Protocol Design and Performance Analysis for Covert Communications in Relay-Assisted Wireless Systems

by

Chan Gao

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Graduate School of Systems Information Science)
in Future University Hakodate
September 2021

To my family

ABSTRACT

Protocol Design and Performance Analysis for Covert Communications in
Relay-Assisted Wireless Systems

by

Chan Gao

With the rapid evolution of wireless communication technologies and the wide coverage of wireless hotspots, wireless systems are of paramount importance to provide ubiquitous wireless connectivity for lots of critical applications in daily life. However, security and privacy are critical in existing and future wireless systems since a large amount of confidential information (e.g., credit card information, physiological information for e-health) is transferred over the open wireless channels. How to guarantee information security has attracted increasing concerns from both academia and industry recently. Covert communication is a potential technique to prevent adversaries from detecting the existence of transmissions among both sides of the communication. Therefore, this thesis focuses on the protocol design and performance analysis for covert communications in the fundamental relay-assisted wireless systems.

We first investigate the covert communication in a two-hop wireless communication system with multiple relays, where a message is first transmitted from its source to a selected relay and then forwarded by the relay to its destination under the detec-

tion of a passive warden. We explore in detail the relay selection protocol design issue for this system. For evaluating the performance of covert communication, we develop a theoretical framework to analyze the transmission outage probability, the detection error probability of warden, and covert capacity based on a relay selection protocol proposed. We also explore covert capacity maximization through efficient numerical searches under a given covertness requirement. Finally, extensive simulation and numerical results are provided to illustrate our theoretical findings and the performance of covert communication in two-hop wireless communication systems with multiple relays.

We then introduce cooperative jamming technology into relay-assisted wireless systems to interfere with the warden. In order to determine the forward relay and the jammer, we illustrate a new relay/jammer selection protocol in such systems. In order to explore the impact of cooperative jamming on the performance of covert communication, we introduce a jam-generating threshold into the theoretical framework and we further derive the expressions for three performance metrics, i.e., transmission outage probability, the detection error probability of warden, and covert capacity. We also explore covert capacity maximization through efficient numerical searches under given covertness and outage requirements. Finally, we present extensive simulation and numerical results to validate our theoretical results, as well as to demonstrate that cooperative jamming can confuse the warden well to improve the performance of covert communication.

We further extend our study to a scenario where the warden will actively attack the communication process as a jammer in relay-assisted wireless systems. We redefine the behavior of the warden that it will perform detection and jamming throughout the covert communication process. Notice that the transmitter has to increase the transmission power to ensure successful decoding due to the jamming of the warden, and thus increases the risk of being detected. To deeply understand such interactions,

based on the related relay selection protocol designed previously, we develop a new theoretical framework to analyze the transmission outage probability, the detection error probability of warden, and covert capacity. Then, we optimize the covert capacity through power control under given covertness and outage requirements. Finally, extensive simulation and numerical results are provided to illustrate our theoretical findings and the performance of covert communication with an active warden in such systems.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my advisor Professor Xiaohong Jiang. He pointed out the research direction for my study, and invested a lot of time and energy to grant me more research methods and important skills, which not only have comprehensively improved my theoretical knowledge and practical ability but also broadened my horizons. He also taught me how to become a better researcher and how to become a better person with his personality charm in my life. I would also like to thank Professor Jiang's wife, Mrs Li, for her meticulous care and support for my life in Hakodate.

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 help me to greatly improve this thesis but also inspire me to widen the area of my future research. I would also like to thank Professor Bin Yang of Chuzhou University, China, who helped me a lot in improving both the quality and the clarity of dissertation research.

My thanks also go to other members in our laboratory Ahmed Salem, Shuangrui Zhao, Ranran Sun, Yeqiu Xiao, Xiaolan Liu, Xiaochen Li, Pingchang Zhang, Wenhao Zhang, Ji He and Huihui Wu, for their contributions in some way to this thesis.

Last but not the least, I would like to thank my family: my parents and husband. 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

CHAPTER I

Introduction

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

1.1 Security in Wireless Communication

With the rapid development of wireless communication technology and large-scale coverage of wireless hotspots, the proliferation of wireless user devices such as s-mart phones, PDAs, laptops, etc., is indispensable in our daily life. During the past decades, wireless communication infrastructure and services have been proliferating with the goal of satisfying the rapidly increasing demands of users [1]. According to the latest publications by the International Telecommunications Union in 2021, 75 percent of the total world population had an active mobile broadband subscription [2]. Such a large-scale application demand gave birth to the Internet of Things (IoT) networks. The recent advances in hardware and information technology have accelerated the deployment of billions of interconnected, smart and adaptive devices in critical infrastructures like health, transportation, environmental control, and home automation[3], which has brought the world into the era of the IoT. The rise of IoT is driving the technology development of the fifth-generation (5G) cellular networks

[4], which has led to an unprecedented increase in the utilization rate of wireless networks. However, this fact leads to an enormous amount of sensitive and confidential information transmitted via wireless channels [5].

Due to the broadcast nature of the wireless mediums, the open communication environment makes wireless transmissions more vulnerable to malicious attacks than wired communication, including the passive eavesdropping for data interception and the active interference for transmission process. The attackers can extract users sensitive information for commercial and military transactions, resulting in global users' privacy exposure. According to a new survey of [6], nearly 330 million people from 10 countries have experienced cybercrime in the last 12 months and spent 2.7 billion hours dealing with the aftermath because the wireless devices were abused for illegal cybercriminal activities, including malicious attacks, computer hacking, data forging, financial information theft, and online bullying/stalking etc. Therefore, improving the security of wireless communication to fight against cybercriminals is crucial, because more and more people are using wireless networks (e.g., cellular networks and Wi-Fi) for online activities.

Wireless networks generally employ the Open Systems Interconnection (OSI) protocol architecture [7], consisting of the application layer, transport layer, network layer, MAC layer, and physical layer [8]. There are relevant security measures at each layer to ensure security requirements, including the authenticity, confidentiality, integrity and availability [9]. Traditionally, cryptography technology plays a critical role in the security of wireless networks because it is widely used in the protection of sensitive data. Although cryptography technology can satisfy the security requirements mentioned above, the demand for computing power is very strict. The process of encryption and decryption of sensitive data may cause network delays. With the continuous improvement of computer power, it has become possible to crack cryptography algorithms. In 2004, Chinese cryptography expert Xiaoyun Wang deciphered the MD5 algorithm which was widely used on computers [10]. After that, she also challenged other cryptographic algorithms. In order to guarantee the authenticity of the transmitter or receiver, existing wireless networks typically employ multiple authentication approaches simultaneously at different protocol layers [11].

It becomes obviously that exploiting multiple authentication mechanisms at different protocol layers is capable of enhancing wireless security, but the corresponding costs in term of computational complexity and latency are high. Recently, physical layer (PHY) security is emerging as a promising method of protecting wireless communications to achieve information-theoretic security against eavesdropping attacks. The philosophy behind PHY security is to exploit the natural randomness of noise and the physical characteristics of wireless channels to provide information-theoretic security, which has been regarded as the potential and valuable form of security irrespective of the computing capabilities of eavesdroppers [12, 13].

1.2 Physical Layer Security

The first study of information-theoretic security is Shannon's research in 1949 [14], which also marked the premier work on PHY security. Subsequently, Wyner considered a system with discrete memoryless wiretap channels in the work [15]. His result has proved that as long as the channel capacity from the source to the destination is higher than that from the source to the eavesdropper, information-theoretically secure communication is possible without using any secret keys. Then, the result of Wyner was extended to the general wiretap channels by Csiszár and Körner in [16]. Their results have uncovered the fact that information-theoretically secure communication between legitimate users is achievable by employing the inherent randomness of the wireless medium. Then, in the study [17], Wyner's result was extended from the discrete memoryless wiretap channel to the Gaussian wiretap channel, where the concept of secrecy capacity was established. They illustrated that secrecy capacity is equal to the difference between the channel capacity of the transmission link and that of the wiretap link. According to these studies in [18, 19], it has been demonstrated that transmission will become insecure if secrecy capacity drops below zero, which means that eavesdroppers will be able to intercept the message from the source. Moreover, the research of PHY security was extended to various wireless channel models such as multi-antenna channel [20] and relay channel [21], etc. Based on the previous studies mentioned above, in order to improve the security of wireless communications, diverse approaches have been proposed in the literature, which mainly include channel security-oriented beamforming [22–25], cooperative jamming [26–29], channel coding [30–32] and cooperative relaying [33–41].

The security-oriented beamforming technology based on multi-antenna signal processing allows the source to transmit the decoded signal in a particular direction to the legitimate receiver. Therefore, the signal received at the eavesdropper will experience destructive interference because it usually stays another direction that is different from the legitimate receiver. This phenomenon will weaken the ability of the eavesdropper. Thus, beamforming technology enhances the security of wireless networks very well. The authors in [22] demonstrated that the beamforming technique improves the secrecy capacity significantly based on the protocol design of orthogonal/non-orthogonal spectrum allocation in heterogeneous networks. Beamforming applications not only maximize the secrecy capacity of all users but also guarantee energy efficiency (SEE) with the energy harvesting constraints [23, 24]. The work in [25] also considered the PHY security enhancement of wireless networks by combining beamforming technology and artificial noise to prevent eavesdropping attacks. However, in practical applications, the beamforming design needs to be adjusted according to the channel state information (CSI). Actually, CSI of the message channel is usually not perfect. Moreover, to achieve the transmission strategy, the cooperation of the source node and the relay node is essential, which often leads to relatively high resource costs in a wireless network with a large number of nodes.

Cooperative jamming is a very important PHY security technology and is usually used in wireless networks with untrusted relays. It achieves secure communication by using artificial jamming signals from helpers nodes to interfere with eavesdroppers. According to the type of jammer distribution, cooperative jamming is divided into two categories. The first one is cooperative jamming with independent identically distributed (i.i.d) Gaussian signals, such as the works in [26, 27]. This method was originally proposed for a multiple access wiretap channel system, where multiple legitimate users hoped to conduct secure communication with target receivers in the presence of eavesdroppers. The second one is based on the potential necessity of channel prefixing and adopts the structured signals, where the jamming signals can be nulled out at the intended receiver [28]. We can conclude that the main difference between cooperative jamming with Gaussian signals and that with structured signals is that, in the latter, the legitimate user decodes jamming signals, and then receives pure message signals, while the eavesdropper's channel still interferes with jamming signals. However, there are still many issues in practical applications. Cooperative jamming requires the relays that serve as jammers to send jamming signals unselfishly, which is a challenge in large wireless networks. This is because the resource at every node is not unlimited, so each node usually serves itself firstly. In addition, the jamming signal not only affects the eavesdropper but also reduces the decoding rate of the receiver.

Channel coding randomly maps each message to one of several codewords to confuse the eavesdropper and improve the security capacity. In [30], the authors showed that achieving more secrecy capacity with any wiretap channel was feasible by using codes with low-density parity-check (LDPC). The authors in work [31] designed an explicit polynomial-time encoding/decoding algorithm and proved that polar codes can be used to improve the secrecy capacity under binary symmetric and deterministic wiretap channels. Recently, channel coding research has been extended to the design of resilient codes for distributed data and cloud storage systems. The work [32] studied the problem of securing distributed storage systems (DSS) against eavesdroppers and malicious adversaries. Then a bound of the secrecy capacity with secure cooperative regenerating codes was established. Although the channel coding technology notably improves the security performance, the construction of the codebook is difficult. In practical applications, each node must be trusted to ensure that the codebook is not leaked. Furthermore, similar to the other PHY security technologies, channel coding also requires the CSI of the eavesdropping channel, which is difficult to achieve.

Cooperative relaying technology aims to improve the security of wireless networks by selecting the transmission links with strong legitimate channels and weak eavesdropping channels. Based on the buffer states of relays, cooperative relaying is divided into two categories, i.e., forward relaying [33–35], and buffer-aided relaying [36–41]. For forward relaying, the max-min principle is the basic scheme of relay selection, which means that the transmission link is selected to maximize the minimum instantaneous secrecy capacity within the two-hop links. As such, the whole transmission process is completed in two consecutive time slots, the source transmits the message to the relay in the first time slot, and the relay forwards the message to the destination in the second time solt. For the buffer-aided relaying, the system can choose to store or transmit information when it is beneficial to itself according to the state of the transmission link, thereby improving the flexibility, throughput, and diversity of the network. Thus, there are three processes of whole transmission, consisting of the source-relay transmission process, the queuing process, and the relay-destination transmission process. Unlike the other PHY security technologies mentioned previously, cooperative relaying is easy to implement because it does not require complex transmission technologies or explicit synchronization procedures. In addition, the cooperative relaying can be flexibly designed according to the CSI of the eavesdropping channel.

In general, both cryptography and PHY security technologies have greatly improved the security of wireless networks. However, the current works on secure communication mainly focused on protecting the content of communication from being attacked. Adversaries still can detect the existence of transmissions among users and even attack them. Therefore, it is not determined as absolute security that the content of the communication is not attacked. Covert communication is a potential technology to prevent adversaries from detecting the existence of transmissions among both sides of the communication. The purpose of covert communication is to ensure that communications are not detected by the warden. Therefore, the research of covert communication has attracted much attention in academia and industry [42].

1.3 Objective and Main Works

This thesis focuses on the protocol design and performance analysis for covert communication in relay-assisted wireless systems. Our objective is to explore the covert communication performances in such systems. Towards this end, we first explore the relay selection protocol design for covert communication in a two-hop wireless communication system with multiple relays and a passive warden. We also conduct a theoretical analysis to derive the corresponding performance metrics. We then introduce cooperative jamming technology into such systems to interfere with the warden and design the related relay/jammer selection protocol. Next, the theoretical analysis is provided to demonstrate the impact of cooperative jamming on covert capacity. We further extend our study to the scenario where the warden will actively attack the communication process as a jammer in such systems.

1.3.1 Covert Communication in Wireless Systems with Multiple Relays

This work focuses on the performance analysis for covert communication in a two-hop wireless communication system with multiple relays. The existing works on the performance of covert communication mainly focus on the two scenarios of one hop or two hops with the help of a single relay (Please refer to Section 2.2 for related works). The former scenario consists of a transmitter, a receiver, and a warden, while for the latter one, there is a relay besides the three nodes. These works show that the relay can significantly improve the covet performance in terms of detection error probability of warden and covert capacity (Please refer to Section 2.1 for related works). However, the above works only consider a simple scenario with no relay or a single relay. Therefore, a challenging issue of relay selection arises in two-hop wireless systems with multiple relays for improving the covert communication performance. This work serves as a first step towards the study of covert communication in a two-hop wireless communication system with multiple relays. We explore the relay selection protocol design for covert communication with a passive warden and conduct a theoretical analysis to derive the corresponding achievable covert capacity. The main contributions of this work can be summarized as follows:

- We first design the relay selection protocol (i.e., random relaying scheme and superior relaying scheme) in a relay-assisted wireless system, where the source needs to transmit two types of messages (i.e., legitimate message and covert message).

- Under the random relaying scheme, we first examine the transmission strategy design for the source and determine the detection error probability at the warden according to the probabilities of the false alarm and missed detection. We then optimize the transmit power of the source to maximize the covert capacity under a given covertness requirement.

- Under the superior relaying scheme, we first examine the transmission strategy design for the source and thus define the necessary condition that the source can transmit the covert message. We then derive the detection error probability of the warden according to the probabilities of the false alarm and missed detection. We further explore covert capacity maximization through efficient numerical searches under a given covertness requirement.

- Finally, numerical results are provided to illustrate the impact of system parameters on the detection error probability and covert capacity, and also to reveal our findings.

1.3.2 Cooperative Jamming based Covert Communication in Relay-Assisted Wireless Systems

Extensive research efforts have been devoted to exploring the PHY security performance of wireless networks by using the cooperative jamming technology in terms of the scaling laws of secrecy capacity and secure transmission probability, etc (Please refer to Section 2.2 for related works). The existing works on the performance of covert communication mainly focus on the two scenarios of one hop or two-hop with the help of a single relay. Hence, the impact of cooperative jamming on the performance of covert communication still remains largely unknown in wireless communication systems with multiple relays. Although we have extended our work to wireless systems with multiple relays in the first work, the performance analysis of covert communication with cooperative jamming remains a technique challenge. This is because such performance 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 (SINR) received at all the jammers. The main contributions of this work are summarized as follows:

- We first design a new relay/jammer selection protocol in a wireless communication system with multiple relays, where the source needs to select a relay to forward the message and some other relays as jammers to confuse the warden based on a jam-generating threshold α.

- We further derive the expressions for three performance metrics, i.e., transmission outage probability, the detection error probability of warden, and covert capacity. Then we explore covert capacity maximization through efficient numerical searches under given covertness and outage requirements.

- Finally, we present extensive simulation and numerical results to validate our theoretical results, and to demonstrate that cooperative jamming can confuse the warden well to improve the performance of covert communication.

1.3.3 Covert Communication in Relay-Assisted Wireless Systems with an Active Warden

Due to the rapid development of wireless network technology, the malicious means of attackers have also become diversified. Available works on the security of wireless networks are no longer limited to propose security recommendations for users. More and more researchers have focused on how to deal with stronger attackers. Therefore, in the study of covert communication, we should consider the attack capability of the warden. This work studies the performance of covert communication in the scenario where the warden will actively attack the communication process as a jammer in a relay-assisted wireless system. It is worth noting that due to the jamming signal of the warden, the transmitter must increase the transmission power to ensure successful decoding, thus increasing the risk of being detected. Moreover, the warden also generates self-interference while it sends jamming signals. The main contributions of this work are summarized as follows:

- We extend our study to a relay-assisted wireless system where the warden works in full-duplex (FD) mode and actively attacks the communication process as a jammer. We redefine the behavior of the warden that it performs detection and jamming throughout the covert communication process.

- Then, we analyze the transmission outage probability, the detection error probability of warden, and covert capacity. Next, we optimize the covert capacity through power control under given covertness and outage requirements.

- Finally, we present extensive simulation and numerical results to validate our theoretical results.

1.4 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 covert communication performance study in wireless communication systems with multiple relays. Chapter IV presents the work on covert communication performance study in relay-assisted wireless communication systems with the help of cooperative jamming and Chapter V introduces the work regarding an active warden in relay-assisted wireless communication systems. Finally, we conclude this thesis in Chapter VI.

1.5 Notations

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

Table 1.1: Main notations

Symbol	Definition
S	Source node

D	Destination node
$Willie$	Warden node
R_k	The i-th relay
R_b	Selected message relay
R_j	Selected jamming relay
n	Number of relays
l	Number of jamming relays
m	Number of channel uses
σ_i^2	Noise variance of node i
$\|h_{i,j}\|^2$	Channel gain between nodes i and j
exp	Exponential function
ln	Logarithmic function
$\mathbb{E}[\cdot]$	Expectation operator
$\mathbb{P}(\cdot)$	Probability operator
$f(\cdot)$	Probability-density-function (PDF)
$\Gamma(\cdot)$	Gamma distribution
P_i	Covert message transmit power of node i
P_i^*	Optimal covert message transmit power of node i
$\gamma_i^{'}$	Signal-to-noise (SNR) at node i
γ_i	Signal-to-interference ratio (SINR) at node i
$P_i^{'}$	Legitimate message transmit power of node i
P_{max}	Maximum transmit power constraint
$Q_{i,j}$	Transmission rate between nodes i and j
C	Channel capacity
CSI	Channel state information
$C_{i,j}$	Channel capacity between nodes i and j
C_c	Covert capacity

C_{c1}	Covert capacity for random relaying scheme
C_{c2}	Covert capacity for superior relaying scheme
C^*	Maximum covert capacity
C_1^*	Maximum covert capacity for random relaying scheme
C_2^*	Maximum covert capacity for superior relaying scheme
H_0	The node isn't sending covert message
H_1	The node is sending covert message
FA	False alarm
MD	Missed detection
α	Jam-generating threshold
λ	Detection threshold
ζ	Total detection error probability (TDP)
$\zeta^\dagger$	The minimum value of TDP
ζ_1	TDP for random relaying scheme
ζ_2	TDP for superior relaying scheme
$\mathcal{R}_1$	Jammer set for first hop
$\mathcal{R}_2$	Jammer set for second hop
θ	Decoding threshold
P_{to}	Transmission outage probability (TOP)
P_{sto}	TOP for superior relaying scheme
ε_c	Covertness requirement
ε_{rto}	TOP constraint for random relaying scheme
ε_{sto}	TOP constraint for superior relaying scheme

CHAPTER II

Related Works

This chapter introduces the available works related to our study in this thesis, including the works on the design of cooperative relaying and cooperative jamming protocols in two-hop wireless networks and the previous researches on covert communication.

2.1 Secure Wireless Communication

In wireless networks, secure wireless communication means the information is securely exchanged among authorized users. However, the communication process is vulnerable to various malicious threats owing to the broadcast nature of the wireless medium. With this background, the issue of how to ensure the security of wireless communication has attracted much attention. Then, many protocols and technologies have been proposed one after another. In this thesis, we focus on cooperative relaying and cooperative jamming technologies.

2.1.1 Secure Communication with Cooperative Relaying

The cooperative relaying technology aims to improve the security of wireless communication networks by choosing a link/relay with a strong legitimate channel and a weak eavesdropping channel meanwhile. The study [33] first proposed an opportunistic relaying scheme for the scenarios with multiple relays. The work in [34] has considered a two-hop wireless network with multiple secondary relays and suggested selecting the "best" relay for assisting the transmission. Then, the authors in [35] presented a comprehensive investigation on the secrecy performance of a system with opportunistic relay selection scheme by employing the decode-and-forward protocol over Rayleigh fading channels. The works [36–41] studied the relay selection protocol for buffer-aided relaying.

2.1.2 Secure Communication with Cooperative Jamming

Cooperative jamming serves as an efficient PHY security technology that uses artificial jamming signals generated by helpers nodes to interfere with eavesdroppers. Recently, the secure outage probability of the relay-assisted system under cooperative jamming mechanism is studied based on the theory of PHY security in [43]. The work [44] exploited PHY security to provide secure cooperative communication for wireless ad hoc networks (WANETs) where involve multiple source-destination pairs and malicious eavesdroppers. The authors in [45] proposed a novel secure buffer-aided and decode-and-forward relay selection that amalgamates the benefits of the buffer-state-based relay selection, the max-ratio criterion, the simultaneous activation of multiple source-to-relay links, and the cooperative beamforming in dual-hop networks. Motivated by this work, the authors in [46] studied the important secrecy outage performance of wireless communications under eavesdropper collusion, where the PHY security was adopted to counteract such attack. For analysis on the secrecy outage, both opportunistic relaying scheme and cooperative jamming were used.

