Secure Communication Protocol Design for Buffer-Aided Relaying Systems

by

Ji He

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(The School of Systems Information Science)
in Future University Hakodate
September, 2020

To my family

ABSTRACT

Secure Communication Protocol Design for Buffer-Aided Relaying Systems

by

Ji He

With the rapid evolution of information and communication technologies, more complicated network architectures and more advanced network topologies and access techniques are exploited to support the unprecedented growth of data traffic in the 5G communication. This fact, therefore, leads to an enormous amount of sensitive and confidential information transmitted via the wireless channels, e.g., financial data, medical records, and customer files. How to guarantee information security has attracted increasing concerns from both academia and industry recently. Physical layer (PHY) security has been proposed as one promising technology to provide security guarantee for wireless communications, owing to its unique advantages over traditional cryptography-based mechanisms, like an everlasting security guarantee and no need for costly secret key distribution/management and complex encryption algorithms. This thesis, therefore, focuses on the design of communication protocols with PHY security techniques to secure a buffer-aided relaying system, where relay buffers are adopted to help the transmission of information.

We first investigate the secure communication in a two-hop cooperative wireless network, where a buffer-aided relay helps forward data from the source to destina-

tion, and a passive eavesdropper attempts to intercept data transmission from both the source and relay. To ensure the transmission security and communication quality of service (QoS) of the system, we design the novel communication protocols for two cases that the instantaneous channel state information is available or unavailable at the source node. For the evaluation of system performance, we then derive the closed-form expressions of end-to-end secrecy outage probability, system throughput and secrecy throughput, respectively. Based on the theoretical performance analysis, we further explore the performance optimization issues, revealing the insightful tradeoffs between transmission security and QoS. An iterative algorithm is developed to identify the optimal setting of link selection parameters, which is helpful for the practical configuration of link selection policies to satisfy various system performance requirements. Finally, we conduct simulations to validate our theoretical performance analysis, and also provide extensive numerical results to illustrate the efficiency of the proposed communication protocols for ensuring secure communication in the buffer-aided relaying system.

We then investigate the secure communication in a wireless relaying system where the packet lifetime is limited, multiple buffer-aided relays help the source forward packets to the destination, and a passive eavesdropper attempts to wiretap the transmissions over both hops. To guarantee the end-to-end transmission security and timeliness in the system, we design a novel security/delay-aware communication protocol that grants transmission nodes different priorities for packet delivery based on the wireless channel state, real-time buffer state, and packet delay requirement. To evaluate the performance of the proposed protocol, we then develop a Markov chain-based theoretical framework to fully characterize the packet occupancy process in the relay buffers. With the help of this framework, we further derive under two typical fading channel cases the closed-form expressions for three fundamental system performance metrics, namely the reliable outage probability, packet discarding prob-

ability and achievable secrecy throughput. Finally, we present extensive simulation and numerical results to validate our theoretical results, as well as to demonstrate the efficiency of the proposed protocol for ensuring secure and timely communication in the buffer-aided relaying system. The results indicate that the proposed communication protocol can be flexibly controlled according to different lifetime constraints to satisfy different performance requirements of the system.

ACKNOWLEDGEMENTS

I would like to express my sincere appreciation to all those who have helped and supported me in one way or the other during this amazing journey. Without any of them, this research would not have been possible.

First and foremost, my heartfelt appreciation goes to my advisor Prof. Xiaohong Jiang, for his valuable guidance and technical inputs throughout my course of study at Future University Hakodate. His outstanding professional advice helps me a lot in improving my skills of research, technical writing and presentation.

Special thanks also go to Prof. Yulong Shen of Xidian University, who gives me great support on both academic research and pursuit of career. I would like to express my gratitude to Dr. Jia Liu and Dr. Yuanyu Zhang for numerous technical discussions and suggestions that have found their way into this dissertation.

I would also like to acknowledge my Ph.D. examining committee members, including Prof. Yuichi Fujino, Prof. Hiroshi Inamura, and Prof. Masaaki Wada, for their insightful comments and suggestions which help me greatly improve the quality of my research. In addition, I would like to give my sincere thanks to the staff of Future University Hakodate, Mr. Igi, Mr. Yoshida, Ms. Kawagishi, Ms. Arashida, etc., for their continuous assistance through my study at FUN.

TABLE OF CONTENTS

CHAPTER

LIST OF FIGURES

Figure

LIST OF TABLES

Table

LIST OF APPENDICES

Appendix

CHAPTER I

Introduction

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

1.1 Physical Layer Security

With the rapid evolution of information and communication technologies, heterogeneous network architectures and access techniques are exploited to support the unprecedented growth in data traffic in 5G communications [1]. This fact leads to an enormous amount of sensitive and confidential information transmitted via wireless channels [2]. However, due to the broadcast nature of the wireless mediums, communications over wireless networks are susceptible to eavesdropping attacks from unauthorized users (i.e., eavesdroppers). Therefore, how to guarantee wireless communication security has been attracting increasing attention from both academia and industry recently.

Traditionally, data is secured by applying the key-based enciphering (cryptographic) techniques in the upper layers of the network protocol stack [3]. Although these cryptographic methods have shown their effectiveness in wired networks, the inherent difficulty of secret key distribution/management without centralized control and the involved complex encryption algorithms may significantly limit their applications in decentralized wireless networks [4]. More importantly, all cryptographic measures are based on the premise that it is computationally infeasible for them to be deciphered without the secret key, which is still unproven in mathematics. However, ciphers that were considered virtually unbreakable in the past are continually surmounted due to the potential transformative progress in computing, e.g., quantum computing [5]. These motivate the introduction of physical layer (PHY) security technology recently as the complementary approach to further enhancing the security in wireless communications [6]. The philosophy behind PHY security is to exploit the natural randomness of noise and the physical characteristics of wireless channels (like fading) to provide information-theoretic security, which has been regarded as the strongest form of security irrespective of the computing capabilities of eavesdroppers [7–9]. Thus, PHY security techniques are highly promising to guarantee everlasting secure communication for wireless networks [10–12].

The story of PHY security starts from Shannon's work in 1949 [13], where the concept of secrecy communication was investigated based on the information theory. Subsequently, Wyner introduced the noise wiretap channel model [14], where both links from the legitimate transmitter to the legitimate receiver and the eavesdropper are noisy. His result has uncovered the fact that, if the legitimate user's observation is better than the eavesdropper's observation, information-theoretically secure communication between the legitimate users is possible while keeping the eavesdropper completely ignorant of the secure message without using any secret keys. Wyner's work established the fundamental framework for the study of PHY security. Then, Wyner's result was generalized to the general (i.e., not necessarily degraded) wiretap channel by Csiszár and Körner in [15], determining the secrecy capacity for this general wiretap channel model. Their result has shown that even if the eavesdropping channel is not inferior to the legitimate channel, information-theoretically secure communication between the legitimate users can still be possible by exploiting the inherent randomness of the wireless medium. Following this line, the research of PHY security was conducted under various wireless channel models, such as Gaussian channel [16], multi-antenna channel [17] and relay channel [18], etc. Motivated by these early studies, diverse approaches for improving PHY security have been proposed in the literature, which mainly include channel beamforming [19–21], cooperative jamming [22–24], channel coding [25–27] and cooperative relaying [28–48].

Beamforming is a signal processing technique used in the multiple-in-multiple-out (MIMO) network for directional signal transmission or reception, where all nodes are equipped with antennas and one data stream can be transmitted to the intended receiver over multiple antennas. It enhances the information transmission security for the wireless network in such a way that signals at particular angles experience constructive interference while others experience destructive interference. It has been proved in [19] that beamforming can be highly effective in improving the secrecy rate of heterogeneous networks with orthogonal/non-orthogonal spectrum allocation strategies by optimizing the beam-forming weights at the macrocell and femtocell. The Beamforming application also can maximize the minimum secrecy rate among all users and secure energy efficiency (SEE) under the energy harvesting constraints, which are testified in [20] and [21], respectively. However, the beamformer optimization heavily depends on the channel state informations (CSIs). Thus, the high coordination requirements (such as synchronization and central optimization) among the source and relay nodes are required, which leads to the high overhead in implementation, as a large amount of information will be exchanged between the nodes.

Cooperative jamming ensures the security of wireless networks by employing the helper nodes to act as jammers, which generate artificial jamming signals at the eavesdropper, such that the achievable secrecy rate between the legitimate pair can be increased. According to the types of jamming signals, cooperative jamming can be classified into two categories. One is cooperative jamming with independent identically distributed (i.i.d) Gaussian signals, where the jamming signal will cause interference to both the legitimate receivers and the eavesdropper, but may result in zero secure degrees of freedom (s.d.o.f.) [22]. Another is based on the potential necessity of channel prefixing and adopts the structured signals, where the jamming signals could be nulled out at the intended receiver [23]. In [24], the s.d.o.f. equal to 1/2 can be achieved using real interference alignment whenever the value of the channel gain is any irrational number. The major difference between cooperative jamming with Gaussian noise and that with structured signals is that, in the latter, the legitimate user is able to decode the confusion signal, hence receiving a clean information-carrying signal whereas the eavesdropper's channel remains jammed. However, there are still several challenges in practical implementation. First, it is difficult to realize any dedicated helper node in the network, as nodes tend to make independent and selfish decisions in large scale networks. Second, the legitimate nodes may only have limited or even no CSI at the eavesdropper, especially if the eavesdropper operates in the passive mode, which imposes great challenges to cooperative jamming since the involved power allocation schemes usually rely on perfect channel estimation. This issue is of more concerning for jamming nodes because power allocation schemes for cooperative jamming usually rely on perfect channel estimation. Third, to minimize the gap between research efforts and practical implementation of the device cooperation, standardization is necessary. It is considerably difficult to standardize the friendly jamming under different network topologies, because the decision is based on the nature of jammers to either cooperate or stay independent.

Channel coding employs a nested wiretap code structure, mapping each message to one of several codewords at random to increase the confusion of the eavesdropper. In [25], the authors showed how capacity-achieving codes can be used to achieve the secrecy capacity for any wiretap channel and proved that it is possible to construct linear-time decodable secrecy codes based on low-density parity-check (LDPC) codes to achieve secrecy. The authors constructed the explicit polynomial-time encoding/decoding algorithm, the recently polar codes invented by Arıkan [49] has been shown to achieve the secrecy capacity for binary symmetric and deterministic wiretap channels in [26]. Recently, the channel coding research has been extended to the design of resilient codes for distributed data and cloud storage systems. The authors in [27] studied the problem of securing distributed storage systems (DSS) against eavesdroppers and malicious adversaries, and established a bound on the secrecy capacity with secure cooperative regenerating codes. Although this technique can notably achieve the high-security performance of the network, the construction of the codebook is hard and even challenging, especially for the sophisticated network in 5G. Furthermore, similar to the majority of the above two PHY security techniques, channel coding also requires the CSI knowledge of the eavesdropping channel.

Cooperative relaying technique aims to improve the security of wireless networks by choosing a link/relay with a strong legitimate channel and meanwhile a weak eavesdropping channel. According to whether the relay is equipped with buffers or not, cooperative relaying can be divided into two categories, i.e., traditional relaying [28–31] and buffer-aided relaying [32–48]. In traditional relaying, its transmission manner is pre-determined, i.e., the source-relay-destination transmission manner. The main basis for selection strategy is the Max-Min principle, i.e., the involved link/relay is selected to maximize the minimum instantaneous secrecy capacity of the two-hop links. If one link/relay is selected, the information transmission should be finished in two consecutive time slots. In the previous time slot, the source transmits the information to the selected relay and the selected relay will directly transmit the information to the destination in the later time slot. However, this pre-determined scheduling may lead to significant performance degradation in wireless systems, since the qualities of the transmitting and receiving channels significantly vary with time and such scheduling may prevent the relays from exploiting the best transmitting and the best receiving channels. For the buffer-aided relaying, the system is able to store and transmit the information in favorable wireless conditions, which increases the network's resiliency, throughput and diversity (see, for example, [50] [51]). Thus, each information now may experience three processes, i.e., the source-relay transmission process, queuing process in a relay buffer, and the relay-destination transmission process. Accordingly, in each time slot, there are three possible transmission states, i.e., source-relay transmission, relay-destination transmission, and no transmission. The analysis has shown that buffering can provide improved throughput, increased stability region, and better traffic load for each relay. Compared with the traditional relaying protocol, the authors in [36] showed that buffer-aided relaying can achieve a full diversity gain which is two times the number of relays in the network. Different from other PHY security techniques above, the relaying protocol technique is easy to be implemented as the sophisticated transmission techniques or explicit synchronization process are not required. Furthermore, the relaying protocol can be flexibly designed according to the states of CSI of the eavesdropper channel.

1.2 Objective and Main Works

This thesis focuses on the design of buffer-aided relaying protocol to ensure the security of wireless communications, taking into consideration the practical implementation under various network scenarios. Our objective is to fully explore the diversity gain of buffer and design the effectively secure communication protocol for buffer-aided relaying systems, while satisfying the various QoS requirements of users. Towards this end, we first design the communication protocols to ensure the transmission security and communication QoS of the two-hop buffer-aided relaying system with/without the instantaneous CSI at the transmitter, respectively, where the eavesdropper can intercept the information in both two hops. Considering the delivery delay constraint, we then design a novel security/delay-aware communication protocol for a two-hop buffer-aided relaying system with multiple relays. Four commonly-used performance metrics are of particular interest, which are the end-to-end (E2E) secrecy outage probability (SOP), throughput, secrecy throughput (ST), and packet discarding probability (PDP). E2E SOP characterizes the probability that the eavesdropper can decode the information without error. Throughput and ST characterize the long-term time-average on the number of messages that are successfully and securely delivered on both hops from the source to the destination, respectively. PDP characterizes the sum of the probability that the information is discarded at the source node and all relays due to expiration. The main works and contributions of this thesis are summarized in the following subsections.

1.2.1 Secure Communication Protocol for Buffer-Aided Relaying Systems

This work studies the design of the buffer-aided relaying protocol for two network scenarios that the instantaneous CSI of eavesdropping channel is available and unavailable. By now, a substantial amount of works have been devoted to the design of link selection schemes for guaranteeing PHY security performance in relaying networks [32, 34–36, 39, 43] (Please refer to Section 2.1 for related works). Even though these works demonstrated that activating the advisable link with favorable channel conditions can enhance the transmission security, however, how to conduct link selection to reconcile the transmission security with communication QoS is still an open issue. As a step forward in this direction, this work investigates the important trade-off issue between transmission security and communication QoS and designs the corresponding link selection policies. This work considers a practical eavesdropping scenario, in which the eavesdropper passively intercepts data transmission which can be hardly monitored. In addition, we adopt the assumption that the exact instantaneous/statistical CSI of the eavesdropping channel is unavailable, which differs from the assumption in existing works. The main contributions of this work are four-fold:

- We design link selection policies to ensure the communication security for both cases that the instantaneous CSI is available/unavailable at the source, which adopt adaptive-rate transmission mechanism and fixed-rate transmission mechanism, respectively. Particularly, according to the qualities of legitimate channels, the policies fully utilize the flexibility provided by buffer-aided relaying to select source-to-relay, relay-to-destination, or no link transmission, which are different from the conventional simple on-off schemes.
- We develop an analytical framework for the performance evaluation of proposed link selection policies. The closed-form expressions of three fundamental metrics, i.e., end-to-end secrecy outage probability (SOP), system throughput and secrecy throughput are derived, respectively.
- We explore the performance optimization issues and propose an iterative algorithm to optimize the link selection parameters. The study of performance optimizations reveals the inherent tradeoffs between the transmission security and communication quality of service (QoS), providing insightful guidelines for the practical configuration of link selection schemes to satisfy various system requirements.
- We conduct simulations to demonstrate the validity of theoretical performance evaluation, and also provide extensive numerical results to illustrate the efficiency of the proposed link selection policies for the secure communication in wireless cooperative networks.

1.2.2 Security/Delay Aware Protocol for Buffer-Aided Relaying Systems

It is worth noting that all the available works are based on the ideal assumption that the packet lifetime is unlimited (Please refer to Section 2.2 for related works).

However, in many practical wireless networks, packets are regarded to be invalid once the delivery time exceeds a limited validity period, especially for the delay-sensitive networks such as vehicular networks and military networks. Therefore, it is of great importance to further investigate the system design and performance analysis of buffer-aided relaying networks with limited packet lifetime. As the first attempt in this direction, this work proposes a novel security/delay-aware communication protocol for the end-to-end packet delivery in a wireless relaying network with limited packet lifetime, where multiple buffer-aided relays help the source forward packets to the destination and a passive eavesdropper wiretaps the data transmission. In this context, the limited packet lifetime will cause the complex heterogeneous queuing problem in the buffers, and meanwhile, the interaction among transmission security, efficiency, and the delivery delay will greatly increase the difficulty of the system performance evaluation. To address these issues, we develop a Markov chain-based theoretical framework to fully characterize the packet occupancy process in the relay buffers, which enables the fundamental system performance metrics to be derived in closed-form. The main contributions of this work are three-fold:

- A secure and delay-aware communication protocol: We propose a novel communication protocol to guarantee the security and timeliness of packet transmission in a buffer-aided relaying system with limited packet lifetime. Our protocol tracks the instantaneous CSI of transmission channels, the real-time buffer state as well as the packet delivery delay, and then grants the source and relays different transmission priorities such that a flexible interaction among the security requirement, transmission efficiency, and delay constraint can be achieved.

