical computations for the two-hop AF and DF cooperative schemes are presented to validate the performance of the proposed relay selection algorithm. A two-dimensional topology for the simulation setup is considered as shown in Fig. 3.3, where the coordinates of the source and destination are at points (0, 0) and (10, 0) respectively and N trusted relays are distributed dispersedly between them. The eavesdropper is moved from source to destination, i.e., from (0, 10) to (10, 10). Monte-Carlo simulations with 10^5 independent trials are executed to find the results. The effect of *(i)* the relevance parameters *(α* and *β)* of the proposed algorithm; *(ii)* power allocation factor (a); and *(iii)* the number of relay nodes (N); on secrecy rate are examined and the

results are presented. For EPA strategy, equal power is allocated to source and relay nodes, and for OPA, derivative method and exhaustive search algorithms are used for power optimization. Rayleigh fading channel is assumed. The summary of the simulation parameters are presented in the Table 3.2.

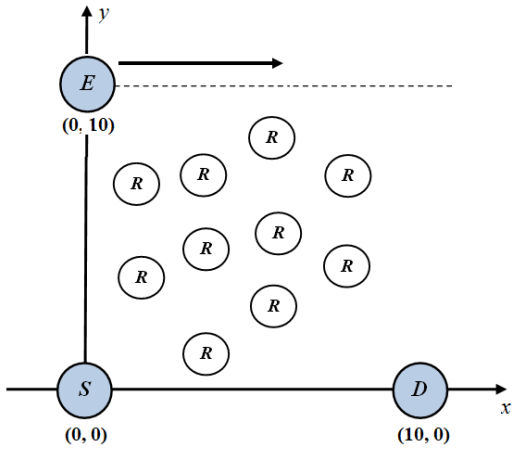


Fig. 3.3 Network topology

Table 3.2 Simulation Parameters

Parameters	**Specification**
Total transmit power (P)	30 dBm
Path loss coefficient (L)	3
Number of relay nodes (N)	20
SNR	10 dB
Power allocation factor for EPA (a)	0.5

Fig. 3.4 presents the secrecy performance of AF and DF transmission protocols with proposed and traditional BRS and PRS schemes for α

$= \beta = 2$. For proposed AF and DF BRS schemes, (3.23) and (3.25) respectively are used for selecting the relay and for proposed AF and DF PRS schemes, (3.20) is used for selecting the relay. Similarly, (3.24) and (3.26) are used to find the relay for traditional AF and DF BRS schemes respectively whereas (3.21) is used for selecting the relay for AF and DF PRS schemes. Then the secrecy rate is computed by using (3.29) and (3.30) for AF and DF respectively. In the simulation model, the curves for the proposed and traditional schemes overlap as the best relay selected is the same in both cases. With the same performance as traditional algorithm, the proposed algorithm has the flexibility to find the secrecy rate in three different cases, i.e., in the case of a traditional wireless scenario, in a fading and path loss models and its performance is illustrated in Fig. 3.5.

It is evident from the figure that secrecy increases with source-eavesdropper distance. This is because when the distance between the source and eavesdropper increases, the received signal power at the eavesdropper from both the source and relay decrease, which increases the secrecy. The eavesdropper has more chance to intercept the information when it comes near to the source and therefore system becomes insecure. Since only source to relay channel is considered in PRS, it shows poor performance when compared to BRS. For DF transmission scheme, we take the assumption that the relay completely decodes the message. This is because the selected relay produces less decoding errors as its channel has got good channel properties compared to other relays. With this assumption, DF protocol shows better secrecy performance compared to AF for both PRS/BRS schemes.

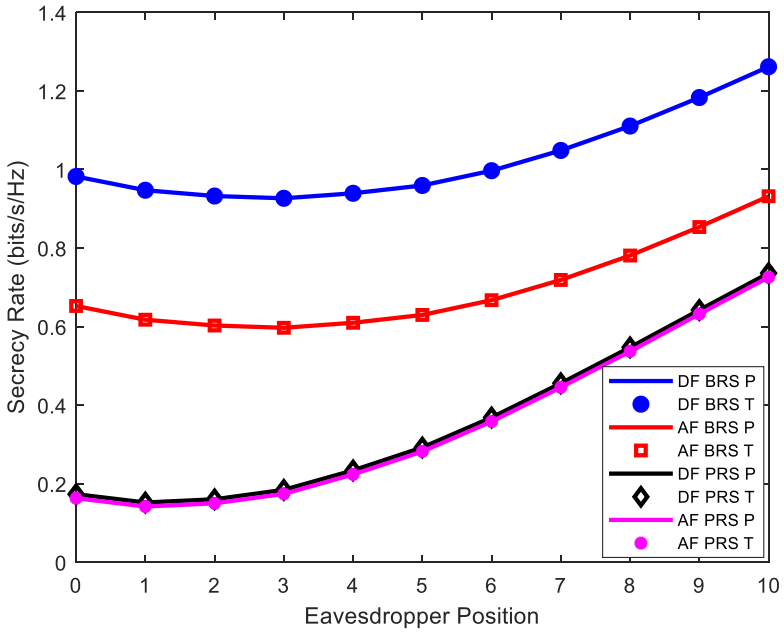


Fig. 3.4 Secrecy performance of AF/ DF protocols with proposed and traditional BRS and PRS schemes

The proposed relay selection algorithm finds the secrecy rate in three wireless scenarios depending on the values of the relevance parameters α and β and is illustrated in Fig. 3.5. The scenario maps to *i)* a traditional wireless model for equal values of α and β , where both *G* and *h* are given equal preference; *ii)* a fading model when α is zero and β is non-zero, where only *h* is significant; and *iii)* a path loss model when β is zero and α is non-zero, where only *G* is significant. For the simulation, we chose the values as $\alpha = \beta = 2$ for the traditional model $\alpha = 0$ and $\beta = 2$ for fading model and $\alpha = 2$ and $\beta = 0$ for the path loss model. If we consider the same channel coefficients, for both AF and DF protocols, the secrecy performance for equal values of α and β is the highest, and the system exhibits the

same secrecy performance as traditional best relay selection scheme. For unequal α and β values, the secrecy performance is less as the relevance of one of the parameters is varied with respect to other. If one of the parameters is zero as in the second and third cases, the influence of only non-zero parameter is considered; hence secrecy is reduced. Thus by choosing relevance parameters different wireless scenarios can be selected. This shows the flexibility of the proposed relay selection scheme that can be applied to different wireless scenarios. The path selection process of ACO algorithm was explained in Table 3.1.

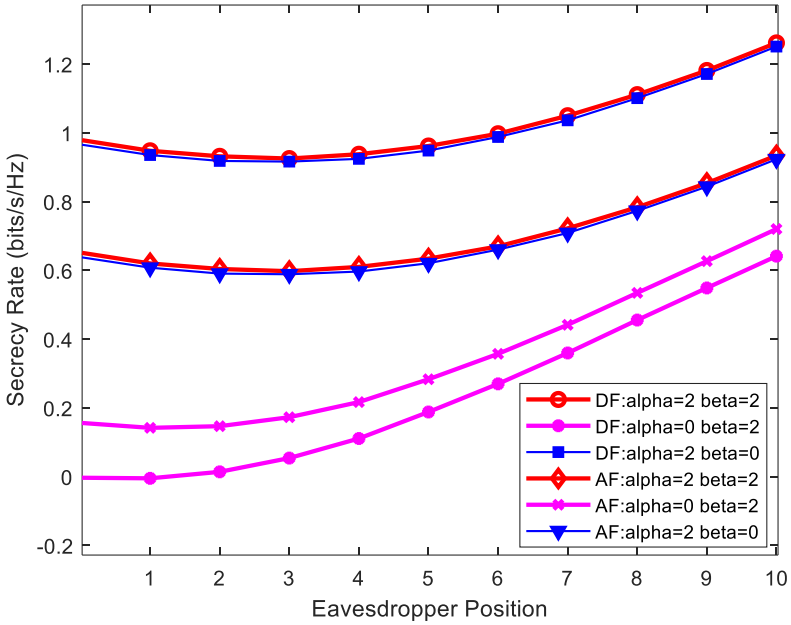


Fig. 3.5 Secrecy performance of proposed AF/DF BRS scheme for different values of relevance parameters

Fig. 3.6 illustrates the secrecy performance on power allocation factor a when eavesdropper lies near to source, with $\alpha = \beta = 2$. The

eavesdropper near to source is considered for the analysis as it is the worst case of insecurity; since it gets more chance to interrupt the signal than when it is away from the source. Power requirement in cooperative networks depends on the position of relay and eavesdropper. For PRS, relay close to source is selected and for BRS, relay at the center of the network model is selected as best relays. Therefore, PRS requires less source power P_s for transmission than that required for BRS. The maximum secrecy is reached when $a = 0.5$ for BRS and $a = 0.1$ for PRS; i.e., when $P_s = 0.5$W and 0.1W for BRS and PRS schemes respectively. As discussed before, for the case when relay can decode the exact signal transmitted, the performance of DF is better for both schemes. It is clear from the figure that PRS does not show considerable performance improvement as only source to relay channel is considered. For other eavesdropper positions, performance is similar to worst case, but with high secrecy due to increase in the source-eavesdropper distance.

Fig. 3.7 shows the effect of number of relay nodes N on secrecy when the eavesdropper is near to source. For AF and DF protocols, the secrecy increases with relay nodes for both PRS/BRS schemes. This is because the probability of choosing a better helper increases when more number of intermediate nodes is deployed. This in turn shows the benefits of using multiple relays against eavesdropping. However, it can be seen from the figure that when the number of relay nodes continues to increase, the secrecy rate increases slowly and gets saturated. This indicates that there is a limit to improve the secrecy through increasing the relay nodes (Li Wang *et al.*, 2014).

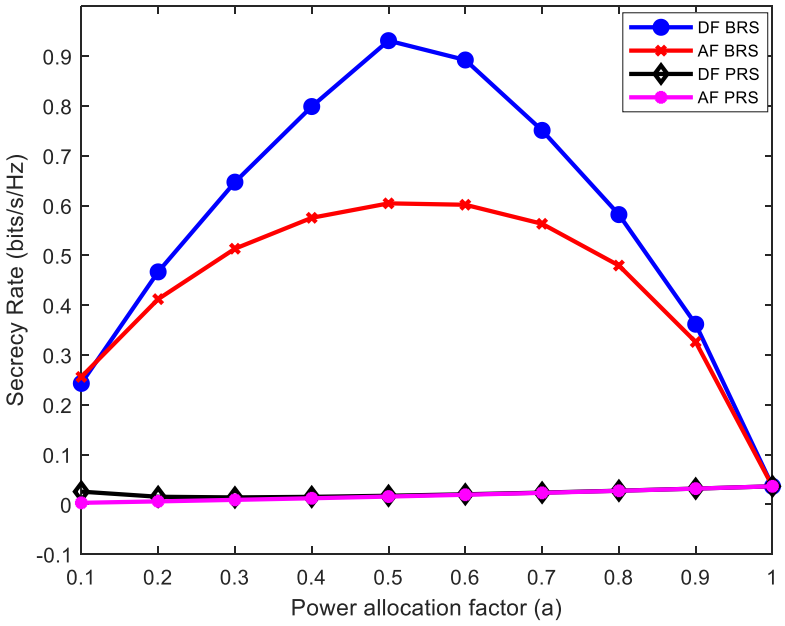


Fig. 3.6 Effect of ***a*** on secrecy for the proposed AF/DF schemes

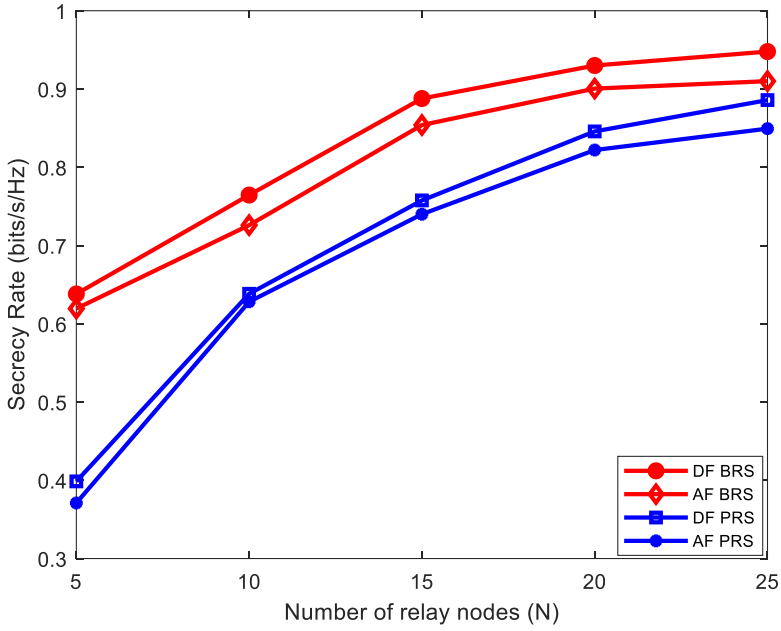


Fig. 3.7 Effect of number of relay nodes on secrecy for the proposed AF/DF transmission schemes

In Fig. 3.8 *a* and Fig. 3.8 *b*, the variation of β for $\alpha = 1$ and $\alpha = 5$ for AF and DF schemes is plotted against secrecy for eavesdropper near to source i.e., E (0, 10). The best relay and hence the secrecy rate depends on the values of relevance parameters α and β. For both the curves, the secrecy rate is maximum for equal values of relevance parameters but it decreases when one of the parameters is varied with respect to other, i.e., for $\alpha = 1$, secrecy rate reduces with increase in β, and for $\alpha = 5$, secrecy increases with β giving its maximum at $\beta = 5$ and thereafter it reduces. For fixed α and $\alpha > \beta$, if the relevance of β increases secrecy increases and vice versa. The advantage of choosing high α and β values is that, the variation can be done over a wide range depending upon the network scenario, which further helps to analyse the performance of the system under consideration.

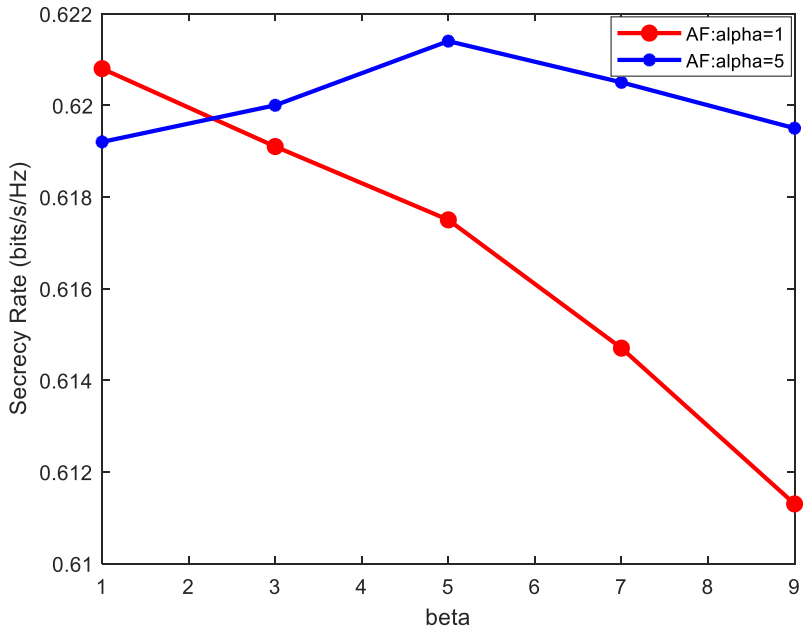


Fig. 3.8*a* Secrecy versus β of proposed AF BRS scheme for α =1 & 5

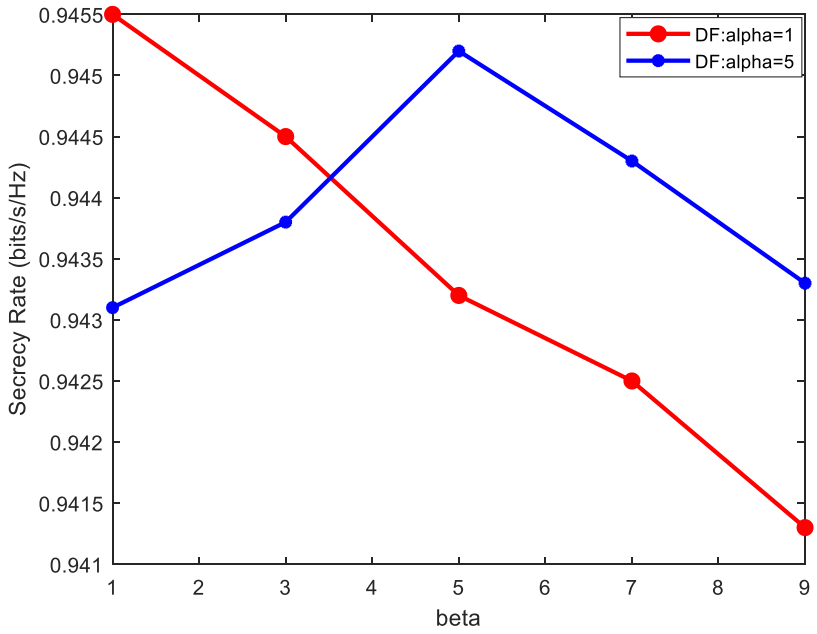


Fig. 3.8*b* Secrecy versus β of proposed DF BRS scheme for α =1 & 5

Table 3.3 gives the comparison of the power optimization by gradient-based and exhaustive search algorithms with EPA strategy; for the case of best relay position. The gradient-based method uses second derivative test to find the maxima of the function; i.e., the concavity of the function at a critical point determines whether it has got a maximum/minimum at that point. Exhaustive search method is the simplest of all search methods, accurate results could be obtained for smaller step size δ or larger number of iterations *m*. But this method is computationally inefficient and time consuming.

The results presented in the table for the BRS and PRS schemes show that the secrecy with OPA methods is better compared with that of EPA strategy. For BRS, the best relay is the one that has the same

source-relay SNR (γ_{sr}) and relay-destination SNR (γ_{rd}) and normally it lies at the centre of the network model and therefore requires same source and relay powers. For PRS, relay close to source is selected and therefore it requires less $P_{s.}$ Therefore EPA with PRS shows less secrecy performance when compared to OPA methods. A good match could be observed between the results of derivative and exhaustive search methods from the table.

Table 3.3 Comparison of OPA and EPA results

Transmission protocol	Relay selection scheme	Derivative Method		Exhaustive search method *m = 20*		EPA	
		a	R_s	*a*	R_s	a	*Rs*
AF	BRS	0.5029	0.6523	0.5	0.6509	0.5	0.65
	PRS	0.1461	0.2184	0.15	0.2181	0.5	0.1612
DF	BRS	0.5999	1.06362	0.55	0.9951	0.5	0.934
	PRS	0.0213	0.18602	0.025	0.2681	0.5	0.174

A comparison of OPA/EPA based secrecy rate as a function of eavesdropper position for AF is illustrated in Fig. 3.9. The OPA with gradient method shows better performance compared with other methods. Power is allocated based on the position of relays and eavesdropper in OPA; whereas in EPA equal power is allocated, hence EPA shows less performance for the relays near to source and destination. EPA performance is good only for symmetric case when $\gamma_{sr} = \gamma_{rd}$; i.e., for the relay at the centre of the network model as is the case with BRS. Similar is the performance with DF scheme.

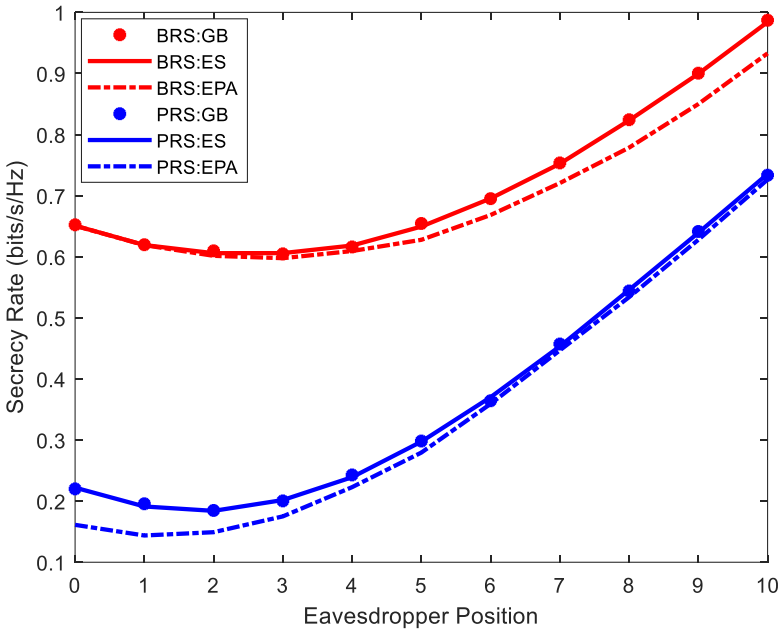


Fig. 3.9 Comparison of OPA and EPA results of AF BRS/PRS schemes

3.7 Chapter Summary

This chapter proposed a relay selection technique based on the probability of path selection criterion of Ant Colony Optimization algorithm, for two-hop cooperative networks employing amplify-and-forward and decode-and-forward transmission protocols, in the presence of a passive eavesdropper. By equal power and optimal power allocation strategies, the secrecy is evaluated in three wireless scenarios namely traditional, path loss and fading models; depending on the significance of channel gain and fading coefficients of the path. The performance is evaluated for partial relay selection and best relay selection schemes and for different eavesdropper position. Numerical results by Monte Carlo simulations through MATLAB show the

merits of the proposed relay selection scheme in terms of secrecy rate in different wireless scenarios as compared to traditional schemes. The effect of number of relay nodes on secrecy is also examined. It is found that increasing the number of relay nodes improves the secrecy rate for both AF and DF BRS/PRS schemes, showing the advantage of exploiting multiple relays against eavesdropping. However, when the number of relay nodes continues to increase, the secrecy rate increases slowly and gets saturated.

Perfect secrecy cannot be always guaranteed by relay selection techniques because the secrecy rate will reduce or even drop to zero when the legitimate channel conditions are poor. Cooperative jamming is an efficient technique to overcome this problem. The proposed relay selection algorithm based on ACO, exploiting the channel gain and fading coefficients is used in the jamming schemes addressed in the following chapters.

Chapter 4
Enhancing Secrecy via Power Optimized Source and Relay Based Jamming

4.1 Introduction

Cooperative communication can efficiently mitigate the effect of fading with the help of relays and proper relay selection techniques. In a cooperative communication system intermediate nodes are utilized as relays to forward the data from source to destination over independent wireless channels. Relay selection in the cooperative system; where a single relay or subset of relays are used to forward data; has been considered as an effective method to improve the performance of cooperative communication (A. Bletsas *et al.*, 2006; A. Bletsas *et al.*, 2007; X. Chen *et al.*, 2011). Relay selection overcomes the inefficient spectral usage of cooperative relays. However, when it comes to secrecy, it cannot always guarantee perfect secrecy because the secrecy rate will reduce or even drop to zero when the legitimate channel conditions are poor. Cooperative jamming (CJ) is an efficient technique to overcome this problem.