2.2 Covert Wireless Communication

2.2.1 Covert Communication in One Hop Scenario

In the one hop scenario, the authors in [47–49] proved that $\mathcal{O}\sqrt{n}$ bits of information can be transmitted to a legitimate receiver reliably and covertly in n channel uses when $n \to \infty$. Then, the works were extended to different channel models such as the binary symmetric channel [50], the discrete memoryless channel (DMC) [51, 52], the multiple-access channels [53], the state-dependent channel [54], the memoryless broadcast channel [55] and the uncertain channel [56].

Based on these pioneering works on covert communication, much research effort was dedicated to the study of covert communication in various scenarios [57–64] . The work in [57] explored the impact of imperfect knowledge of the channel gain and noise power on the average detection error probability at the eavesdropper and the covert capacity under the Rayleigh fading channel. The work in [58] proved that covert communication is achievable by adopting channel inversion power control with Rayleigh fading channels. The authors in [59] utilized the artificial noise from full-duplex receiver to confuse a warden and derived a closed-form expression for the optimal detection performance of the warden. The work [65] analyzed the joint impact of imperfect knowledge of the channel gain (channel uncertainty) and noise power (noise uncertainty) on the average probability of detection error at the eavesdropper and the covert capacity in the Rayleigh fading channel. The authors in [66] studied covert communication with noise uncertainty. Specifically, a worst-case approach from the warden's perspective and new metrics for measuring the covertness, are proposed to explore the maximum achievable rate for a given covertness requirement under both bounded and unbounded noise uncertainty models.

The work in [60] considered a Poisson field of interferers in a covert communication scenario and proved that the density and the transmit power of the interferers have no effect on the covert capacity as long as the system stays in the interference-limited regime, for both the non-fading and the fading channels. The authors in [61] studied the throughput performance of the covert communication under a stochastic geometry framework in a system where multi-antenna-aided covert communications coexist with randomly located wardens and interferers. The authors in [62] took into account the effect of delay constraints in covert communication. The covert communication could be realized from a sequential change-point detection (SCPD) perspective in [63]. The work of [64] proposed two covert schemes based on the numbers of antennas at a base station which transmitted artificial noise to confuse adversaries in a D2D underlaying cellular system. The work in [67] derived covert transmit bits in a dense IoT system with lower frequency Additive white Gaussian noise (AWGN) channels and demonstrated that covert communication was achievable by utilizing the reflection or diffuse scattering from a rough surface in a terahertz band IoT system.

2.2.2 Covert Communication in Two-hop Scenario

Regarding a two-hop scenario with a single relay, the authors in [68, 69] studied the covert communication performance in terms of detection error probability and source's limited rate under AWGN channels. The work in [70] proved that channel uncertainty introducing confusions can degrade the performance of Willie's detection. In the work of [71], the authors studied the impact of a greedy relay on covert communication performance. The work in [72] examined the possibility, performance limits, and associated costs for a self-sustained relay to transmit its own covert information to a destination. Recently, the authors in [73] first considered problem of joint covert communication and secure transmission in untrusted relaying networks when multiple wardens exist in the network. A system model in which both eavesdroppers (untrusted relays) and detector exist is considered. The result of [73] was a novel observation of a fundamental trade-off between covert requirement and secrecy performance. However, the authors used cooperative jamming technology when targeting untrusted relays, but did not explore relay selection protocols. In addition, the idea that multiple relays and multiple wardens coexist mentioned at the end of this work is very meaningful.

CHAPTER III

Covert Communication in Wireless Systems with Multiple Relays

In this chapter, we explore the relay selection protocol design for covert communication in two-hop wireless communication systems with multiple relays and a passive warden. Then, we conduct a theoretical analysis to derive the corresponding achievable covert capacity. We first introduce the model and preliminaries, including the system model, the channel mode, and some key assumptions and definitions. We then introduce the transmission schedule and design relay selection protocol. Next, we develop a theoretical framework to analyze the transmission outage probability, the detection error probability of warden, and the covert capacity. Then we also explore the covert capacity maximization through efficient numerical searches under a given covertness requirement. Finally, extensive simulation and numerical results are provided to illustrate the performance of covert communication in a two-hop wireless communication system with multiple relays.

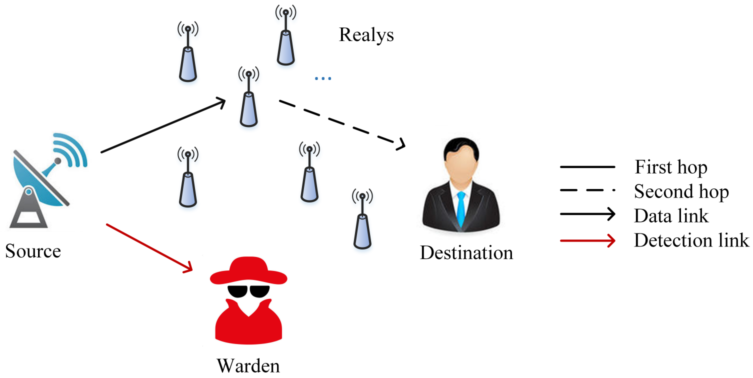


Figure 3.1: Covert communication scenario.

3.1 System Model

3.1.1 System Model

As shown in Fig.(3.1), we consider a two-hop relay wireless system consisting of a source (S), multiple relays, a destination (D), and a warden ($Willie$). With the two-hop relay routing, S first transmits the legitimate message to the relay, and the relay then forwards the messages to D. In particular, S opportunistically transmits covert messages to the relay on top of transmitting legitimate messages. $Willie$ tries to detect whether S is transmitting covert messages or not. S employs power P_s to transmit its messages. Once the transmit power P_s exceeds its maximum power constraint P_{max}, $Willie$ can detect that S is transmitting covert messages. We assume that the time is evenly divided into equal-sized time slots, and the independent quasi-static Rayleigh fading is used to model wireless channels in our work, where each channel keeps unchanged in a time slot, but randomly and independently from the current time slot to the next one. The channel coefficients are modeled as complex Gaussian random variables with zero mean and unit variance. There are in total three channels in the system, i.e., the channel from S to the relay, the one from the relay to D, and the one from S to $Willie$, whose channels coefficients are denoted as $h_{S,R}$, $h_{R,D}$ and $h_{W,S}$, respectively. The $|h_k|^2$ is the channel gain, where $k \in \{SR, RD, WS\}$.

We assume that S knows $|h_{S,R}|^2$ and $|h_{R,D}|^2$,and $Willie$ knows $|h_{W,S}|^2$. In addition, the channel noise is AWGN with variance σ^2. We assume that the system bandwidth is W MHZ. Without loss of generality, we assume $W = 1$ throughout this thesis.

3.1.2 Performance Metrics

To decide whether S is transmitting covet messages to the relay or not, $Willie$ conducts two hypotheses, i.e., null hypothesis H_0 and alternative hypothesis H_1. The former represents that S does not transmit covert messages while the latter represents that S transmits. Then, we define two performance metrics as follows.

Detection error probability: It is the probability that $Willie$ makes a wrong decision on whether or not S is transmitting covert messages, which is expressed as

$$\zeta = \mathbb{P}_{FA} + \mathbb{P}_{MD}, \tag{3.1}$$

where ζ denotes the detection error probability, $\mathbb{P}_{FA}$ denotes the probability of false alarm that $Willie$ trusts H_1, while H_0 is true, $\mathbb{P}_{MD}$ denotes the probability of missed detection that $Willie$ trusts H_0, while H_1 is true.

Covert capacity: It is defined as the covert rate at which messages from S is transmitted covertly to D with high detection error probability at $Willie$. In our work, we consider that $Willie$ only detects the messages transmission of S, and the relay can employ high transmit power to forward the messages to D. Therefore, the covert capacity is equal to that from S to the relay.

3.2 Protocol Design and Detection Schemes

3.2.1 Relay Selection Protocol Design

In this work, we assume that the whole transmission can be conducted in one slot. For the two-hop scenario where there are multiple relays, we propose two relay selection schemes.

Random relaying scheme: S randomly chooses one message relay from all the relays before the S to D transmission is conducted in two hops with the random relaying scheme. This message relay is denoted as R_b and announces itself as the message relay before the transmission in the first hop.

Superior relaying scheme: To enhance the covert capacity performance, we propose a superior relaying scheme to promise there will not occur transmission outage. We have made improvements based on the opportunity relaying scheme [33]. The selected message relay is denoted as R_b, which should be the maximum value of $\min\{|h_{S,R_n}|^2, |h_{R_n,D}|^2\}$ for all relays (where $|h_{S,R_n}|^2$ and $|h_{R_n,D}|^2$ represent the channel gain from S to the nth relay, and the one from the nth relay to D, respectively), and in order to ensure the transmission reliability, the channel gain $\min\{|h_{S,R_b}|^2, |h_{R_b,D}|^2\}$ needs ensure no transmission outage occur. Similarly, the message relay R_b will announce itself as the message relay before the transmission in the first hop.

3.2.2 Detection Scheme of Warden

Warden uses two kinds of hypothesis tests to determine whether S has sent a covert message based on its observation vector y_w of one block. One is H_0 representing that S does not send a covert message, and the other is H_1 which represents the opposite situation. Based on these hypothesis tests, there are two types of errors: false alarm (FA) and missed detection (MD) [47]. The probabilities of FA and MD are denoted as $\mathbb{P}_{FA}$ and $\mathbb{P}_{MD}$, respectively. The false alarm which means $Willie$ believes that covert communication exists, but actually it does not. And missed detection is that $Willie$ decides on H_0 while H_1 is true. To achieve covert communication, a condition should be satisfied as follow: for any $\varepsilon > 0$, the $Willie$'s detection error probability should satisfy $\mathbb{P}_{FA} + \mathbb{P}_{MD} \geq 1 - \varepsilon$ when $n \to \infty$ [48].

3.3 Performance Analysis and Optimization

In this section, we first propose transmission strategies of S, then derive the detection error probability of $Willie$ and covert capacity under the two relay selection schemes.

3.3.1 Performance Analysis and Optimization under Random Relaying Scheme

3.3.1.1 Transmission Strategies

We propose two transmission strategies without/with covert messages under the random relaying scheme. With the selection scheme, S randomly chooses one R_b from all relays. The selection scheme does not consider the quality of the channel from S to the relay, which may result in transmission outage once if the received signal strength at the relay is smaller than its required threshold.

1. S's transmission without covert message

We consider that S only transmits the legitimate message with power $P_s^{'}$ subject to maximum power constraint P_{max}. Then, the received signal at R_b is given by

$$y_{R_b} = \sqrt{P_s^{'}} h_{S,R_b} x_r + n_{R_b}, \tag{3.2}$$

where x_r denotes the legitimate message signal transmitted by S, and $n_{R_b} \sim \mathcal{CN}(0, \sigma_{R_b}^2)$ represents the received noise at R_b.

Accordingly, the signal-to-noise (SNR) at R_b is determined as

$$\gamma_{R_b}^{'} = \frac{P_s^{'} |h_{S,R_b}|^2}{\sigma_{R_b}^2}. \tag{3.3}$$

2. S's transmission with covert message

When S sends covert message on top of transmitting legitimate messages, the received signal at R_b is determined as

$$y_{R_b} = \sqrt{P'_s} h_{S,R_b} x_r + \sqrt{P_s} h_{S,R_b} x_c + n_{R_b}, \tag{3.4}$$

where $P_s^{'}$ and P_s represent the transmit power of transmitting the legitimate message x_r and the covert message x_c, respectively.

To ensure that the legitimate messages from S can be received, the relay R_b first decodes x_r and regards x_c as interference. Then, the signal-to-interference ratio (SINR) at R_b is determined as

$$\gamma_{R_b} = \frac{P'_s |h_{S,R_b}|^2}{P_s |h_{S,R_b}|^2 + \sigma_{R_b}^2}. \tag{3.5}$$

3.3.1.2 Detection Error Probability

To determine the detection error probability at $Willie$, we first introduce the hypothesis test of $Willie$ to decide on whether S is transmitting or not.

1. Hypothesis test

We consider that $Willie$ only detects whether S sends covert messages. Thus, the received signal y_w at $Willie$ under the random relaying scheme is given by

$$y_w = \begin{cases} \sqrt{P'_s} h_{S,W} x_r + n_w, & \text{if } H_0 \text{ is true} \\ \sqrt{P'_s} h_{S,W} x_r + \sqrt{P_s} h_{S,W} x_c + n_w, & \text{if } H_1 \text{ is true} \end{cases} \tag{3.6}$$

where $n_w \sim \mathcal{CN}(0, \sigma_w^2)$ represents the received noise at $Willie$.

To minimize the detection error probability at $Willie$, the optimal decision rule can be expressed as [74]

$$T \underset{D_0}{\overset{D_1}{\gtrless}} \lambda, \tag{3.7}$$

where D_0 and D_1 denote that $Willie$ makes a decision in favor of H_0 and H_1, respectively, λ is a detection threshold, and $T = 1/m \sum_{i=1}^{m} |y_w^i|^2$ is the received power at $Willie$ in a time slot. Here, y_w^i is the received signal at $Willie$ in ith channel use, and n is the number of channel uses. According to the Lebesgue's dominated convergence theorem, T can be determined as

$$T = \begin{cases} P_s^{'}|h_{S,W}|^2 + \sigma_w^2, & \text{if } H_0 \text{ is true} \\ P_s^{'}|h_{S,W}|^2 + P_s|h_{S,W}|^2 + \sigma_w^2. & \text{if } H_1 \text{ is true} \end{cases} \tag{3.8}$$

2. Detection error probability of $Willie$

It can be determined as

$$\zeta = \mathbb{P}_{FA} + \mathbb{P}_{MD}, \tag{3.9}$$

where

$$\begin{aligned} \mathbb{P}_{FA} &= P(P_s^{'}|h_{S,W}|^2 + \sigma_w^2 \geq \lambda) = P\left(|h_{S,W}|^2 \geq \frac{\lambda - \sigma_w^2}{P_s^{'}}\right) \\ &= \begin{cases} \exp\left(\frac{\sigma_w^2 - \lambda}{P_s^{'}}\right), & \text{if } \lambda \geq \sigma_w^2 \\ 1, & \text{otherwise} \end{cases} \end{aligned} \tag{3.10}$$

and

$$\begin{aligned} \mathbb{P}_{MD} &= P(P_s^{'}|h_{S,W}|^2 + P_s|h_{S,W}|^2 + \sigma_w^2 < \lambda) = P\left(|h_{S,W}|^2 < \frac{\lambda - \sigma_w^2}{P_s^{'} + P_s}\right) \\ &= \begin{cases} 1 - \exp\left(\frac{\sigma_w^2 - \lambda}{P_s^{'} + P_s}\right), & \text{if } \lambda > \sigma_w^2 \\ 0. & \text{otherwise} \end{cases} \end{aligned} \tag{3.11}$$

To achieve covert communication, it should guarantee that $\zeta \geq 1 - \varepsilon_c$ for any

$\varepsilon_c > 0$, when n tends to infinity [48].

Now, we optimize λ to maximize the detection error probability ζ. To this end, we rewrite (3.26) as

$$\zeta = \begin{cases} 1 - \exp\left(\frac{\sigma_w^2 - \lambda}{P_s^{'} + P_s}\right) + \exp\left(\frac{\sigma_w^2 - \lambda}{P_s^{'}}\right), & \text{if}\, \lambda > \sigma_w^2 \\ 1. & \text{otherwise} \end{cases} \tag{3.12}$$

Under the case of $\lambda \leq \sigma_w^2$, $\zeta = 1$. This means that *Willie* cannot detect the transmission from S to relay absolutely. Thus, we only consider the case of $\lambda > \sigma_w^2$. Take the derivation of (3.12) with respect to λ, we have

$$\frac{\partial \zeta}{\partial \lambda} = \frac{1}{P_s^{'} + P_s} \exp\left(\frac{\sigma_w^2 - \lambda}{P_s^{'} + P_s}\right) - \frac{1}{P_s^{'}} \exp\left(\frac{\sigma_w^2 - \lambda}{P_s^{'}}\right) = 0. \tag{3.13}$$

Then, we have

$$\lambda^* = \frac{(P_s^{'} + P_s)P_s^{'}}{P_s} \ln\left(\frac{P_s^{'} + P_s}{P_s^{'}}\right) + \sigma_w^2. \tag{3.14}$$

Substituting (3.14) into (4.16), we can obtain that $\frac{\partial \zeta}{\partial \lambda} > 0$, if $\lambda > \lambda^*$ and $\frac{\partial \zeta}{\partial \lambda} < 0$, if $\lambda < \lambda^*$. Thus, *Willie* can know the optimal threshold $\lambda^\dagger = \lambda^*$ to achieve the minimum value of ζ, i.e., $\zeta^\dagger = \zeta(\lambda^\dagger)$.

3.3.1.3 Covert Capacity

To derive the covert capacity, we first determine the probability that transmission from S to relay does not occur outage.

1. Transmission outage probability

A signal received at the relay can be successfully decoded if and only if the channel capacity $C_{S,R}$ from S to relay is greater than the required threshold $Q_{S,D}$ at the relay, and we say that outage happens if $C_{S,R} \leq Q_{S,D}$. When H_1 is true, the probability of transmission outage P_{to} at the relay is determined as

$$\begin{aligned}
P_{rto} &= P(SIR_{R_b} \leq \theta) \\
&= 1 - P\left(|h_{ar}|^2 \geq \frac{\theta \sigma_{R_b}^2}{P_s^{'} - \theta P_s}\right) \\
&= 1 - \exp\left(-\frac{\theta \sigma_{R_b}^2}{P_s^{'} - \theta P_s}\right),
\end{aligned} \tag{3.15}$$

where $\theta = 2^{R_{S,R}} - 1$. We know that $P_s^{'} - \theta P_s > 0$ in (3.15). Since $P_s^{'} + P_s \leq P_{max}$, $P_s \leq P_{max}/(1+\theta)$. Notice that the increasing of P_s leads to the decreasing of $P_s^{'}$ such that the outage may happen.

2. Expected Covert capacity

Based on the probability P_{rto} and channel capacity C from S to relay for covert message transmission, the expected covert capacity C_{c1} can be determined as

$$\begin{aligned}
C_{c1} &= C(1 - P_{rto}) \\
&= \log_2\left(1 + \frac{P_s |h_{S,R_b}|^2}{P_s^{'} |h_{S,R_b}|^2 + \sigma_{R_b}^2}\right) \exp\left(-\frac{\theta \sigma_{R_b}^2}{P_s^{'} - \theta P_s}\right).
\end{aligned} \tag{3.16}$$

3. Covert capacity maximization

The objective of covert capacity maximization is to maximize the covert capacity C while maintaining a high detection error probability at $Willie$. It can be formulated as the following optimization problem.

$$\text{Maximize} \quad C_{c1} \tag{3.17a}$$

$$s.t. \quad \zeta^{\dagger} \geq 1 - \varepsilon_c, \tag{3.17b}$$

$$0 < P_s \leq P_{max}/(1+\theta), \tag{3.17c}$$

where P_s^* denotes optimal covert transmit power, constraint (4.24b) represents that the minimum detection error probability is greater than some value, ε_c denotes the covertness requirement, and constraint (3.17c) denotes the rang of covert transmit power.

Note that (3.17) is an one dimensional optimization problem, which can be easily solved by numerical search. By substituting P_s^* into (3.16), we then obtain the maximum capacity denoted as C^*.

3.3.2 Performance Analysis and Optimization under Superior Relaying Scheme

In this section, we first propose the superior relaying scheme, transmission strategy of S, and then derive the detection error probability at $Willie$ and covert capacity under the superior relaying scheme.

3.3.2.1 Transmission Strategy

We consider two transmission strategies of S.

1. S's transmission without covert message

When S transmits the legitimate message, the received signal at the relay is given by

$$y_{R_b} = \sqrt{P_s'} h_{S,R_b} x_r + n_{R_b}, \tag{3.18}$$

where $P_s^{'}$ denotes the power used to transmit the legitimate message of S.

Then, the SNR at the relay is given by

$$\gamma_{R_b}^{'} = \frac{P_s^{'} |h_{S,R_b}|^2}{\sigma_{R_b}^2}. \tag{3.19}$$

We know that when the required signal threshold of the relay $Q_{S,D} \leq C_{S,R}$, the outage will not happen. Here, $C_{S,R}$ denotes the channel capacity from S to relay, which is determined as $C_{S,R_b} = \log_2(1+\gamma_{R_b})$. Thus, we obtain $|h_{S,R_b}|^2 \geq \theta\sigma^2_{R_b}/P^{'}_s$, where $\theta = 2^{Q_{S,D}} - 1$. Then, we have

$$P^{'}_s = \begin{cases} \frac{\theta\sigma^2_{R_b}}{|h_{S,R_b}|^2}, & \text{if} \, |h_{S,R_b}|^2 \geq \frac{\theta\sigma^2_{R_b}}{P_{max}} \\ 0. & \text{if} \, |h_{S,R_b}|^2 < \frac{\theta\sigma^2_{R_b}}{P_{max}} \end{cases} \tag{3.20}$$

2. S's transmission with covert message

When S transmits the legitimate and covert message, the received signal at the relay is given by

$$y_{R_b} = \sqrt{P^{'}_s} h_{S,R_b} x_r + \sqrt{P_s} h_{S,R_b} x_c + n_{R_b}, \tag{3.21}$$

where $P^{'}_s$ denotes the power used to transmit the legitimate message of S. In general, $P_s < P^{'}_s$ for the purpose of covert communication. The relay first decodes the legitimate message and thus regards the covert message as interference. Thus, the SINR at the relay is given by

$$\gamma_{R_b} = \frac{P^{'}_s |h_{S,R_b}|^2}{P_s |h_{S,R_b}|^2 + \sigma^2_{R_b}}. \tag{3.22}$$

Notice that when the selected relay should not lead to the outage, $Q_{S,D} \leq C_{S,R_b}$. Thus, we have $|h_{S,R_b}|^2 \geq \theta\sigma^2_{R_b}/(P_{max} - (1+\theta)P_s)$. Then, we have

$$P_s = \begin{cases} \frac{\theta(P_s|h_{S,R_b}|^2 + \sigma^2_{R_b})}{|h_{S,R_b}|^2}, & \text{if} \, |h_{S,R_b}|^2 \geq \frac{\theta\sigma^2_{R_b}}{P_{max} - (1+\theta)P_s} \\ \frac{\theta\sigma^2_{R_b}}{|h_{S,R_b}|^2}, & \text{if} \, \frac{\theta\sigma^2_{R_b}}{P_{max}} \leq |h_{S,R_b}|^2 < \frac{\theta\sigma^2_{R_b}}{P_{max} - (1+\theta)P_s} \\ 0, & \text{if} \, |h_{S,R_b}|^2 < \frac{\theta\sigma^2_{R_b}}{P_{max}} \end{cases} \tag{3.23}$$

where the first case represents that S keeps silent, the second one represents that S only sends the legitimate message, and the third one represents that S sends the legitimate and covert message simultaneously. With the maximum power constraint, we can obtain $P_s \leq (P_{max} - \theta\sigma_{R_b}^2/|h_{S,R_b}|^2)/(1+\theta)$.