- A theoretical framework for network performance modeling: We first built a delicate *current deliver time (CDT) bitmap* structure to fully depict the packet occupancy processes and packet delay updates in the buffer queues. Then, we apply the Markov chain theory to model the state transition process of the bitmap caused by operating the proposed communication protocol, such that the stationary occupancy state distribution of the relay buffer can be obtained. With the help of the stationary state distribution, we eventually derive the closed-form expressions of three fundamental system-level performance metrics under two fading channel cases, including reliable outage probability, packet discarding probability and achievable secrecy throughput.

- Extensive simulation and numerical results: We conduct extensive simulations and also provide plentiful numerical results to validate the efficiency of our theoretical analysis framework as well as to demonstrate the performance of the proposed communication protocol. These results testify that the proposed communication protocol can guarantee both the transmission security and timeliness of the considered network. The optimal parameter settings of the protocol to cope with different performance requirements are also discussed.

1.3 Thesis Outline

The remainder of this thesis is outlined as follows. Chapter II introduces the related works of this thesis. In Chapter III, we introduce our work regarding the design of secure communication protocol for two-hop buffer-aided relaying systems, and Chapter IV presents the work on the design of security/delay-aware communication protocol for two-hop buffer-aided relaying systems with multiple relays. Finally, we conclude this thesis in Chapter V.

Table 1.1: Main notations

Notation	Definition
s	Source node

d	Destination node
e	Eavesdropper
exp	Exponential function
$\mathcal{M}$	Relay set
M	Number of relays
m ($m \in \mathcal{M}$)	The m-th relay
m^* ($m^* \in \mathcal{M}$)	Selected message relay
k ($k \in \mathcal{M}$)	Selected jammer
L	Buffer Size
$\mathbb{E}\{\cdot\}$	Expectation operator
$\lvert h_{i,j}\rvert^2$	Channel gain of link from node i to j
$\Omega_{i,j}$	Average channel gain of link from node i to j
σ_i	Noise variance of node i
$\gamma_{i,j}$	Signal-to-noise ratio (SNR) of link i to j
p_i	Transmission power of node i
I	Indicator variable of the link decision
R_t	Codeword rate
R_s	Target confidential message rate
$C_{i,j}$	Instantaneous channel capacity of link i to j
α, β	Link selection parameter
P_{so}	End-to-end (E2E) secrecy outage probability (SOP)
Φ	Throughput
Φ_S	Secrecy throughput
$f(\cdot)$	Probability-density-function (PDF)
$F(\cdot)$	Cumulative-density-function (CDF)
P_{up}	A given threshold of secrecy outage probability
β_i	Interference cancellation factor of node i

$\mathcal{D}$	Relay selection decision
t_c	Current deliver time (CDT)
t_d	Deliver time (DT)
t_a	The time that the packet arrives at the destination node
τ	Packet lifetime
U_i	CDT bitmap of node i
$\mathscr{U} = \{U_s, U_1, U_2, \ldots, U_M\}$	The CDT bitmap set of the sytem
$\mathbb{S} = \{S_1, S_2, \ldots, S_I\}$	The state set of Markov chain (MC)
π_i	The unique stationary probability distribution of S_i
A	The state transition matrix of the MC in S_i
$A_{i,j}$	The state transition probability from S_i to S_j
Ψ_{S_i}	The total number of the available links in S_i
$\Psi_{S_i}^{sm}$	The number of the available $s \rightarrow m$ links in S_i
$\Psi_{S_i}^{md}$	The number of the available $m \rightarrow d$ links in S_i
$\mathbb{G}_l^{PNI}$	The link set where the involved relay owns l packets
$\mathbb{G}_d^{DSI}$	The link set where the delay sate information of the oldest packet of the involved relay is d
P_{ro}	The reliable outage probability (ROP)
P_{dis}	The packet discarding probability (PDP)
$\mathcal{Q}$	The achievable secrecy throughput

CHAPTER II

Related Works

This chapter introduces the existing works related to our study in this thesis, including the works on the design of secure communication protocols with/without deliver delay constraint for two-hop buffer-aided relaying wireless systems.

2.1 Secure Communication Protocol for Buffer-Aided Relaying Systems

By now, many works have been devoted to the design of secure communication protocol for buffer-aided relaying networks. These works mainly focused on two-hop relaying systems with single/multiple relays. For the scenario with single relay, the protocol design reduces to the selection of a link among the links of source-relay, relay-destination and source-destination to enhance the PHY security of the system. Taking into account the transmission efficiency and security constraint, Huang *et al.* [32] designed the novel link selection scheme in a two-hop buffer-aided relaying network to achieve tradeoff between secrecy throughput and secrecy outage probability. Considering that the relay operate in full-duplex (FD), the authors proposed a secure communication protocol that allows the relay to switch between the FD mode and half-duplex (HD) mode. The optimal setting of mode switching probability was examined in [33] for the maximization of secrecy network throughput. Considering that the power control can significantly improve the secrecy capacity, the optimal joint link selection and power control protocol that maximize the secrecy throughput was proposed in [34]. This work was then extended to the buffer-aided network assisted by an energy harvesting relay in [35], the authors considered two cases, i.e., the knowledge of the energy harvesting and fading channels states is known in a non-causal manner (offline) and causal manner (online), two secure communication protocols were designed to ensure the transmission efficiency and information security, respectively.

Regarding the two-hop relaying systems with multiple relays, Chen *et al.* [36] put forward the max-ratio (MR) selection scheme for half-duplex decode-and-forward (DF) relaying networks. The MR scheme activates the link with the largest channel gain ratio based on the knowledge of both legitimate and wiretap channel state information (CSI), and it can achieve a better secrecy performance than the conventional max-min-ratio scheme [37]. For the relay system with direct source-destination link, the authors in [38] proposed a communication protocol based on artificial noise injection, where the node not involved in the transmission serves as a jammer for noise injection. The secrecy throughput maximization issue was also explored in [38] under certain SOP constraint. For a buffer-aided relaying MIMO system, the authors proposed a joint transmit antenna and relay selection protocol to enhance the secrecy performance [39]. Then, this work was extended to the more general network scenario with multi-antenna destination, the authors in [40] proposed three secure communication protocols for secrecy improvement i.e., 1) maximal-ratio combining (MRC), 2) maximal-ratio combining/cooperative jamming (MRC/CJ), and 3) zero-forcing beamforming/cooperative jamming (ZFB/CJ). The secrecy diversity gains of the proposed protocols were analyzed for different relay numbers and buffer sizes. The authors in [41] proposed the novel communication protocol to secure the transmission in a buffer-aided MIMO relaying system with multiple eavesdroppers system. The optimal transmission rates were derived to maximize the average secrecy throughput under the intended secrecy outage probability constraint.

These works demonstrated that secure communication protocol is flexible and promising for achieving a desirable PHY security performance for buffer-aided relaying systems. It is notable, however, that current protocols are based on the ideal assumption on the CSIs of eavesdropping channels, and the conventional protocols cannot ensure the security for both hops, especially when the channel quality of eavesdropping channels is better than the ones of main channels. Furthermore, in order to secure the information transmission, they would reduce the transmission opportunities and sacrifice other performance of the network. Thus, one natural and crucial question arises: how to design the communication protocol while securing the E2E security and satisfying the communication QoS. Answering this question is very important for the applications of buffer-aided relay systems in future wireless communication scenarios.

2.2 Security/Delay-Aware Communication for Buffer-Aided Relaying Systems

Since the pioneer works of Zlatanov [50] [51], the various communication protocols have been proposed to enhance the PHY security performances for buffer-aided relaying systems [32–41]. However, the buffer at the relay can introduce additional delay to the communication between the source and destination due to its buffer queuing process and relay selection process. First, activating the relay-destination link, a packet at the source or the head of a certain relay queue may have to wait for a long time (i.e., service time) before it is served by the selected link; Second, the buffer queuing process, i.e., the process when a packet moves from the end of the relay queue of a certain relay to the head of this queue, may also incur a long queuing delay at the relay since a relay usually needs to help forward multiple packets. In current wireless systems, multimedia traffic such as mobile video has surged significantly, and the delay has become an important consideration. Thus, the benefits of the buffer-aided relay under delay constraints were further investigated in [42]. The authors considered the instantaneous qualities of the involved links but also took the states of the queues at the buffers into account, and proposed two heuristic but efficient delay-constrained protocols to approach the throughput upper bound for a buffer-aide relaying systems. Motivated by this work, the authors in [43] studied of E2E security and delay performances for two-hop buffer-aided relaying systems with Max-Ratio communication protocol. Based on the established Markov theoretical framework, a clear trade-off between the E2E security performance and delay performance was revealed. In order to decrease the transmit delay, the authors proposed a secure cooperative transmission protocol with the optimization of transmit delay in [44]. The rateless code and multicast scheme was applied to make sure that multiple relays can obtain total data reliably with a lower transmission delay. With consideration of the small buffer size in [45], one novel communication protocol named max-weight secure link selection (MWSLS) was designed to ensure the security and delay constraint. However, the more hazardous scenarios with diversity-combining eavesdroppers that combine the signals in two hops to decode the packets are largely ignored. The authors in [46] proposed two communication protocols to ensure the security and delay for perfect and partial eavesdropper CSIs, respectively.

However, it is worth noting that all the existing works only consider the statistic delay constraint. In practical wireless networks, the information is regarded to be invalid once the delivery time exceeds a given limited validity period. Therefore, the communication protocol needs to be carefully designed which can ensure the transmission security and provide flexible control of both the secrecy throughput and packet delay. Furthermore, the new analytical framework needs to be established to model the packet discarding behavior at both source and relays due to outdate.

CHAPTER III

Secure Communication Protocol for Buffer-Aided Relaying Systems

This chapter investigates the secure communication in a two-hop cooperative wireless network, where a buffer-aided relay helps forward data from the source to destination, and a passive eavesdropper attempts to intercept data transmission from both the source and relay. To ensure the transmission security and communication quality of service (QoS) of the system, we design novel link selection policies for two cases that the instantaneous channel state information is available or unavailable at the source node. For evaluating the system performance, we then derive the closed-form expressions of end-to-end secrecy outage probability, system throughput and secrecy throughput, respectively. Based on the theoretical performance analysis, we further explore the performance optimization issues, revealing the insightful tradeoffs between transmission security and QoS. An iterative algorithm is developed to identify the optimal setting of link selection parameters, which is helpful for the practical configuration of link selection policies to satisfy various system performance requirements. Finally, we conduct simulations to validate our theoretical performance analysis, and also provide extensive numerical results to illustrate the efficiency of the proposed link selection policies for ensuring secure communication in a two-hop cooperative network.

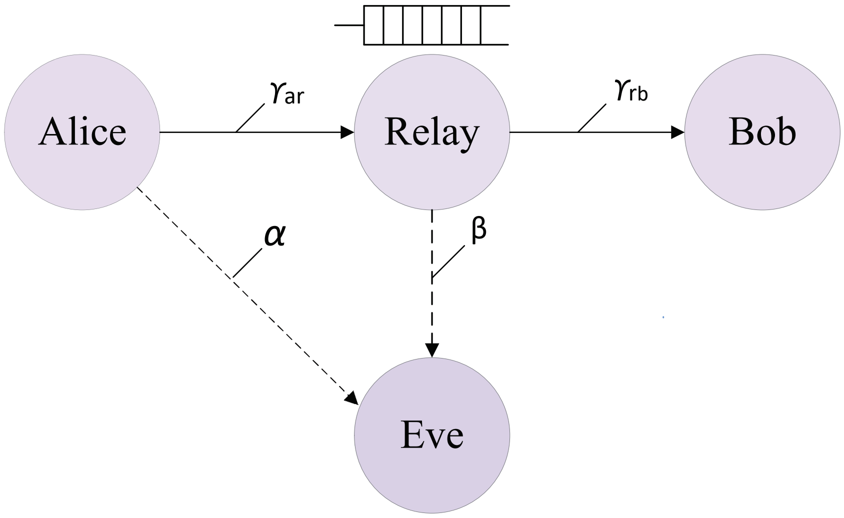


Figure 3.1: Illustration of system model.

3.1 System Model and Definitions

In this section, we introduces the system models and some basic definitions in detail.

3.1.1 Network Model

As shown in Fig. 3.1, we consider a two-hop wireless cooperative network which consists of a source (Alice), a destination (Bob), a relay (Relay) and a passive eavesdropper (Eve). We assume that there is no direct link from Alice to Bob so that the messages from Alice can be delivered to Bob only via Relay. Relay is equipped with infinite buffer to temporarily store the messages from Alice and operates in the half-duplex mode, thus it can not transmit and receive simultaneously. Moreover, we apply the randomize-and-forward (RF) strategy [52]. Different from the conventional DF relaying, the buffer-aided RF relaying allows the decoded data to be stored in the relay buffer temporarily and be forwarded to Bob by adopting the independent and randomized signal transmission in some future time slot. Thus, a time slot is not divided into two halves. We assume that Alice and Relay transmit messages with fixed power P_a and P_r, respectively. Eve attempts to intercept signals from both Alice and Relay, but due to the RF strategy, it cannot process the signals from two hops by applying combing techniques such as MRC [53].

We consider the single relay scenario in this study mainly due to the following reasons. First, the mathematical tractability under the single relay scenario allows us to gain important insights into the link selection design for security-QoS tradeoffs. Second, the analysis under the single relay scenario lays the foundation for the analysis under the multiple relay scenarios.

3.1.2 Wireless Channel Model

We consider a time-slotted system where the time is divided into successive slots with equal duration. All wireless links are characterized by the quasi-static Rayleigh block fading such that the channel fading coefficient of each link remains constant during one time slot, but changes independently and randomly from one time slot to the next. We use $h_{i,j}[k]$ to denote the fading coefficient from node i to node j at time slot k, where $i \in \{a, r\}$, $j \in \{r, b, e\}$ and $k \in \{1, 2, \cdots, T\}$, here a, r, b, e are short for Alice, Relay, Bob and Eve, respectively, and T is the total observation time. With the quasi-static Rayleigh block fading model, the channel gain of a link is independently and exponentially distributed with mean $\mathbb{E}\{|h_{i,j}[k]|^2\} = \Omega_{i,j}$, where $\mathbb{E}\{\cdot\}$ is the expectation operator. In addition, complex additive white Gaussian noise (AWGN) is imposed on each link and its variance at Relay, Bob and Eve are δ_r^2, δ_b^2 and δ_e^2, respectively. Therefore, the instantaneous signal-to-noise ratio (SNR) $\gamma_{i,j}[k]$ of a link at time slot k is determined as

$$\gamma_{i,j}[k] = \frac{P_i}{\delta_j^2} |h_{i,j}[k]|^2. \tag{3.1}$$

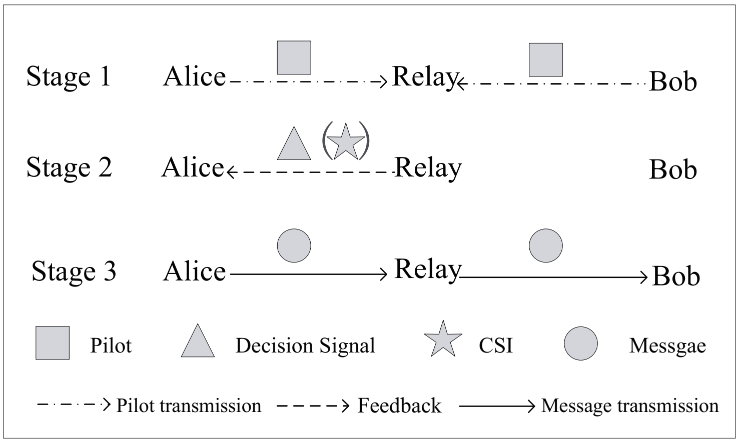


Figure 3.2: Illustration of transmission scheduling process in a time slot.

$\gamma_{i,j}[k]$ is also exponentially distributed with the probability density function (p.d.f) given by

$$f_{\gamma_{i,j}[k]}(x) = \frac{1}{\bar{\gamma}_{i,j}} \exp\left(-\frac{x}{\bar{\gamma}_{i,j}}\right), \quad x \geq 0, \tag{3.2}$$

where $\bar{\gamma}_{i,j} = \frac{P_i}{\delta_j^2}\Omega_{i,j}$. Considering the fact that Eve is a passive eavesdropper, the instantaneous CSIs from Alice and Relay to Eve, i.e., $h_{a,e}[k]$ and $h_{r,e}[k]$, are *unavailable* in this study.