Recently, cooperative jamming has emerged as a promising technique to enhance wireless PLS (R. Liu and W. Trappe, 2010). The jamming signals in cooperative jamming technique can create interference at the eavesdropper; thereby reduces the SNR at the eavesdropper which further enhances the secrecy. The power allocated to the jamming signal should be high enough to interrupt the received signal at the eavesdropper; however allocating too much

power on the jamming signal can degrade the signal quality at the destination. Thus, it is essential to assign optimum power to the jamming signals so as to maximize the secrecy rate (L Dong *et al.*, 2010). Cooperative jamming techniques can be implemented by the networks nodes, i.e., source, relay or destination; or two of the nodes, i.e., source and destination or source and relay to transmit the jamming signals. Accordingly, CJ is of source based jamming (SBJ), friendly jammer based jamming, destination based jamming (DBJ) and hybrid jamming; depending on which node/nodes are transmitting the jamming signals.

In this chapter, an OPA scheme based on gradient-free optimization algorithm for a hybrid jamming scheme is proposed to enhance the secrecy of cooperative relay networks. Being a low complexity protocol, AF relaying protocol is used in the work. The proposed source and relay based jamming scheme (SRBJ) allows the source and selected relay to transmit the jamming signal along with the information in order to degrade the eavesdropper. The performance based on secrecy rate is evaluated for N trusted relays distributed randomly between the source and destination. The best relay in the network model is selected based on the path probability selection criterion of ACO algorithm, which is explained in Section 3.4.

This chapter is an extension of the work presented in (A Li *et al.*, 2015) with cooperative relays and OPA problem. In contrast to (A Li *et al.*, 2015), where only one relay node without power optimization is considered to ensure security, the problem of multiple relays and relay selection technique together with OPA is considered here. OPA

strategy normally adopts gradient-based optimization methods to maximize the secrecy rate. But, gradient-based methods have problems with noisy and discontinuous functions, non-differentiable functions and/or constraints, mixed variable functions or functions of large dimensionality (J. A. Nelder and R. Mead, 1965; Joaquim R. R. A. Martins, 2012). Since the secrecy rate in the proposed method is a non-linear function of three independent variables, it is difficult to find the partial derivatives of the function at all relay positions so as to do the gradient-based optimization for maximizing the secrecy. So, Nelder-Mead method, a gradient-free optimization method is used here for power optimization (J. A. Nelder and R. Mead, 1965). In addition to that, we also analysed the power allocation problem based on two benchmark schemes - gradient-based optimization and three-dimensional exhaustive search algorithms. The secrecy performance is compared with conventional AF and jamming scheme without power optimization (EPA) and impact of single and multiple relays on secrecy performance is also evaluated. Numerical results reveal that, compared with the gradient-based method and exhaustive search algorithm, the proposed power allocation strategy achieves better performance. Also, the proposed OPA results show a significantly higher secrecy rate than the EPA strategy for both SRBJ and AF schemes.

4.2 Transmission Scheme

4.2.1 Source and Relay Based Jamming Scheme

The system model given in Fig. 3.1 is considered here. A practical scenario where random distribution of intermediate nodes between

the source and destination, and direct links exist between source to destination (S-D) and source to eavesdropper (S-E) are considered. Here, the source and the selected relay send jamming signals along with the information in order to degrade the eavesdropper with the assumptions that a legitimate receiver (relay or destination) has apriori knowledge of the jamming signal, which could be implemented in practice with a small amount of overhead (L Dong *et al.*, 2011). Assuming the channels to be quasi-static and the channel knowledge is available; the jamming signals can be completely removed from the signal received at the legitimate receivers. The proposed transmission scheme is shown in Fig. 4.1.

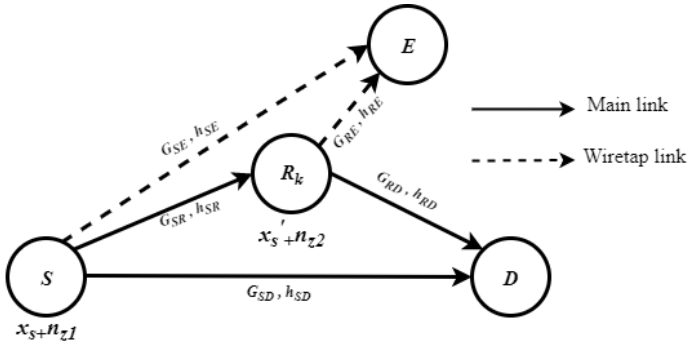


Fig. 4.1 Proposed transmission model

The relay R is the selected trusted relay, n_{z1} and n_{z2} are the jamming signals added at the source and relay respectively. Since the relays operate in half-duplex mode, they cannot transmit and receive simultaneously. Hence, the signal transmission involves two phases, i.e., the broadcast phase and the relaying phase. The source broadcasts the signal x_s with power aa_sP and jamming signal n_{z1} with power $a(1-a_s)P$ during the broadcast phase of the transmission. $a \in$

(0,1) and $a_s \in (0,1)$ denote respectively the power allocation between the source and relay and between the information (x_s) and jamming signal(n_{z1}) at the source.

The signal from the source is given by

$$x = \sqrt{aa_s P}x_s + \sqrt{a(1-a_s)P}n_{z_1} \tag{4.1}$$

The wireless channel is characterized by the channel gain *G* and fading coefficients *h* (M. Dohler, Y. Li, 2010). The signal received at the k^{th} relay, destination and eavesdropper is expressed as

$$y_{SR_k} = \sqrt{aa_s P}G_{SR_k}h_{SR_k}x_s + \sqrt{a(1-a_s)P}G_{SR_k}h_{SR_k}n_{z_1} + n_{R_k} \tag{4.2}$$

$$y_{SD} = \sqrt{aa_s P}G_{SD}h_{SD}x_s + \sqrt{a(1-a_s)P}G_{SD}h_{SD}n_{z_1} + n_{D_1} \tag{4.3}$$

$$y_{SE} = \sqrt{aa_s P}G_{SE}h_{SE}x_s + \sqrt{a(1-a_s)P}G_{SE}h_{SE}n_{z_1} + n_{E_1} \tag{4.4}$$

The channel gain G_{ij} between the nodes *i* and *j* is dependent on the distance between the nodes and is given by (3.4). We assume that the channel gains are acquired from CSI of a system by using a reference signal and all relays in the system are aware of the used power for the transmission of a signal. The relay selection is done prior to the second phase of transmission. The relay cancels out the noise from the source as it has apriori knowledge of the same.

During the second phase, the selected relay amplifies and forwards the signal with another jamming signal n_{Z2} independent of n_{Z1} to destination. The powers allocated to the information and jamming signals from the relay are $(1\text{-}a)a_r P$ and $(1\text{-}a)(1\text{-}a_r)P$ respectively, where $a_r \in (0, 1)$ denotes the PA between the information (x_{Rk}) and

jamming signal (n_{z2}) at the selected relay. The signal transmitted by the relay is therefore expressed as

$$x_{R_k} = \sqrt{(1-a)a_r P}\, g\; y_{SR_k} + \sqrt{(1-a)(1-a_r)P}\, n_{z_2} \tag{4.5}$$

The amplification factor g at the k^{th} relay (ratio of the relay power to the power of the received signal at the k^{th} relay) is

$$g = \sqrt{\frac{(1-a)P}{\left|G_{SR_k} h_{SR_k}\right|^2 a a_s P + {\sigma_R}^2}} \tag{4.6}$$

The power of the signal received at the relay is obtained from (4.2). The received signal at the destination and eavesdropper nodes with the assumption that the vector g is known at the destination and eavesdropper is

$$\begin{aligned} y_{R_k D} = {} & \sqrt{a a_s a_r P} G_{SR_k} h_{SR_k} G_{R_k D} h_{R_k D}\, g\; x_s + \sqrt{a_r} G_{R_k D} h_{R_k D}\, g\; n_{R_k} + \\ & \sqrt{(1-a)(1-a_r)P} G_{R_k D} h_{R_k D} n_{z_2} + n_{D_2} \end{aligned} \tag{4.7}$$

$$\begin{aligned} y_{R_k E} = {} & \sqrt{a a_s a_r P} G_{SR_k} h_{SR_k} G_{R_k E} h_{R_k E}\; g\; x_s + \sqrt{a_r} G_{R_k E} h_{R_k E}\; g\; n_{R_k} + \\ & \sqrt{(1-a)(1-a_r)P} G_{R_k E} h_{R_k E}\; n_{z_2} + n_{E_2} \end{aligned} \tag{4.8}$$

The destination node cancels out the noise and the overall SNR applying MRC is given by

$$\begin{aligned} \gamma_{D_{SRBJ}} &= a a_s P \frac{\left|G_{SD} h_{SD}\right|^2}{{\sigma_D}^2} + \frac{g^2 a a_s a_r P \left|G_{SR_k} h_{SR_k}\right|^2 \left|G_{R_k D} h_{R_k D}\right|^2}{g^2 a_r \left|G_{R_k D} h_{R_k D}\right|^2 {\sigma_R}^2 + {\sigma_D}^2} \\ &= a a_s \gamma_{SD} + \frac{a(1-a) a_s a_r \gamma_{SR_k} \gamma_{R_k D}}{1 + a a_s \gamma_{SR_k} + (1-a) a_r \gamma_{R_k D}} \end{aligned} \tag{4.9}$$

The SNR at the eavesdropper applying MRC is given by

$$\gamma_{E_{SRBJ}} = \frac{aa_s P\left|G_{SE}h_{SE}\right|^2}{a(1-a_s)P\left|G_{SE}h_{SE}\right|^2+{\sigma_E}^2} + \frac{g^2 aa_s a_r P\left|G_{SR_k}h_{SR_k}\right|^2\left|G_{R_kE}h_{R_kE}\right|^2}{g^2 a_r\left|G_{R_kE}h_{R_kE}\right|^2{\sigma_R}^2+(1-a)(1-a_r)P\left|G_{R_kE}h_{R_kE}\right|^2+{\sigma_E}^2}$$

$$= \frac{aa_s\gamma_{SE}}{1+a(1-a_s)\gamma_{SE}} + \frac{a(1-a)a_s a_r\gamma_{SR_k}\gamma_{R_kE}}{1+aa_s\gamma_{SR_k}+(1-a)\gamma_{R_kE}+a(1-a)a_s(1-a_r)\gamma_{SR_k}\gamma_{R_kE}} \quad (4.10)$$

where γ_{ij} , the instantaneous SNR between the nodes *i* and *j* is given by (3.10)

Assume that all the noise variances are equal. i.e., ${\sigma_R}^2 = {\sigma_D}^2 = {\sigma_E}^2$. The destination cancels out the noises send by the source and relay, which enhances the reliability results from cooperation diversity.

4.2.2 Performance Analysis

The instantaneous secrecy rate for the proposed jamming scheme is obtained by substituting (4.9) and (4.10) into (3.17).

$$R_{S_{SRBJ}} = \left[\frac{1}{2}\log_2\left(\frac{1+\gamma_{D_{SRBJ}}}{1+\gamma_{E_{SRBJ}}}\right)\right]^+$$

$$= \left[\frac{1}{2}\log_2\left(\frac{1+aa_s\gamma_{SD}+\frac{a(1-a)a_s a_r\gamma_{SR_k}\gamma_{R_kD}}{1+aa_s\gamma_{SR_k}+(1-a)a_r\gamma_{R_kD}}}{1+\frac{aa_s\gamma_{SE}}{1+a(1-a_s)\gamma_{SE}}+\frac{a(1-a)a_s a_r\gamma_{SR_k}\gamma_{R_kE}}{1+aa_s\gamma_{SR_k}+(1-a)\gamma_{R_kE}+a(1-a)a_s(1-a_r)\gamma_{SR_k}\gamma_{R_kE}}}\right)\right]^+ \quad (4.11)$$

where $[x]^+ = \max\{0, x\}$; and the secrecy rate becomes (Lu Lv *et al.*, 2017),

$$\overline{R_{S_{SRBJ}}}(a,a_s,a_r)=$$

$$\max_{a,a_s,a_r\in(0,1)} \mathbf{E}\left[\frac{1+aa_s\gamma_{SD}+\frac{a(1-a)a_sa_r\gamma_{SR_k}\gamma_{R_kD}}{1+aa_s\gamma_{SR_k}+(1-a)a_r\gamma_{R_kD}}}{1+\frac{aa_s\gamma_{SE}}{1+a(1-a_s)\gamma_{SE}}+\frac{a(1-a)a_sa_r\gamma_{SR_k}\gamma_{R_kE}}{1+aa_s\gamma_{SR_k}+(1-a)\gamma_{R_kE}+a(1-a)a_s(1-a_r)\gamma_{SR_k}\gamma_{R_kE}}}\right] \quad (4.12)$$

The best relay R_k is selected using the probability of path selection criterion of ACO algorithm (3.23). NM method is applied to the function in (4.11) to estimate the optimal values of a, a_s and a_r for maximizing the secrecy rate. Since NM method finds the minimum of a function, the function is inverted to get the maximum value. For EPA scheme, the secrecy is obtained by taking $a = a_s = a_r = 0.5$. In this algorithm, the power is optimally allocated between the signals; hence $R_s \geq 0$ is achievable.

4.3. Nelder-Mead Algorithm for Optimal Power Allocation

4.3.1 Introduction

The Nelder-Mead (NM) algorithm is a gradient-free optimization method devised by J.A. Nelder and R. Mead in 1965. It is one of the most widely used methods for multidimensional non-linear unconstrained optimization (J. A. Nelder and R. Mead, 1965). The benefits of gradient-free optimization method are *i)* its ability to solve problems that are difficult to solve using gradient-based methods *ii)* it does not require any derivative function for computation and *iii)* the objective function need not be smooth. However, this method has problems with large number of design variables; i.e., if the number of variables exceeds ten, convergence would be really difficult (Emmerich M.T.M., Deutz A.H, 2018).

NM algorithm is used for minimizing a function f of n variables

depending on the function values at (n+1) vertices of a general simplex (J. A. Nelder and R. Mead, 1965). The simplex is a geometric figure in n dimensions with n+1 vertex. A simplex with vertices $x_1, x_2, \ldots, x_{n+1}$ is denoted by Δ. The algorithm starts with this simplex and then modifies it at each iteration using four operations namely reflection, expansion, contraction and shrinking. The operations to be performed are selected on the basis of the relative values of the objective function at each point. After each iteration, the vertices $\{x_i\}_{i=1}^{n+1}$ are ordered according to the function values

$$f(x_1) \leq f(x_2) \leq \ldots\ldots \leq f(x_{n+1}) \tag{4.13}$$

Because we seek to minimize the function f, we refer to $\boldsymbol{x}_1$ as the *best* vertex and to $\boldsymbol{x}_{n+1}$ as the *worst* vertex. After each iteration, the worst vertex, where the function value is the largest, is removed and replaced with a new vertex. This forms a new simplex and the search is continued. At the end, the vertex of the simplex that yields that most optimal objective value is returned (John H Mathews and Kurtis K Fink, 2004). Four scalar parameters are defined for NM method: coefficient of reflection (ρ), expansion (ψ), contraction (ε), and shrinkage (γ). According to (J. A. Nelder and R. Mead, 1965), these parameters should satisfy

$$\rho > 0;\ \psi > 1;\ \psi > \rho;\ 0 < \varepsilon < 1; \text{ and } 0 < \gamma < 1 \tag{4.14}$$

The universally accepted standard values for the NM algorithm are

$\rho = 1;\ \psi = 2;\ \epsilon = ½$; and $\gamma = ½$.

Since the secrecy rate of the proposed work is dependent on three

variables corresponding to the power allocation factors a, a_s and a_r; the simplex is a tetrahedron (4 vertices) in 3-dimensional space.

4.3.2 Steps in NM Algorithm

The main steps in NM algorithm are presented here (Fuchang Gao, Lixing Han, 2010). Let the function to be minimized be f which is our R_s.

1. Generate the simplex

The first step of the simplex algorithm is to find the n+1 points of the simplex, given an initial guess x_o. This can be easily done by simply adding a step to each component of x_o to generate n new points. Simplex of equal length is preferred; assuming that the length of all sides is r (r = 1), and the initial guess x_o be the $(n+1)^{th}$ point. The other vertices of the simplex are obtained by adding a vector to the initial guess, whose components are all q except for the i^{th} component which is set to p, where

$$q = \frac{r}{n\sqrt{2}}\left(\sqrt{n+1}-1\right) \tag{4.15}$$

$$p = q + \frac{r}{\sqrt{2}} \tag{4.16}$$

In our case, n = 3, so there are 4 vertices; each vertex is having three components corresponding to the power allocation factors - a, a_s and a_r . Therefore, for a simplex of three variables, the four vertices {x_1, x_2, x_3, x_4} are [p, q, q], [q, p, q], [q, q, p] and the initial guess x_o. The initial guess for the proposed scheme is taken as [0.5, 0.5, 0.5], assuming that the EPA provides fairly good results. After generating the initial simplex, evaluate the function at the four vertices of Δ, and order them so as to satisfy (4.13).

2. Reflection

The reflection point x_r is computed as

$$x_r = \bar{x} + \rho(\bar{x} - x_{n+1}) \tag{4.17}$$

where the centroid of n best vertices $\bar{x}$ is defined as

$$\bar{x} = \sum_{i=1}^{n} \frac{x_i}{n} \tag{4.18}$$

The function is then evaluated at x_r; if $f(x_1) \leq f(x_r) < f(x_n)$, replace x_{n+1} with x_r.

3. Expansion

If $f(x_r) < f(x_1)$, the expansion point x_e is computed as

$$x_e = \bar{x} + \psi(x_r - \bar{x}) \tag{4.19}$$

The function value at x_e is evaluated; if $f(x_e) < f(x_r)$, replace x_{n+1} with x_e, otherwise replace x_{n+1} with x_r.

4. *Outside contraction*

If $f(x_n) \leq f(x_r) < f(x_{n+1})$, outside contraction is performed

$$x_{oc} = \bar{x} + \varepsilon(x_r - \bar{x}) \tag{4.20}$$

Evaluate the function at x_{oc}; if $f(x_{oc}) \leq f(x_r)$, replace x_{n+1} with x_{oc}; otherwise shrink (step 6).

5. *Inside contraction*

If $f(x_r) \geq f(x_{n+1})$, inside contraction is done

$$x_{ic} = \bar{x} - \varepsilon(x_r - \bar{x}) \tag{4.21}$$

The function at x_{ic} is evaluated: If $f(x_{ic}) \leq f(x_{n+1})$, replace x_{n+1} with x_{ic} ; otherwise shrink (step 6).

6. *Shrink*

For $2 \leq i \leq n+1$, define shrinking function as

$$x_i = x_1 + \gamma\,(x_i - x_1) \tag{4.22}$$

This completes the iteration and new simplex is formed with new points for the next iteration.

The structure of NM algorithm is shown in Fig. 4.2.

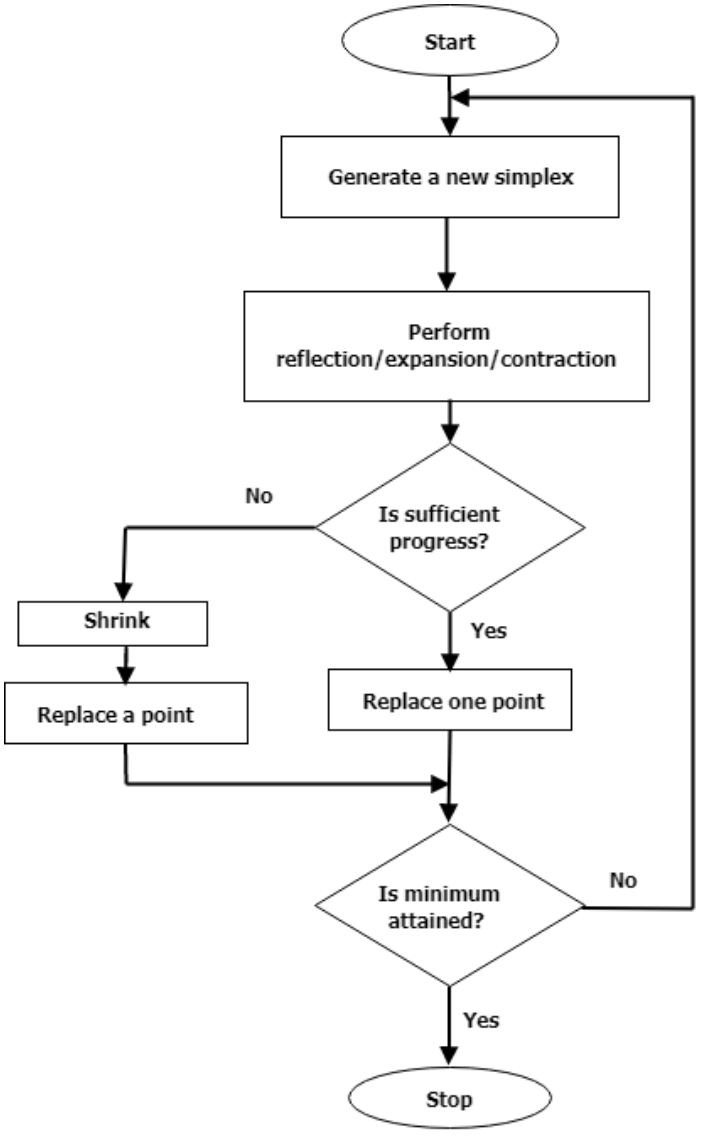


Fig. 4.2 Flowchart of NM algorithm

4.3.3 Computational Complexity of NM Algorithm

If $y(n)$ represents the number of operations needed for the computation of the function $f(x)$, for a given $x \in R^n$; then the worst case behavior for one iteration of NM algorithm is given by (Zhao Q. H. *et al.*, 2009)

i) $\max\{O(n \log n), O(y(n))\}$, if shrinking step is not used

ii) $O(n\, y(n))$, if shrinking step is used. (4.23)

4.4 Benchmark Schemes

4.4.1 Conventional Amplify-and-Forward Scheme (AF)

The conventional AF relaying protocol described in detail in Chapter 3 is used here for comparison. Here, the total power (P) is allocated between the source and relay with $P_s = a_{AF}P$ and $P_r = (1\text{-}a_{AF})P$, where $a_{AF} \in (0, 1)$ is the PA between them. These nodes then transmit the signal with all the available power. The instantaneous secrecy rate for the conventional AF scheme is obtained by (3.29) and it can be expressed as

$$R_{s_{AF}}(a_{AF}) = \left[\frac{1}{2}\log_2 \left(\frac{1 + a_{AF}\gamma_{SD} + \dfrac{a_{AF}(1-a_{AF})\gamma_{SR_k}\gamma_{R_kD}}{1 + a_{AF}\gamma_{SR_k} + (1-a_{AF})\gamma_{R_kD}}}{1 + a_{AF}\gamma_{SE} + \dfrac{a_{AF}(1-a_{AF})\gamma_{SR_k}\gamma_{R_kE}}{1 + a_{AF}\gamma_{SR_k} + (1-a_{AF})\gamma_{R_kE}}} \right) \right]^{+} \quad (4.24)$$

For AF scheme, we need to optimize only one power allocation factor a_{AF} for maximizing the secrecy rate. One dimensional optimization by NM method is not reliable (Lagarias J C *et al.*, 1998), hence derivative method is used. The secrecy rate maximization is done by gradient-based method i.e., by means of differentiation, by taking the derivative of the function to determine the optimum value of a_{AF} that gives the maximum secrecy rate.