3.3.2.2 Detection Error Probability

To determine the detection error probability at $Willie$, we first introduce the hypothesis test of $Willie$ to make a decision on whether S is transmitting or not.

1. Hypothesis test

We consider that $Willie$ only detects whether S sends covert message. Thus, the received signal y_w at $Willie$ under random relaying scheme is given by

$$y_w = \begin{cases} \sqrt{P_s'} h_{S,W} x_r + n_w, & \text{if } H_0 \text{ is true} \\ \sqrt{P_s'} h_{S,W} x_r + \sqrt{P_s} h_{S,W} x_c + n_w, & \text{if } H_1 \text{ is true} \end{cases} \tag{3.24}$$

where $n_w \sim \mathcal{CN}(0, \sigma_w^2)$ represents the received noise at $Willie$.

According to (3.7), the received power T at $Willie$ is determined as

$$T = \begin{cases} P_s' |h_{S,W}|^2 + \sigma_w^2, & \text{if } H_0 \text{ is ture} \\ P_s' |h_{S,W}|^2 + P_s |h_{S,W}|^2 + \sigma_w^2, & \text{if } H_1 \text{ is ture} \end{cases} \tag{3.25}$$

2. Detection error probability of $Willie$

It is determined as

$$\zeta = \mathbb{P}_{FA} + \mathbb{P}_{MD}. \tag{3.26}$$

We need to calculate $\mathbb{P}_{FA}$ and $\mathbb{P}_{MD}$. Based on (3.23) (3.24) and (3.25), we have

$$\begin{aligned}\mathbb{P}_{FA} &= P\left(\frac{\theta\sigma_{R_b}^2}{|h_{S,R_b}|^2}|h_{S,W}|^2+\sigma_w^2 \geq \lambda\right)\\ &= P\left[|h_{S,W}|^2 \geq \frac{(\lambda-\sigma_w^2)|h_{S,R_b}|^2}{\theta\sigma_{R_b}^2}\right]\\ &= \begin{cases}\exp\left[\dfrac{(\sigma_w^2-\lambda)|h_{S,R_b}|^2}{\theta\sigma_{R_b}^2}\right], & \text{if}\,\lambda \geq \sigma_w^2\\ 1, & \text{otherwise}\end{cases}\end{aligned} \tag{3.27}$$

and

$$\begin{aligned}\mathbb{P}_{MD} &= P\left[\left(\frac{\theta\sigma_{R_b}^2}{|h_{S,R_b}|^2}+(1+\theta)P_s\right)|h_{S,W}|^2+\sigma_w^2 < \lambda\right]\\ &= P\left[|h_{S,W}|^2 < \frac{\lambda-\sigma_w^2}{(1+\theta)P_s+\frac{\theta\sigma_{R_b}^2}{|h_{S,R_b}|^2}}\right]\\ &= \begin{cases}1-\exp\left[\dfrac{\sigma_w^2-\lambda}{(1+\theta)P_s+\frac{\theta\sigma_{R_b}^2}{|h_{S,R_b}|^2}}\right], & \text{if}\,\lambda > \sigma_w^2\\ 0. & \text{otherwise}\end{cases}\end{aligned} \tag{3.28}$$

Now, we optimize λ to maximize the detection error probability ζ. To this end, we rewrite (3.26) with (3.27) and (3.28) as

$$\zeta = \begin{cases}1-\exp\left(\dfrac{\sigma_w^2-\lambda}{B+A}\right)+\exp\left(\dfrac{\sigma_w^2-\lambda}{A}\right), & \text{if}\,\lambda > \sigma_w^2\\ 1, & \text{otherwise}\end{cases} \tag{3.29}$$

where $A = \theta\sigma_{R_b}^2/|h_{S,R_b}|^2$, and $B = (1+\theta)P_s$.

When $\lambda < \sigma_w^2$, $\zeta = 1$. This indicates that $Willie$ cannot detect the transmission from S to relay absolutely. Thus, we only need to consider the case of $\lambda < \sigma_w^2$. Take the derivation of (33) with respect to λ, we have

$$\frac{\partial \zeta}{\partial \lambda} = \frac{1}{B+A}\exp\left(\frac{\sigma_w^2-\lambda}{B+A}\right) - \frac{1}{A}\exp\left(\frac{\sigma_w^2-\lambda}{A}\right) = 0. \tag{3.30}$$

Then, we obtain

$$\lambda^* = \frac{(B+A)A}{B}\ln\left[\frac{(B+A)}{A}\right] + \sigma_w^2. \tag{3.31}$$

We further obtain that $\frac{\partial \zeta}{\partial \lambda} > 0$, if $\lambda > \lambda^*$ and $\frac{\partial \zeta}{\partial \lambda} < 0$, if $\lambda < \lambda^*$. Thus, $Willie$ can know the optimal threshold $\lambda^\dagger = \lambda^*$ to achieve the minimum value of ζ, i.e., $\zeta^\dagger = \zeta(\lambda^\dagger)$.

3.3.2.3 Optimal Covert Capacity

1. Expected covert capacity

Based on the channel capacity C from S to relay for covert message transmission, the covert capacity C_{c2} can be determined as

$$C_{c2} = C = \log_2\left(1 + \frac{P_s|h_{S,R_b}|^2}{\theta(P_s|h_{S,R_b}|^2 + \sigma_{R_b}^2) + \sigma_{R_b}^2}\right). \tag{3.32}$$

2. Covert capacity maximization

The covert capacity maximization aims to maximize the covert capacity C while keeping a high detection error probability at $Willie$. We can formulate covert capacity maximization as the following optimization problem.

$$\text{Maximize} \quad C_{c2} \tag{3.33a}$$

$$s.t. \quad \zeta^\dagger \geq 1 - \varepsilon_c, \tag{3.33b}$$

$$0 < P_s \leq \frac{P_{max} - \theta\sigma_{R_b}^2/|h_{S,R_b}|^2}{(1+\theta)} \tag{3.33c}$$

where P_s^* denotes optimal covert transmit power, constraint (3.33b) represents that the minimum detection error probability is greater than some value, ε_c denotes the covertness requirement, and constraint (3.33c) denotes the rang of covert transmit power.

Unitizing numerical search, we can solve the one dimensional optimization problem in (3.33). By substituting P_s^* into (3.32), we then obtain the maximum capacity denoted as C^*.

3.4 Numerical Results

In this section, extensive numerical results are provided to illustrate the impact of various system parameters on the detection error probability at $Willie$ and covert capacity performance, and also to reveal our findings under these two relay selection schemes. Some parameters used in our paper is set as $Q_{S,D} = 1$ Mbit/s/Hz, $\sigma_w^2 = \sigma_{R_b}^2 = 0$ dB and $P_{max} = 10$ W, unless otherwise specified.

In the following figures, the **dashed lines** and **solid lines** are used to show the results under the random relaying scheme and the superior relaying scheme, respectively.

3.4.1 Validation

To validate our proposed theoretical results, we compare the theoretical results with the simulation ones under the two relay selection schemes with the setting of covert transmit power $P_s = 2$ W. We summarize in Fig.(3.2) how the detection error probability ζ varies with the detection error threshold λ. We can see from Fig.(3.2) that for each relay selection scheme, the theoretical ζ matches well with the simulation one. This demonstrates that our theoretical results can well capture the performance of covert communication under these two relay selection schemes.

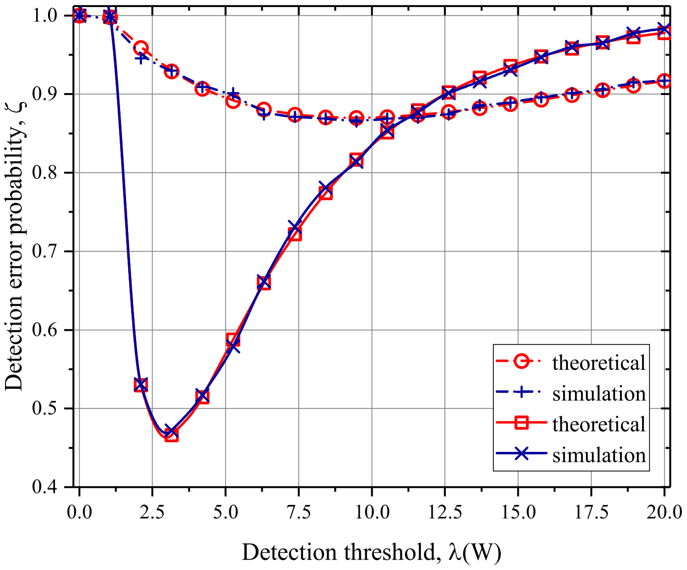


Figure 3.2: Detection error probability validation.

3.4.2 Covert Performance Analysis

We first explore the impact of detection threshold λ on the detection error probability ζ under these two relay selection schemes. We summarize in Fig.(3.3) how ζ varies with λ under the two schemes with the setting of covert power $P_s = \{0.5, 1.5, 2.5\}$ W. We can see from Fig.(3.3) that for each setting of P_s, as λ increases, ζ first decreases and then increases under both the schemes. This can be explained as follows. We know that ζ is the sum of false alarm probability P_{FM} and missed detection probability P_{MD}. P_{FM} is a decreasing function of λ while P_{MD} is an increasing function. As λ is relative small, the former one dominates ζ, leading to the decreasing of ζ with λ. On the other hand, as λ further increases, the latter one dominates ζ, leading to the increasing of ζ. As shown in Fig.(3.3), there exists a minimum ζ, at which $Willie$ has the strongest detection ability to detect the transmission from S to relay. Notice that the decreasing of P_s not only increases ζ but also decreases covert capacity. Thus, P_s needs to be carefully set so as to satisfy different application requirements with detection error probability and covert capacity.

A careful observation of Fig.(3.3) indicates that for each fixed λ, ζ under random

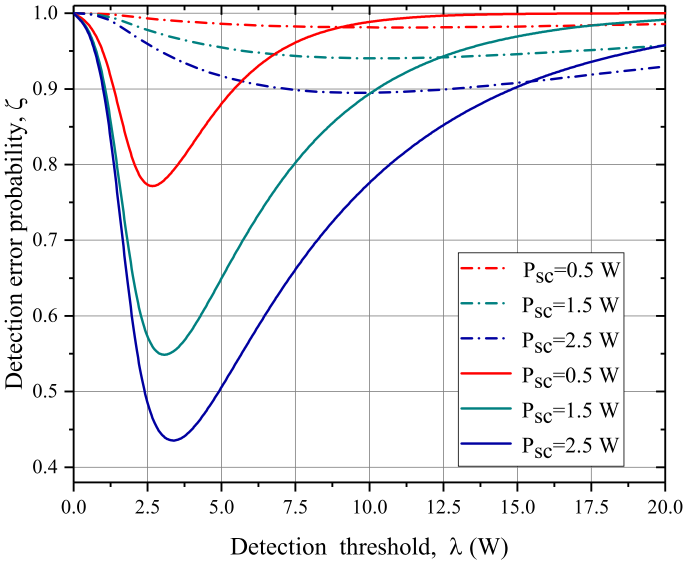


Figure 3.3: The impact of detection threshold on detection error probability.

relaying scheme is greater than that under superior relaying scheme. It is due to the following reasons. In comparison with random relaying scheme, the channel quality from S to relay is better under superior relaying scheme, such that S under the former needs to higher power to send its legitimate message. This will extremely confuse the $Willie$ under the former. Thus, the detection error probability ζ at $Willie$ under the former is greater than that the latter. In practical application, we need to consider a more powerful $Willie$, so that our research will be more meaningful. In the second selection strategy, the detection error probability ζ at $Willie$ is significantly reduced under superior relaying scheme, which means that the superior relaying scheme is more adaptable to the more severe scenarios.

To investigate the impact of covert transmit power P_s on the detection error probability ζ, we summarize in Fig.(3.4) how ζ varies with the increasing of P_s under these two relay selection schemes with the setting of $\lambda = \{3, 5, 7\}$ W. It can be observed from Fig.(3.4) that as P_s increases, ζ decreases under both the schemes. This is because the increasing of P_s leads to the increasing of probability that the transmission from S to relay is detected by $Willie$, and thus the detection error probability ζ decreases with P_s. We can also see from Fig.(3.4) that for each fixed P_s, ζ under the random relaying scheme is greater than that under the superior relaying scheme. This can be explained as follows. The channel quality from S to relay under the former is worse than that under the latter one. To reduce the outage probability under the former, S needs to increase the power to transmit its legitimate message which confuses $Willie$. Thus, ζ under the former one is more than the latter.

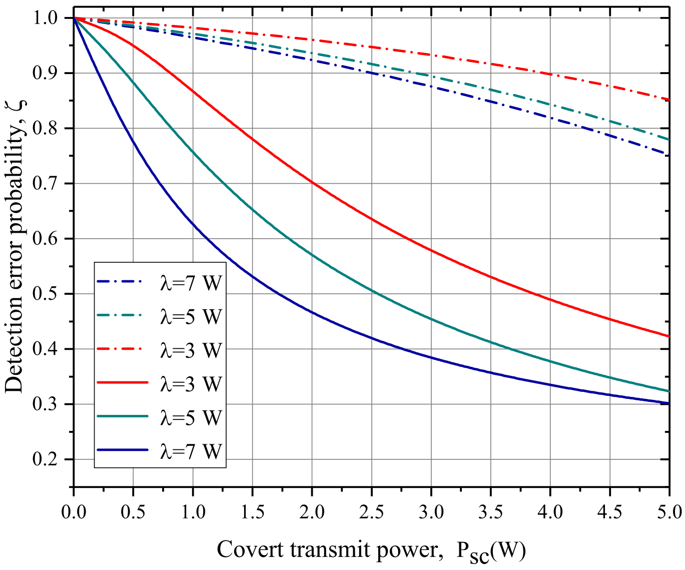


Figure 3.4: The impact of covert transmit power on detection error probability.

We now proceed to explore how the covert transmit power P_s affects the covert capacity C_c under these two relay selection schemes. We summarize in Fig.(3.5) how C_c varies with P_s for a setting of channel gain $|h_{S,R_b}|^2 = \{0.5, 1.0, 2.0\}$. We observe from Fig.(3.5) that as P_s increases, C_c first increases and then decreases under the random relaying scheme, while C_c always increases under the superior relaying scheme. This can be explained as follows. The transmit power of S consists of covert transmit power P_s and the power $P_s^{'}$ used to transmit legitimate power, and is subject to the constraint of a maximum transmit power P_{max}. Under the former, we know that C_c is related to outage probability and covert transmit power. As P_s is relatively small, the latter power is high. Although P_s increases, the relative high $P_s^{'}$

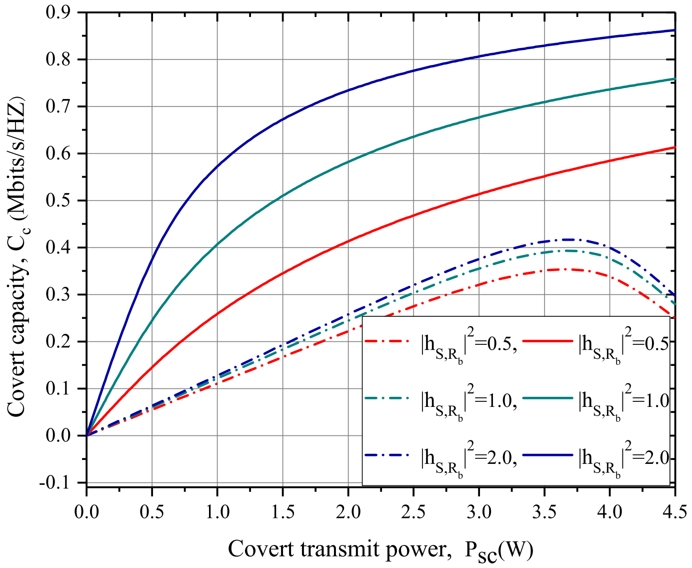


Figure 3.5: The impact of covert transmit power on covert capacity.

corresponds to a small outage probability. Thus, the positive effect of P_s dominates the negative effect of outage probability, leading to the increasing of covert capacity C_c. As P_s further increases, $P_s^{'}$ becomes relatively small, which leads to a high outage probability, such that the negative effect of outage probability dominates the positive effect of P_s, leading to the decreasing of C_c. Notice that under the superior relaying scheme, the covert capacity C_c is only related to the covert transmit power P_s. Thus, the covert capacity C_c increases with P_s. A more careful observation from Fig.(3.5) indicates that for each fixed P_s, the C_c under the random relaying scheme is lower than that under the superior relaying scheme. This is because there does not exist a negative effect of outage probability on the covert capacity under the superior relaying scheme, leading to a bigger C_c. This also means that S can achieve higher covert capacity and reduce transmission cost in disguise under the superior relaying scheme when the transmitting power of covert message is constant.

We further observe from Fig.(3.5) that for each fixed P_s, the covert capacity C_c increases with the increasing of channel gain $|h_{S,R_b}|^2$ under each selection scheme. This is because a large $|h_{S,R_b}|^2$ leads to a strong received signal at relay under each scheme, and also low outage probability under the random relaying scheme, which results in a large covert capacity C_c.

3.4.3 Performance Optimization

We explore the impact of covertness requirement ε_c and maximum power constraint P_{max} on the maximum covert capacity C^* under the two relay selection schemes. Fig.(3.6) illustrates that the impact of covertness requirement ε_c on the maximum covert capacity C^* under the two relay selection schemes with the setting of $|h_{S,R_b}|^2 = \{0.5, 1.0, 2.0\}$. We can see from Fig.(3.6) that as ε_c increases, the C^* first increases and then decreases under the random relaying scheme while it always increases under the superior relaying scheme. The phenomenon can be explained as follows. The optimal covert transmit power $P_s^{\dagger}$ increases with the decreasing of detection error probability $\zeta^{\dagger}$, and $\zeta^{\dagger}$ decreases with ε_c increases. Thus, the increasing of ε_c is equivalent to that of optimal covert transmit power. Similar to the analysis of Fig.(3.5), as the optimal covert transmit power is relatively small, the power $P_s^{'}$ is high. The relatively high $P_s^{'}$ corresponds to a small outage probability. Thus, the positive effect of optimal covert transmit power dominates the negative effect of outage probability, leading to the increasing of maximum covert capacity C^*. As the optimal covert transmit power further increases up to a large value, $P_s^{'}$ becomes relatively small, which leads to a high outage probability, such that the negative effect of outage probability dominates the positive effect of optimal covert transmit, leading to the decreasing of C^*. Notice that under the superior relaying scheme, the maximum covert capacity C^* is only related to the covert transmit power P_s. Thus, the maximum covert capacity C^* increases with the optimal covert transmit power.

A careful observation of Fig.(3.6) indicates that for each fixed $|h_{S,R_b}|^2$, as ε_c increases, the maximum covert capacity C^* under the superior relaying scheme is less than that under the random relaying scheme, and then the former is greater than the latter. This can be explained as follows. We know that $Willie$ treats the power $P_s^{'}$ as background noise. Due to the worse link under the random relaying scheme, S employs higher power to transmit its legitimate message. Thus, the background noise under the random relaying scheme is stronger than that under the superior relaying scheme for each fixed ε_c, such that the detection error probability under the former is higher than that under the latter. To achieve the same detection error probability under both these two schemes, the optimal covert transmit power $P_s^{\dagger}$ needs to be increased under the former aiming to reduce the detection error probability, which leads to the increasing of maximum covert capacity C^*. But as ε_c becomes larger, the outage probability has a significant effect on C^* under the former, thus the maximum covert capacity under the former is then smaller than that under the latter.

From Fig.(3.6), we can also find that when ε_c is less than a threshold, it can achieve higher maximum covert capacity under the random relaying scheme, otherwise it is not. Therefore, S can decide which relay selection scheme to adopt according to the requirement of ε_c in practice. However, referring to the previous analysis, we can know that S has to pay more transmission costs under the random relaying scheme and the maximum covert capacity is not greatly improved.

Finally, we examine how the maximum power constraint P_{max} affects the maximum covert capacity C^* under two relay selection schemes. Given a setting of covertness requirement $\varepsilon_c = \{0.1, 0.2, 0.4\}$, we summarize in Fig.(3.7) how C^* varies with P_{max}. We can see from Fig.(3.6) that as P_{max} increases, C^* always increases under the random relaying scheme for each fixed $\varepsilon_c \in \{0.1, 0.2\}$. Particularly, $C^* = 0$ when $\varepsilon_c = 0.4$ under such a scheme. On the other hand, C^* first increases and then remains unchanged under the superior relaying scheme. The reasons behind the phenomenon can be explained as follows. For each fixed $\varepsilon_c \in \{0.1, 0.2\}$ under the random relaying scheme, the power $P_s^{'}$ increases with the increasing of P_{max}, which can reduce the negative effect of outage probability on C^*. Meanwhile, the covert transmit pow-

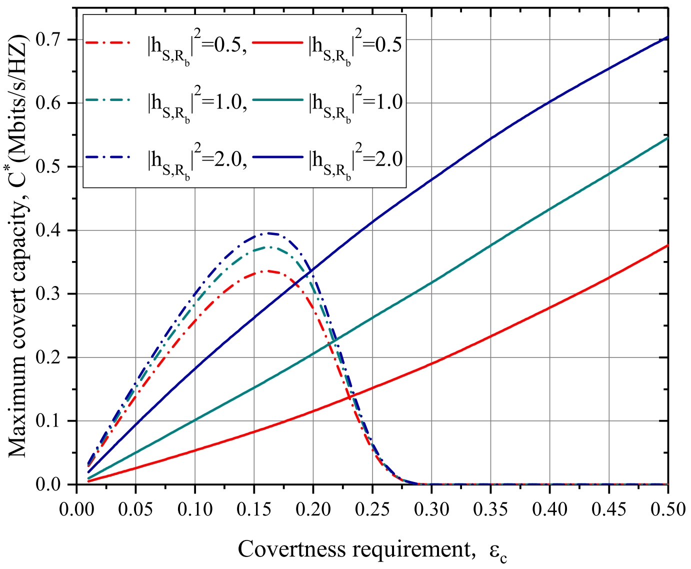


Figure 3.6: The impact of covertness requirement on maximum covert capacity.

