Physical Layer Security Performance Study for Wireless Networks with Cooperative Jamming

by

Yuanyu Zhang

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(The School of Systems Information Science)
in Future University Hakodate
March 2017

To my family

ABSTRACT

Physical Layer Security Performance Study for Wireless Networks with Cooperative Jamming

by

Yuanyu Zhang

Due to the rapid development of wireless communication technology and widespread proliferation of wireless user equipment, wireless networks become indispensable for lots of applications in daily life. The broadcast nature of wireless medium makes information exchange in such networks vulnerable to eavesdropping attacks from malicious eavesdroppers, resulting in network security one of the major concerns for system designers. Physical layer (PHY) security has been proposed as one promising technology to provide security guarantee for wireless communications, owing to its unique advantages over traditional cryptography-based mechanisms, like an everlasting security guarantee and no need for costly secret key distribution/management and complex encryption algorithms. This thesis therefore focuses on the PHY security performance study for wireless networks with cooperative jamming (a typical PHY security technique), where non-transmitting helper nodes generate jamming signals to counteract eavesdropping attacks.

We first explore the PHY security performances of small-scale wireless networks with *non-colluding* (i.e., independently-operating) eavesdroppers, for which we study

the eavesdropper-tolerance capability (ETC) of a two-hop wireless network with one source-destination pair, multiple relays and multiple non-colluding eavesdroppers. We consider two relay selection schemes to forward the packets from the source to the destination, i.e., random relaying and opportunistic relaying. For both relaying schemes, we first derive the secrecy outage probability (SOP) and transmission outage probability (TOP) of the network by applying the classical Probability Theory. We then determine the ETC of the network by solving an optimization problem that aims to maximize the number of eavesdroppers that can be tolerated under a certain SOP constraint and a certain TOP constraint. Finally, we present extensive simulation and numerical results to demonstrate the validity of the theoretical analysis and also to illustrate our theoretical findings.

We then investigate the PHY security performances of small-scale wireless networks with *colluding* (i.e., cooperatively-operating) eavesdroppers, for which we study the SOP performance of a two-hop wireless network with one source-destination pair, multiple relays and multiple colluding eavesdroppers. Based on the classical Probability Theory, we first conduct analysis on the SOP of the simple non-colluding case. For the SOP analysis of the more hazardous M-colluding scenario, where any M eavesdroppers can combine their observations to decode the message, the techniques of Laplace transform, keyhole contour integral, and Cauchy Integral Theorem are jointly adopted to work around the highly cumbersome multifold convolution problem involved in such analysis, such that the related signal-to-interference ratio modeling for all colluding eavesdroppers can be conducted and thus the corresponding SOP can be analytically determined. Finally, simulation and numerical results are provided to demonstrate the validity of the theoretical analysis also to illustrate our theoretical findings.

Finally, we examine the cooperative jamming design issue in large-scale wireless networks. Towards this end, we propose a friendship-based cooperative jamming

scheme to ensure secure communications in a finite Poisson network with one source-destination pair, multiple legitimate nodes and multiple eavesdroppers distributed according to two independent and homogeneous Poisson Point Processes (PPP), respectively. The jamming scheme consists of a Local Friendship Circle (LFC) and a Long-range Friendship Annulus (LFA), where all legitimate nodes in the LFC serve as jammers, but the legitimate nodes in the LFA are selected as jammers through three location-based policies. To understand both the security and reliability performances of the proposed jamming scheme, we first model the sum interference at any location in the network by deriving its Laplace transform under two typical path loss scenarios. With the help of the interference Laplace transform results, we then derive the exact expression for the TOP and determine both the upper and lower bounds on the SOP, such that the overall outage performances of the proposed jamming scheme can be depicted. Finally, we present extensive numerical results to validate the theoretical analysis of TOP and SOP and also to illustrate the impacts of the friendship-based cooperative jamming on the network performances.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my advisor Professor Xiaohong Jiang, not only for his warm encouragement and thoughtful guidance in my research, but also for his financial support that makes me able to fully concentrate on my research. He has been teaching me, both consciously and unconsciously, the important skills required to be a good researcher and the great personality traits that make a better man. It is a great honor for me to be one of his Ph.D. students and the Ph.D. experience under his supervision is definitely life-changing for me. I would also like to thank Professor Jiang's wife, Mrs Li, for her meticulous care and support for my life. I could not have imagined how hard my life in Hakodate would be without her help. I believe the time we spent together would be the greatest and fantastic memory that I will treasure forever.

Besides my advisor, I would like to thank the rest of my thesis committee: Professor Yuichi Fujino, Professor Hiroshi Inamura and Professor Masaaki Wada for their encouragement and insightful comments that not only helps me to greatly improve this thesis and but also inspires me to widen the area of my future research.

I would also like to give my sincere gratitude to Professor Yulong Shen of Xidian University, China, who gave me the opportunity to work together with Professor Xiaohong Jiang and other members in the laboratory when I was a Master student. He opened the door of scientific research for me and showed me the way to be an excellent researcher.

My sincere thanks also go to other members in our laboratory Juntao Gao, Yin

Chen, Jinxiao Zhu, Bin Yang, Jia Liu, Yang Xu, Bo Liu, Lisheng Ma, Xuening Liao, Xiaolan Liu, Xiaochen Li and Ji He for their contributions in some way to this thesis. I also want to thank my Japanese teachers Katsuko Takahashi, Keiko Ishikawa and Takako Shikauchi; the university staffs Mr. Yoshida, Mr. Terasaki, Mrs Kawagishi and Mrs Mitobe; my dear friends Aiko Nakamura, Wataru Ohtani, and Guannan Guo, who made my life in Hakodate colorful and memorable.

Last but not the least, I would like to thank my family: my parents, brother and sister. Words cannot express how grateful I am to them for all of the sacrifices they have made for me.

TABLE OF CONTENTS

LIST OF FIGURES

Figure

LIST OF TABLES

Table

LIST OF APPENDICES

Appendix

CHAPTER I

Introduction

In this chapter, we first introduce the background of physical layer security and then we present the objective and main works of this thesis. Finally, we give the outline and main notations of this thesis.

1.1 Physical Layer Security

With the rapid development of wireless communication technology and the proliferation of wireless user equipment such as smart phones, PDAs, laptops, etc., wireless networks such as the global cellular networks, satellite communications and wireless local area networks, become indispensable for lots of applications in our daily life [1–3]. Due to the broadcast nature of wireless medium, information exchange over wireless channels is vulnerable to eavesdropping attacks from malicious nodes (i.e., eavesdroppers). As a result, security against the eavesdropping attacks becomes one of the key issues in the design of wireless networks [4–6].

Traditional solutions to protect wireless information transfer from eavesdropping attacks are mainly based on cryptography, which encrypts information with secret keys through various kinds of cryptographic protocols, e.g., the Data Encryption Standard (DES) and RSA algorithm [7]. In cryptography, eavesdroppers are assumed to have limited computing power, such that even if they capture the encrypted infor-

mation, they cannot decrypt it without the secret keys. However, as the computing power of eavesdroppers advances rapidly nowadays, these solutions are facing increasingly high risk of being broken by the relentless brute-force attacks of eavesdroppers [8, 9]. In addition, the lack of centralized control makes the secret key management and distribution in wireless networks, especially in decentralized wireless networks, very costly and complex to be implemented. This necessitates the introduction of more powerful approaches to ensure wireless network security. Physical layer (PHY) security has been recognized as one of these approaches to provide a strong form of security guarantee for wireless networks [10]. The basic principle of PHY security is to exploit the inherent randomness of noise and wireless channels to ensure the confidentiality of information against any eavesdropper regardless of its computing power [11]. Compared to the cryptography-based solutions, PHY security can offer some unique advantages, like an everlasting security guarantee, no need for costly secret key management/distribution and complex cryptographic protocols, and a high scalability for the next-generation wireless communications [12].

The first work regarding PHY security goes back to Wyner's paper [13], which introduced the noisy wiretap channel model. In this model, a legitimate transmitter wishes to communicate securely with a legitimate receiver over a noisy main channel, which is wiretapped by an eavesdropper through another noisy channel, called eavesdropper channel. Wyner's results revealed that a non-zero secrecy rate can be achieved without using any secret keys between the legitimate transmission pair if the eavesdropper channel is a degraded version of the main channel. Csiszár and Körner generalized Wyner's results to a general wiretap channel where the eavesdropper channel is not necessarily degraded with respect to the main channel [14]. Their results showed that a non-zero secrecy rate is still achievable when the eavesdropper channel is not degraded, by using the technique of channel prefix to inject additional randomness into both the main and eavesdropper channels such that a rel-

atively better main channel over the eavesdropper channel can be created. Stimulated by the above observations, extensive research efforts have been devoted to developing PHY security techniques based on the idea of changing the randomness of both the main and eavesdroppers channels so as to yield a channel advantage for the main channel [15, 16]. These techniques mainly includes *cooperative jamming* [17–20], *relay selection* [21–24] and *beamforming/precoding* [25–28].

Cooperative jamming allows non-transmitting helper nodes to send jamming signals to improve the security of a given transmitter-receiver pair. The jamming signal can be Gaussian noise independent of the intended information signal, which will cause interference to both the intended receiver and the eavesdropper and probabilistically yield a net channel gain for the intended receiver [17]. The jamming signal can also be some codeword with a certain structure that can be eliminated only at the legitimate receiver side [19]. Cooperative jamming with Gaussian noise is easy to implement and requires no channel state information (CSI) about the eavesdropper channel, but it could also hurt the main channel. Cooperative jamming with structured codeword can certainly improve the security, but it usually needs a complex design of the codeword and relies heavily on the CSI of eavesdropper channels, which is usually impossible in practice, especially for passive eavesdroppers that only overhear information without sending any signal in order to conceal themselves.

The basic idea of relay selection is to enlarge the channel advantage of the main channel over the eavesdropper channel by selecting a relay that can construct a strong main link but a weak eavesdropper link. Relay selection can be roughly classified into two categories depending on whether the buffers of relays are involved, i.e., normal relay selection [21, 22] and buffer-aided relay selection [23, 24]. Normal relay selection usually selects a *best relay* from all available relays by utilizing the diversity gain offered by multiple relays. Once the relay is selected, the transmission must be conducted in a prefixed manner (e.g., source-relay-destination manner for a two-

hop transmission), even if the channel quality of current transmission is relatively poor. To address this limitation, buffer-aided relay selection utilizes the diversity gain offered by buffers of relays to selects a *best link* from all available links as the current transmission, which certainly improves the security. Relay selection will not do harm to the main channel, but it usually also requires the knowledge of eavesdropper CSI. Besides, the frequent message exchange in the process of relay selection might incur a relatively high overhead to the network.

The technique of beamforming/precoding is based on multi-antenna signal processing. Beamforming refers to transmitting one date stream through multiple antennas, while precoding refers to transmitting multiple data streams simultaneously over multiple antennas. This technique controls the direction and strength of signals such that the signal is radiated towards the direction of the intended receiver, while receivers in other directions can hardly receive the signal. The effect of beamforming/precoding in improving the security is obvious, but it usually requires high coordination (e.g., synchronization) among the nodes involved and high computation overhead to choose the weight of each antenna, which makes it relatively complex to be implemented. Besides, this technique also requires the perfect knowledge of eavesdropper CSI.

Notice that the above techniques focus on changing the channel randomness to ensure the PHY security, while there are also techniques that focus on exploiting rather than changing the inherent randomness of wireless channels. A good example of such kind of techniques is coding [29–31]. Borrowing the idea from stochastic encoding, the coding technique associates each confidential message with multiple protection messages carrying no information. To transmit a confidential message, the encoder will randomly choose a protection message and encode the confidential message and the protection message together into a single codeword. Assuming the eavesdropper channel is worse than the main channel, such protection message is

designed detrimental enough to interfere with the eavesdropper, but still ensuring the resolvability of the confidential message at the intended receiver. This technique can effectively translate the channel advantage of the main channel into a secrecy rate of the confidential message, but the main challenge is how to construct the codebooks. Similar to the majority of the above techniques, coding also requires the knowledge of eavesdropper CSI.

1.2 Objective and Main Works

This thesis adopts the cooperative jamming with Gaussian noise to ensure the security of wireless communications, considering its possibility of being implemented in practice without knowing the CSI of eavesdroppers. Our objective is to fully explore the PHY security performances of wireless networks with cooperative jamming. Towards this end, we first study the PHY security performances of small-scale wireless networks with *non-colluding* eavesdroppers that intercept information independently based on their own signal. We then investigate the PHY security performances of small-scale wireless networks with *colluding* eavesdroppers that can exchange and combine their signals to cooperatively intercept information. Finally, we examine the cooperative jamming design issue in large-scale wireless networks. Three commonly-used PHY security performance metrics are of particular interest, which are *eavesdropper-tolerance capability* (ETC) [32], *secrecy outage probability* (SOP) and *transmission outage probability* (TOP) [33]. ETC characterizes the maximum number of eavesdroppers that can be tolerated by a wireless network. SOP defines the probability that the message from a transmitter is successfully intercepted by eavesdroppers. TOP defines the probability that the intended receiver fails to successfully decode the message from the transmitter. The main works and contributions of this thesis are summarized in the following subsections.

1.2.1 PHY Security Performance Study of Small-Scale Wireless Networks with Non-Colluding Eavesdroppers

This work focuses on the ETC study of two-hop wireless networks with non-colluding eavesdroppers. While existing works [32, 34–36] regarding the ETC study of two-hop wireless networks mainly derived either lower bounds or scaling law results that depict how the ETC scales up as the network size tends to infinity (Please refer to Section 2.1 for related works), the exact ETC of such networks remains largely unexplored. In this work, as a first step towards the study of actual ETC in more general wireless networks, we study the exact ETC of a two-hop wireless network with one source-destination pair, multiple relays and multiple non-colluding eavesdroppers. We consider two relay selection schemes (i.e., random relaying and opportunistic relaying) to forward packets from the source node to the destination node. The main contributions of this work can be summarized as follows:

- We first apply the tools from Probability Theory (e.g., Central Limit Theorem) to develop theoretical models for both the SOP and TOP analysis of the source-destination transmission under both the random relaying and opportunistic relaying schemes.

- We then formulate the ETC problem as an optimization problem that aims to maximize the number of eavesdroppers that can be tolerated under a certain SOP constraint and a certain TOP constraint. Based on the Stochastic Ordering Theory, we then conduct analysis to reveal the monotonicity properties of the SOP and TOP, based on which we solve the optimization problem and determine the ETC of the concerned network.

- Extensive simulation results are presented to validate the efficiency of our theoretical framework and numerical results are also provided to illustrate the ETC of the concerned network with cooperative jamming under both relaying

schemes.

1.2.2 PHY Security Performance Study of Small-Scale Wireless Networks with Colluding Eavesdroppers

Extensive research efforts have been devoted to exploring the PHY security performances of wireless networks with colluding eavesdroppers in terms of the scaling laws of secrecy capacity and ETC, secure connection probability, etc. [37–48] (Please refer to Section 2.2 for related works). These works indicated that eavesdropper collusion represents a more hazardous threat to the security of wireless networks, which can greatly improve the eavesdroppers' capability of intercepting information. Despite the extensive research efforts as mentioned above, the analysis of secrecy outage performance of wireless network with colluding eavesdroppers remains a technique challenge. This is mainly due to that such secrecy outage analysis usually involves highly cumbersome multi-fold convolutions related to the modeling of the probability density function (pdf)/cumulative distribution function (cdf) of the aggregate Signal-to-Interference Ratio (SIR) of all colluding eavesdroppers. This work aims to tackle this challenge and focuses on the SOP study of a two-hop wireless network with one source-destination pair, multiple relays and multiple colluding eavesdroppers. We consider two eavesdropping cases, i.e., non-colluding case and M-colluding case where any M eavesdroppers can combine their observations to decode the message. The main contributions of this work are summarized as follows:

- Based on the classical Probability Theory, we first derive the SOP for the simple non-colluding case, where each eavesdropper works independently and decodes the message solely based on its own observation.

- For the secrecy outage analysis of the more hazardous M-colluding scenario, the techniques of Laplace transform, keyhole contour integral and Cauchy Integral

Theorem are jointly adopted to work around the highly cumbersome multi-fold convolution involved in such analysis, such that the related SIR modeling for all colluding eavesdroppers can be conducted and thus the corresponding SOP can be analytically determined.

- Finally, we provide simulation and numerical results to validate our theoretical analysis and also to illustrate our theoretical findings.

1.2.3 Cooperative Jamming Design in Large-Scale Wireless Networks

Due to the rapid proliferation of smart phones, tablets and PDAs, hand-held devices have been an essential integral part of wireless networks. As these devices are usually carried by human beings, wireless networks, such as mobile ad hoc networks [49], cellular networks [50] and delay-tolerant networks [51], exhibit some social behaviors (e.g., friendship, social trust) nowadays. The potentials of social relationships among network nodes in improving the quality of many important data communication services (e.g., content distribution, data sharing and data dissemination) has been extensively examined (see [52] and references therein). Motivated by this, some recent efforts have been devoted to the cooperative jamming design with the consideration of social relationships among networks [53, 54] (Please refer to Section 2.3 for related works).

While the above works represent a significant process in the study of PHY security-based secure communication in wireless networks with social relationships, the social relationships they considered are simply modeled by an indicator variable. Although these variables are acceptable for characterizing some location-independent social relationships, like social tie and social trust, they may fail to model some important social properties closely related to geometric properties of networks, e.g., small-world phenomenon [55, 56]. Also, the network scenarios they considered are quite simple, which consists of either only one eavesdropper and several jammers or only two clus-

ters of jammers. To the best of our knowledge, the study of PHY security-based secure communication in more general large scale wireless networks with small-world social relationships still remains unknown, which is the scope of this work.

We consider a finite large-scale Poisson network consisting of one source-destination pair, multiple legitimate nodes and multiple eavesdroppers distributed according to two independent and homogeneous Poisson Point Processes (PPP), respectively. A more realistic location-based friendship model is adopted to depict the social relationships among network nodes. The cooperative jamming design in this work takes such friendship into consideration and exploits the fact that only legitimate nodes that are friends of the source are willing to serve as jammers. The main contributions of this work are summarized as follows:

- This paper proposes a friendship-based cooperative jamming scheme to ensure the PHY security-based secure communication between the transmitter and receiver. The jamming scheme comprises a Local Friendship Circle (LFC) and a Long-range Friendship Annulus (LFA), where all legitimate nodes in the LFC serve as jammers, and three location-based policies are designed to select legitimate nodes in the LFA as jammers.

- The TOP and SOP are adopted to model the reliability and security performance of the proposed jamming scheme. For the modeling of these performance metrics, we first conduct analysis on the sum interference at any location in the network by deriving its Laplace transforms under the three jammer selection policies and two typical path loss scenarios [1]. With the help of the interference Laplace transform results, we then derive the exact expression for the TOP and determine both the upper and lower bounds on the SOP, such that the overall outage performances of the proposed jamming scheme can be fully depicted.

- Finally, we present extensive numerical results to validate the theoretical anal-

ysis of TOP and SOP and also to illustrate the impacts of the friendship-based cooperative jamming on the network performance.

1.3 Thesis Outline

The remainder of this thesis is outlined as follows. Chapter II introduces the related works of this thesis. In Chapter III, we introduce our work regarding PHY security performance study of small-scale wireless networks with non-colluding eavesdroppers. Chapter IV presents the work on PHY security performance study of small-scale wireless networks with colluding eavesdroppers and Chapter V introduces the work regarding cooperative jamming design in large-scale wireless networks. Finally, we conclude this thesis in Chapter VI.

1.4 Notations

The main notations of this thesis are summarized in Table 1.1.

Table 1.1: Main notations

Symbol	Definition
S	source node
D	destination node
n	number of relays
m	number of eavesdroppers
M	eavesdropper intensity
R_i	the i-th relay
R_r	selected message relay for random relaying
R_b	selected message relay for opportunistic relaying
E_j	the j-th eavesdropper

$\|h_{i,j}\|^2$	channel gain between nodes i and j
$\mathbb{E}[\cdot]$	expectation operator
$\mathbb{P}[\cdot]$	probability operator
P_t	common transmit power of source and relay nodes
$\mathcal{J}$	jammer set
τ	noise-generating threshold
$\mathrm{SIR}_{i,j}$	signal-to-interference ratio (SIR) from node i to node j
SIR_{agg}	aggregate SIR of colluding eavesdroppers
SIR_x	SIR at location x of a network
γ	minimum required decoding SIR for legitimate nodes
γ_e	minimum required decoding SIR for eavesdroppers
P_{to}	transmission outage probability (TOP)
P_{to}^{ran}	TOP for random relaying
P_{to}^{opp}	TOP for opportunistic relaying
P_{so}	secrecy outage probability (SOP)
P_{so}^{c}	SOP for colluding scenario
P_{so}^{nc}	SOP for non-colluding scenario
$I(x)$	interference at node x
ε_t	TOP constraint
ε_s	SOP constraint
$\mathcal{M}_{ran}$	eavesdropper-tolerance capability of random relaying
$\mathcal{M}_{opp}$	eavesdropper-tolerance capability of opportunistic relaying
$\mathcal{L}_f(\cdot)$	Laplace transform of function f
$\mathcal{B}(o,\mathcal{D})$	two-dimensional finite Poisson Network with radius $\mathcal{D}$
l	distance of source-destination pair
α	path-loss exponent

Φ	Poisson Point Process (PPP) of legitimate nodes
Φ_E	PPP of eavesdroppers
$\Phi_{\mathcal{J}}$	PPP of jammers
λ	density of legitimate nodes
λ_E	density of eavesdroppers
$\mathcal{A}_1$	local friendship circle (LFC)
$\mathcal{A}_2$	long-range friendship annulus (LFA)
$\mathcal{R}_1$	radius of LFC (inner radius of LFA)
$\mathcal{R}_2$	outer radius of LFA
$\mathcal{P}(\cdot)$	location-based jammer selection policy
$\Lambda(\cdot)$	intensity measure of PPP

CHAPTER II

Related Work

This section introduces the existing works related to our study in this thesis, including the works on the ETC study of wireless networks, the works on the PHY security performance study of wireless networks under eavesdropper collusion and the works on the cooperative jamming schemes with social relationships.

2.1 ETC Study of Two-Hop Wireless Networks

Some recent works have been done on the ETC study of wireless networks. These works can be classified into two categories according to the network size. For networks with infinite size or infinite number of nodes, the scaling law of ETC against the per-node throughput was studied in [32] by constructing a highway system. Goeckel *et al.* [34] considered a two-hop relay wireless network with one source-destination pair, multiple relays and eavesdroppers and derived the scaling law of ETC. Sheikholeslami *et al.* [35] then extended this result to a wireless network with multiple source-destination pairs where cooperative jamming signals are generated from concurrent transmitters. For finite networks, Shen *et al.* showed the exact *lower bound* on the ETC of a two-hop relay wireless network [36]. It is noticed that all the above works have focused on either the order-sense scaling law results for infinite networks, or bounds for finite networks. Such order sense results or bounds are certainly im-

portant but cannot reflect the the actual ETC of more practical network scenarios with finite nodes and finite size, which is more important for the system designers. However, to the best of our knowledge, the exact result of ETC has been unexplored yet, mainly due to the challenges posed by modeling the spatial correlation of the signal-to-interference-plus-noise ratio (SINR) in multiple hops and the complexity in determining the distribution of interference.

2.2 PHY Security Performance Study of Wireless Networks with Colluding eavesdroppers

The security performance study of wireless communications under eavesdropper collusion and physical layer security can be classified into two categories, depending on the considered network scenario.

For two-hop wireless networks, the secure connection probability, i.e., the probability that the secrecy rates in two hops are both positive, was investigated in [37] to study when a relay is needed to establish a more secure connection. The authors in [38] proposed novel relay strategies to neutralize information leakage from each user to the colluding eavesdroppers by choosing the forwarding matrix of an amplify-and-forward relay in a multi-antenna non-regenerative relay-assisted multi-carrier interference channel. For a multiuser peer-to-peer (MUP2P) relay network with multiple source-destination pairs, multiple relays and a colluding eavesdropper with multiple antennas, the authors in [39] optimized the transmit power of the source and the beamforming weights of the relays jointly to maximize the secrecy rate subject to the minimum signal-to-interference-noise-ratio constraint at each user and the individual and total power constraints. In [40], Vasudevan *et al.* considered a very similar system model with opportunistic relaying and cooperative jamming schemes as in this thesis, whereas they focused on the scaling law of ETC.

For other wireless networks, the scaling law of secrecy capacity was examined for large-scale networks in [41, 42] as network size tends to infinity. The secrecy-constrained connectivity property of large multi-hop wireless networks with colluding eavesdroppers was considered in [43]. The problem of finding a secure minimum energy routing path of K hops between two nodes in an arbitrary wireless network was considered in [44], subject to constraints on the end-to-end successful eavesdropping probability and throughput over the path. The security scheme design issue and the related optimization problem under eavesdropper collusion also attracted considerable attention for various network scenarios [45, 46]. The SOP i.e., the probability that instantaneous secrecy rate between a transmitter-receiver pair is below some threshold, was investigated for various stochastic networks [47, 48].

2.3 Cooperative Jamming Scheme with Social Relationships

Some recent efforts have been devoted to the study of PHY security-based secure communication in wireless networks with social relationships. Wang *et al.* [53] considered a D2D communication scenario, where the head of two D2D user (DUE) clusters wish to communicate with the help of an intermediate Decode-and-Forward relay. The communication security is guaranteed by the cooperative jamming scheme, where multiple friendly jammers send jamming signals to suppress eavesdroppers, and the social relationship is modeled by a social trust parameter $\mu \in [0, 1]$. Two sets of jammers are selected from DUEs with social trust above some threshold μ_{min}. With the consideration of power constraint, the authors studied the optimal selection of relay and jammers to maximize the secrecy rate of DUE transmission and also to ensure a required SINR level to cellular users. Tang *et al.* [54] considered a wireless network consisting of one source-destination pair, a set of cooperative jammers and one eavesdropper. Cooperative jamming is adopted to ensure the security and the concept of social tie is introduced to model the social relationship between jammers

and the source/destination. The strength of social tie of the n-th jammer is denoted by $a_n \in \{0, 1\}$, where 1 (0) indicates that the jammer is (is not) willing to participate in the cooperative jamming. The authors modeled the decision problem of jammers as a social tie-based cooperative jamming game and then explored the secrecy outage performance of the source-destination pair by computing the Nash equilibrium of the game.

CHAPTER III

Physical Layer Security Performance Study of Small-Scale Wireless Networks with Non-Colluding Eavesdroppers

This chapter focuses on the PHY security performance study of small-scale wireless network with non-colluding eavesdroppers, for which we study the eavesdropper-tolerance capability (ETC) of a two-hop wireless network with non-colluding eavesdroppers. We consider two relaying schemes, i.e., the random relaying which randomly selects a relay from the available relays and the opportunistic relaying which selects the *best* relay based on the link conditions of each relay. For both relaying schemes, we first theoretically analyze the performances of secrecy outage probability (SOP) and transmission outage probability (TOP), based on which we further explore the ETC of the network with both relaying schemes under the constraints of both SOP and TOP. Finally, simulation and numerical results are provided to validate our theoretical analysis and also to illustrate our theoretical findings.

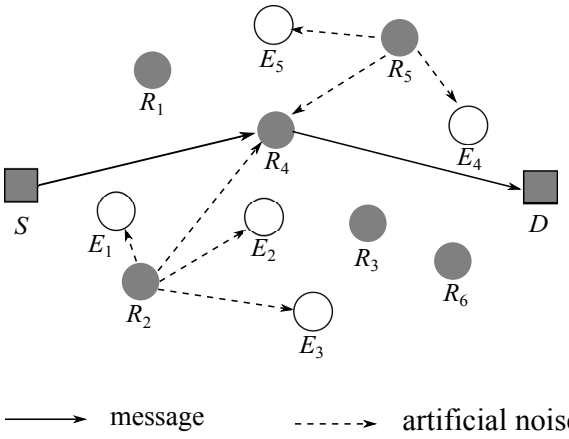


Figure 3.1: System scenario: a source S is transmitting messages to a destination D with the help of relays $R_1, R_2, \cdots, R_n$ ($n = 6$ in this figure) while eavesdroppers $E_1, E_2, \cdots, E_m$ ($m = 5$ in this figure) are attempting to intercept the messages. In this figure, R_4 is the message relay and R_2, R_5 are jammers.

3.1 System Model

3.1.1 Network Model

As depicted in Figure 3.1, we consider a two-hop wireless network consisting of a source node S, a destination node D, n legitimate half-duplex relays $R_1, R_2, \cdots, R_n$ that cannot transmit and receive at the same time and m passive eavesdroppers $E_1, E_2, \cdots, E_m$ of unknown channel information. The eavesdroppers are assumed non-colluding such that they intercept information solely based on their own received signal. We assume that the direct link between S and D does not exist due to deep fading and thus S needs to transmit messages to D via one of the relays. Meanwhile, some of the remaining $n - 1$ relays will be selected as jammers to generate random Gaussian noise to suppress the eavesdroppers during the transmission. We aim to ensure both secure and reliable transmissions from S to D against the eavesdroppers.

Time is slotted and a slow, flat, block Rayleigh fading environment is assumed, where the channel remains static for one time slot and varies randomly and independently from slot to slot. The channel coefficient from a transmitter A to a receiver B is modeled by a complex zero-mean Gaussian random variable $h_{A,B}$ and

thus $|h_{A,B}|^2$ is an exponential random variable. We assume that $|h_{A,B}|^2 = |h_{B,A}|^2$ and $\mathbb{E}\big[|h_{A,B}|^2\big] = 1$, where $\mathbb{E}\big[\,\cdot\,\big]$ stands for the expectation operator. All channel gains $|h_{S,R_i}|^2$, $|h_{R_i,D}|^2$, $|h_{S,E_j}|^2$, $|h_{R_i,E_j}|^2$ and $|h_{R_i,R_k}|^2$ for $i \in [1,n]$, $k \in [1,n], k \neq i$ and $j \in [1,m]$ are assumed independent and identically distributed (i.i.d.). It is assumed that the source S and the relays transmit with the same power P_t. In addition, we assume that the network is interference-limited and thus the noise at each receiver is negligible.