4.4.2 Direct Transmission Scheme (DT)

This subsection gives the secrecy rate of conventional direct transmission without relay. In direct transmission scheme, the source transmits a signal x_s, (E ($|x_s|^2$) =1) with power P and this signal is received by the destination and eavesdropper. The SNR at the destination $\gamma_{D_{DT}}$ and eavesdropper $\gamma_{E_{DT}}$ for DT is given by

$$\gamma_{D_{DT}} = \frac{P\left|G_{SD}h_{SD}\right|^2}{{\sigma_D}^2} = \gamma_{SD} \tag{4.25}$$

$$\gamma_{E_{DT}} = \frac{P\left|G_{SE}h_{SE}\right|^2}{{\sigma_E}^2} = \gamma_{SE} \tag{4.26}$$

Therefore, the secrecy rate of conventional direct transmission without relay is

$$R_{s_{DT}} = \log_2\left(\frac{1+\gamma_{SD}}{1+\gamma_{SE}}\right) \tag{4.27}$$

4.4.3 Direct Transmission Scheme With Jamming (DT WJ)

The source transmits the jamming signal along with the information in order to confuse the eavesdropper. If P is the total transmit power, the signal transmitted by the source is

$$x = \sqrt{a_s P}x_s + \sqrt{(1-a_s)P}n_{Z_1} \tag{4.28}$$

where a_s is the power allocation factor at the source. The signal is received at the destination and eavesdropper and the corresponding SNR is

$$\gamma_{D_{DTWJ}} = \frac{a_s P\left|G_{SD}h_{SD}\right|^2}{{\sigma_D}^2} = a_s\gamma_{SD} \tag{4.29}$$

$$\gamma_{E_{DTWJ}} = \frac{a_s P \left| G_{SE} h_{SE} \right|^2}{(1-a_s) P \left| G_{SE} h_{SE} \right|^2 + {\sigma_E}^2} = \frac{a_s \gamma_{SE}}{1+(1-a_s)\gamma_{SE}} \tag{4.30}$$

Therefore, the achievable secrecy rate of DT WJ is

$$R_{s_{DTWJ}} = \log_2 \left(\frac{1+\gamma_{D_{DTWJ}}}{1+\gamma_{E_{DTWJ}}} \right) = \log_2 \left(\frac{1+a_s \gamma_{SD}}{1+\frac{a_s \gamma_{SE}}{1+(1-a_s)\gamma_{SE}}} \right) \tag{4.31}$$

4.5 Numerical Results and Analysis

To verify the validity of the proposed algorithm, the following simulations are conducted. We used the same topology for the simulation setup and the simulation parameters as in Chapter 3. A two-dimensional plane as shown in Fig. 3.2 is assumed, where the coordinates are set to (0, 0) for source and (10, 0) for destination; with *N* trusted relays, and the eavesdropper is moved from S-D. Monte-Carlo experiments with 10^5 independent trials are carried out to obtain the results. $a = a_s = a_r = 0.5$ for EPA strategy; Rayleigh fading channel is assumed. For proposed jamming scheme, the OPA factors and secrecy rate are estimated by NM method, and its performance is compared with gradient-based optimization and exhaustive search algorithms. The secrecy performance of SRBJ is also compared with conventional AF scheme. OPA factors for AF scheme are obtained by gradient-based method and exhaustive search algorithms. The effect of *(i)* the relevance parameters *(*α and β*)* of the proposed algorithm; *(ii)* source and relay signal and noise power allocation factors (a_s and a_r); and *(iii)* the number of relay nodes (*N*); on secrecy rate are examined and the results are presented.

Fig. 4.3 presents the comparison of secrecy performance of the proposed jamming scheme with conventional AF and direct transmission schemes with respect to eavesdropper position. For simulation, equal values of the relevance parameters α and β are considered for the analysis ($\alpha = \beta = 2$) as it gives the best secrecy performance [Fig. 3.5, Chapter 3]. For proposed schemes, the best relay is selected with the chosen α and β values using equation (3.23). The secrecy rate for the proposed model is calculated using (4.12) and that of the benchmark schemes by (4.24), (4.27) and (4.31) for different eavesdropper position.

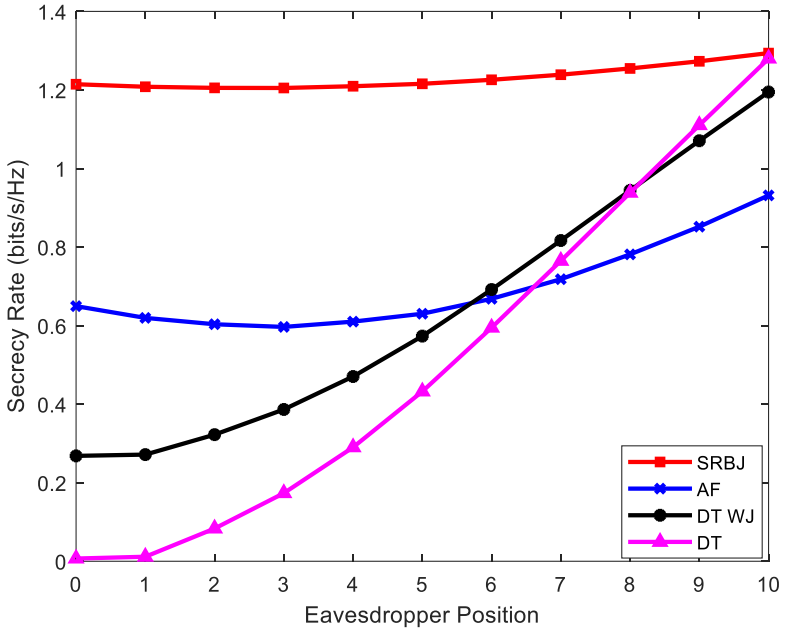


Fig.4.3 Secrecy rate versus eavesdropper position of the proposed and traditional schemes

It is clear from the figure that the secrecy rate of all the schemes increases when the distance between the source and eavesdropper

increases and vice versa. This is because the received signal power at the eavesdropper from both the source and relay decreases with source-eavesdropper distance, hence secrecy increases. The eavesdropper has more chance to intercept the information when it comes near to source and the system becomes insecure. But the jamming signals transmitted from the source and relay can reduce the SNR of the eavesdropper while they have no influence on the SNR of the legitimate channel. Therefore, performance with jamming is better than that of the system without jamming; i.e., SRBJ outperforms the other schemes. Further, the negative secrecy rate of DT is improved by jamming as in DT WJ scheme.

Fig. 4.4 shows the secrecy rate versus eavesdropper's position of proposed SRBJ and traditional AF relaying schemes for different values of relevance parameters α and β. Since the channel gain G and fading coefficients h defining a wireless channel are considered separately, the proposed algorithm has the flexibility to find the secrecy rate in three different cases, i.e., in the case of a traditional wireless scenario, in a fading and pathless models. The model maps to *i)* a traditional wireless model when $\alpha = \beta = 2$, *ii)* a fading model when $\alpha = 0$ and $\beta = 2$ and *iii)* a path loss model when $\alpha = 2$ and $\beta = 0$. Equal values of α and β correspond to a traditional wireless scenario where both G and h are given equal preference**.** The secrecy is highest for equal values of α and β irrespective of their numerical values, if we use the same simulation parameters. For unequal α and β values, the secrecy performance is less as the relevance of one of the parameters is varied with respect to other. If one of the parameters is

zero, we consider the effect of non-zero parameter while keeping the other one constant. For the proposed second case (α = 0 and β = 2) the scenario maps to a fading model where only *h* is significant and for the third case (α = 2 and β = 0), the scenario maps to a path loss model where only *G* is significant. This shows the flexibility of the proposed algorithm to find the secrecy of different wireless models by choosing different values for relevance parameters. Similar is the secrecy performance with AF but with less performance compared to SRBJ.

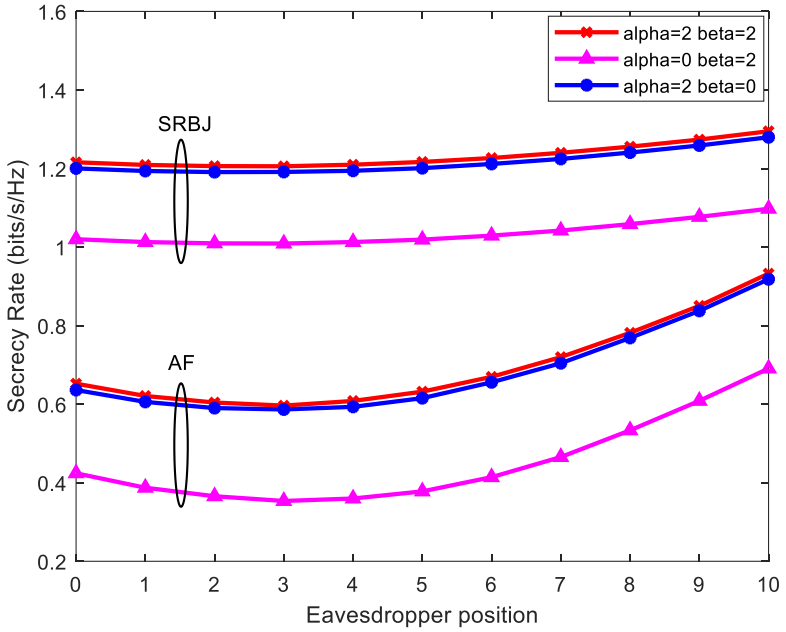


Fig.4.4 Secrecy rate versus eavesdropper position of SRBJ and AF schemes for different values of α and β

Fig. 4.5 demonstrates the comparison of secrecy rate among OPA and EPA strategies for SRBJ and AF transmission schemes in terms of eavesdropper position. From the figure, it is clear that the secrecy performance is better for OPA strategy compared to EPA for both

schemes. This is because, in OPA scheme the system allocates power to the nodes based on the position of relay and eavesdropper; whereas in EPA, the transmitting nodes are allocated equal power ($0.5P$) irrespective of the position of relay and eavesdropper.

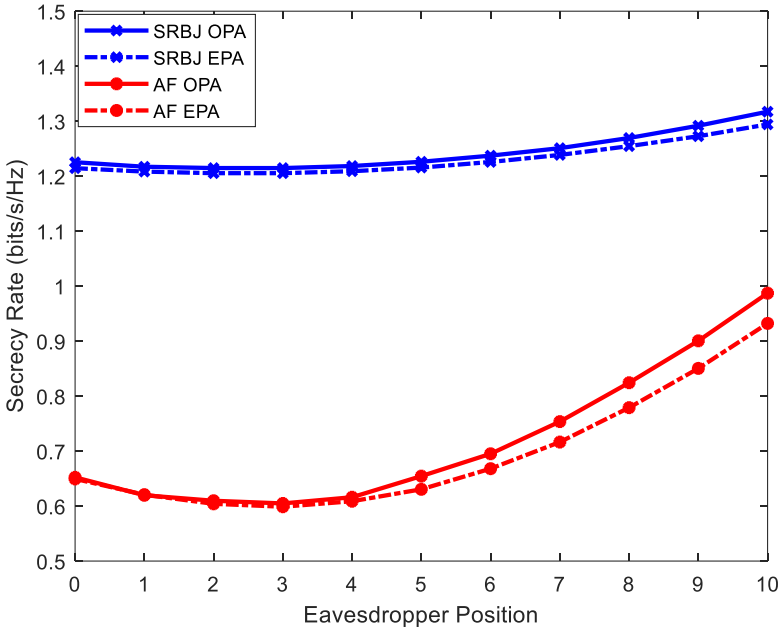


Fig.4.5 Comparison of secrecy rates among CJ/AF OPA/EPA strategies in terms of eavesdropper position

Fig. 4.6 shows the variation of power allocation factors, corresponding to the OPA results of SRBJ and AF schemes of Fig. 4.5 when $\alpha = \beta = 2$. The power allocated to information and jamming signals at the source and relay nodes depend on the position of relays and eavesdropper; hence the power allocation factors. Since the selected relay appears at the center of the network model in the best relay position, source and relay nodes require equal power for transmission; hence, a takes the value of 0.5 approximately, i.e. it lies

within 0.49 to 0.56 for different eavesdropper position. When eavesdropper lies near to source more jamming power from the source (1-a_s) is needed, whereas when it appears near to relay node, more jamming power from the relay (1-a_r) is needed so as to confuse the eavesdropper and it is clearly understood from the figure.

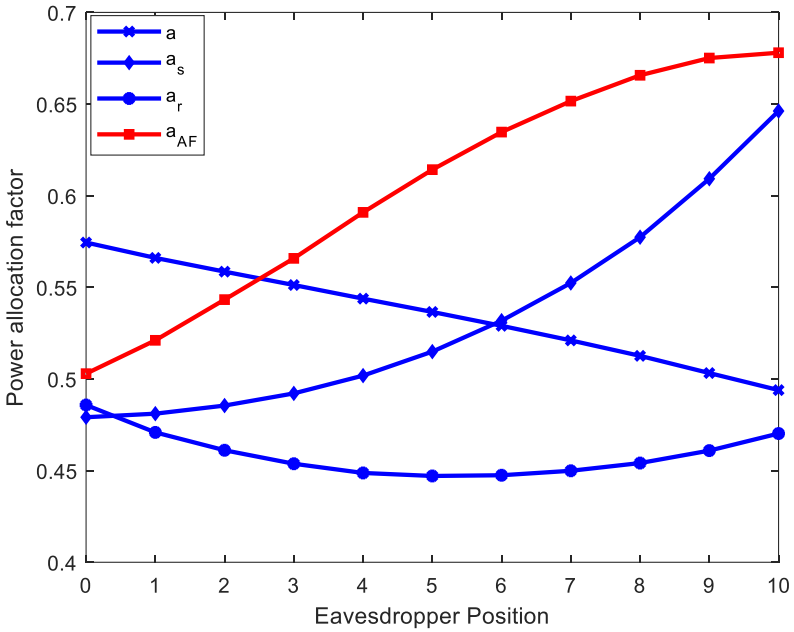


Fig. 4.6 Power allocation factors versus eavesdropper position when $\alpha = \beta = 2$

Table 4.1 gives the comparison of the proposed OPA strategy based on NM method with the gradient-based optimization and three dimensional exhaustive search algorithms; for the case of best relay position. The results presented in the table 4.1 for the symmetric case with E near to source show that the proposed NM method gives best secrecy performance compared to other methods. The best relay is the one that has the same source-relay SNR (γsr) and relay-destination

SNR (γ_{rd}). Such relay normally appears in the middle of the source destination pair. Since the secrecy rate given by (4.12) is a nonlinear function of three independent variables, for the asymmetric case where $\gamma_{sr} >> \gamma_{rd}$ or $\gamma_{sr} << \gamma_{rd}$; the derivatives of the function in gradient-based optimization method are complicated to compute, rather it is time consuming and may not produce results. But for NM method, since the objective function need not be differentiable, it is easy to get the results for all relay positions. The steps involved in gradient-based method for secrecy rate maximization are given in Appendix 1, Part A.

Table 4.1 Comparison of proposed NM method with gradient-based and exhaustive search algorithms for the best relay position

Optimization parameters/ Secrecy rate (bits/s/Hz)	Nelder-Mead Method	Gradient-based method	Exhaustive Search method			
			m=20 δ =0.05	m=40 δ=0.025	m =100 δ =0.01	m =500 δ =0.002
a	0.574444	0.567594	0.55	0.575	0.57	0.576
a_s	0.479125	0.479494	0.5	0.475	0.48	0.486
a_r	0.485786	0.476274	0.5	0.475	0.48	0.48
R_s	**1.225344**	**1.219525**	**1.223**	**1.2238**	**1.2248**	**1.2251**

Exhaustive search method is the simplest of all search methods, accurate results could be obtained for smaller step size δ or larger number of iterations m and is clearly understood from the results of m = 20, 40, 100 and 500. The results are obtained by simulation and the corresponding plot that show maximum secrecy for m = 20 is given in Fig. 4.7. The exhaustive search method is a simultaneous search method in which all the experiments are conducted before any

judgement is made regarding the location of the optimum point. So it is time consuming. This method is computationally inefficient especially when dealing with problems of higher dimensionality, hence this method replaces with heuristic approach.

The computational complexity of gradient method and exhaustive search algorithm is explained in Chapter 3 and that of NM method in 4.3.3. Though the complexity of gradient method seems to be less, it may not converge or produce optimal results at all relay positions because of non-linear secrecy rate function.

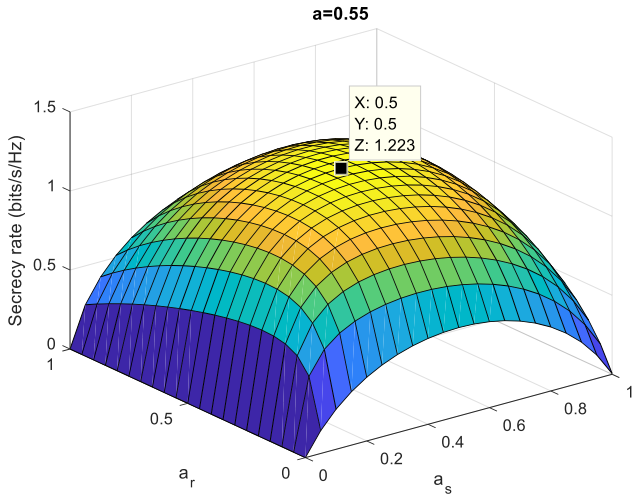


Fig. 4.7 Secrecy rate as a function of power allocation factors a, a_s & a_r for SRBJ scheme

In exhaustive search algorithm, sometimes there is a chance to miss out the maximum value obtained with larger step size, if the step size is not uniformly increased as multiples of initial step size. i.e., the maximum obtained with step size 0.025 may not be considered for the case with step size 0.002.

For performance comparison, the conventional AF scheme with

gradient-based optimization and exhaustive search method are presented in Table 4.2. Here, only one power allocation factor aAF need to be optimized for maximizing the secrecy rate given by (4.24) and derivative method is used for optimization. One dimensional exhaustive search method for m =20 is done by simulation and the corresponding plot is given in Fig. 4.8. A good match could be observed between the results of derivative/exhaustive search methods.

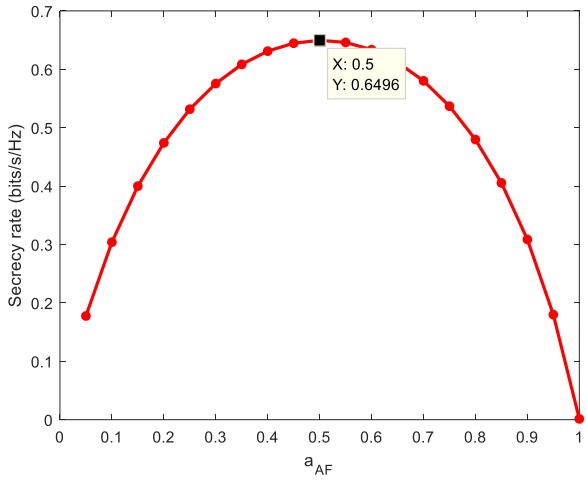


Fig.4.8 Secrecy rate as a function of power allocation factor a_{AF} for AF scheme

Table 4.2 Comparison of gradient-based and exhaustive search methods of AF scheme

Gradient-Based Method		Exhaustive Search Method (m=20)	
a_{AF}	R_s (bits/s/Hz)	a_{AF}	R_s (bits/s/Hz)
0.5037	0.6501	0.5	0.6496

Table 4.3 presents the average number of iterations in terms of SNR values for both symmetric/asymmetric cases. As the number of

iteration varies each time the function is executed, we considered the average number of iterations here. If the pattern is so that the optimum is close to one point defined by the pattern, the number of iteration may be small. On the contrary, the number of iterations may be large if the pattern does not come close to the optimum (Lagarias J C *et al.*, 1998). The algorithm converges when the working simplex Δ becomes sufficiently small in some sense, or when the function values *fi* are close enough in some sense.

Table 4.3 Complexity analysis in terms of average number of iterations

SNR(dB)	Average number of iterations		
	Symmetric case	Asymmetric case	
	$\gamma_{sr} = \gamma_{rd}$	$\gamma_{sr} > \gamma_{rd}$	$\gamma_{sr} < \gamma_{rd}$
0	142	501	502
2	98	502	502
4	94	502	502
6	86	118	502
8	84	98	502
10	86	94	302
12	88	96	102
14	86	86	104
16	82	90	98
18	78	98	94
20	80	94	92

It is clear from the table that the symmetric case requires less number of iterations for convergence than asymmetric case. It is also evident that the average number of iterations decreases with SNR, showing

almost constant or less variation beyond 10 dB in both cases. When the number of iteration increases, complexity increases which further increases the computational time and memory usage as expected.

Fig.4.9 illustrates the comparison of OPA/EPA strategies when secrecy rate is plotted against SNR for symmetric and asymmetric cases. OPA achieves better secrecy when compared to EPA. For CJ scheme, the secrecy rate increases with SNR owing to the addition of jamming signals at the source and relay nodes. The overall SNR at the eavesdropper reduces when noise is added which results in the improvement of secrecy. Whereas, for AF scheme, the secrecy rate is independent of SNR in the high SNR regime and therefore secrecy remains constant. Being the worst case of secrecy, eavesdropper near to source is considered for the analysis.

Case 1 in Fig.4.9 shows the performance of best relay position and case 2 shows the asymmetric case where relay lies near to destination. Since EPA shows good performance for the best relay position, not much variation among EPA/OPA can be seen for all SNR range and this can be understood from the figure. When the distance of the relay from the source increases, the received SNR at the eavesdropper decreases, hence secrecy increases. Therefore for case 2, OPA shows fairly a good performance at all SNR region. For case 1, the variation among EPA/OPA is found to be 0.0619 bits/s/Hz at 2 dB, 0.0111 bits/s/Hz at 10 dB and it increases to 0.0259 bits/s/Hz at 18 dB whereas for case 2, the variation among EPA/OPA is found to be 0.2069 bits/s/Hz, 0.3814 bits/s/Hz and 0.4558 bits/s/Hz respectively at 2dB, 10dB and 18dB.