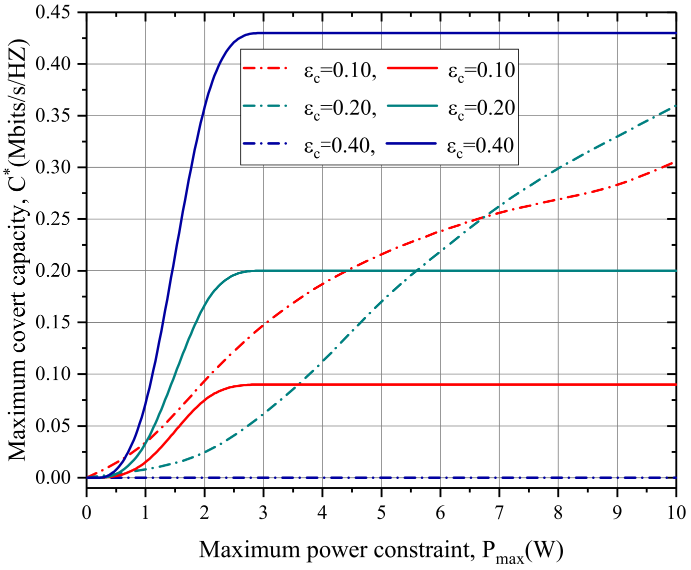


Figure 3.7: The impact of maximum power constraint on maximum covert capacity.

er also increases to keep an unchanged value of ε_c, leading to the increasing of C^*. When $\varepsilon_c = 0.4$, we can obtain a large optimal covert transmit power and a small P_s', leading to occurring of outage. Thus, $C^* = 0$. Regarding the superior relaying scheme without transmission outage, we can determine an optimal covert transmit power. As P_{max} is relatively small, the covert transmit power is less than the optimal value. Thus, the covert transmit power increases with the increasing of P_{max}, which leads to the increasing of maximum covert capacity C^*. If P_{max} increases more than a threshold, the covert transmit power achieves the optimal value and keeps unchanged, which leads to a constant C^*.

Similar to the previous analysis, S can decide which relay selection scheme can achieve greater maximum covert capacity according to its own maximum power constraint P_{max}. From Fig.(3.6), we can see that under the random relaying scheme, if the maximum power is large enough, the maximum covert capacity C^* can be increased all the time, which means that S must always transmit with full power. However, under the superior relaying scheme, even if the P_{max} is relatively small, it can stably achieve a better maximum covert capacity C^* and reduce the transmission costs.

3.5 Discussion

In this chapter, we analyze the performance of covert communication in wireless systems with multiple relays by deriving the detection error probability and optimizing the covert capacity. Numerical results indicate that the covert capacity increases with the increasing of covert transmit power under the random relaying scheme, while there exists an optimal covert transmit power to achieve a maximum covert capacity under the superior relaying scheme.

However, in practical applications, although the superior relaying scheme saves resources in covert power, it has a higher requirement on the channel state of relay and requires the cooperation of all relays. If there is no relay that meets the requirements, the source will choose to stop transmitting covert information. This leads to limited slots of covert transmissions that can be completed within a period of time. Thus, the source will decide which relay selection scheme to use according to different channel states and its own resource constraints. If the source's covert demand for the communication is not extremely high, and the available power is more, then the random relaying scheme can already satisfy the requirements. If the transmit power of the source is limited and there is a relay that meets the requirements of non-outage, the superior relaying scheme is better.

In addition, if the transmission power of source is limited and there is no relay that satisfies the superior relaying scheme, we also consider combining two relay selection schemes (e.g., sort all channel states and randomly select one of the top three channels). This not only guarantees the transmission quality but also saves power as much as possible. We will further analyze the covert performance under this relay selection scheme in future work.

The two relay selection schemes proposed in this chapter show that designing a flexible relaying protocol will improve the covert capacity. This concept proposes a new issue for the future research of covert communication in a two-hop wireless communication system with multiple relays.

3.6 Summary

This chapter investigated the performance of covert communication in multiple relays assisted wireless systems. To this end, we proposed two relay selection schemes, i,e., random relaying scheme and superior relaying scheme. We then derived the expressions for the detection error probability and covert capacity under each selection scheme. Moreover, we also derived the maximum detection error probability by optimizing the detection threshold. We further optimized the covert transmit power to maximize the covert capacity performance under a given covertness requirement. Extensive numerical results were presented to illustrate the impact of various parameters on detection error probability and covert capacity.

In particular, the impact of covertness requirement on the maximum covert capacity exhibits similar behaviors under the proposed two relaying schemes. Furthermore, the increasing of maximum power constraint can increase the maximum covert capacity under the random relaying scheme by carefully setting the covertness requirements, while the maximum covert capacity converges to be a constant with the increasing of maximum power constraint under the superior relaying scheme. Remarkably, both the detection error probability and covert capacity performance under the superior relaying scheme are better than those under the random relaying scheme as covert transmit power increases.

CHAPTER IV

Cooperative Jamming based Covert Communication in Relay-Assisted Wireless Systems

In this chapter, we introduce cooperative jamming technology into relay-assisted wireless systems to interfere with the warden. In order to determine the forward relay and the jammer, we illustrate a new relay/jammer selection protocol in this system. In order to explore the impact of cooperative jamming on the performance of covert communication, we introduce a jam-generating threshold into the theoretical framework and we further derive the expressions for three performance metrics, i.e., transmission outage probability, the detection error probability of warden and covert capacity. We also explore covert capacity maximization through efficient numerical searches under given covertness and outage requirements. Finally, we present extensive simulation and numerical results to validate our theoretical results and to demonstrate that cooperative jamming can improve the performance of covert communication by confusing the warden.

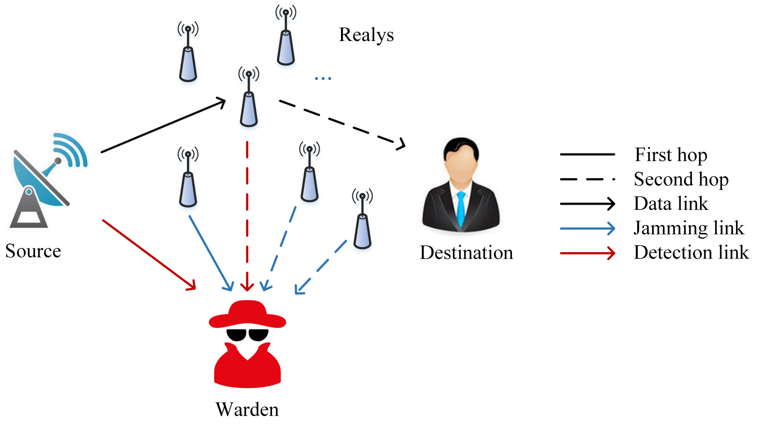


Figure 4.1: Covert communication scenario.

4.1 System Model and Performance Metrics

4.1.1 System Model

The two-hop wireless network, where a message is first transmitted from its source to intermediate relay(s) and then forwarded by the relay(s) to its destination, is a crucial network model and is widely used in wireless communications. In this work, we consider a two-hop wireless network (depicted in Fig.(4.1)), consisting of a sensing source S, a destination D, n legitimate relays R_1,R_2,R_3,...,R_n, and a warden $Willie$. Each node employs a single antenna and operates in a half-duplex mode. The direct link between S and D is assumed to be unavailable due to deep fading or limited transmit power. With the two-hop relay routing, S first transmits the message to a relay, and the relay then forwards the message to D. In particular, S selects a relay R_b to forward the message and selects some of the remaining relays helper jammers R_j to send jamming signals to confuse $Willie$. $Willie$ always observes the environment passively and silently, and tries to detect whether S and R_b are transmitting the message or not in two hops, respectively. We assume that S and R_b employ the same power to transmit the message, all R_j employ the same power to generate artificial noise, and there is a maximum power constraint P_{max}. We assume that the time is evenly divided into equal-sized time slots, and the independent quasi-static Rayleigh fading is used to model wireless channels in our work, where each channel keeps unchanged in a time slot, but randomly and independently from the current time slot to the next one. The channel coefficient $h_{k,l}$ of link $k \to l$ is modeled as complex Gaussian random variables with zero mean and unit variance. There are in total five channels in the system, i.e., the channel from S to relay, the one from relay to D, the one from relay to relay, the one from S to $Willie$ and the one from relay to $Willie$ whose channels coefficients are denotes as $h_{S,R}$, $h_{R,D}$, $h_{R,R}$, $h_{S,W}$ and $h_{R,W}$, respectively. The $|h_k|^2$ is the channel gain, where $k \in \{SR, RD, RR, SW, RW\}$. We assume that S and relay know $|h_{S,R}|^2$, $|h_{R,D}|^2$, and $|h_{R,R}|^2$. We also assume $Willie$ knows $|h_{S,W}|^2$ and $|h_{R,W}|^2$. In addition, the channel noise is AWGN with variance σ^2. We assume that the system bandwidth is W MHZ. Without loss of generality, we assume $W = 1$ throughout this work.

4.1.2 Performance Metrics

To decide whether transmitter is transmitting message or not, warden conducts two hypotheses, i.e., null hypothesis H_0 and alternative hypothesis H_1. The former represents that transmitter does not transmit covert message while the latter represents that it transmits. Then, we define two performance metrics as follows.

Detection error probability: It is the probability that warden makes a wrong decision on whether or not transmitter is transmitting covert message, which is expressed as

$$\zeta = \mathbb{P}_{FA} + \mathbb{P}_{MD}, \tag{4.1}$$

where ζ denotes the detection error probability. $\mathbb{P}_{FA}$ denotes the probability of false alarm that warden trusts H_1, while H_0 is true. $\mathbb{P}_{MD}$ denotes the probability of missed detection that warden trusts H_0, while H_1 is true.

Covert capacity: It is defined as the covert rate at which message from S is transmitted covertly to D with high detection error probability at warden. In our study, we consider that the warden detects S at the first hop and detects R_b at the second hop. According to our previous assumptions about the transmit power, the detection situation of the second hop is the same as that of the first hop. Therefore, we give the expected value of the covert capacity under two relay selection schemes.

4.2 Protocol Design with Cooperative Jamming

In this work, we assume that the whole transmission can be conducted in one slot. We need to design the relay selection and cooperative jamming protocols.

4.2.1 Relay Selection Protocol Design

For the two-hop scenario where there are multiple relays, we propose two relay selection schemes. The first one is the random relaying scheme which means S randomly chooses one message relay from all the relays before the S to D transmission is conducted in two hops. Another one is the superior relaying scheme which means S selects one message relay with the largest $\min\{|h_{S,R_n}|^2, |h_{R_n,D}|^2\}$ and satisfies the no outage requirement.

4.2.2 Cooperative Jamming Protocol Design

To better guarantee covert communication, we consider cooperative jamming, a typical physical layer security method where helper jammers generate artificial noise to resist the adversaries.

In the first hop, once S chooses the message relay R_b, then S determines the helper jammers among the remaining relays. In order to use resources reasonably, we assume that the relays with indices in $\mathcal{R}_1 = \{j|j \neq b, |h_{R_j,R_b}|^2 < \alpha\}$ serve as helper jammers to confuse warden, where α is the jam-generating threshold to control the interference received by the receiver. In the second hop, if R_b is successful in decoding the message, relays with indices in $\mathcal{R}_2 = \{j | j \neq b, |h_{R_j,D}|^2 < \alpha\}$ serve as helper jammers to generate artificial noise.

Based on the two message relay selection schemes we mentioned previously, the transmission situations of the second hop are different. Under the random relaying scheme, if R_b is successful in decoding the message from S, it re-encodes the message and then transmits it to D in the second hop. If R_b fails to decode the message, there will occur a transmission outage and S then decides to suspend the transmission. Under the superior relaying scheme, according to our requirement for the channel gain, there will not occur transmission outage.

4.3 Performance Analysis and Optimization

In this section, we first propose the transmission strategy of source and then derive the detection error probability of the warden. We also explore covert capacity under the relay/jammer selection protocol.

4.3.1 Performance Analysis and Optimization under Random Relaying Scheme

4.3.1.1 Transmission Strategy

Based on the relay selection scheme, we assume S randomly chooses one message relay R_b from all relays without considering the quality of channel at the first hop, which may result in transmission outage once if the signal-to-noise (SNR) at R_b is smaller than its required threshold θ. The received signal at R_b can be formulated as

$$y_{R_b} = \sqrt{P_s} h_{S,R_b} x_s + \sum_{j \in \mathcal{R}_1} \sqrt{P_J} h_{R_j,R_b} x_j + n_{R_b}, \tag{4.2}$$

and the received signal at D can be formulated as

$$y_D = \sqrt{P_{R_b}} h_{R_b,D} x_r + \sum_{j \in \mathcal{R}_2} \sqrt{P_J} h_{R_j,R_b} x_j + n_D. \tag{4.3}$$

Accordingly, the SINR at R_b is determined as

$$\gamma_{R_b} = \frac{P_s |h_{S,R_b}|^2}{\sum_{j \in \mathcal{R}_1} P_J |h_{R_j,R_b}|^2 + \sigma_{R_b}^2}, \tag{4.4}$$

the SINR at D is determined as

$$\gamma_D = \frac{P_{R_b} |h_{R_b,D}|^2}{\sum_{j \in \mathcal{R}_2} P_J |h_{R_j,R_b}|^2 + \sigma_D^2}, \tag{4.5}$$

where the P_s and P_{R_b} are the transmission power of S and R_b subject to maximum power constraint P_{max}, and P_J is the jamming power. The x_s, x_r and x_j are the transmitted symbols of of S, R_b, and $\mathcal{R}_1$, respectively. The $n_{R_b} \sim \mathcal{CN}(0, \sigma_{R_b}^2)$ and $n_D \sim \mathcal{CN}(0, \sigma_D^2)$ represents the received noise at R_b and D, respectively.

4.3.1.2 Detection Error Probability

We consider that $Willie$ detects S at the first hop and then detects R_b at the second hop. According to our previous assumptions about the transmit powers of S, R_b and P_J, the detection situation of the second hop is the same as that of the first hop. Therefore, we first analyze how $Willie$ performs the hypothesis test in the first hop and we can deduce the detection error probability of $Willie$ later.

1. Hypothesis test

In the first hop, the received signal y_w of $Willie$ under the random relaying scheme is given by

$$y_w = \begin{cases} \sum_{j \in \mathcal{R}_1} \sqrt{P_J} h_{R_j,W} x_j + n_w, & \text{if } H_0 \text{ is true} \\ \sqrt{P_s} h_{S,W} x_s + \sum_{j \in \mathcal{R}_1} \sqrt{P_J} h_{R_j,W} x_j + n_w, & \text{if } H_1 \text{ is true} \end{cases} \tag{4.6}$$

where $n_w \sim \mathcal{CN}(0, \sigma_w^2)$ represents the received noise of $Willie$. According to the previous analysis $T = 1/m \sum_{i=1}^{n} |y_w^i|^2$, which is determined as

$$T = \begin{cases} \sum_{j \in \mathcal{R}_1} P_J |h_{R_j,W}|^2 + \sigma_w^2, & \text{if } H_0 \text{ is true} \\ P_s |h_{S,W}|^2 + \sum_{j \in \mathcal{R}_1} P_J |h_{R_j,W}|^2 + \sigma_w^2. & \text{if } H_1 \text{ is true} \end{cases} \tag{4.7}$$

2. Detection error probability of $Willie$

It is determined as following under the random relaying scheme,

$$\zeta = \mathbb{P}_{FA} + \mathbb{P}_{MD}, \tag{4.8}$$

where

$$\mathbb{P}_{FA} = \begin{cases} \frac{\Gamma(l)}{(l-1)!}, & \text{if } \lambda \geq \sigma_w^2 \\ 1, & \text{otherwise} \end{cases} \tag{4.9}$$

and

$$\mathbb{P}_{MD} = \begin{cases} 1 - \left(\frac{P_s}{P_s - P_J} \right)^l \exp\left(\frac{\sigma_w^2 - \lambda}{P_s} \right), & \text{if } \lambda > \sigma_w^2 \\ 0, & \text{otherwise} \end{cases} \tag{4.10}$$

where l is the number of relays actually serving as helper jammers in $\mathcal{R}_1$, $a = (\lambda -$

$\sigma_w^2)/P_J$ and gamma function $\Gamma(l)$ is given by

$$\Gamma(l) = \int_0^\infty x^{(l-1)}\exp^{-x}\,dx.$$

Then the formula (4.32) can be rewritten as

$$\zeta = \begin{cases} 1 + \dfrac{\Gamma(l)}{(l-1)!} - \left(\dfrac{P_s}{P_s - P_J}\right)^l \exp\left(\dfrac{\sigma_w^2 - \lambda}{P_s}\right), \text{if}\, \lambda \geq \sigma_w^2 \\ 1. \qquad \text{otherwise} \end{cases} \tag{4.11}$$

Proof : Z is defined as the event that there are l relays actually serve as helper jammers in the first hop.

$$\begin{aligned} \mathbb{P}_{FA} &= P(\sum_{j\in\mathcal{R}_1} P_J |h_{R_j,W}|^2 + \sigma_w^2 \geq \lambda) \\ &= P\left(\sum_{j\in\mathcal{R}_1} |h_{R_j,W}|^2 \geq \frac{\lambda - \sigma_w^2}{P_J}\right) \\ &= \int_{\left(\frac{\lambda-\sigma_w^2}{P_J}\right)}^{\infty} f_{\sum_{j\in\mathcal{R}_1}|h_{R_j,W}|^2}(x)dx. \end{aligned} \tag{4.12}$$

As we known, the PDF (probability density function) of $|h_{R_j,W}|^2$ for any $j \in \mathcal{R}_1$ is

$$f_{|h_{R_j,W}|^2}(x) = e^{-x}, \text{if}\, 0 < x < \infty \tag{4.13}$$

By using the convolution theorem, we deduce the PDF of $\sum_{j\in\mathcal{R}_1} |h_{R_j,W}|^2$ as

$$f_{\sum_{j\in\mathcal{R}_1}|h_{R_j,W}|^2}(x) = \frac{1}{(l-1)!}x^{(l-1)}e^{-x}, \text{if}\, 0 < x < \infty \tag{4.14}$$

hence, the expression (4.9) can be obtained.

Next, applying the law of total probability, the expression of $\mathbb{P}_{MD}$ is given by

$$\begin{aligned}
\mathbb{P}_{MD} &= P(P_s|h_{S,W}|^2 + \sum_{j\in\mathcal{R}_1} P_J|h_{R_j,W}|^2 + \sigma_w^2 < \lambda) \\
&= \sum_{l=0}^{n-1} P(P_s|h_{S,W}|^2 + \sum_{j\in\mathcal{R}_1} P_J|h_{R_j,W}|^2 + \sigma_w^2 < \lambda|Z)P(Z) \\
&= \mathbb{E}_{|h_{R_j,W}|^2, j\in\mathcal{R}_1}\left[1 - \exp\left(\frac{\sum_{j\in\mathcal{R}_1} P_J|h_{R_j,W}|^2 + \sigma_w^2 - \lambda}{P_s}\right)\right] \\
&= 1 - \mathbb{E}_{|h_{R_j,W}|^2, j\in\mathcal{R}_1}\exp\left(\frac{\sum_{j\in\mathcal{R}_1} P_J|h_{R_j,W}|^2 + \sigma_w^2 - \lambda}{P_s}\right) \\
&= 1 - \exp\left(\frac{\sigma_w^2 - \lambda}{P_s}\right)\prod_{j\in\mathcal{R}_1}\mathbb{E}_{|h_{R_j,W}|^2, j\in\mathcal{R}_1}\exp\left(\frac{P_J|h_{R_j,W}|^2}{P_s}\right) \\
&= 1 - \exp\left(\frac{\sigma_w^2 - \lambda}{P_s}\right)\prod_{j\in\mathcal{R}_1}\int_0^\infty \exp\left(\frac{P_J|h_{R_j,W}|^2}{P_s}\right) f_{|h_{R_j,W}|^2}(x)dx, \qquad (4.15)
\end{aligned}$$

where $\mathbb{E}(\cdot)$ is expectation function.

To achieve covert communication, detection error probability of $Willie$ should satisfy $\zeta \geq 1 - \varepsilon$ for any $\varepsilon > 0$, when m tends to infinity [48].

Under the case of $\lambda \leq \sigma_w^2$, $\zeta = 1$. This means that $Willie$ cannot detect the transmission from S to R_b absolutely, we consider this $Willie$ is incompetent. Thus, we only consider the case of $\lambda > \sigma_w^2$. Take the derivation of (4.11) with respect to λ, we have

$$\frac{\partial\zeta}{\partial\lambda} = -\frac{(\lambda - \sigma_w^2)^{(l-1)}\exp(\frac{\sigma_w^2 - \lambda}{P_J})}{P_J(l-1)!} + \frac{1}{P_s}\left(\frac{P_s}{P_s - P_J}\right)^l \exp\left(\frac{\sigma_w^2 - \lambda}{P_s}\right). \qquad (4.16)$$

Let λ^* denotes the solution of $\frac{\partial\zeta}{\partial\lambda} = 0$, then we have the optimal threshold $\lambda^\dagger = \lambda^*$ to achieve the minimum value of ζ, i.e., $\zeta^\dagger = \zeta(\lambda^\dagger)$.

4.3.1.3 Covert Capacity

1. Transmission outage probability

To derive the covert capacity, we first determine the transmission outage probability for transmission from S to D. If the received signal strength at the receiver is smaller than its required threshold θ, which means that it fails to decode the message, we determine that there is a transmission outage. In a two-hop wireless network, ensuring that the transmission of each hop is reliable can ensure the reliability of the entire transmission. Therefore, the transmission outage probability (TOP) can be expressed as

$$\begin{aligned} P_{to} &= P(SIR_{S,R_b} < \theta \bigcup SIR_{R_b,D} < \theta) \\ &= 1 - \exp\left(-\frac{\theta(\sigma_{R_b}^2 + \sigma_D^2)}{P_s}\right)\left[\frac{1-e^{(-\alpha(1+K))}}{(1+K)(1-e^{-\alpha})}\right]^{2n-2}, \end{aligned} \tag{4.17}$$

where $K = \theta P_J / P_s$.