3.1.2 Relaying Schemes and Cooperative Jamming

To ensure the two-hop transmission between S and D, we consider the following transmission protocol which involves both the relay selection and cooperative jamming schemes:

1. **Channel measurement:** In this step, the source S first broadcasts a pilot signal such that each relay can measure the channel coefficient from S to itself. Similarly, the destination D broadcasts a pilot signal to allow each relay to measure the channel coefficient from D to itself. We assume that each relay and eavesdropper can exactly measure the channel coefficients from its observations. Hence, each relay R_i, $i = 1, 2, \cdots, n$ exactly knows h_{S,R_i} and $h_{R_i,D}$, and each eavesdropper E_j, $j = 1, 2, \cdots, m$ exactly knows h_{S,E_j} and h_{D,E_j}.

2. **Relay selection and declaration:** A relay is selected from the n relays as the message relay. We use i^* to denote the index of the message relay. The relay R_{i^*} then broadcasts a pilot signal to declare itself as the message relay. After this step, each relay R_i, $i = 1, 2, \cdots, n, i \neq i^*$ and eavesdropper E_j, $j = 1, 2, \cdots, m$ exactly knows $h_{R_i,R_{i^*}}$ and $h_{E_j,R_{i^*}}$, respectively.

3. **Message transmission from S to R_{i^*}:** In this step, the source S transmits a message to R_{i^*}. At the same time, the ***cooperative jamming*** technique

is adopted to ensure the security of this transmission. This technique allows relays in the set $\mathcal{J}_1 = \{R_i \neq R_{i^*} : |h_{R_i,R_{i^*}}|^2 < \tau\}$ to generate random Gaussian noise in order to suppress the eavesdroppers, where τ is the noise-generating threshold.

4. **Message transmission from R_{i^*} to D:** In this step, the message relay R_{i^*} sends the message to the destination D. Cooperative jamming is also used in this step and relays in the set $\mathcal{J}_2 = \{R_i \neq R_{i^*} : |h_{R_i,D}|^2 < \tau\}$ generate random Gaussian noise to assist the message transmission.

In Step 2, we consider two relay selection schemes. The first one is the ***random relaying***, which randomly selects a relay from $R_1, R_2, \cdots, n$ as the message relay. We use R_r to denote the message relay selected by this scheme. The second one is the ***opportunistic relaying***, which selects a best relay from $R_1, R_2, \cdots, R_n$ that maximizes the minimum of the source-relay channel gain and relay-destination channel gain (i.e., $min\{|h_{S,R_i}|^2, |h_{R_i,D}|^2\}$. We use R_b to denote the relay selected by the opportunistic relaying scheme and

$$b \triangleq \arg\max_{i\in[1,n]} \ min\{|h_{S,R_i}|^2, |h_{R_i,D}|^2\}.$$

Remark 1 *It is notable that the above relay selection requires only the channel state information (CSI) of legitimate channels, which can be estimated by the pilot signals (e.g., ready-to-send (RTS) packet from the source, clear-to-send (CTS) packet from the destination) in practice [57].*

Suppose that the source S is sending signal x to the message relay R_{i^*} during some slot. At the same time, the relay R_i in the set $\mathcal{J}_1$ is sending jamming signal x_i.

The received signal at the message relay is then given by

$$y_{R_{i^*}} = \sqrt{P_t} h_{S,R_{i^*}} x + \sum_{i \in \mathcal{J}_1} \sqrt{P_t} h_{R_i,R_{i^*}} x_i, \tag{3.1}$$

and the received signal at the eavesdropper $E_j, j = 1, 2, \cdots, m$ is given by

$$y_{E_j} = \sqrt{P_t} h_{S,E_j} x + \sum_{i \in \mathcal{J}_1} \sqrt{P_t} h_{R_i,E_j} x_i, \tag{3.2}$$

Hence, the received signal-to-interference ratio (SIR) at R_{i^*} and at E_j in the first hop can be given by

$$\text{SIR}_{S,R_{i^*}} = \frac{|h_{S,R_{i^*}}|^2}{\sum_{i \in \mathcal{J}_1} |h_{R_i,R_{i^*}}|^2}, \text{SIR}_{S,E_j} = \frac{|h_{S,E_j}|^2}{\sum_{i \in \mathcal{J}_1} |h_{R_i,E_j}|^2}. \tag{3.3}$$

Similarly, suppose that the message relay R_{i^*} is forwarding the received signal x to the destination D in the second hop and the relay R_i in the set $\mathcal{J}_2$ is sending jamming signal x_i concurrently. The received signal at D is given by

$$y_D = \sqrt{P_t} h_{R_{i^*},D} x + \sum_{i \in \mathcal{J}_2} \sqrt{P_t} h_{R_i,D} x_i, \tag{3.4}$$

and the received signal at the eavesdropper $E_j, j = 1, 2, \cdots, m$ is given by

$$y_{E_j} = \sqrt{P_t} h_{R_{i^*},E_j} x + \sum_{i \in \mathcal{J}_2} \sqrt{P_t} h_{R_i,E_j} x_i, \tag{3.5}$$

Hence, the received SIR at D and at E_j in the second hop can be given by

$$\text{SIR}_{R_{i^*},D} = \frac{|h_{R_{i^*},D}|^2}{\sum_{i \in \mathcal{J}_2} |h_{R_i,D}|^2}, \text{SIR}_{R_{i^*},E_j} = \frac{|h_{R_{i^*},E_j}|^2}{\sum_{i \in \mathcal{J}_2} |h_{R_i,E_j}|^2}. \tag{3.6}$$

3.1.3 Problem Formulation

In this subsection, we first formulate the transmission outage probability and secrecy outage probability of the concerned network, based on which we then formulate the ETC as an optimization problem.

In practice, a minimum SIR is usually required for receivers to correctly decode the received signal. We define γ the minimum required SIR for legitimate nodes and γ_e that for eavesdroppers. Consider the transmission in a single hop (e.g., the first hop). We say that transmission outage in this hop happens if the message relay cannot correctly decode the message (i.e., $\mathrm{SIR}_{S,R_{i^*}} < \gamma$) and secrecy outage happens if at least one of the eavesdroppers (say E_j) can correctly decode the message (i.e., $\mathrm{SIR}_{S,E_j} \geq \gamma_e$). Generalizing these two outages to the case of two-hop transmission from S to D, we say that transmission (secrecy) outage for the two-hop transmission occurs if the transmission in either hop suffers from transmission (secrecy) outage. Thus, the ***transmission outage probability*** (TOP) for the two-hop transmission is thus defined as the probability that the transmission from S to D suffers from transmission outage and can be formulated as

$$P_{to} = \mathbb{P}\left(\mathrm{SIR}_{S,R_{i^*}} < \gamma \text{ or } \mathrm{SIR}_{R_{i^*},D} < \gamma\right), \tag{3.7}$$

where $\mathbb{P}(\cdot)$ represents the probability operator. The ***secrecy outage probability*** (SOP) is defined as the probability that the transmission from S to D suffers from secrecy outage and can be formulated as

$$P_{so} = \mathbb{P}\left(\bigcup_{j=1}^{m}\left\{\mathrm{SIR}_{S,E_j} \geq \gamma_e\right\} \text{ or } \bigcup_{j=1}^{m}\left\{\mathrm{SIR}_{R_{i^*},E_j} \geq \gamma_e\right\}\right). \tag{3.8}$$

Since security and reliability are two important metrics in network design, we use an SOP constraint ε_s and a TOP constraint ε_t to represent the security and

reliability requirements of the two-hop transmission. We say that the transmission from S to D is *secure if and only if* $P_{so} \leq \varepsilon_s$ and *reliable if and only if* $P_{to} \leq \varepsilon_t$. Based on the definitions of security and reliability, we define the ***eavesdropper-tolerance capability*** (ETC) as the maximum number of eavesdroppers that can be tolerated such that the transmission from S to D is both reliable and secure. From the formulation of SOP and the security constraint, we can see that the maximum number of eavesdroppers that can be tolerated under only the security constraint ε_s is a function of the noise-generating threshold τ for a given n. We use $\mathbf{M}(\tau)$ to denote this function, which is given by

$$\mathbf{M}(\tau) = \max\{m : P_{so}(n, m, \tau) \leq \varepsilon_s\}.$$

Taking the reliability constraint ε_t into consideration, we can now formulate the ETC as the following optimization problem

$$\begin{aligned} \underset{\tau}{\text{maximize}} \quad & \mathbf{M}(\tau) \\ \text{subject to} \quad & P_{to}(n, \tau) \leq \varepsilon_t, \tau \geq 0 \\ & \varepsilon_t \in [0, 1], \varepsilon_s \in [0, 1]. \end{aligned} \tag{3.9}$$

The ETC can thus be determined as the maximum of $\mathbf{M}(\tau)$.

3.2 Outage Performance Analysis

In this section, we theoretically analyze the TOP and SOP of the two-hop transmission from S to D under both the random relaying and opportunistic relaying.

3.2.1 TOP Analysis

We first derive the analytical expression for the TOP of the random relaying and then given an accurate approximation to the TOP of the opportunistic relaying.

3.2.1.1 TOP for Random Relaying

The expression for the TOP of the random relaying is summarized in the following theorem.

Theorem III.1 *Consider the network scenario in Figure 3.1 with cooperative jamming scheme. The TOP P_{to}^{ran} under the random relaying scheme can be given by*

$$P_{to}^{ran} = 1 - \left(e^{-\tau} + \frac{1 - e^{-(1+\gamma)\tau}}{1+\gamma} \right)^{2n-2}, \tag{3.10}$$

where n is the number of relays, τ is the noise-generating threshold in cooperative jamming and γ is the minimum required SIR for legitimate receivers to correctly decode the source message.

Proof 1 *Using the fact that SIR_{S,R_r} and $\mathrm{SIR}_{R_r,D}$ are i.i.d., we can write the TOP in (3.7) as*

$$P_{to}^{ran} = 1 - \mathbb{P}\left(\mathrm{SIR}_{S,R_r} \geq \gamma\right)^2. \tag{3.11}$$

Thus, we only focus on deriving $\mathbb{P}\left(\mathrm{SIR}_{S,R_r} \geq \gamma\right)$, which is

$$\mathbb{P}\left(\mathrm{SIR}_{S,R_r} \geq \gamma\right) = \mathbb{P}\left(\frac{|h_{S,R_r}|^2}{\sum_{i \in \mathcal{J}_1} |h_{R_i,R_r}|^2} \geq \gamma \right).$$

Since the message relay R_r is randomly selected from n relays, $|h_{S,R_r}|^2$ is exponentially distributed with unit mean. Next, we consider the term $\sum_{i \in \mathcal{J}_1} |h_{R_i,R_r}|^2$ which is the summation of random variables less than τ among $n-1$ i.i.d. random variables. We

first define a new random variable

$$U\left(|h_{R_i,R_r}|^2\right) = \mathbf{1}\left(|h_{R_i,R_r}|^2 < \tau\right) \cdot |h_{R_i,R_r}|^2$$

for each R_i*, where* $\mathbf{1}(\cdot)$ *is an indicator variable that equals* 1 *if* $|h_{R_i,R_r}|^2 < \tau$ *and* 0 *otherwise. We then have*

$$\sum_{i\in\mathcal{J}_1} |h_{R_i,R_r}|^2 = \sum_{i=1,i\neq r}^{n} U(|h_{R_i,R_r}|^2),$$

which becomes the summation of $n-1$ *i.i.d. random variables. Notice that* $U(|h_{R_i,R_r}|^2)$ *is a mixed random variable, and the distribution of its discrete part can be given by* $\mathbb{P}\left(U(|h_{R_i,R_r}|^2) = 0\right) = e^{-\tau}$ *and the distribution of its continuous part can be given by*

$$f_{U>0}(u) = \begin{cases} 0, & u \geq \tau \\ e^{-u}, & 0 < u < \tau \end{cases}.$$

Now, we can derive the probability $\mathbb{P}\left(\mathrm{SIR}_{S,R_r} \geq \gamma\right)$ *as*

$$\begin{aligned}
\mathbb{P}\left(\mathrm{SIR}_{S,R_r} \geq \gamma\right) &= \mathbb{E}_{\{U(|h_{R_i,R_r}|^2)\}}\left[\mathbb{P}\left(|h_{S,R_r}|^2 \geq \gamma\left(\sum_{i=1,i\neq r}^{n} U(|h_{R_i,R_r}|^2)\right)\right)\right] \\
&= \mathbb{E}_{\{U(|h_{R_i,R_r}|^2)\}}\left[e^{-\gamma\left(\sum_{i=1,i\neq r}^{n} U(|h_{R_i,R_r}|^2)\right)}\right] \\
&= \mathbb{E}_{\{U(|h_{R_i,R_r}|^2)\}}\left[\prod_{i=1,i\neq r}^{n} e^{-\gamma U(|h_{R_i,R_r}|^2)}\right] \\
&= \prod_{i=1,i\neq r}^{n} \mathbb{E}_{U(|h_{R_i,R_r}|^2)}\left[e^{-\gamma U(|h_{R_i,R_r}|^2)}\right] \\
&= \prod_{i=1,i\neq r}^{n}\left(1\cdot e^{-\tau} + \int_0^{\tau} e^{-\gamma u} f_{U>0}(u)\mathrm{d}u\right) \\
&= \left(e^{-\tau} + \frac{1-e^{-(1+\gamma)\tau}}{1+\gamma}\right)^{n-1}. \qquad \textit{(3.12)}
\end{aligned}$$

Substituting (3.12) into (3.11) completes the proof.

3.2.1.2 TOP for Opportunistic Relaying

Before determining the TOP for the opportunistic relaying, we first define the total interference at the legitimate receiver in two phases by $I(R_b) = \sum_{i\in\mathcal{J}_1} |h_{R_i,R_b}|^2$ and $I(D) = \sum_{i\in\mathcal{J}_2} |h_{R_i,D}|^2$. Then, we establish the following lemmas regarding the probability distribution of $I(R_b)$, $I(D)$ and an important joint probability of the channel gains in two phases, which is critical in deriving P_{to}^{opp}.

Lemma 1 *For one message transmission from* S *to* D*, the total interference* $I(R_b)$ *and* $I(D)$ *are i.i.d., and can be approximated by a normal random variable with a probability distribution function (pdf)*

$$f(x) \approx \hat{f}(x) = \frac{e^{-\frac{(x-\mu)^2}{2\sigma^2}}}{\sigma\sqrt{2\pi}},$$

where

$$\mu = (n-1)\left[1-(1+\tau)e^{-\tau}\right]$$

is the mean and

$$\sigma = \sqrt{(n-1)\Big[1-\tau^2e^{-\tau}-(1+\tau)^2e^{-2\tau}\Big]}$$

is the standard derivation of the normal random variable.

Lemma 2 *For one message transmission from* S *to* D*, the joint probability that* $|h_{S,R_b}|^2$ *is greater than some constant* $x \geq 0$ *and* $|h_{R_b,D}|^2$ *is greater than some constant* $y \geq 0$ *can be determined as*

$$\begin{aligned}&\mathbb{P}\left(|h_{S,R_b}|^2 \geq x, |h_{R_b,D}|^2 \geq y\right)\\ &= 1-(1-e^{-2max\{x,y\}})^n + ne^{-max\{x,y\}}\left[\varphi\left(n, min\{x,y\}\right) - \varphi\left(n, max\{x,y\}\right)\right],\end{aligned}$$

where $\varphi(n,x) = e^{-x}{}_2F_1\left(\frac{1}{2}, 1-n; \frac{3}{2}; e^{-2x}\right)$ *and* ${}_2F_1$ *is the Gaussian hypergeometric function.*

Remark 2 *Since S and relays transmit with the same power P_t, we can omit the P_t in $I(R_b)$ and $I(D)$ in Lemma 1. The proofs of the above lemmas can be found in Appendix A.1.*

For a two-hop wireless network with the opportunistic relaying scheme, we are now ready to derive its TOP P_{to}^{opp} of the end-to-end transmission based on Lemma 1 and Lemma 2.

Theorem III.2 *Consider the network scenario in Figure 3.1 with the cooperative jamming scheme. The TOP P_{to}^{opp} under the opportunistic relaying can be given by*

$$\begin{aligned} P_{to}^{opp} \approx 2\int_0^{(n-1)\tau} g(n,\gamma,x)\hat{f}(x)\left[\xi\left(\frac{x-\mu}{\sigma}\right)-\xi\left(-\frac{\mu}{\sigma}\right)\right]\mathrm{d}x \\ -2\int_0^{(n-1)\tau}\int_0^{x} ne^{-\gamma x}\varphi(n,\gamma y)\hat{f}(x)\hat{f}(y)\mathrm{d}y\mathrm{d}x, \end{aligned} \tag{3.13}$$

where where n is the number of relays, τ is the noise-generating threshold in cooperative jamming, γ is the minimum required SIR for legitimate receivers to correctly decode the source message, $\hat{f}(x) = \frac{e^{-\frac{(x-\mu)^2}{2\sigma^2}}}{\sigma\sqrt{2\pi}}$, $\xi(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-\frac{t^2}{2}}\mathrm{d}t$, $\mu = (n-1)\left[1-(1+\tau)e^{-\tau}\right]$, $\sigma = \sqrt{(n-1)\left[1-\tau^2e^{-\tau}-(1+\tau)^2e^{-2\tau}\right]}$, $g(n,\gamma,x) = (1-e^{-2\gamma x})^n + ne^{-\gamma x}\varphi\left(n,\gamma x\right)$, $\varphi(n,x) = e^{-x}{}_2F_1\left(\frac{1}{2},1-n;\frac{3}{2};e^{-2x}\right)$ and ${}_2F_1$ is the Gaussian hypergeometric function.

Proof 2 *According to the definition of TOP in (3.7), we have*

$$\begin{aligned} P_{to}^{opp} &= 1-\mathbb{P}\left(\mathrm{SIR}_{S,R_b}\geq\gamma,\,\mathrm{SIR}_{R_b,D}\geq\gamma\right) \\ &= 1-\mathbb{P}\left(|h_{S,R_b}|^2\geq\gamma I(R_b),|h_{R_b,D}|^2\geq\gamma I(D)\right), \end{aligned}$$

where $I(R_b)$ and $I(D)$ are the total interferences in the first hop and second hop, respectively. Applying the law of total probability, we have

$$P_{to}^{opp} = 1-\mathbb{E}_{I(R_b),I(D)}\left[\mathbb{P}\left(|h_{S,R_b}|^2\geq\gamma I(R_b),|h_{R_b,D}|^2\geq\gamma I(D)\right)\right] \tag{3.14}$$

Applying Lemma 1, we have

$$P_{to}^{opp} \approx 1 - \int_0^{(n-1)\tau} \int_0^{(n-1)\tau} \mathbb{P}\left(|h_{S,R_b}|^2 \geq \gamma x, |h_{R_b,D}|^2 \geq \gamma y\right) \hat{f}(x)\hat{f}(y)\mathrm{d}y\mathrm{d}x$$

Applying Lemma 2, we have

$$\begin{aligned} P_{to}^{opp} &= 2\int_0^{(n-1)\tau} \int_0^{x} \left\{(1-e^{-2\gamma x})^n - ne^{-\gamma x}\left[\varphi(n,\gamma y) - \varphi(n,\gamma x)\right]\right\} \hat{f}(x)\hat{f}(y)\mathrm{d}y\mathrm{d}x \\ &= 2\int_0^{(n-1)\tau} \int_0^{x} g(n,\gamma,x)\hat{f}(x)\hat{f}(y)\mathrm{d}y\mathrm{d}x \\ &\quad -2\int_0^{(n-1)\tau} \int_0^{x} ne^{-\gamma x}\varphi(n,\gamma y)\hat{f}(x)\hat{f}(y)\mathrm{d}y\mathrm{d}x \\ &= 2\int_0^{(n-1)\tau} g(n,\gamma,x)\hat{f}(x)\left[\xi\left(\frac{x-\mu}{\sigma}\right) - \xi\left(-\frac{\mu}{\sigma}\right)\right]\mathrm{d}x \qquad (3.15) \\ &\quad -2\int_0^{(n-1)\tau} \int_0^{x} ne^{-\gamma x}\varphi(n,\gamma y)\hat{f}(x)\hat{f}(y)\mathrm{d}y\mathrm{d}x, \end{aligned}$$

which completes the proof.

3.2.2 SOP Analysis

From the definition of SOP in (3.8), we have

$$\begin{aligned} P_{so} &= \mathbb{P}\left(\bigcup_{j=1}^{m}\left\{\mathrm{SIR}_{S,E_j} \geq \gamma_e\right\} \text{or} \bigcup_{j=1}^{m}\left\{\mathrm{SIR}_{R_{i^*},E_j} \geq \gamma_e\right\}\right) \qquad (3.16) \\ &= 1 - \mathbb{P}\left(\bigcap_{j=1}^{m}\left\{\mathrm{SIR}_{S,E_j} < \gamma_e\right\}, \bigcap_{j=1}^{m}\left\{\mathrm{SIR}_{R_{i^*},E_j} < \gamma_e\right\}\right) \\ &= 1 - \left[\mathbb{P}\left(\bigcap_{j=1}^{m}\left\{\mathrm{SIR}_{S,E_j} < \gamma_e\right\}\right)\right]^2 \\ &= 1 - \left[\mathbb{P}\left(\bigcap_{j=1}^{m}\left\{\frac{|h_{S,E_j}|^2}{\sum_{i\in\mathcal{J}_1}|h_{R_i,E_j}|^2} < \gamma_e\right\}\right)\right]^2. \end{aligned}$$

It can be seen from (3.16) that actually the SOP under both relaying schemes is identical. The analytical result of the SOP is summarized in the following theorem.

Theorem III.3 *Consider the network scenario in Figure 3.1 with cooperative jamming scheme. The SOP P_{so} under both the random relaying scheme and the opportunistic relaying scheme can be given by*

$$P_{so} = 1 - \left(\sum_{k=1}^{m} \binom{m}{k} (-1)^k \left[(1 - e^{-\tau}) \left(\frac{1}{1+\gamma_e} \right)^k + e^{-\tau} \right]^{n-1} \right)^2, \qquad (3.17)$$

where m is the number of eavesdroppers, n is the number of relays, τ is the noise-generating threshold in cooperative jamming and γ_e is the minimum required SIR for eavesdroppers to correctly decode the source message.

Proof 3 *According to (3.16), we need to derive the probability*

$$\mathbb{P}\left(\bigcap_{j=1}^{m} \left\{ \frac{|h_{S,E_j}|^2}{\sum_{i \in \mathcal{J}_1} |h_{R_i,E_j}|^2} < \gamma_e \right\} \right).$$

Note that the number of noise-generating relays in the first hop $|\mathcal{J}_1|$ follows the binomial distribution $B(n-1, 1-e^{-\tau})$. We define the event that there are s noise-

generating relays in the first hop (i.e., $|\mathcal{J}_1| = s$) by B_s and thus we have

$$\begin{aligned}
&\mathbb{P}\left(\bigcap_{j=1}^{m}\left\{\frac{|h_{S,E_j}|^2}{\sum_{i\in\mathcal{J}_1}|h_{R_i,E_j}|^2} < \gamma_e\right\}\right) \qquad (3.18)\\
&= \sum_{s=0}^{n-1}\mathbb{P}\left(\bigcap_{j=1}^{m}\left\{\frac{|h_{S,E_j}|^2}{\sum_{i\in\mathcal{J}_1}|h_{R_i,E_j}|^2} < \gamma_e\right\}\Big|B_s\right)\mathbb{P}(B_s)\\
&\overset{(a)}{=} \sum_{s=0}^{n-1}\prod_{j=1}^{m}\mathbb{P}\left(\frac{|h_{S,E_j}|^2}{\sum_{i\in\mathcal{J}_1}|h_{R_i,E_j}|^2} < \gamma_e\Big|B_s\right)\mathbb{P}(B_s)\\
&\overset{(b)}{=} \sum_{s=0}^{n-1}\prod_{j=1}^{m}\mathbb{E}\left[1-e^{-\gamma_e\sum_{i\in\mathcal{J}_1}|h_{R_i,E_j}|^2}\right]\mathbb{P}(B_s)\\
&\overset{(c)}{=} \sum_{s=0}^{n-1}\prod_{j=1}^{m}\left(1-\prod_{i\in\mathcal{J}_1}\mathbb{E}\left[e^{-\gamma_e|h_{R_i,E_j}|^2}\right]\right)\mathbb{P}(B_s)\\
&= \sum_{s=0}^{n-1}\left[1-\left(\frac{1}{1+\gamma_e}\right)^s\right]^m\binom{n-1}{s}(1-e^{-\tau})^s(e^{-\tau})^{n-1-s}\\
&= \sum_{k=1}^{m}\binom{m}{k}(-1)^k\left[(1-e^{-\tau})\left(\frac{1}{1+\gamma_e}\right)^k+e^{-\tau}\right]^{n-1},
\end{aligned}$$

where (a) follows since all the $\{\mathrm{SIR}_{S,E_j}, j = 1,\cdots,m\}$ are conditionally independent given the event B_s, (b) follows by applying the law of total probability and the expectation is computed with respect to $\{|h_{R_i,E_j}|^2, i \in \mathcal{J}_1\}$ and (c) follows since all the $|h_{R_i,E_j}|^2$ are i.i.d.. Therefore, (3.17) follows after substituting (3.18) into (3.16).

3.3 Eavesdropper-Tolerance Capability Analysis

In this section, we determine the ETC of the twp-hop relay wireless network under the TOP and SOP constraints for both the random relaying and opportunistic relaying schemes. For each relaying scheme, we first analyze the properties of the optimization problems in (3.9) and then solve the related optimization problem to obtain the ETC.

3.3.1 ETC for Random Relaying

It can be observed from (3.9) that the noise-generating threshold τ is a critical parameter in determining the ETC. A too large τ will do harm to the legitimate transmission, while a too small τ is not enough to suppress the eavesdroppers. Therefore, finding an optimal τ is the key step to solving our considered problem. Before solving the problem, we first establish two lemmas regarding the monotonicity of P_{to}^{ran} and P_{so}, respectively.

Lemma 3 *The TOP for the random relaying P_{to}^{ran} increases monotonically as the noise-generating threshold τ increases.*

Proof 4 *Define the term $e^{-\tau} + \frac{1-e^{-(1+\gamma)\tau}}{1+\gamma}$ in the expression of P_{to}^{ran} in Theorem III.1 as a function $h(\tau)$. We can easily compute its derivative as $e^{-(1+\gamma)\tau} - e^{-\tau}$, which is less than 0 for $\gamma > 0$. Thus, P_{to}^{ran} increases monotonically as τ increases.*

Before giving the lemma regarding the monotonicity P_{so}, we establish the following lemma based on the Stochastic Ordering in [58].

Lemma 4 *Let $\mathbf{X}$ and $\mathbf{Y}$ be two N-dimensional random vectors such that*

$$\mathbb{P}(\mathbf{X} \in \mathcal{U}) \leq \mathbb{P}(\mathbf{Y} \in \mathcal{U}) \text{ for all upper sets } \mathcal{U} \in \mathbb{R}^N.$$

Then $\mathbf{X}$ is said to be smaller than $\mathbf{Y}$ in the usual stochastic order (denoted by $\mathbf{X} \leq_{st} \mathbf{Y}$). And for all increasing function Δ, we always have $\mathbb{E}[\Delta(\mathbf{X})] \leq \mathbb{E}[\Delta(\mathbf{Y})]$.

Based on the above lemma, we are now ready to establish the following lemma in terms of the monotonicity of SOP with respect to τ and m.

Lemma 5 *The SOP P_{so} decreases monotonically as the noise-generating threshold τ increases, but increases as the number of eavesdroppers m increases.*

Proof 5 *Notice that the step following (c) in (3.18) can also be written as*

$$\mathbb{E}\left[1-\left(\frac{1}{1+\gamma_e}\right)^{|\mathcal{J}_1|}\right],$$

where the expectation is with respect to $|\mathcal{J}_1|$*. For any* $0 \leq \tau_1 < \tau_2$*, we use two random variables* $|\mathcal{J}_1^1|$ *and* $|\mathcal{J}_1^2|$ *to represent the number of noise-generating relays in the first phase, where* $|\mathcal{J}_1^1| \sim B(n-1, 1-e^{-\tau_1})$ *and* $|\mathcal{J}_1^2| \sim B(n-1, 1-e^{-\tau_2})$*. It is shown in [59] that* $|\mathcal{J}_1^1| \leq_{st} |\mathcal{J}_1^2|$*. Applying Lemma 4, we can see that*

$$\mathbb{E}\left[1-\left(\frac{1}{1+\gamma_e}\right)^{|\mathcal{J}_1^1|}\right] < \mathbb{E}\left[1-\left(\frac{1}{1+\gamma_e}\right)^{|\mathcal{J}_1^2|}\right].$$

Therefore, the SOP P_{so} *decreases as* τ *increases.*

Next, we consider the step following (c) in (3.18) again. It is easy to see that the term $1-(\frac{1}{1+\gamma_e})^l \in [0,1)$*. Thus, the term* $\left[1-\left(\frac{1}{1+\gamma_e}\right)^l\right]^m$ *decreases with* m*. Therefore, the SOP* P_{so} *increases as* m *increases.*

Based on Lemma 3 and Lemma 5, we can give the ETC of the random relaying in the following theorem.

Theorem III.4 *Consider the network scenario in Figure 3.1 with the random relaying scheme. The ETC of the concerned network with* n *relays under a security constraint* ε_s *and a reliability constraint* ε_t *is*

$$\mathcal{M}_{ran} = \max\{m : G(m, n, \tau_{ran}^*) \geq \sqrt{1-\varepsilon_s}\},$$

where $G(m, n, \tau_{ran}^*) = \sum_{k=1}^{m} \binom{m}{k}(-1)^k \left[(1-e^{-\tau_{ran}^*})\left(\frac{1}{1+\gamma_e}\right)^k + e^{-\tau_{ran}^*}\right]^{n-1}$*,* τ_{ran}^* *is the solution of* $P_{to}^{ran} = \varepsilon_t$ *and* P_{to}^{ran} *is given in Theorem III.1.*

Proof 6 *As shown in the formulation of ETC in (3.9), we need to find the optimal*

τ that maximizes $\mathbf{M}_{ran}(\tau)$, where

$$\mathbf{M}_{ran}(\tau) = \max\{m : G(m, n, \tau) \geq \sqrt{1-\varepsilon_s}\}$$

according to its definition. Since the TOP P_{to}^{ran} increases with τ according to Lemma 3, in order to guarantee the reliability (i.e., $P_{to}^{ran} \leq \varepsilon_t$), τ must take values in the region $[0, \tau_m]$, where τ_m is the solution of $P_{to}^{ran} = \varepsilon_t$.