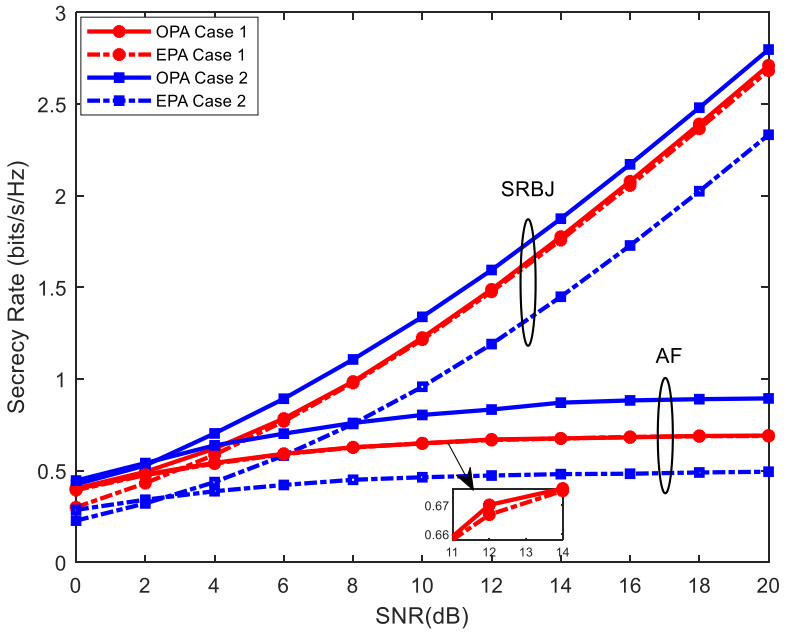


Fig.4.9 Comparison of secrecy rate among OPA/EPA strategies in terms of SNR

The secrecy is normally evaluated in the medium-to-high SNR regime. However, the number of iterations needed for the optimization beyond 10 dB do not vary much, which can be make out from the table 4.3; 10 dB is taken as the standard SNR for the analysis.

A comparison of secrecy rate and their power allocation factors as a function of relay distance from the source is made for SRBJ and AF schemes and is illustrated in Figures 4.10 and 4.11; with SNR as 10 dB and eavesdropper near to source. As always, OPA outperforms EPA because of power optimization. Since eavesdropper gets signal from both the source and relay, the relay away from the source has better secrecy performance compared to the one near to source or at

center. Accordingly, for relay position 5 and above, the secrecy performance with OPA increases and this is evident from the variation between OPA/EPA results from the graph in figure 4.10. When the distance of the relay from the source increases more source power *(a)* is needed for transmission i.e., a and a_{AF} increases with relay distance from source. Also more jamming power from the source (1- a_s) is required when the eavesdropper lies near to source. These are evident from the Fig. 4.11.

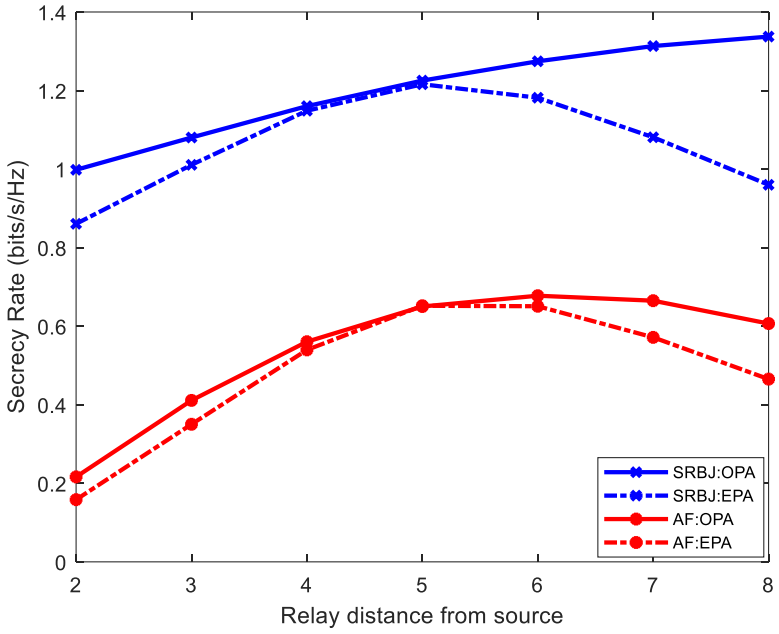


Fig. 4.10 Secrecy rate versus relay distance

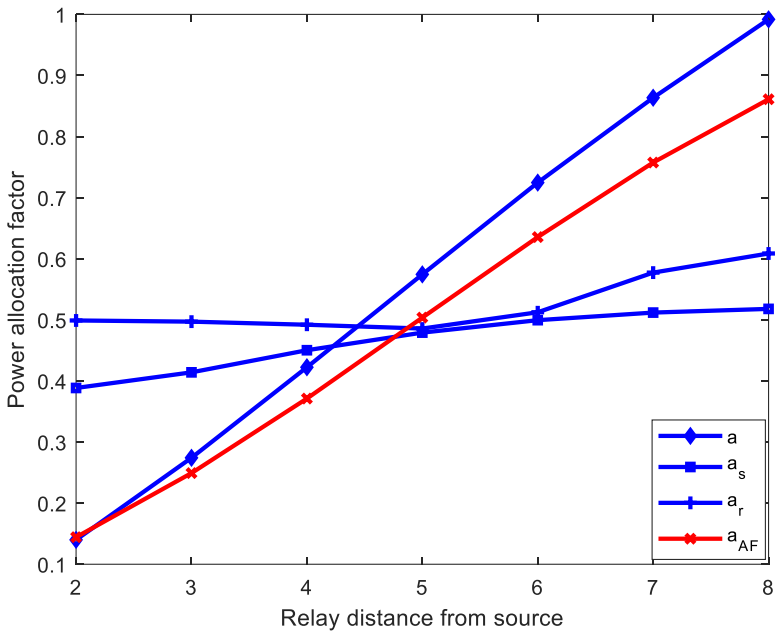


Fig. 4.11 Power allocation factors versus relay distance

Fig. 4.12 shows the performance of SRBJ and AF schemes with best relay (BR) and multiple relay (MR) participation cases. With multiple relays, the secrecy performance is poor for the case of AF compared to best relay, whereas for the CJ scheme, multiple relay case provides better secrecy compared to best relay. When multiple relays send jamming signals in SRBJ scheme, the SNR at the eavesdropper reduces eventually which increases the secrecy rate as expected. But it is not practical for all the relays to generate and transmit jamming signals; hence hybrid jamming scheme with multiple relays is not advisable.

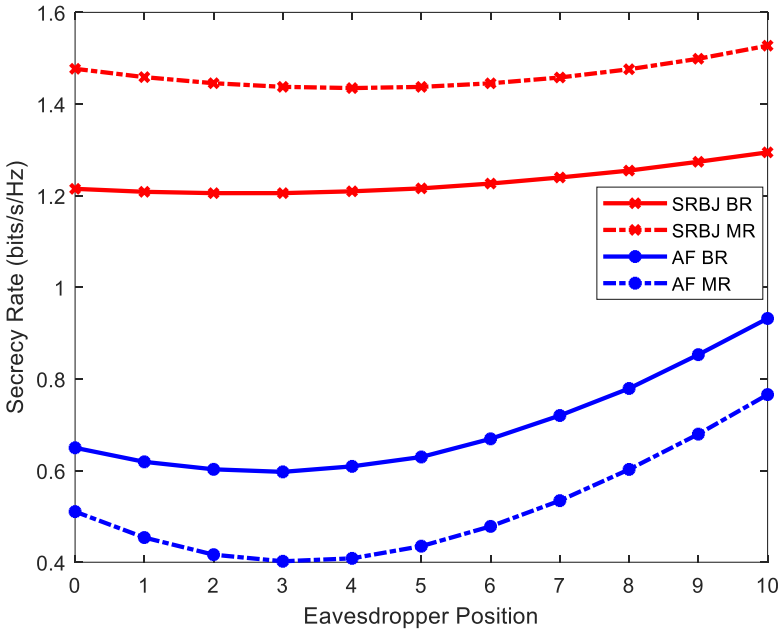


Fig. 4.12 Impact of single and multiple relays on secrecy performance

4.6 Chapter Summary

In this chapter, an optimal power allocation based on Nelder-Mead algorithm is proposed for an amplify-and-forward cooperative network with multiple trusted relays and an eavesdropper employing source and relay based jamming scheme. The path probability criterion of ACO algorithm is used for relay selection; and secrecy performance in traditional, path loss and fading model wireless scenarios are analyzed. The performance of the proposed power optimization algorithm is compared with gradient-based algorithm and exhaustive search methods and its complexity analysis is carried out. The conventional AF scheme and the secrecy performance with EPA strategy are also derived for comparison. The effect of relay location on secrecy is also examined for both schemes. It is observed

from the numerical results that the proposed optimization algorithm provides better performance compared with the gradient-based and exhaustive search algorithms. Also the secrecy performance of the proposed scheme is superior compared to AF and SRBJ without optimization (EPA), as power is allocated based on the position of relay and eavesdropper. The impact of single and multiple relays on secrecy is also evaluated for both proposed and AF schemes. The proposed NM algorithm can be applied to any cooperative networks like cooperative device-to-device networks, cognitive networks, wireless powered networks etc., where power allocation problem is critical.

The limitation of the model is the complexity in generating and processing two jamming signals at the source and relay. The second issue is with the nature of the relays; the jamming signal from the source can be removed only if the relays are considered trusted. The methods used to overcome these problems are addressed in the following chapters.

Chapter 5
Enhancing Secrecy via Power Optimized Source Based Jamming

5.1 Introduction

Due to the broadcast nature of the wireless medium, transmitting confidential information securely in the presence of eavesdroppers is of great importance. Recently, cooperative jamming has emerged as a promising technique to enhance wireless PLS (R. Liu and W. Trappe, 2010). In the SRBJ scheme proposed in Chapter 4, the source and relay nodes are allowed to use some of their available power to transmit jamming signals in order to create interference at the eavesdropper. But SRBJ scheme has problems with *i)* complexity in processing of two jamming signals at the source and relay and *ii)* the nature of the relays; the noise removal at the relay is possible only if the relay is considered trusted. With slight reduction in performance, these problems can be mitigated by employing a single jamming signal added either at the source or relay node.

In this chapter, a source based jamming (SBJ) scheme is proposed to improve the secrecy of AF cooperative networks, over Rayleigh fading channels in the presence of a passive eavesdropper (E); utilizing the direct link between source and destination . The secrecy is evaluated for N trusted relay nodes randomly distributed between the source and destination. The system allows the source to use some of its available power to transmit jamming signal in order to create interference at the eavesdropper. The power allocation between the

source and relay nodes as well as that between the information and jamming signals for maximizing the secrecy rate are estimated by Nelder-Mead algorithm and their performance is compared with EPA results. ACO path probability selection criterion for relay selection helps to find the secrecy performance in different wireless scenarios namely- traditional, path loss and fading models, depending on the significance of channel gain and fading coefficients of the path. It is observed from the numerical results that the proposed SBJ scheme shows almost similar performance as that of the SRBJ scheme for the best relay position. The conventional AF schemes, direct transmission scheme with and without jamming are used as benchmark schemes for comparison. It is observed that the secrecy performance of the proposed OPA outperforms other schemes. Also from the complexity analysis, it is observed that the proposed SBJ is less complex than SRBJ.

5.2 Transmission Scheme

5.2.1 Source Based Jamming Scheme

The same system model as in Fig. 3.1 is considered here. In the SBJ scheme, the system allocates some of its source power to transmit jamming signal along with the information to degrade the eavesdropper. The destination has prior knowledge of the jamming signal send by the source, and this assumption is made by exploiting the reciprocity of the channel between the source and the legitimate destination (Lu Lv *et al.*, 2017).

During the broadcast phase of signal transmission, the source transmits the information signal x_s and the jamming signal n_z with

powers aa_sP and $a(1\text{-}a_s)P$ respectively where $0 \leq \{a, a_s\} \leq 1$; where a is the power allocation factor between the source and relay and a_s is that between the information and jamming signals. The signal transmitted by the source is given by

$$x = \sqrt{aa_sP}x_s + \sqrt{a(1-a_s)P}n_z \tag{5.1}$$

The channel is represented by the channel parameters G and h separately h (M. Dohler, Y. Li, 2010), which is helpful in applying the ACO based relay selection algorithm. The signal received at the k^{th} relay, destination, and eavesdropper during the first phase can be expressed as,

$$y_{SR_k} = \sqrt{aa_sP}G_{SR_k}h_{SR_k}x_s + \sqrt{a(1-a_s)P}\,G_{SR_k}h_{SR_k}n_z + n_{R_k} \tag{5.2}$$

$$y_{SD} = \sqrt{aa_sP}G_{SD}h_{SD}x_s + \sqrt{a(1-a_s)P}G_{SD}h_{SD}n_z + n_{D_1} \tag{5.3}$$

$$y_{SE} = \sqrt{aa_sP}G_{SE}h_{SE}x_s + \sqrt{a(1-a_s)P}G_{SE}h_{SE}n_z + n_{E_1} \tag{5.4}$$

After relay selection, the selected relay amplifies the signal and forwards it to destination which is also received by the eavesdropper. During the relaying phase, the received signal at the destination and eavesdropper are,

$$\begin{aligned} y_{R_kD} = {} & g\sqrt{aa_sP}G_{SR_k}h_{SR_k}G_{R_kD}h_{R_kD}x_s + \\ & g\sqrt{a(1-a_s)P}G_{SR_k}h_{SR_k}G_{R_kD}h_{R_kD}\,n_z + gG_{R_kD}h_{R_kD}n_{R_k} + n_{D_2} \end{aligned} \tag{5.5}$$

$$\begin{aligned} y_{R_kE} = {} & g\sqrt{aa_sP}G_{SR_k}h_{SR_k}G_{R_kE}h_{R_kE}x_s + \\ & g\sqrt{a(1-a_s)P}G_{SR_k}h_{SR_k}G_{R_kE}h_{R_kE}n_z + gG_{R_kE}h_{R_kE}n_{R_k} + n_{E_2} \end{aligned} \tag{5.6}$$

where the amplification factor g at the selected relay is given by

$$g = \sqrt{\frac{(1-a)P}{\left|G_{SR_k} h_{SR_k}\right|^2 aP + {\sigma_{R_k}}^2}} \tag{5.7}$$

The destination cancels out the noise as it has prior knowledge of the noise send by the source. The SNR at the relay, destination, and eavesdropper after the first phase is

$$\gamma_{R_k} = \frac{aa_s\gamma_{SR_k}}{1+a(1-a_s)\gamma_{SR_k}} \tag{5.8}$$

$$\gamma_{D_1} = aa_s\gamma_{SD} \tag{5.9}$$

$$\gamma_{E_1} = \frac{aa_s\gamma_{SE}}{1+a(1-a_s)\gamma_{SE}} \tag{5.10}$$

During the second phase, the SNR at the destination and eavesdropper is

$$\gamma_{D_2} = \frac{a(1-a)a_s\gamma_{SR_k}\gamma_{R_kD}}{1+a\gamma_{SR_k}+(1-a)\gamma_{R_kD}} \tag{5.11}$$

$$\gamma_{E_2} = \frac{a(1-a)a_s\gamma_{SR_k}\gamma_{R_kE}}{1+a(1-a)(1-a_s)\gamma_{SR_k}\gamma_{R_kE}+a\gamma_{SR_k}+(1-a)\gamma_{R_kE}} \tag{5.12}$$

Therefore, the overall SNR at the destination and eavesdropper applying MRC, assuming that all the noise variances are equal is

$$\gamma_{D_{SBJ}} = aa_s\gamma_{SD} + \frac{a(1-a)a_s\gamma_{SR_k}\gamma_{R_kD}}{1+a\gamma_{SR_k}+(1-a)\gamma_{R_kD}} \tag{5.13}$$

$$\gamma_{E_{SBJ}} = \frac{aa_s\gamma_{SE}}{1+a(1-a_s)\gamma_{SE}} + \frac{a(1-a)a_s\gamma_{SR_k}\gamma_{R_kE}}{1+a(1-a)(1-a_s)\gamma_{SR_k}\gamma_{R_kE}+a\gamma_{SR_k}+(1-a)\gamma_{R_kE}} \tag{5.14}$$

An illustration of the system model with the selected relay is shown

in Fig. 5.1. The relay R is the selected trusted relay, n_z is the jamming signal added at the source. The solid lines and the dotted lines indicate the legitimate channel and the wiretap channel respectively.

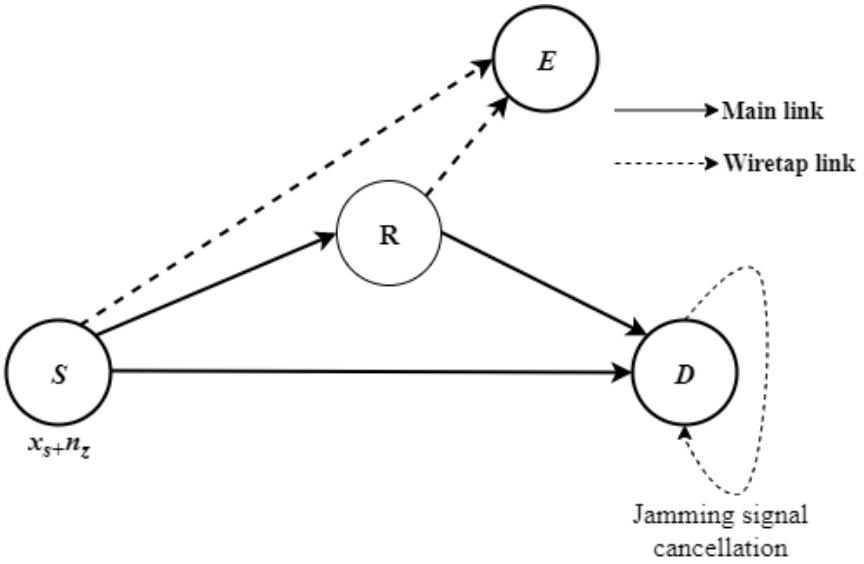


Fig. 5.1 Illustration of the system model

5.2.2 Performance Analysis

The instantaneous secrecy rate for the proposed SBJ scheme is obtained by substituting (5.13) and (5.14) into (3.17).

$$R_{s_{SBJ}}(a,a_s)=\left[\frac{1}{2}\log_2\left(\frac{1+aa_s\gamma_{SD}+\dfrac{a(1-a)a_s\gamma_{SR_k}\gamma_{R_kD}}{1+a\gamma_{SR_k}+(1-a)\gamma_{R_kD}}}{1+\dfrac{aa_s\gamma_{SE}}{1+a(1-a_s)\gamma_{SE}}+\dfrac{a(1-a)a_s\gamma_{SR_k}\gamma_{R_kE}}{1+a(1-a)(1-a_s)\gamma_{SR_k}\gamma_{R_kE}+a\gamma_{SR_k}+(1-a)\gamma_{R_kE}}}\right)\right]^{+} \quad (5.15)$$

The secrecy rate becomes (Lu Lv *et al.*, 2017),

$$\overline{R_{s_{SBJ}}}(a,a_s) = \max_{a,a_s \in (0,1)} \mathbf{E}\left[\frac{1+aa_s\gamma_{SD}+\frac{a(1-a)a_s\gamma_{SR_k}\gamma_{R_kD}}{1+a\gamma_{SR_k}+(1-a)\gamma_{R_kD}}}{1+\frac{aa_s\gamma_{SE}}{1+a(1-a_s)\gamma_{SE}}+\frac{a(1-a)a_s\gamma_{SR_k}\gamma_{R_kE}}{1+a(1-a)(1-a_s)\gamma_{SR_k}\gamma_{R_kE}+a\gamma_{SR_k}+(1-a)\gamma_{R_kE}}} \right] \quad (5.16)$$

The relay R_k is selected based on the probability of path selection criterion of ACO algorithm (3.23). Nelder-Mead method is applied to the function in (5.16) to estimate the optimal values of a and a_s for secrecy rate maximization. Since the NM method finds the minimum of a function, the function is inverted to get the maximum value. For EPA scheme, the secrecy is obtained by taking $a = a_s = 0.5$.

5.3 Nelder-Mead Method for Power Optimization

The NM method used for the minimization of a function of n variables, depend on the function values at (n+1) vertices of a general simplex (J. A. Nelder and R. Mead, 1965). Since the secrecy rate of the proposed scheme is dependent on two variables - a and a_s; the simplex is a triangle. The three vertices of the triangle are named as the best x_b, good x_g (next to best) and worst x_w points; corresponding to the smallest, second largest and the largest function values respectively. A pattern search that compares the function values at three vertices of the triangle is then conducted. After each iteration, the vertex with the largest function value is removed and replaced with a new vertex. This forms a new triangle and the search is continued. A sequence of triangles with different shapes is produced, for which the function values at the vertices get smaller and smaller. Finally we get the smallest triangle and the coordinates of the minimum point (John H Mathews and Kurtis K Fink, 2004). The

algorithm is explained in Session 4.3. The detailed steps of NM algorithm with two variables are given in Appendix II.

5.4 Benchmark Schemes

5.4.1 Transmission schemes

The SRBJ scheme for secrecy enhancement where jamming signals are added by the source and relay is presented in Chapter 4. Since relays are used for transmission and powers are to be allocated to the jamming signals at the source and relay nodes, three parameters need to be optimized for secrecy rate maximization. NM method is used for power optimization. The other transmission schemes used for comparison include conventional amplify-and-forward scheme (AF), direct transmission scheme (DT) and direct transmission scheme with jamming (DT WJ) are explained in Chapter 4.

5.4.2 Optimization Methods

The gradient-based method which uses differentation and exhaustive search algorithm are used for the comparison of the proposed optimization scheme.

5.5 Numerical Results and Analysis

The following simulations are conducted to verify the validity of the proposed algorithm. For the proposed jamming scheme, NM method is used for power optimization, and its performance is compared with gradient-based optimization and exhaustive search algorithms. The secrecy performance of SBJ is also compared with SRBJ, conventional AF and direct transmission schemes. The secrecy rate for the proposed SBJ scheme is calculated using (5.15). For EPA

schemes, the power allocation factors are assigned the value of 0.5. (i.e., $a = a_s = 0.5$). Relay selection is done based on the path probability selection criterion of ACO algorithm using (3.23).

Fig. 5.2 shows the results of ACO based relay selection algorithm, where secrecy rate is plotted against SNR for different values of relevance parameters. With EPA strategy, three cases of relevance parameters, α and β are considered and is illustrated as follows. Case 1: when $\alpha = \beta = 2$, the scenario maps to a traditional wireless model; case 2: when $\alpha = 0$ and $\beta = 2$, the scenario maps to a fading model and case 3: when $\alpha = 2$ and $\beta = 0$, the scenario maps to a path loss model. This shows the advantage of ACO based relay selection algorithm that can be applied to different wireless scenarios. If we consider the same channel coefficients, secrecy is highest for the case when α and β are equal. For the other two cases the effect of only non-zero factor is considered, hence secrecy is reduced. With SBJ and SRBJ schemes, the secrecy monotonically increases with increase in SNR. Since only one jamming signal is used in SBJ; the secrecy performance is reduced a little when compared with SRBJ scheme. The complexity is reduced in SBJ by use of single jamming signal; and it is illustrated in table 5.2. The secrecy rate remains constant for AF in the high SNR regime since the secrecy rate given by (4.24) is independent of SNR. The eavesdropper near to source is considered for the analysis, being the worst case of secrecy.