3.2 Secure Communication Protocol Design

In order to ensure the transmission security for the concerned system, we design the link selection policies in two cases that the instantaneous CSI is available/unavailable at Alice. We first present the overall scheduling of the policies in a time slot, and then detail the link selection strategies and corresponding transmission mechanisms in the two cases, respectively.

3.2.1 Transmission Scheduling

Regarding the transmission scheduling process in a time slot, in order to ensure the transmission security and avoid channel outage [54], we first need to estimate the instantaneous CSIs of legitimate links. Then, link selection can be conducted according to some strategies. Finally, the system conducts transmission operation or *remains idle* according to the selection decision. Therefore, as illustrated in Fig. 3.2, the overall scheduling of our link selection policies consist of the following three stages.

Stage 1 (**CSI Estimation**)

Alice and Bob transmit the pilot sequences to Relay in turn. By assuming that the reciprocity property [55] of antenna holds, Relay can estimate the CSIs of both Alice-to-Relay and Relay-to-Bob links.

Stage 2 (**Link Selection**)

With the CSIs of two links, Relay acts as the *central node* to make link selection decision based on some strategies. According to that whether Relay feeds back the CSI to Alice, we consider the following two cases.

a) CSI *is available* at Alice: Relay makes link selection decision based on the strategy described in Subsection 3.2.2. If Alice-to-Relay link is selected, Relay feeds back the decision signal and the CSI to Alice.

b) CSI *is not available* at Alice: Relay makes link selection decision based on the strategy described in Subsection 3.2.3. If Alice-to-Relay link is selected, Relay only feeds back the decision signal to Alice.

Stage 3 (**Message Transmission**)

According to the link selection decision, Alice or Relay transmits the message, or the system remains idle. The details of transmission mechanisms in the two cases will be introduced in Subsections 3.2.2 and 3.2.3, respectively.

Remark 1 *It is worth noting that the overall scheduling of our policies incurs at most three handshakes before the actual message transmission, thus the system operation is* *of low-complexity. The overhead includes n pilot symbols for the channel measurement (which is determined by the channel estimation methods),* 4*-bit channel quality index (CQI), and* 1*-bit for link selection declaration (*1 *and* 0 *indicates that the link is and is not selected for transmission, respectively.)*

3.2.2 Link Selection Policy with CSI Feedback

With the existing link selection policies such as [32], either Alice-to-Relay or Relay-to-Bob link is selected for data transmission in any time slot. However, since the eavesdropper Eve intercepts messages from both links, once in a time slot the channel qualities of both legitimate links are worse than those of corresponding wiretap links, the transmission security cannot be ensured no matter which link is selected.

With the above observation, in our new policy the system will remain idle when both the legitimate links are not of good quality. Specifically, we let I_k be an indicator variable to denote the link decision in time slot k, where $I_k = 0$, $I_k = 1$ and $I_k = -1$ indicate the selection of Alice-to-Relay link, Relay-to-Bob link and no link, respectively.

To guarantee the secure transmission, we employ the well-known Wyner's encoding scheme [14]. When a transmission is conducted, the transmitter (Alice or Relay) chooses two rates, one is the codeword rate R_t, another is the confidential message rate R_s. The difference between the two rates $R_e = R_t - R_s$, i.e., the rate redundancy, reflects the cost of secrecy transmission against eavesdropping. If the wiretap channel capacity is larger than R_e, i.e., $C_e > R_e$, the secrecy outage happens. Thus, the necessary condition of secure transmission is $R_t \geq R_s + C_e$. Let $R_{a,r}[k]$ and $R_{r,b}[k]$ denote the codeword rates when Alice and Relay are selected for transmission at time slot k, respectively. Under the policy with CSI feedback, since Alice and Relay know the the corresponding instantaneous CSI, they adaptively adjusts the codeword rate to be arbitrarily close to the channel capacity, termed as ***adaptive-rate (AR)***

transmission. Therefore, $R_{a,r}[k]$ and $R_{r,b}[k]$ can be determined as

$$R_{a,r}[k] = C_{a,r}[k] = \log_2(1 + \gamma_{a,r}[k]), \tag{3.3}$$

$$R_{r,b}[k] = C_{r,b}[k] = \log_2(1 + \gamma_{r,b}[k]), \tag{3.4}$$

where $C_{i,j}[k]$ denotes the channel capacity between nodes i and j, and it is determined by the Shannon Theorem [13].

Note that we consider the practical scenario where the instantaneous/statistical CSI of the wiretap channel is unknown, Alice (*resp.* Relay) cannot judge that whether $R_{a,r}[k] \geq R_s + C_{a,e}[k]$ (*resp.* $R_{r,b}[k] \geq R_s + C_{r,e}[k]$) holds. Hence, we adopt two non-negative parameters α and β to serve as the thresholds for the channel qualities of two legitimate links, respectively. Only if the condition $\gamma_{a,r}[k] \geq \alpha$ (*resp.* $\gamma_{r,b}[k] \geq \beta$) is satisfied, Alice-to-Relay (*resp.* Relay-to-Bob) link can be selected for message transmission. If $\gamma_{a,r}[k] < \alpha$ and $\gamma_{r,b}[k] < \beta$, no link will be selected. When both the legitimate links are of high channel quality, i.e., both $\gamma_{a,r}[k] \geq \alpha$ and $\gamma_{r,b}[k] \geq \beta$ hold, the link with a relative better quality will be selected, i.e., $I_k = 0$ if $\frac{\gamma_{a,r}[k]}{\alpha} \geq \frac{\gamma_{r,b}[k]}{\beta}$ and $I_k = 1$ if $\frac{\gamma_{a,r}[k]}{\alpha} < \frac{\gamma_{r,b}[k]}{\beta}$.

Finally, in order to guarantee the codeword rate of the selected link can cover the confidential message rate R_s, i.e., $R_{a,r}[k] \geq R_s$ and $R_{r,b}[k] \geq R_s$, we ensure that the thresholds need to satisfy $\alpha \geq 2^{R_s} - 1$ and $\beta \geq 2^{R_s} - 1$. Therefore, our link selection algorithm with CSI feedback can be summarized as Algorithm 1.

3.2.3 Link Selection Policy without CSI Feedback

With the concern of system complexity and overhead, we also explore the link selection policy without CSI feedback. Since the design is similar to that in the previous subsection, we only explain the differences in the link selection algorithm and corresponding transmission mechanism.

Algorithm 1 Link Selection Algorithm with CSI Feedback

```
Require:
  Instantaneous CSIs of two legitimate links, confidential message rate $R_s$ and thresholds $\alpha$ and $\beta$ which satisfy $\alpha \geq 2^{R_s} - 1$ and $\beta \geq 2^{R_s} - 1$;
Ensure:
  Link decision indicator $I_k$, $k \in \{1, 2, \cdots, T\}$;
  for $k = 1$; $k \leq T$; $k++$ do
    Calculate $\gamma_{a,r}[k]$ and $\gamma_{r,b}[k]$ based on the instantaneous CSIs;
    if $\gamma_{a,r}[k] \geq \alpha \wedge \frac{\gamma_{a,r}[k]}{\alpha} \geq \frac{\gamma_{r,b}[k]}{\beta}$ then
      $I_k = 0$;
    else if $\gamma_{r,b}[k] \geq \beta \wedge \frac{\gamma_{r,b}[k]}{\beta} > \frac{\gamma_{a,r}[k]}{\alpha}$ then
      $I_k = 1$;
    else
      $I_k = -1$;
    end if
  end for
```

For the link selection policy without CSI feedback, when Alice-to-Relay link is selected, the transmitter Alice don't know the corresponding instantaneous CSI, thus it cannot adaptively adjust the codeword rate to be the channel capacity. Instead, Alice always sets the codeword rate $R_{a,r}[k]$ as a fixed rate R_a ($R_a \geq R_s$), termed as ***fixed-rate (FR) transmission***. When Relay-to-Bob link is selected, the codeword rate $R_{r,b}[k]$ is the same as (3.4) since Relay always knows the instantaneous CSI.

Same as the previous subsection, we also adopt two non-negative parameters α and β to serve as the thresholds for the channel qualities of two legitimate links. Another consideration is that when Alice conducts the information transmission, if the instantaneous channel capacity is less than the codeword rate, i.e., $C_{a,r}[k] = \log_2(1+\gamma_{a,r}[k]) < R_a$, the channel outage happens such that Relay cannot decode the information correctly. In order to avoid the channel outage, we further design that Alice-to-Relay link cannot be selected if Relay finds $\gamma_{a,r}[k] < 2^{R_a} - 1$, even though $\gamma_{a,r}[k] \geq \alpha$ holds. Therefore, our link selection algorithm without CSI feedback can be summarized as Algorithm 2.

Algorithm 2 Link Selection Algorithm without CSI Feedback

```
Require:
  Instantaneous CSIs of two legitimate links, fixed codeword rate of Alice $R_a$, confidential message rate $R_s$ and thresholds $\alpha$ and $\beta$ which satisfy $R_a \geq R_s$, $\alpha \geq 2^{R_s} - 1$ and $\beta \geq 2^{R_s} - 1$;
Ensure:
  Link decision indicator $I_k$, $k \in \{1, 2, \cdots, T\}$;
  for $k = 1$; $k \leq T$; $k++$ do
    Calculate $\gamma_{a,r}[k]$ and $\gamma_{r,b}[k]$ based on the instantaneous CSIs;
    if $\gamma_{a,r}[k] \geq \max\{\alpha, 2^{R_a} - 1\}$ then
      if $\frac{\gamma_{a,r}[k]}{\alpha} \geq \frac{\gamma_{r,b}[k]}{\beta}$ then
        $I_k = 0$;
      else
        $I_k = 1$;
      end if
    else if $\gamma_{r,b}[k] \geq \beta$ then
      $I_k = 1$;
    else
      $I_k = -1$;
    end if
  end for
```

For a better understanding of our link selection policy without CSI feedback, we illustrate in Fig. 3.3 the value of I_k in different SNR regions. We can see from Fig. 3.3(a) that when we set the threshold $\alpha \geq 2^{R_a} - 1$, the value of I_k in different SNR regions decided by the policy without CSI feedback is the same as that with CSI feedback. However, if we set the threshold $\alpha < 2^{R_a} - 1$, for the interval $\gamma_{a,r}[k] \in [\alpha, 2^{R_a} - 1)$, even though in the region of $\frac{\gamma_{a,r}[k]}{\alpha} \geq \frac{\gamma_{r,b}[k]}{\beta}$, I_k is still set to be 1 once $\gamma_{r,b}[k] > \beta$ is satisfied, as shown in the triangle area of Fig. 3.3(b).

3.3 Performance Evaluation and Optimization

In this section we evaluate the performance for our proposed link selection policies. We focus on three widely-used fundamental performance metrics including *secrecy outage probability* (SOP), *throughput* and *secrecy throughput (ST)*, and develop the

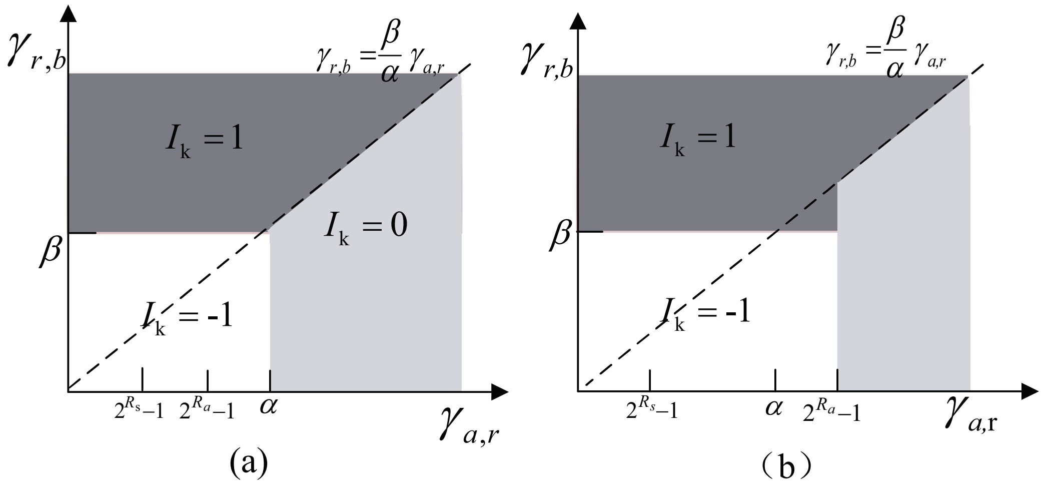


Figure 3.3: The value of I_k in different SNR regions. (a) $\alpha \geq 2^{R_a}-1$. (b) $\alpha < 2^{R_a}-1$.

analytical framework to derive their closed-form expressions.

3.3.1 Secrecy Outage Probability

According to Wyner's encoding scheme [14], for a transmission over a wireless channel wiretapped by an eavesdropper, the event of secrecy outage refers to the case that the transmission rate redundancy (i.e., the difference between the codeword rate and the confidential message rate) is less than the channel capacity of wiretap link, such that the message can be decoded by the eavesdropper. Secrecy outage probability (SOP) is defined as the probability that the event of secrecy outage happens. Therefore, the end-to-end (E2E) SOP of the system is the probability that the event of secrecy outage happens on at least one of the two hops when a message is delivered from Alice to Bob. The E2E SOP is of great significance as it serves as a measure of the transmission security level.

Let $\Gamma_{a,r}[k]$ and $\Gamma_{r,b}[k]$ be two indicator variables defined as

$$\Gamma_{a,r}[k] = \begin{cases} 1, & R_{a,r}[k] - R_s < C_{a,e}[k] \\ 0, & \text{otherwise} \end{cases} \tag{3.5}$$

$$\Gamma_{r,b}[k] = \begin{cases} 1, & R_{r,b}[k] - R_s < C_{r,e}[k] \\ 0. & \text{otherwise} \end{cases} \tag{3.6}$$

Based on the above definitions, the SOPs of Alice-to-Relay link and Relay-to-Bob link are given by[1]

$$P_{so}^{a,r} = \Pr\{\Gamma_{a,r}[k] = 1 | I_k = 0\}, \tag{3.7}$$

$$P_{so}^{r,b} = \Pr\{\Gamma_{r,b}[k] = 1 | I_k = 1\}. \tag{3.8}$$

Therefore, the end-to-end (E2E) SOP can be formulated as

$$P_{so} = 1 - (1 - P_{so}^{a,r})(1 - P_{so}^{r,b}). \tag{3.9}$$

In order to derive the closed-form expression for SOP, we first need the following two lemmas.

Lemma 1 *The probability P_A that Alice is selected to transmit message at a time slot is determined as*

$$P_A = \begin{cases} \mu(\alpha,\beta), & \textit{for AR case} \\ \nu(\alpha,\beta), & \textit{for FR case} \wedge \alpha < 2^{R_a} - 1 \\ \mu(\alpha,\beta), & \textit{for FR case} \wedge \alpha \geq 2^{R_a} - 1 \end{cases} \tag{3.10}$$

where $\mu(\alpha,\beta)$ and $\nu(\alpha,\beta)$ are given by

$$\mu(\alpha,\beta) = \exp\left(-\frac{\alpha}{\bar{\gamma}_{a,r}}\right) - \frac{\alpha\bar{\gamma}_{r,b}}{\alpha\bar{\gamma}_{r,b} + \beta\bar{\gamma}_{a,r}} \exp\left(-\frac{\alpha}{\bar{\gamma}_{a,r}} - \frac{\beta}{\bar{\gamma}_{r,b}}\right), \tag{3.11}$$

[1] Since the channel gain of a link is independent and identically distributed in each time slot, the SOP of a link is the same in each time slot and the time indicator k can be omitted.

$$\nu(\alpha,\beta)=\exp\left(\frac{1-2^{R_a}}{\bar{\gamma}_{a,r}}\right)\left[1-\frac{\alpha\bar{\gamma}_{r,b}}{\alpha\bar{\gamma}_{r,b}+\beta\bar{\gamma}_{a,r}}\exp\left(\frac{\beta(1-2^{R_a})}{\alpha\bar{\gamma}_{r,b}}\right)\right], \tag{3.12}$$

and $\wedge$ *is the logical AND operator.*

Proof: The proof is given in Appendix A.1. ■

Lemma 2 *The probability* P_R *that Relay is selected to transmit message at a time slot is determined as*

$$P_R=\begin{cases}\bar{\mu}(\alpha,\beta), & \textit{for AR case}\\ \bar{\nu}(\alpha,\beta), & \textit{for FR case}\wedge\alpha<2^{R_a}-1\\ \bar{\mu}(\alpha,\beta), & \textit{for FR case}\wedge\alpha\geq 2^{R_a}-1\end{cases} \tag{3.13}$$

where $\bar{\mu}(\alpha,\beta)$ and $\bar{\nu}(\alpha,\beta)$ are given by

$$\bar{\mu}(\alpha,\beta)=\exp\left(-\frac{\beta}{\bar{\gamma}_{r,b}}\right)-\frac{\beta\bar{\gamma}_{a,r}\exp\left(-\frac{\alpha}{\bar{\gamma}_{a,r}}-\frac{\beta}{\bar{\gamma}_{r,b}}\right)}{\alpha\bar{\gamma}_{r,b}+\beta\bar{\gamma}_{a,r}}, \tag{3.14}$$

$$\bar{\nu}(\alpha,\beta)=\exp\left(-\frac{\beta}{\bar{\gamma}_{r,b}}\right)+\exp\left(\frac{1-2^{R_a}}{\bar{\gamma}_{a,r}}\right)\left[\frac{\alpha\bar{\gamma}_{r,b}\exp\left(\frac{\beta(1-2^{R_a})}{\alpha\bar{\gamma}_{r,b}}\right)}{\alpha\bar{\gamma}_{r,b}+\beta\bar{\gamma}_{a,r}}-\exp\left(-\frac{\beta}{\bar{\gamma}_{r,b}}\right)\right]. \tag{3.15}$$

Proof: The proof is the same as that for Lemma 1, so we omit it here. ■

Then, based on the exact results of P_A and P_R, we have the following theorem regarding the closed-form expression of SOP.