Next, we need to prove that τ_m is the optimal τ (i.e.,$\tau_{ran}^* = \tau_m$) that achieves the ETC. That is, for any $\tau \in [0, \tau_m)$, we always have $\mathbf{M}_{ran}(\tau) \leq \mathbf{M}_{ran}(\tau_m)$. Now we prove it by contradiction. Suppose there exists a $\tau' \in [0, \tau_m)$ such that $\mathbf{M}_{ran}(\tau') \geq \mathbf{M}_{ran}(\tau_m) + 1$. By Lemma 5, it can be seen that $G(m, n, \tau)$ increases with τ, while decreasing with m. Thus, it is easy to see that

$$G(\mathbf{M}_{ran}(\tau_m) + 1, n, \tau_m) < \sqrt{1-\varepsilon_s},$$

since $\mathbf{M}_{ran}(\tau_m)$ is the largest m satisfying $G(m, n, \tau_m) \geq \sqrt{1-\varepsilon_s}$. Thus, we have

$$G(\mathbf{M}_{ran}(\tau_m) + 1, n, \tau') < G(\mathbf{M}_{ran}(\tau_m) + 1, n, \tau_m) < \sqrt{1-\varepsilon_s}$$

and

$$G(\mathbf{M}_{ran}(\tau_m) + 1, n, \tau') \geq G(\mathbf{M}_{ran}(\tau'), n, \tau') \geq \sqrt{1-\varepsilon_s}.$$

We can see a contradiction from the above two inequalities. Thus, for any $\tau \in [0, \tau_m)$ we always have $\mathbf{M}_{ran}(\tau) \leq \mathbf{M}_{ran}(\tau_m)$ (i.e., $\tau_{ran}^* = \tau_m$) and thus the ETC is achieved at τ_{ran}^*.

3.3.2 ETC for Opportunistic Relaying

Following the idea of determining the ETC of the random relaying, we first establish the following lemma regarding the monotonicity of P_{to}^{opp} with respect to τ.

Lemma 6 *The TOP P_{to}^{opp} for the opportunistic relaying scheme increases as τ increases.*

Proof 7 *For any $0 < \tau_1 < \tau_2$, we use random vector $\mathbf{I}_1 = (I(R_b)^1, I(D)^1)$ to represent the interferences in two hops when the noise-generating threshold is τ_1 and $\mathbf{I}_2 = (I(R_b)^2, I(D)^2)$ to represent those for τ_2. For any upper set*

$$\mathcal{U} = \left\{(I(R_b), I(D))\middle| I(R_b) \geq x \geq 0, I(D) \geq y \geq 0\right\},$$

we always have

$$\mathbb{P}(\mathbf{I}_1 \in \mathcal{U}) = \mathbb{P}(I(R_b)^1 \geq x)\mathbb{P}(I(D)^1 \geq y)$$

and

$$\mathbb{P}(\mathbf{I}_2 \in \mathcal{U}) = \mathbb{P}(I(R_b)^2 \geq x)\mathbb{P}(I(D)^2 \geq y).$$

It is easy to see that $\mathbb{P}(I(R_b)^1 \geq x) < \mathbb{P}(I(R_b)^2 \geq x)$ and $\mathbb{P}(I(D)^1 \geq y) < \mathbb{P}(I(D)^2 \geq y)$, since more interference can be generated as τ increases. Therefore, we have $\mathbb{P}(\mathbf{I}_1 \in \mathcal{U}) < \mathbb{P}(\mathbf{I}_2 \in \mathcal{U})$ and then $\mathbf{I}_1 \leq_{st} \mathbf{I}_2$ according to Lemma 4. Define the term $\mathbb{P}\left(|h_{S,R_b}|^2 \geq \gamma I(R_b), |h_{R_b,D}|^2 \geq \gamma I(D)\right)$ in (3.14) by $\Gamma(\mathbf{I})$ which decreases as $\mathbf{I}$ increases, where $\mathbf{I} = (I(R_b), I(D))$. Thus, we have $\mathbb{E}[\Gamma(\mathbf{I}_1)] > \mathbb{E}[\Gamma(\mathbf{I}_2)]$ according to Lemma 4. That is, for any $0 < \tau_1 < \tau_2$, we always have $P_{to}^{opp}(\tau_1) < P_{to}^{opp}(\tau_2)$, which indicates the TOP P_{to}^{opp} increases with τ.

By applying Lemma 5 and Lemma 6, we can establish the following theorem for the ETC achieved by the opportunistic relaying.

Theorem III.5 *Consider the network scenario in Figure 3.1 with the opportunistic relaying scheme. The ETC of the concerned network with n relays under a security constraint ε_s and a reliability constraint ε_t is*

$$\mathcal{M}_{opp} = \max\{m : G(m, n, \tau_{opp}^*) \geq \sqrt{1-\varepsilon_s}\},$$

where $G(m,n,\tau^*_{opp}) = \sum_{k=1}^{m}\binom{m}{k}(-1)^k\left[(1-e^{-\tau^*_{opp}})\left(\frac{1}{1+\gamma_e}\right)^k + e^{-\tau^*_{opp}}\right]^{n-1}$ *and* τ^*_{opp} *is the solution of* $P_{to}^{opp} = \varepsilon_t$ *and* P_{to}^{opp} *is given in Theorem III.2.*

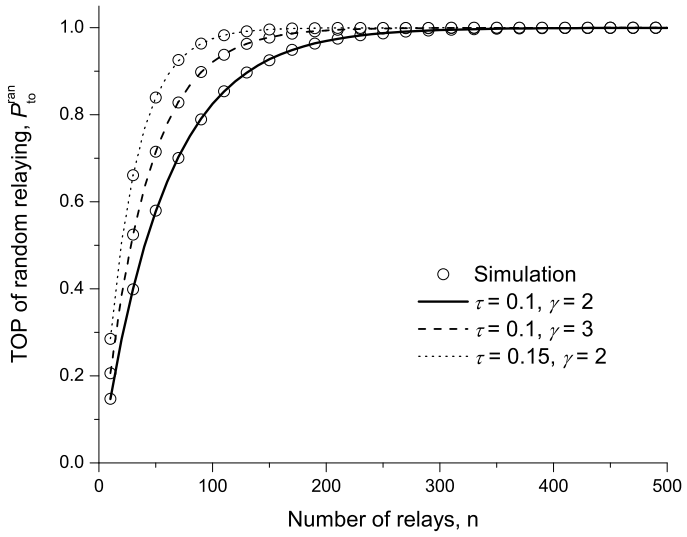
Proof 8 *The proof follows the same idea in proving the ETC of the random relaying, so we omit it here.*

3.4 Numerical Results and Discussions

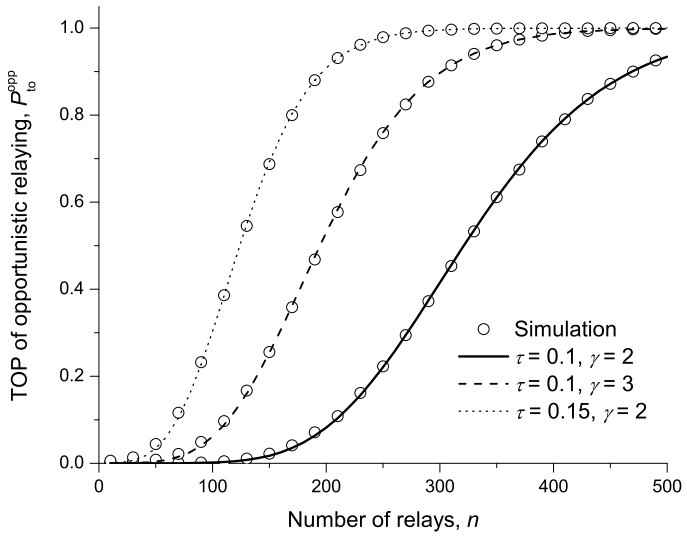
In this section, we first verify our theoretical model for TOP and SOP through extensive simulations. We then explore the impact of network parameters on the TOP and SOP performances of both relaying scheme. Finally, we examine explore how the number of relays n, the SIR thresholds γ and γ_e, the security constraint ε_s and the reliability constraint ε_t affect the ETC of both relaying schemes.

3.4.1 Model Validation

A simulator was developed in C++ to simulate the message transmission from the source S to the destination D based on the relaying and cooperative jamming schemes introduced in Section 3.1, which is now available at [60]. The total number of end-to-end transmissions from S to D is fixed as 100000. The simulated TOP (SOP) is calculated as the ratio of the number of transmissions suffering from transmission outage (secrecy outage) to the total number of transmissions 100000. To verify the validity of the expressions for the TOP of both relaying schemes, we vary the number of relays n from 10 to 490 with an interval of 20 and consider three different settings in terms of the noise-generating threshold τ and the minimum required SIR γ, i.e., ($\tau = 0.1$, $\gamma = 2$), ($\tau = 0.1$, $\gamma = 3$) and ($\tau = 0.15$, $\gamma = 2$). For the validation of the SOP, we set the minimum required SIR as $\gamma_e = 0.5$ and vary n from 20 to 800 with an interval of 20 and also consider three different network scenarios of ($m = 100, \tau = 0.05$), ($m = 100, \tau = 0.1$) and ($m = 500, \tau = 0.05$), which correspond to sparse eavesdroppers with



(a) TOP for random relaying P_{to}^{ran} vs. number of relays n.



(b) TOP for opportunistic relaying P_{to}^{opp} vs. number of relays n.

Figure 3.2: TOP vs. the number of relays n for different settings of τ and γ.

low interference, sparse eavesdroppers with high interference, and dense eavesdroppers with low interference. The corresponding simulated results and theoretical results are summarized in Figure 3.2 and Figure 3.3. Notice that simulations with other settings can be easily performed by our simulator as well.

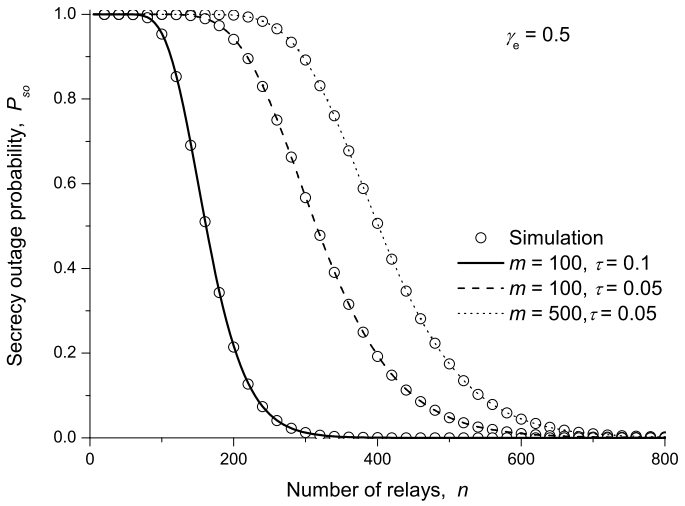


Figure 3.3: SOP P_{so} vs. number of relays n with different settings of m and τ for $\gamma_e = 0.5$.

Figure 3.2 and Figure 3.3 indicate clearly that the simulated results match nicely with the theoretical ones for both TOP and SOP, so our theoretical model can be used to effectively explore the TOP and SOP performances as well as the eavesdropper-tolerance performance of the concerned network with the opportunistic (random) relaying and cooperative jamming schemes.

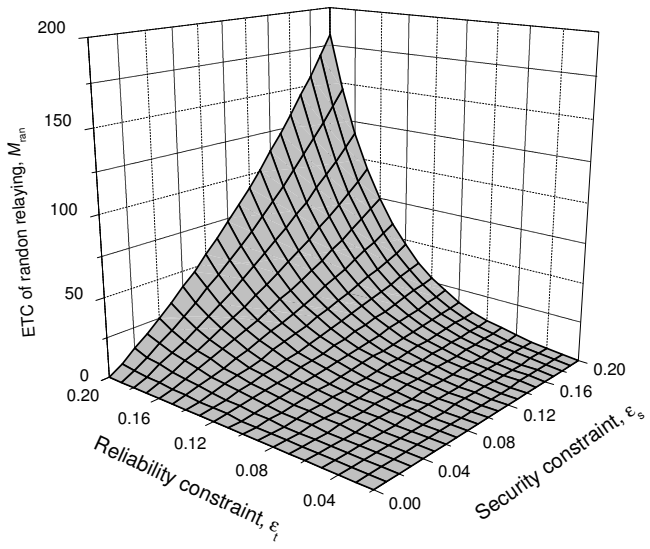
3.4.2 TOP and SOP Performance

We now explore the impact of the number of relays n, the noise-generating threshold τ and the minimum required SIR γ on the impact of TOP under both relaying schemes. We can see from Figure 3.2 that the TOP under both relaying schemes (i.e., P_{to}^{opp} and P_{to}^{ran}) increases with the number of relays n. This is because that adding more relays to the network has no impact on the link quality determined by the random relaying, but will generate more interference at the intended receiver. For the opportunistic relaying scheme, although adding more relays will improve the diversity gain offered by the relays and thus improve the link quality, but the inter-

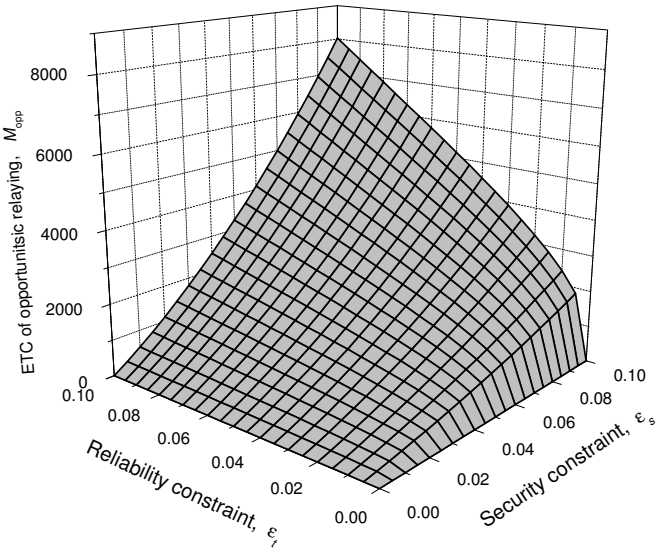
ference from the noise-generating relays dominates the trend of the received SIR at legitimate receivers. By comparing these three curves in Figure 3.2, it can also be observed that both P_{to}^{opp} and P_{to}^{ran} increases as τ increases. This is due to the reason that more interferences will be generated at the intended receiver for lager τ, and thus it is more difficult for the receivers to successfully recover the messages. We can also observe that for both relaying scheme, the TOP increases as the minimum required SIR γ increases. This is because that a larger γ means a poorer decoding ability for the intended receivers, thus resulting a larger TOP. Finally, comparing the results in Figure 3.2a and Figure 3.2b, we can see that the opportunistic relaying achieves a much smaller TOP than the random relaying, due to the improved link quality from S to D by selecting the best relay. We now explore the impact of the number of relays n, the noise-generating threshold τ and the number of eavesdroppers m on the impact of SOP. We can see from Figure 3.3 that P_{so} decreases as n increases. This is because more interferences can be generated at the eavesdroppers by distributing more relays for a specific τ. By comparing these three curves in Figure 3.3, it can also be observed that P_{so} increases as m increases while decreases as τ increases. This is intuitive since distributing more eavesdroppers by the adversary would post more potential threats to the end-to-end transmission and increasing τ would generate more interferences at the eavesdroppers, so it is more difficult for them to successfully decode the messages.

3.4.3 Eavesdropper-tolerance Performances

Based on the SOP and TOP models, we now explore the ETC performance of both relaying schemes for opportunistic relaying scheme. To illustrate the impact of the security constraint ε_s and the reliability constraint ε_t on the ETC of both relaying scheme, we show in Figure 3.4 the behavior of ETC vs. ε_t and ε_s for the network scenario of $n = 2000, \gamma_e = 0.5$. For the random relaying scheme, we set $\gamma = 1.0$, while for the opportunistic relaying scheme, we set $\gamma = 10$, which means that we consider



(a) ETC of random relaying $\mathcal{M}_{ran}$ vs. ε_t and ε_s for $\gamma = 1.0$.



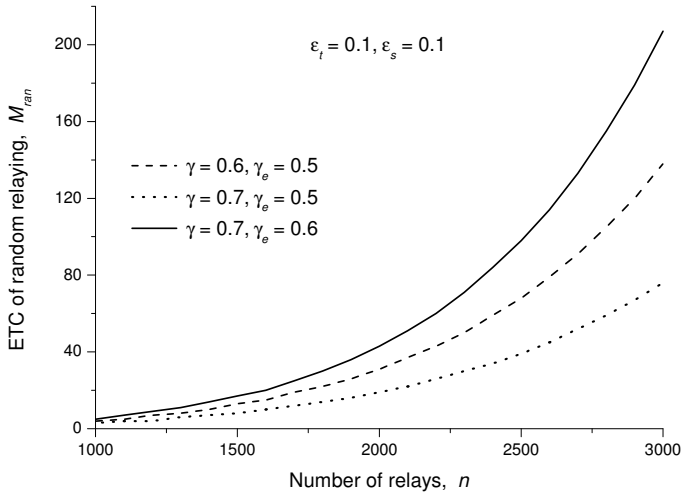
(b) ETC of opportunistic relaying $\mathcal{M}_{opp}$ vs. ε_t and ε_s for $\gamma = 10$.

Figure 3.4: ETC vs. reliability constraint ε_t and security constraint ε_s for $n = 2000$ and $\gamma_e = 0.5$.

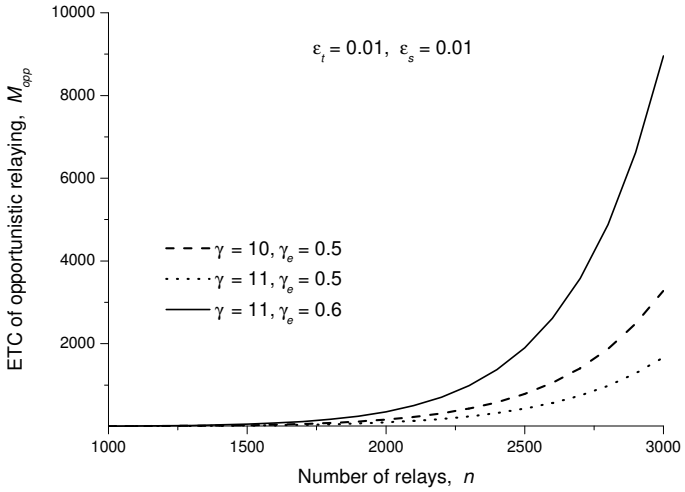
more powerful intended receivers in terms of the decoding ability for the random relaying scheme. Notice that both values of γ imply that the legitimate receivers has

a worse decoding ability than the eavesdroppers. We can observe from Figure 3.4 that the ETC of both relaying schemes increases as ε_t and ε_s increase. This reflects that the network can tolerate more eavesdroppers by relaxing either the security or reliability constraint. A careful observation of both figures in Figure 3.4 indicates a clear trade-off between the reliability and security in order to guarantee a certain level of ETC. For example, in Figure 3.4b, ε_t has to increase from 0.04 to 0.085 as ε_s decreases from 0.03 to 0.02 for achieving an eavesdropper-tolerance capacity of about1000. This suggests that either the security or reliability requirement has to sacrifice for the other one in order to achieve a certain ETC. Comparing the results in Figure 3.4a and Figure 3.4b, we can see that the opportunistic relaying scheme can achieve a much better ETC performance, which is orders of magnitude more than that ensured by the random relaying scheme, even we consider a much worse decoding ability for the receivers in the scenario with opportunistic relaying scheme. For example, the ETC of random relaying scheme is about 10, while the ETC of opportunistic relaying is about 8000 for $\varepsilon_t = 0.1$ and $\varepsilon_s = 0.1$.

To explore how the number of relays n, the minimum required SIR γ and γ_e affect the eavesdropper-tolerance capability, we show the behaviors of ETC vs. n for both relaying schemes in Figure 3.5. We set $\varepsilon_t = 0.1$ and $\varepsilon_s = 0.1$ for the random relaying scheme and consider three different settings of γ and γ_e, i.e., ($\gamma = 0.6$, $\gamma_e = 0.5$), ($\gamma = 0.7$, $\gamma_e = 0.5$) and ($\gamma = 0.7$, $\gamma_e = 0.6$). The corresponding results are summarized in Figure 3.5a. For the scenario of opportunistic relaying scheme, we set $\varepsilon_t = 0.01$ and $\varepsilon_s = 0.01$ and also consider three different settings of γ and γ_e, i.e., ($\gamma = 10$, $\gamma_e = 0.5$), ($\gamma = 11$, $\gamma_e = 0.5$) and ($\gamma = 11$, $\gamma_e = 0.5$). It can be observed from Figure 3.5 that both $\mathcal{M}_{ran}$ and $\mathcal{M}_{opp}$ increase as n increases. This is because that although the optimal noise-generating threshold threshold τ decreases as n increase for a specific reliability constraint ε_t, the corresponding expected number of noise-generating nodes increases, so more interferences can be generated to suppress the eavesdroppers while



(a) ETC of random relaying $\mathcal{M}_{ran}$ vs. n for $\varepsilon_t = 0.1$ and $\varepsilon_s = 0.1$.



(b) ETC of opportunistic relaying $\mathcal{M}_{opp}$ vs. n for $\varepsilon_t = 0.01$ and $\varepsilon_s = 0.01$.

Figure 3.5: ETC vs. number of relays n.

the desired reliability can still be ensured. By comparing the three curves in both figures, we can also observe that the ETC of both relaying schemes increases as γ_e increases, while decreases as γ increases. This is intuitive since decreasing the decoding ability (i.e., increasing γ_e) of the eavesdroppers would decrease the SOP, while decreasing the decoding ability (i.e., increasing γ) of legitimate receivers would

increase the TOP. It is interesting to notice that both $\mathcal{M}_{ran}$ and $\mathcal{M}_{opp}$ increases dramatically when n is above some threshold in Figure 3.5a and 3.5b. For example, for the case of $\gamma = 11$ and $\gamma_e = 0.6$ in Figure 3.5b, this threshold is about 2500. Thus, distributing more relays would be an effective approach to enhance the eavesdropper-tolerance capability of a network.

By comparing Figure 3.5a and Figure 3.5b, we can still see that the ETC of opportunistic relaying is much larger than that of the random relaying scheme, even we consider more stringent security and reliability constraints and much worse decoding ability for the opportunistic relaying scheme. For example, when the network has $n = 3000$ relays, for the case of ($\gamma = 0.7$, $\gamma_e = 0.6$), the network can tolerate about 200 eavesdroppers (in Figure 3.5a) for the random relaying scheme, which is much less than about 9000 eavesdroppers in the case of ($\gamma = 11$, $\gamma_e = 0.6$) in Figure 3.5b for the opportunistic relaying scheme. This again proves that the opportunistic relaying scheme significantly outperforms the random relaying schemes in terms of the ETC performance.

3.5 Summary

This chapter considered the secure and reliable transmission from the source to the destination via cooperative jamming in two-hop relay wireless networks with multiple passive and independently-operating eavesdroppers of unknown location and channel information. Instead of scaling law results for infinite networks and bounds for finite networks, we determined the exact eavesdropper-tolerance capability to ensure the desired security and reliability based on the metrics of secrecy outage probability and transmission outage probability. We consider two relaying schemes, i.e., the random relaying and opportunistic relaying. For both schemes, the results in this paper indicate that the eavesdropper-tolerance capability of the network can be increased if we distribute more relays or relax either the requirement of reliability

or the requirement of security. More importantly, we observe that the opportunistic relaying scheme can achieve a much better ETC performance, which is usually orders of magnitude more than that ensured by the random relaying scheme.

CHAPTER IV

Physical Layer Security Performance Study of Small-Scale Wireless Networks with Colluding Eavesdroppers

This chapter focuses on the PHY security performance study of small-scale wireless networks with colluding eavesdroppers, for which we investigate the SOP performance of a two-hop relay wireless networks under eavesdropper collusion. We consider two eavesdropper scenarios to depict the behavior of eavesdroppers, i.e., non-colluding scenario where eavesdroppers do not collude and operate independently and M-colluding scenario where M eavesdroppers can collude to exchange and combine the received signals so as to improve the successful decoding probability. We first derive the analytical expression for the SOP under the non-colluding scenario, we then derive the SOP under the M-colluding scenario by applying the techniques of Laplace transform, keyhole contour integral and Cauchy Integral Theorem. Finally, simulation and numerical results are provided to demonstrate the validity of the theoretical analysis also to illustrate our theoretical findings.

4.1 System Model and Problem Formulation

4.1.1 Network Model

We consider a two-hop wireless network (depicted in Figure 4.1), consisting of a source node S, a destination node D, n legitimate relays $R_1, R_2, \cdots, R_n$ and m passive eavesdroppers $E_1, E_2, \cdots, E_m$ of unknown channel information. Each node employs a single antenna and operates in half-duplex mode. The direct link between S and D is assumed unavailable due to deep fading or limited transmit power. The n relays assist in forwarding the message from S to D while preventing the eavesdroppers from intercepting the message. We assume that time is slotted and all channels, suffering from Rayleigh fading, remain constant during one time slot and vary randomly and independently from slot to slot. The channel coefficient $h_{i,j}$ of link $i \to j$ is modeled as a complex zero-mean Gaussian random variable with unit variance and thus $|h_{i,j}|^2$ is exponentially distributed with unit mean. All channel coefficients ($S-R$, $R-D$, $R-R$, $S-E$, $R-E$) are assumed i.i.d.. The network is assumed interference-limited and thus the noise at each receiver is negligible.

To accomplish the secure two-hop transmission from S to D, we adopt the opportunistic relaying, cooperative jamming and transmission schemes as introduced in Chapter III. A relay R_b with the largest $min\{|h_{S,R_i}|^2, |h_{R_i,D}|^2\}$ announces itself as the message relay in a distributed manner before the transmission. We assume that only one $S-D$ transmission, including the relay selection, can be conducted in one time slot. In the first hop, S transmits its message to R_b, while relays with indices in $\mathcal{J}_1 = \left\{i \middle| i \neq b, |h_{R_i,R_b}|^2 < \tau\right\}$ serve as helper jammers to generate random Gaussian noise. Here, τ is the noise-generating threshold to mitigate interference at intended receivers. We assume a common transmit power P_t for all transmitters. Hence, the

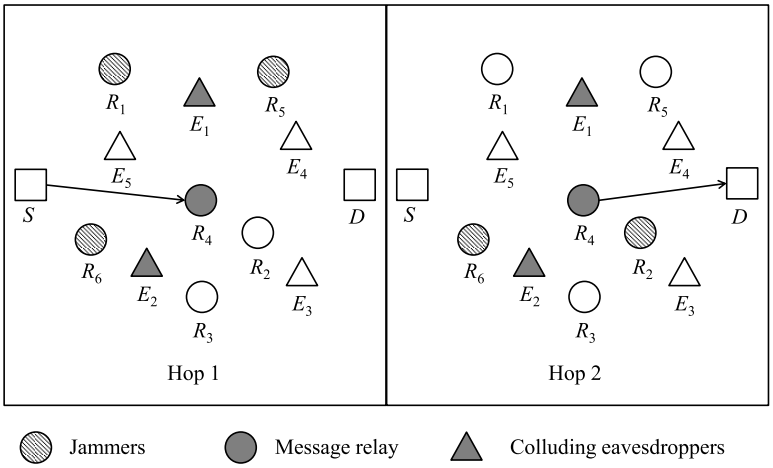


Figure 4.1: Network model: A source S is communicating with a destination D with the help of relays $R_1, R_2, \cdots, R_n, n = 6$. R_4 is selected as the message relay based on the opportunistic relaying scheme. In Hop 1, R_1, R_5 and R_6 are jammers that generate artificial noise, while R_2 and R_6 are jammers in Hop 2. $E_1, E_2, \cdots, E_m, m = 5$ are eavesdroppers that try to intercept the message, and E_1 and E_2 are colluding eavesdroppers.

received SIR at R_b and that at E_j can be given by

$$\mathrm{SIR}_{S,R_b} = \frac{|h_{S,R_b}|^2}{\sum_{i\in\mathcal{J}_1}|h_{R_i,R_b}|^2}, \ \mathrm{SIR}_{S,E_j} = \frac{|h_{S,E_j}|^2}{\sum_{i\in\mathcal{J}_1}|h_{R_i,E_j}|^2}. \tag{4.1}$$

If R_b is successful in decoding the message received from S, it re-encodes the message and then sends it to D in the second hop. Meanwhile, relays with indices in $\mathcal{J}_2 = \left\{i \middle| i \neq b, |h_{R_i,D}|^2 < \tau\right\}$ serve as helper jammers to generate artificial noise. If R_b fails to decode the message, the transmission will be suspended. We assume that R_b will send back an ACK message to inform S whether a decoding failure happens or not, based on which S will then decide whether to suspend the transmission or not. If a transmission suspension happens during one time slot, it will end at the end of that time slot, and retransmission of the suspended message will be conducted in the next time slot. The received SIR at D and E_j can be given by

$$\mathrm{SIR}_{R_b,D} = \frac{|h_{R_b,D}|^2}{\sum_{i\in\mathcal{J}_2}|h_{R_i,D}|^2}, \ \mathrm{SIR}_{R_b,E_j} = \frac{|h_{R_b,E_j}|^2}{\sum_{i\in\mathcal{J}_2}|h_{R_i,E_j}|^2}. \tag{4.2}$$

A legitimate receiver (eavesdropper) is said successful in decoding the received signal if its received SIR is above a minimum required SIR γ (γ_e).

4.1.2 Eavesdropper Scenarios

Regarding the eavesdropper behavior, we focus on the following two scenarios,

1. **Non-Colluding case**: each eavesdropper works independently and decodes the message from the source solely based on its available observations, i.e., the first-hop observation if the transmission is suspended in the second hop or the combined observations in both hops, otherwise.

2. **M-Colluding case**: any M eavesdroppers (say, $E_1, E_2, \cdots, E_M, 1 \leq M \leq m$, $M = 2$ as illustrated in Figure 4.1) can combine their available observations to decode the message from the source.