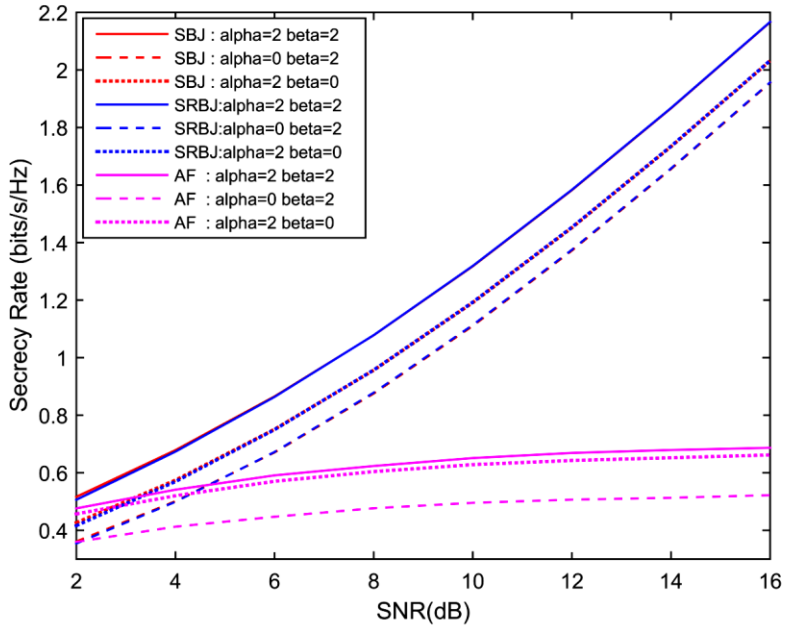


Fig.5.2 Comparison of secrecy rate among SBJ/SRBJ/AF schemes in terms of SNR

Fig.5.3 shows the comparison of secrecy performance of the proposed SBJ with SRBJ, conventional AF and direct transmission schemes for the best relay position. For simulation analysis, equal values of relevance parameters α and β are considered ($\alpha = \beta = 2$) as it gives the best secrecy performance. It is understood from the figure that the proposed SBJ shows almost same performance as that of SRBJ for the best relay position. Also the secrecy performance of all the schemes increases with source-eavesdropper distance. This is because the received signal power at the eavesdropper from both the source and relay decreases with source-eavesdropper distance. The performance with jamming is better than that of the schemes without jamming; since it reduces the SNR of the eavesdropper. i.e.,

SBJ/SRBJ outperforms the other schemes. The negative secrecy rate of DT is also improved by jamming as in DT WJ scheme.

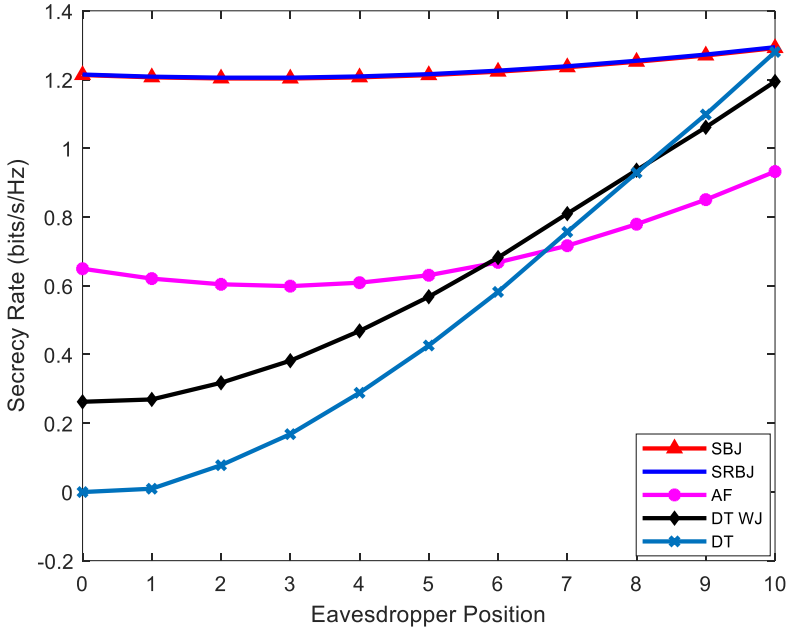


Fig.5.3 Comparison of secrecy performance of various schemes in terms of eavesdropper position

Fig.5.4 demonstrates the OPA and EPA secrecy rate comparison among SBJ and AF transmission schemes in terms of eavesdropper position, for best relay position with $\alpha = \beta = 2$. From the figure, it is clear that the OPA shows better secrecy performance compared to EPA for both schemes. In OPA scheme, the system allocates power to the nodes based on the position of relay and eavesdropper; whereas in EPA, equal power ($0.5P$) is allocated irrespective of the position of relay and eavesdropper, which results in poor performance.

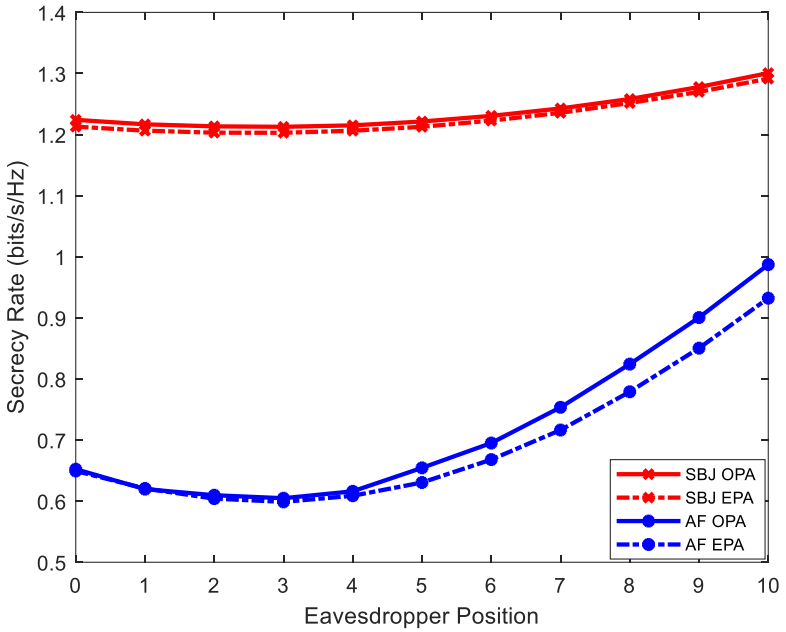


Fig.5.4 OPA/EPA comparisons of secrecy rates among SBJ/AF schemes for best relay position

Fig.5.5 shows the variation of power allocation factors corresponding to the OPA results of SBJ and AF schemes of Fig. 5.4 and also with the SRBJ scheme proposed in chapter 4. The power allocated to information and jamming signals depend on the position of relays and eavesdropper; hence the power allocation factors. Since the selected relay appears at the center of the network model in the best relay position, source and relay nodes require equal power for transmission; hence, a_{SBJ} lies within 0.56 to 0.58 for different eavesdropper position. This shows that the EPA and OPA results for best relay position are almost same. The eavesdropper has more chance to intercept the information when it comes near to source and the system becomes insecure. The jamming signal transmitted from the source can reduce the SNR of the eavesdropper. Therefore, performance with jamming is

better than that of the system without jamming. The received signal power at the eavesdropper from the source decreases with source-eavesdropper distance. Hence more jamming power (1-as_{SBJ}) is needed for degrading when eavesdropper appears near to source than when it appears near to destination. Accordingly, from the graph, jamming power of 0.52W is taken for the case when it comes near to source and that of 0.46W when it comes near to destination.

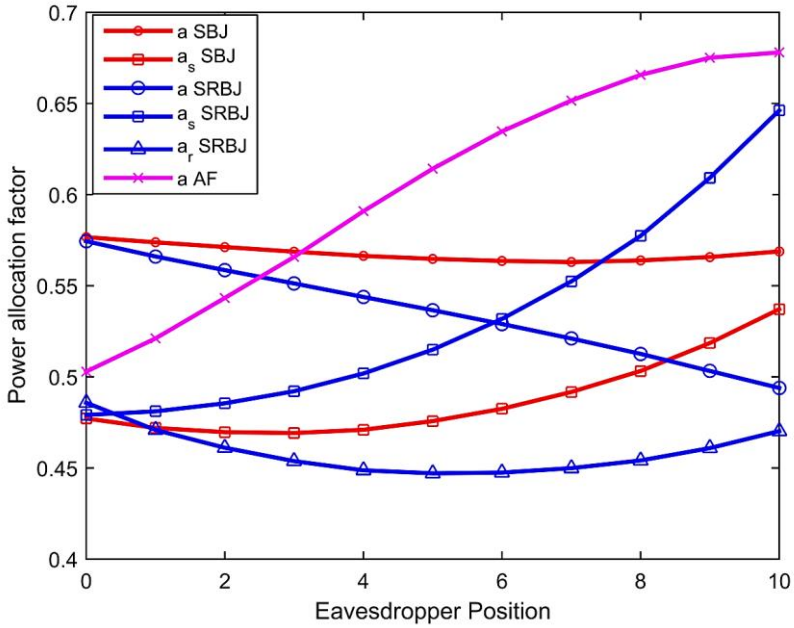


Fig.5.5 Power allocation factors versus eavesdropper position for best relay position

When the power allocation factors for SBJ and SRBJ schemes are compared, it is seen that SBJ scheme has more information signal power *a* compared with SRBJ; whereas SRBJ takes less source jamming signal power (1-as_{SRBJ}) which seem to be advantageous in both cases. The less source jamming power of SRBJ is mainly because of which, it employs another jamming signal at the relay. AF

scheme requires less source power when eavesdropper appears near to source and less relay power when it comes near to destination and this is clearly understood from a_{AF} curve in the figure.

Fig.5.6 shows the secrecy rate versus the number of relay nodes for two scenarios – Case 1: eavesdropper near to source and Case 2: eavesdropper near to destination. The SNRs are fixed at 5dB and 10dB.

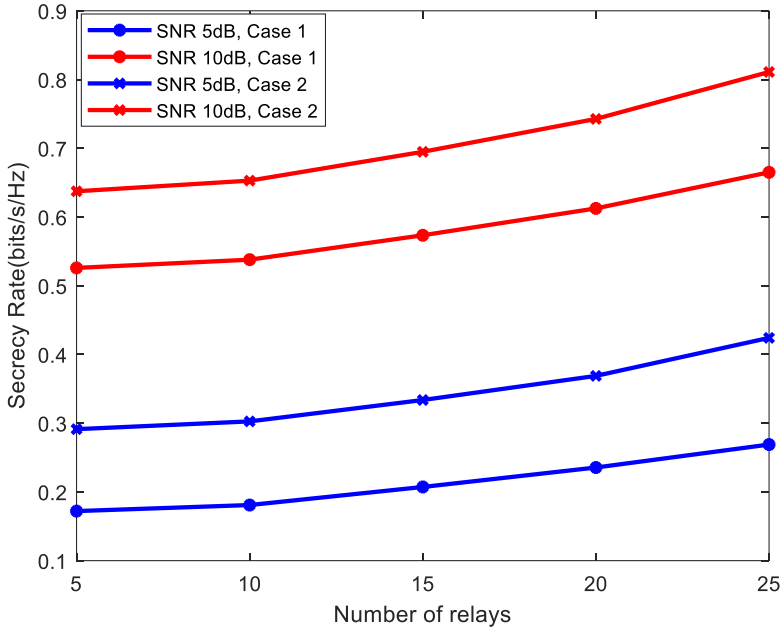


Fig.5.6 Secrecy rate versus number of relays

The variation of secrecy rate depends on the size of the cluster where relays are deployed. The presence of more relays provides a higher probability for selecting a better helper; hence secrecy increases with the number of relay nodes. When the number of relay nodes continues to increase, the secrecy rate increases slowly and gets

saturated. The secrecy rate gets saturated faster for small cluster size than for large cluster size. As discussed earlier, secrecy of the proposed scheme increases with SNR. Further, secrecy increases when the eavesdropper moves away from the source, since the received signal power at the eavesdropper is reduced.

Fig. 5.7 and Fig. 5.8 illustrate the secrecy rate and power allocation factors respectively of the proposed jamming scheme as a function of relay distance from the source; taking the SNR as 10 dB.

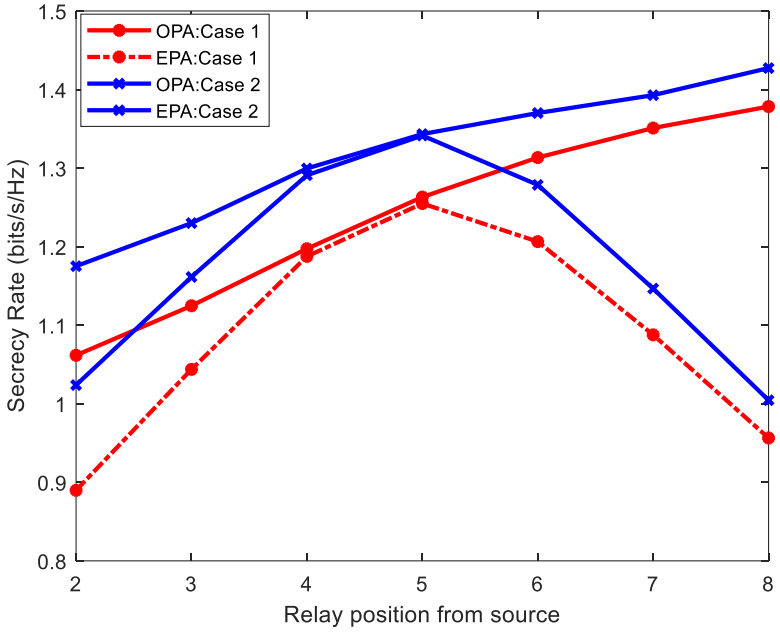


Fig. 5.7 Secrecy rate versus relay distance

The performance with EPA is good only for the case when relay at the centre of the network model; hence the variation between OPA and EPA is very less. For relay near to source and near to destination, EPA shows poor performance; hence it shows much variation

between OPA and EPA. Eavesdropper near to destination (Case 2) shows better secrecy than that near to source (Case 1). From Fig. 5.8, it is understood that *a* increases with source-relay distance as more source power *(a)* is needed for transmission. a_s depends on eavesdropper position and therefore it does not have much influence on source-relay distance, hence remain constant.

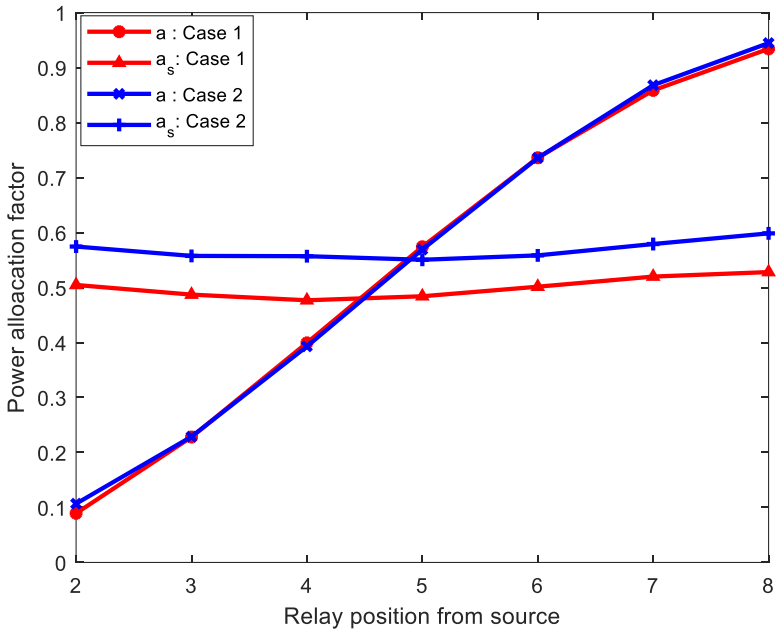


Fig. 5.8 Power allocation factors versus relay distance

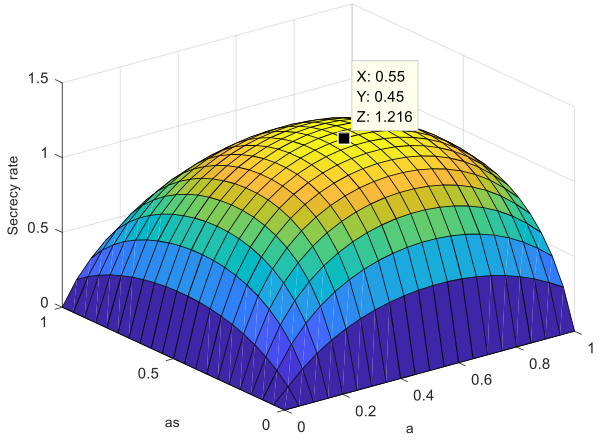
Table 5.1 presents the comparison of the results of proposed NM method with gradient-based and two-dimensional exhaustive search algorithms. The results are compared for two cases; *i)* symmetric case where the relay is at the center of the network model, *ii)* asymmetric case where the relay is near to source. The results in the table shows that NM method provides best secrecy performance using low jamming signal power (1- a_s) for both cases. Exhaustive search method

is the simplest method which produces accurate results. The accuracy of ES method increases with the number of iterations *m*, but this method is computationally inefficient. The results of ES algorithm are obtained by simulation and the plots for symmetric and asymmetric cases for *m*=20 are given in figures 5.9 (a) and (b) respectively.

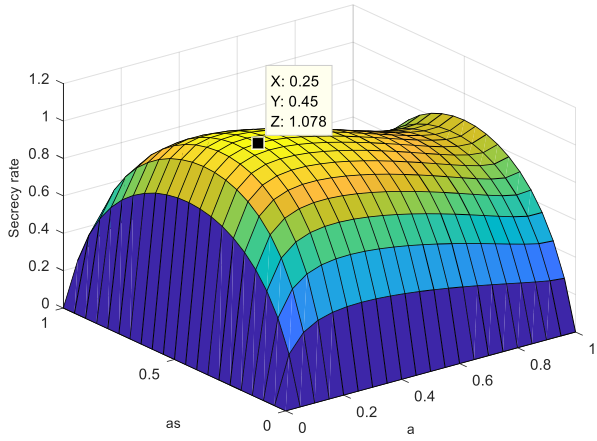
Table 5.1 Performance comparison of proposed Nelder-Mead method with other optimization methods

Relay position		Symmetric case			Asymmetric case		
Optimization method		a	a_s	R_s	a	a_s	R_s
NM method		0.5765663	0.4734986	1.22043	0.2479251	0.468518	1.083343
Gradient method		0.57528	0.47332	1.2166	0.246731	0.471446	1.07758
Exhaustive search	m=20	0.55	0.45	1.216	0.2	0.45	1.078
	m=40	0.57	0.475	1.2183	0.2	0.475	1.0807
	m=100	0.575	0.47	1.2201	0.2	0.48	1.0817

The steps involved in gradient-based method for two-variable optimization are given in Appendix 1, Part B.



(a)



(b)

Fig. 5.9 Secrecy rate as a function of power allocation factors a & $a_=$
a) Symmetric case: $\gamma_{sr} = \gamma_{rd}$ b) Asymmetric case $\gamma_{sr} > \gamma_{rd}$

The comparison of complexity analysis among SBJ and SRBJ schemes based on the average number of iterations are presented in Table 5.2. From the table it is understood that the SBJ requires less number of iterations to converge than SRBJ. i.e., SBJ is less complex than SRBJ.

Table 5.2 Complexity analysis among SBJ/SRBJ schemes

SNR(dB)	**Average number of iterations**	
	SBJ	**SRBJ**
0	65	142
2	59	98
4	51	94
6	49	86
8	47	84
10	41	86
12	43	88
14	41	86
16	43	82
18	45	78
20	43	80

5.6 Chapter Summary

This chapter presented a power optimized source-based jamming (SBJ) scheme to improve the secure communication in a two-hop amplify-and-forward relaying network with multiple trusted relays and a passive eavesdropper. The SBJ scheme overcomes the complexity of the network model with two jamming signals as in source and relay based jamming. The Nelder-Mead algorithm is used for estimating the optimal power allocation values for maximizing the secrecy rate. The effects of relay location and number of relay nodes on secrecy are also examined. With ACO path probability based relay selection algorithm, secrecy performance is evaluated for traditional, path loss and fading models. Numerical results show that OPA scheme provides better secrecy performance compared to EPA and also with other optimization methods like gradient-based and exhaustive search algorithms. Also the proposed scheme outperforms the SRBJ scheme, conventional AF and DT schemes. It is also observed from the complexity analysis that the SBJ scheme is less complex than SRBJ scheme.

Chapter 6
Power Optimization for Secure Transmission in Untrusted Relay Networks

6.1 Introduction

Cooperative communication scenarios normally assume a complete trust between cooperating nodes and allow the information to be decoded at the cooperating nodes. But in practice, it is likely to come across public ad hoc networks where relays used for connectivity may not be authenticated. In such cases, secrecy of the information transmitted via relay nodes need to be protected, despite the fact that the relay is a cooperating node. In heterogeneous networks, or in practical scenarios where direct communication between source and destination is too expensive in terms of power consumption or in cases where direct communication may be used to send very low rate signals to initialize the communication, the assistance of the intermediate relaying node is essential to convey a confidential message from the source to the destination. In such cases the relays may not be authenticated and have a lower security clearance in the network; hence it is not trusted with the information it is relaying (X. He and A. Yener, 2009; X. He and A. Yener, 2010). This does not mean the relay node is malicious; it may be part of the network that it is willing to faithfully carry out the designated relaying scheme. Thus, untrusted relays can be observed as beneficial nodes as well as potential eavesdroppers (W. Wang *et al.,* 2016b). Equivalently, we can assume that the confidential message used for identification of the source node for authentication, should never be revealed to such a

relay node, so as not to cause an attack (X He and A Yener, 2009). Even in the absence of external eavesdroppers, secrecy cannot be guaranteed in untrusted networks (X He and A Yener, 2010). Therefore, it is necessary to develop a secrecy enhancement scheme for untrusted relaying networks.

In this chapter, a power optimized source based jamming scheme is proposed to improve the secrecy performance of multiple untrusted AF relay networks in the presence of an external eavesdropper, where the source-destination direct link is assumed. For power optimization, Nelder-Mead (NM) method, a gradient-free method is used (Nelder J. A. and Mead R.,1965), which overcome the problems with conventional gradient-based power optimization method. The secrecy performance of untrusted relaying scheme is compared with the worst case scenario; where the eavesdropper and untrusted relays are assumed to be cooperating with each other. We have proposed a secure relay selection scheme based on the path probability selection criterion of ACO algorithm. The relay selection algorithm helps in finding the secrecy performance in three wireless scenarios namely traditional, path loss and fading models, under aggregate power constraint. The performance of the proposed NM method is compared with gradient-based and two dimensional exhaustive search algorithms for symmetric and asymmetric relay positions. The performance comparison with EPA strategy (CJ without power optimization) is also performed. The complexity analysis of the proposed algorithm is also studied. Numerical results reveal that the proposed OPA scheme outperforms other optimization methods, EPA strategy and the worst case scenario.

6.2 System Model and Proposed Scheme

The system model shown in Fig. 6.1, consists of a source S, a destination D, N untrusted non-colluding AF relays represented by $\boldsymbol{R} = \{R_k \mid k = 1, 2, \ldots, N\}$, randomly distributed between source and destination and a passive external eavesdropper E_e who hide its existence in the network. The relays act as helpers of transmitting information as well as potential eavesdroppers, hence named as internal eavesdroppers. In order to distinguish the passive eavesdropper from the internal eavesdroppers, it is indicated as *Ee*.