Theorem III.1 (Secrecy Outage Probability) *For a concerned cooperative network with the system models described in Section 3.1, we apply the link selection policies proposed in Section 3.2 for information transmission, then the end-to-end*

$$\omega(\alpha,\beta,R_s)=1-\frac{2^{R_s}\bar{\gamma}_{a,e}(\beta\bar{\gamma}_{a,r}+\alpha\bar{\gamma}_{r,b})\exp\left(\frac{2^{R_s}-\alpha-1}{\bar{\gamma}_{a,e}2^{R_s}}\right)\left[\frac{\beta}{\alpha}+\left(\frac{\bar{\gamma}_{r,b}}{\bar{\gamma}_{a,r}}+\frac{\bar{\gamma}_{r,b}}{\bar{\gamma}_{a,e}2^{R_s}}\right)\left(1-\exp\left(-\frac{\beta}{\bar{\gamma}_{r,b}}\right)\right)\right]}{(2^{R_s}\bar{\gamma}_{a,e}+\bar{\gamma}_{a,r})\left[\beta\bar{\gamma}_{a,r}\left(1-\exp(-\frac{\beta}{\bar{\gamma}_{r,b}})\right)+\alpha\bar{\gamma}_{r,b})\right]\left(\frac{\beta}{\alpha}+\frac{\bar{\gamma}_{r,b}}{\bar{\gamma}_{a,r}}+\frac{\bar{\gamma}_{r,b}}{\bar{\gamma}_{a,e}2^{R_s}}\right)} \tag{3.18}$$

$$\varphi(\alpha,\beta,R_s)=1-\frac{2^{R_s}\bar{\gamma}_{r,e}(\beta\bar{\gamma}_{a,r}+\alpha\bar{\gamma}_{r,b})\exp\left(\frac{2^{R_s}-\beta-1}{\bar{\gamma}_{r,e}2^{R_s}}\right)\left[\frac{\alpha}{\beta}+\left(\frac{\bar{\gamma}_{a,r}}{\bar{\gamma}_{r,b}}+\frac{\bar{\gamma}_{a,r}}{\bar{\gamma}_{r,e}2^{R_s}}\right)\left(1-\exp\left(-\frac{\alpha}{\bar{\gamma}_{a,r}}\right)\right)\right]}{(2^{R_s}\bar{\gamma}_{r,e}+\bar{\gamma}_{r,b})\left[\alpha\bar{\gamma}_{r,b}\left(1-\exp(-\frac{\alpha}{\bar{\gamma}_{a,r}})\right)+\beta\bar{\gamma}_{a,r})\right]\left(\frac{\alpha}{\beta}+\frac{\bar{\gamma}_{a,r}}{\bar{\gamma}_{r,b}}+\frac{\bar{\gamma}_{a,r}}{\bar{\gamma}_{r,e}2^{R_s}}\right)} \tag{3.19}$$

$$\bar{\varphi}(\alpha,\beta,R_s)=1-\frac{2^{R_s}\bar{\gamma}_{a,e}\exp\left(-\frac{\beta+1-2^{R_s}}{2^{R_s}\bar{\gamma}_{a,e}}\right)\left(1-\exp\left(-\frac{2^{R_a}-1}{\bar{\gamma}_{a,r}}\right)\right)}{(2^{R_s}\bar{\gamma}_{a,e}+\bar{\gamma}_{r,b})\left[1+\exp\left(-\frac{2^{R_a}-1}{\gamma_{a,r}}\right)\left(\frac{\alpha\bar{\gamma}_{r,b}}{\alpha\bar{\gamma}_{r,b}+\beta\bar{\gamma}_{a,r}}\exp\left(-\frac{\beta(2^{R_a}-1)}{\alpha\bar{\gamma}_{r,b}}\right)-1\right)\right]} \tag{3.20}$$

---

secrecy outage probability is given by

$$P_{so}=1-\begin{cases}\omega(\alpha,\beta,R_s)\cdot\varphi(\alpha,\beta,R_s), & \textit{for AR case}\\ \bar{\omega}(R_s)\cdot\bar{\varphi}(\alpha,\beta,R_s), & \textit{for FR case}\wedge\alpha<2^{R_a}-1\\ \bar{\omega}(R_s)\cdot\varphi(\alpha,\beta,R_s), & \textit{for FR case}\wedge\alpha\geq 2^{R_a}-1\end{cases} \tag{3.16}$$

where $\bar{\omega}(R_s)$ is determined as

$$\bar{\omega}(R_s)=1-\exp\left(-\frac{2^{R_a-R_s}-1}{\bar{\gamma}_{a,e}}\right), \tag{3.17}$$

$\omega(\alpha,\beta,R_s)$, $\varphi(\alpha,\beta,R_s)$ and $\bar{\varphi}(\alpha,\beta,R_s)$ are expressed as (3.18)-(3.20), respectively.

Proof: Considering the case of AR transmission mechanism (i.e., link selection policy with CSI feedback), based on formula (3.7), we have

$$P_{so}^{a,r}=\Pr\{\Gamma_{a,r}[k]=1|I_k=0\}=\frac{\Pr\{\Gamma_{a,r}[k]=1,I_k=0\}}{\Pr\{I_k=0\}}, \tag{3.21}$$

where $\Pr\{I_k = 0\}$ is given by equation (3.11) and

$$\Pr\{\Gamma_{a,r}[k] = 1, I_k = 0\} = \Pr\left\{\max\{\alpha, \frac{\alpha}{\beta}\gamma_{r,b}[k]\} < \gamma_{a,r}[k] < 2^{R_s}(1+\gamma_{a,e}[k]) - 1\right\}$$
$$= \left(\int_{\beta}^{\infty}\int_{\frac{\alpha y+\beta}{\beta 2^{R_s}}-1}^{\infty}\int_{\frac{\alpha y}{\beta}}^{2^{R_s}(1+z)-1} + \int_{0}^{\beta}\int_{\frac{\alpha y+1}{2^{R_s}}-1}^{\infty}\int_{\alpha}^{2^{R_s}(1+z)-1}\right) f_{\bar{\gamma}_{a,r}}(x) f_{\bar{\gamma}_{a,e}}(z) f_{\bar{\gamma}_{r,b}}(y)\,dxdzdy. \tag{3.22}$$

By substituting (3.11) and (3.22) into (3.21) as well as some integral and algebraic calculations, we can obtain the expression of $\omega(\alpha,\beta,R_s)$ as (3.18).

Similarly, based on formula (3.8), we have

$$P_{so}^{r,b} = \Pr\{\Gamma_{r,b}[k] = 1 | I_k = 1\} = \frac{\Pr\{\Gamma_{r,b}[k] = 1, I_k = 1\}}{\Pr\{I_k = 1\}}, \tag{3.23}$$

where $\Pr\{I_k = 1\}$ is given by equation (3.14) and

$$\Pr\{\Gamma_{r,b}[k] = 1, I_k = 1\}$$
$$= \Pr\left\{\max\{\beta, \frac{\beta}{\alpha}\gamma_{a,r}[k]\} < \gamma_{r,b}[k] < 2^{R_s}(1+\gamma_{r,e}[k]) - 1\right\}$$
$$= \left(\int_{\alpha}^{\infty}\int_{\frac{\beta x+\alpha}{\alpha 2^{R_s}}-1}^{\infty}\int_{\frac{\beta x}{\alpha}}^{2^{R_s}(1+z)-1} + \int_{0}^{\alpha}\int_{\frac{\beta x+1}{2^{R_s}}-1}^{\infty}\int_{\beta}^{2^{R_s}(1+z)-1}\right) f_{\bar{\gamma}_{r,b}}(x) f_{\bar{\gamma}_{r,e}}(z) f_{\bar{\gamma}_{a,r}}(y)\,dydzdx. \tag{3.24}$$

By substituting (3.14) and (3.24) into (3.23) as well as some integral and algebraic calculations, we can obtain the expression of $\varphi(\alpha,\beta,R_s)$ as (3.19).

Considering the case of FR transmission mechanism (i.e., link selection policy without CSI feedback), based on formula (3.7), we have

$$P_{so}^{a,r} = \Pr\left\{R_a - C_{a,e} < R_s | \gamma_{a,r}[k] \geq \max\{\alpha, 2^{R_a} - 1, \frac{\alpha\gamma_{r,b}[k]}{\beta}\}\right\}$$
$$= \Pr\{R_a - C_{a,e} < R_s\} = \bar{\omega}(R_s). \tag{3.25}$$

When $\alpha \geq 2^{Ra}-1$, we can observe from Fig. 3.3 that $P_{so}^{r,b}$ in the FR case is the same as that in the AR case, so we have $P_{so}^{r,b} = \varphi(\alpha,\beta,R_s)$. When $\alpha < 2^{Ra}-1$, according to formula (3.8), we have

$$P_{so}^{r,b} = \Pr\{\Gamma_{r,b}[k]=1|I_k=1\} = \frac{\Pr\{\Gamma_{r,b}[k]=1, I_k=1\}}{\Pr\{I_k=1\}}, \tag{3.26}$$

where $\Pr\{I_k=1\}$ is given by equation (3.15) and

$$\begin{aligned}
&\Pr\{\Gamma_{r,b}[k]=1, I_k=1\} = \Pr\left\{\max\{\beta, \frac{\beta}{\alpha}\gamma_{a,r}[k]\} < \gamma_{r,b}[k] < 2^{R_s}(1+\gamma_{r,e}[k])-1\right\}\\
&+\Pr\left\{\alpha < \gamma_{a,r}[k] < 2^{R_a}-1, \beta < \gamma_{r,b}[k] < \frac{\beta}{\alpha}\gamma_{a,r}[k],\ \gamma_{r,b}[k] < 2^{R_s+C_{r,e}[k]}-1\right\}\\
&= (3.24) + \int_{\alpha}^{2^{R_a}-1}\left(\int_0^{\frac{\beta x+\alpha}{\alpha 2^{R_s}}-1}\int_\beta^{\frac{\beta x}{\alpha}} + \int_\beta^{2^{R_s}(1+z)-1}\int_{\frac{\beta x+\alpha}{\alpha 2^{R_s}}-1}^{\infty}\right)\\
&\quad f_{\bar{\gamma}_{r,b}}(y) f_{\bar{\gamma}_{r,e}}(z) f_{\bar{\gamma}_{a,r}}(x)dydzdx.
\end{aligned} \tag{3.27}$$

By substituting (3.15), (3.24) and (3.27) into (3.26) as well as conducting some integral calculations, we can obtain the expression of $\bar{\varphi}(\alpha$,β,$R_s)$ as (3.20). By substituting the above results into formula (3.9), P_{so} can be expressed as (3.16). ■

Based on Theorem III.1, we have the following corollary.

Corollary 1 *When $\frac{\gamma_{a,r}[k]}{\alpha} \gg \frac{\gamma_{r,b}[k]}{\beta}$, the E2E SOP is determined as*

$$P_{so} = \begin{cases} \frac{\gamma_{a,e}2^{R_s}}{\gamma_{a,r}+\gamma_{a,e}2^{R_s}} \exp\left(-\frac{\alpha+1-2^{R_s}}{\gamma_{a,e}2^{R_s}}\right), & \textit{for AR case}\\ 1-\bar{\omega}(R_s), & \textit{for FR case}\end{cases} \tag{3.28}$$

When $\frac{\gamma_{a,r}[k]}{\alpha} \ll \frac{\gamma_{r,b}[k]}{\beta}$, the E2E SOP for both AF and FR cases is determined as

$$P_{so} = \frac{\gamma_{r,e}2^{R_s}}{\gamma_{r,b}+\gamma_{r,e}2^{R_s}} \exp\left(-\frac{\beta+1-2^{R_s}}{\gamma_{r,e}2^{R_s}}\right) \tag{3.29}$$

where $\bar{\omega}(R_s)$ is expressed as (3.17).

3.3.2 Throughput and Secrecy Throughput

The system throughput $\varPhi$ and the secrecy throughput (ST) $\varPhi_S$ are defined as the long-term time-average on the number of messages (in units of bits/slot) that are delivered and ***securely delivered on both hops*** from Alice to Bob, respectively. They are of great significance since the throughput reflects the communication quality of service (QoS) of the system, while ST serves as an integrated measure for both the security and QoS performance.

We use $Q_r[k]$ to denote the amount of confidential data (in units of bits) stored in the buffer of Relay at the end of time slot k, then $\varPhi$ can be formulated as

$$\varPhi = \lim_{T\to\infty} \frac{1}{T} \sum_{k=1}^{T} (|I_k + \frac{1}{2}| - \frac{1}{2}) \cdot \min\{R_s, Q[k-1]\}. \tag{3.30}$$

Note that the E2E SOP refers to the probability that the event of secrecy outage happens on at least one of the two hops when a message is delivered from Alice to Bob. Therefore, $(1 - P_{so})$ is the probability that a message is securely delivered on both hops, and ST can be formulated as

$$\varPhi_S = \varPhi \cdot (1 - P_{so}). \tag{3.31}$$

Theorem III.2 (Throughput and Secrecy Throughput) *For a concerned cooperative network with the system models described in Section 3.1, we apply the link selection policies proposed in Section 3.2 for information transmission, then the system throughput $\varPhi$ is determined as*

$$\varPhi = \min\{P_A, P_R\} \cdot R_s \tag{3.32}$$

and the secrecy throughput $\varPhi_S$ is determined as

$$\varPhi_s = \min\{P_A, P_R\} \cdot R_s \cdot (1 - P_{so}), \tag{3.33}$$

where P_A, P_R and P_{so} are given by (3.10), (3.13) and (3.16), respectively.

Proof: In order to derive the closed-form expression for the system throughput, we analyze the queuing process in the buffer of Relay. It is notable that after decoding the signal from Alice, Relay only need to store the useful data, i.e., the confidential messages, in its buffer. As a result, the evolution of data stored in Relay's buffer at the next time slot can be characterized as

$$Q_r[k+1] = \begin{cases} Q_r[k] + R_s, & \text{Alice-to-Relay is selected} \\ \{Q_r[k] - R_s\}^+, & \text{Relay-to-Bob is selected} \\ Q_r[k], & \text{No link is selected} \end{cases} \tag{3.34}$$

where $\{x\}^+ = \max\{x, 0\}$.

By regarding R_s bits of confidential data as one *packet*, then the packet arrival process at the buffer of Relay is a Bernoulli process with arrival probability P_A, the packet service process at the buffer of Relay is also a Bernoulli process with service opportunity P_R. Therefore, the Relay can be characterized as a Bernoulli/Bernoulli queue [56].

Let π_i denote the probability that there are i packets stored in the buffer of Relay at the stationary state, then the stationary distribution of the number of packets stored in the buffer $\mathbf{\Pi} = [\pi_0, \pi_1, \cdots]$ can be determined as [56]

$$\pi_i = \begin{cases} \dfrac{1}{1-P_A} H^{-1}, & i = 0 \\ \dfrac{1}{1-P_A} \dfrac{\tau^i}{1-P_R} H^{-1}, & i \geq 1 \end{cases}$$

where $\tau = \dfrac{P_A(1-P_R)}{P_R(1-P_A)}$, and H is the normalization constant. Notice that $\mathbf{\Pi}{\cdot}\mathbf{1} = 1$, where $\mathbf{1}$ is a column vector with all elements being 1, we have

$$\pi_0 = \begin{cases} 0, & P_A \geq P_R \\ 1 - \dfrac{P_A}{P_R}. & P_A < P_R \end{cases} \tag{3.35}$$

The system throughput is the departure rate of the Bernoulli/Bernoulli/queue, thus it can be determined as

$$\mathit{\Phi} = P_R R_s \cdot (1 - \pi_0) = \min\{P_A, P_R\} \cdot R_s. \tag{3.36}$$

Then, the ST can be determined as

$$\mathit{\Phi}_s = \mathit{\Phi} \cdot (1 - P_{so}) = \min\{P_A, P_R\} \cdot R_s \cdot (1 - P_{so}). \tag{3.37}$$

■

Based on the results of Theorem III.2, we have the following corollary.