Here, M is referred to as the *collusion intensity* to quantify the level of eavesdropper collusion. As assumed in [37–48, 61], these colluding eavesdroppers can be treated as a super eavesdropper with M antennas, whose SIR is given by the aggregate SIR of all antennas.

4.1.3 Problem Formulation

We adopt the SOP metric as introduced in Chapter III to characterize the security performance of the concerned network under eavesdropper collusion, which is defined as the probability that the received SIR of at least one of the eavesdroppers is above γ_e. Therefore, by defining A as the event that the transmission is suspended in the second hop, the SOP P_{so}^{nc} for the non-colluding case can be formulated as

$$P_{so}^{nc} = \mathbb{P}\left(\bigcup_{j=1}^{m}\{\mathrm{SIR}_{S,E_j} \geq \gamma_e\}, A\right) + \mathbb{P}\left(\bigcup_{j=1}^{m}\{\mathrm{SIR}_{S,E_j} + \mathrm{SIR}_{R_b,E_j} \geq \gamma_e\}, \bar{A}\right), \quad (4.3)$$

where $\bar{A}$ is the complement of event A. Similarly, the SOP P_{so}^{c} for the M-colluding case can be formulated as

$$P_{so}^{c} = \mathbb{P}\left(\left\{\mathrm{SIR}_{agg}^{A} \geq \gamma_e \text{ or } \bigcup_{j=M+1}^{m} \{\mathrm{SIR}_{S,E_j} \geq \gamma_e\}\right\}, A\right) \tag{4.4}$$

$$+\mathbb{P}\left(\left\{\mathrm{SIR}_{agg}^{\bar{A}} \geq \gamma_e \text{ or } \bigcup_{j=M+1}^{m} \{\mathrm{SIR}_{S,E_j} + \mathrm{SIR}_{R_b,E_j} \geq \gamma_e\}\right\}, \bar{A}\right), \tag{4.5}$$

where

$$\mathrm{SIR}_{agg}^{A} = \sum_{j=1}^{M} \mathrm{SIR}_{S,E_j}$$

denotes the aggregate SIR of M colluding eavesdroppers under event A and

$$\mathrm{SIR}_{agg}^{\bar{A}} = \sum_{j=1}^{M} \mathrm{SIR}_{S,E_j} + \mathrm{SIR}_{R_b,E_j}$$

denotes that under event $\bar{A}$.

4.2 Secrecy Outage performance under Non-Colluding Case

In this section, we derive the SOP of the non-colluding eavesdropper case, for which we will first establish the following lemma regarding the probability that the transmission is suspended in the second hop, conditioned on the number of jammers in the first hop.

Lemma 7 *Define the number of jammers in Hop h $(h = 1, 2)$ by J_h and the event $J_h = s$ by J_h^s. For a two-hop $S - D$ transmission with the opportunistic relaying and cooperative jamming schemes, the probability $p_{A|J_1^s}$ that the transmission is suspended in the second hop under the condition J_1^s can be determined as*

$$p_{A|J_1^s} = \sum_{k=0}^{n} \binom{n}{k} \frac{(-1)^k}{2k-1} \left[k\left(\frac{1-e^{-(1+\gamma)\tau}}{(1-e^{-\tau})(1+\gamma)}\right)^s + (k-1)\left(\frac{1-e^{-(2k\gamma+1)\tau}}{(1-e^{-\tau})(2k\gamma+1)}\right)^s\right],$$

where n is the number of relays, τ is the noise-generating threshold in cooperative jamming and γ is the minimum required SIR for legitimate receivers to correctly decode the source message.

Proof 9 *Please refer to Appendix B.1.*

Based on Lemma 7, the SOP of the non-colluding case can be obtained by applying the law of total probability, which is given by the following theorem.

Theorem IV.1 *Consider a two-hop wireless network as shown in Figure 4.1. For the $S-D$ transmission under the opportunistic relaying, cooperative jamming and non-colluding eavesdropper case, the corresponding SOP P_{so}^{nc} can be formulated as*

$$P_{so}^{nc} = 1 - \sum_{s=0}^{n-1}\sum_{t=0}^{n-1}\binom{n-1}{s}\binom{n-1}{t}(1-e^{-\tau})^{s+t}e^{-(2n-2-s-t)\tau}\left[(1-p_{A|J_1^s})p_2^m + p_{A|J_1^s}p_1^m\right],$$

where n is the number of relays, τ is the noise-generating threshold in cooperative jamming, $p_1 = 1-\left(\frac{1}{1+\gamma_e}\right)^s$, $p_2 = \int_0^{\gamma_e}\left[1-\frac{1}{(1+\gamma_e-x)^t}\right]\frac{s}{(1+x)^{s+1}}\mathrm{d}x$ and $p_{A|J_1^s}$ is given in Lemma 7.

Proof 10 *We start the proof with the first term in (4.3). By the law of total probability, we have*

$$\begin{aligned}
&\mathbb{P}\left(\bigcup_{j=1}^{m}\{\mathrm{SIR}_{S,E_j}\geq\gamma_e\}, A\right) \qquad (4.6)\\
&=\sum_{s=0}^{n-1}\mathbb{P}\left(\bigcup_{j=1}^{m}\{\mathrm{SIR}_{S,E_j}\geq\gamma_e\}, A\Big|J_1^s\right)\mathbb{P}(J_1^s)\\
&=\sum_{s=0}^{n-1}\mathbb{P}\left(\bigcup_{j=1}^{m}\{\mathrm{SIR}_{S,E_j}\geq\gamma_e\}\Big|J_1^s\right)p_{A|J_1^s}\mathbb{P}(J_1^s)\\
&=\sum_{s=0}^{n-1}\left[1-\mathbb{P}\left(\bigcap_{j=1}^{m}\{\mathrm{SIR}_{S,E_j}<\gamma_e\}\Big|J_1^s\right)\right]p_{A|J_1^s}\mathbb{P}(J_1^s)\\
&=\sum_{s=0}^{n-1}\left[1-\mathbb{P}\left(\mathrm{SIR}_{S,E_j}<\gamma_e|J_1^s\right)^m\right]p_{A|J_1^s}\mathbb{P}(J_1^s).
\end{aligned}$$

Next, we consider the cumulative distribution function (cdf) of SIR_{S,E_j} *under the condition* J_1^s*, which can be given by*

$$\begin{aligned} F_{\gamma_{S,E_j}}(x|J_1^s) &= \mathbb{P}\left(\mathrm{SIR}_{S,E_j} < x \middle| J_1^s\right) \\ &= \mathbb{P}\left(|h_{S,E_j}|^2 < x \sum_{i\in\mathcal{J}_1} |h_{R_i,E_j}|^2 \middle| J_1^s\right) \\ &= 1 - \mathbb{E}_{\{|h_{R_i,E_j}|^2, i\in\mathcal{J}_1\}}\left[e^{-x\sum_{i\in\mathcal{J}_1}|h_{R_i,E_j}|^2} \middle| J_1^s\right] \\ &= 1 - \prod_{i\in\mathcal{J}_1} \mathbb{E}_{|h_{R_i,E_j}|^2}\left[e^{-x|h_{R_i,E_j}|^2}\right] \\ &= 1 - \left(\frac{1}{1+x}\right)^s. \end{aligned}$$

From the above cdf, it is easy to see that

$$\mathbb{P}\left(\mathrm{SIR}_{S,E_j} < \gamma_e | J_1^s\right) = 1 - \left(\frac{1}{1+\gamma_e}\right)^s = p_1. \tag{4.7}$$

As J_1 *is a binomial random variable, it follows that*

$$\mathbb{P}(J_1^s) = \binom{n-1}{s}(1-e^{-\tau})^s e^{-(n-1-s)\tau}. \tag{4.8}$$

Hence, substituting (4.7) and (4.8) into (4.6) yields

$$\mathbb{P}\left(\bigcup_{j=1}^{m}\{\mathrm{SIR}_{S,E_j} \geq \gamma_e\}, A\right) = \sum_{s=0}^{n-1}\binom{n-1}{s}(1-e^{-\tau})^s e^{-(n-1-s)\tau}(1-p_1^m)p_{A|J_1^s}. \tag{4.9}$$

We now consider the second term in (4.3). Likewise, taking the expectation of (4.3) in terms of J_1 *and* J_2 *yields*

$$\begin{aligned} &\mathbb{P}\left(\bigcup_{j=1}^{m}\{\mathrm{SIR}_{S,E_j} + \mathrm{SIR}_{R_b,E_j} \geq \gamma_e\}, \bar{A}\right) \qquad (4.10) \\ &= \sum_{s=0}^{n-1}\sum_{t=0}^{n-1}\left[1 - \mathbb{P}\left(\mathrm{SIR}_{S,E_j} + \mathrm{SIR}_{R_b,E_j} < \gamma_e | J_1^s, J_2^t\right)^m\right]\mathbb{P}(\bar{A}|J_1^s)\mathbb{P}(J_1^s)\mathbb{P}(J_2^t). \end{aligned}$$

It is straightforward to see that $\mathbb{P}(\bar{A}|J_1^s) = 1-p_{A|J_1^s}$, *and* $\mathbb{P}(J_2^t) = \binom{n-1}{t}(1-e^{-\tau})^t e^{-(n-1-t)\tau}$. *Similar to (4.7), the cdf of* SIR_{R_b,E_j} *under the condition* J_2^t *can be given by* $F_{\mathrm{SIR}_{R_b,E_j}}(x|J_2^t) = 1-(\frac{1}{1+x})^t$. *From (4.7), the pdf of* SIR_{S,E_j} *under the condition* J_1^s *is* $f_{\mathrm{SIR}_{S,E_j}}(x|J_1^s) = \frac{s}{(1+x)^{s+1}}$. *Hence,*

$$\begin{aligned} &P\left(\mathrm{SIR}_{S,E_j} + \mathrm{SIR}_{R_b,E_j} < \gamma_e | J_1^s, J_2^t\right) \\ &= \int_0^{\gamma_e} \left[1 - \frac{1}{(1+\gamma_e - x)^t}\right] \frac{s}{(1+x)^{s+1}} \mathrm{d}x = p_2. \end{aligned} \tag{4.11}$$

Substituting (4.8), (4.11), $\mathbb{P}(\bar{A}|J_1^s)$ *and* $\mathbb{P}(J_2^t)$ *into (4.10) yields*

$$\begin{aligned} &P\left(\bigcup_{j=1}^{m}\{\mathrm{SIR}_{S,E_j} + \mathrm{SIR}_{R_b,E_j} \geq \gamma_e\}, \bar{A}\right) \\ &= \sum_{s=0}^{n-1}\sum_{t=0}^{n-1} \binom{n-1}{s}\binom{n-1}{t}(1-e^{-\tau})^{s+t} e^{-(2n-2-s-t)\tau}(1-p_2^m)(1-p_{A|J_1^s}). \end{aligned} \tag{4.12}$$

Finally, the theorem follows after summing (4.9) and (4.12).

4.3 Secrecy Outage Performance under M-Colluding Case

In this section, the SOP of the M-colluding case is investigated, for which we will first derive the cdf of the aggregate SIR SIR_{agg}^{A} and $\mathrm{SIR}_{agg}^{\bar{A}}$ of any M colluding eavesdroppers, based on which we then determine the SOP.

4.3.1 Aggregate SIR Analysis

Notice that the aggregate SIR SIR_{agg}^{A} and $\mathrm{SIR}_{agg}^{\bar{A}}$ are the sums of multiple i.i.d. random variables. The derivation of their cdf usually involves a multi-fold convolution, which is highly cumbersome in general. To work around this problem, we first take the Laplace transforms of their pdf and then compute the related inverse Laplace transform by applying the keyhole contour integral and Cauchy Integral Theorem.

Finally, the cdf can be obtained from the corresponding pdf. The related lemma and proof are summarized as follows.

Lemma 8 *Define the cdf of* SIR_{agg}^{A} *under event* A *by* $F_M(x)$ *and that of* $\mathrm{SIR}_{agg}^{\bar{A}}$ *under event* $\bar{A}$ *by* $F_{2M}(x)$*. For a two-hop* $S-D$ *transmission under the opportunistic relaying, cooperative jamming and* M*-colluding eavesdropper case,* $F_M(x)$ *under the conditions* J_1^s *and* J_2^t *can be given by*

$$F_M(x) = s^M \sum_{k=0}^{\lfloor \frac{M-1}{2} \rfloor} \binom{M}{2k+1} (-\pi^2)^k \times \int_0^\infty \frac{1}{u}(1-e^{-xu}) e^{-Mu} \mathrm{EI}_s(u)^{M-2k-1} \left(\frac{u^s}{s!}\right)^{2k+1} \mathrm{d}u \tag{4.13}$$

and $F_{2M}(x)$ *under the conditions* J_1^s *and* J_2^t *can be given by*

$$F_{2M}(x) = (st)^M \sum_{k=0}^{\lfloor \frac{M-1}{2} \rfloor} \binom{M}{2k+1} (-\pi^2)^k \times \int_0^\infty \frac{1}{u}(1-e^{-xu}) e^{-2Mu} \left[\mathrm{EI}_s(u)\mathrm{EI}_t(u) - \pi^2 \frac{u^{s+t}}{s!t!}\right]^{M-2k-1} \times \left[\mathrm{EI}_s(u)\frac{u^t}{t!} + \mathrm{EI}_t(u)\frac{u^s}{s!}\right]^{2k+1} \mathrm{d}u \tag{4.14}$$

where

$$\mathrm{EI}_s(u) = \frac{u^s}{s!}\left(\sum_{k=1}^{s}\frac{1}{k} - c_E - \ln u\right) - \sum_{k=0,k\neq s}^{\infty} \frac{u^k}{(k-s)k!} \tag{4.15}$$

and $c_E = 0.5772156649...$ *is the Euler's constant.*

Proof 11 *Define* $f_M(x)$ *the pdf of* SIR_{agg}^{A} *and* $\mathcal{L}_{f_M}(z)$ *its Laplace transform. Based on the pdf* $f_{\mathrm{SIR}_{S,E_j}}(x) = \frac{s}{(1+x)^{s+1}}$ *of* SIR_{S,E_j} *under the condition* J_1^s*,* $\mathcal{L}_{f_M}(z)$ *can be determined as* $\mathcal{L}_{f_M}(z) = (se^z E_{s+1}(z))^M$ *by the convolution property of Laplace transform, where* $E_{s+1}(z) = \int_1^\infty \frac{e^{-zv}}{v^{s+1}}\mathrm{d}v$ *is the generalized exponential integral.*

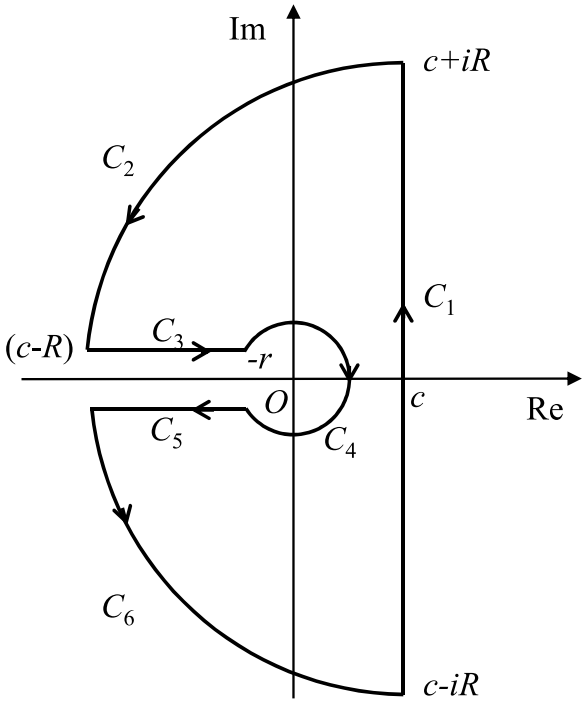


Figure 4.2: Illustration of the keyhole contour, where C_1 is a vertical line from $c-iR$ to $c+iR$, C_2 and C_6 forms a large (almost) semi-circle centered at $s=c$ with radius R, C_3 is a line from $c-R$ to $-r$, C_4 is a small (almost) circle centered at the origin with radius r, C_5 is a line from $-r$ to $c-R$.

Next, $f_M(x)$ can be obtained by taking the inverse Laplace transform of $\mathcal{L}_{f_M}(z)$, that is, $f_M(x) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} e^{zx}\mathcal{L}_{f_M}(z)\mathrm{d}z$, where $c>0$ is an arbitrary constant greater than the real part of all singularities of $\mathcal{L}_{f_M}(z)$. Since $E_{s+1}(z)$ is analytical in the complex plane except its branch cut along the negative real axis and branch point at the origin, the above integral can be evaluated as a part of the integral along a keyhole contour Ω [62], as illustrated in Figure 4.2. As $\mathcal{L}_{f_M}(z)$ is analytical in Ω, by the Cauchy Integral Theorem, we have $\int_\Omega e^{zx}\mathcal{L}_{f_M}(z)\mathrm{d}z = 0$. Hence,

$$
\begin{aligned}
f_M(x) &= \frac{1}{2\pi i}\lim_{R\to\infty}\int_{C_1} e^{zx}\mathcal{L}_{f_M}(z)\mathrm{d}z \qquad (4.16)\\
&= -\frac{1}{2\pi i}\lim_{R\to\infty,r\to 0}\int_{C_2}+\int_{C_3}+\int_{C_4}+\int_{C_5}+\int_{C_6} e^{zx}\mathcal{L}_{f_M}(z)\mathrm{d}z\\
&= -\frac{1}{2\pi i}\lim_{R\to\infty,r\to 0}\int_{C_3}+\int_{C_5} e^{zx}\mathcal{L}_{f_M}(z)\mathrm{d}z.
\end{aligned}
$$

To see this, we need to prove that the integrals along C_2, C_4 and C_6 vanish in the limit. First, letting $z = c + Re^{i\theta}$, $\theta \in [\pi/2, \pi]$ for any point z on C_2 yields

$$\begin{aligned}
\lim_{R\to\infty}\left|\int_{C_2} e^{zx}\mathcal{L}_{f_M}(z)\mathrm{d}z\right| &= \lim_{R\to\infty}\left|\int_{\frac{\pi}{2}}^{\pi} e^{x(c+Re^{i\theta})}\mathcal{L}_{f_M}(c+Re^{i\theta})iRe^{i\theta}\mathrm{d}\theta\right| \\
&\leq \lim_{R\to\infty}\int_{\frac{\pi}{2}}^{\pi}\left|e^{x(c+Re^{i\theta})}\right|\left|\mathcal{L}_{f_M}(c+Re^{i\theta})\right|\left|iRe^{i\theta}\right|\mathrm{d}\theta \\
&\leq \lim_{R\to\infty}\max_{\theta\in[\pi/2,\pi]}\left|\mathcal{L}_{f_M}(c+Re^{i\theta})\right| Re^{xc}\int_{\frac{\pi}{2}}^{\pi} e^{xR\cos\theta}\mathrm{d}\theta \\
&= \lim_{R\to\infty}\max_{\theta\in[\pi/2,\pi]}\left|\mathcal{L}_{f_M}(c+Re^{i\theta})\right| Re^{xc}\int_{0}^{\frac{\pi}{2}} e^{-xR\sin\alpha}\mathrm{d}\alpha.
\end{aligned}$$

Since $\sin\alpha \geq \frac{2\alpha}{\pi}$ *for any* $\alpha \in [0, \frac{\pi}{2}]$*, then we have*

$$\int_0^{\frac{\pi}{2}} e^{-xR\sin\alpha}\mathrm{d}\alpha \leq \int_0^{\frac{\pi}{2}} e^{-2xR\alpha/\pi}\mathrm{d}\alpha = \frac{\pi}{2xR}(1-e^{-xR}) \leq \frac{\pi}{2xR},$$

and thus

$$\lim_{R\to\infty}\left|\int_{C_2} e^{zx}\mathcal{L}_{f_M}(z)\mathrm{d}z\right| \leq \lim_{R\to\infty}\frac{\pi e^{xc}}{2x}\max_{\theta\in[\pi/2,\pi]}\left|\mathcal{L}_{f_M}(c+Re^{i\theta})\right|.$$

From Equation (5.1.51) in [63], we know

$$e^z E_{s+1}(z) \sim \frac{1}{z} - \frac{s+1}{z^2} + \frac{(s+1)(s+2)}{z^3} + \cdots,$$

hence

$$|e^{c+Re^{i\theta}}E_{s+1}(c+Re^{i\theta})| = O(1/R)$$

and then

$$\max_{\theta\in[\pi/2,\pi]}\left|\mathcal{L}_{f_M}(c+Re^{i\theta})\right| = O(1/R^M),$$

as $R\to\infty$*. Therefore,* $\lim_{R\to\infty}\left|\int_{C_2} e^{zx}\mathcal{L}_{f_M}(z)\mathrm{d}z\right| = 0$*. Likewise, it can be easily seen that the integral along* C_6 *vanishes as* R *tends to infinity and that along* C_4 *vanishes*

as r tends to zero.

Now, we proceed to evaluate the integrals along C_3 and C_5. By letting $z = ue^{i\pi}$ for the integral along C_3 and $z = ue^{-i\pi}$ for that along C_5, we have

$$\begin{aligned} f_M(x) &= -\frac{1}{2\pi i} \lim_{R\to\infty, r\to 0} \int_{C_3} + \int_{C_5} e^{zx} \mathcal{L}_{f_M}(z) \mathrm{d}z \\ &= -\frac{1}{2\pi i} \lim_{R\to\infty, r\to 0} \int_{c-R}^{-r} + \int_{-r}^{c-R} e^{zx} \mathcal{L}_{f_M}(z) \mathrm{d}z \\ &= \frac{1}{2\pi i} \int_0^\infty e^{-xu} \left(\mathcal{L}_{f_M}(ue^{-i\pi}) - \mathcal{L}_{f_M}(ue^{i\pi}) \right) \mathrm{d}u \\ &= \frac{s^M}{2\pi i} \int_0^\infty e^{-(x+M)u} \left[E_{s+1}(ue^{-i\pi})^M - E_{s+1}(ue^{i\pi})^M \right] \mathrm{d}u. \end{aligned} \tag{4.17}$$

From Equation (5.1.12) in [63], we have $E_{s+1}(ue^{\pm i\pi}) = \mathrm{EI}_s(u) \mp i\pi \frac{u^s}{s!}$, where $\mathrm{EI}_s(u) = \frac{u^s}{s!} \left(\sum_{k=1}^s \frac{1}{k} - c_E - \ln u \right) - \sum_{k=0, k\neq s}^\infty \frac{u^k}{(k-s)k!}$ and $c_E = 0.5772156649...$ is the Euler's constant. Hence,

$$\begin{aligned} & E_{s+1}(ue^{-i\pi})^M - E_{s+1}(ue^{i\pi})^M \\ &= \left(\mathrm{EI}_s(u) + i\pi \frac{u^s}{s!} \right)^M - \left(\mathrm{EI}_s(u) - i\pi \frac{u^s}{s!} \right)^M \\ &= 2\pi i \sum_{k=0}^{\lfloor \frac{M-1}{2} \rfloor} \binom{M}{2k+1} (-\pi^2)^k \mathrm{EI}_s(u)^{M-2k-1} \left(\frac{u^s}{s!} \right)^{2k+1}. \end{aligned} \tag{4.18}$$

Substituting (4.18) into (4.17) yields

$$f_M(x) = \int_0^\infty e^{-(x+M)u} \kappa(M, s, u) \mathrm{d}u,$$

where

$$\kappa(M, s, u) = s^M \sum_{k=0}^{\lfloor \frac{M-1}{2} \rfloor} \binom{M}{2k+1} (-\pi^2)^k \mathrm{EI}_s(u)^{M-2k-1} \left(\frac{u^s}{s!} \right)^{2k+1}.$$

The cdf $F_M(x)$ *of* SIR_{agg}^{A} *can be determined via the integration of* $f_M(x)$ *as*

$$F_M(x) = \int_0^\infty \frac{1}{u}(1 - e^{-xu})e^{-Mu}\kappa(M, s, u)\mathrm{d}u.$$

Finally, taking the integral for each summand involving u *in* $\kappa(M, s, u)$ *first and then summing the integrals yields (4.13).*

We now consider the cdf $F_{2M}(x)$ *of* $\mathrm{SIR}_{agg}^{\bar{A}}$*. Similarly, we define* $f_{2M}(x)$ *the pdf of* $\mathrm{SIR}_{agg}^{\bar{A}}$ *and* $\mathcal{L}_{f_{2M}}(z)$ *its Laplace transform. Again, by the convolution property of Laplace transform, we have* $\mathcal{L}_{f_{2M}}(z) = (s \cdot t \cdot e^{2z} E_{s+1}(z)E_{t+1}(z))^M$ *under the conditions* J_1^s *and* J_2^t*. Taking the inverse Laplace transform of* $\mathcal{L}_{f_{2M}}(s)$ *along again the keyhole contour in Figure 4.2 yields*

$$\begin{aligned} & f_{2M}(x) \qquad (4.19) \\ &= \frac{(st)^M}{2\pi i}\int_0^\infty e^{-(x+2M)u}\left[(E_{s+1}(ue^{-i\pi})E_{t+1}(ue^{-i\pi}))^M - (E_{s+1}(ue^{i\pi})E_{t+1}(ue^{i\pi}))^M\right]\mathrm{d}u \\ &= \int_0^\infty e^{-(x+2M)u}\phi(M, s, t, u)\mathrm{d}u, \end{aligned}$$

where

$$\begin{aligned} \phi(M, s, t, u) = (st)^M \sum_{k=0}^{\lfloor\frac{M-1}{2}\rfloor} \binom{M}{2k+1}(-\pi^2)^k \qquad (4.20) \\ \times \left[\mathrm{EI}_s(u)\frac{u^t}{t!} + \mathrm{EI}_t(u)\frac{u^s}{s!}\right]^{2k+1}\left[\mathrm{EI}_s(u)\mathrm{EI}_t(u) - \pi^2\frac{u^{s+t}}{s!t!}\right]^{M-2k-1}. \end{aligned}$$

The cdf $F_{2M}(x)$ *of* $\mathrm{SIR}_{agg}^{\bar{A}}$ *is determined as*

$$F_{2M}(x) = \int_0^\infty \frac{1}{u}(1 - e^{-xu})e^{-2Mu}\phi(M, s, t, u)\mathrm{d}u. \qquad (4.21)$$

Likewise, taking the integral for each summand in $\phi(M, s, t, u)$ *first and then summing the integrals yields (4.14).*

4.3.2 SOP Modeling

Based on Lemma 8, the SOP of M-colluding case is given by the following theorem.

Theorem IV.2 *Consider a two-hop wireless network as shown in Figure 4.1. For the $S-D$ transmission under the opportunistic relaying, cooperative jamming and M-colluding eavesdropper case as described in Section 4.1, the corresponding SOP P_{so}^{c} can be formulated as*

$$P_{so}^{c} = 1 - \sum_{s=0}^{n-1}\sum_{t=0}^{n-1}\binom{n-1}{s}\binom{n-1}{t}(1-e^{-\tau})^{s+t}e^{-(2n-2-s-t)\tau} \tag{4.22}$$

$$\times\Big[(1-p_{A|J_1^s})p_2^{m-M}F_{2M}(\gamma_e) + p_{A|J_1^s}p_1^{m-M}F_M(\gamma_e)\Big], \tag{4.23}$$

where m is the number of eavesdroppers, M denotes the collusion intensity, n is the number of relays, τ is the noise-generating threshold in cooperative jamming, γ_e is the minimum required SIR for eavesdroppers to correctly decode the source message, $p_1 = 1-\left(\frac{1}{1+\gamma_e}\right)^s$, $p_2 = \int_0^{\gamma_e}\left[1-\frac{1}{(1+\gamma_e-x)^t}\right]\frac{s}{(1+x)^{s+1}}\mathrm{d}x$, $p_{A|J_1^s}$ is given in Lemma 7, and $F_M(\gamma_e)$ and $F_{2M}(\gamma_e)$ can be directly obtained from Lemma 8.

Proof 12 *Similar to the proof of Theorem IV.1, the first term in (4.4) can be determined by taking its expectation in terms of J_1 as*

$$\mathbb{P}\left(\left\{\mathrm{SIR}_{agg}^{A} \geq \gamma_e \text{ or } \bigcup_{j=M+1}^{m}\{\mathrm{SIR}_{S,E_j} \geq \gamma_e\}\right\}, A\right) \tag{4.24}$$

$$= \mathbb{E}_{J_1}\left[\mathbb{P}\left(\left\{\mathrm{SIR}_{agg}^{A} \geq \gamma_e \text{ or } \bigcup_{j=M+1}^{m}\{\mathrm{SIR}_{S,E_j} \geq \gamma_e\}\right\}, A\Big| J_1^s\right)\right]$$

$$= \sum_{s=0}^{n-1}\left[1-\mathbb{P}\left(\mathrm{SIR}_{agg}^{A} < \gamma_e\Big| J_1^s\right)\mathbb{P}\left(\mathrm{SIR}_{S,E_j} < \gamma_e\Big| J_1^s\right)^{m-M}\right]p_{A|J_1^s}\mathbb{P}(J_1^s)$$

$$= \sum_{s=0}^{n-1}\binom{n-1}{s}(1-e^{-\tau})^s e^{-(n-1-s)\tau}\Big[1-p_1^{m-M}F_M(\gamma_e)\Big]p_{A|J_1^s}.$$

The second term in (4.4) can be determined by taking its expectation in terms of J_1

and J_2 *as*

$$\mathbb{P}\left(\left\{\mathrm{SIR}_{agg}^{\bar{A}} \geq \gamma_e \text{ or } \bigcup_{j=M+1}^{m}\{\mathrm{SIR}_{S,E_j} + \mathrm{SIR}_{R_b,E_j} \geq \gamma_e\}\right\}, \bar{A}\right) \tag{4.25}$$

$$= \sum_{s=0}^{n-1}\sum_{t=0}^{n-1}\mathbb{P}(\bar{A}|J_1^s)\mathbb{P}(J_1^s)\mathbb{P}(J_2^t)$$

$$\times\left[1-\mathbb{P}\left(\mathrm{SIR}_{agg}^{\bar{A}} < \gamma_e \middle| J_1^s, J_2^t\right)\mathbb{P}\left(\mathrm{SIR}_{S,E_j} + \mathrm{SIR}_{R_b,E_j} < \gamma_e | J_1^s, J_2^t\right)^{m-M}\right]$$

$$= \sum_{s=0}^{n-1}\sum_{t=0}^{n-1}\binom{n-1}{s}\binom{n-1}{t}(1-e^{-\tau})^{s+t}e^{-(2n-2-s-t)\tau}(1-p_{A|J_1^s})\left[1-p_2^{m-M}F_{2M}(\gamma_e)\right].$$

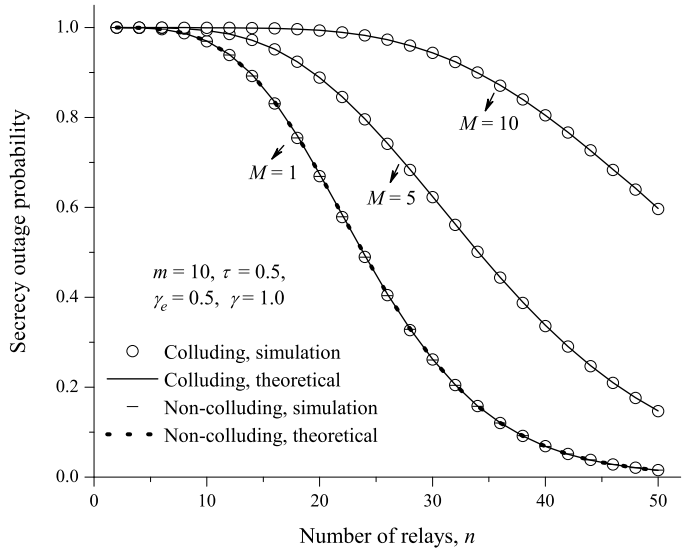
Finally, summing (4.24) and (4.25), the theorem then follows.