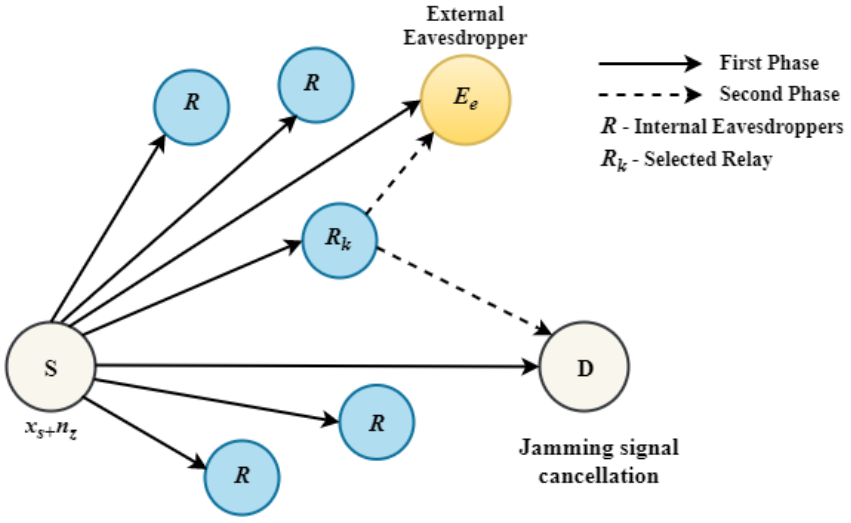


Fig. 6.1 System model of untrusted relaying scheme

An SBJ scheme, where the system allocates some of its source power to transmit the jamming signal to degrade the internal/external eavesdroppers is proposed. The signal transmission involves broadcast and relaying phases. Denoting x_s and n_z as the information and jamming signals respectively, the signal transmitted from the

source x is

$$x = \sqrt{aa_s P}\, x_s + \sqrt{a(1-a_s)P}\, n_z \tag{6.1}$$

During the first phase of transmission, the received signal at the internal and external eavesdroppers i ($i \in \{1, 2,\ldots, N, E_e\}$), can be expressed as,

$$y_i^{\,1} = \sqrt{aa_s P}\, G_{si} h_{si} x_s + \sqrt{a(1-a_s)P}\, G_{si} h_{si} n_z + n_{i_1} \tag{6.2}$$

The signal received at the destination D is,

$$y_d^{\,1} = \sqrt{aa_s P}\, G_{sd} h_{sd} x_s + \sqrt{a(1-a_s)P}\, G_{sd} h_{sd} n_z + n_{d_1}$$

$$= \sqrt{aa_s P}\, G_{sd} h_{sd} x_s + n_{d_1}\text{; after noise cancellation.} \tag{6.3}$$

n_i is the additive noise at the node i.

The channel gain G_{ij} between the nodes i and j is given by (3.4).

A relay k is selected based on the path probability selection criterion of ACO algorithm. k ($k \in \{1,2,\ldots N\}$) indicates the index of the selected relay R_k. For simplicity, the index of the relay is used in the equations. The relay selection is done prior to the second phase of transmission.

The selected relay k then amplifies the signal by an amplification factor g given by

$$g = \sqrt{\frac{(1-a)P}{\left|G_{sk} h_{sk}\right|^2 aP + {\sigma_k}^2}} \tag{6.4}$$

and broadcasts the message $x_k = g\, y_k$ to destination which is also received by the other untrusted relays and external eavesdropper E_e.

The signal received at the eavesdroppers i, ($i \neq k$) during the second transmission phase is

$$\begin{aligned} y_i^{\,2} &= gG_{ki}h_{ki}y_k + n_{i_2} \\ &= g\sqrt{aa_sP}G_{sk}h_{sk}G_{ki}h_{ki}x_s + g\sqrt{a(1-a_s)P}G_{sk}h_{sk}G_{ki}h_{ki}n_z + gG_{ki}h_{ki}n_k + n_{i_2} \end{aligned} \tag{6.5}$$

The signal at the destination

$$\begin{aligned} y_d^{\,2} &= g\sqrt{aa_sP}G_{sk}h_{sk}G_{kd}h_{kd}x_s + g\sqrt{a(1-a_s)P}G_{sk}h_{sk}G_{kd}h_{kd}n_z + gG_{kd}h_{kd}n_k + n_{d_2} \\ &= g\sqrt{aa_sP}G_{sk}h_{sk}G_{kd}h_{kd}x_s + gG_{kd}h_{kd}n_k + n_{d_2}; \end{aligned} \tag{6.6}$$

From (6.2), the signal to interference and noise ratio (SINR) at the selected relay k, internal and external eavesdroppers i, $i \in \{R, E_e\}$ and at the destination during the first transmission phase is

$$\gamma_k = \frac{aa_s\gamma_{sk}}{1+a(1-a_s)\gamma_{sk}} \tag{6.7}$$

$$\gamma_i^{\,1} = \frac{aa_s\gamma_{si}}{1+a(1-a_s)\gamma_{si}} \tag{6.8}$$

$$\gamma_d^{\,1} = aa_s\gamma_{sd} \tag{6.9}$$

γ_{si}, γ_{sk} and γ_{sd} are the instantaneous SNR in the source-malicious node, source-selected relay and source-destination channels respectively.

From (6.5), the SINR at the internal and external eavesdroppers i, ($i \neq k$); during the second transmission phase is

$$\gamma_i^{\,2} = \frac{a(1-a)a_s\gamma_{sk}\gamma_{ki}}{1+a(1-a)(1-a_s)\gamma_{sk}\gamma_{ki}+a\gamma_{sk}+(1-a)\gamma_{ki}} \tag{6.10}$$

and at the destination is

$$\gamma_d{}^2 = \frac{a(1-a)a_s\gamma_{sk}\gamma_{kd}}{1+a\gamma_{sk}+(1-a)\gamma_{kd}} \tag{6.11}$$

The overall SNR at the destination applying MRC is

$$\begin{aligned}\gamma_D &= \gamma_d{}^1 + \gamma_d{}^2 \\ &= aa_s\gamma_{sd} + \frac{a(1-a)a_s\gamma_{sk}\gamma_{kd}}{1+a\gamma_{sk}+(1-a)\gamma_{kd}}\end{aligned} \tag{6.12}$$

All the noise variances are set equal for simplicity.

6.3 Performance Analysis

The secrecy rate is used as the performance metric here also. In the proposed scenario, both untrusted relays (internal eavesdroppers) and external eavesdropper exist in the network at the same time. The untrusted relays act as both essential relays and malicious eavesdroppers, which can eavesdrop the information. In cooperative communication system the instantaneous secrecy rate is computed by (Ali Kuhestani *et al.,* 2018a)

$$R_s = \left(R_D - R_E\right)^+ = \left[\frac{1}{2}\log_2\left(1+\gamma_D\right) - \frac{1}{2}\log_2\left(1+\gamma_E\right)\right]^+ \tag{6.13}$$

where $(x)^+ = \max\{0, x\}$;

γ_E is the amount of information leaked to the malicious nodes; i.e., both untrusted relays and external eavesdropper. Since the power optimization method used here can allocate powers optimally between the source and relay nodes as well as between information and jamming signals, $R_s \geq 0$ is achievable. Hence instantaneous secrecy rate (6.13) is changed to (Ali Kuhestani and Abbas Mohammadi, 2016)

$$R_s = \frac{1}{2}\log_2\left(1+\gamma_D\right) - \frac{1}{2}\log_2\left(1+\gamma_E\right) \tag{6.14}$$

6.3.1 Relay Selection

The optimal relay *k* is the one that gives maximum secrecy rate and it needs to satisfy

$$k^* = \underset{1\le k\le N}{\arg\max}\ R_s^{(k)} \tag{6.15}$$

The instantaneous CSI of each link has to be known for finding the relay of (6.15). Since it is difficult to adopt the optimal relay in practical systems as we cannot get the information of external eavesdropper accurately, we go for suboptimal selection. A relay selection which avoids using the CSI of external eavesdropper is used. Accordingly, we consider the model without external eavesdropper. If *k* is the selected relay, R_D and R_{Rk} are the rates at destination and selected relay respectively, the achievable secrecy rate is given as (L. Sun *et.al*, 2012)

$$\begin{aligned} R_{S_{wo\_ed}}^{(k)} &= \left[R_D - \underset{1\le k\le N}{\arg\max}\left(R_{R_k}\right)\right]^+ \\ &= \left[\frac{1}{2}\log_2(1+\gamma_D) - \underset{1\le k\le N}{\arg\max}\left(\frac{1}{2}\log_2(1+\gamma_k)\right)\right]^+ \end{aligned} \tag{6.16}$$

$$= \left[\frac{1}{2}\log_2\left(1+aa_s\gamma_{sd}+\frac{a(1-a)a_s\gamma_{sk}\gamma_{kd}}{1+a\gamma_{sk}+(1-a)\gamma_{kd}}\right) - \underset{1\le k\le N}{\arg\max}\left(\frac{1}{2}\log_2\left(1+\frac{aa_s\gamma_{sk}}{1+a(1-a_s)\gamma_{sk}}\right)\right)\right]^+$$

According to which the relay selection criterion is

$$k^* = \underset{1\le k\le N}{\arg\max}\left(aa_s\gamma_{sd}+\frac{a(1-a)a_s\gamma_{sk}\gamma_{kd}}{1+a\gamma_{sk}+(1-a)\gamma_{kd}}\right) \tag{6.17}$$

It is found that the optimal relay obtained by (6.17) is the relay that maximizes the SNR at the destination. Hence relay selection based on the probability of selecting a route in the solution of ACO algorithm can be used here (Marco Dorigo and Thomas Stutzle, 2006). By considering the channel parameters namely, channel gain *(G)* and coefficients of fading *(h)* separately, the secrecy performance is analyzed in three scenarios: *(i)* a traditional model characterized by both *G* and *h* (*ii)* a fading model defined by only *h* and *(iii)* a path-loss model defined by only *G*. The best relay *k* is obtained by the harmonic mean of best probability pair $p_{S,k}$ and $p_{k,D}$ given by

$$k = \arg\max_{k \in R} \left(\frac{p_{S,k} p_{k,D}}{p_{S,k} + p_{k,D}} \right) \tag{6.18}$$

where $p_{S,k}$ and $p_{k,D}$ represent the probabilities of the transmitted signal from source to k^{th} relay and from k^{th} relay to destination given by (3.18) and (3.19) respectively (Marco Dorigo and Thomas Stutzle, 2006).

6.3.2 System Secrecy Rate

The secrecy rate for the proposed untrusted relaying scheme (UT) is obtained by (6.13). *N* untrusted relays and an external eavesdropper comprise a total of (*N*+1) malicious nodes. Here, the signals received by the malicious nodes during the first and second phases are considered separately. The amount of information leakage γ_E is the maximum of leakage to untrusted relays and external eavesdropper (Ali Kuhestani *et al.,* 2018a).

$$\gamma_E = \max_{1 \le i \le N+1, i \ne k} \left\{ \gamma_k, \gamma_i^1, \gamma_i^2 \right\} \tag{6.19}$$

The instantaneous secrecy rate with the selected relay is given by

$$R_s^{(k)}(a,a_s)=\left\{\frac{1}{2}\log_2\left(1+aa_s\gamma_{sd}+\frac{a(1-a)a_s\gamma_{sk}\gamma_{kd}}{1+a\gamma_{sk}+(1-a)\gamma_{kd}}\right)-\frac{1}{2}\log_2\left(1+\max_{1\le i\le N+1,i\ne k}\left\{\gamma_k,\gamma_i^{\,1},\gamma_i^{\,2}\right\}\right)\right\}^+ \tag{6.20}$$

6.3.3 Secrecy Rate of Worst Case Scenario

The performance of the untrusted relaying scheme (UT) is compared with the worst case scenario (WC), where the external eavesdropper and untrusted relays cooperate with each other. Here, the information leakage to the untrusted relays and the external eavesdropper is considered separately. The information received at the external eavesdropper in both phases can be combined. The amount of information leakage for the worst case scenario γ_{E_WC} is given by Ali Kuhestani *et al* (2018a).

$$\gamma_{E\_WC}=\max\left\{\max_{1\le i\le N,i\ne k}\left\{\gamma_k,\gamma_i^{\,1},\gamma_i^{\,2}\right\},\left(\gamma_{E_e}^{\,1}+\gamma_{E_e}^{\,2}\right)\right\} \tag{6.21}$$

where $\max_{1\le i\le N,i\ne k}\left\{\gamma_k,\gamma_i^{\,1},\gamma_i^{\,2}\right\}$ is the information leakage to the untrusted nodes R and $\left(\gamma_{E_e}^{\,1}+\gamma_{E_e}^{\,2}\right)$ is the leakage to the external eavesdropper E_e. The instantaneous secrecy rate is therefore given by,

$$R_{s_{WC}}^{(k)}(a,a_s)=\left\{\frac{1}{2}\log_2\left(1+aa_s\gamma_{sd}+\frac{a(1-a)a_s\gamma_{sk}\gamma_{kd}}{1+a\gamma_{sk}+(1-a)\gamma_{kd}}\right)-\frac{1}{2}\log_2\left(1+\max\left\{\max_{1\le i\le N,i\ne k}\left\{\gamma_k,\gamma_i^{\,1},\gamma_i^{\,2}\right\},\left(\gamma_{E_e}^{\,1}+\gamma_{E_e}^{\,2}\right)\right\}\right)\right\}^+ \tag{6.22}$$

Nelder-Mead method is applied to the functions in (6.20) and (6.22)

to estimate the optimal values of a and a_s for the proposed untrusted case and worst case scenario respectively. Since the NM method finds the minimum of a function, the functions are inverted to get the maximum value. For EPA scheme, the secrecy is obtained by taking $a = a_s = 0.5$. The NM algorithm for general case is explained in Session 4.3. The detailed steps involved in NM algorithm with two variables are given in Appendix II.

6.4 Results and Analysis

In this section, some numerical results to verify the performance of the proposed OPA scheme by Monte Carlo simulations are presented. In the simulation setup, we assumed the same topology and the simulation parameters as in Chapter 3. A two-dimensional plane in Fig. 3.2 is assumed, where the coordinates are set to (0, 0) for source and (10, 0) for destination; with N untrusted relays, and an external eavesdropper E_e randomly distributed between the source and destination. For the proposed scheme, the secrecy is analyzed by NM algorithm and their performance is compared with EPA results and other optimization methods like gradient-based and exhaustive search algorithms.

Fig. 6.2 demonstrates the use of path probability selection of ACO in relay selection algorithm with EPA strategy, where secrecy is plotted against SNR for different α and β values. The scenario maps to a traditional model for equal α and β values ($\alpha = \beta = 2$); a path-loss model when β is zero and α is non- zero ($\alpha = 2$, $\beta = 0$) and a fading model when α is zero and β is non-zero ($\alpha = 0$, $\beta = 2$). The system shows similar performance as traditional BRS algorithm for the case

when α and β are equal, irrespective of their numerical value. If we consider the same channel coefficients, secrecy is highest for the case when α and β are equal compared with the other two cases, where the effect of only non-zero factor is considered. Since the external eavesdropper and untrusted relays cooperate with each other, i.e., it shares information and make the attack more effective, the worst case scenario shows poor secrecy performance compared with untrusted relaying case.

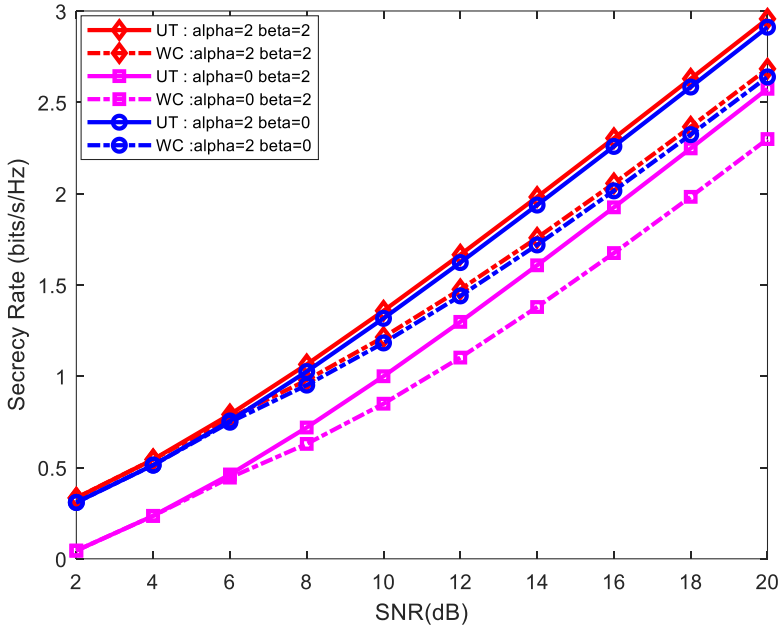


Fig. 6.2 Secrecy rate versus SNR for different values of α and β

Fig. 6.3 gives the comparison of secrecy rate of OPA/EPA schemes. Case 1 and 2 represent the symmetric and asymmetric cases respectively depending on the relay position. The best relay case with relay at the center of the network model is assumed for symmetric case and the relay near to source is considered for asymmetric case. It

is clear from the figure that the secrecy increases with SNR and with jamming signals, since the overall SNR at the eavesdropper reduces. OPA shows better secrecy at low SNRs; as power is distributed based on the location of internal and external eavesdroppers. This effect is more predominant in asymmetric case. For both UT and WC scenarios, EPA shows good performance almost same as OPA for symmetric case and therefore the variation among EPA and OPA is very less for the entire SNR range. The secrecy rate changes at a rate of 0.02 bits/s/Hz for Case 1 and 0.16 bits/s/Hz for Case 2 for every 2dB change in SNR.

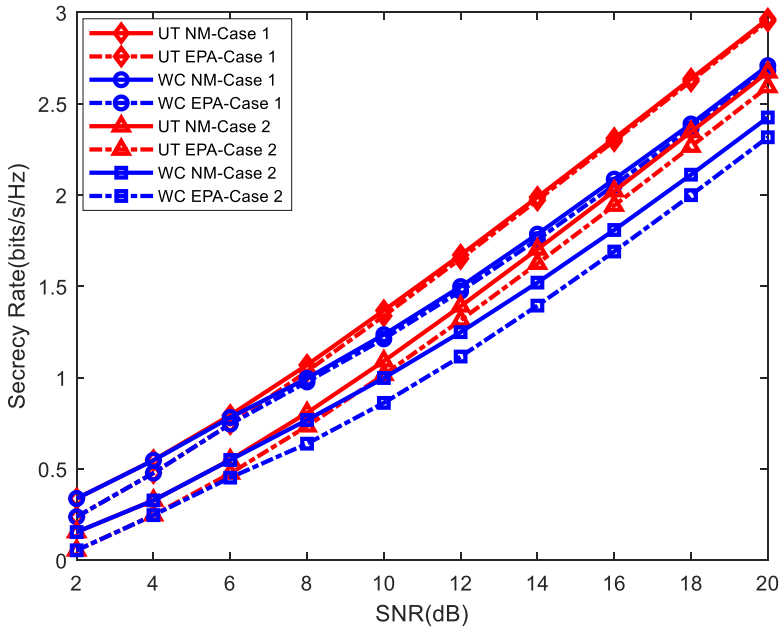


Fig. 6.3 OPA/EPA secrecy rate comparisons for untrusted and worst case scenarios

Fig. 6.4 shows the variation of power allocation factors corresponding to the OPA results of Fig. 6.3 for the proposed untrusted scheme. a and a_s depend on the position of internal and external eavesdroppers.

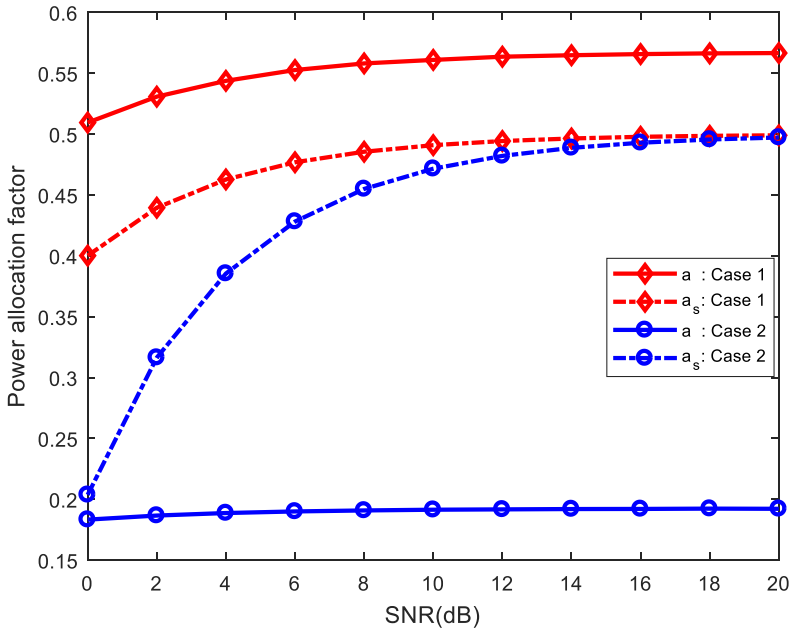


Fig. 6.4 Power allocation factors versus SNR for the proposed untrusted case

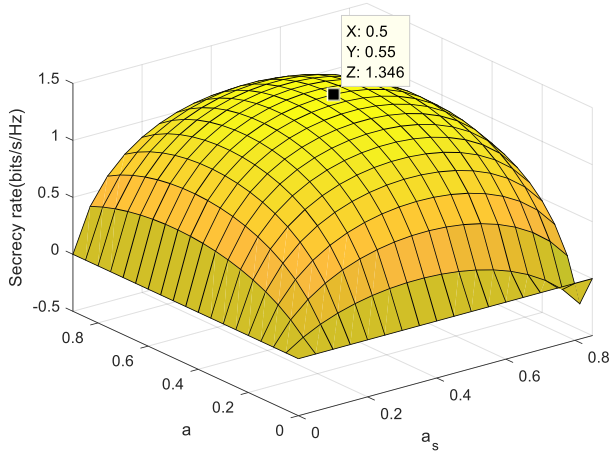
For symmetric case, when the selected relay appears at the middle of the network model, source and relay nodes take same powers for transmission. Hence *a* remains almost constant at 0.5; the variation of *a* is between 0.52 and 0.56 for the entire SNR range. For the asymmetric case, source requires less power compared to relay (*a* = 0.19) since the relay near to source is considered. The external eavesdropper near to source is assumed for the analysis. More power should be given to jamming signals in order to confuse the eavesdroppers during the first phase than the second phase. This is clear from the curves of a_s. Jamming powers (1-a_s) of 0.5091 and 0.5284 are allocated for case 1 and case 2 respectively at 10dB. Since secrecy is dependent on SNR, the variation is effective for SNRs of 10 dB and above. Similar is the results with WC scenario, but with

less performance than UT relaying case.