Corollary 2 *A necessary condition of the throughput $\mathit{\Phi}$ reaching its maximum is $P_A = P_R$, i.e., the Relay queue is at the edge of non-absorbing state.*

Proof: The proof is given in Appendix A.2. ■

Remark 2 *From Theorem III.2, we can find that: (1) The system throughput is heavily affected by the transmission chances of both Alice and Relay. Thus, when the channel qualities of the two hops are significantly different, i.e., $\gamma_{a,r} \gg \gamma_{r,b}$ or $\gamma_{a,r} \ll \gamma_{r,b}$, the values of the thresholds α and β need to be deliberately selected to ensure the transmission chances of both Alice and Relay, such that a non-zero system throughput can be guaranteed; (2) The secrecy throughput only counts for the messages that are securely delivered on both hops.".*

3.3.3 Performance Optimization

From the performance evaluation, we can find that the thresholds α and β as well as the confidential message rate R_s will determine the E2E SOP, system throughput and secrecy throughput. Moreover, it is worth noting that improving the transmission security usually comes with a cost of QoS (i.e., the system throughput) degradation [57–60]. Therefore, the design of α, β and R_s is of great significance to enable the system to meet various performance requirements and achieve optimal security-throughput tradeoffs.

To this end, in this section we address the following three fundamental problems. P1: Under the condition that a certain degree of transmission security is ensured, i.e., the E2E SOP does not exceed some threshold θ_{so}, what is the maximum throughput the system can achieve? P2: Under the condition that a certain degree of throughput is guaranteed, i.e., $\varPhi$ is no less than some threshold $\theta_{\varPhi}$, what is the minimum SOP can be achieved? In addition, since the secrecy throughput is an integrated metric for the transmission security and communication QoS, we also explore the following integrated performance optimization problem, i.e., P3: What is the maximum secrecy throughput the system can achieve? It should be pointed out that addressing these problems can reveal us important insights into the link policy design for coping with different demands of various practical applications.

With the help of the results of performance evaluation, problems P1, P2 and P3 can be mathematically formulated as the following optimization issues, respectively.

$$\begin{aligned} \text{P1:} \quad \max_{R_s,\alpha,\beta} \quad & \varPhi = \min\{P_A, P_R\} \cdot R_s && \text{(3.38a)} \\ \text{s.t.} \quad & P_{so} \leq \theta_{so}, && \text{(3.38b)} \\ & \min\{\alpha, \beta\} \geq 2^{R_s} - 1, && \text{(3.38c)} \\ & R_s > 0. && \text{(3.38d)} \end{aligned}$$

$$
\begin{aligned}
\text{P2:} \quad \min_{R_s,\alpha,\beta} \quad & P_{so} = 1-(1-P_{so}^{a,r})(1-P_{so}^{r,b}) && \text{(3.39a)}\\
\text{s.t.} \quad & \mathit{\Phi} \geq \theta_{\mathit{\Phi}}, && \text{(3.39b)}\\
& \min\{\alpha,\beta\} \geq 2^{R_s}-1 \geq 0, && \text{(3.39c)}
\end{aligned}
$$

$$
\begin{aligned}
\text{P3:} \quad \max_{R_s,\alpha,\beta} \quad & \mathit{\Phi}_s = \min\{P_A, P_R\} \cdot R_s \cdot (1-P_{so}) && \text{(3.40a)}\\
\text{s.t.} \quad & \min\{\alpha,\beta\} \geq 2^{R_s}-1 \geq 0. && \text{(3.40b)}
\end{aligned}
$$

Notice that problems P1 and P3 contain the form of "max − min", we can eliminate such a form by transforming the original problem into two sub-problems. We take problem P1 in AR case as an example. According to the expressions (3.11) and (3.12), we have $P_A \leq P_R$ for $\bar{\gamma}_{a,r}\beta \leq \bar{\gamma}_{r,b}\alpha$, and $P_A > P_R$ for $\bar{\gamma}_{a,r}\beta > \bar{\gamma}_{r,b}\alpha$. Thus, P1 is transformed into the following two sub-optimization problems:

$$
\begin{aligned}
\text{sub-P11:} \quad \max_{R_s,\alpha,\beta} \quad & \mathit{\Phi} = P_A R_s\\
\text{s.t.} \quad & P_{so} \leq \theta_{so},\\
& \min\{\alpha,\beta\} \geq 2^{R_s}-1 \geq 0,\\
& \bar{\gamma}_{a,r}\beta \leq \bar{\gamma}_{r,b}\alpha,
\end{aligned}
$$

and

$$
\begin{aligned}
\text{sub-P12:} \quad \max_{R_s,\alpha,\beta} \quad & \mathit{\Phi} = P_R R_s\\
\text{s.t.} \quad & P_{so} \leq \theta_{so},\\
& \min\{\alpha,\beta\} \geq 2^{R_s}-1 \geq 0,\\
& \bar{\gamma}_{a,r}\beta > \bar{\gamma}_{r,b}\alpha,
\end{aligned}
$$

The optimal solution of P1 can be obtained by comparing the maximum throughput of sub-P11 and sub-P12.

From the results of performance evaluation, we can see that the expressions of P_{so}, $\mathit{\Phi}$ and $\mathit{\Phi}_s$ are all in complicated forms and thus it is very difficult to obtain the analytical solutions for the optimization problems. Therefore, we develop an iterative search algorithm inspired by the Zoutendijk Method [61] to asymptotically approach the optimal solutions. Since maximizing $\mathit{\Phi}$ and $\mathit{\Phi}_s$ is equivalent to minimizing $-\mathit{\Phi}$ and $-\mathit{\Phi}_s$, respectively, we let our iterative search algorithm focus on the feasible descend directions of $-\mathit{\Phi}$ in P1 and $-\mathit{\Phi}_s$ in P3. Before introducing our algorithm, we need the following lemma.

Lemma 3 *Suppose that the feasible point $\mathbf{x}^{(n)} = (\alpha^{(n)}, \beta^{(n)}, {R_s}^{(n)})$ is obtained at the n^{th} iteration, finding the strictly feasible descent direction $\mathbf{d}^{(n)}$ at this point is equivalent to solving the following linear programming (LP) problem:*

$$\min_{\mathbf{d},\sigma<0} \quad \sigma \tag{3.43a}$$

$$\text{s.t.} \quad \mathbf{d}^T \nabla \Psi(\mathbf{x}^{(n)}) \leq \sigma, \tag{3.43b}$$

$$-\mathbf{d}^T \nabla g_i(\mathbf{x}^{(n)}) \leq \sigma, \tag{3.43c}$$

$$\mid \mathbf{d}_j \mid \leq 1, j = 1, 2, 3, \tag{3.43d}$$

where $\Psi(\mathbf{x})$ and $g_i(\mathbf{x})$ are the objective and constraint functions, respectively, $\mid \cdot \mid$ denotes the norm of a vector, T is the transpose symbol, ∇ is the gradient symbol, i is the effective constraint indicator which will be introduced in our algorithm, $\mathbf{d}_j$ ($j \in \{1, 2, 3\}$) denotes the element of $\mathbf{d}$ in the α, β and R_s directions, respectively.

Proof: The proof is given in Appendix A.3. ■

Based on Lemma 3, the optimal solution can be approximated by iteratively searching in the strictly feasible descent direction $\mathbf{d}$. Therefore, we propose the Link

Parameters Optimization Algorithm to solve the problems P1, P2 and P3, as summarized in Algorithm 3.

Algorithm 3 Link Parameters Optimization Algorithm

```
Initialization:
    Set the initial feasible point $\mathbf{x}^{(0)}$, $\epsilon_0 > 0$ and the convergence tolerance of objective function $\varepsilon > 0$, $0 \Longrightarrow N$ ;
Ensure:
    The optimal link selection parameters $\mathbf{x}^*$
Step 1: Determine the effective constraint indicator set: $I(\mathbf{x}^{(n)}, \epsilon_n) = \{| \; i \; | \; 0 \leq g_i(\mathbf{x}^{(n)}) \leq \epsilon_n\}$, then compute the gradient of objective function: $\nabla\Psi(\mathbf{x}^{(n)})$;
if $I(\mathbf{x}^{(n)}, \epsilon_n) = \varnothing$ and $\| \nabla\Psi(\mathbf{x}^{(n)}) \| \leq \varepsilon$ then
    stop iteration and $\mathbf{x}^* = \mathbf{x}^{(n)}$;
else if $\| \nabla\Psi(\mathbf{x}^{(n)}) \| > \varepsilon$ then
    set $-\nabla\Psi(\mathbf{x}^{(n)} = \mathbf{d}^{(n)}$ and $\sigma_{(n)} = -1$, then update iteration point: execute Procedure 1;
else
    find the feasible descend direction: goto Step 2;
end if
Step 2: Compute the linear programming problem (3.43), then return $\mathbf{d}^{(n)}, \sigma_n$;
if $\sigma_n = 0$ and $\epsilon_n < \varepsilon$ then
    stop iteration and $\mathbf{x}^* = \mathbf{x}^{(n)}$;
else
    update $\epsilon_n = \frac{\epsilon_n}{2}$, goto Step 1;
end if
```

Notice that the condition $g_i(\mathbf{x}^{(n)}) \leq \epsilon_n$ in Step 1 avoids the sawtooth [62], which ensures the iterative algorithm can converge to the Fritz-John point. A special case would occur when solving the LP problem (3.43), i.e., the effective constraint set is a null set but $\nabla\Psi$ does not satisfy the convergence condition. To this end, we apply Procedure 1 to find a new feasible point.

It is notable that Algorithm 3 transforms the nonlinear problem of finding feasible points into a linear programming problem (41). Thus, the complexity of Algorithm 3 is mainly decided by the procedure for solving the linear programming. Currently, there are many mature and effective methods for solving the linear programming problems, such as simplex method, interior point method, etc, and it has been demonstrated that the complexity of these methods does not exceed the problem dimension

Procedure 1 Update iteration point

```
1: Find a suitable step size: for $i \notin I(\mathbf{x}^{(n)}, \epsilon_n)$, first compute $a_{max} = \min\{t_i | (g_i(\mathbf{x}^{(n)}) + t_i \mathbf{d}^{(n)}) = 0, t_i > 0\}$, then obtain $a_n$ by solving:
       $\begin{cases} \min \Psi(\mathbf{x}^{(n)} + a_n \mathbf{d}^{(n)}) \\ 0 \le a_n \le a_{max} \end{cases}$
2: Update the iteration point: set $\mathbf{x}^{(n+1)} = \mathbf{x}^{(n)} + a_n \mathbf{d}^{(n)}$;
3: if $\| \mathbf{x}^{(n+1)} - \mathbf{x}^{(n)} \| < \varepsilon$ then
4:     stop iteration and $\mathbf{x}^* = \mathbf{x}^{(n+1)}$;
5: else
6:     update $\epsilon_n = \epsilon_n$ for $\epsilon_n \le -\sigma_n$, $\epsilon_n = \frac{\epsilon_n}{2}$ for $\epsilon_n > -\sigma_n, n = n + 1$, goto Step 1.
7: end if
```

and a $\log(1/\epsilon)$ time [63]. The problems P1, P2 and P3 are three-dimensional. Therefore, the complexity of Algorithm 3 can be determined as $O(log(1/\epsilon))$.

3.4 Simulation Results and Discussions

In this section, we first conduct simulations to validate our theoretical analysis in terms of the E2E SOP, system throughput and secrecy throughput. Based on the theoretical results, we then provide discussions for the security-QoS tradeoffs. Finally, we compare the performance of the proposed link selection policies with another typical one to demonstrate their efficiencies.

3.4.1 Simulation Settings

For the validation of theoretical performance evaluation, a dedicated C++ simulator was developed to simulate the message delivery processes under our link selection policies, which is available at [64]. With the help of the simulator, we conduct extensive simulations to calculate the simulated results of E2E SOP, system throughput and secrecy throughput. The duration of each task of simulation is set to be 1×10^8 time slots and our link selection policies are performed once per slot. In addition, we set all the noise variance and the transmission power to be 1, and the average channel

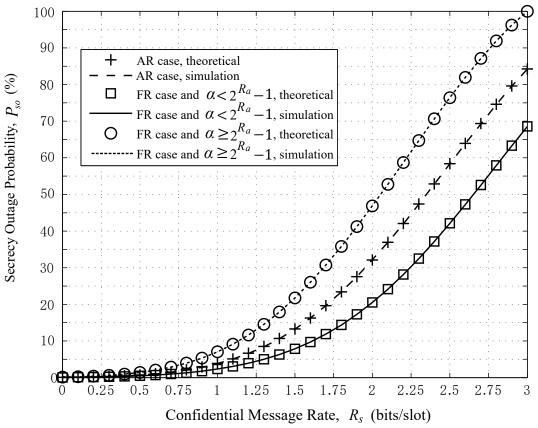


Figure 3.4: E2E SOP P_{so} vs. confidential message rate R_s. $\alpha = 7.0$, $\beta = 8.0$, $R_a = 3.0$ bits/slot for $\alpha \geq 2^{R_a} - 1$, $R_a = 4.0$ bits/slot.

gain of links as $\Omega_{a,r} = 5\text{dB}$, $\Omega_{r,b} = 10\text{dB}$, $\Omega_{a,e} = 0\text{dB}$, $\Omega_{r,e} = 2\text{dB}$. Readers can also flexibly perform our C++ simulator with any other desired parameter settings.

We count the number of bits received by Bob and the number of bits eavesdropped by Eve in a task of simulation as N_0 and N_1, respectively. Then, the simulated SOP is calculated as

$$\text{Simulated SOP} = 100\% \times \frac{N_1}{N_0}. \tag{3.44}$$

The simulated throughput and secrecy throughput are calculated as

$$\text{Simulated throughput} = \frac{N_0}{10^8}, \tag{3.45}$$

$$\text{Simulated secrecy throughput} = \frac{N_0 - N_1}{10^8}. \tag{3.46}$$

3.4.2 Validation

We first summarize in Fig. 3.4 the theoretical and simulation results of E2E SOP in both AR and FR cases, where we set $\alpha = 7.0$, $\beta = 8.0$, $R_a = 3.0$ bits/slot for $\alpha \geq 2^{R_a} - 1$ and $R_a = 4.0$ bits/slot for $\alpha < 2^{R_a} - 1$. Fig. 3.4 shows clearly that the simulation results match well with the corresponding theoretical curves for all the

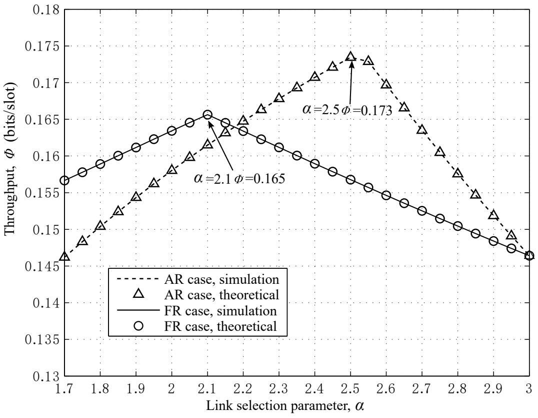


Figure 3.5: Throughput Φ vs. threshold α. $\beta = 8.0$, $R_s = 0.5$ bits/slot, $R_a = 2.0$ bits/slot.