4.4 Numerical Results and Discussions

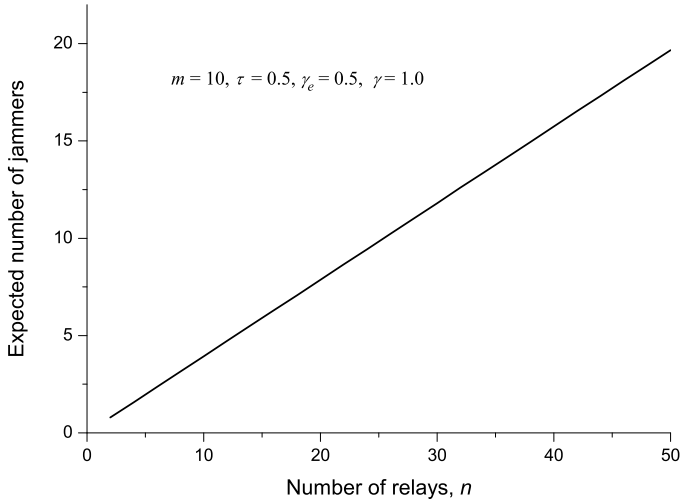
In this section, we first validate our theoretical analysis for SOP modeling through extensive simulations and then explore how the number of relays n, noise-generating threshold τ, SIR thresholds γ_e and γ, and the collusion intensity M affect the secrecy outage performance of the network.

4.4.1 Model Validation

A simulator was developed in C++ to simulate the $S-D$ transmission under the system model as described in Section 4.1, which is now available at [64]. The total number of $S-D$ transmissions is fixed as 100000 and the SOP is measured as the ratio of the number of transmissions suffering from secrecy outage to the total number of transmissions. To verify our theoretical analysis, we conduct extensive simulations for both the non-colluding case and the colluding case under various settings of n and M. The number of eavesdroppers is set as $m = 10$, the noise-generating threshold is set as $\tau = 0.5$, the transmit power is set as $P_t = 100$, and the decoding thresholds for eavesdroppers and legitimate receivers are set as $\gamma_e = 0.5$ and $\gamma = 1.0$, respectively.



(a) Model Validation



(b) Expected number of jammers considered for model validation

Figure 4.3: Model validation for different collusion intensity M, with $m = 10$, $\tau = 0.5$, $\gamma_e = 0.5$ and $\gamma = 1.0$.

Simulations with other settings can be easily conducted by our simulator as well. The simulation results and the related theoretical ones are summarized in Figure 4.3.

It can be observed from Figure 4.3 that the simulation results match fairly well with the theoretical ones for both the non-colluding case and the colluding case with

different collusion intensity M, which implies that our theoretical analysis is effective in modeling the secrecy outage performance of the concerned system. A careful observation in Figure 4.3 reveals that the curve $M = 1$ of the colluding case coincides with that of the non-colluding case, which is intuitive and further proves the effectiveness of our theoretical analysis.

4.4.2 Performance Evaluation

Regarding the impact of the number of relays n on the secrecy outage performance, it can be observed from Figure 4.3 that the SOP decreases as n increases for both the non-colluding case and the colluding case with different collusion intensity M. This is mainly due to the reason that, in the cooperative jamming scheme, more interference will be generated at the eavesdroppers for a larger number of relays, and thus the probability that eavesdroppers successfully decode the source message would decrease. This suggests that distributing more relays is an effective approach to decreasing the possibility of secrecy outage, and thus improving the security of the concerned network. A careful observation from Figure 4.3 indicates that to degrade the SOP to 50%, at least 20 relay nodes are required for $M = 1$ and at least 30 nodes are required for $M = 5$. This is because that the artificial noises generated from the jammers not only degrade the eavesdropper channels but also degrade those of the legitimate transmitter-receiver pairs at the same time.

To understand the impact of eavesdropper collusion M on the secrecy outage performance, we summarize in Figure 4.4 how the SOP varies with M for three different γ_e (i.e., $\gamma_e = 0.3$, $\gamma_e = 0.5$ and $\gamma_e = 1.0$), when $n = 30$, $m = 10$, $\tau = 0.5$ and $\gamma = 1.0$. We can see from Figure 4.4 that as the collusion intensity M increases, so does the SOP, implying that the eavesdropper collusion will significantly increase the possibility of secrecy outage, i.e., deteriorate the security performance of the concerned network. For example, the SOP for $\gamma_e = 1.0$ when all the eavesdroppers

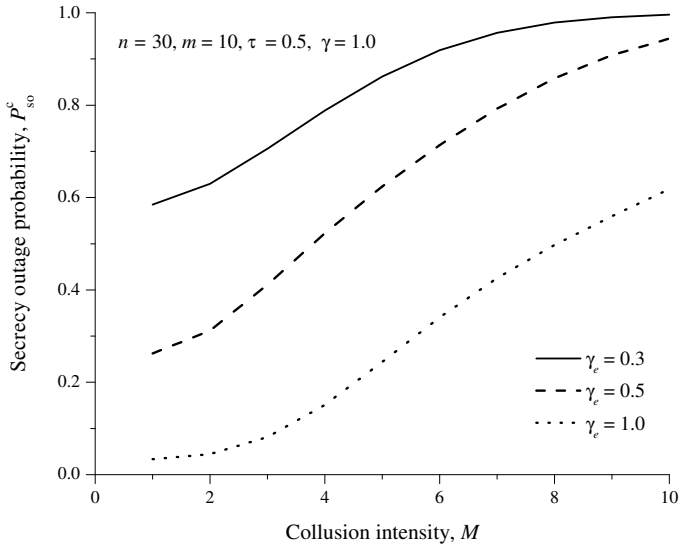


Figure 4.4: Secrecy outage probability vs. collusion intensity M for different γ_e, with $n = 30$, $m = 10$, $\tau = 0.5$ and $\gamma = 1.0$.

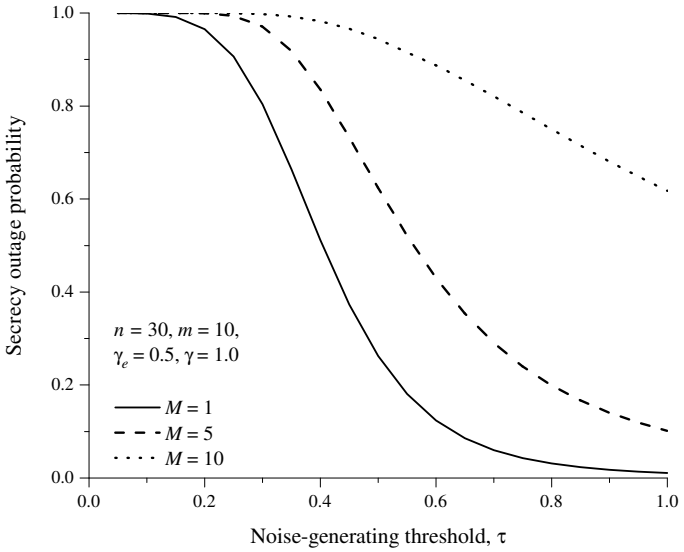


Figure 4.5: SOP vs. noise-generating threshold τ for different M, with $n = 30$, $m = 10$, $\gamma_e = 0.5$ and $\gamma = 1.0$.

collude (i.e., $M = m = 10$) is 0.61825, which is much greater than the one 0.03346 when no eavesdroppers collude (i.e., $M = 1$). Another observation from Figure 4.4

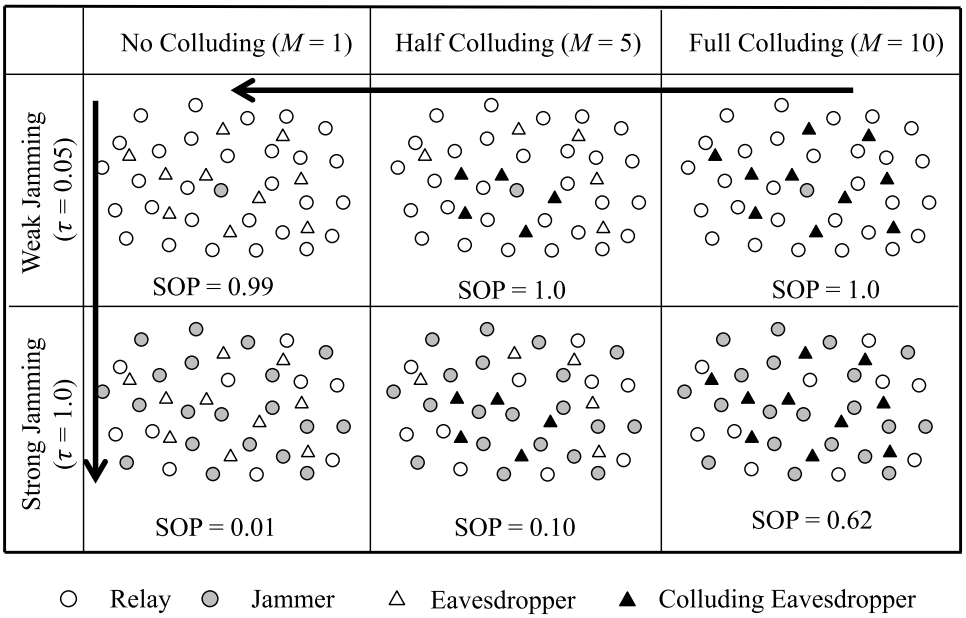


Figure 4.6: Relationship between theoretical results and representative network cases.

reveals that the SOP increases as the SIR threshold γ_e for eavesdroppers decreases, which is very intuitive since a smaller γ_e results in a greater decoding ability for eavesdroppers.

To see how the noise-generating threshold τ affect the secrecy outage performance, we summarize in Figure 4.5 how the SOP varies with τ for different collusion intensity M, when $n = 30$, $m = 10$, $\gamma_e = 0.5$ and $\gamma = 1.0$. The results in Figure 4.5 indicate that the SOP decreases as the noise-generating threshold τ increases for both the non-colluding ($M = 1$) and colluding cases ($M > 1$), which is also because that more interference will be generated at the eavesdroppers for a greater τ. This indicates that increasing the noise-generating threshold is also an effective way to enhance the security performance of the concerned network.

To illustrate the relationships between the theoretical SOP results and network cases, we provide the SOP results for six representative networks cases in Figure 4.6 for $n = 30$, $m = 10$, $\gamma_e = 0.5$ and $\gamma = 1.0$. We consider three different cases of collusion intensity (i.e., $M = 1$, $M = 5$ and $M = 10$), which correspond to the cases of no colluding, half colluding and full colluding respectively. For the jamming

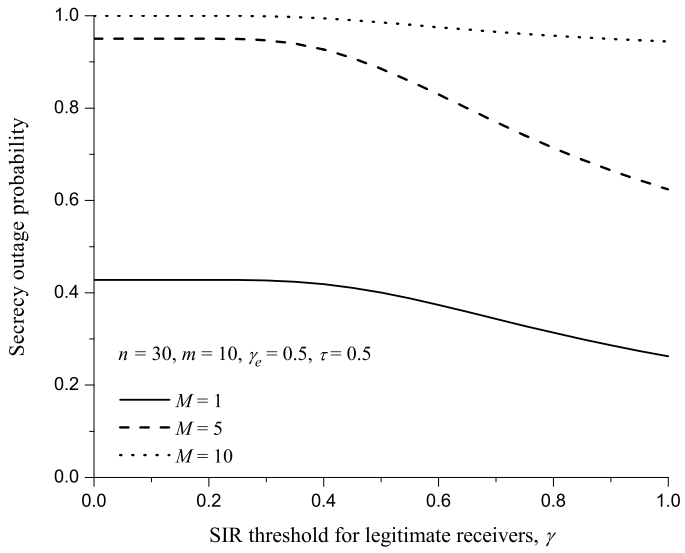


Figure 4.7: SOP vs. SIR threshold for legitimate receivers γ for different M, with $n = 30$, $m = 10$, $\gamma_e = 0.5$ and $\tau = 0.5$.

strength, we consider two cases of noise-generating threshold (i.e., $\tau = 0.05$ and $\tau = 1.0$), which correspond to the cases of weak jamming and strong jamming. We can see from Figure 4.6 that the SOP increases as the collusion intensity increases, while the SOP decreases as the jamming strength increases.

To further investigate the impact of the SIR threshold for legitimate receivers γ on the secrecy outage performance, we summarize in Figure 4.7 how the SOP varies with γ for different collusion intensity M, when $n = 30$, $m = 10$, $\gamma_e = 0.5$ and $\tau = 0.5$. It can be observed from Figure 4.7 that as γ increases the SOP first remain constant and then decreases. This is mainly due to the reason that there exists some threshold (e.g., about 0.2 in Figure 4.7) on γ. The transmission is conducted in two hops almost surely for γ less than this threshold, whereas the probability that the transmission is suspended in the second hop increases as γ increases beyond the threshold. Therefore, the eavesdroppers can overhear the source message in two hops at the beginning but then only in the first hop with an increasing probability as γ increases.

To illustrate the inherent tradeoff between the number of relays n and the noise-

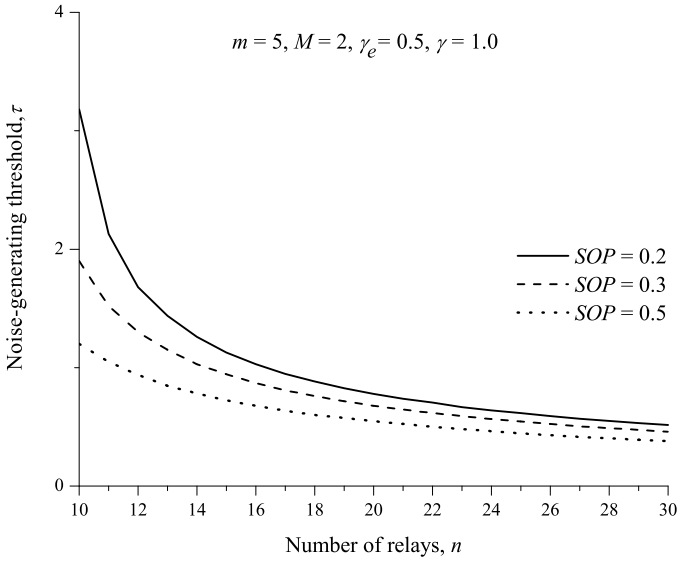


Figure 4.8: Feasible (n, τ) curve under the constraint of SOP = 0.2, 0.3 and 0.5, for $m = 5$, $M = 2$, $\gamma_e = 0.5$ and $\gamma = 1.0$.

generating threshold τ, we summarized in Figure 4.8 the feasible (n, τ) pairs to achieve a target SOP, under the setting of $m = 5$, $M = 2$, $\gamma_e = 0.5$ and $\gamma = 1.0$. It can be observed from Figure 4.8 that the noise-generating threshold τ decreases with the number of relays n. This means that if more relays nodes are distributed in the network, a smaller noise-generating threshold is enough to achieve the same target SOP. A careful observation from Figure 4.8 indicates that as the number of relays n increases, the SOP is more sensitive to the change of noise-generating threshold τ. For example, to decrease the SOP from 0.5 to 0.2, an increase of τ from 1.2 to 3.2 is required for $n = 10$, whereas a much smaller increase of τ (i.e., the increase from 0.378 to 0.515) is enough for $n = 30$.

4.5 Summary

This chapter conducted theoretical analysis to explore the secrecy outage performance of a two-hop wireless network under eavesdropper collusion, where coopera-

tive jamming is adopted to counteract such attack. Two eavesdropper cases were considered, i.e., the non-colluding case where eavesdroppers operate independently and the M-colluding case where any M eavesdroppers combine their observations to conduct eavesdropping attacks. We first derived the SOP of non-colluding case and then determined the SOP for M-colluding case by jointly applying the Laplace and inverse Laplace transform, the keyhole contour integral and the Cauchy Integral Theorem. Our results indicate that eavesdropper collusion can significantly increase the possibility of secrecy outage, and thus, deteriorate the security performance of the concerned network. Another important finding of this paper is that the cooperative jamming scheme can improve the network security by either distributing more relays or increasing the noise-generating threshold.

CHAPTER V

Cooperative Jamming Design in Large-Scale Wireless Networks

In this chapter, we focus on the cooperative jamming design in large-scale wireless networks, for which we propose a friendship-based cooperative jamming scheme to ensure the security of a finite Poisson Network with one source-destination pair, multiple legitimate nodes and multiple eavesdroppers distributed according to two independent and homogeneous Poisson Point Processes (PPP), respectively. To evaluate the performances of the proposed jamming scheme, we derive analytical expressions for the SOP and TOP of the concerned network under two typical cases of the path-loss exponent, by applying the tools from Stochastic Geometry. Extensive simulation and numerical results are presented to validate our theoretical analysis as well as to illustrate the performances of the proposed cooperative jamming scheme.

5.1 Preliminaries and Jamming Scheme

5.1.1 System Model

As illustrated in Figure 5.1, we consider a finite wireless network with nodes distributed over a bi-dimensional disk $\mathcal{B}(o, \mathcal{D}) \subset \mathbb{R}^2$ with radius $\mathcal{D}$. The network consists of a source S located at the origin o and a destination D at location y_0 with fixed

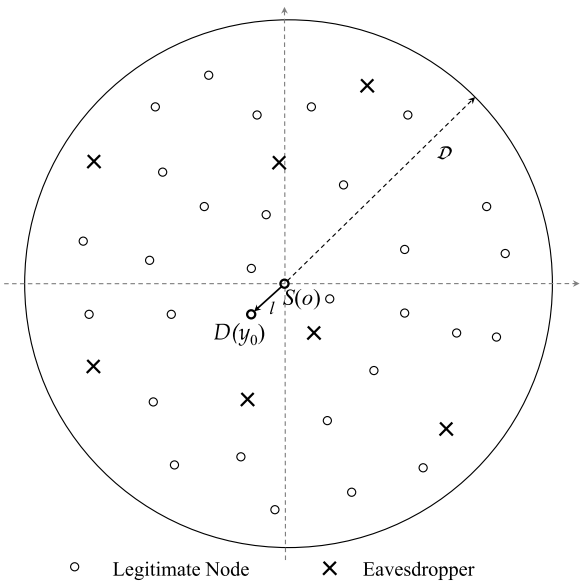


Figure 5.1: System model: nodes are distributed over a bi-dimensional disk $\mathcal{B}(o, \mathcal{D})$ with radius $\mathcal{D}$. The source S is located at the origin o and the destination D is located at y_0 with $||y_0|| = l$. Legitimate nodes and eavesdroppers are distributed according to two independent homogeneous PPPs.

distance $||y_0|| = l$ to the origin o. Also present in the network are multiple legitimate nodes and multiple eavesdroppers, whose locations are modeled as two independent and homogeneous PPPs Φ and Φ_E with intensities λ and λ_E, respectively. Throughout this paper we will use x (z) to denote the random location of a legitimate node (eavesdropper) as well as the node (eavesdropper) itself. To suppress the eavesdroppers, a set of legitimate nodes will serve as jammers (i.e., $\mathcal{J}$) to generate random Gaussian noise. The set of jammer locations is denoted as $\Phi_{\mathcal{J}}$.

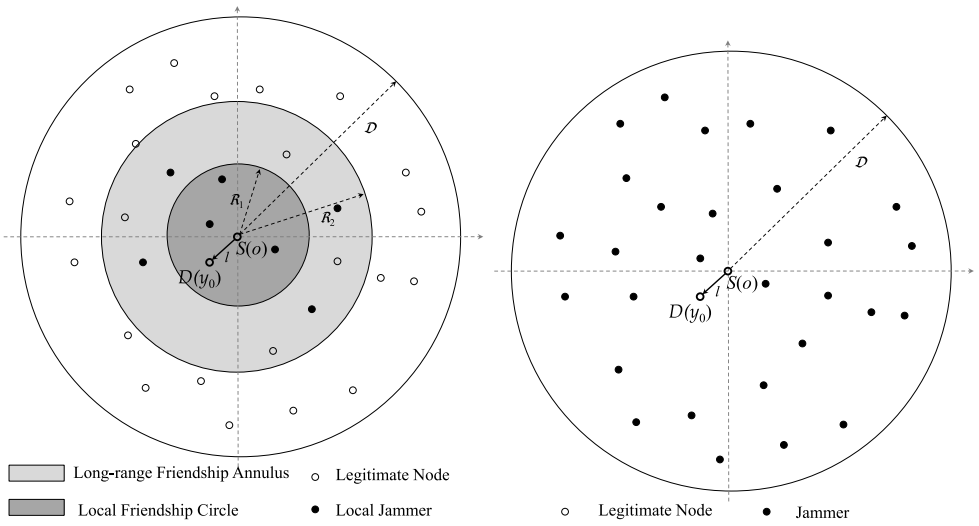
We assume all channel suffer from both small-scale Rayleigh fading and large-scale log-distance path loss with exponent $\alpha \geq 2$ [1]. The fading coefficient is constant for a block of transmission and varies randomly and independently from block to block for all channels. We assume that the source and jammers transmit with the same power P_t. Without loss of generality, we assume $P_t = 1$. The sum interference caused by the set of jammers at any location y in the network is then given by $I(y) = \sum_{x \in \Phi_{\mathcal{J}}} |h_{x,y}|^2 ||x-y||^{-\alpha}$, where $h_{x,y}$ and $||x-y||$ are the fading coefficient and distance

between x and y, respectively. Due to the Rayleigh fading assumption, $|h_{x,y}|^2$ is exponentially distributed and we assume unit mean for $|h_{x,y}|^2$, i.e., $\mathbb{E}[|h_{x,y}|^2] = 1$. The network is assumed interference-limited, and hence, the ambient noise is negligible. The signal-to-interference ratio (SIR) for the destination D from the source S is then given by $\text{SIR}_{y_0} = \frac{|h_{o,y_0}|^2 l^{-\alpha}}{I(y_0)}$ and the SIR for any eavesdropper $z \in \Phi_E$ is given by $\text{SIR}_z = \frac{|h_{o,z}|^2 ||z||^{-\alpha}}{I(z)}$.

5.1.2 Friendship-based Cooperative Jamming

This paper adopts the cooperative jamming technique to ensure the transmission security. Conventional cooperative jamming schemes usually do not exploit the inherent social behaviors among networks and allow all nodes being jammers equally likely. In practice, however, some nodes may refuse to serve as jammers, only because that they have no social relationships with the transmitter. Based on this idea, this paper proposes a friendship-based cooperative jamming scheme (as illustrated in Figure 5.2a) by exploiting the inherent friendship between the source and legitimate nodes. Different from conventional cooperative jamming schemes, the proposed jamming scheme aims to allow only the legitimate nodes that are friends of the source to serve as jammers (see Figure 5.2 for the difference). To model the friendship among network nodes, we adopt the so-called octopus friendship model (see Figure 5.3) in [56], where each node (say A) has not only local friends in a circle (called local friendship circle) around itself but also N long-range friends randomly selected from the region outside the local circle. Here, N can be drawn from any given discrete probability distribution, such as power law, Poisson, geometric or uniform distribution.

Based on the octopus friendship model, the proposed cooperative jamming scheme is composed of a Local Friendship Circle (LFC) with radius $\mathcal{R}_1$ and a Long-range Friendship Annulus (LFA) with inner radius $\mathcal{R}_1$ and outer radius $\mathcal{R}_2$, where $0 < \mathcal{R}_1 \leq \mathcal{R}_2 \leq \mathcal{D}$ (illustrated in Figure 5.2a). Both the LFC and LFA are centered at



(a) Conventional (b) Friendship-based

Figure 5.2: Friendship-based vs. conventional cooperative jamming.

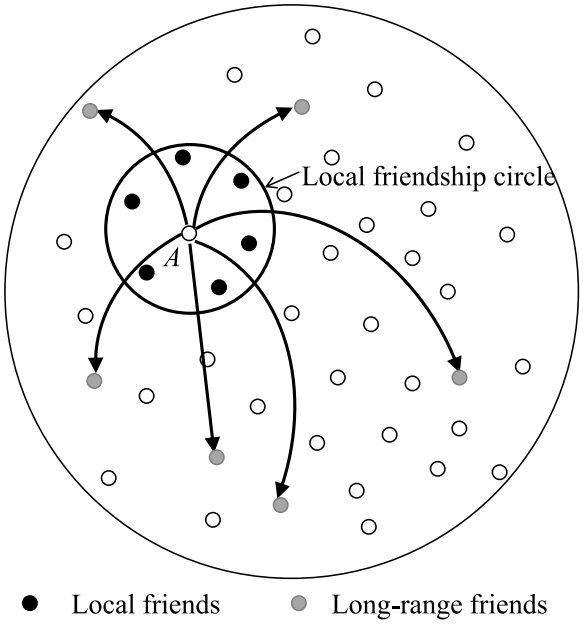


Figure 5.3: Octopus friendship model.

the source (i.e., the origin o). We use $\mathcal{A}_1$ to denote the LFC and $\mathcal{A}_2$ to denote the LFA. In the proposed jamming scheme, all legitimate nodes in $\mathcal{A}_1$ serve as jammers, while each legitimate node x in $\mathcal{A}_2$ serves as a jammer through a location-based policy $\mathcal{P}(||x||) \in [0, 1]$. Notice that different $\mathcal{P}(||x||)$ can yield different distributions of long-range jammers (i.e., different $\Phi_{\mathcal{J}}$). In this paper, we design three policies $\mathcal{P}(||x||)$,

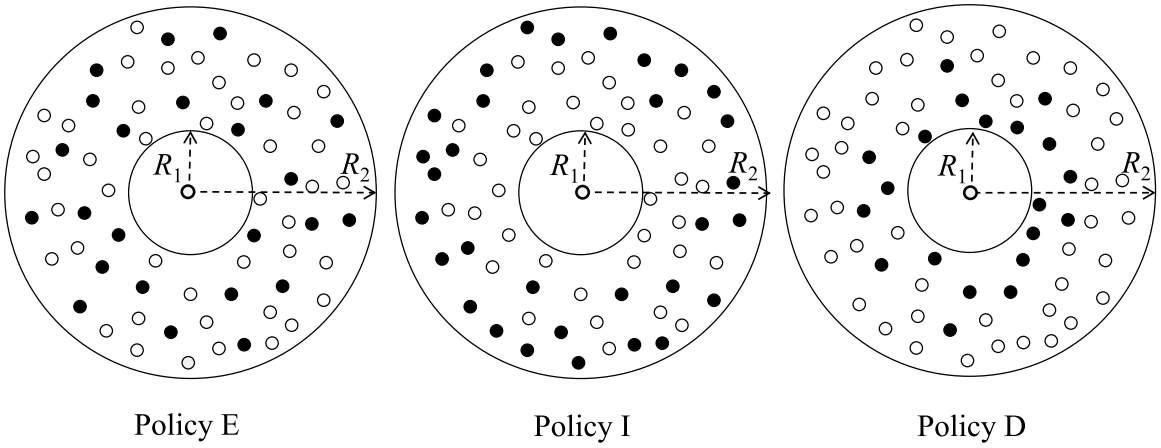


Figure 5.4: Illustration of long-range jammer selection policy.

which are summarized as follows.

- **Policy E**: In this policy, each node $x \in \Phi \cap \mathcal{A}_2$ is selected as a jammer with *Equal* probability $P(||x||) = p \in [0, 1]$. This policy corresponds to the scenario where long-range jammers are uniformly distributed over $\mathcal{A}_2$ (see Figure 5.4).

- **Policy I**: In this policy, each node $x \in \Phi \cap \mathcal{A}_2$ is selected as a jammer with probability $P(||x||)$ *Increasing* with its path loss to the transmitter, i.e.,

$$\mathcal{P}(||x||) = \frac{||x||^\alpha - \mathcal{R}_1^\alpha}{\mathcal{R}_2^\alpha - \mathcal{R}_1^\alpha}. \tag{5.1}$$

  This policy corresponds to the scenario where most of the long-range jammers are distributed near the outer circle of the LFA (see Figure 5.4).

- **Policy D**: In this policy, each node $x \in \Phi \cap \mathcal{A}_2$, is selected as a jammer with probability $P(||x||)$ is *Decreasing* with its path loss to the transmitter, i.e.,

$$\mathcal{P}(||x||) = \frac{\mathcal{R}_2^\alpha - ||x||^\alpha}{\mathcal{R}_2^\alpha - \mathcal{R}_1^\alpha}. \tag{5.2}$$

  This policy corresponds to the scenario where most of the long-range jammers are distributed near the inner circle of the LFA (see Figure 5.4).