Proof : The TOP of a two-hop wireless network is expressed as

$$\begin{aligned} P_{to} &= P(SIR_{S,R_b} < \theta \bigcup SIR_{R_b,D} < \theta) \\ &= 1 - P(SIR_{S,R_b} \geq \theta \bigcap SIR_{R_b,D} \geq \theta). \end{aligned} \tag{4.18}$$

Since the first and the second hop are independent of each other, and S and R_b use the same transmit power, we can obtain

$$P_{to} = 1 - P(SIR_{S,R_b} \geq \theta)P(SIR_{R_b,D} \geq \theta). \tag{4.19}$$

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

$$f_{|h_{R_j,R_b}|^2}(x) = \begin{cases} \dfrac{e^{-x}}{1-e^{-\alpha}}, & \text{if}\, 0 \leq x \leq \alpha \\ 0, & \text{if}\, x \geq \alpha \end{cases} \tag{4.20}$$

then,

$$
\begin{aligned}
&P(SIR_{S,R_b} \geq \theta) = P(\gamma_b \geq \theta)\\
=&P\left[|h_{S,R_b}|^2 \geq \frac{\theta(\sum_{j\in\mathcal{R}_1} P_J|h_{R_j,R_b}|^2 + \sigma^2_{R_b})}{P_s}\right]\\
=&\mathbb{E}\left[\exp\left(-\frac{\theta(\sum_{j\in\mathcal{R}_1} P_J|h_{R_j,R_b}|^2 + \sigma^2_{R_b})}{P_s}\right)\right]\\
=&\exp\left(-\frac{\theta\sigma^2_{R_b}}{P_s}\right)\prod_{j=1,j\neq b}\mathbb{E}\left[\exp\left(-\frac{\theta P_J|h_{R_j,R_b}|^2}{P_s}\right)\right]\\
=&\exp\left(-\frac{\theta\sigma^2_{R_b}}{P_s}\right)\prod_{j=1,j\neq b}\mathbb{E}\left[\int_0^\alpha \exp\left(-\frac{\theta P_J|h_{R_j,R_b}|^2}{P_s}\right) f_{|h_{R_j,R_b}|^2}(x)dx\right]\\
=&\exp\left(-\frac{\theta\sigma^2_{R_b}}{P_s}\right)\left[\frac{1-e^{(-\alpha(1+K))}}{(1+K)(1-e^{-\alpha})}\right]^{n-1}, \qquad (4.21)
\end{aligned}
$$

similarly,

$$
\begin{aligned}
&P(SIR_{R_b,D} \geq \theta)\\
=&\exp\left(-\frac{\theta\sigma^2_{D}}{P_s}\right)\left[\frac{1-e^{(-\alpha(1+K))}}{(1+K)(1-e^{-\alpha})}\right]^{n-1}. \qquad (4.22)
\end{aligned}
$$

Substituting (4.21) and (4.22) into (4.19), (4.17) can be obtained.

2. Expected covert capacity

According to the definition of the channel capacity C of a two-hop wireless network, we can get an expected value of the covert capacity C_{c1} under random relaying scheme as follows

$$
\begin{aligned}
C_{c1} &= C(1-P_{to})\\
&= \min\{C_1, C_2\}(1-P_{to}), \qquad (4.23)
\end{aligned}
$$

where C_1 and C_2 are the channel capacity of the first and second hop, respectively.

3. Covert capacity maximization

The objective of covert capacity maximization is to maximize the covert capacity C_{c1} while maintaining a high detection error probability of $Willie$. It can be formulated as the following optimization problem.

$$\begin{aligned} &\text{Maximize} \quad C_{c1}. && \text{(4.24a)} \\ &s.t. \quad \zeta^{\dagger}(P_s) \geq 1 - \varepsilon_c, && \text{(4.24b)} \\ &\qquad P_{to}(n, \alpha) \leq \varepsilon_{to}, && \text{(4.24c)} \\ &\qquad \varepsilon_c \in (0, 1), && \text{(4.24d)} \\ &\qquad \varepsilon_{to} \in (0, 1), && \text{(4.24e)} \end{aligned}$$

where ε_c is the covertness requirement and ε_{to} is the TOP requirement. In order to achieve a satisfactory covert capacity, we must limit the TOP as (4.24c) by finding the optimal α with the number of relays in this system.

4.3.2 Performance Analysis and Optimization under Superior Relaying Scheme

In this section, we also first propose the transmission strategy of S and then derive detection error probability of the warden. We also explore the covert capacity under the relay/jammer selection protocol.

4.3.2.1 Transmission Strategy

Based one the superior relaying scheme, we assume S chooses one message relay R_b with the largest $\min\{|h_{S,R_n}|^2, |h_{R_n,D}|^2\}$ and there will not occur transmission outage. Furthermore, if no relay can satisfy this condition, S stops transmission.

The received signal at R_b can be formulated as

$$y_{R_b} = \sqrt{P_s} h_{S,R_b} x_s + \sum_{j \in \mathcal{R}_1} \sqrt{P_J} h_{R_j,R_b} x_j + n_{R_b}, \tag{4.25}$$

and the received signal at D can be formulated as

$$y_D = \sqrt{P_{R_b}} h_{R_b,D} x_r + \sum_{j \in \mathcal{R}_2} \sqrt{P_J} h_{R_j,R_b} x_j + n_D. \tag{4.26}$$

Accordingly, the SINR at R_b is determined as

$$\gamma_{R_b} = \frac{P_s |h_{S,R_b}|^2}{\sum_{j \in \mathcal{R}_1} P_J |h_{R_j,R_b}|^2 + \sigma^2_{R_b}}, \tag{4.27}$$

the SINR at D is determined as

$$\gamma_D = \frac{P_{R_b} |h_{R_b,D}|^2}{\sum_{j \in \mathcal{R}_2} P_J |h_{R_j,R_b}|^2 + \sigma^2_D}, \tag{4.28}$$

where the P_s and P_{R_b} are the transmission power of S and R_b subject to maximum power constraint P_{max}, and P_J is the jamming power. The $n_{R_b} \sim \mathcal{CN}(0, \sigma^2_{R_b})$ represents the received noise at R_b.

Notice our transmission condition $SIR_{S,R_b} \geq \theta$ and $P_s = P_{R_b}$, we have $|h_{S,R_b}|^2 \geq \theta(\sum_{j \in \mathcal{R}_1} P_J |h_{R_j,R_b}|^2 + \sigma^2_{R_b})/P_s$ and then we have

$$P_s = \frac{\theta(\sum_{j \in \mathcal{R}_1} P_J |h_{R_j,R_b}|^2 + \sigma^2_{R_b})}{|h_{S,R_b}|^2} \tag{4.29}$$

4.3.2.2 Detection Error Probability

Similar to the random relaying scheme, we give the hypothesis test and the detection error probability of the $Willie$.

1. Hypothesis test

In the first hop, the received signal y_w at the $Willie$ under the random relaying scheme is given by

$$y_w = \begin{cases} \sum_{j\in\mathcal{R}_1} \sqrt{P_J} h_{R_j,W} x_j + n_w, & \text{if } H_0 \text{ is true} \\ \sqrt{P_s} h_{S,W} x_s + \sum_{j\in\mathcal{R}_1} \sqrt{P_J} h_{R_j,W} x_j + n_w, & \text{if } H_1 \text{ is true} \end{cases} \tag{4.30}$$

where $n_w \sim \mathcal{CN}(0, \sigma_w^2)$ represents the received noise at the $Willie$. Based on (3.7), (4.29) and (4.30), T is determined as

$$T = \begin{cases} \sum_{j\in\mathcal{R}_1} P_J |h_{R_j,W}|^2 + \sigma_w^2, & \text{if } H_0 \text{ is true} \\ \dfrac{\theta(\sum_{j\in\mathcal{R}_1} P_J |h_{R_j,R_b}|^2 + \sigma_{R_b}^2)|h_{S,W}|^2}{|h_{S,R_b}|^2} & \\ + \sum_{j\in\mathcal{R}_1} P_J |h_{R_j,W}|^2 + \sigma_w^2. & \text{if } H_1 \text{ is true} \end{cases} \tag{4.31}$$

2. Detection error probability of $Willie$

Based on (4.31), the detection error probability of $Willie$ can be determined as

$$\zeta = \mathbb{P}_{FA} + \mathbb{P}_{MD}, \tag{4.32}$$

where

$$\mathbb{P}_{FA} = \begin{cases} \dfrac{\Gamma(l)}{(l-1)!}, & \text{if } \lambda \geq \sigma_w^2 \\ 1, & \text{otherwise} \end{cases} \tag{4.33}$$

and

$$\mathbb{P}_{MD} = \begin{cases} 1 - \left(\dfrac{1}{1-\varphi}\right)^l \exp\left(\dfrac{\varphi(\sigma_w^2 - \lambda)}{P_J}\right), & \text{if} \, \lambda > \sigma_w^2 \\ 0, & \text{otherwise} \end{cases} \tag{4.34}$$

where Γ is Gamma distribution, l is the number of relays actually serving as helper jammers in $\mathcal{R}_1$, $b = (\lambda - \sigma_w^2)/P_J$ and $\varphi = (P_J|h_{S,R_b}|^2)/\theta(\sum_{j \in \mathcal{R}_1} P_J |h_{R_j,R_b}|^2 + \sigma_{R_b}^2)$. Then the formula (4.32) can be rewritten as

$$\zeta = \begin{cases} 1 + \dfrac{\Gamma(l)}{(l-1)!} - \left(\dfrac{1}{1-\varphi}\right)^l \exp\left(\dfrac{\varphi(\sigma_w^2 - \lambda)}{P_J}\right), & \text{if} \, \lambda \geq \sigma_w^2 \\ 1. & \text{otherwise} \end{cases} \tag{4.35}$$

Proof : The proof of $\mathbb{P}_{FA}$ is similar to the random relaying scheme. Then, we also define Z as the event that there are l relays actually serve as helper jammers in the first hop. By applying the law of total probability, the expression of $\mathbb{P}_{MD}$ is given by

$$\begin{aligned}
\mathbb{P}_{MD} &= P(P_s|h_{S,W}|^2 + \sum_{j \in \mathcal{R}_1} P_J |h_{R_j,W}|^2 + \sigma_w^2 < \lambda) \\
&= \sum_{l=0}^{n-1} P(P_s|h_{S,W}|^2 + \sum_{j \in \mathcal{R}_1} P_J |h_{R_j,W}|^2 + \sigma_w^2 < \lambda | Z) P(Z) \\
&= \sum_{l=0}^{n-1} P\left[\frac{\theta(\sum_{j \in \mathcal{R}_1} P_J |h_{R_j,R_b}|^2 + \sigma_{R_b}^2)}{|h_{S,R_b}|^2} |h_{S,W}|^2 + \sum_{j \in \mathcal{R}_1} P_J |h_{R_j,W}|^2 + \sigma_w^2 < \lambda\right] P(Z) \\
&= \mathbb{E}_{|h_{R_j,W}|^2, j \in \mathcal{R}_1}\left[1 - \exp\left(\frac{(\sum_{j \in \mathcal{R}_1} P_J |h_{R_j,W}|^2 + \sigma_w^2 - \lambda)|h_{S,R_b}|^2}{\theta(\sum_{j \in \mathcal{R}_1} P_J |h_{R_j,R_b}|^2 + \sigma_{R_b}^2)}\right)\right] \\
&= 1 - \exp\left[\frac{(\sigma_{R_b}^2 - \lambda)\varphi}{P_J}\right] \prod_{j \in \mathcal{R}_1} \mathbb{E}_{|h_{R_j,W}|^2, j \in \mathcal{R}_1} \exp(|h_{R_j,W}|^2 \varphi) \\
&= 1 - \exp\left[\frac{(\sigma_{R_b}^2 - \lambda)\varphi}{P_J}\right] \prod_{j \in \mathcal{R}_1} \int_0^\infty \exp(|h_{R_j,W}|^2 \varphi) f_{|h_{R_j,W}|^2}(x) dx,
\end{aligned} \tag{4.36}$$

where $\mathbb{E}(\cdot)$ is expectation function.

The covert communication can be achieved if $\zeta \geq 1 - \varepsilon$ for any $\varepsilon > 0$. Under the case of $\lambda \leq \sigma_w^2$, $\zeta = 1$. This means that $Willie$ cannot detect the transmission from S to R_b absolutely, we can consider this $Willie$ is incompetent. Thus, we only consider the case of $\lambda > \sigma_w^2$. Take the derivation of (4.35) with respect to λ, we have

$$\begin{aligned}\frac{\partial \zeta}{\partial \lambda} = & -\frac{(\lambda - \sigma_w^2)^{(l-1)}\exp(\frac{\sigma_w^2 - \lambda}{P_J})}{P_J(l-1)!} \\ & + \frac{\varphi}{P_J}(\frac{1}{1-\varphi})^l \exp(\frac{\varphi(\sigma_w^2 - \lambda)}{P_J}). \end{aligned} \tag{4.37}$$

Let $\lambda^\dagger$ denotes the solution of $\frac{\partial \zeta}{\partial \lambda} = 0$, then we have the optimal threshold $\lambda^\dagger = \lambda^*$ to achieve the minimum value of ζ, i.e., $\zeta^\dagger = \zeta(\lambda^\dagger)$.

4.3.2.3 Covert Capacity

1. Expected covert capacity

Similarly, we can get an expected value of the covert capacity C_{c2} under the superior relaying scheme as

$$C_{c2} = C = \min\{C_1, C_2\}, \tag{4.38}$$

where C_1 and C_2 are the channel capacity of the first and second hop, respectively.

In addition, the outage probability under the superior relaying scheme is given by (4.39), which means that the link of selected message relay still has the possibility of outage subject to the number of relays n and jam-generating threshold α. Based on

(5.32), we have

$$
\begin{aligned}
&P_{sto} = P(\min\{SIR_{S,R_b}, SIR_{R_b,D}\} < \theta)\\
&= \sum_{0}^{n} \binom{n}{k} (-1)^k \frac{1}{2k-1} k\exp\left[-\frac{\theta(P_J \sum_{j\in\mathcal{R}_1} |h_{R_b,R_j}|^2 + \sigma^2_{R_b})}{P_s}\right]\\
&+ \sum_{0}^{n} \binom{n}{k} (-1)^k \frac{1}{2k-1} (k-1)\exp\left[-2k\frac{\theta(P_J \sum_{j\in\mathcal{R}_1} |h_{R_b,R_b}|^2 + \sigma^2_{R_b})}{P_s}\right]\\
&= \sum_{0}^{n} \binom{n}{k} (-1)^k \frac{1}{2k-1} k\exp\left(\frac{-\theta\sigma^2_{R_b}}{P_s}\right) \prod_{j\in\mathcal{R}_1} \mathbb{E}_{|h_{R_b,R_j}|^2}\left[\exp(-z\sum_{j\in\mathcal{R}_1} |h_{R_b,R_j}|^2)\right]\\
&+ \sum_{0}^{n} \binom{n}{k} (-1)^k \frac{1}{2k-1} (k-1)\exp\left(\frac{-\theta\sigma^2_{R_b}}{P_s}\right) \prod_{j\in\mathcal{R}_1} \mathbb{E}_{|h_{R_b,R_j}|^2}\left[\exp(-2kz\sum_{j\in\mathcal{R}_1} |h_{R_b,R_j}|^2)\right]\\
&= \sum_{0}^{n} \binom{n}{k} (-1)^k \frac{1}{2k-1} \exp\left(\frac{-\theta\sigma^2_{R_b}}{P_s}\right) k \left[\frac{1-e^{-(1+z)\alpha}}{(1-e^{-\alpha})(1+z)}\right]^l\\
&+ \sum_{0}^{n} \binom{n}{k} (-1)^k \frac{1}{2k-1} \exp\left(\frac{-\theta\sigma^2_{R_b}}{P_s}\right) (k-1) \left[\frac{1-e^{-(2kz+1)\alpha}}{(1-e^{-\alpha})(2kz+1)}\right]^l \qquad (4.39)
\end{aligned}
$$

where $z = \theta P_{R_b}/P_s$. In this work, the transmission strategy of S is to select a relay that satisfies the no outage condition before transmission. Therefore, there is no effect on the covert capacity in a time slot. However, the n and α affect the number of times that covert communication occurs over a period of time.

2. Covert capacity maximization

The objective of covert capacity maximization is to maximize the covert capacity C_{c2} while maintaining a high detection error probability of $Willie$. It can be formulated as the following optimization problem.

$$\text{Maximize} \quad C_{c2}. \qquad (4.40a)$$

$$s.t. \quad \zeta^{\dagger}(P_s) \geq 1 - \varepsilon_c, \qquad (4.40b)$$

$$\varepsilon_c \in (0,1), \qquad (4.40c)$$

where ε_c is the covertness requirement and ε_{ct} is the covert transmission requirement.

Condition (4.40b) is satisfied, which means that covert communication is achieved. Unitizing numerical search, we can easily solve the one dimensional optimization problem in (4.40). By substituting $P_s^\dagger$ into (4.38), the optimal value of n and α, we then obtain the maximum capacity denoted as C^*.

4.4 Numerical Results

In this section, we first validate our theoretical analysis for the transmission outage probability under the random relaying scheme as well as the detection error probability of $Willie$ under two relay selection schemes through extensive simulations, and then explore how the system parameters affect the ζ and covert capacity.

4.4.1 Validation

For the transmission outage probability under random relaying scheme, the total number of transmissions is fixed as 100000 with the corresponding random CSI and the transmission outage probability is measured as the ratio of the number of transmissions suffering from transmission outage to the total number of transmissions. We conduct extensive simulations with the setting of number of relays $n = 50$, jam-generating threshold $\alpha = \{0.3, 0.5, 0.7\}$, transmission power $P_s = 5$ W, threshold $\theta = 1$ jamming power $P_J = 1$ W and received noise $\sigma_{R_b}^2 = \sigma_D^2 = -5$ dB. We can see from Fig.(4.2) that for each α, the theoretical transmission outage probability P_{to} almost matches with the simulation one. The mean of transmission outage probability P_{to} with 50 relays are summarized in Table 4.1.

Obviously we can see that for the same α, as the number of relays increases, the probability of transmission outage continues to increase. This is because the number of jamming relays that meet the threshold conditions increases, resulting in a decrease in the SNR. Similarly, if the α is increased, the relays as jammer will also increase.

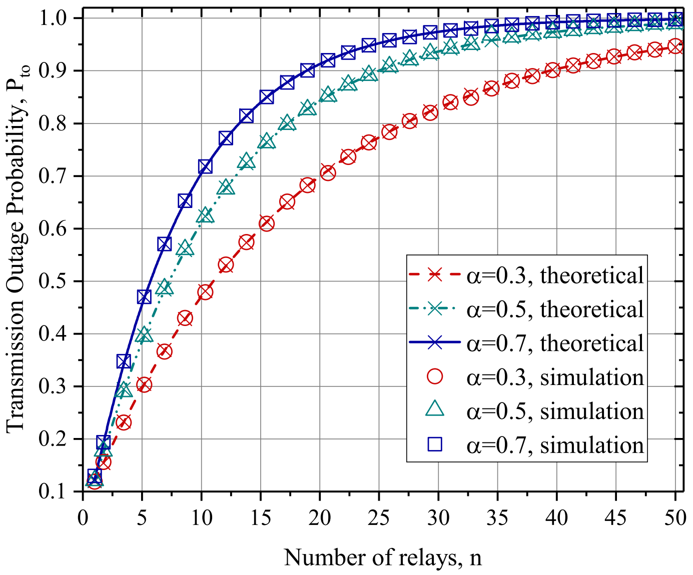


Figure 4.2: Transmission outage probability validation.

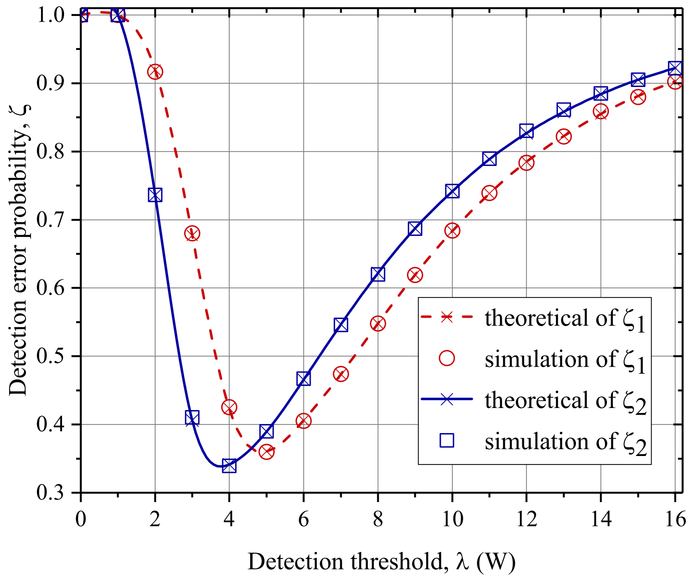


Figure 4.3: Detection error probability validation.

We first explore the impact of detection threshold λ on the detection error probability ζ under these two relay selection schemes is summarized in Fig.(4.4). For the detection error probability of *Willie* under two relay selection schemes, CSI is generated randomly and 17 sample points of detection threshold λ are set. *Willie* performs 100000 detections with the corresponding random CSI and λ. Based on the total detection error probability, we obtain the average value of ζ at each sample point of λ.