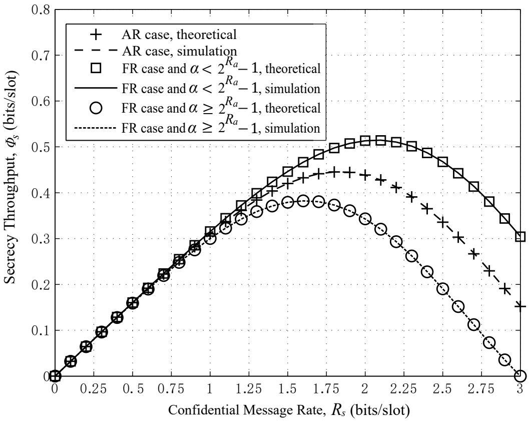
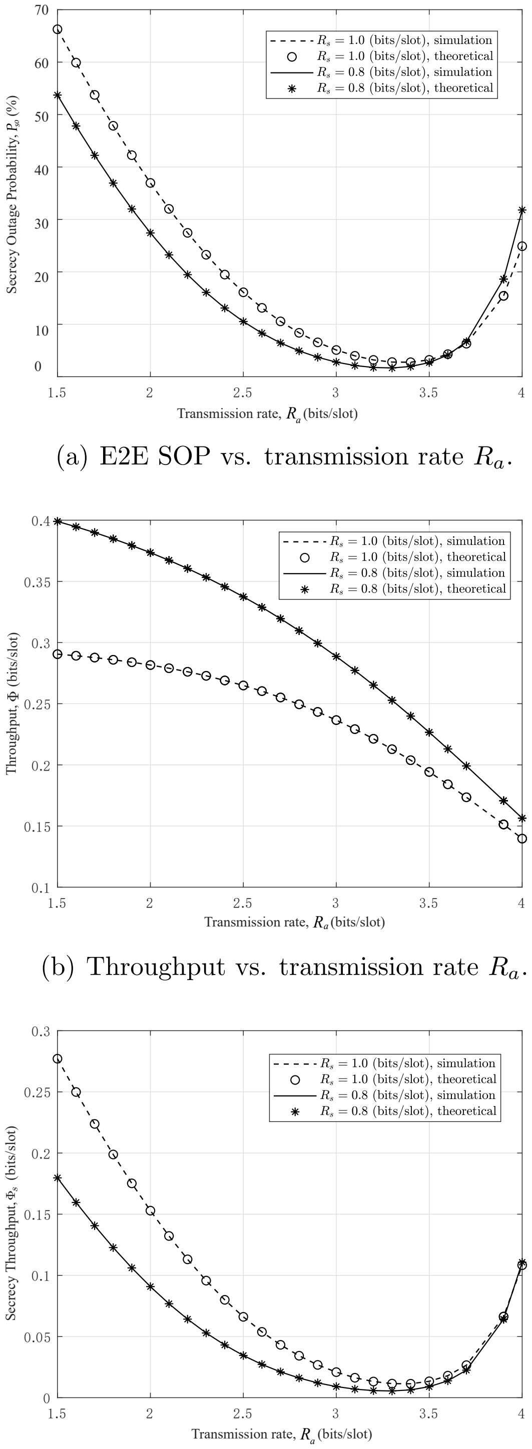


Figure 3.6: Secrecy throughput Φ_s vs. confidential message rate R_s. $\alpha = 7.0$, $\beta = 8.0$, $R_a = 3.0$ bits/slot for $\alpha \geq 2^{R_a} - 1$, $R_a = 4.0$ bits/slot for $\alpha < 2^{R_a} - 1$.

cases considered here, indicating that our theoretical performance analysis is highly efficient to evaluate the E2E SOP of the proposed link selection policies. We can also observe from Fig. 3.4 that the E2E SOP increases monotonically with the increase of confidential message rate R_s, and a larger fixed codeword rate R_a can achieve a lower E2E SOP for the FR case.

We then present the plot of theoretical/simulated throughput versus α in Fig. 3.5, here we set $\beta = 8.0$, $R_s = 0.5$ bits/slot and $R_a = 2.0$ bits/slot. Fig. 3.5 shows that the simulated throughput in both cases matches nicely with the theoretical ones, which



(a) E2E SOP vs. transmission rate R_a.

(b) Throughput vs. transmission rate R_a.

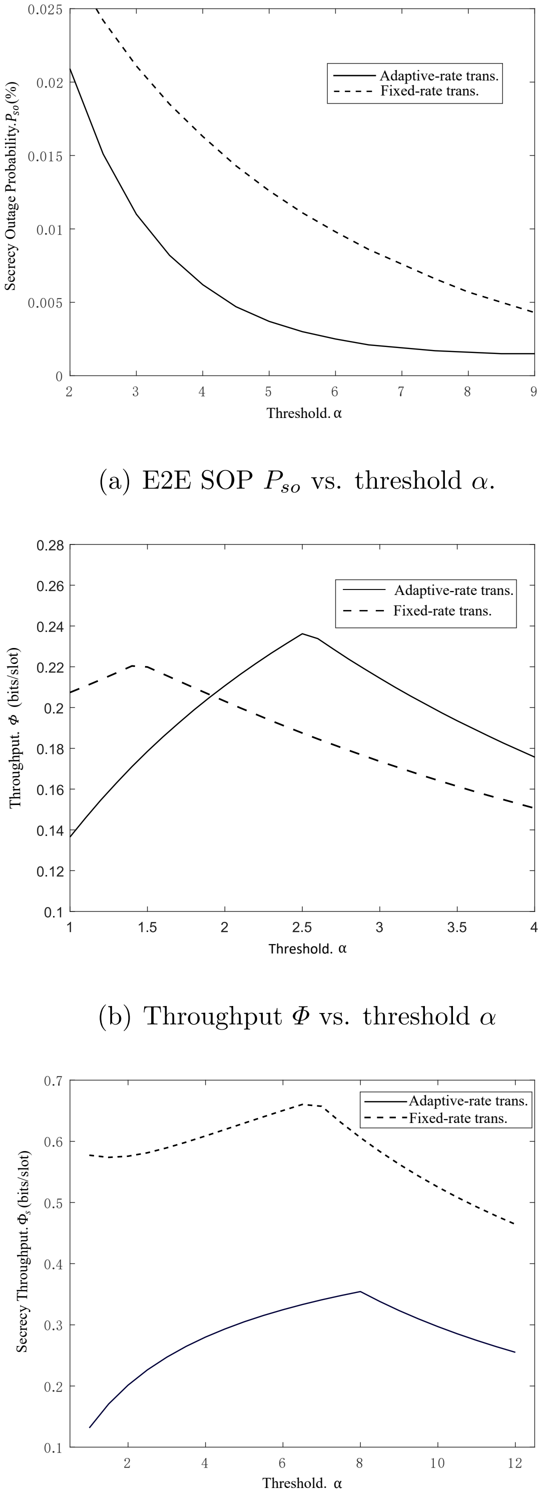
(c) Secrecy throughput vs. transmission rate R_a.

Figure 3.7: Impacts of transmission rate R_a on system performance. $\Omega_{a,r} = \Omega_{r,b} =$ 15dB, $\Omega_{a,e} = 0$dB, $\Omega_{r,e} = 2$dB, $\alpha = 6.0$, $\beta = 8.0$.

demonstrates that our theoretical performance evaluation for the system throughput of the proposed link selection policies is also highly efficient. From Fig. 3.5, it can be observed that when $\alpha = 2.5$ and $\alpha = 2.1$, the system throughput $\varPhi$ in AR case and FR case reaches its peak, i.e., 0.165 and 0.173, respectively. It can be verified by numerical calculation that $P_A = P_R$ holds at the throughput peak, which agrees with the conclusion of Corollary 2.

We further draw Fig. 3.6 to present the theoretical and simulation results of secrecy throughput in both AR and FR cases, where we set $\alpha = 7.0$, $\beta = 8.0$, $R_a = 3.0$ bits/slot for $\alpha \geq 2^{R_a} - 1$ and $R_a = 4.0$ bits/slot for $\alpha < 2^{R_a} - 1$. We can see from Fig. 3.6 that the simulation results match well with the corresponding theoretical curves for all the cases considered here, verifying that our theoretical performance analysis is also highly efficient to capture the secrecy throughput behaviors of the proposed link selection policies. An interesting observation from Fig. 3.6 is that as R_s increases the secrecy throughput first increases to a maximal value and then decreases. This is due to the reason that the secrecy throughput is an integrated measure for both the security and QoS performance, and the effects of R_s on secrecy throughput are two folds. On one hand, a larger R_s leads to a larger throughput; on the other hand, a larger R_s results in a higher SOP. It implies that the tradeoff between the throughput and E2E SOP leads to the unimodal behavior of secrecy throughput, and we can optimize the system performance to satisfy various requirements for transmission security and communication QoS by design appropriate parameters of link selection policies.

We finally plot Fig. 3.7 to show the simulation and theoretical results of the system performance with the variation of the codeword rate R_a in the FR case, where we set $\Omega_{a,r} = \Omega_{r,b} = 15$dB, $\Omega_{a,e} = 0$dB, $\Omega_{r,e} = 2$dB, $\alpha = 6.0$, $\beta = 8.0$. Fig. 3.7 shows that the theoretical curves of all the performance metrics match well with the corresponding simulation results, which validates the efficiency of our analysis framework. We can observe from Fig. 3.7 that as R_a increases, the system throughput monotonically decreases, while the SOP and secrecy throughput decrease first and then increase.



(a) E2E SOP P_{so} vs. threshold α.

(b) Throughput $\mathit{\Phi}$ vs. threshold α

(c) Secrecy throughput $\mathit{\Phi}_s$ vs. threshold α

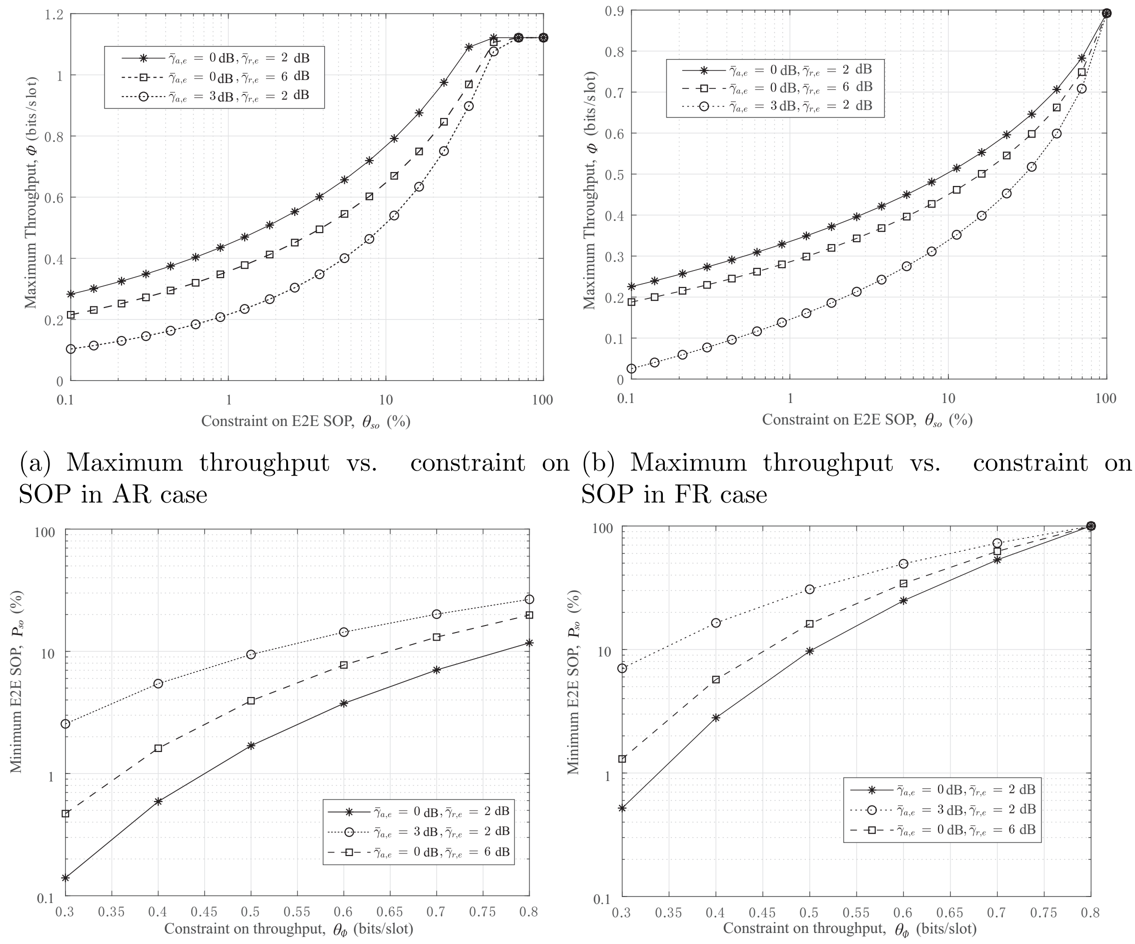
Figure 3.8: Impacts of thresholds on system performance. $\Omega_{ar} = 5$dB, $\Omega_{rb} = 15$dB, $R_s = 0.5$ bits/slot, $R_a = 3.0$ bits/slot for (a) and (b); $\Omega_{ar} = \Omega_{rb} = 15$dB, $R_s = 3.0$ bits/slot, $R_a = 4.0$ bits/slot for (c).

3.4.3 Performance Discussion

Based on the validation of our theoretical performance evaluation, we further develop a MATLAB simulator [64] to obtain various numerical results for the system performance.

We plot Fig. 3.8 to show the impacts of threshold α on the system performance. Fig. 3.8(a) shows that the SOP monotonically decreases as α increases, which indicates that to achieve a good security performance for the system, we should design a large value of the threshold in the link selection policy. We can observe from Fig. 3.8(b) and 3.8(c) that as α increases, both the system throughput and secrecy throughput first increase and then decrease. These behaviors demonstrate that the threshold has great impacts on the system performance, so the threshold can be flexibly designed to enable the system to meet various performance requirements. Since the performance behavior with the variation of β is similar to that with the variation of α, we omit the details here.

We summarize in Fig. 3.9 and Fig. 3.10 the optimal values of problems P1, P2 and P3 in AR case and FR case, respectively, where we set $\bar{\gamma}_{a,r} = 10$dB, $\bar{\gamma}_{r,b} = 15$dB, and $R_a = 4$ bits/slot. The horizontal axis of Fig. 3.9(a) and Fig. 3.9(b) as well as the vertical axis of Fig. 3.9(c) and Fig. 3.9(d) are based on the logarithmic coordinates, and three different settings of the qualities of eavesdropping channels are considered there. Fig. 3.9(a) and Fig. 3.9(b) show how the maximum throughput the system can achieve varies with the constraint on SOP, while Fig. 3.9(c) and Fig. 3.9(d) show how the minimum SOP can be guaranteed varies with the constraint on system throughput. We can observe that as θ_{so} increases, i.e., the constraint on SOP is loosed, the system can achieve a larger throughput; while as θ_{Φ} increases, i.e., the constraint on throughput is loosed, a lower SOP can be ensured. It indicates that important tradeoffs exist between the aspect of transmission security and the aspect of communication QoS, improving the performance for one aspect will incur a cost of



(a) Maximum throughput vs. constraint on SOP in AR case

(b) Maximum throughput vs. constraint on SOP in FR case

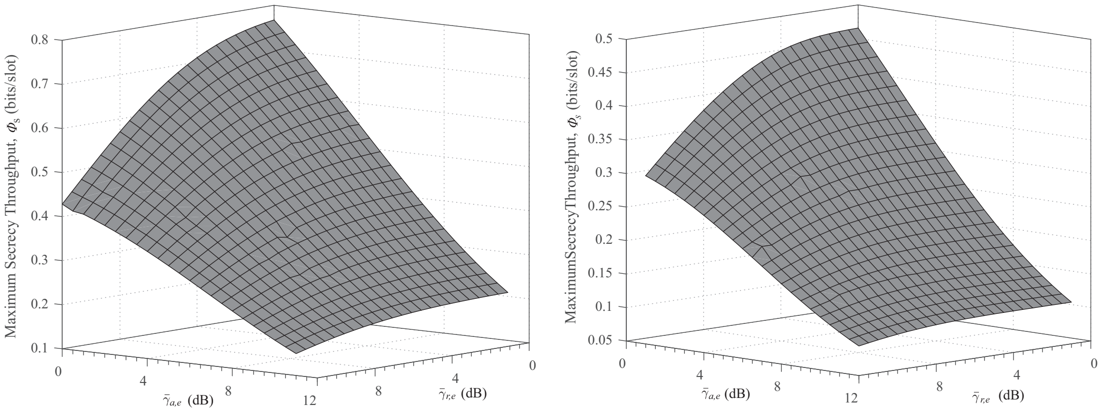
(c) Minimum SOP vs. constraint on throughput in AR case

(d) Minimum SOP vs. constraint on throughput in FR case

Figure 3.9: Optimal values of problems P1 and P2 under different eavesdropping channel qualities. $\bar{\gamma}_{a,r} = 10$dB, $\bar{\gamma}_{r,b} = 15$dB, $R_a = 4.0$bits/slot.

performance degradation of another aspect. Therefore, our theoretical results provide useful guidelines for the design of link selection policies to satisfy various practical performance requirements.

Fig. 3.10(a) and Fig. 3.10(b) present the maximum secrecy throughput with the variations of eavesdropping channel qualities $\bar{\gamma}_{a,e}$ and $\bar{\gamma}_{r,e}$. We can see that as $\bar{\gamma}_{a,e}$ and/or $\bar{\gamma}_{r,e}$ increase, i.e., the situation of transmission being eavesdropped becomes more serious, the maximum achievable secrecy throughput deteriorates. An interesting observation from Fig. 3.10(a) and Fig. 3.10(b) is that the deterioration rate of



(a) Maximum secrecy throughput in AR case. (b) Maximum secrecy throughput in FR case.

Figure 3.10: Optimal values of problems P3 under different eavesdropping channel qualities. $\bar{\gamma}_{a,r} = 10$dB, $\bar{\gamma}_{r,b} = 15$dB, $R_a = 4.0$bits/slot.

secrecy throughput with the growth of $\bar{\gamma}_{a,e}$ is faster than that with the growth of $\bar{\gamma}_{r,e}$, which indicates that compared with the eavesdropping of the second hop, the eavesdropping of the first hop has a greater impact on the performance of such cooperative networks.