Remark 3 *The policy $\mathcal{P}(||x||)$ can be interpreted as a thinning operation on Φ [65]. According to the property of thinning operation, the number of jammers in $\mathcal{A}_2$ still follows a Poisson distribution. Hence, the friendship model in the proposed jamming scheme is a special case of the one in [56], given that N is drawn from a Poisson distribution.*

5.1.3 Performance Metrics

The impact of friendship-based cooperative jamming scheme on the communication between the source S and destination y_0 is two-edged. On one hand, the interference generated by the jammers can degrade the eavesdropper channels, which may greatly enhance the security of the communication. On the other hand, the source-destination link is also impaired by the unintended interference, resulting in a probably unreliable communication. To measure the reliability and security of the source-destination communication, we still use the metrics of TOP and SOP as introduced and defined in Chapter III. In this chapter, the TOP denotes the probability that the SIR at the destination y_0 is below some threshold γ, i.e., $\mathrm{SIR}_{y_0} < \gamma$ and the SOP denotes the probability that the SIR at one or more eavesdroppers is above some threshold γ_e. Formally, the TOP is given by

$$P_{to} = \mathbb{P}(\mathrm{SIR}_{y_0} < \gamma), \tag{5.3}$$

and the SOP is given by

$$P_{so} = \mathbb{P}\left(\bigcup_{z \in \Phi_E} \mathrm{SIR}_{y_0} > \gamma_e\right). \tag{5.4}$$

5.2 Laplace Transform of Sum Interference

In this section, the Laplace transform of the sum interference $I(y)$ at any location $y \in \mathcal{B}(o, \mathcal{D})$ is analyzed for all three long-range jammer selection policies. To make the analysis mathematically tractable, we focus on two typical path loss scenarios of $\alpha = 2$ and $\alpha = 4$.

According to the definition, the Laplace transform of $I(y)$ is given by

$$\begin{aligned}
\mathcal{L}_{I(y)}^{\Xi,\alpha}(s) &= \mathbb{E}_{I(y)}\left[e^{-sI(y)}\right] \\
&= \mathbb{E}_{\Phi_{\mathcal{J}},\{|h_{x,y}|^2\}}\left[\exp\left(-s\sum_{x\in\Phi_{\mathcal{J}}}|h_{x,y}|^2||x-y||^{-\alpha}\right)\right] \\
&= \mathbb{E}_{\Phi_{\mathcal{J}},\{|h_{x,y}|^2\}}\left[\prod_{x\in\Phi_{\mathcal{J}}}\exp\left(-s|h_{x,y}|^2||x-y||^{-\alpha}\right)\right] \\
&= \mathbb{E}_{\Phi_{\mathcal{J}}}\left[\prod_{x\in\Phi_{\mathcal{J}}}\mathbb{E}_{|h_{x,y}|^2}\left[\exp\left(-s|h_{x,y}|^2||x-y||^{-\alpha}\right)\right]\right] \\
&= \mathbb{E}_{\Phi_{\mathcal{J}}}\left[\prod_{x\in\Phi_{\mathcal{J}}}\frac{1}{1+s||x-y||^{-\alpha}}\right], \qquad (5.5)
\end{aligned}$$

where $\Xi = \mathbf{E}, \mathbf{I}, \mathbf{D}$ denotes the selection policy.

From the cooperative jamming scheme in Section 5.1.2, we can see that $\Phi_{\mathcal{J}}$ is indeed an inhomogeneous PPP obtained by applying two independent thinning operations on Φ. We now define the intensity measure of $\Phi_{\mathcal{J}}$ by $\Lambda(\cdot)$, which gives the expected number of nodes in a given set. By applying the probability generating functional of $\Phi_{\mathcal{J}}$, we have

$$\mathcal{L}_{I(y)}^{\Xi,\alpha}(s) = \exp\left\{-\int_{\mathcal{B}(o,\mathcal{D})}\left(1-\frac{1}{1+s||x-y||^{-\alpha}}\right)\Lambda(\mathrm{d}x)\right\}$$
$$= \exp\left\{-\underbrace{\int_{\mathcal{B}(o,\mathcal{D})}\left(\frac{s}{s+||x-y||^{\alpha}}\right)\Lambda(\mathrm{d}x)}_{A}\right\}, \tag{5.6}$$

where $\Lambda(\mathrm{d}x)$ is given by

$$\Lambda(\mathrm{d}x) = \begin{cases} \lambda \mathrm{d}x, & x \in \mathcal{A}_1 \\ \lambda \mathcal{P}(||x||)\mathrm{d}x, & x \in \mathcal{A}_2 \end{cases}, \tag{5.7}$$

following from the thinning property of PPP. The term A in (5.6) can be rewritten as

$$A = \lambda \underbrace{\int_{\mathcal{A}_1}\left(\frac{s}{s+||x-y||^{\alpha}}\right)\mathrm{d}x}_{B_\alpha} + \lambda \underbrace{\int_{\mathcal{A}_2}\left(\frac{s}{s+||x-y||^{\alpha}}\right)\mathcal{P}(||x||)\mathrm{d}x}_{C_\alpha}. \tag{5.8}$$

Changing Cartesian coordinates to polar coordinates, we can rewrite B_α and C_α as

$$B_\alpha = 2\int_0^{\mathcal{R}_1}\int_0^{\pi}\frac{sr\mathrm{d}\theta\mathrm{d}r}{s+(r^2+||y||^2-2r||y||\cos\theta)^{\alpha/2}}, \tag{5.9}$$

and

$$C_\alpha = 2\int_{\mathcal{R}_1}^{\mathcal{R}_2}\int_0^{\pi}\frac{sr\mathcal{P}(r)\mathrm{d}\theta\mathrm{d}r}{s+(r^2+||y||^2-2r||y||\cos\theta)^{\alpha/2}}. \tag{5.10}$$

5.2.1 The Case of $\alpha = 2$

In this subsection, we derive the Laplace transform of $I(y)$ for the case of $\alpha = 2$. The main results are summarized in the following theorem.

Theorem V.1 *For the case of $\alpha = 2$, the Laplace transform of the sum interference $I(y)$ at any location $y \in \mathcal{B}(o, \mathcal{D})$ under Policy* $\mathbf{E}$ *is given by*

$$\mathcal{L}_{I(y)}^{\mathbf{E},2}(s) = \exp\Bigg\{ -\lambda\pi s \Bigg[p \operatorname{arcsinh} \frac{s + \mathcal{R}_2^2 - ||y||^2}{2||y||\sqrt{s}} + (1-p) \operatorname{arcsinh} \frac{s + \mathcal{R}_1^2 - ||y||^2}{2||y||\sqrt{s}} - \ln \frac{\sqrt{s}}{||y||} \Bigg] \Bigg\}, \tag{5.11}$$

where λ denotes the intensity of legitimate nodes, $\mathcal{R}_1$ denotes the radius of LFC (i.e., inner radius of LFA), $\mathcal{R}_2$ denotes the outer radius of LFA, $\operatorname{arcsinh} t = \ln(t + \sqrt{t^2+1})$ *denotes the inverse hyperbolic sine function. The Laplace transform of $I(y)$ under Policy* $\mathbf{I}$ *and Policy* $\mathbf{D}$ *is given by*

$$\mathcal{L}_{I(y)}^{\Xi',2}(s) = \exp\Bigg\{ -\lambda\pi s \Bigg[\Psi_2^{\Xi'}(\mathcal{R}_2, s, ||y||) - \Psi_2^{\Xi'}(\mathcal{R}_1, s, ||y||) + \Bigg(\operatorname{arcsinh} \frac{s + \mathcal{R}_1^2 - ||y||^2}{2||y||\sqrt{s}} - \ln \frac{\sqrt{s}}{||y||} \Bigg) \Bigg] \Bigg\}, \tag{5.12}$$

where $\Xi' = \mathbf{I}$ and $\mathbf{D}$*,*

$$\Psi_2^{\mathbf{I}}(r, s, ||y||) = \frac{\sqrt{(r^4 + 2(s-||y||^2)r^2 + (s+||y||^2)^2}}{\mathcal{R}_2^2 - \mathcal{R}_1^2} - \frac{s + \mathcal{R}_1^2 - ||y||^2}{\mathcal{R}_2^2 - \mathcal{R}_1^2} \operatorname{arcsinh} \frac{s + r^2 - ||y||^2}{2||y||\sqrt{s}},$$

and

$$\Psi_2^{\mathbf{D}}(r, s, ||y||) = \frac{s + \mathcal{R}_2^2 - ||y||^2}{\mathcal{R}_2^2 - \mathcal{R}_1^2} \operatorname{arcsinh} \frac{s + r^2 - ||y||^2}{2||y||\sqrt{s}} - \frac{\sqrt{(r^4 + 2(s-||y||^2)r^2 + (s+||y||^2)^2}}{\mathcal{R}_2^2 - \mathcal{R}_1^2}.$$

Proof 13 *The proof is given in Appendix C.2.*

5.2.2 The Case of $\alpha = 4$

The Laplace transform of $I(y)$ for the case of $\alpha = 4$ is derived in this subsection. The main results are summarized in the following theorem.

Theorem V.2 *For the case of $\alpha = 4$, the Laplace transform of the sum interference $I(y)$ at any location $y \in \mathcal{B}(o, \mathcal{D})$ under Policy* **E** *is given by*

$$\mathcal{L}_{I(y)}^{\mathbf{E},4}(s) = \exp\Bigg\{ -\lambda\pi\sqrt{s}\Bigg[\frac{\pi}{2} - (1-p)\arctan\frac{\sqrt{s} + \psi(\mathcal{R}_1, s, ||y||)}{\eta(\mathcal{R}_1, s, ||y||) + \mathcal{R}_1^2 - ||y||^2} - p\arctan\frac{\sqrt{s} + \psi(\mathcal{R}_2, s, ||y||)}{\eta(\mathcal{R}_2, s, ||y||) + \mathcal{R}_2^2 - ||y||^2}\Bigg]\Bigg\},$$

where λ denotes the intensity of legitimate nodes, $\mathcal{R}_1$ denotes the radius of LFC (i.e., inner radius of LFA), $\mathcal{R}_2$ denotes the outer radius of LFA,

$$\eta(r, s, ||y||) = \frac{\sqrt{\sqrt{(g(r, s, ||y||))^2 + 4s(r^2 + ||y||^2)^2} + g(r, s, ||y||)}}{\sqrt{2}},$$

$$g(r, s, ||y||) = (r^2 - ||y||^2)^2 - s, \tag{5.13}$$

$$\psi(r, s, ||y||) = \frac{\sqrt{s}(r^2 + ||y||^2)}{\eta(r, s, ||y||)}, \tag{5.14}$$

and $\arctan t$ *is the inverse tangent function. The Laplace transform of $I(y)$ under Policy* **I** *and Policy* **D** *is given by*

$$\mathcal{L}_{I(y)}^{\Xi',4}(s) = \exp\Bigg\{ -\lambda\pi\sqrt{s}\Bigg[\frac{\pi}{2} - \arctan\frac{\sqrt{s} + \psi(\mathcal{R}_1, s, ||y||)}{\eta(\mathcal{R}_1, s, ||y||) + \mathcal{R}_1^2 - ||y||^2} + \Psi_4^{\Xi'}(\mathcal{R}_2, s, ||y||) - \Psi_4^{\Xi'}(\mathcal{R}_1, s, ||y||)\Bigg]\Bigg\}, \tag{5.15}$$

where $\Xi' = \mathbf{I}$ *and* $\mathbf{D}$*,*

$$\begin{aligned}\Psi_4^{\mathbf{I}}(r,s,||y||) = &\frac{2\sqrt{s}||y||^2}{\mathcal{R}_2^4-\mathcal{R}_1^4}\ln\left[(\eta(r,s,||y||)+r^2-||y||^2)^2+(\sqrt{s}+\psi(r,s,||y||))^2\right]\\ &-\frac{1}{2(\mathcal{R}_2^4-\mathcal{R}_1^4)}\left[(r^2+3||y||^2)\psi(r,s,||y||)-3\sqrt{s}\eta(r,s,||y||)\right]\\ &+\frac{s+\mathcal{R}_1^4-||y||^4}{\mathcal{R}_2^4-\mathcal{R}_1^4}\arctan\frac{\sqrt{s}+\psi(r,s,||y||)}{\eta(r,s,||y||)+r^2-||y||^2},\end{aligned} \tag{5.16}$$

and

$$\begin{aligned}\Psi_4^{\mathbf{D}}(r,s,||y||) = &-\frac{2\sqrt{s}||y||^2}{\mathcal{R}_2^4-\mathcal{R}_1^4}\ln\left[(\eta(r,s,||y||)+r^2-||y||^2)^2+(\sqrt{s}+\psi(r,s,||y||))^2\right]\\ &+\frac{1}{2(\mathcal{R}_2^4-\mathcal{R}_1^4)}\left[(r^2+3||y||^2)\psi(r,s,||y||)-3\sqrt{s}\eta(r,s,||y||)\right]\\ &-\frac{s+\mathcal{R}_2^4-||y||^4}{\mathcal{R}_2^4-\mathcal{R}_1^4}\arctan\frac{\sqrt{s}+\psi(r,s,||y||)}{\eta(r,s,||y||)+r^2-||y||^2}.\end{aligned} \tag{5.17}$$

Proof 14 *The proof is given in Appendix C.3.*

Corollary 1 *For* $\mathcal{P}(r)=0$*, as* $\mathcal{R}_1\to\infty$*, the Laplace transform of* $I(y)$ *for the case of* $\alpha=4$ *is* $\mathcal{L}_{I(y)}^{\Xi,4}(s)=\exp\left(-\frac{\lambda\sqrt{s}\pi^2}{2}\right)$*, which recovers the well-known Laplace transform of* $I(y)$ *for a homogeneous infinite PPP with* $\alpha=4$ *[66].*

Proof 15 *Letting* $\mathcal{P}(r)=0$ *yields*

$$\mathcal{L}_{I(y)}^{\Xi,4}(s)=\exp\left\{-\lambda\pi\sqrt{s}\left[\frac{\pi}{2}-\arctan\frac{\sqrt{s}+\psi(\mathcal{R}_1,s,||y||)}{\eta(\mathcal{R}_1,s,||y||)+\mathcal{R}_1^2-||y||^2}\right]\right\}.$$

As $\mathcal{R}_1\to\infty$*,*

$$\lim_{\mathcal{R}_1\to\infty}\arctan\frac{\sqrt{s}+\psi(\mathcal{R}_1,s,||y||)}{\eta(\mathcal{R}_1,s,||y||)+\mathcal{R}_1^2-||y||^2}=\arctan\frac{2\sqrt{s}}{\infty-||y||^2}=0, \tag{5.18}$$

which completes the proof.

5.3 Outage Performance

In this section, the TOP and SOP of the proposed cooperative jamming scheme are analyzed. We focus again on the cases of $\alpha = 2$ and $\alpha = 4$. The analysis is based on the Laplace transforms of the sum interference $I(y)$ derived in Section 5.2. We first determine the exact expression for the TOP and then obtain both the upper and lower bounds on the SOP.

5.3.1 Transmission Outage Probability

The TOP can be regarded as a measure of the link reliability between the source S and destination D. For the Rayleigh fading channel model, the TOP can be directly derived by applying the Laplace transform of the sum interference at the location of destination y_0 [66]. The following theorem is established to summarize the result of the TOP.

Theorem V.3 *Consider a finite Poisson network with nodes distributed over a bi-dimensional disk $\mathcal{B}(o, \mathcal{D})$ as illustrated in Figure 5.1 and the friendship-based cooperative jamming scheme in Section 5.1.2, the TOP of the source-destination pair is given by*

$$P_{to} = 1 - \mathcal{L}^{\Xi,\alpha}_{I(y_0)}(\gamma l^\alpha), \tag{5.19}$$

where $\Xi = \mathbf{E}$, $\mathbf{I}$ and $\mathbf{D}$ denotes the long-range jammer selection policy, α denotes the path loss exponent, and the Laplace transform $\mathcal{L}^{\Xi,\alpha}_{I(y_0)}(\gamma l^\alpha)$ of the sum interference at the destination y_0 is given by (5.11), (5.12), (5.13), (5.15) with $||y_0|| = l$, $s = \gamma l^\alpha$ for the cases of $\alpha = 2$ and $\alpha = 4$, respectively.

Proof 16 *From the definition of TOP in (5.3), we have*

$$\begin{aligned} P_{to} &= \mathbb{P}\left(\mathrm{SIR}_{y_0} < \gamma\right) \\ &= \mathbb{P}\left(\frac{|h_{o,y_0}|^2 l^{-\alpha}}{I(y_0)} < \gamma\right) \\ &= \mathbb{E}_{\Phi_{\mathcal{J}}}\left[\mathbb{P}\left(\frac{|h_{o,y_0}|^2 l^{-\alpha}}{I(y_0)} < \gamma \middle| \Phi_{\mathcal{J}}\right)\right] \\ &= \mathbb{E}_{\Phi_{\mathcal{J}}}\left[\mathbb{P}\left(|h_{o,y_0}|^2 < \gamma l^{\alpha} I(y_0) \middle| \Phi_{\mathcal{J}}\right)\right] \\ &= 1 - \mathbb{E}_{I(y_0)}\left[e^{-\gamma l^{\alpha} I(y_0)}\right] \\ &= 1 - \mathcal{L}^{\Xi,\alpha}_{I(y_0)}(\gamma l^{\alpha}), \end{aligned} \tag{5.20}$$

which completes the proof.

5.3.2 Secrecy Outage Probability

The SOP is a commonly-used performance metric to quantify the PHY security. In the performance analysis of large-scale systems, the exact SOP is usually unavailable, mainly due to the reason that the analysis involves computing highly cumbersome integrals in terms of the PPPs of both legitimate nodes and eavesdroppers. We therefore resort to obtain the upper and lower bounds on the SOP by applying the bounding technique used in [67]. We establish the following theorem to summarize the main results.

Theorem V.4 *Consider a finite Poisson network with nodes distributed over a bi-dimensional disk $\mathcal{B}(o, \mathcal{D})$ as illustrated in Figure 5.1 and the friendship-based cooperative jamming scheme in Section 5.1.2, the upper bound on the SOP of the source-destination pair is given by*

$$P_{so}^{\mathrm{UB}} = 1 - \exp\left\{-2\pi\lambda_E \int_0^{\mathcal{D}} \mathcal{L}^{\Xi,\alpha}_{I(z)}(\gamma_e r_e^{\alpha}) r_e \mathrm{d}r_e\right\}, \tag{5.21}$$

and the lower bound is given by

$$P_{so}^{\mathrm{LB}} = \int_0^{\mathcal{D}} 2\lambda_E \pi r_{e^*} \exp(-\lambda_E \pi r_{e^*}^2) \mathcal{L}_{I(z^*)}^{\Xi,\alpha}(\gamma_e r_{e^*}^{\alpha}) \mathrm{d}r_{e^*}, \tag{5.22}$$

where λ_E denotes the intensity of eavesdroppers, γ_e denotes the minimum required SIR for eavesdroppers to correctly decode the message, $\Xi = \mathbf{E}$, $\mathbf{I}$ and $\mathbf{D}$ denotes the long-range jammer selection policy, α denotes the path loss exponent, z^* denotes the eavesdropper nearest to the source o, r_{e^*} denotes the distance between z^* and o, and the Laplace transform $\mathcal{L}_{I(z)}^{\Xi,\alpha}(\gamma r_e^{\alpha})$ is given by (5.11), (5.12), (5.13), (5.15) with $||z|| = r_e$, $s = \gamma r_e^{\alpha}$ for the cases of $\alpha = 2$ and $\alpha = 4$, respectively.

Proof 17 *From the definition of SOP in (5.3), we have*

$$\begin{aligned}
P_{so} &= \mathbb{P}\left(\bigcup_{z \in \Phi_E} \mathrm{SIR}_{y_0} > \gamma_e \right) \\
&= 1 - \mathbb{P}\left(\bigcap_{z \in \Phi_E} \mathrm{SIR}_z < \gamma_e \right) \\
&= 1 - \mathbb{E}_{\Phi_{\mathcal{J}}}\left[\mathbb{E}_{\Phi_E}\left[\mathbb{P}\left(\bigcap_{z \in \Phi_E} \frac{|h_{o,z}|^2 ||z||^{-\alpha}}{I(z)} < \gamma_e \big| \Phi_E, \Phi_{\mathcal{J}} \right) \right] \right] \\
&\overset{(a)}{=} 1 - \mathbb{E}_{\Phi_{\mathcal{J}}}\left[\mathbb{E}_{\Phi_E}\left[\prod_{z \in \Phi_E} \mathbb{P}\left(\frac{|h_{o,z}|^2 ||z||^{-\alpha}}{I(z)} < \gamma_e \big| \Phi_E, \Phi_{\mathcal{J}} \right) \right] \right] \\
&= 1 - \mathbb{E}_{\Phi_{\mathcal{J}}}\left[\mathbb{E}_{\Phi_E}\left[\prod_{z \in \Phi_E} \left(1 - \mathbb{P}\left(\frac{|h_{o,z}|^2 ||z||^{-\alpha}}{I(z)} > \gamma_e \big| \Phi_E, \Phi_{\mathcal{J}} \right) \right) \right] \right] \\
&\overset{(b)}{=} 1 - \mathbb{E}_{\Phi_{\mathcal{J}}}\left[\exp\left\{ -\lambda_E \int_{\mathcal{B}(o,\mathcal{D})} \mathbb{P}\left(\frac{|h_{o,z}|^2 ||z||^{-\alpha}}{I(z)} > \gamma_e \big| \Phi_{\mathcal{J}} \right) \mathrm{d}z \right\} \right],
\end{aligned} \tag{5.23}$$

where (a) follows since $|h_{o,z}|^2$, $z \in \Phi_E$ are i.i.d. random variables, and (b) follows from applying the probability generating functional of Φ_E. Applying the Jensen's Inequality

yields the upper bound on P_{so}, we have

$$\begin{aligned} P_{so} &\leq 1 - \exp\left\{ -\lambda_E \int_{\mathcal{B}(o,\mathcal{D})} \mathbb{E}_{\Phi_{\mathcal{J}}} \left[\mathbb{P}\left(\frac{|h_{o,z}|^2 ||z||^{-\alpha}}{I(z)} > \gamma_e \middle| \Phi_{\mathcal{J}} \right) \right] \mathrm{d}z \right\} \\ &= 1 - \exp\left\{ -\lambda_E \int_{\mathcal{B}(o,\mathcal{D})} \mathcal{L}^{\Xi,\alpha}_{I(z)}(\gamma_e ||z||^{\alpha}) \mathrm{d}z \right\} \\ &= 1 - \exp\left\{ -2\pi\lambda_E \int_0^{\mathcal{D}} \mathcal{L}^{\Xi,\alpha}_{I(z)}(\gamma_e r_e^{\alpha}) r_e \mathrm{d}r_e \right\}. \end{aligned} \tag{5.24}$$

The lower bound is obtained by considering only the eavesdropper z^* nearest to the source S. Let R_{z^*} denote the random distance between z^* and S. The probability distribution function of R_{z^*} can be given by

$$f_{R_{z^*}}(r_{e^*}) = \begin{cases} 2\lambda_E \pi r_{e^*} \exp(-\lambda_E \pi r_{e^*}^2), & 0 \leq r_{e^*} \leq \mathcal{D} \\ 0, & \text{otherwise} \end{cases}.$$

Please refer to Appendix C.4 for the proof. The SOP can then be bounded from below by the probability that z^* causes a secrecy outage, i.e.,

$$\begin{aligned} P_{so} &\geq \mathbb{P}(\mathrm{SIR}_{z^*} > \gamma_e) \\ &= \int_0^{\mathcal{D}} \mathbb{P}\left(\frac{|h_{o,z^*}|^2 r_{e^*}^{-\alpha}}{I(z^*)} > \gamma_e \right) f_{R_{z^*}}(r_{e^*}) \mathrm{d}r_{z^*} \\ &= \int_0^{\mathcal{D}} 2\lambda_E \pi r_{e^*} \exp(-\lambda_E \pi r_{e^*}^2) \mathcal{L}^{\Xi,\alpha}_{I(z^*)}(\gamma_e r_{e^*}^{\alpha}) \mathrm{d}r_{e^*}. \end{aligned} \tag{5.25}$$

5.4 Numerical Results and Discussions

In this section, we first conduct extensive simulations to verify the theoretical analysis of TOP and SOP. We then explore how the parameters of the friendship-based cooperative jamming scheme affect the TOP and SOP performances of the legitimate transmission.

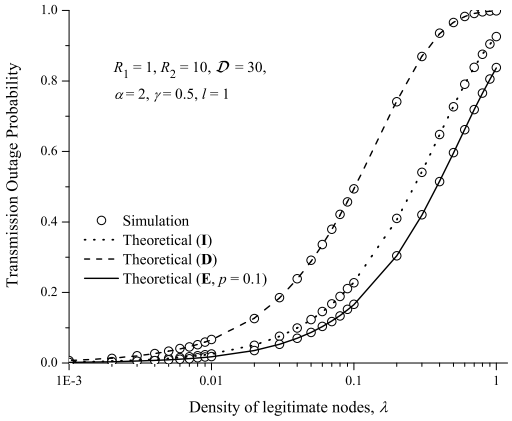
5.4.1 Simulation Settings

A simulator based on C++ was developed to simulate the PPPs Φ and Φ_E, the friendship-based cooperative jamming model and the transmission process between the source S and destination D, which is now available at [68]. The PPP Φ (Φ_E) is simulated by applying the method in [65], where the first step is to generate a Poisson-distributed number N with mean $\lambda\pi\mathcal{D}^2$ ($\lambda_E\pi\mathcal{D}^2$ for Φ_E) and the second step is to distribute N nodes uniformly over the network $\mathcal{B}(o,\mathcal{D})$. The total number of source-destination transmissions is fixed as 100000 and the common transmit power is fixed as 1. The TOP is calculated as the ratio of the number n_{to} of transmissions with transmission outage to the total transmission number, i.e., TOP $= \frac{n_{to}}{100000}$. Similarly, The SOP is calculated as SOP $= \frac{n_{so}}{100000}$, where n_{so} is the number of transmissions with secrecy outage.

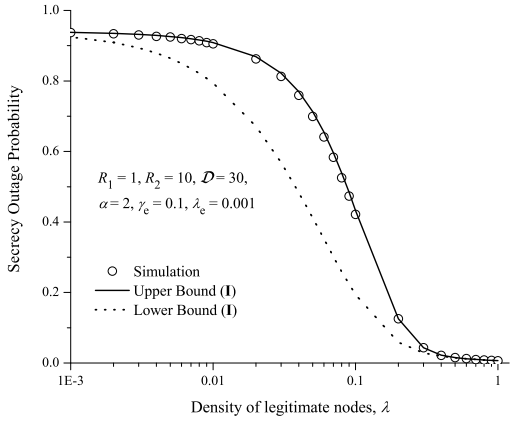
Extensive simulations have been conducted to verify the theoretical analysis of TOP and SOP. We considered the cases of $\alpha = 2$ and $\alpha = 4$ and examined how the TOP and SOP vary with the density of legitimate nodes λ under three long-range jammer selection policies **E**, **I** and **D**. For both path loss cases, the network radius was fixed as $\mathcal{D} = 30$ and the density of eavesdroppers was fixed as $\lambda_E = 0.001$. For the friendship-based cooperative jamming scheme, the radius of the LFC was fixed as $\mathcal{R}_1 = 1$, the outer radius of the LFA was fixed as $\mathcal{R}_2 = 10$ and the selection probability in Policy **E** was set as $p = 0.1$. The SIR thresholds were fixed as $\gamma = 0.5$ for the destination D and $\gamma_e = 0.1$ for eavesdroppers. The source-destination distance was set as $l = 1$. The corresponding simulation results and theoretical results are summarized in Figure 5.5 and Figure 5.6.

5.4.2 Model Validation

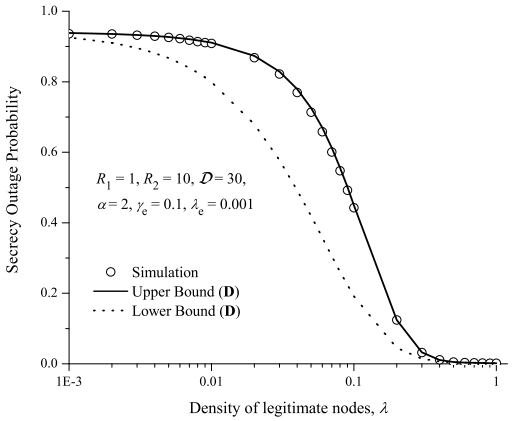
Figure 5.5a and Figure 5.6a indicate clearly that the simulation results of TOP match nicely with the theoretical ones, so our theoretical results can be applied to



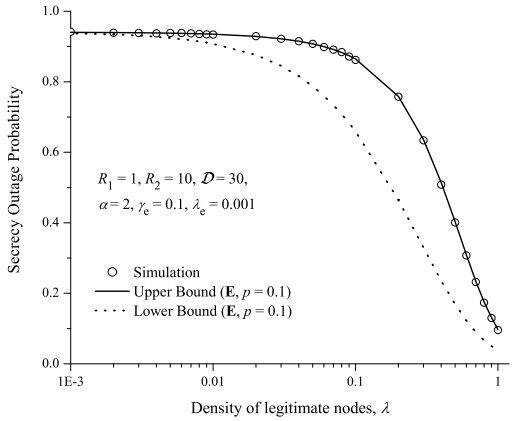
(a) TOP Validation for Policy **I**, **D** and **E**



(b) SOP Validation for Policy **I**



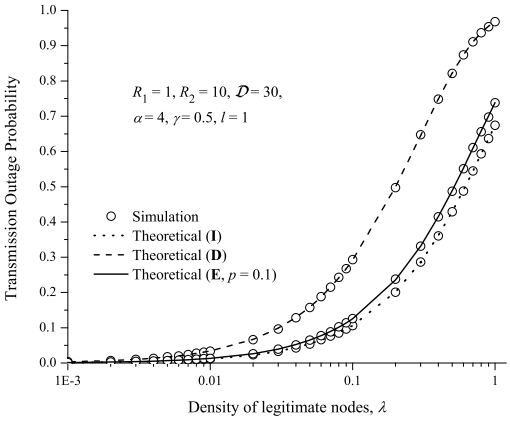
(c) SOP Validation for Policy **D**



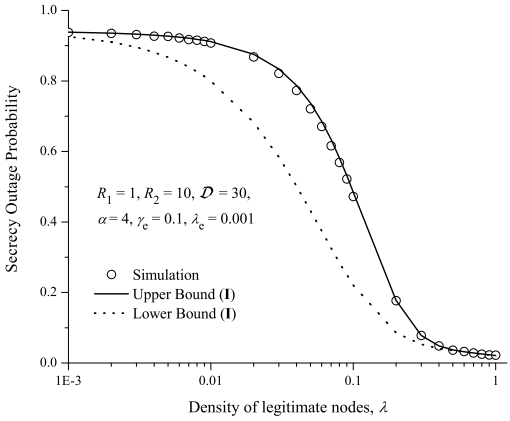
(d) SOP Validation for Policy **E**

Figure 5.5: Simulation results vs. theoretical results for TOP and SOP for $\alpha = 2$.