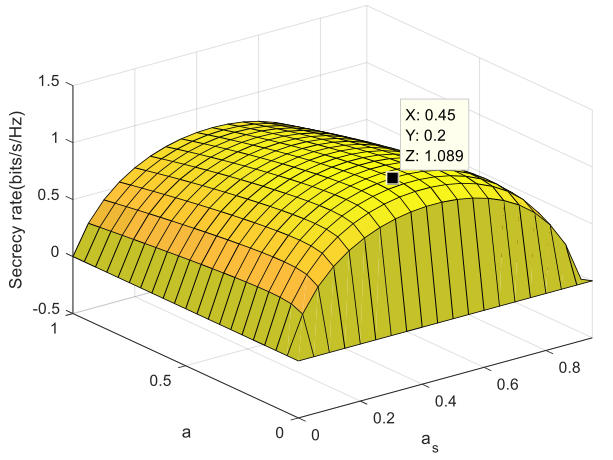
Table 6.1 presents the performance comparison of the NM method for the proposed untrusted case with gradient-based and two dimensional exhaustive search algorithms for symmetric and asymmetric relay positions. Since secrecy rate is a nonlinear function of two variables, it is time consuming rather complicated to compute the function derivatives in gradient method. The NM method produces better results since the objective function is free from finding the derivative as in gradient method. Exhaustive search method, being the simplest of all methods produces accurate results, and the accuracy increases with the number of iterations *m*. This method generally replaces with heuristic approach since it is computationally inefficient. The results of exhaustive search algorithm are obtained by simulation and the plots for symmetric and asymmetric cases with $m = 20$ are given in Fig. 6.5*(a)* and Fig. 6.5*(b)* respectively.

Table 6.1 Performance comparison of NM method with other optimization methods for the proposed untrusted relaying case

Optimization Method	Symmetric case			Asymmetric case		
	$\boldsymbol{a}$	a_s	R_s	a	a_s	R_s
NM method	0.560966	0.490926	**1.367478**	0.191473	0.471595	**1.090262**
Gradient method	0.5604	0.4909	**1.3654**	0.1906	0.4716	**1.0896**
Exhaustive search	0.55	0.5	**1.346**	0.2	0.45	**1.089**



(a)



(b)

Fig. 6.5 Secrecy rate versus power allocation factors a & a_s for the proposed case *a)* Symmetric case *b)* Asymmetric case

One way to determine the complexity of the proposed NM algorithm is to analyse the average number of iterations needed for function convergence during simulation. The comparison of complexity analysis among SBJ untrusted/trusted and SRBJ schemes are presented in Table 6.2.

Table 6.2 Complexity analysis among the proposed schemes

SNR (dB)	Average number of iterations					
	Symmetric case		Asymmetric case		SBJ Trusted	SRBJ
	SBJ: UT	SBJ:WC	SBJ:UT	SBJ:WC		
0	61	61	65	81	65	142
2	63	63	59	79	59	98
4	49	55	51	75	51	94
6	43	48	49	67	49	86
8	40	45	47	51	47	84
10	39	43	41	53	41	86
12	38	39	43	51	43	88
14	38	39	41	53	41	86
16	39	40	43	49	43	82
18	40	41	45	53	45	78
20	40	41	43	51	43	80

For the proposed scheme, the number of iterations for both symmetric and asymmetric untrusted and worst case scenarios are presented. It is clear that the symmetric case requires less number of iterations for convergence than asymmetric case. Being the worst case from the viewpoint of secrecy, WC scenario requires more number of iterations to converge. It is also understood that the SBJ untrusted and trusted schemes show almost same number of iterations to converge, which indicates that they are less complex than SRBJ. It is evident that increase in SNR decreases the average number of iterations; showing not much variation beyond 10 dB in all cases. It is obvious that the average number of iterations increases with complexity; which further increases the computational time and memory usage.

Fig.6.6 and Fig.6.7 illustrate the secrecy rate and their power

allocation factors between both untrusted cases in terms of source-relay distance. The proposed NM method shows better performance compared with the other methods. In OPA, powers allotted at the source and relay depends on the location of internal and external eavesdroppers; whereas equal powers are allotted in EPA. Equal power shows good performance only for the symmetric case where $\gamma_{sk} = \gamma_{kd}$; i.e., for the relay at the centre of the model. Hence the performance of EPA is poor for the cases when relays lie near to source or destination and is clear from the Fig. 6.6. It is understood from the Fig. 6.7 that more source power *(a)* is needed when the source-relay distance increases and more jamming power $(1-a_s)$ is required when the eavesdroppers lie near to source.

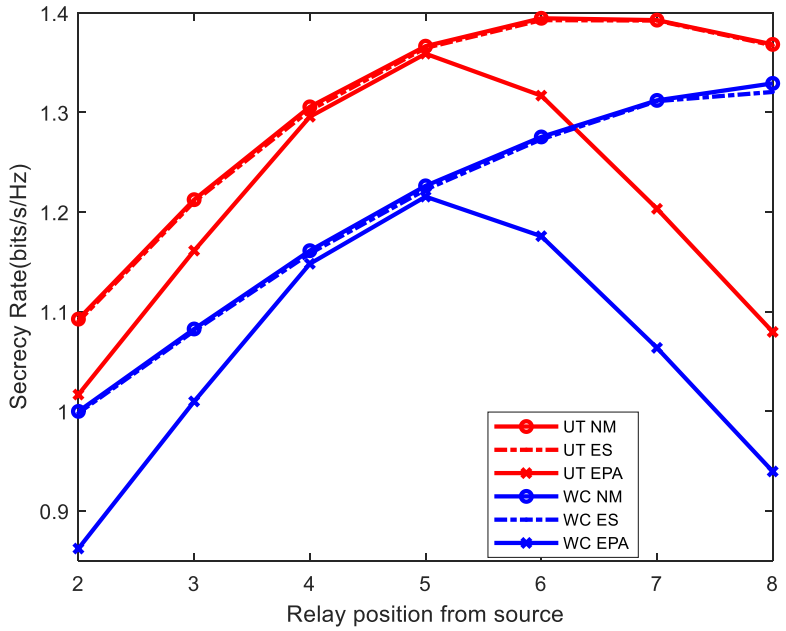


Fig.6.6 OPA/EPA secrecy results among the untrusted and worst case scenarios in terms of source-relay distance

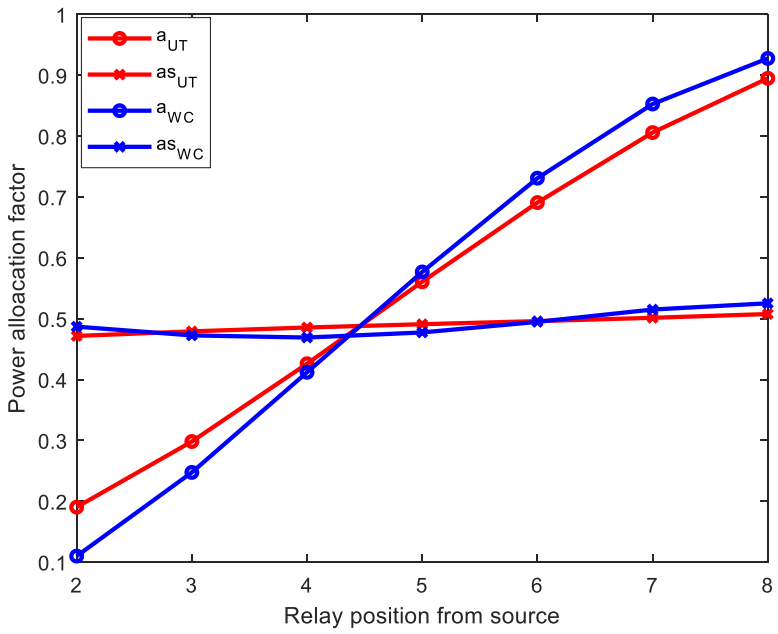


Fig. 6.7 Power allocation factors in terms of source-relay distance

6.5 Chapter Summary

In this chapter, the problem of secure communication in a two-hop AF relaying network with multiple untrusted relays and an external passive eavesdropper is studied by employing a gradient-free power optimization strategy on source-based-jamming scheme. Nelder-Mead method is used for power optimization. ACO path probability criterion based relay selection helps to evaluate the secrecy performance in three wireless scenarios. Optimization methods such as gradient-based method and exhaustive search algorithms are derived for comparison of power optimization algorithm. The secrecy performance of the proposed untrusted relaying scheme is compared with worst case scenario and also with that of jamming scheme without optimization (EPA strategy). Numerical results show that the

proposed OPA outperforms the gradient-based and exhaustive search algorithms. It also provides better secrecy compared to EPA. The complexity analysis is also performed.

The proposed model corresponds to practical scenarios like public ad-hoc networks or heterogeneous networks. From the simulation results, it is found that the complexity of the proposed scheme is more or less same as that of SBJ trusted scheme. Since the model differs from SRBJ/SBJ trusted cases, secrecy cannot be compared, but the proposed model guarantees better secrecy. WC scenario is more complex than UT scheme, hence produces less performance.

Chapter 7
Conclusions and Future Work

In this thesis, physical layer security enhancement techniques in wireless networks are studied. The thesis starts with an extensive and comprehensive review of background information related to current network security issues in wireless communications. Aiming at enhancing the wireless security and improving the inadequacies of existing works, several security enhancement mechanisms of wireless communications by exploiting cooperative diversity solutions are proposed. The summary of the findings and directions of future works are presented in this chapter.

7.1 Summary and Major Findings

7.1.1 Cooperative Relaying and Relay Selection

Cooperative communication can efficiently mitigate the effect of fading with the help of relays and proper relay selection techniques. The thesis proposed a novel relay selection technique based on the probability of path selection criterion of Ant Colony Optimization algorithm, for two-hop cooperative networks using amplify-and-forward and decode-and-forward transmission protocols. The proposed scheme helped to analyze the secrecy performance in different wireless scenarios like traditional, path loss and fading models. It is found that increasing the number of relaying nodes significantly improves the secrecy of both AF/DF schemes, showing the advantage of exploiting multiple relays against eavesdropping. However, when the number of relay nodes continues to increase, the secrecy rate increases slowly and gets saturated.

7.1.2 Source and Relay Based Jamming with Power Optimization

Though relay selection can overcome the inefficient spectral usage of cooperative relays, it cannot always guarantee secrecy when the legitimate channel conditions are poor. Cooperative jamming technique is used to overcome this problem. A source and relay based jamming scheme with a gradient-free power optimization method – Nelder Mead algorithm is proposed for a two-hop trusted AF relaying network. The optimized model shows significant performance improvement compared to traditional transmission schemes, conventional optimization methods and EPA strategy. The impact of single and multiple relays on secrecy is also evaluated. The location of the relay is crucial to the performance. The best performance with AF is achieved when the relay is at the center of the network model.

7.1.3 Source Based Jamming with Power Optimization for Trusted Relaying

The SRBJ scheme has problems with complexity in using two jamming signals and with the nature of relays, i.e., this can be applied only for trusted relaying case. These problems are mitigated by employing a single jamming signal added either at the source or relay node. Based on this, a power optimized source based jamming scheme is proposed. Incorporating the ACO based relay selection scheme and Nelder-Mead algorithm for power optimization into the proposed scheme, the secrecy performance in different wireless scenarios is analyzed and the proposed scheme shows significant secrecy enhancement compared with SRBJ and traditional schemes. The complexity analysis shows a significant reduction in the complexity of SBJ compared to SRBJ model.

7.1.4 Source Based Jamming with Power Optimization for Untrusted Relaying

The thesis proposed an SBJ scheme for cooperative networks in practical scenarios like ad-hoc or heterogeneous networks; where the assistance of the intermediate relaying node is essential to convey a confidential message from the source to the destination. At the same time the information transmitted need to be protected, as the relays may not be authenticated. Adopting the ACO based relay selection scheme and Nelder-Mead power optimization algorithm into the SBJ strategy helped to analyse the secrecy performance in traditional, path loss and fading models. The optimized model shows significant performance improvement over traditional transmission/ optimization methods and also with the worst case scenario, where the eavesdropper and untrusted relays are assumed to be cooperating with each other.

7.2 Comparison of Proposed Algorithms

Parameters	**SRBJ (Chapter 4)**	**SBJ Trusted (Chapter 5)**	**SBJ Untrusted (Chapter 6)**	
			UT	**WC**
a	0.574444	0.5765663	0.5609668	0.5750696
a_s	0.479125	0.4734986	0.4909266	0.4774401
a_r	0.485786	-	-	-
R_s	1.225344	1.22043	1.367478	1.215163
Average number of iterations	86	41	39	43
Inference	Uses two jamming signals, complexity is more, produces better secrecy rate than conventional schemes	Complexity is reduced at the expense of secrecy performance by employing single jamming signal.	Model corresponds to practical scenarios like public ad-hoc networks or heterogeneous networks. Complexity is more or less same as that of SBJ trusted scheme. Since the model differs from the previous cases, secrecy cannot be compared, but guarantees better secrecy. WC scenario is more complex than UT scheme, hence less performance.	

7.3 Future Work

Some potential directions for future work are given below.

- Optimized cooperative jamming model with decode-and-forward protocol can be implemented by incorporating an error correction scheme at the relay which further enhances the secrecy.

- Another approach would be to design a joint relay selection and power allocation strategy for cooperative networks with trusted and untrusted relays, by which the complexity of the system can be reduced.

- The work can be extended to a generalized wireless communication scenario, where there exist multiple eavesdroppers that can wiretap the communication. The scenarios of colluding and non-colluding eavesdropper cases can also be investigated.

- Current physical layer security studies are more concerned about passive eavesdropping attacks; however, cases of active attacks can be considered for future investigation.

- The work can be extended to full duplex relay systems. The conventional half-duplex relay (HDR) considered in the proposed work, performs transmission or reception at one time, whereas a full-duplex relay (FDR) can transmit and receive

simultaneously on the same frequency. Hence, FDR system can significantly improve the secrecy rate.

- Two-hop AF relay systems are considered for cooperative jamming scheme. It is suggested to explore the impact of using the proposed cooperative jamming scheme on the secrecy of multi-hop AF relaying systems.

- The area of research is basically on how to ensure secrecy and protect the information leakage from the illegitimate receiver. Although cooperative diversity improves reliability and latency, these constraints are not considered in this work. This can be considered as future work.

Appendix I

A. Gradient Based Optimization Method (3 Variable Optimization)

The gradient based method uses second derivative test to find the maxima/minima of the function; i.e., the concavity of the function at a critical point determines whether it has got a local maximum/minimum at that point. Since our function R_s for SRBJ scheme is dependent on three power allocation factors viz, a, a_s and a_r; we have to optimize these parameters to get the maximum of R_s.
The steps involved are briefly illustrated below:

1. Find the partial derivative of the function $\frac{\delta R_s}{\delta a}, \frac{\delta R_s}{\delta a_s}, \frac{\delta R_s}{\delta a_r}$

2. Solve for all a, a_s, a_r that satisfy the equations $\frac{\partial R_s}{\partial a} = 0, \frac{\partial R_s}{\partial a_s} = 0, \frac{\partial R_s}{\partial a_r} = 0 \quad \frac{\partial^2 R_s}{\partial a^2} = 0, \frac{\partial^2 R_s}{\partial {a_s}^2} = 0, \frac{\partial^2 R_s}{\partial {a_r}^2} = 0$ to find the critical points. i.e., the points at which the function may have maximum or minimum.
3. Find the Hessian matrix H of second partial derivatives

$$H = \begin{bmatrix} \frac{\partial^2 R_s}{\partial a^2} & \frac{\partial^2 R_s}{\partial a \partial a_s} & \frac{\partial^2 R_s}{\partial a \partial a_r} \\ \frac{\partial^2 R_s}{\partial a_s \partial a} & \frac{\partial^2 R_s}{\partial {a_s}^2} & \frac{\partial^2 R_s}{\partial a_s \partial a_r} \\ \frac{\partial^2 R_s}{\partial a_r \partial a} & \frac{\partial^2 R_s}{\partial a_r \partial a_s} & \frac{\partial^2 R_s}{\partial {a_r}^2} \end{bmatrix}$$

4. Evaluate the Hessian matrix at critical points and check the eigenvalues at those points.
5. *i)* If H is positive definite or if it has all positive eigenvalues, Rs has a local minima at that point

   ii) If H is negative definite or if it has all negative eigenvalues, Rs has a local maxima at that point.

   iii) If H has both positive and negative eigenvalues, then that point is a saddle point of the function.

B. Gradient based Optimization Method (2 Variable Optimization)

The secrecy rate function *Rs* for SBJ scheme is dependent on two power allocation factors viz, a, a_s; we have to optimize these parameters to get the maximum of R_s.

The steps involved are briefly illustrated below:

i. Find the partial derivative of the function $\frac{\delta R_s}{\delta a}, \frac{\delta R_s}{\delta a_s}$

ii. Solve for all a, a_s that satisfy the equations $\frac{\partial R_s}{\partial a} = 0, \frac{\partial R_s}{\partial a_s} = 0$ to find the critical points. i.e., the points at which the function may have maximum or minimum.

iii. Find the second order partial derivatives, $\frac{\partial^2 R_s}{\partial a^2}, \frac{\partial^2 R_s}{\partial a_s{}^2}, \frac{\partial^2 R_s}{\partial a \, \partial a_s}$

iv. Let D be a function of a and a_s such that

$$D(a, a_s) = \frac{\partial^2 R_s}{\partial a^2} \frac{\partial^2 R_s}{\partial a_s{}^2} - \frac{\partial^2 R_s}{\partial a \, \partial a_s}^2$$

v. For each critical value (a, a_s) of $R_s(a, a_s)$, evaluate $D(a, a_s)$ and $\frac{\partial^2 R_s}{\partial a^2}$

i. If $D(a, a_s) > 0$ and $\frac{\partial^2 R_s}{\partial a^2} < 0$, then $R_s(a, a_s)$ is a relative maximum value.

ii. If $D(a, a_s) > 0$ and $\frac{\partial^2 R_s}{\partial a^2} > 0$, then $R_s(a, a_s)$ is a relative minimum value.

iii. If $D(a, a_s) < 0$ then $R_s(a, a_s)$ is a saddle point (neither local max nor local min)

iv. In all other cases, you can conclude nothing.

Appendix II
Nelder-Mead Method of Optimization with Two Variables

The NM algorithm minimizes a function of n variables depending on the function values at (n+1) vertices of a general simplex. Since the SR in this work is a function two variables a and a_s, the simplex is a triangle. The three vertices of the triangle are named as the best x_b, good x_g (next to best) and worst x_w points; corresponding to the smallest, second largest and the largest function values respectively. A pattern search that compares the function values at the vertices of the triangle is then conducted. The NM algorithm starts with a simplex and then modifies it after each iteration using four operations namely reflection, expansion, contraction and shrinking. The sequence of operations that is to be performed depends on the relative values of the objective function at each point. After each iteration, the worst vertex is identified and replaced with a new vertex. This forms a new simplex and the search is continued. The process generates sequence of triangles, with less function values at the vertices, which further reduces the size of the triangles and finally the minimum points are found. Since the NM method finds the minimum of a function, our function is inverted to get the maximum value.

The main steps involved in NM algorithm are presented here for the completeness of the paper. Let the function to be minimized be f. Four scalar factors namely coefficient of reflection (ρ), expansion (ψ), contraction (ε), and shrinkage (γ) are defined for the NM method.

These parameters satisfy the following conditions.

$$\rho > 0;\ \psi > 1;\ \psi > \rho;\ 0 < \varepsilon < 1;\ \text{and}\ 0 < \gamma < 1 \qquad \text{(A2.1)}$$

The universally accepted standard values for the NM algorithm are $\rho = 1;\ \psi = 2;\ \epsilon = ½;$ and $\gamma = ½$.

i **Generate the simplex**: We prefer equal length simplex; assuming the length of the sides of the simplex is r ($r = 1$). Let the initial guess x_o be the third vertex. The other two vertices (p, q) and (q, p) are found by adding a vector to the initial guess, where p and q are

$$q = \frac{r}{2\sqrt{2}}\left(\sqrt{3} - 1\right) \qquad \text{(A2.2)}$$

$$p = q + \frac{r}{\sqrt{2}} \qquad \text{(A2.3)}$$

The three points (p, q), (q, p) and the initial guess x_o correspond to the three vertices $\{x_1, x_2, x_3\}$ of the simplex. Each vertices has two components corresponding to the power allocation factors a and a_s. After generating the initial simplex, evaluate the functions f_1, f_2 and f_3 at the corresponding vertices, where $f_i = f(x_i)$, $i = 1, 2, 3$. The vertices are then ordered such that $f_1 < f_2 < f_3$, so as to rank them as best (x_b), good (x_g) and worst (x_w) respectively. i.e., x_b, x_g and x_w denote the smallest, second largest and the largest function values respectively. Since EPA provides fairly good results, the initial guess is assumed as [0.5, 0.5].

ii **Reflection**: The reflected point x_r is computed as

$$x_r = x_m + \rho\,(x_m - x_w) \qquad \text{(A2.4)}$$

where x_m is the middle point of line joining x_b and x_g given as,

$$x_m = \frac{x_b + x_g}{2} = \left(\frac{x_1 + x_2}{2}, \frac{y_1 + y_2}{2}\right) \qquad \text{(A2.5)}$$

The function value f_r at x_r is evaluated with $\rho = 1$.

iii **Expansion**: If f_r is better than the best point, the reflection is successful and an expansion in the same direction is performed. The expanded point is

$$x_e = x_r + \psi (x_r - x_m) \quad \text{(A2.6)}$$

where the parameter ψ is taken as 2. The function value f_e at x_e is evaluated; the iteration terminates after retaining x_e (if $f_e < f_r$) or x_r (if $f_e > f_r$) .

iv **Contraction**: If the reflected point is poorer than the worst point, a better point occurs between x_w and x_m and perform inside contraction,

$$x_c = x_m - \epsilon (x_m - x_w) \quad \text{(A2.7)}$$

where the contraction parameter ϵ is set to 0.5. If the function f_c at x_c is better than the worst point, keep the new point, else go to shrink (Step 5).

Outside contraction is done if the reflected point is not worse than the worst point, but worse than the good point x_g

$$x_o = x_m + \epsilon (x_m - x_w) \quad \text{(A2.8)}$$

If the function f_o at x_o is better than the reflected point, keep the new point, else go to shrink (Step 5).

v **Shrinking**: The best point is retained and shrinks the simplex. i.e., for all points except the best one, a new point is computed as

$$x_i = x_b + \gamma (x_i - x_b) \quad \text{(A2.9)}$$

where $i = 2, 3$ and the shrinkage parameter γ is usually set as 0.5.

With these steps the iteration completes and a new simplex is formed. Then the process repeats with the new simplex.

Bibiliography

1. **A Bletsas, A. Khisti, D. Reed and A. Lippman** (2006) A simple cooperative diversity method based on network path Selection, *IEEE Journal on Selected Areas in Communications*, 24, 659-672.

2. **A Bletsas, H. Shin, and M. Z. Win** (2007) Cooperative communications with outage-optimal opportunistic relaying, *IEEE Transactions on Wireless Communications* 6(9), 3450 - 3460.

3. **A. D. Wyner** (1975) The Wire-Tap Channel, *Bell System Technical Journal*, 54(8), 1355-1387.