Comparing the results in Fig. 3.9 and Fig. 3.10, we can further find that the performance tradeoffs in AR case are better than those in FR case. For example, under the same settings, the system in AR case can achieve a larger throughput or a lower SOP than that in FR case. This is due to the benefits brought by the CSI feedback, which provides the policy with more information to determine the link selection and codeword rate more appropriately, at the cost of the increase of operation complexity and system overhead.

Finally, we summarize in Table 3.1 the optimal parameter settings for the problem P1 in AR case, corresponding to the points in Fig. 3.9(a). From Table 3.1 we can see that for a larger $\bar{\gamma}_{a,e}$ or $\bar{\gamma}_{r,e}$, we usually need to set a larger α, a larger β and a smaller R_s to guarantee the SOP does not exceed the pre-specified threshold while maximizing the system throughput. Readers can kindly utilize our MATLAB simulator to explore the optimal parameter settings for other optimization problems in both AR case and

Table 3.1: Optimal Parameter Settings for P1 in AR Case

Channel Qualities	**Optimal Parameters**	**Constraint on E2E SOP, Θ_{so}**							
		0.1%	0.3%	0.89%	2.64%	7.85%	23.36%	69.52%	100%
$\bar{\gamma}_{ae} = 0\,\text{dB}$ $\bar{\gamma}_{re} = 2\,\text{dB}$	α	12.1684	10.8700	9.5293	8.1121	6.5709	4.7549	6.5843	6.5843
	β	38.4799	34.3740	30.1345	25.6526	20.779	15.0362	20.821	20.821
	R_s	1.1203	1.2437	1.3979	1.5990	1.8740	2.2764	2.9230	2.9230
$\bar{\gamma}_{ae} = 3\,\text{dB}$ $\bar{\gamma}_{re} = 2\,\text{dB}$	α	18.3808	16.0100	13.5998	11.0788	8.3476	5.3339	6.5843	6.5843
	β	58.1252	50.628	43.0063	35.0343	26.3975	16.8673	20.8212	20.821
	R_s	0.7067	0.8025	0.9282	1.1026	1.3638	1.8111	2.9230	2.9230
$\bar{\gamma}_{ae} = 0\,\text{dB}$ $\bar{\gamma}_{re} = 6\,\text{dB}$	α	13.9589	12.4543	10.9217	9.3109	7.5403	5.3997	6.5843	6.5843
	β	44.1419	39.384	34.5375	29.4437	23.8445	17.0755	20.821	20.821
	R_s	0.9922	1.1051	1.2451	1.4264	1.6746	2.0499	2.9230	2.9230

FR case, we omit the details here.

3.4.4 Comparison Results

In order to demonstrate the efficiency of our proposed link selection policies on ensuring secure communication for two-hop cooperative networks, we further present extensive numerical results for the performance comparison with the typical policies: Max-Link policy [65], Max-Ratio policy [36] and the policy in [32] in AR case and FR case, respectively. Specially, in order to explore the effect of buffer state on the link design and performance analysis, we incorporate the buffer state into the proposed policies and consider the following Algorithm 4 termed as WBS-LSP.

It is worth noting that the policies in [32] always conduct data transmission (either Alice-to-Relay or Relay-to-Bob) in all time slots, while our policies only conduct data transmission when there is a good opportunity (i.e., either of the links is in a good condition). For clarity of exposition, we term our proposed policies as OT-LSP (opportunistic transmission link selection policies), and the policies in [32] as AT-LSP (always transmission link selection policies) hereinafter. Unless otherwise specified, we set $\bar{\gamma}_{a,r} = 10$dB, $\bar{\gamma}_{r,b} = 15$dB, $\bar{\gamma}_{a,e} = 0$dB, $\bar{\gamma}_{r,e} = 2$dB and $R_a = 3$ bits/slot.

1) Performance Comparison in AR Case

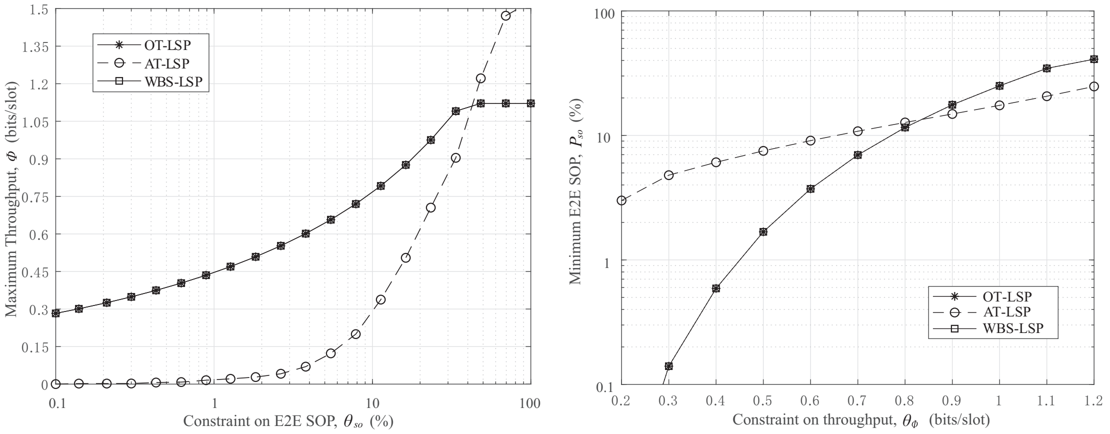
We summarize the comparison results of the tradeoffs between system throughput

Algorithm 4 Buffer State-aware Link Selection Algorithm

```
Require:
    Instantaneous CSIs of legitimate links, confidential message rate $R_s$, transmission rate $R_a$ ($R_a \geq R_s$), thresholds $\alpha$ and $\beta$ and buffer occupancy state information;
Ensure:
    Link decision indicator $I_k$, $k \in \{1, 2, \cdots, T\}$;
for $k = 1$; $k \leq T$; $k++$ do
    Check the buffer occupancy state;
    if The buffer is empty then
        Calculate $\gamma_{a,r}[k]$ based on the instantaneous CSIs;
        if $\gamma_{a,r}[k] \geq \alpha$ for AR case ($\gamma_{a,r}[k] \geq \max(\alpha, 2^{R_a} - 1)$ for FR case) then
            $I_k = 0$;
        else
            $I_k = -1$;
        end if
    else
        Apply Algorithm 1 for AR case or apply Algorithm 2 for FR case;
    end if
end for
```

and E2E SOP in Fig. 3.11. From Fig. 3.11(a), we can observe clearly that OT-LSP outperforms AT-LSP in improving the throughput performance when θ_{so} is less than 0.42, but it is inferior to the latter as we further relax the constraint on SOP. A similar behavior can be seen in Fig. 3.11(b), where the system can achieve a lower SOP with OT-LSP until θ_{Φ} is more than 0.8 bits/slot. Such behaviors are due to the reason that our primary aim is to achieve secure communication, improving the level of transmission security inevitably leads to a degradation of communication QoS, thus the proposed OT-LSP sacrifices some parts of communication QoS to realize a high security performance. Otherwise, we can also observe that the value of maximum throughput Φ first increases and then keeps constant as θ_{so} gradually increases. That is because that, as θ_{so} increase, the feasible region of problem (3.38) increases, and ϕ increases. But when θ_{so} increases to 0.6952, R_s, α and β are optimal and ϕ reaches its peak. After that, even θ_{so} increases, the value of maximum throughput keeps constant.

We then provide Fig. 3.12 to show the behaviors of maximum secrecy throughput



(a) Maximum throughput vs. constraint on SOP.

(b) Minimum SOP vs. constraint on throughput.

Figure 3.11: Comparisons of the tradeoffs between throughput and E2E SOP in AR case.

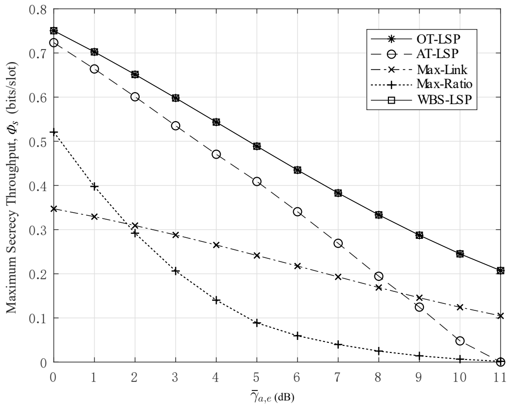
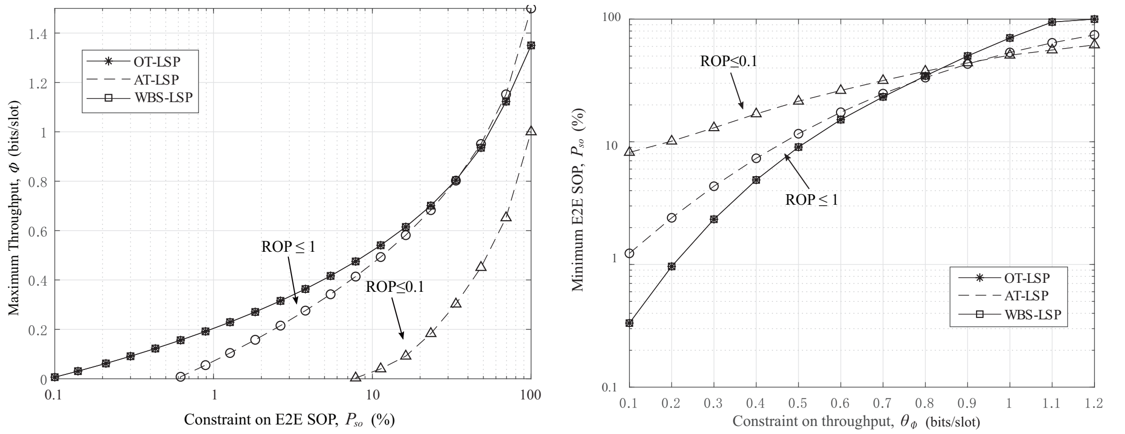


Figure 3.12: Comparison in terms of maximum secrecy throughput in AR case.

the system can achieve with OT-LSP, Max-Link, Max-Ratio and AT-LSP. We can see from Fig. 3.12 clearly that the maximum achievable secrecy throughput with OT-LSP is always superior to that with the other policies, indicating that the proposed link selection policy in AR case is efficient for achieving secure communication in two-hop cooperative networks. A more careful observation is that as $\bar{\gamma}_{a,e}$ increases, the performance gap between the two policies gradually increases, which implies that as the eavesdropping situation becomes more serious, our link selection policy can bring a greater improvement for secrecy throughput.



(a) Maximum throughput vs. constraint on SOP.

(b) Minimum SOP vs. constraint on throughput.

Figure 3.13: Comparisons of the tradeoffs between throughput and E2E SOP in FR case.

From Fig. 3.11 and Fig. 3.12, we can see that all results with WBS-LSP matches nicely with the proposed policy in AR case. It is because that the backlogged source leads to few empty buffer states. Even we don't consider the buffer state in this work, the proposed policies are still effective for security-QoS tradeoffs for AR case.

2) Performance Comparison in FR Case

Regarding the FR case, it is worth noting that the event of channel outage (i.e., the event that the transmission rate exceeds the channel capacity) can be completely avoided with OT-LSP but is inevitable with AT-LSP. Therefore, for the sake of fairness, we provide comparison results under two typical restrictions for channel outage probability (termed ROP in [32]) of AT-LSP, i.e., ROP ≤ 0.1 which approaches the effect of OT-LSP, and ROP ≤ 1 which means there is no restriction on channel outage probability. In Fig. 3.13, the performance of OT-LSP and AT-LSP is compared in terms of the tradeoffs between throughput and E2E SOP. From Fig. 3.13(a) we can see that the system throughput with OT-LSP is higher than that with AT-LSP for ROP ≤ 0.1, and such a behavior generally holds even for ROP ≤ 1. Similarly, Fig. 3.13(b) shows that when $\theta_{\Phi} \leq 0.5$ bits/slot, the minimum E2E SOP declines by an order of magnitude with OT-LSP compared with AT-LSP. For ROP ≤ 1, OT-LSP

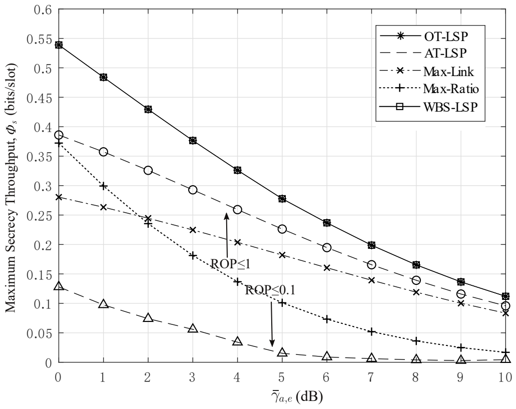


Figure 3.14: Comparison in terms of maximum secrecy throughput in FR case.

still outperforms AT-LSP until θ_{Φ} exceeds 0.8 bits/slot.

Finally, we summarize the performance of secrecy throughput in Fig. 3.14. This figure shows clearly that the maximum secrecy throughput can be achieved by the system with OT-LSP is superior to that with Max-Link, Max-Ratio, and also is superior to that with AT-LSP for both ROP ≤ 0.1 and ROP ≤ 1. In particular, for ROP ≤ 0.1, i.e., AT-LSP will approach the effect of OT-LSP on channel outage, OT-LSP can make a great improvement for secrecy throughput. All above comparison results indicate that the proposed link selection policy can ensure secure communication efficiently while avoiding the channel outage.

Similar with the AR case, we can see that the numerical results with WBS-LSP still match with ones with the proposed policy from Fig. 3.13 and Fig. 3.14. It indicate the proposed policy is still effective for security-QoS tradeoffs for FR case. Otherwise, readers can kindly utilize our MATLAB simulator to simulate the communication process and investigate how many the number of time slots in which the buffer is empty state, we omit the details here.

3.5 Summary

This chapter proposed two secure communication protocols for two-hop buffer-aided relaying systems. The theoretical analysis of the E2E SOP, system throughput and secrecy throughput were conducted to model the communication QoS and security performance of the proposed policies. Some fundamental optimization issues were further explored to provide insights into the performance tradeoffs. Extensive simulation and numerical results indicate the proposed policies can efficiently improve the transmission security and satisfy various system performance requirements by optimizing the policy parameters. It is expected that the results in this study can pave the way for the design of communication protocol to achieve secure communication in more complicated wireless networks. Notice that, in this work, we only consider that the confidential message rate is fixed. Thus, a future direction is to apply the dynamic confidential message rate to further improve the performance in buffer-aided relaying systems. Furthermore, we only provide simulation results for the link selection scheme with the consideration of buffer state. Therefore, in our future work we will further investigate how to theoretically evaluate the corresponding system performance. Another appealing research direction is to investigate the design of secure communication protocol and the performance analysis under multiple relay scenarios.

CHAPTER IV

Security/Delay-Aware Communication Protocol for Buffer-Aided Relaying Systems

This chapter investigates the security/delay-aware communication in a wireless relaying system, where the packet lifetime is limited, multiple buffer-aided relays help the source forward packets to the destination, and a passive eavesdropper attempts to wiretap the transmissions over both hops. To guarantee the end-to-end transmission security and timeliness in the network, we design a novel communication protocol that grants transmission nodes different priorities for packet delivery based on the wireless channel state, real-time buffer state, and packet delay requirement. For performance evaluation of the proposed protocol, we then develop a Markov chain-based theoretical framework to fully characterize the packet occupancy process in the relay buffers. With the help of this framework, we further derive under two typical fading channel cases the closed-form expressions for three fundamental system performance metrics, namely reliable outage probability, packet discarding probability and achievable secrecy throughput. Finally, we present extensive simulation and numerical results to validate our theoretical results, as well as to demonstrate the efficiency of the proposed protocol for ensuring secure and timely communication in the buffer-aided relaying system.

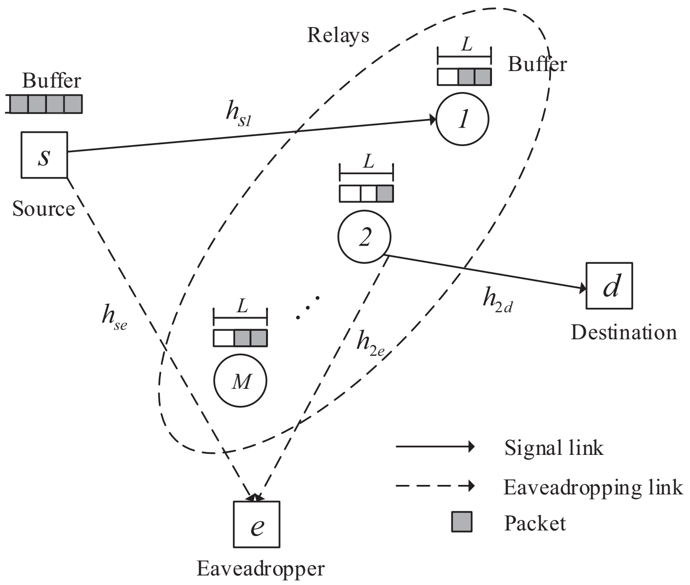


Figure 4.1: System model.