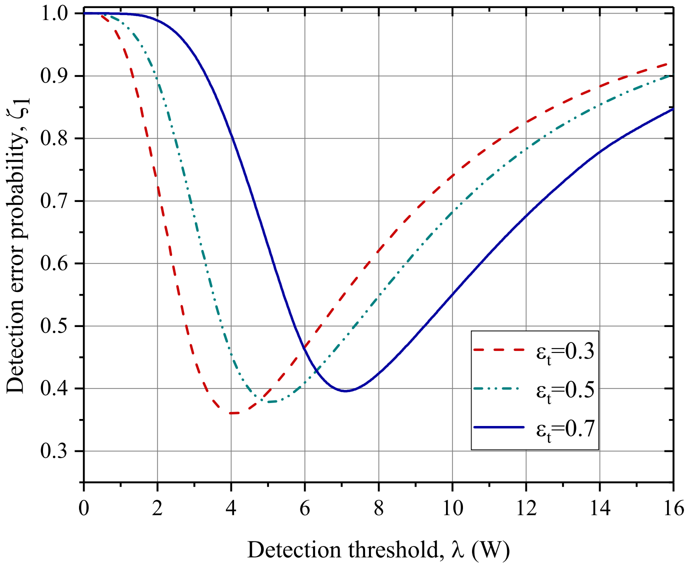
Table 4.1: Mean of transmission outage probability

	α=0.3	α=0.5	α=0.7
Theoretical	0.822	0.914	0.948
Simulation	0.831	0.909	0.953

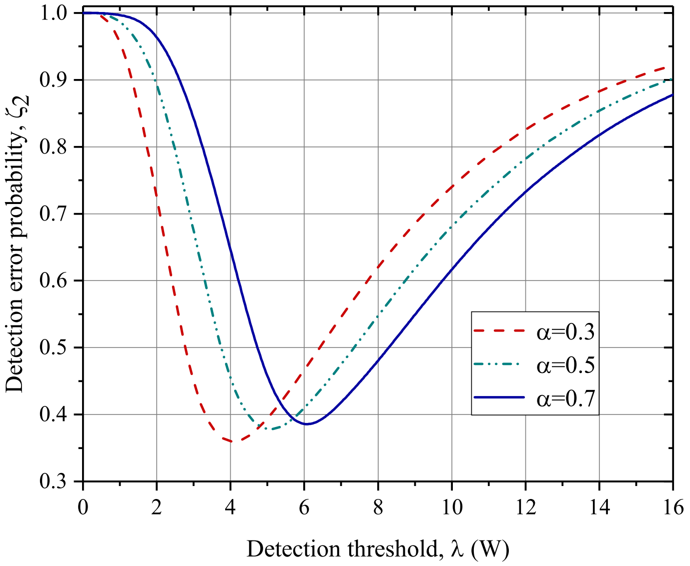
We compare the theoretical results with the simulation ones under the two relay selection schemes with the setting of jamming power $P_J = 1$ W and received noise $\sigma_w^2 = -5$ dB at $Willie$. We can observe from Fig.(4.3) that for each relay selection scheme, the theoretical ζ almost matches with the simulation one. This demonstrates that our theoretical results can well capture the performance of covert communication under these two relay selection schemes.

4.4.2 Covert Performance Analysis

How ζ varies with λ under the random relaying scheme is shown as Fig.(4.4(a)) with the setting of outage requirement $\varepsilon_{to} = \{0.3, 0.5, 0.7\}$, transmission power $P_s = 5$ W, threshold $\theta = 1$, jamming power $P_J = 1$ W, channel gain $|h_{S,R_b}|^2 = |h_{R_b,D}|^2 = 1$ and received noise $\sigma_w^2 = -5$ dB at $Willie$. According to the ε_{to}, we set the number of relays $n = 20$ and then determine the expected number of jammers l by the value of α. The Fig.(4.4(b)) shows how ζ varies with λ under the superior relaying scheme with the setting of $\alpha = \{0.3, 0.5, 0.7\}$ and the other parameters are same as former ones. We can observe from Fig.(4.4) that for each setting of ε_{to} and α, as λ increases, ζ first decreases and then increases under both the schemes. This can be explained as follows. We know that ζ is the sum of false alarm probability $\mathbb{P}_{FA}$ and missed detection probability $\mathbb{P}_{MD}$. It can be determined from our theoretical analysis that



(a) ζ vs. λ



(b) ζ vs. λ

Figure 4.4: The impact of detection threshold on detection error probability.

$\mathbb{P}_{FA}$ is a decreasing function of λ while $\mathbb{P}_{MD}$ is an increasing function. As λ is relative small, the former one dominates ζ, leading to the decreasing of ζ with λ. On the other hand, as λ further increases, the latter one dominates ζ, leading to the increasing of ζ. There exists a minimum ζ which means $Willie$ has the strongest detection ability to detect the transmission of two hops, then we can find a corresponding maximum transmission power limit of S and R_b. Fig.(4.4) also shows that for each fixed λ,

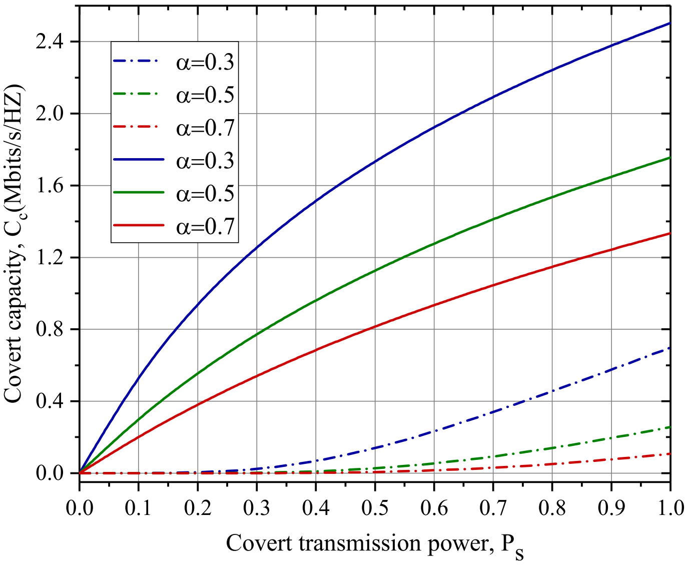


Figure 4.5: The impact of covert transmission power on covert capacity.

the minimum value of ζ increases with the increase of ε_c and α. This is because the increase in the number of jammer increases the noise power received at $Willie$, then increases the probability of detection errors.

To investigate the impact of covert transmit power P_s on the covert capacity C_c, we summarize in Fig.(4.5) how C_c varies with the increasing of P_s under these two relay selection schemes with the setting of $\alpha = \{0.3, 0.5, 0.7\}$ and $\sigma^2_{R_b} = \sigma^2_D = -5$ dB. We also set 20 relays and determine the expected number of jammers l by the value of α. In the Figures of showing that covert capacity and max covert capacity, the **dashed lines** and **solid lines** are used to show the results under the random relaying scheme and the superior relaying scheme, respectively. It can be observed from Fig.(4.5) that as P_s increases, C_c increases under both the schemes. This is because the increasing of P_s leads to the increasing of the SNR at the receiver. A careful observation of Fig.(4.5) indicates that for each fixed P_s, as α further increases, the C_c will decreases. The reason for this phenomenon is that the number of relays satisfying the selection conditions of the jammer increases, which leads to an increase in the total jamming power, then resulting in a decrease in the SNR of the receiver.

We can also see from that for each fixed P_s, C_c under the random relaying scheme is lower than that under the superior relaying scheme. This can be explained as follows. The channel quality of under the former is unstable and may cause transmission outage, hence the covert capacity will also be affected. However, the superior relaying scheme does not occur transmission outage, so the covert capacity will be higher compared to the random relaying scheme with the same covert transmit power which will reduce transmission cost in disguise when the transmitting power of covert message is constant.

4.4.3 Performance Optimization

We explore the impact of covertness requirement ε_c on the maximum covert capacity C^* under the two relay selection schemes. Fig.(4.6) illustrates that the impact

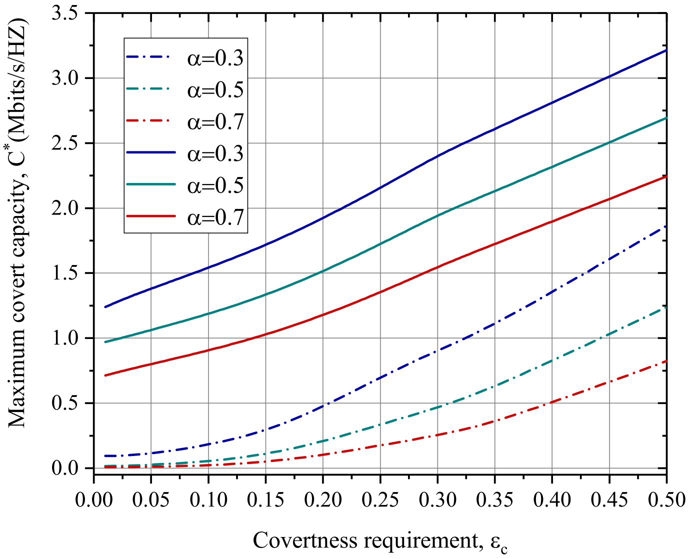


Figure 4.6: The impact of covertness requirement on maximum covert capacity.

of covertness requirement ε_c on the maximum covert capacity C^* under the two relay selection schemes with the setting of $\alpha = \{0.3, 0.5, 0.7\}$, $\sigma_{R_b}^2 = \sigma_D^2 = -5$ dB. For the random relaying scheme, regarding the transmission outage maybe occur, according to the expression of optimization problem, we set $n = 20$, then we get the expected number of the jammers and the ε_{to} according to the α. For the superior relaying scheme, according to the expression of optimization problem, the optimal transmission power P_s^* could be found through efficient numerical search.

We can observe from Fig.(4.6) that as ε_c increases, the C^* increases under the two relay selection schemes. This is because the increasing of ε_c leads to the increasing of the optimal transmission power P_s^*, which corresponds to an increase in the probability of transmission being detected. A careful observation of Fig.(4.6) indicates that for each fixed ε_c, as α increases, the maximum covert capacity C^* decreases, and the C^* under the random relaying scheme is less than that under the superior relaying scheme. The reason of this phenomenon is that the increase of α not only increases the jamming power but also increases the probability of transmission outage. Notice that under the superior relaying scheme, the maximum covert capacity C^* is related to only the optimal transmission power P_s^*. Thus, a higher covert capacity can be achieved without considering the transmission outage.

According to the previous analysis, it is worth noting that in order to reduce the transmission outage probability under the former relay selection scheme, S needs to increase the power to transmit its message within the maximum power constraint P_{max}. Unlike the former scheme, P_s^* can be adjusted according to P_J because the channel gain of the second scheme is excellent. Therefore, it can stably achieve a better maximum covert capacity and reduce the transmission cost under the superior relaying scheme in practical application.

4.5 Discussion

In this chapter, we introduce the cooperative jamming technology into relay-assisted wireless systems to confuse the warden under two relay selection schemes. We also derive the expressions for three performance metrics, i.e., transmission outage probability, the detection error probability of warden, and covert capacity. Then we explore the covert capacity maximization through efficient numerical searches under given covertness and outage requirements.

Relay-assisted systems are very common in practical applications and cooperative jamming technology is very suitable for application in such systems. In fact, the jamming signal not only has a confusing effect on the warden but also reduces the decoding rate of the receiver, thereby may damage the covert capacity. To fix this point, we use a jam-generating threshold α to control the effect of the jamming signal on the receiver as much as possible. Numerical analysis results prove that as the number of relays increases, the probability of the occurrence of relays that satisfy the jam-generating threshold and the conditions for forwarding relay will increase, but the workload of testing the channel status will also increase.

Therefore, we have discussed how to choose the relay selection scheme in the former chapter. For systems with a large number of relays, the use of cooperative jamming technology can increase the covert capacity, satisfy a higher covert requirement, and maximize the use of resources. In this chapter, we put forward a transmission scheme that joint cooperative jamming and relay selection, which extends the current researches of covert communication.

4.6 Summary

This chapter investigated the performance of cooperative Jamming based covert communication in a relay-assisted wireless system. To this end, we illustrate the relay/jammer selection scheme in this system. In order to explore the impact of cooperative jamming on the performance of covert communication, we introduce a jam-generating threshold into the theoretical framework and we then derive the expressions for three performance metrics, i.e., transmission outage probability, the detection error probability of warden and covert capacity. We also explore covert capacity maximization through efficient numerical searches under given covertness and outage requirements. Finally, we present extensive simulation and numerical results to validate our theoretical results, and to illustrate the impact of various parameters on detection error probability and covert capacity.

Numerical results indicate that the covert capacity increases with the increasing of covert transmit power under the two selection schemes, while the better maximum covert capacity is achieved under the superior relaying scheme. In particular, the impact of the covertness requirement on the maximum covert capacity exhibits similar behaviors under the proposed two relaying schemes. However, the jam-generating threshold is on the contrary. Although the increase of jam-generating threshold can increase the probability of detection error of warden, the maximum covert capacity is reduced due to excessive jamming power. Therefore, in actual applications, users should choose the appropriate jam-generating threshold according to the number of relays and the covertness requirement. Remarkably, the covert capacity performance under the superior relaying scheme is obviously more excellent in the case of power limitation.

CHAPTER V

Covert Communication in Relay-Assisted Wireless Systems with an Active Warden

In this chapter, we focus on the performance of covert communication in a scenario where the warden actively attacks the communication process as a jammer in relay-assisted wireless systems. We introduce a new transmission strategy and redefine the behavior of the warden that it performs detection and jamming throughout the covert communication process. Notice that the transmitter has to increase the transmission power to ensure successful decoding due to the jamming of the warden, and thus increases the risk of being detected. To deeply explore such interactions, based on the related relay selection protocol designed previously, we develop a new theoretical framework to analyze the transmission outage probability, the detection error probability of warden, and covert capacity. Then, we optimize the covert capacity through power control under given covertness and outage requirements. Finally, extensive simulation and numerical results are provided to illustrate our theoretical findings and the performance of covert communication with an active warden in such systems.

5.1 System Model and Performance Metrics

5.1.1 System Model

In this chapter, we still consider a two-hop wireless system with multiple relays, where a message is first transmitted from its source to intermediate relay(s) and then forwarded by the relay(s) to its destination. However, the actively attack from warden was not considered in the previous works. In this work, we consider a two-hop wireless network (depicted in Fig. 1), consisting of a sensing source S, a destination D, n legitimate relays R_1,R_2,R_3,...,R_n, and a warden $Willie$. Each node employs a single antenna and operates in a half-duplex mode except for $Willie$, which works in full-duplex mode. The direct link between source S and destination D is assumed to be unavailable due to deep fading or limited transmit power. With the two-hop relay routing, S first transmits messages to a relay and the relay then forwards the messages to D. In particular, S will select a relay R_b to forward messages. $Willie$ always observes the environment passively, silently and tries to detect whether the transmitter is transmitting message or not. Moreover, $Willie$ always actively sends jamming signals with a fixed power P_w to disrupt the transmission. We assume that S knows the fixed power P_w of $Willie$ and achieves the covert communication by adjusting its own transmission power P_s.

We assume that the time is evenly divided into equal-sized time slots, and the independent quasi-static Rayleigh fading is used to model wireless channels in our work, where each channel keeps unchanged in a time slot, but randomly and independently from the current time slot to the next one. The channel coefficient $h_{k,l}$ of link $k \to l$ is modeled as complex Gaussian random variables with zero mean and unit variance. There are in total six channels in the system, i.e., the channel from S to relay, the one from relay to D, the one from S to $Willie$, the one from relay to $Willie$, the one from D to $Willie$, and the one from $Willie$ to $Willie$ (self-interference), whose

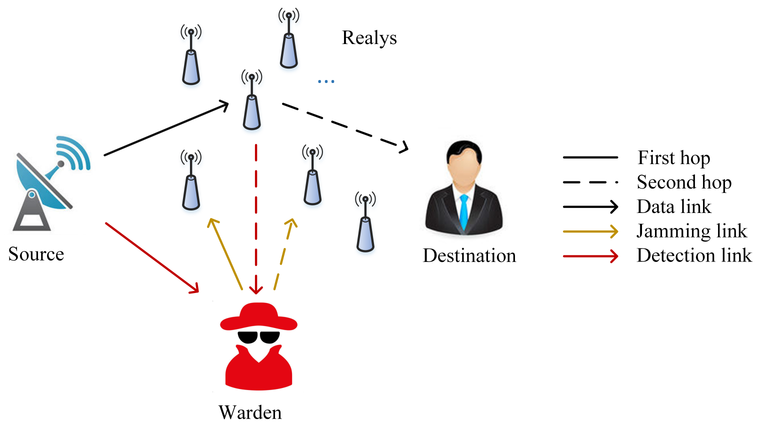


Figure 5.1: Covert communication scenario.

channels coefficients are denoted as $h_{S,R}$, $h_{R,D}$, $h_{S,W}$, $h_{R,W}$, $h_{D,W}$, and $h_{W,W}$, respectively. The $|h_{k,l}|^2$ is the channel gain that includes channel fading and path loss, where $k \in \{SR, RD, SW, RW, DW, WW\}$. We assume that S and relay know $|h_{S,R}|^2$ and $|h_{R,D}|^2$, and $Willie$ knows $|h_{S,W}|^2$, $|h_{D,W}|^2$, and $|h_{R,W}|^2$. In addition, the channel noise is AWGN with variance σ^2. We assume that the system bandwidth is W MHZ. Without loss of generality, we assume $W = 1$ throughout this paper.

5.1.2 Performance Metrics

To decide whether transmitter is transmitting message or not, $Willie$ conducts two hypotheses, i.e., null hypothesis H_0 and alternative hypothesis H_1. The former represents that transmitter does not transmit covert message while the latter represents that it transmits. Then, we define two performance metrics as follows.

Detection error probability: It is the probability that $Willie$ makes a wrong decision on whether or not transmitter is transmitting covert message, which is expressed as

$$\zeta = \mathbb{P}_{FA} + \mathbb{P}_{MD}, \tag{5.1}$$

where ζ denotes the detection error probability, $\mathbb{P}_{FA}$ denotes the probability of false alarm that $Willie$ trusts H_1, while H_0 is true, $\mathbb{P}_{MD}$ denotes the probability of missed detection that $Willie$ trusts H_0, while H_1 is true.

Covert capacity: It is defined as the covert rate that message from S is transmitted covertly to D with high detection error probability of $Willie$. In this work, we assume that $Willie$ detects the source S at first hop and the forward relay R_b at second hop. According to our previous assumptions about the transmit power, the detection situation of the second hop is the same as that of the first hop. Therefore, we give the expected value of the covert capacity under two relay selection schemes.

5.2 Protocol Design with an Active Warden

5.2.1 Relay Selection Protocol Design

In this work, we assume that the whole transmission, including the relay selection, can be conducted in one slot. For a two-hop scenario where there are multiple relays, we propose two relay selection schemes.

Random relaying scheme: S randomly chooses one message relay from all the relays before the S to D transmission is conducted in two hops with the random relaying scheme. This message relay is denoted as R_b and announces itself as the message relay before the transmission in the first hop.

Superior relaying scheme: To enhance the performance of covert communication, we propose the superior relaying scheme. The selected message relay is denoted as R_b, which with the largest $\min\{|h_{S,R_n}|^2, |h_{R_n,D}|^2\}$ ($|h_{S,R_n}|^2$ and $|h_{R_n,D}|^2$ represent the channel gain from S to the nth relay, and the one from the nth relay to D, respectively). It is worth noting that S does not know the channel gain between itself and $Willie$ and therefore cannot determine the condition for no outage transmission.

5.3 Performance Analysis and Optimization

In this section, we first propose the transmission strategy, then derive detection error probability of $Willie$ and covert capacity under the relay selection protocol.

5.3.1 Performance Analysis and Optimization under Random Relaying Scheme

5.3.1.1 Transmission Strategy

Based on the selection scheme, we assume S randomly chooses one message relay R_b from all relays without considering the quality of channel at the first hop, which may result in transmission outage once if the received signal strength at R_b is smaller than its required threshold θ. The received signal at R_b can be formulated as

$$y_{R_b} = \sqrt{P_s} h_{S,R_b} x_s + \sqrt{P_w} h_{R,W} x_w + n_{R_b}, \tag{5.2}$$

and the received signal at D can be formulated as

$$y_D = \sqrt{P_{R_b}} h_{R_b,D} x_r + \sqrt{P_w} h_{D,W} x_w + n_D. \tag{5.3}$$

Accordingly, the SINR at R_b is determined as

$$\gamma_{R_b} = \frac{P_s |h_{S,R_b}|^2}{P_w |h_{R,W}|^2 + \sigma_{R_b}^2}, \tag{5.4}$$

the SINR at D is determined as

$$\gamma_D = \frac{P_{R_b} |h_{R_b,D}|^2}{P_w |h_{D,W}|^2 + \sigma_D^2}, \tag{5.5}$$

where the P_s and P_{R_b} are the transmission power of S at the first hop and R_b at the second hop subject to maximum power constraint P_{max}, and P_w is the jamming power.

The x_s, x_r and x_w are the transmitted symbols of of S, R_b and $Willie$, respectively. The $n_b \sim \mathcal{CN}(0, \sigma_{R_b}^2)$ and $n_D \sim \mathcal{CN}(0, \sigma_D^2)$ represents the received noise at R_b and D, respectively.

5.3.1.2 Detection Error Probability

We consider that $Willie$ detects S at the first hop and then detects R_b at the second hop. According to our previous assumptions about the transmit powers of S, R_b and jamming power P_w of $Willie$, the detection situation of the second hop is the same as that of the first hop. Therefore, we first analyze how $Willie$ performs the hypothesis test in the first hop and we can deduce the detection error probability at $Willie$ later.

1. Hypothesis test

In the first hop, the received signal y_w at $Willie$ under the random relaying scheme is given by

$$y_w = \begin{cases} \sqrt{P_w} h_{W,W} x_w + n_w, & \text{if } H_0 \text{ is true} \\ \sqrt{P_s} h_{S,W} x_s + \sqrt{P_w} h_{W,W} x_w + n_w, & \text{if } H_1 \text{ is true} \end{cases} \tag{5.6}$$

where $n_w \sim \mathcal{CN}(0, \sigma_w^2)$ represents the received noise at $Willie$.

According to the previous analysis $T = 1/m \sum_{i=1}^{n} |y_w^i|^2$, so it is determined as

$$T = \begin{cases} P_w |h_{W,W}|^2 + \sigma_w^2, & \text{if } H_0 \text{ is true} \\ P_s |h_{S,W}|^2 + P_w |h_{W,W}|^2 + \sigma_w^2. & \text{if } H_1 \text{ is true} \end{cases} \tag{5.7}$$

2. Detection error probability of $Willie$

It can be determined as following under the random relaying scheme,

$$\zeta = \mathbb{P}_{FA} + \mathbb{P}_{MD}, \tag{5.8}$$

where

$$\begin{aligned}\mathbb{P}_{FA} &= P(P_w|h_{W,W}|^2 + \sigma_w^2 \geq \lambda) \\ &= \begin{cases} \exp\left(\dfrac{\sigma_w^2 - \lambda}{P_w}\right), \text{if}\, \lambda \geq \sigma_w^2 \\ 1, \qquad\qquad\qquad \text{otherwise} \end{cases}\end{aligned} \tag{5.9}$$

and

$$\begin{aligned}\mathbb{P}_{MD} &= P(P_s|h_{S,W}|^2 + P_w|h_{W,W}|^2 + \sigma_w^2 < \lambda) \\ &= \begin{cases} 1 + \left(\dfrac{P_w}{P_s - P_w}\right)\exp\left(\dfrac{\sigma_w^2 - \lambda}{P_w}\right) - \left(\dfrac{P_s}{P_s - P_w}\right)\exp\left(\dfrac{\sigma_w^2 - \lambda}{P_s}\right), & \text{if}\, \lambda > \sigma_w^2 \\ 0, & \text{otherwise} \end{cases}\end{aligned} \tag{5.10}$$

Then the formula (5.8) can be rewritten as

$$\zeta = \begin{cases} 1 + \left(\dfrac{P_s}{P_s - P_w}\right)\left[\exp\left(\dfrac{\sigma_w^2 - \lambda}{P_w}\right) - \exp\left(\dfrac{\sigma_w^2 - \lambda}{P_s}\right)\right], & \text{if}\, \lambda \geq \sigma_w^2 \\ 1. & \text{otherwise} \end{cases} \tag{5.11}$$

To achieve covert communication, it should guarantee that $\zeta \geq 1-\varepsilon$ for any $\varepsilon > 0$, when m tends to infinity [48].