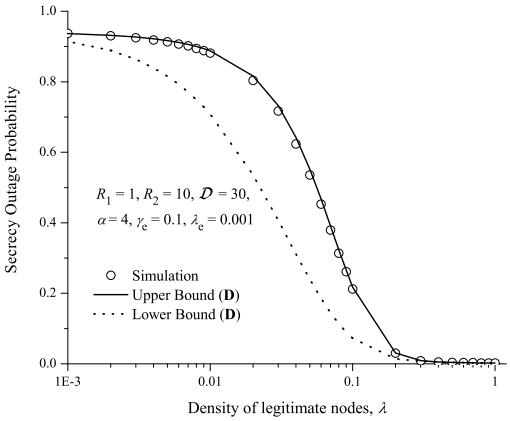
model the TOP performance of the Poisson networks under Policy **E**, Policy **I** and Policy **D** for the cases of $\alpha = 2$ and $\alpha = 4$. Figures 5.5b, 5.5c, 5.5d, 5.6b, 5.6c and 5.6d indicate that the simulation results of SOP are very close to the corresponding theoretical upper bounds, while they are different from the lower bounds, so our theoretical upper bounds can serve as accurate approximations for the exact SOP of the legitimate transmission under Policy **E**, Policy **I** and Policy **D** for the cases of $\alpha = 2$ and $\alpha = 4$. In the following, we mainly focus on the case of $\alpha = 4$, as the behaviors of TOP and SOP for $\alpha = 2$ and $\alpha = 4$ are similar. In addition, we use the



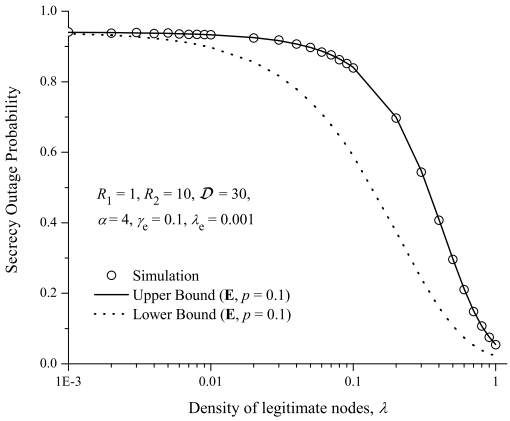
(a) TOP Validation for Policy **I**, **D** and **E**



(b) SOP Validation for Policy **I**



(c) SOP Validation for Policy **D**



(d) SOP Validation for Policy **E**

Figure 5.6: Simulation results vs. theoretical results of TOP and SOP for $\alpha = 4$.

theoretical upper bounds on SOP in the discussions of the SOP performance.

5.4.3 TOP and SOP vs. Jamming Parameters

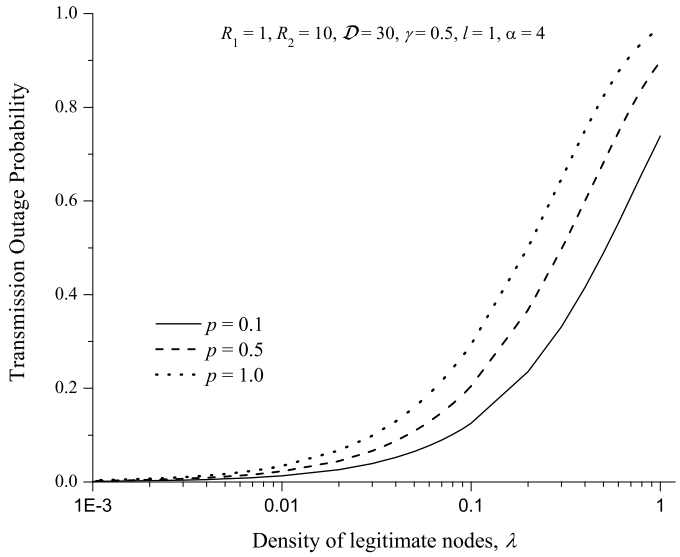
We now explore how the TOP and SOP performances of the network vary with the parameters of the friendship-based cooperative jamming scheme with different long-range jammer selection policies. We first examine the impact of the density of legitimate nodes λ on the TOP and SOP performances. It can be observed from Figure 5.5 and Figure 5.6 that the TOP increases as λ increases, while the SOP de-

creases as λ increases under all policies **E**, **I** and **D** for both $\alpha = 2$ and $\alpha = 4$. This is very intuitive since a larger sum interference can be generated in the network as λ increases, degrading both the source-destination channel and eavesdropper channels. As shown in Figure 5.5 and Figure 5.6 in general, Policy **I** outperforms Policy **D** in terms of the TOP performance, while Policy **D** can ensure a better SOP performance than Policy **I**. This is due to the following two reasons. The first one is that Policy **D** has much more long-range jammers than Policy **I**, so it will generate more interference in the network, resulting in a better SOP performance but a worse TOP performance. The other reason is that the long-range jammers of Policy **D** are much closer to the source than those of Policy **I**. Notice that near (i.e., close to the source) eavesdroppers dominate the behavior of SOP, so Policy **D** is more effective to suppress near eavesdroppers than Policy **I**, achieving a better SOP performance.

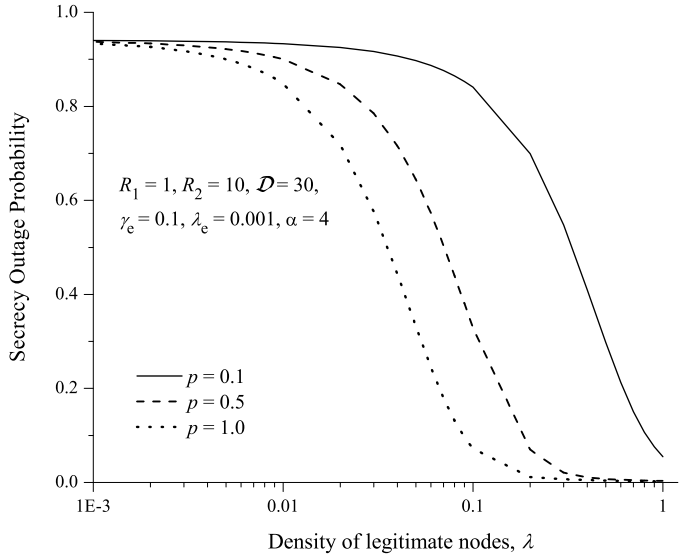
Notice that in Figure 5.5 and Figiure 5.6, the jammer selection probability of Policy **E** is fixed as $p = 0.1$, which corresponds to a weak long-range jamming scenario. For the moderate long-range jamming scenario ($p = 0.5$) and strong long-range jamming scenario ($p = 1.0$), Figure 5.7 shows TOP and SOP vs. λ for $\alpha = 4$. As shown in Figure 5.7 that the behaviors of TOP and SOP are similar for different p. One can also observe from Figure 5.7 that the TOP increases as p increases, while the SOP decreases as p increases. This indicates that we can flexibly control the TOP and SOP performances of Policy **E** by varying the long-range jammer selection probability p.

5.4.3.1 TOP and SOP vs. $\mathcal{R}_1$

We now investigate how the TOP and SOP performances are affected by the radius of LFC $\mathcal{R}_1$, i.e., the inner radius of LFA. For the scenario of $\mathcal{R}_2 = 10$, $\mathcal{D} = 30$, $\gamma = 0.5$, $\lambda = 0.1$, $l = 2$ and $\alpha = 4$, Figure 5.8a illustrates how the TOP varies with $\mathcal{R}_1$ for Policy **I**, Policy **D** and Policy **E** with $p = 0.5$. We can see from Figure 5.8a that the TOP first increases as $\mathcal{R}_1$ increases, then saturates to a constant value and



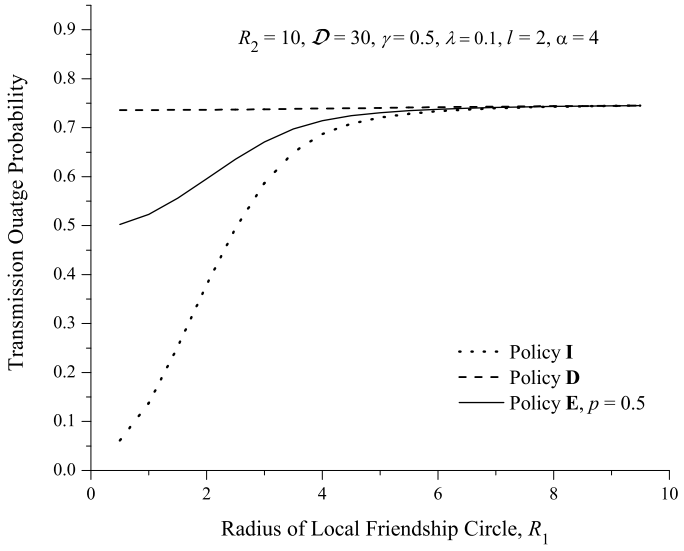
(a) TOP vs. p



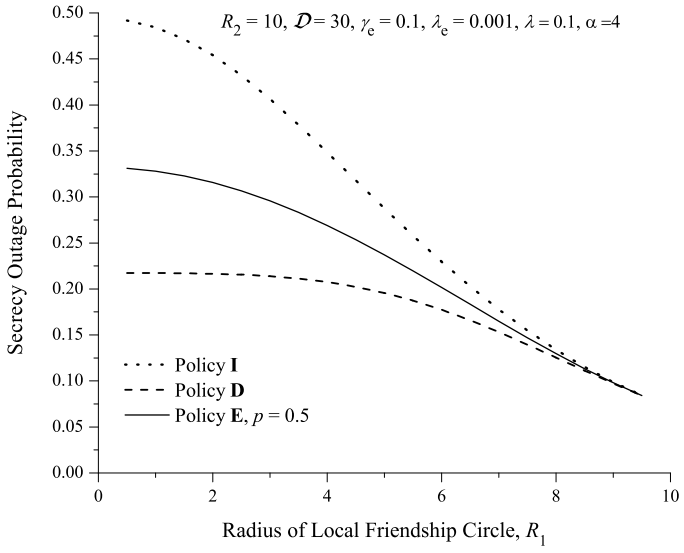
(b) SOP vs. p

Figure 5.7: Impact of p on TOP and SOP for Policy **E**.

finally stays almost the same for Policy **I** and Policy **E**. Actually, this is also the case for Policy **D**. The increasing behavior of TOP is because that the total number of jammers increases as $\mathcal{R}_1$ increases, although the number of long-range jammers



(a) TOP vs. $\mathcal{R}_1$



(b) SOP vs. $\mathcal{R}_1$

Figure 5.8: Impact of $\mathcal{R}_1$ on TOP and SOP.

decreases, which results in a larger sum interference in the network. The behavior that TOP of all policies saturates to a same constant is due to the fact that all policies finally reach to the same jamming pattern at the point of $\mathcal{R}_1 = \mathcal{R}_2$. For the scenario

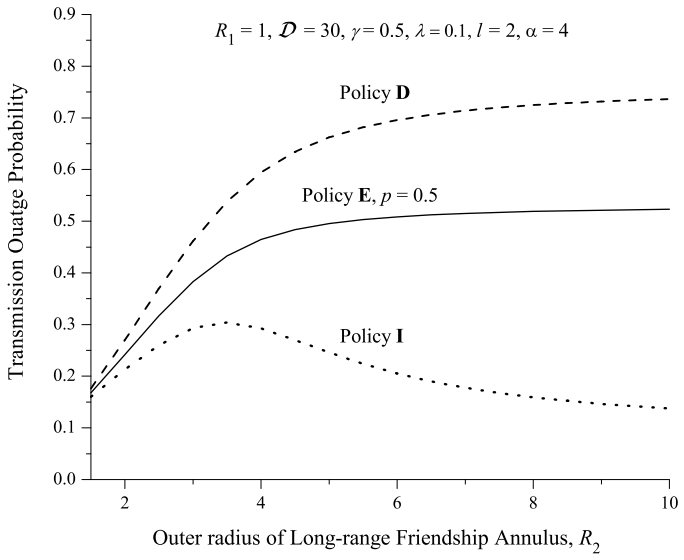
of $\mathcal{R}_2 = 10$, $\mathcal{D} = 30$, $\gamma_e = 0.1$, $\lambda_E = 0.001$, $\lambda = 0.1$ and $\alpha = 4$, Figure 5.8b shows how the SOP varies with $\mathcal{R}_1$ for Policy **I**, Policy **D** and Policy **E** with $p = 0.5$. It can be observed from Figure 5.8b that the SOP first decreases as $\mathcal{R}_1$ increases, then saturates to a constant value and finally stays almost the same for all policies. This is due to the same reason as explained above.

5.4.3.2 TOP and SOP vs. $\mathcal{R}_2$

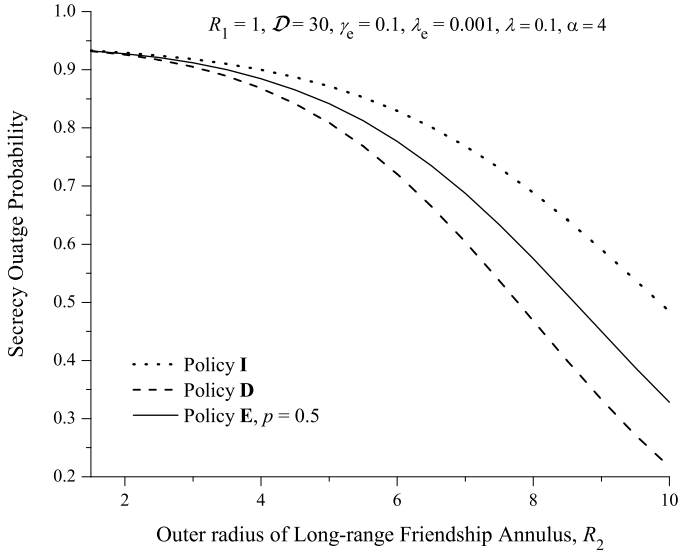
Regarding the impact of the outer radius of LFA $\mathcal{R}_2$ on the TOP performance, we show in Figure 5.9a how the TOP varies with $\mathcal{R}_2$ for Policy **I**, Policy **D** and Policy **E** with $p = 0.5$ under the settings of $\mathcal{R}_1 = 1$, $\mathcal{D} = 30$, $\gamma = 0.5$, $\lambda = 0.1$, $l = 2$ and $\alpha = 4$. As shown in Figure 5.9a that the TOP of Policy **E** and Policy **D** always monotonically increases as $\mathcal{R}_2$ increases, but this is not the case for Policy **I**. The increasing behavior of TOP for all policies are because that the number of long-range jammers increases as $\mathcal{R}_2$ increases, generating a larger sum interference in the network. The decreasing behavior of TOP for Policy **I** is due to that its long-range jammers are getting further away from the destination as $\mathcal{R}_2$ continues to increase, since these jammers are mainly located in a small annulus region near $\mathcal{R}_2$. For the impact of $\mathcal{R}_2$ on the SOP performance, we illustrate in Figure 5.9b SOP vs. $\mathcal{R}_2$ for Policy **I**, Policy **D** and Policy **E** with $p = 0.5$ under the settings of $\mathcal{R}_1 = 1$, $\mathcal{D} = 30$, $\gamma_e = 0.1$, $\lambda_E = 0.001$, $\lambda = 0.1$ and $\alpha = 4$. As expected, we can observe from Figure 5.9b that the SOP decreases as $\mathcal{R}_2$ increases for all policies.

5.5 Summary

This chapter explored the physical layer security-based secure communications in a finite Poisson network with social friendships among nodes, for which a social friendship-based cooperative jamming scheme is proposed. The jamming scheme consists of a Local Friendship Circle (LFC) and a Long-range Friendship Annulus (LFA),



(a) TOP vs. $\mathcal{R}_2$



(b) SOP vs. $\mathcal{R}_2$

Figure 5.9: Impact of $\mathcal{R}_2$ on TOP and SOP.

where all legitimate nodes in the LFC serve as jammers, but the legitimate nodes in the LFA are selected as jammers through three location-based policies, namely, Policy **E**, Policy **I** and Policy **D**. To understand the security and reliability performances of

the proposed jamming scheme, we analyzed its TOP and SOP based on the Laplace transforms of the sum interference at any location in the network. The results in this paper indicated that, in general, Policy **I** outperforms Policy **D** in terms of the reliability performance, while Policy **D** can ensure a better security performance than Policy **I**. Also, we can flexibly control the reliability and security performances of Policy **E** by varying its long-range jammer selection probability. An interesting observation from the results in this paper showed that increasing the outer radius of the LFA beyond some threshold under Policy **I** can improve both the reliability and security performances of the proposed jamming scheme.

CHAPTER VI

Conclusion

In this thesis, we studied the PHY security performances of wireless networks, where the PHY security technique of cooperative jamming is adopted to ensure secure communications. We first explored the PHY security performance of small-scale wireless networks with *non-colluding* eavesdroppers, and then investigated the PHY security performance of small-scale wireless networks with *colluding* eavesdroppers. Finally, we examined the cooperative jamming design issue in large-scale wireless networks.

For the PHY security performance of small-scale wireless networks with *non-colluding* eavesdroppers, we studied in Chapter III the eavesdropper-tolerance capability (ETC) of a two-hop wireless network with one source-destination pair, multiple relays and multiple on-colluding eavesdroppers. We first theoretically analyzed the secrecy outage probability (SOP) and transmission outage probability (TOP) of a two-hop relay wireless network with cooperative jamming under two relaying schemes, i.e., random relaying and opportunistic relaying. Based on the SOP and TOP results, we then determined the ETC of both schemes. The main results in Chapter III showed that cooperative jamming is an effective technique to provide security for wireless communications. In addition, we found that the opportunistic relaying scheme can achieve a much better ETC performance, which is usually orders of magnitude more

than that ensured by the random relaying scheme.

For the PHY security performance of small-scale wireless networks with *colluding* eavesdroppers, we investigated in Chapter IV the SOP of a two-hop wireless network with one source-destination pair, multiple relays and multiple colluding eavesdroppers. We consider two eavesdropper scenarios to depict the behavior of eavesdroppers, i.e., non-colluding scenario where eavesdroppers do not collude and operate independently and M-colluding scenario where M eavesdroppers can collude to exchange and combine the received signals so as to improve the successful decoding probability. We first derive the analytical expression for the SOP under the non-colluding scenario, we then derive the SOP under the M-colluding scenario by applying the techniques of Laplace transform, keyhole contour integral and Cauchy Integral Theorem. The results in this chapter showed that eavesdropper collusion can significantly increase the possibility of secrecy outage, and thus, deteriorate the security performance of the concerned network.

In Chapter V, we addressed the cooperative jamming design issue in large-scale wireless networks, for which proposed a friendship-based cooperative jamming scheme to ensure the secure transmission of a finite Poisson network with one source-destination pair, multiple legitimate nodes and multiple eavesdroppers, whose locations are modeled by two independent and homogeneous Poisson Point Processes, respectively. The jamming scheme comprises an LFC and an LFA, where all legitimate nodes in the LFC serve as jammers, and three location-based policies (i.e, Policy E, Policy I and Policy D) are designed to select legitimate nodes in the LFA as jammers. The analytical expressions for the SOP and TOP were also derived to evaluate the performances of the proposed scheme. The results in this paper indicated that, in general, Policy I outperforms Policy D in terms of the reliability performance, while Policy D can ensure a better security performance than Policy I. Also, we can flexibly control the reliability and security performances of Policy E by varying its long-range jammer selection

probability. An interesting observation from the results in this paper demonstrated that increasing the outer radius of the LFA beyond some threshold under Policy I can improve both the reliability and security performances of the proposed jamming scheme.

It is notable that, this thesis considers a relatively simple block Rayleigh fading channel model where channel gains remain constant during a block of time. In practice, however, the channel may vary very fast even for a small time block. So, one of the interesting and important future work is to study the PHY security performances of wireless networks under more practice channel models.

APPENDICES

APPENDIX A

Proofs in Chapter III

A.1 Proof of Lemma 1 and 2

Proof of Lemma 1 : From the transmission protocol and the i.i.d fading assumption, we can easily see that I_1 and I_2 are the sum of random variables which are smaller than τ among $n-1$ i.i.d random variables and thus I_1 and I_2 are independent and identically distributed. Now we take I_1 for example to determine the distribution of the total interference in both hops. By using the function $U(x) = \mathbf{1}_{x<\tau}(x) \cdot x$ in the proof of Theorem III.1, we can rewrite $I_1 = \sum_{j=1,j\neq b}^{n} U(|h_{R_j,R_b}|^2)$. The mean and variance of the mixed-type random variable $U(|h_{R_j,R_b}|^2)$ can be given by $\mu_1 = 1-(1+\tau)e^{-\tau}$ and $\sigma_1^2 = 1 - \tau^2 e^{-\tau} - (1+\tau)^2 e^{-2\tau}$. Therefore, the pdf of I_1 can be recursively given by the following mixed density and mass function

$$f(x) = \begin{cases} e^{-(n-1)\tau}, & x = 0 \\ p_{n-1}(x)e^{-x}, & 0 < x \leq (n-1)\tau \\ 0, & otherwise, \end{cases}$$

where $p_{n-1}(x)$ is a piecewise function and coincides with different polynomial functions of degree at most $n-2$ on each interval $(k\tau,(k+1)\tau]$ for $0 \leq k \leq n-2$. However, it is quite difficult to determine the function $p_{n-1}(x)$, especially for large n. Thus, we approximate I_1 by a normal random variable with mean $\mu = (n-1)\mu_1$ and variance $\sigma^2 = (n-1)\sigma_1^2$, according to the Central Limit Theorem and its pdf can be approximated by $f(x) \approx \hat{f}(x) = \frac{e^{-\frac{(x-\mu)^2}{2\sigma^2}}}{\sigma\sqrt{2\pi}}$ where $\mu = (n-1)\Big[1-(1+\tau)e^{-\tau}\Big]$ and $\sigma = \sqrt{(n-1)\Big[1-\tau^2e^{-\tau}-(1+\tau)^2e^{-2\tau}\Big]}$.

Proof of Lemma 2: Before deriving the probability in Lemma 2, we first define the event that relay $R_k, k = 1,\cdots,n$ is selected as the message relay by A_k (i.e., $b=k$). Besides, we use a new random variable S_j to define $min\{|h_{S,R_j}|^2, |h_{R_j,D}|^2\}$ for each relay R_j. It is notable that $S_j, j = 1,\cdots,n$ is an exponential random variable with mean $\frac{1}{2}$. Then, we have $A_k \triangleq \bigcap_{j=1,j\neq k}^{n}(S_j \leq S_k)$.

Now, applying the law of total probability, we have

$$
\begin{aligned}
&\mathbb{P}\Big(|h_{S,R_b}|^2 \geq x, |h_{R_b,D}|^2 \geq y\Big) \qquad (A.1)\\
&= \sum_{k=1}^{n} \mathbb{P}\left(|h_{S,R_k}|^2 \geq x, |h_{R_k,D}|^2 \geq y, A_k\right)\\
&= \sum_{k=1}^{n} \mathbb{P}\left(|h_{S,R_k}|^2 \geq x, |h_{R_k,D}|^2 \geq y, \bigcap_{j=1,j\neq k}^{n}(S_j \leq S_k)\right)\\
&= \sum_{k=1}^{n} \int_0^{\infty} \mathbb{P}\left(|h_{S,R_k}|^2 \geq x, |h_{R_k,D}|^2 \geq y, S_k = s, \bigcap_{j=1,j\neq k}^{n}(S_j \leq s)\right)\mathrm{d}s\\
&= \sum_{k=1}^{n} \int_0^{\infty} \mathbb{P}\Big(|h_{S,R_k}|^2 \geq x, |h_{R_k,D}|^2 \geq y, S_k = s\Big)\mathbb{P}\left(\bigcap_{j=1,j\neq k}^{n}(S_j \leq s)\right)\mathrm{d}s\\
&= \sum_{k=1}^{n} \int_0^{\infty} \mathbb{P}\Big(|h_{S,R_k}|^2 \geq x, |h_{R_k,D}|^2 \geq y, S_k = s\Big)(1-e^{-2s})^{n-1}\mathrm{d}s,
\end{aligned}
$$

When $x \geq y \geq 0$, (A.1) can be reduced to

$$\begin{aligned}
&\mathbb{P}\Big(|h_{S,R_b}|^2 \geq x, |h_{R_b,D}|^2 \geq y\Big) \qquad \text{(A.2)}\\
&= \sum_{k=1}^{n} \Bigg\{ \int_x^{\infty} \mathbb{P}\Big(|h_{S,R_k}|^2 = s, |h_{R_k,D}|^2 \geq s\Big)(1-e^{-2s})^{n-1} ds \\
&\quad + \int_y^{x} \mathbb{P}\Big(|h_{S,R_k}|^2 > x, |h_{R_k,D}|^2 = s\Big)(1-e^{-2s})^{n-1} ds \\
&\quad + \int_x^{\infty} \mathbb{P}\Big(|h_{S,R_k}|^2 > s, |h_{R_k,D}|^2 = s\Big)(1-e^{-2s})^{n-1} ds \Bigg\} \\
&= 2n \int_x^{\infty} \frac{(1-e^{-2s})^{n-1}}{e^{2s}} ds + ne^{-x} \int_y^{x} \frac{(1-e^{-2s})^{n-1}}{e^{s}} ds \\
&= 1 - (1-e^{-2x})^n + ne^{-x} \int_{e^{-x}}^{e^{-y}} (1-t^2)^{n-1} dt \\
&= 1 - (1-e^{-2x})^n + ne^{-x} \Big[\varphi(n,y) - \varphi(n,x)\Big],
\end{aligned}$$

where $\varphi(n,x) = e^{-x}{}_2F_1\left(\frac{1}{2}, 1-n; \frac{3}{2}; e^{-2x}\right)$ and ${}_2F_1$ is the Gaussian hypergeometric function. Similarly, when $0 \leq x < y$, (A.1) can be reduced to

$$P\Big(|h_{S,R_b}|^2 \geq x, |h_{R_b,D}|^2 \geq y\Big) = 1 - (1-e^{-2y})^n + ne^{-y}\Big[\varphi(n,x) - \varphi(n,y)\Big]$$

Combining (A.2) and (A.3), Lemma 2 then follows.

APPENDIX B

Proofs in Chapter IV

B.1 Proof of Lemma 7

It can be seen from the definition of event A that

$$p_{A|J_1^l} = P\left(\gamma_{S,R_b} < \gamma \middle| J_1^l\right) = P\left(|h_{S,R_b}|^2 < \gamma \sum_{j\in\mathcal{J}_1} |h_{R_j,R_b}|^2 \middle| J_1^l\right).$$

Hence, we first need to determine the distribution of $|h_{S,R_b}|^2$. Define $min\{|h_{S,R_k}|^2, |h_{R_k,D}|^2\}$ for each relay R_k, $k = 1, \cdots, n$ by T_k and the event that relay R_k announces itself as the message relay by B_k (i.e., $b = k$). It is easy to see that $B_k \triangleq \bigcap_{j=1,j\neq k}^{n} (T_j \leq T_k)$, and all T_k's are i.i.d. and exponential random variables with mean $1/2$. Thus, apply-

ing the law of total probability, we have

$$
\begin{aligned}
& P\left(|h_{S,R_b}|^2 < x\right) \\
&= \sum_{k=1}^{n} P\left(|h_{S,R_k}|^2 < x, B_k\right) \\
&= \sum_{k=1}^{n} P\left(|h_{S,R_k}|^2 < x, \bigcap_{j=1,j\neq k}^{n} (T_j \leq T_k)\right) \\
&= \sum_{k=1}^{n} \int_0^{\infty} P\left(|h_{S,R_k}|^2 < x, \bigcap_{j=1,j\neq k}^{n} (T_j \leq t), T_k = t\right) \mathrm{d}t \\
&= \int_0^{\infty} nP\left(|h_{S,R_k}|^2 < x, T_k = t\right) (1-e^{-2t})^{n-1} \mathrm{d}t.
\end{aligned} \tag{B.1}
$$

Again, by the law of total probability, we have

$$
\begin{aligned}
& P\left(|h_{S,R_k}|^2 < x, T_k = t\right) \\
&= \begin{cases}
P\left(|h_{S,R_k}|^2 = t, |h_{R_k,D}|^2 > t\right) & \\
+P\left(t < |h_{S,R_k}|^2 < x, |h_{R_k,D}|^2 = t\right), & 0 \leq t \leq x \\
0, & otherwise
\end{cases} \\
&= \begin{cases}
e^{-t}(2e^{-t} - e^{-x}), & 0 \leq t \leq x \\
0, & otherwise.
\end{cases}
\end{aligned} \tag{B.2}
$$

Hence, after substituting (B.2) into (B.1) and conducting some algebraic manipulation, we have

$$
P(|h_{S,R_b}|^2 < x) = \sum_{k=0}^{n} \binom{n}{k} (-1)^k \frac{ke^{-x} + (k-1)e^{-2kx}}{2k-1}. \tag{B.3}
$$

Next, the probability distribution of $|h_{R_j,R_b}|^2$ for any $j \in \mathcal{J}_1$ can be given by

$$
f_{|h_{R_j,R_b}|^2}(x) = \begin{cases}
\frac{e^{-x}}{1-e^{-\tau}}, & 0 \leq x < \tau \\
0, & x \geq \tau
\end{cases}. \tag{B.4}
$$

Hence, we have

$$
\begin{aligned}
p_{A|J_1^l} &= \mathbb{E}_{\{|h_{R_j,R_b}|^2, j\in\mathcal{J}_1\}}\Bigg[\sum_{k=0}^{n}\binom{n}{k}(-1)^k\frac{1}{2k-1} \\
&\quad \left(ke^{-\gamma\sum|h_{R_j,R_b}|^2}+(k-1)e^{-2k\gamma\sum|h_{R_j,R_b}|^2}\right)\Bigg|J_1^l\Bigg] \\
&= \sum_{k=0}^{n}\binom{n}{k}(-1)^k\frac{1}{2k-1}\Bigg(k\mathbb{E}\left[e^{-\gamma\sum|h_{R_j,R_b}|^2}|J_1^l\right] \\
&\quad +(k-1)\mathbb{E}\left[e^{-2k\gamma\sum|h_{R_j,R_b}|^2}|J_1^l\right]\Bigg) \\
&= \sum_{k=0}^{n}\binom{n}{k}(-1)^k\frac{1}{2k-1}\Bigg[k\left(\frac{1-e^{-(1+\gamma)\tau}}{(1-e^{-\tau})(1+\gamma)}\right)^l \\
&\quad +(k-1)\left(\frac{1-e^{-(2k\gamma+1)\tau}}{(1-e^{-\tau})(2k\gamma+1)}\right)^l\Bigg].
\end{aligned}
\tag{B.5}
$$

APPENDIX C

Proofs in Chapter V

C.1 Integral Identities

Identity 1 *For $a, b \in \mathbb{R}$ and $a > |b|$, we have from [69] and [70]*

$$\int_0^{\pi} \frac{\mathrm{d}\theta}{(a + b\cos\theta)^{n+1}} = \frac{\pi P_n(\frac{a}{\sqrt{a^2-b^2}})}{(a^2-b^2)^{\frac{n+1}{2}}}, \tag{C.1}$$

where $P_n(\cdot)$ is the n^{th}-Legendre polynomial and $P_0(\cdot) = 1$.