4. **A. Ibrahim, A. Sadek, W. Su, and K. Liu** (2008) Cooperative communications with relay-selection: When to cooperate and whom to cooperate with?, IEEE *Transactions on Wireless Communication*, 7(7), 2814–2827.

5. **A. Jindal, C. Kundu, and R. Bose** (2014a) Secrecy outage of dual-hop AF relay system with relay selection without Eavesdropper's CSI, *IEEE Communication Letters*, 18(10), 1759–1762.

6. **A. Jindal, C. Kundu, and R. Bose** (2014b) Secrecy outage of dual-hop amplify and-forward system and its application to relay selection, *Proceedings of IEEE 79th VTC Spring*, May, 1– 5.

7. **A. Khisti and G. W. Wornell** (2010a) Secure transmission with multiple antennas—Part I: The MISOME wire-tap channel, *IEEE Transactions on Information Theory*, 56(7) 3088–3104.

8. **A. Khisti and G. W. Wornell** (2010b) Secure transmission with multiple antennas - Part II: the MIMOME wire-tap channel, *IEEE Transactions on Information Theory*, 56(11), 5515–5532.

9. **A Li, Xu Y, Wang Y, Sun L** (2017) Artificial noise-aided secure communication in a bidirectional relaying network, *International Journal of Communication Systems*, 31 (3),1-11.

10. **A Li, Yizhu Xu, Yuhao Wang and Lihua Sun** (2015) Amplify-and-forward-based cooperative jamming strategy with power allocation for secure communication', *International Journal of Communication Systems*, 28(10), 1621-1627.

11. **A. Nosratinia, T E Hunter (2006)** Grouping and partner selection in cooperative wireless networks, *IEEE Journal on Selected Areas in Communications*, 54(4), 369-378.

12. **A. Nosratinia, T. Hunter, and A. Hedayat** (2004) Cooperative communication in wireless networks, IEEE *Communication Magazine*, 42(10),74–80.

13. **Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone.** *Handbook of Applied Cryptography*. CRC press, 1996.

14. **Ali Kuhestani, Abbas Mohammadi, Mohammadali Mohammadi** (2018a), Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive eavesdroppers, *IEEE Transactions on Information Forensics and Security*, 13(2) 341-355.

15. **Ali Kuhestani, Abbas Mohammadi and P. L. Yeoh** (2018b) Optimal power allocation and secrecy sum rate in two-way untrusted relaying networks with an external jammer, *IEEE Transactions on Communications*, 66(6), 2671-2684.

16. **Ali Kuhestani, Abbas Mohammadi, K. Wong, P. L. Yeoh, M. Moradikia and M. R. A. Khandaker** (2018c), Optimal Power Allocation by Imperfect Hardware Analysis in Untrusted Relaying Networks' *IEEE Transactions on Wireless Communications*, 17(7), 4302-4314.

17. **Asma Mabrouk, Ahmed El Shafie, Kamel Tourki, and Naofal Al-Dhahir** (2017) AN-aided relay-selection scheme for securing untrusted RF-EH relay systems,' *IEEE Transactions on Green Communications and Networking*, 1(4), 481 - 493.

18. **Ali Kuhestani and Abbas Mohammadi** (2016), Destination-based cooperative jamming in untrusted amplify-and-forward relay networks: resource allocation and performance study, *IET Communications*, Volume 10, Issue 1, 04 January 2016, p. 17 – 23.

19. **B . Schneier** (1988) Cryptographic design vulnerabilities, IEEE *Computer*, 31(9), 29–33.

20. **C. E. Shannon** (1949) Communication theory of secrecy systems, *Bell System Technical Journal*, 28, 656–715.

21. **C. Jeong, I.M. Kim, and D. I. Kim** (2012) Joint Secure Beamforming Design at the Source and the Relay for an Amplify-and-Forward MIMO untrusted relay system, *IEEE Transactions on Signal Processing*, 60(1), 310–325.

22. **C. S. R. Murthy and B. S. Manoj** *Ad Hoc Wireless Networks: Architectures and Protocols*, Prentice Hall PTR, 2004.

23. **C. Wang, H. Wang and X. Xia** (2015) Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks, *IEEE Transactions on Wireless Communications*, 14 (2), 589-605.

24. **Chaudhuri Manoj Kumar Swain, Susmita Das** (2018) Effects of threshold based relay selection algorithms on the performance of an IEEE 802.16j mobile multi-hop relay (MMR) WiMAX network, Digital *Communications and Networks*, 4, 58–68.

25. **Chinmoy Kundu, Sarbani Ghose, and Ranjan Bose** (2015), Secrecy Outage of Dual-Hop Regenerative Multi-Relay

System with Relay Selection, *IEEE Transactions on Wireless Communications*, 14(8), 4614-4625.

26. **Chinmoy Kundu, Telex M. N. Ngatched, and Octavia A. Dobre** (2016) Relay Selection to Improve Secrecy in Cooperative Threshold Decode-and-Forward Relaying, *Proceedings of IEEE Global Communications Conference (GLOBECOM),* Washington DC, USA, pp. 1-6.

27. **Coello C.A.C.** (2018) Multi-objective Optimization. In: Martí R., Panos P., Resende M. (eds), *Handbook of Heuristics*, Springer, Cham

28. **Dan Deng, Xutao Li, Lisheng Fan, Wen Zhou, Rose Qingy angHu and ZhiliZhou** (2017) Secrecy analysis of multiuser untrusted amplify-and-forward relay networks, *Wireless Communications and Mobile Computing,* 2017.

29. **Doaa H. Ibrahim, Emad S. Hassan, Sami A. El Dolil** (2015) Relay and jammer selection schemes for improving physical layer security in two-way cooperative networks, *Computers & Security*, 50, 47-59.

30. **Dong Wang, Bo Bai, Wenbo Zhao, and Zhu Han** (2018) A Survey of optimization approaches for Wireless Physical Layer Security, *IEEE Communications Surveys & Tutorials*, 21(2), 1878 – 1911

31. **E. C. Van Der Meulen** (1971) Three-Terminal Communication Channels, *Advanced Applied Probability*, 3, 120–54.

32. **Emmerich, M.T.M., Deutz, A.H.** (2018), A tutorial on multiobjective optimization: fundamentals and evolutionary methods. *Nat Comput* **17,** 585–609.

33. **F. Oggier and B. Hassibi** (2011) The Secrecy Capacity of the MIMO Wiretap Channel, *IEEE Transactions on Information*

Theory, 57 (8), 4961–4972.

34. **Fatemeh Mansourkiaie and M H Ahmed** (2015) Cooperative Routing in Wireless Networks: A Comprehensive Survey', *IEEE Communication Surveys & Tutorials*, 17(2), 604 – 626.

35. **Fawaz S. Al-Qahtani, Caijun Zhong and Hussein M. Alnuweiri** (2015), Opportunistic relay selection for secrecy enhancement in cooperative networks, *IEEE Transactions on Communications*, 63 (8), 2959-2971.

36. **Fuchang Gao, Lixing Han** (2010) Implementing the Nelder-Mead simplex algorithm with adaptive parameters, *Computational Optimization and Applications*, 51(1), 259-277.

37. **G. Zheng, L C Choo, K K Wong** (2011) Optimal cooperative jamming to enhance physical layer security using relays, *IEEE Transactions on Signal Processing*, 59(3), 1317–1322.

38. **H. Hui, A. Lee Swindlehurst, G. Li and J. Liang** (2015) Secure relay and jammer selection for Physical Layer Security, *IEEE Signal Processing Letters*, 22(8), 1147-1151.

39. **H M Wang, C. Wang, and D. W. K. Ng** (2015) Artificial noise assisted secure transmission under training and feedback, *IEEE Transactions on Signal Processing*, 63, 6285–6298.

40. **H M Wang, M. Luo, Q. Yin, and X. G. Xia** (2013 a) Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdroppers CSI, IEEE Signal Processing Letters, 20(1) 39–42.

41. **H M Wang, M Luo, Q Yin, XG Xia** (2013 b) Hybrid Cooperative beamforming and jamming for physical layer security of two-way relay networks, *IEEE Transactions on*

Information Forensics and Security, 8 (12), 2007–20.

42. **Hesam Moharrer, Ali Olfat** (2014) Joint relay selection and cooperative beamforming in two-hop multi-relay decode-and-forward networks, *IET Communications*, 8(18), 3245-3253.

43. **I. Csiszar, J Korner** (1978) Broadcast channels with confidential messages, *IEEE Transactions on Information Theory*, 24, 339–348.

44. **I. Krikidis** (2010) Opportunistic relay selection for cooperative networks with secrecy constraints, *IET Communications*, 4 (15), 1787–1791.

45. **I. Krikidis, J. Thompson, S. McLaughlin, and N. Goertz** (2009a) Max-min relay selection for legacy amplify-and-forward systems with interference, *IEEE Transactions on Wireless Communications*, 8 (6), 3016–3027.

46. **I. Krikidis, J S Thompson, S McLaughlin** (2009b) Relay selection for secure cooperative networks with jamming, *IEEE Transactions on Wireless Communications*, 8 (10), 5003–5011.

47. **I. Krikidis, J. Thompson, S. McLaughlin, and N. Goertz** (2008) Amplify-and-forward with partial relay selection, IEEE Communication Letters, 12(4), 235–237.

48. **J.A. Nelder, R. Mead** (1965) A simplex method for function minimization, *The Computer Journal*, 7 (4), *308*–313

49. **J Huang, A Mukherjee, A L Swindlehurst** (2013) Secure communication via an untrusted non-regenerative relay in fading channels, *IEEE Transactions on Signal Processing*, 61 (10), 2536–2550.

50. **J Li, A P Petropulu, S Weber** (2011) On cooperative relaying schemes for wireless physical layer security, *IEEE Transactions on Signal Processing*, 59(10), 4985–4997.

51. **J N. Laneman, D. N. C. Tse, and G. W. Wornell** (2004) Cooperative diversity in wireless networks efficient protocols and outage behavior, *IEEE Transactions on Information Theory*, 50(12), 3062–3080.

52. **J Nievergelt** (2000) Exhaustive search, combinatorial optimization and enumeration: Exploring the potential of raw computing power, *Sofsem 2000 - Theory and Practice of Informatics*, Springer LNCS 1963, 18-35.

53. **Jianrong Bao, Jiawen Wu, Chao Liu, Bin Jiang, and Xianghong Tang** (2017) Optimized Power Allocation and Relay Location Selection in Cooperative Relay Networks, *Wireless Communications and Mobile Computing*, 2, 1-10.

54. **Joaquim R. R. A. Martins** *A Short Course on Multidisciplinary Design Optimization*, Multidisciplinary Design Optimization Laboratory, University of Michigan, July 2012.

55. **John H Mathews and Kurtis K Fink** *Numerical methods using Matlab*, 4th Edition, Prentice Hall Inc., 2004.

56. **K. J. Rayliu, A. K. Sadek Weifengsu, and Andres Kwasinski** *Cooperative Communications and Networking*, Cambridge University Press, 2009.

57. **L Dong, H Yousefi'zadeh, H Jafarkhani** (2011) Cooperative jamming and power allocation for wireless relay networks in presence of eavesdropper, Proceedings *of ICC 2011*, Kyoto, Japan.

58. **L Dong, Z Han, A P Petropulu** (2010) Improving wireless physical layer security via cooperating relays, *IEEE Transactions on Signal Processing*, 58(3), 1875–1888.

59. **L J Rodríguez, Nghi H. Tran, Trung Q. Duong, Tho Le-Ngoc, Maged Elkashlan, and Sachin Shetty** (2015) Physical layer security in wireless cooperative relay networks: state of the art and beyond, *IEEE Communications Magazine*, 32-39.

60. **L Lai** and **H El Gamal** (2008) The relay-eavesdropper channel: cooperation for secrecy, *IEEE Transactions on Information Theory*, 54(9), 4005–4019.

61. **L. Sun, P. Ren, Q. Du, Y. Wang, and Z. Gao** (2015) Security-aware relaying scheme for cooperative networks with untrusted relay nodes, *IEEE Communication Letters*, 19 (3), 463-466.

62. **L. Sun, T Zhang, Y Li, H Niu** (2012) Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes, *IEEE Transactions on Vehicular Technology*, 61, 3801–3807.

63. **L Wang, M Elkashlan, J Huang, Nghi H Tran, T Q Duong** (2014) Secure transmission with optimal power allocation in untrusted relay networks, *IEEE Wireless Communications Letters*, 3(3), 289–292

64. **Lagarias, J.C., Reeds, J.A., Wright, M.H., and Wright, P.E.** (1998) Convergence Properties of the Nelder-Mead Simplex Method in Low Dimensions, *Society for Industrial and Applied Mathematics* 9(1), 112–147.

65. **Liang Y, Poor HV, Shamai S.** (2008) Secure communication over fading channels, *IEEE Transactions on Information Theory*, 54(6), 2470- 2492.

66. **Lin Z, Erkip E, Stefanov A** (2006) Cooperative regions and partner choice in coded cooperative systems, *IEEE Transactions on Communications*, 54(7), 1323-1334.

67. **Li Wang, Chunyan Cao, Mei Song, and Yu Cheng** (2014) Joint cooperative relaying and jamming for maximum secrecy capacity in wireless networks, *Proceedings of IEEE International Conference on Communications (ICC)*, Sydney, June.

68. **Long Yang, Jian Chen, Hai Jiang, Sergiy A. Vorobyov,**

and Hailin Zhang (2017), Optimal Relay Selection for Secure Cooperative Communications with an Adaptive Eavesdropper, *IEEE Transactions on Communications*, 16 (1), 26-42.

69. **Lu Lv, Jian Chen, Long Yang, Yonghong Kuo** (2017) Improving physical layer security in untrusted relay networks: cooperative jamming and power allocation, *IET Communications*, 11(3), 393–399.

70. **M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin** (2008) Wireless information-theoretic security, *IEEE Transactions on Information Theory*, 54(6), 2515–2534.

71. **M. Bloch, Matthieu, and Joao Barros** *Physical-layer security: from information theory to security engineering*, Cambridge University Press, 2011.

72. **Marco Dorigo and Thomas Stutzle**. *Ant Colony Optimization*, Prentice-Hall of India Private Ltd., New Delhi, 2006.

73. **Mischa Dohler, Yonghui Li** *Cooperative Communications Hardware, Channel & Phy*, John Wiley & Sons, 2010, 192 p.

74. **Nan Run Zhou, Xun Chen, Chisheng Li, Zhi Xue** (2017) Secrecy rate of two-hop AF relaying networks with an untrusted relay, *Wireless Personal Communications*, 75(1), 119-129.

75. **Nan Run Zhou, Zhi Juan Kang, Xiao Rong Liang (2015)** Secure cooperative communication via artificial noise for wireless two-hop relaying networks, *Wireless Personal Communication*, 82, 1759–1771.

76. **R. Liu and W. Trappe** (Ed.) *Securing Wireless Communications at the Physical Layer*, Springer, 2010.

77. **R. Madan, N. Mehta, A. Molisch, and J. Zhang** (2008) Energy-efficient cooperative relaying over fading channels

with simple relay selection, *IEEE Transactions on Wireless Communication,* 7(8), 3013–3025.

78. **R V L Hartley** (1928) Transmission of information, *Bell System Technical Journal*, 7, 535-563.

79. **Raef Bassily, Ersen Ekrem, Xiang He, Ender Tekin, Jianwei Xie, Matthieu R. Bloch, Sennur Ulukus, Aylin Yener (2013)** Cooperative security at the physical layer: A summary of recent advances, *IEEE Signal Processing Magazine*, 30 (5), 16-28.

80. **S. A. A. Fakoorian and A. Lee Swindlehurst** (2013) Full rank solutions for the MIMO Gaussian wiretap channel with an average power constraint, *IEEE Transactions on Signal Processing*, 61(10), 2620–2631.

81. **S. Abdulhadi, M. Jaseemuddin, and A. Anpalagan** (2012) A survey of distributed relay selection schemes in cooperative wireless ad hoc networks, *Wireless Personal Communications*, 63, 917–935.

82. **S. Goel and R. Negi** (2008) Guaranteeing secrecy using artificial noise, *IEEE Transactions on Wireless Communications*, 7 (6), 2180–2189.

83. **S. Ikki and M. Ahmed** (2010) Performance analysis of adaptive decode-and forward cooperative diversity networks with best-relay selection, *IEEE Transactions on Communications*, 58(1), 68–72.

84. **S. K. Leung Yan Cheong and M. E. Hellman** (1978) The Gaussian Wiretap Channel, *IEEE Transactions on Information Theory*, 24(7), vol. 24, 451–456.

85. **Sarbani Ghose, Chinmoy Kundu, Ranjan Bose** (2016) Secrecy performance of dual-hop decode-and forward relay system with diversity combining at the eavesdropper, *IET Communications*, 10(11), 1282-1293.

86. **T. M. Cover and A. A. El Gamal (1979)** Capacity Theorems for the Relay Channel, *IEEE Transactions on Information Theory*, 25, 572–84.

87. **Tong Li, Tianyu Zhang, Bin Zhong, Zhongshan Zhang, Athanasios V. Vasilakos (2015)** Physical Layer Security via Maximal Ratio Combining and Relay Selection over Rayleigh Fading Channel, *Proceedings of IEEE 26th International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC): Fundamentals and PHY*.

88. **V. N. Q. Bao, N. Linh-Trung, and M. Debbah** (2013) Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers, *IEEE Transactions on Wireless Communications*, 12(12) , 6076–6085.

89. **V. N. Q. Bao, N L Trung** (2012) Multihop decode-and-forward relay networks: secrecy analysis and relay position optimization, *REV J. Electronic Communication*, 2 (1–2), 33–41.

90. **W. Stalling** *Cryptography and Network Security: Principles and Practices*, 3rd ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2010.

91. **W. Wang, K. C. Teh, and K. H. Li** (2016a) Generalized relay selection for improved security in cooperative DF relay networks, IEEE *Wireless Communications Letters*, 5(1), 28 - 31.

92. **W. Wang, K. C. Teh, and K. H. Li** (2016b) Relay selection for secure successive AF relaying networks with untrusted nodes, *IEEE Transactions on Information Forensics and Security*, 11(11), 2466–2476.

93. **W. Zhuang and M. Ismail** (2012) Cooperation in wireless communication networks, *IEEE Transactions on Wireless Communications*, 19(2), 10–20.

94. **X. Chen, Q.F. Zhou, T.W. Siu, F.C.M. Lau** (2011)

Asymptotic analysis of opportunistic relaying based on the max-generalized-mean selection criterion, *IEEE Transactions on Wireless Communication*, 10 (4), 1050-1057.

95. **X. He and A. Yener** (2010) Cooperation with an untrusted relay: A secrecy perspective, *IEEE Transactions on Information Theory*, 56(8), 3807–3827.

96. **X. He and A. Yener** (2009) Two-hop secure communication using an untrusted relay, *EURASIP Journal on Wireless Communications and Networking*, 2009, 1–13.

97. **Xiangyun Zhou**, **Lingyang Song**, **Yan Zhang** Physical *Layer Security in Wireless Communications*, CRC Press, 2013.

98. **Xin-She Yang Zhihua Cui Renbin Xiao Amir Hossein Gandomi Mehmet Karamanoglu** *Swarm Intelligence and Bio-Inspired Computation*, Elsevier 2013.

99. **Y. Jiang, C. Lin, X. Shen, and M. Shi** (2006) Mutual authentication and key exchange protocols for roaming services in wireless mobile networks, *IEEE Transactions on Wireless Communication* 5(9), 2569–2577.

100. **Y. Zou, Jia Zhu, Xianbin Wang**M (2015) Improving Physical-Layer Security in Wireless Communications Using Diversity Techniques, *IEEE Network*, 29(1): 42-48.

101. **Y. Zou, X.Wang, and W. Shen** (2013) Optimal relay selection for physical-layer security in cooperative wireless networks, *IEEE Journal on Selected Areas in Communications*, 31(10), 2099–2111.

102. **Y. Zhao, R. Adve, and T. J. Lim (2007)** Improving Amplify-and-Forward Relay Networks: Optimal Power Allocation versus Selection, *IEEE Transactions on Wireless Communications*, 6 (8), 3114-3123.

103. **Yi Sheng Shiu, Shih Yu Chang, Hsiao Chun Wu, Scott**

C.H. Huang, Hsiao Hwa Chen (2011) Physical layer security in wireless networks: a tutorial, *IEEE Wireless Communications*, 18(2), 66-74.

104. **Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley** (2011), Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting, *IEEE Transactions on Wireless Communications*, 10 (6),1725–1729.

105. **Z. Ding, M. Xu, J. H. Lu, and F. Liu** (2012) Improving wireless security for bidirectional communication scenarios, *IEEE Transactions on Vehicular Technology*, 61(6), 2842–2848.

106. **Zhao, Q. H., D. Urosevic, N. Mladenovic and P. Hansen** (2009) A restarted and modified simplex search for unconstrained optimization', *Computers & Operations Research*, 36(12), 3263–3271.

List of Papers

I. Refereed Journals

1. **P.M. Shemi**, M.G. Jibukumar, M.A. Ali (2019) Nelder-Mead–based power optimization for secrecy enhancement in amplify-and-forward cooperative relay networks, *International Journal of Communication Systems*, Vol 32, Issue 11.
2. **P.M. Shemi**, M.G. Jibukumar, M.K. Sabu (2018) A novel relay selection algorithm using ant colony optimization with artificial noise for secrecy enhancement in cooperative networks, *International Journal of Communication Systems*, Vol 31, Issue 14.

II. Presentation in Conferences

1. **P M Shemi**, M G Jibukumar, M A Ali, Enhancing secrecy in cooperative networks via power optimized source based jamming, 2nd IEEE Middle East and North Africa COMMunications Conference (IEEE MENACOMM'19), Bahrain, 19-22 November 2019.
2. **P M Shemi**, M G Jibukumar, M A Ali, Performance Analysis of Relay Selection based on ACO in AF and DF Cooperative Networks, *4th International Conference on Next Generation Computing Technologies (NGCT 2018)*, UPES, Dehradun, 21-22 Nov 2018.

3. **P M Shemi**, M G Jibukumar, M A Ali, Ant Colony Optimization based relay selection for secrecy enhancement in Decode-and-Forward relay networks, *14th IEEE International Wireless Communications & Mobile Computing Conference (IWCMC)*, Cyprus, 25-29 June 2018.
4. **P M Shemi**, M G Jibukumar, M A Ali, Artificial Noise aided secrecy enhancement in Amplify-and-Forward relay networks, *5th IEEE International Conference on Signal Processing and Integrated Networks (SPIN)*, Noida, Delhi, February 2018.

Curriculum Vitae

1.	**Name**	:	SHEMI P.M.
2.	**Date of Birth**	:	21-10-1972
3.	**Gender**	:	Female
4.	**Educational Qualifications**		

1994 Bachelor of Engineering (BE)

Institution: Noorul Islam College of Engineering,
Kanyakumari, Tamil Nadu
Branch : Electronics and Communication Engg.

2002 Master of Technology (M Tech)

Institution: Department of Electronics,
Cochin University of Science & Technology
Branch : Digital Electronics

Doctor of Philosophy (Ph.D.)

Institution: Cochin University of Science & Technology
Registration Date: 13.10.2014