Under the case of $\lambda \leq \sigma_w^2$, $\zeta = 1$. This means that *Willie* cannot detect the transmission from S to R_b absolutely, we can consider this *Willie* is incompetent. Thus, we only consider the case of $\lambda > \sigma_w^2$. Let λ^* denotes the solution of $\frac{\partial \zeta}{\partial \lambda} = 0$, then we have the optimal threshold as

$$\lambda^{\dagger} = \left(\frac{P_s P_w}{P_s - P_w}\right) \ln\left(\frac{P_s}{P_w}\right) + \sigma_w^2, \tag{5.12}$$

thus, the minimum value of ζ can be obtained as

$$\zeta^{\dagger} = 1 - \left(\frac{P_s}{P_w}\right)^{(\frac{P_s}{P_w - P_s})}. \tag{5.13}$$

5.3.1.3 Covert Capacity

1. Transmission outage probability

To derive the covert capacity, we first determine the transmission outage probability for transmission from S to D. If the received signal strength at the receiver is smaller than its required threshold θ, which means that it fails to decode the message. In a two-hop wireless network, ensuring that the transmission of each hop is reliable can ensure the reliability of the entire transmission. Therefore, the transmission outage probability can be expressed as

$$\begin{aligned} P_{to} &= P(SIR_{S,R_b} < \theta \bigcup SIR_{R_b,D} < \theta) \\ &= 1 - \exp\left(-\frac{\theta(\sigma_{R_b}^2 + \sigma_D^2)}{P_s}\right)\left[\frac{P_s}{\theta P_w + P_s}\right]^2, \end{aligned} \tag{5.14}$$

Proof : The transmission outage probability of a two-hop wireless network is as follows

$$\begin{aligned} P_{to} &= P(SIR_{S,R_b} < \theta \bigcup SIR_{R_b,D} < \theta) \\ &= 1 - P(SIR_{S,R_b} \geq \theta \bigcap SIR_{R_b,D} \geq \theta). \end{aligned} \tag{5.15}$$

Since the first and the second hop are independent of each other, and S and R_b use the same transmit power, we can obtain

$$P_{to} = 1 - P(SIR_{S,R_b} \geq \theta)P(SIR_{R_b,D} \geq \theta). \tag{5.16}$$

Next, the probability distribution of $|h_{R_b,W}|^2$ and $|h_{D,W}|^2$ is given by

$$f_{|h_{R_b,W}|^2}(x) = f_{|h_{D,W}|^2}(x) = e^{-x}, 0 \leq x \leq \infty \tag{5.17}$$

$$\tag{5.18}$$

then,

$$\begin{aligned}
&P(SIR_{S,R_b} \geq \theta) \\
&= P(\gamma_b \geq \theta) \\
&= P[|h_{S,R_b}|^2 \geq \frac{\theta(P_w|h_{R_b,W}|^2 + \sigma_{R_b}^2)}{P_s}] \\
&= \mathbb{E}\left[\exp\left(-\frac{\theta(P_w|h_{R_b,W}|^2 + \sigma_{R_b}^2)}{P_s}\right)\right] \\
&= \exp\left(\frac{-\theta\sigma_{R_b}^2}{P_s}\right)\mathbb{E}\left[\exp\left(\frac{-\theta|h_{R_b,W}|^2 P_w}{P_s}\right)\right] \\
&= \exp\left(-\frac{\theta\sigma_{R_b}^2}{P_s}\right)\left[\frac{P_s}{\theta P_w + P_s}\right],
\end{aligned} \tag{5.19}$$

similarly,

$$P(SIR_{R_b,D} \geq \theta) = \exp\left(-\frac{\theta\sigma_D^2}{P_s}\right)\left[\frac{P_s}{\theta P_w + P_s}\right]. \tag{5.20}$$

Substituting (5.19) and (5.20) into (5.16), (5.16) can be obtained.

2. Expected covert capacity

According to the definition of the channel capacity C of a two-hop wireless network, we can get an expected value of the covert capacity C_{c1} under random relaying scheme as follows

$$\begin{aligned}
C_{c1} &= C(1 - P_{to}) \\
&= \min\{C_1, C_2\}(1 - P_{to}),
\end{aligned} \tag{5.21}$$

where C_1 and C_2 are the channel capacity of the first and second hop, respectively.

3. Covert capacity maximization

The objective of covert capacity maximization is to maximize the covert capacity C_{c1} while maintaining a high detection error probability at $Willie$. It can be formulated as the following optimization problem.

$$\text{Maximize} \quad C_{c1}. \tag{5.22a}$$

$$s.t. \quad \zeta^{\dagger}(P_s) \geq 1 - \varepsilon_c, \tag{5.22b}$$

$$\varepsilon_c \in (0, 1), \tag{5.22c}$$

where ε_c is the covertness requirement. Stochastic gradient descent algorithm is used to solve this optimization problem.

5.3.2 Performance Analysis and Optimization under Superior Relaying Scheme

In this section, we also first propose the transmission strategy of S, then derive the detection error probability of $Willie$ and covert capacity under the superior relaying scheme.

5.3.2.1 Transmission Strategy

Based one the superior relaying scheme, we assume S chooses one message relay R_b with the largest $\min\{|h_{S,R_n}|^2, |h_{R_n,D}|^2\}$.

The received signal at R_b can be formulated as

$$y_{R_b} = \sqrt{P_s} h_{S,R_b} x_s + \sqrt{P_s} h_{W,R_b} x_w + n_{R_b}, \tag{5.23}$$

and the received signal at D can be formulated as

$$y_D = \sqrt{P_{R_b}} h_{R_b,D} x_r + \sqrt{P_{R_b}} h_{W,D} x_w + n_D. \tag{5.24}$$

Accordingly, the signal-to-noise (SNR) at R_b is determined as

$$\gamma_b = \frac{P_s |h_{S,R_b}|^2}{P_w |h_{R,W}|^2 + \sigma_{R_b}^2}, \tag{5.25}$$

the signal-to-noise (SNR) at D is determined as

$$y_D = \sqrt{P_{R_b}} h_{R_b,D} x_r + \sqrt{P_w} h_{D,W} x_w + n_D, \tag{5.26}$$

where the P_s and P_{R_b} are the transmission power of S and R_b, respectively. The P_w is the jamming power of $Willie$. The $n_{R_b} \sim \mathcal{CN}(0, \sigma_{R_b}^2)$ represents the received noise at R_b.

5.3.2.2 Detection Error Probability

Similar to the random relaying scheme, we give the hypothesis test and the detection error probability of $Willie$. In the transmission scenario we consider in this chapter, there is no interference from other nodes, so the detection error probability of $Willie$ is the same as that under the random relaying scheme. According to the previous analysis, the detection error probability of $Willie$ can be determined under the superior relaying scheme as following

$$\zeta = \begin{cases} 1 + \left(\dfrac{P_s}{P_s - P_w}\right)\left[\exp\left(\dfrac{\sigma_w^2 - \lambda}{P_w}\right) - \exp\left(\dfrac{\sigma_w^2 - \lambda}{P_s}\right)\right], & \text{if}\, \lambda \geq \sigma_w^2 \\ 1. & \text{otherwise} \end{cases} \tag{5.27}$$

Hence, we also obtain the minimum value of ζ can be obtained the same as (5.13).

5.3.2.3 Covert Capacity

1. Transmission outage probability

To enhance the covert capacity performance, we propose a superior relaying scheme to select the message relay. Based on this relay selection scheme, the message relay with the largest $\min\{|h_{S,R_k}|^2, |h_{R_k,D}|^2\}$. However, the channel gains between *Willie* and R_b, *Willie* and D are unknown. Although we have selected the best link, the transmission outage may still occur. Then, the transmission outage probability of the superior relaying scheme is determined as

$$P_{sto} = \sum_{0}^{n} \binom{n}{k} (-1)^k \frac{1}{2k-1}$$
$$\left[k\left(\frac{P_s}{\theta P_w + P_s}\right)\exp\left(\frac{-\theta\sigma_b^2}{P_s}\right) + (k-1)\left(\frac{P_s}{2k\theta P_w + P_s}\right)\exp\left(\frac{-2k\theta\sigma_b^2}{P_s}\right)\right] \tag{5.28}$$

Proof : For each relay R_k where $k = 1, 2, ..., n$, let $M_k = \min\{|h_{S,R_k}|^2, |h_{R_k,D}|^2\}$, and D_k denote the event that S select the relay. We then have

$$D_k \triangleq \bigcap_{l=1, l\neq k}^{n} (M_l \leq M_k), \tag{5.29}$$

where M_k is an exponential random variable with mean 1/2.

If $M_k = |h_{S,R_k}|^2$, then based on the law of total probability, we have

$$\begin{aligned}
P(|h_{S,R_b}|^2 < x) &= \sum_{k=1}^{n} P(|h_{S,R_k}|^2 < D_k) \\
&= \sum_{k=1}^{n} P\{|h_{S,R_k}|^2 < x, \bigcap_{l=1,l\neq k}^{n} (M_l \leq M_k)\} \\
&= \sum_{k=1}^{n} \int_0^\infty P\{|h_{S,R_k}|^2 < x, \bigcap_{l=1,l\neq k}^{n} (M_l \leq t), M_k = t\} dt \\
&= \int_0^\infty nP(|h_{S,R_k}|^2 < x, M_k = t)(1 - e^{-2t})^{n-1} dt,
\end{aligned} \tag{5.30}$$

where

$$P(|h_{S,R_k}|^2 < x, M_k = t) = \begin{cases} e^{-t}(2e^{-t} - e^{-x}), & \text{if}\, 0 \leq t \leq x \\ 0. & \text{otherwise,} \end{cases} \tag{5.31}$$

Then, we further obtain

$$\begin{aligned} & P(|h_{S,R_b}|^2 < x) \\ & = \int_0^x ne^{-t}(2e^{-t} - e^{-x})(1 - e^{-2t})^{n-1} dt \\ & = (1 - e^{-2x})^n - ne^{-x} \int_0^x e^{-t}(1 - e^{-2t})^{n-1} dt \\ & = \sum_0^n \binom{n}{k} (-1)^k \frac{ke^{-x} + (k-1)e^{-2kx}}{2k-1}. \end{aligned} \tag{5.32}$$

The transmission outage probability can be expressed as

$$\begin{aligned} & P_{sto} = P(SIR_{S,R_b} < \theta) \\ & = \sum_0^n \binom{n}{k} (-1)^k \frac{1}{2k-1} [k\text{exp}(-\frac{\theta(P_w|h_{R_b,W}|^2 + \sigma_{R_b}^2)}{P_s}) \\ & + (k-1)\text{exp}(-2k\frac{\theta(P_w|h_{R_b,W}|^2 + \sigma_{R_b}^2)}{P_s})] \\ & = \sum_0^n \binom{n}{k} (-1)^k \frac{1}{2k-1} k\text{exp}\left(\frac{-\theta\sigma_b^2}{P_s}\right) \mathbb{E}\left[\text{exp}\left(-\frac{\theta(P_w|h_{R_b,W}|^2)}{P_s}\right)\right] \\ & + \sum_0^n \binom{n}{k} (-1)^k \frac{1}{2k-1} (k-1)\text{exp}\left(\frac{-2k\theta\sigma_b^2}{P_s}\right) \mathbb{E}\left[\text{exp}\left(-\frac{2k\theta(P_w|h_{R_b,W}|^2)}{P_s}\right)\right] \\ & = \sum_0^n \binom{n}{k} (-1)^k \frac{1}{2k-1} k\text{exp}\left(\frac{-\theta\sigma_b^2}{P_s}\right) \int_0^\infty \text{exp}\left(-\frac{\theta(P_w|h_{R_b,W}|^2)}{P_s}\right) f_{|h_{R_b,R_W}|^2}(x) dx \\ & + \sum_0^n \binom{n}{k} (-1)^k \frac{1}{2k-1} (k-1)\text{exp}\left(\frac{-2k\theta\sigma_b^2}{P_s}\right) \int_0^\infty \text{exp}\left(-\frac{2k\theta(P_w|h_{R_b,W}|^2)}{P_s}\right) f_{|h_{R_b,R_W}|^2}(x) dx \end{aligned} \tag{5.33}$$

(5.28) can be obtained.

2. Expected covert capacity

Similarly, we can get an expected value of the covert capacity C_{c2} under the superior relaying scheme as

$$\begin{aligned} C_{c2} &= C(1 - P_{sto}) \\ &= \min\{C_1, C_2\}(1 - P_{sto}), \end{aligned} \tag{5.34}$$

where C_1 and C_2 are the channel capacity of the first and second hop, respectively.

3. Covert capacity maximization

The objective of covert capacity maximization is to maximize the covert capacity C_{c2} while maintaining a high detection error probability of $Willie$. It can be formulated as the following optimization problem.

$$\text{Maximize} \quad C_{c2}. \tag{5.35a}$$

$$s.t. \quad \zeta^{\dagger}(P_{s2}) \geq 1 - \varepsilon_c, \tag{5.35b}$$

$$P_{sto} < \varepsilon_{sto}, \tag{5.35c}$$

$$\varepsilon_c \in (0, 1), \tag{5.35d}$$

$$\varepsilon_{sto} \in (0, 1), \tag{5.35e}$$

where ε_c is the covertness requirement and ε_{sto} is the TOP constraint. (5.35c) is the outage requirement under the superior relaying scheme. Unitizing numerical search, we can easily solve the one dimensional optimization problem in (5.35). By substituting $P_s^{\dagger}$ into (5.34), we then obtain the maximum capacity denoted as C^*.

5.4 Numerical Results and Discussions

In this section, we first validate our theoretical analysis for the transmission outage probability under superior relaying scheme as well as the detection error probability of Willie under two relay selection schemes through extensive simulations, and then explore how the system parameters affect the ζ and covert capacity.

5.4.1 Validation

For the transmission outage probability under the superior relaying scheme, the total number of transmissions is fixed as 100000 with the corresponding random CSI and the transmission outage probability is measured as the ratio of the number of transmissions suffering from transmission outage to the total number of transmissions. We conduct extensive simulations with the setting of number of relays $n = \{10, 30\}$, jamming power $P_w = 1$ W, threshold $\theta = 1$ and received noise $\sigma^2_{R_b} = \sigma^2_D = -5$ dB. We can see from Fig.(5.2) that for each P_s, the theoretical transmission outage probability P_{sto} almost matches with the simulation one. It is easily observed that as the P_s increases, the P_{sto} decreases. As we know, P_{sto} represents the probability of outage from S to message relay R_b. Hence, S can enhance its transmit power to reduce the negative impact of P_{sto}. However, this will also increase the risk of being detected.

Fig.(5.2) also shows that as the number of relays n increases, the P_{sto} decreases with the same P_s. This is because the channel gain of the selected message relay is more likely to meet the no outage condition as the number of relays increases. Therefore, in a large-scale system with more multiple relays, the performance of covert communication is better.

For the detection error probability (both two relay selection schemes), the CSI is generated randomly and the range of detection threshold λ varies from 0 to 5. Then

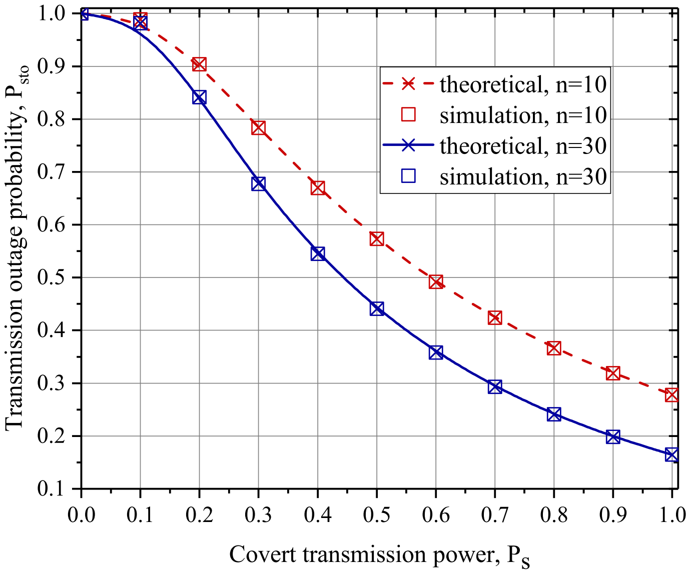


Figure 5.2: Transmission outage probability validation.

$Willie$ performs 100000 detections for each λ with the corresponding CSI. Then we get the average value of detection error probability. We compare the theoretical results with the simulation ones under the two relay selection schemes with the setting of jamming power $P_w = 1$ W, covert transmit power $P_s = 0.3$ W, and received noise $\sigma_w^2 = -5$ dB at $Willie$. We can observe from Fig.(5.3) that the theoretical ζ almost matches with the simulation one. This demonstrates that our theoretical results can well capture the performance of covert communication.

5.4.2 Covert Performance Analysis

We first explore the impact of detection threshold λ on the detection error probability ζ with different P_s and summarize in Fig.(5.4). How ζ varies with λ is shown as Fig.(5.4) with the setting of $P_w = 1$ W, $\theta = 1$ and $\sigma_w^2 = -5$ dB. We can observe from Fig.(5.4) that for each setting of P_s and α, as λ increases, ζ first decreases and then increases. This can be explained as follows. We know that ζ is the sum of false alarm probability $\mathbb{P}_{FA}$ and missed detection probability $\mathbb{P}_{MD}$. It can be determined from our theoretical analysis that $\mathbb{P}_{FA}$ is a decreasing function of λ while $\mathbb{P}_{MD}$ is an

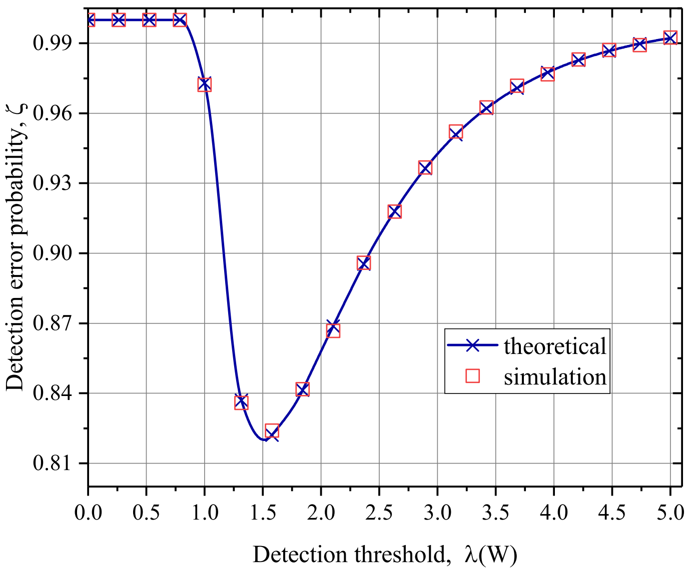


Figure 5.3: Detection error probability validation.

increasing function. As λ is relatively small, the former one dominates ζ, leading to the decrease of ζ with λ. On the other hand, as λ further increases, the latter one dominates ζ, leading to the increase of ζ. There exists a minimum ζ which means $Willie$ has the strongest detection ability to detect the transmission of two hops, then we can find a corresponding maximum transmission power limit of S and R_b. It is obvious that for each fixed λ, the minimum value of ζ increases with the decrease of P_s. This is because the increase of the covert transmit power will enhance the probability of being detected.

To investigate the impact of covert transmit power P_s on the covert capacity C_c, we summarize in Fig.(5.5) how C_c varies with the increasing of P_s under these two relay selection schemes with the setting of $P_w = \{0.5, 1.0, 1.5\}$ W, $|h_{S,R_b}|^2 = |h_{R_b,D}|^2 = 1$, $n = 30$ and $\sigma_{R_b}^2 = \sigma_D^2 = -5$ dB. In the figures of showing that covert capacity and max covert capacity, the **dashed lines** and **solid lines** are used to show the results under the random relaying scheme and the superior relaying scheme, respectively. A careful observation of Fig.(5.5) indicates that for each fixed P_w, as P_s further increases, the C_c will increases. This is due to the enhanced transmit power increases the SINR.

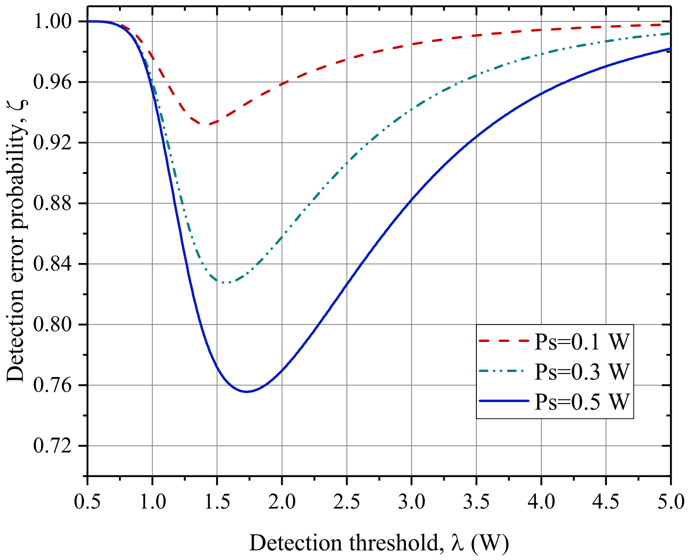


Figure 5.4: The impact of detection threshold on detection error probability.

Fig.(5.5) also shows that for each fixed P_s, as P_w further increases, the C_c will decreases. This is due to the enhanced interference signal reduces the decoding rate and the covert capacity. This is because the enhancement of the jamming signal leads to a decrease in the decoding rate, which results in a decrease in the covert capacity.

By comparing the result of the two schemes, we can easily observe that the covert capacity of the superior relaying scheme is better than the random relaying scheme. The reason for this phenomenon is that even though there are transmission outages under both two relay selection schemes, the link status of the latter one is better. When S uses small covert transmit power, the link state determines the covert capacity.