Identity 2 *Let $a, b, c \in \mathbb{R}$ and $c > 0$. Defining $Q = ct^2 + bt + a$ and $\Delta = 4ac - b^2$, we have from [69] and [70]*

$$\begin{aligned} \int \frac{\mathrm{d}t}{\sqrt{Q}} &= \frac{1}{\sqrt{c}} \ln(2\sqrt{cQ} + 2ct + b) \ [c > 0] \\ &= \frac{1}{\sqrt{c}} \operatorname{arcsinh} \frac{2ct + b}{\sqrt{\Delta}} \ [c > 0, \Delta > 0], \end{aligned} \tag{C.2}$$

Identity 3 *For $m, n \in \mathbb{Z}$ and $Q = ct^2 + bt + a$, we have from [69]*

$$\int \frac{t^m}{\sqrt{Q^{2n+1}}}\mathrm{d}t = \frac{t^{m-1}}{(m-2n)c\sqrt{Q^{2n-1}}} - \frac{(2m-2n-1)b}{2(m-2n)c}\int \frac{t^{m-1}}{\sqrt{Q^{2n+1}}}\mathrm{d}t - \frac{(m-1)a}{(m-2n)c}\int \frac{t^{m-2}}{\sqrt{Q^{2n+1}}}\mathrm{d}t, \tag{C.3}$$

where $a, b, c \in \mathbb{R}$ and $c > 0$.

C.2 Proof of Theorem V.1

For $\alpha = 2$, we can rewrite B_α as

$$B_2 = 2\int_0^{R_1}\int_0^{\pi} \frac{sr\mathrm{d}\theta\mathrm{d}r}{s + r^2 + ||y||^2 - 2r||y||\cos\theta}. \tag{C.4}$$

Applying Identity 1 in Appendix C.1, we have

$$\begin{aligned} B_2 &= \pi s\int_0^{R_1} \frac{2r\mathrm{d}r}{\sqrt{r^4 + 2(s-||y||^2)r^2 + (s+||y||^2)^2}} \\ &\overset{t\leftrightarrow r^2}{=} \pi s\int_0^{R_1^2} \frac{\mathrm{d}t}{\sqrt{(t^2 + 2(s-||y||^2)t + (s+||y||^2)^2}}, \end{aligned} \tag{C.5}$$

We then apply Identity 2 in Appendix C.1 and substitute t with r^2 to obtain

$$B_2 = \pi s\left(\operatorname{arcsinh}\frac{s + R_1^2 - ||y||^2}{2||y||\sqrt{s}} - \ln\frac{\sqrt{s}}{||y||}\right). \tag{C.6}$$

Similarly, applying Identity 1, we can rewrite C_α as

$$C_2 = \pi s\int_{R_1}^{R_2} \frac{2rP(r)\mathrm{d}r}{\sqrt{r^4 + 2(s-||y||^2)r^2 + (s+||y||^2)^2}}. \tag{C.7}$$

For Policy E, $P(r) = p$. Then, we have

$$C_2 = p\pi s \operatorname{arcsinh} \frac{s + r^2 - ||y||^2}{2||y||\sqrt{s}}\Big|_{r=R_1}^{R_2}. \tag{C.8}$$

Substituting (C.8) and (C.6) into (5.9) in Section 5.2, and then substituting (5.9) into (5.8) yields the Laplace transform of $I(y)$ under Policy E for $\alpha = 2$.

Next, $P(r)$ can be written as $P(r) = u + vr^2$, where $u = -\frac{R_1^2}{R_2^2 - R_1^2}$, $v = \frac{1}{R_2^2 - R_1^2}$ for Policy I, and $u = \frac{R_2^2}{R_2^2 - R_1^2}$, $v = -\frac{1}{R_2^2 - R_1^2}$ for Policy D. Hence,

$$\begin{aligned}
C_2 &= \pi s \int_{R_1}^{R_2} \frac{2r(u + vr^2)\mathrm{d}r}{\sqrt{r^4 + 2(s - ||y||^2)r^2 + (s + ||y||^2)^2}} \\
&= \pi s \int_{R_1^2}^{R_2^2} \frac{(u + vt)\mathrm{d}t}{\sqrt{(t^2 + 2(s - ||y||^2)t + (s + ||y||^2)^2}} \\
&= \pi s \Bigg[u \int_{R_1^2}^{R_2^2} \frac{\mathrm{d}t}{\sqrt{(t^2 + 2(s - ||y||^2)t + (s + ||y||^2)^2}} \\
&\quad + v \int_{R_1^2}^{R_2^2} \frac{t\mathrm{d}t}{\sqrt{(t^2 + 2(s - ||y||^2)t + (s + ||y||^2)^2}} \Bigg] \\
&\overset{t \leftrightarrow r^2}{=} \pi s \Bigg[(u - vs + v||y||^2) \operatorname{arcsinh} \frac{s + t - ||y||^2}{2||y||\sqrt{s}} \\
&\quad + v\sqrt{(t^2 + 2(s - ||y||^2)t + (s + ||y||^2)^2} \Bigg] \Bigg|_{t=R_1^2}^{R_2^2},
\end{aligned} \tag{C.9}$$

Substituting t with r^2, we have

$$\begin{aligned}
C_2 = \pi s \Bigg[&(u - vs + v||y||^2) \operatorname{arcsinh} \frac{s + r^2 - ||y||^2}{2||y||\sqrt{s}} \\
&+ v\sqrt{(r^4 + 2(s - ||y||^2)r^2 + (s + ||y||^2)^2} \Bigg] \Bigg|_{r=R_1}^{R_2}.
\end{aligned} \tag{C.10}$$

Finally, we substitute (C.6) and (C.10) into (5.9) in Section 5.2, and then substitute (5.9) into (5.8) to obtain the Laplace transform of $I(y)$ under Policy I and Policy D for $\alpha = 2$.

C.3 Proof of Theorem V.2

For $\alpha = 4$, we can rewrite B_α as

$$\begin{aligned} B_4 &= 2\int_0^{R_1}\int_0^{\pi} \frac{sr\mathrm{d}\theta\mathrm{d}r}{s+(r^2+||y||^2-2r||y||\cos\theta)^2} \\ &= 2\int_0^{R_1} \frac{\sqrt{s}r}{2i}\int_0^{\pi} \frac{\mathrm{d}\theta\mathrm{d}r}{(r^2+||y||^2-2r||y||\cos\theta-i\sqrt{s})} \\ &\quad -\frac{\mathrm{d}\theta\mathrm{d}r}{(r^2+||y||^2-2r||y||\cos\theta+i\sqrt{s})} \end{aligned} \tag{C.11}$$

Applying Identity 1, we have $B_4 = \frac{\pi\sqrt{s}}{2i}\int_0^{R_1}\frac{2r\mathrm{d}r}{\sqrt{\mathcal{C}_1}} - \frac{2r\mathrm{d}r}{\sqrt{\mathcal{C}_2}}$ and applying Identity 2, we have $B_4 = \frac{\pi\sqrt{s}}{2i}\ln\frac{\sqrt{\mathcal{C}_1}+r^2-(i\sqrt{s}+||y||^2)}{\sqrt{\mathcal{C}_2}+r^2+(i\sqrt{s}-||y||^2)}\Big|_{r=0}^{R_1}$ where $\mathcal{C}_1 = (r^2-||y||^2)^2 - s - 2i\sqrt{s}(r^2+||y||^2)$ and $\mathcal{C}_2 = \mathcal{C}_1^*$ is the complex conjugate of $\mathcal{C}_1$. Now, we rewrite $\mathcal{C}_1$ as

$$\mathcal{C}_1 = (\eta - i\psi)^2 = \eta^2 - \psi^2 - 2i\eta\psi, \tag{C.12}$$

for some real-valued functions $\eta(r,s,||y||)$ and $\psi(r,s,||y||)$. For the simplicity of notation, we also use η and ψ to represent $\eta(r,s,||y||)$ and $\psi(r,s,||y||)$, respectively. We can then establish the following equation system

$$\begin{cases} \eta^2-\psi^2 &= (r^2-||y||^2)^2 - s \\ \eta\psi &= \sqrt{s}(r^2+||y||^2). \end{cases} \tag{C.13}$$

The functions η and ψ can be obtained by solving the above equation system. Given $\mathcal{C}_1$ as in (C.12),

$$\begin{aligned} B_4 &= \frac{\pi\sqrt{s}}{2i} \ln \frac{\eta + r^2 - ||y||^2 - i(\sqrt{s}+\psi)}{\eta + r^2 - ||y||^2 + i(\sqrt{s}+\psi)}\Bigg|_{r=0}^{R_1} \\ &= \frac{\pi\sqrt{s}}{2i} \ln \frac{1 - i\frac{\sqrt{s}+\psi}{\eta+r^2-||y||^2}}{1 + i\frac{\sqrt{s}+\psi}{\eta+r^2-||y||^2}}\Bigg|_{r=0}^{R_1} \\ &= -\pi\sqrt{s} \arctan \frac{\sqrt{s}+\psi}{\eta + r^2 - ||y||^2}\Bigg|_{r=0}^{R_1} \\ &= \pi\sqrt{s}\left(\frac{\pi}{2} - \arctan \frac{\sqrt{s}+\psi(R_1, s, ||y||)}{\eta(R_1, s, ||y||) + R_1^2 - ||y||^2}\right), \end{aligned} \tag{C.14}$$

where the last step follows from

$$\lim_{r\to 0} \arctan \frac{\sqrt{s}+\psi(r,s,||y||)}{\eta(r,s,||y||)+r^2-||y||^2} = \lim_{r\to 0} \arctan \frac{\sqrt{s}+\sqrt{2s}}{||y||^2+r^2-||y||^2} = \arctan\infty = \frac{\pi}{2}.$$

Similarly, applying Identity 1, we can rewrite C_α as

$$C_4 = \frac{\pi\sqrt{s}}{2i} \int_{R_1}^{R_2} \frac{2rP(r)\mathrm{d}r}{\sqrt{\mathcal{C}_1}} - \frac{2rP(r)\mathrm{d}r}{\sqrt{\mathcal{C}_2}}, \tag{C.15}$$

For Policy E, $P(r) = p \in [0,1]$. Then,

$$C_4 = -p\pi\sqrt{s} \arctan \frac{\sqrt{s}+\psi(r,s,||y||)}{\eta(r,s,||y||) + r^2 - ||y||^2}\Bigg|_{r=R_1}^{R_2}. \tag{C.16}$$

Substituting (C.16) and (C.14) into (5.9) in Section 5.2, and then substituting (5.9) into (5.8) yields the Laplace transform of $I(y)$ under Policy E for $\alpha = 4$.

Next, $P(r)$ can be written as $P(r) = u + vr^4$, where $u = -\frac{R_1^4}{R_2^4 - R_1^4}$, $v = \frac{1}{R_2^4 - R_1^4}$ for

Policy I, and $u = \frac{R_2^4}{R_2^4 - R_1^4}$, $v = -\frac{1}{R_2^4 - R_1^4}$ for Policy D . Hence,

$$\begin{aligned} C_4 &= \frac{\pi\sqrt{s}}{2i} \int_{R_1}^{R_2} \frac{2r(u+vr^4)\mathrm{d}r}{\sqrt{\mathcal{C}_1}} - \frac{2r(u+vr^4)\mathrm{d}r}{\sqrt{\mathcal{C}_2}}\mathrm{d}r \\ &\overset{t\leftrightarrow r^2}{=} \frac{\pi\sqrt{s}}{2i} \int_{R_1}^{R_2} \frac{(u+vt^2)\mathrm{d}t}{\sqrt{t^2 - 2(i\sqrt{s} + ||y||^2)t + (||y||^2 - i\sqrt{s})^2}} \\ &\quad - \frac{(u+vt^2)\mathrm{d}t}{\sqrt{t^2 + 2(i\sqrt{s} - ||y||^2)t + (||y||^2 + i\sqrt{s})^2}}, \end{aligned} \tag{C.17}$$

Next, we have

$$\begin{aligned} &\int \frac{(u+vt^2)\mathrm{d}t}{\sqrt{t^2 - 2(i\sqrt{s} + ||y||^2)t + (||y||^2 - i\sqrt{s})^2}} \\ &= u \int \frac{\mathrm{d}t}{\sqrt{t^2 - 2(i\sqrt{s} + ||y||^2)t + (||y||^2 - i\sqrt{s})^2}} \\ &\quad + v \int \frac{t^2\mathrm{d}t}{\sqrt{t^2 - 2(i\sqrt{s} + ||y||^2)t + (||y||^2 - i\sqrt{s})^2}} \\ &\overset{(g)}{=} \frac{v}{2}(r^2 + 3||y||^2 + 3i\sqrt{s})(\eta - i\psi) \\ &\quad + (u + v||y||^4 - vs + i4v\sqrt{s}||y||^2) \ln\left[\sqrt{\mathcal{C}_1} + r^2 - (i\sqrt{s} + ||y||^2)\right], \end{aligned} \tag{C.18}$$

where the last step follows after applying Identity 3 in Appendix C.1 and substituting t with r^2. Similarly, we have

$$\begin{aligned} &\int \frac{(u+vt^2)\mathrm{d}t}{\sqrt{t^2 + 2(i\sqrt{s} - ||y||^2)t + (||y||^2 + i\sqrt{s})^2}} \\ &= \frac{v}{2}(r^2 + 3||y||^2 - 3i\sqrt{s})(\eta + i\psi) \\ &\quad + (u + v||y||^4 - vs - i4v\sqrt{s}||y||^2) \ln\left[\sqrt{\mathcal{C}_2} + r^2 - (i\sqrt{s} + ||y||^2)\right]. \end{aligned} \tag{C.19}$$

Thus, substituting (C.18) and (C.19) into (C.17) and then conducting some alge-

braic manipulations yields

$$C_4 = 2\pi vs||y||^2 \ln\left[(\eta(r,s,||y||)+r^2-||y||^2)^2+(\sqrt{s}+\psi(r,s,||y||))^2\right] \quad \text{(C.20)}$$
$$-\pi\sqrt{s}\left\{\frac{v}{2}\left[(r^2+3||y||^2)\psi(r,s,||y||)-3\sqrt{s}\eta(r,s,||y||)\right]\right.$$
$$\left.+(u+v||y||^4-vs)\arctan\frac{\sqrt{s}+\psi(r,s,||y||)}{\eta(r,s,||y||)+r^2-||y||^2}\right\}\Bigg|_{r=R_1}^{R_2}.$$

Finally, we substitute (C.14) and (C.20) into (5.9) in Section 5.2, and then substitute (5.9) into (5.8) to obtain the Laplace transform of $I(y)$ under Policy I and Policy D for $\alpha = 4$.

C.4 Probability Density Function of R_{z^*}

The complementrary cdf of $\bar{F}_{R_{z^*}}(r_{e^*})$ of the random distance R_{z^*} equals the probability that no eavesdroppers are in $\mathcal{B}(o, r_{e^*})$ for $0 \le r_{e^*} \le D$. Hence, the cdf of R_{z^*} is given by

$$\begin{aligned}
F_{R_{z^*}}(r_{e^*}) &= 1-\bar{F}_{R_{z^*}}(r_{e^*}) \\
&= 1-\mathbb{P}\left(\Phi_E(\mathcal{B}(o,r_{e^*}))=0\right) \\
&= 1-\sum_{n=0}^{\infty}\mathbb{P}\left(\Phi_E(\mathcal{B}(o,r_{e^*}))=0\middle|\Phi_E(\mathcal{B}(o,D))=n\right)\mathbb{P}(\Phi_E(\mathcal{B}(o,D))=n) \\
&= 1-\sum_{n=0}^{\infty}\left(1-\frac{r_{e^*}^2}{D^2}\right)^n\frac{(\lambda_e\pi D^2)^n\exp(-\lambda_e\pi D^2)}{n!} \\
&= 1-\exp(-\lambda_e\pi D^2)\sum_{n=0}^{\infty}\left(1-\frac{r_{e^*}^2}{D^2}\right)^n\frac{(\lambda_e\pi D^2)^n}{n!} \\
&= 1-\exp(-\lambda_e\pi D^2)\exp\left[\left(1-\frac{r_{e^*}^2}{D^2}\right)\lambda_e\pi D^2\right] \\
&= 1-\exp(-\lambda_e\pi r_{e^*}^2), \qquad \text{(C.21)}
\end{aligned}$$

for $0 \leq r_{e^*} \leq D$. Therefore, the pdf of R_{z^*} is given by

$$f_{R_{z^*}}(r_{e^*}) = \begin{cases} 2\lambda_e \pi r_{e^*} \exp(-\lambda_e \pi r_{e^*}^2), & 0 \leq r_{e^*} \leq D \\ 0, & \text{otherwise} \end{cases}.$$

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] T. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2001.

[2] A. Goldsmith, *Wireless Communications*. New York, NY, USA: Cambridge University Press, 2005.

[3] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[4] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in *Wireless Network Security*. Springer, 2007, pp. 103–135.

[5] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *Commun. Surveys Tuts.*, vol. 8, no. 2, pp. 2–23, Apr. 2006.

[6] T. Karygiannis and L. Owens, "Wireless network security," *NIST special publication*, vol. 800, p. 48, 2002.

[7] W. Stallings, *Cryptography and network security: principles and practice*, 5th ed. Prentice Hall, January 2010.

[8] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proc. IEEE FOCS*, 1994, pp. 124–134.

[9] R. K. Nichols and P. C. Lekkas, *Wireless security*. McGraw-Hill New York, 2002.

[10] M. Bloch and J. Barros, *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[11] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts*, vol. 16, no. 3, pp. 1550–1573, 2014.

[12] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5g wireless communication networks using physical layer security," *Communications Magazine, IEEE*, vol. 53, no. 4, pp. 20–27, 2015.

[13] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[14] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[15] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. R. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 16–28, Sept 2013.

[16] Y.-W. Hong, P.-C. Lan, and C.-C. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sept 2013.

[17] E. Tekin and A. Yener, "The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, June 2008.

[18] J. Huang and A. Swindlehurst, "Cooperative jamming for secure communications in mimo relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, 2011.

[19] X. He and A. Yener, "Providing secrecy with structured codes: Two-user gaussian channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 4, pp. 2121–2138, April 2014.

[20] J. Xie and S. Ulukus, "Secure degrees of freedom of one-hop wireless networks," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3359–3378, June 2014.

[21] I. Krikidis, J. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, 2009.

[22] R. Bassily and S. Ulukus, "Deaf cooperation and relay selection strategies for secure communication in multiple relay networks," *IEEE Trans. Signal Process.*, vol. 61, no. 6, pp. 1544–1554, 2013.

[23] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. A. Chambers, "Max-ratio relay selection in secure buffer-aided cooperative wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 719–729, April 2014.

[24] J. Huang and A. Swindlehurst, "Buffer-aided relaying for two-hop secure communication," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 152–164, Jan 2015.

[25] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas i: The misome wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[26] ——, "Secure transmission with multiple antennas – part ii: The mimome wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov 2010.

[27] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532–3545, 2012.

[28] H. M. Wang, F. Liu, and X. G. Xia, "Joint source-relay precoding and power allocation for secure amplify-and-forward mimo relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 8, pp. 1240–1250, Aug 2014.

[29] A. Thangaraj, S. Dihidar, A. Calderbank, and S. Mclaughlin, "Applications of ldpc codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, 2007.

[30] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[31] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, Oct 2011.

[32] S. Vasudevan, D. Goeckel, and D. Towsley, "Security-capacity trade-off in large wireless networks using keyless secrecy," in *Proc. ACM MobiHoc*, 2010, pp. 21–30.

[33] X. Zhou, M. McKay, B. Maham, and A. Hjrungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, March 2011.

[34] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 29, pp. 2067–2076, 2011.

[35] A. Sheikholeslami, D. Goeckel, H. Pishro-Nik, and D. Towsley, "Physical layer security from inter-session interference in large wireless networks," in *Proc. IEEE INFOCOM*, 2012, pp. 1179–1187.

[36] Y. Shen, X. Jiang, and J. Ma, "Flexible relay selection for secure communication in two-hop wireless networks," in *WiOpt Workshop*, 2013, pp. 648–651.

[37] C. Cai, Y. Cai, X. Zhou, W. Yang, and W. Yang, "When does relay transmission give a more secure connection in wireless ad hoc networks?" *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 624–632, April 2014.

[38] Z. Ho, E. Jorswieck, and S. Engelmann, "Information leakage neutralization for the multi-antenna non-regenerative relay-assisted multi-carrier interference channel," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1672–1686, September 2013.

[39] C. Wang, H. M. Wang, D. W. K. Ng, X. G. Xia, and C. Liu, "Joint beamforming and power allocation for secrecy in peer-to-peer relay networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 6, pp. 3280–3293, June 2015.

[40] S. Vasudevan, S. Adams, D. Goeckel, Z. Ding, D. Towsley, and K. Leung, "Multi-user diversity for secrecy in wireless networks," in *Proc. IEEE ITA*, Jan 2010, pp. 1–9.

[41] J. Zhang, L. Fu, and X. Wang, "Asymptotic analysis on secrecy capacity in large-scale wireless networks," *IEEE/ACM Trans. Netw.*, vol. 22, no. 1, pp. 66–79, Feb 2014.

[42] M. Mirmohseni and P. Papadimitratos, "Scaling laws for secrecy capacity in cooperative wireless networks," in *Proc. IEEE INFOCOM*, April 2014, pp. 1527–1535.

[43] T. Yang, G. Mao, and W. Zhang, "Connectivity of wireless information-theoretic secure networks," in *Proc. IEEE GLOBECOM*, Dec 2014, pp. 317–323.

[44] M. Ghaderi, D. Goeckel, A. Orda, and M. Dehghan, "Minimum energy routing and jamming to thwart wireless network eavesdroppers," *IEEE Trans. Mobile Comput.*, vol. 14, no. 7, pp. 1433–1448, July 2015.

[45] M. Khandaker and K.-K. Wong, "Masked beamforming in the presence of energy-harvesting eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 40–54, 2015.

[46] J. Yang, I.-M. Kim, and D. I. Kim, "Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2840–2852, June 2013.

[47] J. Bai, X. Tao, J. Xu, and Q. Cui, "The secrecy outage probability for the i th closest legitimate user in stochastic networks," *IEEE Commun. Lett.*, vol. 18, no. 7, pp. 1230–1233, July 2014.

[48] G. Geraci, S. Singh, J. Andrews, J. Yuan, and I. Collings, "Secrecy rates in broadcast channels with confidential messages and external eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2931–2943, May 2014.

[49] N. Kayastha, D. Niyato, P. Wang, and E. Hossain, "Applications, architectures, and protocol design issues for mobile social networks: A survey," *Proceedings of the IEEE*, vol. 99, no. 12, pp. 2130–2158, 2011.

[50] Y. Zhang, E. Pan, L. Song, W. Saad, Z. Dawy, and Z. Han, "Social network aware device-to-device communication in wireless networks," *Wireless Communications, IEEE Transactions on*, vol. 14, no. 1, pp. 177–190, 2015.

[51] K. Wei, X. Liang, and K. Xu, "A survey of social-aware routing protocols in delay tolerant networks: Applications, taxonomy and design-related issues," *Communications Surveys Tutorials, IEEE*, vol. 16, no. 1, pp. 556–578, 2014.

[52] F. Xia, L. Liu, J. Li, J. Ma, and A. Vasilakos, "Socially aware networking: A survey," *Systems Journal, IEEE*, vol. 9, no. 3, pp. 904–921, 2015.

[53] L. Wang, C. Cao, and H. Wu, "Secure inter-cluster communications with cooperative jamming against social outcasts," *Computer Communications*, vol. 63, pp. 1–10, 2015.

[54] L. Tang, H. Chen, and Q. Li, "Social tie based cooperative jamming for physical layer security," *Communications Letters, IEEE*, vol. 19, no. 10, pp. 1790–1793, 2015.

[55] J. Kleinberg, "The small-world phenomenon: An algorithmic perspective," in *Proceedings of the Thirty-second Annual ACM Symposium on Theory of Computing*, ser. STOC '00, 2000, pp. 163–170.

[56] H. Inaltekin, M. Chiang, and H. V. Poor, "Delay of social search on small-world graphs," *The Journal of Mathematical Sociology*, vol. 38, no. 1, pp. 1–46, 2014.

[57] A. Bletsas, S. Khisti, D. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 3, pp. 659–672, Mar. 2006.

[58] M. Shaked and J. Shanthikumar, *Stochastic orders*, 1st ed., ser. Springer Series in Statistics. Springer, Nov. 2010.

[59] A. Klenke and L. Mattner, "Stochastic ordering of classical discrete distributions," *Advances in Applied Probability*, vol. 42(2), pp. 393–410, 2010.

[60] C++ simulator for two-hop transmission with cooperative jamming and opportunistic relaying. [Online]. Available: http://mdlval.blogspot.jp/

[61] A. Rawat, O. Koyluoglu, N. Silberstein, and S. Vishwanath, "Optimal locally repairable and secure codes for distributed storage systems," *IEEE Trans. Inf. Theory*, vol. 60, no. 1, pp. 212–236, Jan 2014.

[62] C. M. Ramsay, "The distribution of sums of certain i.i.d. pareto variates," *Communications in Statistics - Theory and Methods*, vol. 35, no. 3, pp. 395–405, 2006.

[63] M. Abramowitz and I. Stegun, *Handbook of mathematical functions: with formulas, graphs, and mathematical tables*, ser. Applied mathematics series. U.S. Department of Commerce, National Bureau of Standards, 1972.

[64] C++ simulator for two-hop transmission with colluding eavesdroppers. [Online]. Available: http://mdlval.blogspot.jp/

[65] S. Chiu, D. Stoyan, W. Kendall, and J. Mecke, *Stochastic Geometry and Its Applications*, 3rd ed. Wiley, 2013.

[66] M. Haenggi and R. K. Ganti, "Interference in large wireless networks," *Found. Trends Netw.*, vol. 3, no. 2, pp. 127–248, 2009.

[67] X. Zhou, R. Ganti, J. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, 2011.

[68] C++ simulator for friendship-based cooperative jamming in poisson networks. [Online]. Available: http://mdlval.blogspot.jp/

[69] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 6th ed. New York: Academic Press, 2000.

[70] R. Tanbourgi, H. Jäkel, and F. K. Jondral, "Interference in poisson networks with isotropically distributed nodes," *arXiv preprint arXiv:1211.4755*, 2012.

Publications

Jounal Articles

[1] Yuanyu Zhang, Yulong Shen, Jinxiao Zhu and Xiaohong Jiang. Eavesdropper-tolerance capability in two-hop wireless networks via cooperative jamming. *Ad Hoc and Sensor Wireless Networks* 29(1-4): 113-131 (2015).

[2] Yuanyu Zhang, Yulong Shen, Hua Wang, Yanchun Zhang and Xiaohong Jiang. On secure wireless communications for service oriented computing. *IEEE Transactions on Services Computing*, Published online: Sept.14, 2015. DOI:10.1109/TSC.2015.2478453.

[3] Yuanyu Zhang, Yulong Shen, Hua Wang and Xiaohong Jiang. On secure wireless communications for IoT under eavesdropper collusion. *IEEE Transactions on Automation Science and Engineering*, vol. 13, no. 3, pp. 1281-1293, July 2016.

[4] Yuanyu Zhang, Yulong Shen, Hua Wang and Xiaohong Jiang. Friendship-based cooperative jamming for secure communication in poisson networks. *Submitted.*

[5] Yulong Shen, Yuanyu Zhang. Transmission protocol for secure big data in two-hop wireless networks with cooperative jamming. *Information Sciences*, 281: 201-210 (2014).

[6] Yulong Shen, Yuanyu Zhang. Exploring relay cooperation for secure and reliable transmission in two-hop wireless networks. *EAI Endorsed Trans. Scalable Information Systems* 1(2): e2 (2014).

Conference Papers

[7] Yuanyu Zhang, Yulong Shen and Xiaohong Jiang. Eavesdropper Tolerance Capability Study in Two-Hop Cooperative Wireless Networks. 2nd IEEE/CIC International Conference on Communications in China (ICCC), 2013, pp. 219-223.

[8] Yuanyu Zhang, Yulong Shen, Yuezhi Zhou, and Xiaohong Jiang. Eavesdropper-Tolerance Capability of Two-Hop Wireless Networks with Cooperative Jamming and Opportunistic Relaying. The 9th FTRA International Conference on Future Information Technology (FutureTech 2014), vol. 309, pp. 145-150.

[9] Bo Liu, Yuanyu Zhang, Xiaohong Jiang, and Zhenqiang Wu. An Energy-Efficient Data Collection Scheme in Body Area Nanonetworks. 2015 Third International Symposium on Computing and Networking (CANDAR), pp. 240-245. IEEE, 2015.

[10] Xuning Liao, Zhenqiang Wu, Yuanyu Zhang and Xiaohong Jiang. The Delay-Security Trade-Off in Two-Hop Buffer-Aided Relay Wireless Network. 2016 International Conference on Networking and Network Applications (NaNA), Hakodate, 2016, pp. 173-177.