5.4.3 Performance Optimization

We explore the impact of covertness requirement ε_c on the maximum covert capacity C^* under the two relay selection schemes.

Fig.(5.6) illustrates that the impact of covertness requirement ε_c on the maximum covert capacity C^* under the two relay selection schemes with the setting of $P_w =$

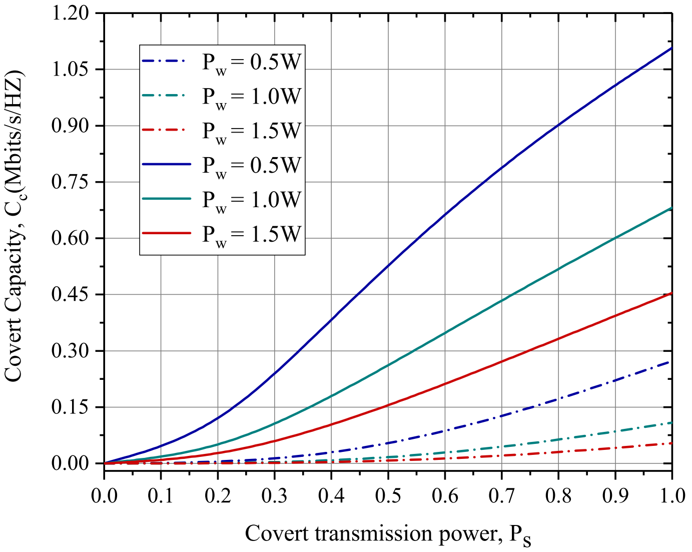


Figure 5.5: The impact of covert transmission power on covert capacity.

$\{1.0, 1.5, 2.0\}$ W, $|h_{S,R_b}|^2 = |h_{R_b,D}|^2 = 1$, $n = 30$, $\sigma_w^2 = 0$ dB, and $\sigma_{R_b}^2 = \sigma_D^2 = -5$ dB.

We can observe from Fig.(5.6) that as ε_c increases, the C^* increases under the two relay selection schemes. This is because the increasing of ε_c leads to the increasing of the optimal transmission power P_s^*, which corresponds to an increase in the probability of transmission being detected. A careful observation of Fig.(5.6) indicates that for each fixed ε_c, as the jamming power P_w increases, the maximum covert capacity C^* increases, and the C^* under the random relaying scheme is less than that under the superior relaying scheme with same conditions. The reason of this phenomenon as follows. When $Willie$ transmits jamming signals, it will also be affected by self-interference, which leads to a decrease in its detection ability and an increase in detection error probability. Hence, P_s^* will increase as P_w increases due to the P_w is part of the background noise for $Willie$. Notice that the probability of transmission outage under superior relaying scheme is more lower than the former scheme so it can achieve the maximum covert capacity.

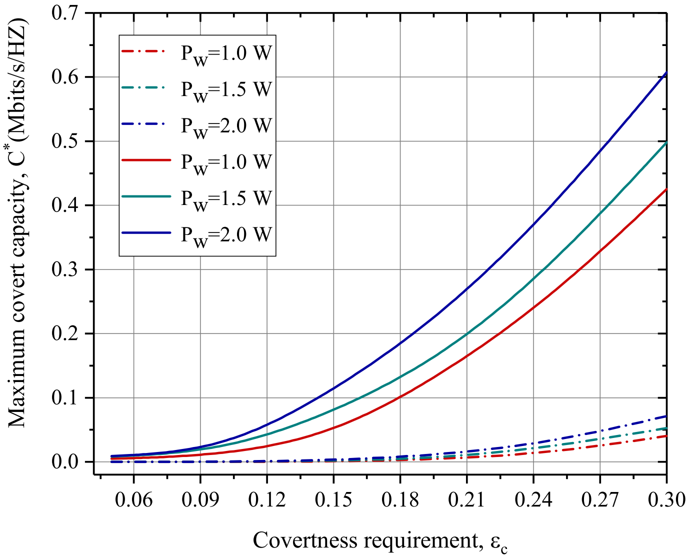


Figure 5.6: The impact of covertness requirement on maximum covert capacity.

5.5 Discussion

In this chapter, we study the performance of covert communication in a scenario where the warden will actively attack the communication process as a jammer in a relay-assisted wireless system. We then introduce the transmission strategy and redefine the behavior of the warden that it will perform detection and jamming throughout the covert communication process. Notice that the transmitter has to increase the transmission power to ensure successful decoding due to the jamming of the warden, and thus increases the risk of being detected. It is worth noting that the CSI between the warden and the receiver is unknown, the transmitter chooses the relay that can maximize the covert capacity but the problem of transmission outage cannot be guaranteed.

Through theoretical analysis, we found that while warden actively attacks covert communications, it also interferes with itself, leading to an increase in the detection error probability. Therefore, the warden must control the jamming power according to its background noise to avoid frequent errors. In practical applications, the warden may not only perform detection missions but also send jamming signals or even as an eavesdropper. The work of this chapter proposes a new research direction for future study of covert communication.

5.6 Summary

In this chapter, we investigated the performance of cover communications in relay-assisted wireless systems with an active warden. To this end, we redefine the propose of the warden that it will perform detection and jamming throughout the covert communication process. Notice that the transmitter has to increase the transmission power to ensure successful decoding due to the jamming of warden, and thus increases the risk of being detected. To deeply understand such interactions, based on the related relay selection protocol designed previously, we develop a new theoretical framework to analyze the transmission outage probability, the detection error probability of warden, and covert capacity. Then, we optimize the covert capacity through power control under given covertness and outage requirements. Finally, extensive simulation and numerical results are provided to illustrate our theoretical findings and the performance of covert communication with an active warden in such systems.

Numerical results indicate that the covert capacity increases with the increasing of covert transmit power under the two selection schemes, while the better maximum covert capacity is achieved under the superior relaying scheme. Remarkably, the warden is also affected by self-interference when it transmits jamming signals, which prevents the warden from using higher jamming power. Therefore, covert communication can still be achieved by a flexible power control.

CHAPTER VI

Conclusion

In this thesis, we studied the design of relay/jammer selection protocol the analysis of covert performance for covert communications in relay-assisted wireless systems. We first explore the relay selection protocol design for covert communication in a two-hop wireless communication system with multiple relays and a passive warden. Based on this system, we conduct a theoretical analysis to derive the corresponding achievable covert capacity. We then introduce cooperative jamming technology into this system to interfere with the warden and design related relay/jammer selection protocol. Next, we provide a theoretical analysis to demonstrate the impact of cooperative jamming on covert capacity. We further extend our study to a scenario where the warden will actively attack the communication process as a jammer in a relay-assisted wireless system.

For the covert communication in two-hop wireless systems with multiple relays, we studied in Chapter III where a message is first transmitted from the source to a message relay and then forwarded by the relay to the destination under the detection of a passive warden. We explore in detail the relay selection protocol design issue for this system. For evaluating the performance of covert communication, we develop a theoretical framework to analyze the transmission outage probability, the detection error probability of warden, and covert capacity based on the relay selection protocol.

We also explore covert capacity maximization through efficient numerical searches under a given covertness requirement. The main results in Chapter III show that the superior relaying scheme can achieve a much better covert performance with lower resource consumption.

For cooperative jamming based covert communication in relay-assisted wireless systems, we investigated in Chapter IV where the cooperative jamming technique is adopted to prove covert performance. In order to determine the message relay and the jammer, we illustrate a new relay/jammer selection protocol in this system. In order to explore the impact of cooperative jamming on the performance of covert communication, we introduce a jam-generating threshold into the theoretical framework and we further derive the expressions for three performance metrics, i.e., transmission outage probability, the detection error probability of warden, and covert capacity. We also explore covert capacity maximization through efficient numerical searches under given covertness and outage requirements. The main results in Chapter IV show that although the increase of jam-generating threshold can increase the probability of detection error of warden, the maximum covert capacity is reduced due to excessive jamming power. Therefore, in practical applications, users should choose appropriate jam-generating threshold according to their covertness and outage requirements.

In Chapter V, we further extend our study to a scenario where the warden will actively attack the communication process as a jammer in a relay-assisted wireless system. We redefine the purpose of the warden that it will perform detection and jamming throughout the covert communication process. Notice that the transmitter has to increase the transmission power to ensure successful decoding due to the jamming of warden, and thus increases the risk of being detected. To deeply understand such interactions, based on the related relay selection protocol designed previously, we develop a new theoretical framework to analyze the transmission outage probability, the detection error probability of warden, and covert capacity. The main results in Chapter V show that the maximum covert capacity decreases due to the jamming signals of the warden. However, when the warden transmits jamming signals, it is also affected by self-interference, resulting in a decrease in detection capability. Remarkably, both the detection error probability and covert capacity performance under the superior relaying scheme are better than those under the random relaying scheme as covert transmit power increases.

It is notable that, the scenarios and transmission modes considered in this thesis are relatively limited. However, in practical applications, there are many factors that affect covert communication. Therefore, one of the interesting and important future works is to study covert performance in more complex transmission models, such as buffered relays and more variable channels.

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A survey on wireless security: Technical challenges, recent advances, and future trends,” *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[2] “Digital trends in asia pacific 2021,” [EB/OL], https://www.itu.int/en/myitu/Publications/2021/03/08/09/13/Digital-Trends-in-Asia-Pacific-2021/ Accessed March, 2021.

[3] A. Yang, C. Zhang, Y. Chen, Y. Zhuansun, and H. Liu, “Security and privacy of smart home systems based on the internet of things and stereo matching algorithms,” *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2521–2530, 2020.

[4] S. T. Shiwei Lai, Rui Zhao, J. Xia, F. Zhou, and L. Fan, “Intelligent secure mobile edge computing for beyond 5g wireless networks,” *Physical Communication*, vol. 45, pp. 1874–4907, 2021.

[5] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, “A survey on the internet of things (iot) forensics: Challenges, approaches, and open issues,” *IEEE Communications Surveys Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020.

[6] “Covid 19 pandemic leaves consumers vulnerable to cybercrime,” [EB/OL], https://investor.nortonlifelock.com/About/Investors/press-releases/press-release-details/2021/COVID-19-Pandemic-Leaves-Consumers-Vulnerable-to-Cybercrime/default.aspx.

[7] F. Foukalas, V. Gazis, and N. Alonistioti, “Cross-layer design proposals for wireless mobile networks: A survey and taxonomy,” *IEEE Communications Surveys Tutorials*, vol. 10, no. 1, pp. 70–85, 2008.

[8] C. V. Saradhi and S. Subramaniam, “Physical layer impairment aware routing (pliar) in wdm optical networks: issues and challenges,” *IEEE Communications Surveys Tutorials*, vol. 11, no. 4, pp. 109 –130, 2009.

[9] C. Kolias, G. Kambourakis, and S. Gritzalis, “Attacks and countermeasures on 802.16: Analysis and assessment,” *IEEE Communications Surveys Tutorials*, vol. 15, no. 1, pp. 487–514, 2013.

[10] "Experience of wang xiaoyun," [EB/OL], hhttps://en.wikipedia.org/wiki/Wang_Xiaoyun.

[11] X. Zhou, Y. Xiong, F. Miao, and M. Li, "A new dynamic user authentication scheme using smart cards for wireless sensor network," in *2011 IEEE 2nd International Conference on Computing, Control and Industrial Engineering*, vol. 2, 2011, pp. 1–4.

[12] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *2006 IEEE International Symposium on Information Theory*, 2006, pp. 356–360.

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

[14] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

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

[16] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[17] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[18] Y. Zou, X. Wang, and W. Shen, "Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack," in *2013 IEEE International Conference on Communications (ICC)*, 2013, pp. 2183–2187.

[19] ——, "Eavesdropping attack in collaborative wireless networks: Security protocols and intercept behavior," in *Proceedings of the 2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, 2013, pp. 704–709.

[20] P. Parada and R. Blahut, "Secrecy capacity of simo and slow fading channels," in *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.*, 2005, pp. 2152–2155.

[21] L. Lai and H. El Gamal, "The relayceavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.

[22] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 6, pp. 1154–1170, 2015.

[23] A. A. Nasir, H. D. Tuan, T. Q. Duong, and H. V. Poor, “Secrecy rate beamforming for multicell networks with information and energy harvesting,” *IEEE Transactions on Signal Processing*, vol. 65, no. 3, pp. 677–689, 2017.

[24] Z. Sheng, H. D. Tuan, T. Q. Duong, and H. V. Poor, “Beamforming optimization for physical layer security in miso wireless networks,” *IEEE Transactions on Signal Processing*, vol. 66, no. 14, pp. 3710–3723, 2018.

[25] H. Qin, X. Chen, Y. Sun, M. Zhao, and J. Wang, “Optimal power allocation for joint beamforming and artificial noise design in secure wireless communications,” in *2011 IEEE International Conference on Communications Workshops (ICC)*, 2011, pp. 1–5.

[26] E. Tekin and A. Yener, “Achievable rates for the general gaussian multiple access wire-tap channel with collective secrecy,” *CoRR*, vol. abs/cs/0612084, 2006.

[27] ——, “The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming,” *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[28] J. Xie and S. Ulukus, “Secure degrees of freedom of the gaussian wiretap channel with helpers and no eavesdropper csi: Blind cooperative jamming,” in *2013 47th Annual Conference on Information Sciences and Systems (CISS)*, 2013, pp. 1–5.

[29] ——, “Secure degrees of freedom of one-hop wireless networks,” *CoRR*, vol. 60, no. 6, pp. 3359–3378, 2012.

[30] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, “Applications of ldpc codes to the wiretap channel,” *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933–2945, 2007.

[31] H. Mahdavifar and A. Vardy, “Achieving the secrecy capacity of wiretap channels using polar codes,” *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6428–6443, 2011.

[32] O. O. Koyluoglu, A. S. Rawat, and S. Vishwanath, “Secure cooperative regenerating codes for distributed storage systems,” *IEEE Transactions on Information Theory*, vol. 60, no. 9, pp. 5228–5244, 2014.

[33] A. Bletsas, A. Khisti, D. Reed, and A. Lippman, “A simple cooperative diversity method based on network path selection,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 3, pp. 659–672, 2006.

[34] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, “Relay-selection improves the security-reliability trade-off in cognitive radio systems,” *IEEE Transactions on Communications*, vol. 63, no. 1, pp. 215–228, 2015.

[35] F. S. Al-Qahtani, C. Zhong, and H. M. Alnuweiri, “Opportunistic relay selection for secrecy enhancement in cooperative networks,” *IEEE Transactions on Communications*, vol. 63, no. 5, pp. 1756–1770, 2015.

[36] D. Wang, P. Ren, and J. Cheng, “Cooperative secure communication in two-hop buffer-aided networks,” *IEEE Transactions on Communications*, vol. 66, no. 3, pp. 972–985, 2018.

[37] C. Wei, W. Yang, Y. Cai, X. Tang, and G. Kang, “Secrecy outage performance for df buffer-aided relaying networks with a multi-antenna destination,” *IEEE Access*, vol. 7, pp. 41 349–41 364, 2019.

[38] X. Liao, Y. Zhang, Z. Wu, Y. Shen, X. Jiang, and H. Inamura, “On security-delay trade-off in two-hop wireless networks with buffer-aided relay selection,” *IEEE Transactions on Wireless Communications*, vol. 17, no. 3, pp. 1893–1906, 2018.

[39] X. Liao, Y. Zhang, Z. Wu, and X. Jiang, “Buffer-aided relay selection for secure two-hop wireless networks with decode-and-forward relays and a diversity-combining eavesdropper,” *Ad Hoc Networks*, vol. 98, p. 102039, 2020.

[40] J. He, J. Liu, Y. Xu, and X. Jiang, “Buffer-aided relaying for two-hop secure communication with limited packet lifetime,” in *2019 IEEE 20th International Conference on High Performance Switching and Routing (HPSR)*, 2019, pp. 1–7.

[41] J. He, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, “Link selection for security-qos tradeoffs in buffer-aided relaying networks,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1347–1362, 2020.

[42] S. Yan, Y. Cong, S. V. Hanly, and X. Zhou, “Gaussian signalling for covert communications,” *IEEE Transactions on Wireless Communications*, vol. 18, no. 7, pp. 3542–3553, 2019.

[43] Y. Zheng, S. Yang, H. Fu, and T. Chen, “Secure outage probability analysis of relay networks based on cooperative jamming,” in *2018 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 2018, pp. 55–553.

[44] B. Han, J. Li, J. Su, M. Guo, and B. Zhao, “Secrecy capacity optimization via cooperative relaying and jamming for wanets,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 1117–1128, 2015.

[45] R. Nakai and S. Sugiura, “Physical layer security in buffer-state-based max-ratio relay selection exploiting broadcasting with cooperative beamforming and jamming,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 431–444, 2019.

[46] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, "On secure wireless communications for iot under eavesdropper collusion," *IEEE Transactions on Automation Science and Engineering*, vol. 13, no. 3, pp. 1281–1293, 2016.

[47] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE journal on selected areas in communications*, vol. 31, no. 9, pp. 1921–1930, 2013.

[48] ——, "Square root law for communication with low probability of detection on AWGN channels," in *Proc. IEEE International Symposium on Information Theory Proceedings*, July, 2012, pp. 448–452.

[49] B. A. Bash, D. Goeckel, and D. Towsley, "LPD communication when the warden does not know when," in *Proc. IEEE International Symposium on Information Theory*, June, 2014, pp. 606–610.

[50] P. H. Che, M. Bakshi, and S. Jaggi, "Reliable deniable communication: Hiding messages in noise," in *Proc. IEEE International Symposium on Information Theory*, July, 2013, pp. 2945–2949.

[51] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Transactions on Information Theory*, vol. 62, no. 6, pp. 3493–3503, 2016.

[52] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Transactions on Information Theory*, vol. 62, no. 5, pp. 2334–2354, 2016.

[53] K. S. K. Arumugam and M. R. Bloch, "Keyless covert communication over multiple-access channels," in *2016 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2016, pp. 2229–2233.

[54] S. Lee, L. Wang, A. Khisti, and G. W. Wornell, "Covert communication with channel-state information at the transmitter," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2310–2319, 2018.

[55] K. S. Kumar Arumugam and M. R. Bloch, "Embedding covert information in broadcast communications," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 10, pp. 2787–2801, 2019.

[56] K. Shahzad, X. Zhou, and S. Yan, "Covert communication in fading channels under channel uncertainty," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*. IEEE, 2017, pp. 1–5.

[57] D. Goeckel, B. Bash, S. Guha, and D. Towsley, "Covert communications when the warden does not know the background noise power," *IEEE Communications Letters*, vol. 20, no. 2, pp. 236–239, 2016.

[58] J. Hu, S. Yan, X. Zhou, S. Feng, and J. Li, "Covert wireless communications with channel inversion power control in rayleigh fading," *IEEE Transactions on Vehicular Technology*, vol. PP, no. 99, 2019.

[59] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Transactions on Wireless Communications*, vol. 17, no. 12, pp. 8517–8530, 2018.

[60] B. He, S. Yan, X. Zhou, and H. Jafarkhani, "Covert wireless communication with a poisson field of interferers," *IEEE Transactions on Wireless Communications*, vol. 17, no. 9, pp. 6005–6017, 2018.

[61] T. Zheng, H. Wang, D. W. K. Ng, and J. Yuan, "Multi-antenna covert communications in random wireless networks," *IEEE Transactions on Wireless Communications*, vol. 18, no. 3, pp. 1974–1987, 2019.

[62] K. Shahzad, X. Zhou, and S. Yan, "Covert wireless communication in presence of a multi-antenna adversary and delay constraints," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 12, pp. 12 432–12 436, 2019.

[63] K. Huang, H. Wang, D. Towsley, and H. V. Poor, "Lpd communication: A sequential change-point detection perspective," *IEEE Transactions on Communications*, vol. 68, no. 4, pp. 2474–2490, 2020.

[64] Y. Jiang, L. Wang, and H. Chen, "Covert communications in D2D underlaying cellular networks with antenna array assisted artificial noise transmission," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 3, pp. 2980–2992, 2020.

[65] H. Q. Ta and S. W. Kim, "Covert communication under channel uncertainty and noise uncertainty," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 2019, pp. 1–6.

[66] B. He, S. Yan, X. Zhou, and V. K. N. Lau, "On covert communication with noise uncertainty," *IEEE Communications Letters*, vol. 21, no. 4, pp. 941–944, 2017.

[67] Z. Liu, J. Liu, Y. Zeng, and J. Ma, "Covert wireless communication in IoT network: From AWGN channel to THz band," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3378–3388, 2020.

[68] H. Wu, X. Liao, Y. Dang, Y. Shen, and X. Jiang, "Limits of covert communication on two-hop AWGN channels," in *2017 International Conference on Networking and Network Applications (NaNA)*. IEEE, 2017, pp. 42–47.

[69] H. Wu, Y. Zhang, X. Liao, Y. Shen, and X. Jiang, "On covert throughput performance of two-way relay covert wireless communications," *Wireless Networks*, pp. 1–15, 2020.

[70] J. Wang, W. Tang, Q. Zhu, X. Li, H. Rao, and S. Li, “Covert communication with the help of relay and channel uncertainty,” *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 317–320, 2018.

[71] J. Hu, S. Yan, X. Zhou, F. Shu, J. Li, and J. Wang, “Covert communication achieved by a greedy relay in wireless networks,” *IEEE Transactions on Wireless Communications*, vol. 17, no. 7, pp. 4766–4779, 2018.

[72] J. Hu, S. Yan, F. Shu, and J. Wang, “Covert transmission with a self-sustained relay,” *IEEE Transactions on Wireless Communications*, vol. 18, no. 8, pp. 4089–4102, 2019.

[73] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yeoh, “Covert communication and secure transmission over untrusted relaying networks in the presence of multiple wardens,” *IEEE Transactions on Communications*, vol. 68, no. 6, pp. 3737–3749, 2020.

[74] H. Wang, Y. Zhang, X. Zhang, and Z. Li, “Secrecy and covert communications against UAV surveillance via multi-hop networks,” *IEEE Transactions on Communications*, vol. 68, no. 1, pp. 389–401, 2020.

Publications

Jounal Articles

[1] Chan Gao, Bin Yang, Xiaohong Jiang, Hiroshi Inamura and Masaru Fukushi. Covert Communication in Relay-Assisted IoT Systems. *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6313-6323, April, 2021.

Conference Papers

[2] Chan Gao, Bin Yang, Xiaohong Jiang, Hiroshi Inamura and Masaru Fukushi. Covert Communication in Relaying Sensor Systems. 1st International Workshop on Physical-Layer Augmented Security for Sensor Systems (PLAS), pp. 3-8, 2020.