4.1 System Model and Assumptions

We consider a buffer-aided relaying system as shown in Fig. 4.1, which is composed of a source node s, multiple buffer-aided relay nodes, a destination node d and an eavesdropping node e. The number of relays is M and the set of relays are denoted as $\mathcal{M} = \{1, 2, \ldots, M\}$. There is no direct link from s to d so that the data of s can be delivered to d only via relays. The transmitted data is counted in packets. Node s has an infinite buffer for storing the external packets, while each relay node $m \in \mathcal{M}$ has a finite buffer of L packets. We assume that all nodes are equipped with a single antenna and operate in the half-duplex mode, and all the buffer queues follow the First-In-First-Out (FIFO) discipline.

We consider the eavesdropper e can wiretap the transmission over both hops. When forwarding a packet, each relay adopts the randomize-and-forward decoding strategy such that the eavesdropper cannot perform the maximal-ratio combining to process the received signals of the two hops [52]. The transmission time is split into successive slots with equal duration, and each packet is assumed to own a lifetime of τ

time slots. Moreover, we adopt the non-selective Rayleigh block fading channel model where the channel coefficients of all links are constant during one time slot but change independently from one time slot to another. We use $h_{i,j}[n]$ to denote the complex-valued fading coefficient of a channel from transmitter i to receiver j at time slot n ($i \in \{s\} \bigcup \mathcal{M}$, $j \in \{d, e\} \bigcup \mathcal{M}$, $i \neq j$), and the channel gain $g_{i,j} = |h_{i,j}[n]|^2$ follows the exponential distribution with mean $\Omega_{i,j}$. We assume that the CSI associated with a legitimate receiver is perfectly available, while the instantaneous CSI associated with the eavesdropper is unavailable but the channel distribution information (i.e., $\Omega_{s,e}$ and $\Omega_{m,e}$) is available. The additive white Gaussian noise at node j is denoted as n_j with variance δ_j.

To improve the transmission security and timeliness of the system, our communication protocol (as elaborated in Section 4.2) can employ an idle relay as a jammer to disrupt the received signal at the eavesdropper. Meanwhile, all relays adopt the technique of successive interference cancellation (SIC) but have different SIC capabilities. Let β_m ($0 \leq \beta_m \leq 1$) denote the SIC factor of relay m, e.g., $\beta_m = 0$ represents the perfect SIC and $\beta_m = 1$ indicates m cannot use SIC. When node i transmits a signal x_i to node j, the received signals y_j at node j and y_e at the eavesdropper e can be respectively expressed as

$$y_j = \begin{cases} \sqrt{P_i} h_{i,j} x_i + n_j, & \text{no relay is selected as a jammer,} \\ \sqrt{P_i} h_{i,j} x_i + \sqrt{\beta_j P_k} h_{k,j} x_k + n_j, & \text{relay } k \text{ is selected as a jammer.} \end{cases} \tag{4.1}$$

$$y_e = \begin{cases} \sqrt{P_i} h_{i,e} x_i + n_e, & \text{no relay is selected as a jammer,} \\ \sqrt{P_i} h_{i,e} x_i + \sqrt{P_k} h_{k,e} x_k + n_e, & \text{relay } k \text{ is selected as a jammer.} \end{cases} \tag{4.2}$$

where P_i is the transmission power of node i, P_k and x_k are the jamming power and jamming signal of relay k, respectively.

4.2 Security/Delay-Aware Communication Protocol Design

In this section, we first present the necessary condition of the secure transmission, and then combine it with the packet occupancy state in the relay buffer as well as the packet delivery delay information to design a novel communication protocol for the concerned system.

To ensure the secrecy of transmitted packets, the transmitters employ the eminent Wyner's encoding scheme [14]. When conducting transmission, a transmitter chooses two rates, one is the codeword rate R_t, another is the confidential data rate R_s. Since we can only obtain the statistical information of eavesdropping channels, the secrecy outage [17, 66] (i.e., the event that the transmission rate redundancy $R_t - R_s$ is less than the channel capacity of wiretap channel) would occur, which means existing information leakage to the eavesdropper. Fortunately, we can guarantee information leakage under a certain level by selecting a favorable relay. For the extreme situation when all links are in low channel quality, we can select an advisable relay as a cooperative jammer to increase the transmission opportunity and reduce the data waiting time. Overall, these results are summarized as the following proposition.

Proposition 1 *To ensure the secrecy outage probability (SOP) P_{so} is less than a given threshold P_{up} (i.e., $P_{so} \leq P_{up}$), if no relay is selected as a jammer the channel gain of the transmission link $s \to m$ or $m \to d$ must satisfy the following condition*

$$g_{s,m}[n] \geq \theta_s \quad \textit{and} \quad g_{m,d}[n] \geq \theta_m, \tag{4.3}$$

where $\theta_s = -2^{-R_s}\Omega_{s,e} \ln P_{up}$ and $\theta_m = -2^{-R_s}\Omega_{m,e} \ln P_{up}$. If relay k is selected as a jammer, the channel gains of the transmission and jamming links $s \to m$, $m \to k$ or $m \to d$, $k \to d$ must satisfy

$$g_{s,m}[n] \geq g_{k,m}[n]\Xi_{sk}^{m} \quad \textit{and} \quad g_{m,d}[n] \geq g_{k,d}[n]\Xi_{mk}^{d}, \tag{4.4}$$

where $\Xi_{sk}^{m} = 2^{R_s}\beta_m\Omega_{s,e}(1-P_{up})/(P_{up}\Omega_{k,e})$, $\Xi_{mk}^{d} = 2^{R_s}\beta_d\Omega_{m,e}(1-P_{up})/(P_{up}\Omega_{k,e})$, *and* R_s *is the intended secrecy rate.*

Proof: The proof is given in Appendix B.1. ■

In each time slot, we should first find out the link sets of the first and second hop satisfying the condition (4.3), which are denoted as $\mathbb{D}_1^R$ and $\mathbb{D}_2^R$, respectively. We group all events into two cases, i.e., case 1: $\mathbb{D}_1^R \notin \emptyset$ or $\mathbb{D}_2^R \notin \emptyset$, and case 2: $\mathbb{D}_1^R \in \emptyset$ and $\mathbb{D}_2^R \in \emptyset$. For case 1, when $\mathbb{D}_2^R \notin \emptyset$, to keep the packet fresh we give the highest priority to the involved relay which owns the oldest packet for transmission. When $\mathbb{D}_2^R \in \emptyset$ and $\mathbb{D}_1^R \notin \emptyset$, to reduce the packet waiting time we give the highest priority to the involved relay which owns the fewest packets for reception. If there exist multiple relays owning the fewest packets, we can select one of them uniformly.

For case 2, due to the packet lifetime limitation, we can select a proper relay as a cooperative jammer to degrade the reception of the eavesdropper so as to increase the transmission opportunity. For each relay, we can find out all feasible jammers where the corresponding transmission and jamming links satisfy the condition (4.4). We denote the effective partner pair sets for the first and second hop as $\mathbb{D}_1^{R,J}$ and $\mathbb{D}_2^{R,J}$, respectively. When $\mathbb{D}_2^{R,J} \notin \emptyset$, for the same reason as case 1, we select the relay m with the oldest packet as the transmitter and select another relay k which causes the least interference at the destination (i.e., $\min\{g_{k,d}\beta_d\}$) as the jammer. Similarly, when $\mathbb{D}_2^{R,J} \in \emptyset$ and $\mathbb{D}_1^{R,J} \notin \emptyset$, we select the relay m with the fewest packets as the receiver and select the relay k which leads to the least interference at m (i.e., $\min\{g_{k,m}\beta_m\}$) as the jammer. When $\mathbb{D}_1^{R,J} \in \emptyset$ and $\mathbb{D}_2^{R,J} \in \emptyset$, the system will be idle in this time slot.

Consequently, based on the above principles and considerations, we propose the secure and delay-aware communication protocol for the buffer-aided relaying system with limited packet lifetime, as summarized in Algorithm 5.

Algorithm 5 Security/Delay-Aware Communication Protocol

```
Require:
    Instantaneous CSIs of legitimate links, intended secrecy rate $R_s$, upper bound of SOP $P_{up}$, interference cancellation factor $\beta_m$ and $\beta_d$;;
Ensure:
    Selection decision $\mathcal{D}$;
Find out the link sets $\mathbb{D}_1^R$ and $\mathbb{D}_2^R$ where the channel gains satisfy the condition (4.3) for the first and second hop, respectively
if $\mathbb{D}_2^R \notin \emptyset$ then
    Use the involved relay $m$ for transmission which owns the oldest packet in $\mathbb{D}_2^R$ and $\mathcal{D} = m$;
else if $\mathbb{D}_2^R \in \emptyset$ and $\mathbb{D}_1^R \notin \emptyset$ then
    Capture the involved relays which owns the fewest packets in $\mathbb{D}_1^R$;
    if $\frac{\gamma_{a,r}[k]}{\alpha} \geq \frac{\gamma_{r,b}[k]}{\beta}$ then
        Choose one $m^*$ of them uniformly to receive the message and $\mathcal{D} = m^*$;
    else
        Choose the only one $m^*$ to receive the message and $\mathcal{D} = m^*$;
    end if
else
    Determine whether there are relay-jammer pairs that satisfy condition (4.4), if yes, execute Procedure 2 and find out the optimal partner pair;
end if
Return $\mathcal{D}$;
```

4.3 CDT Bitmap Framework for Packet Delivery Delay Modeling

Procedure 2 Find out the optimal partner pair

```
Find out all possible partner pairs for both hops, where the effective sets are denoted as $\mathbb{D}_1^{R,J}$ and $\mathbb{D}_2^{R,J}$, respectively, where
    • $\mathbb{D}_1^{R,J} = \{(m,k)|\text{satisfy the condition (4.4)}\}$
    • $\mathbb{D}_2^{R,J} = \{(m,k)|\text{satisfy the condition (4.4)}\}$
if $\mathbb{D}_2^{R,J} \notin \emptyset$ then
    Choose relay $m^*$ that owns the oldest packet as the transmitter in $\mathbb{D}_2^{R,J}$, then choose the corresponding jammer $k = \min\{g_{k,d}\beta_d\}$, thus $\mathcal{D} = (m^*, k)$;
else if $\mathbb{D}_1^{R,J} \notin \emptyset$ and $\mathbb{D}_2^{R,J} \in \emptyset$ then
    Choose relay $m^*$ that owns the fewest packets as the receiver in $\mathbb{D}_1^{R,J}$, then choose the corresponding jammer $k = \min\{g_{k,m}\beta_m\}$, thus $\mathcal{D} = (m^*, k)$;
else
    The system is reliable outage and $\mathcal{D} = \emptyset$;
end if
```

4.3.1 CDT Bitmap Modeling

In this section, we construct the delicate CDT bitmap to track the packet occupancy and delay information in the buffer queue. For a better understanding of the packet discarding behaviors at the source or relays, we introduce the following definitions.

Current Deliver Time (CDT) t_c: CDT is defined as the difference between the current time slot t and the time slot t_s that the packet arrives at the head of the source queue, i.e., $t_c = t - t_s$.

Deliver Time (DT) t_d: DT is defined as the difference between the time slot t_a that the packet arrives at the destination node and the time slot t_s that the packet becomes the head packet in source queue, i.e., $t_d = t_a - t_s$.

Note that each packet needs at least two time slots to reach the destination node, such that the CDT of the packet in the source (*resp.* relay) queue is required to $0 \leq t_c \leq \tau - 2$ (*resp.* $\tau - 1$) (otherwise the packet will be discarded). Besides, the DT for each packet must be more than two time slots but less than the lifetime τ, i.e., $2 \leq t_d \leq \tau$. With the help of the above definitions, we can track the DT for each packet, check overdue packets and drop the packets with CDTs exceeding the delay constraint in the buffer of source and relays before transmission.

According to Algorithm 5, in each time slot we need to track both the packet number and delay information before the selection decision. For easy tracking, we create a specific structure for source and relays which can fully depict the information. Note that each packet reaches and departs the buffer queue at different time slots, thus the specific structure cannot be modeled as a sequential backlog form, which is referred to as the *heterogeneous queuing problem*. To build the buffer state space that is flat and mathematical trackable, *CDT bitmap* is introduced to carefully study the problem.

CDT bitmap: We use $\mathscr{U} = \{U_s, U_1, U_2, \ldots, U_M\}$ to denote a set of integers and each element of $\mathscr{U}$ is called *CDT bitmap* of the corresponding node, which has a fixed bit-width of $\tau - 1$. Due to the infinite backlog, the *least significant bit* (LSB) of the CDT bitmap U_s of the source node always equals 1 indicating the existence of a head packet with 0 CDT delay, and the *most significant bit* (MSB) indicates to the existence state of a packet with the maximum tolerable CDT delay $\tau - 2$. For the CDT bitmap U_m of relay m, the LSB equals 1 (*resp.* 0) means the existence (*resp.* absence) of a packet with 1 CDT delay and the MSB means the existence state of a packet with the maximum tolerable CDT delay $\tau - 1$.

Therefore, the packet number and delay information can be uniquely represented by the number and position of the non-zero bits of the CDT bitmap, respectively. Expediently, we use the functions $\psi(U_m)$ and $\phi(U_m)$ to backtrack the number of filled non-zero bits and the position of the oldest packet for node m, respectively. Benefiting from the CDT bitmap, we can track the state transitions of the buffer queue by some useful bitwise operations caused by the decision of the proposed protocol. The operations are summarized as follows.

$\mathbf{U_m \ll 1}$: This bitwise "left-shift" operation shifts every bit of U_m to one bit left, the MSB is discarded and a new 0 is moved into the LSB position. This operation corresponds to the case where a packet has stayed in the queue for one more time slot, and any packet exceeding the delay constraint is dropped.

$\mathbf{U_m \bigoplus V}$: This bitwise "XOR" operation inverts the positive bit in U_m with the same position in V, where V is an integer with only one positive bit. This operation corresponds to the case where a packet should be cleared.

$\mathbf{U_m \bigotimes V}$: This bitwise "OR" operation converts the bit 0 of U_m into the positive one with the same position in V, where V has the same assumption as above. This operation is useful to demonstrate that a packet enters into the buffer queue.

By applying these bitwise operations, we can flexibly attach each network event to the corresponding state update of CDT bitmap.

Source Transmission: If the source is selected to transmit a packet, the head packet will depart from the buffer queue, and then the second packet will become the new head packet. Thus, the CDT bitmap update of the source node is given by

$$U_s^t = ((U_s \bigoplus 2^{\phi(U_s)-1}) \ll 1) \bigotimes 1. \tag{4.5}$$

For all relays, the packets stay in the buffer queue for more one slot, and the arrival packet will be added into the buffer queue of the selected relay m. Recall that the packet position in the source node represents the packet delay minus one, but the packet position in relays represents the packet delay. Therefore, while updating the CDT bitmap of relays, we only invert the bit whose position is corresponding to the transmitted packet but not perform the shift operation in U_m. The CDT bitmap update of the relay is given by

$$U_m^r = \begin{cases} (U_m \ll 1) \bigotimes 2^{\phi(U_s)-1}, & \text{if } m{=}m^*, \\ U_m \ll 1, & \text{otherwise.} \end{cases} \tag{4.6}$$

Relay Transmission: If the non-empty relay m (i.e., $\psi(U_m) \neq 0$) is selected to transmit a packet, the bit in the position of the oldest packet will be set to zero and the delay of other uninvolved packets are added to more one slot. Thus, we can obtain the CDT bitmap update of relays as

$$U_m^t = \begin{cases} (U_m \bigoplus 2^{\phi(U_m)-1}) \ll 1, & \text{if } m{=}m^*, \\ U_m \ll 1, & \text{otherwise.} \end{cases} \tag{4.7}$$

Similarly, the delay of the head packet in the source buffer increases by *one* time slot and the CDT update of the source node is

$$U_s^r = U_s \ll 1. \tag{4.8}$$

Reliable Outage: For reliable outage event, no transmission occurs and updating the CDT bitmap of source and relays only perform the shift operation, which is respectively given by

$$U_s^o = U_s \ll 1 \quad \text{and} \quad U_m^o = U_m \ll 1. \tag{4.9}$$

4.3.2 CDT Bitmap Analysis

In this section, we develop a Markov Chain-based theoretical framework to analyze the CDT bitmap established in Subsection 4.3.1. First, we study the states of MC resulting from the proposed communication protocol. Then we derive the state transition matrix under both the i.n.d (independent but non-identically distributed) and i.i.d (independent and identically distributed) channel models. Finally, we derive the MC stationary distribution.

4.3.2.1 States of Markov Chain

Recall that each node state can be denoted by its corresponding CDT bitmap, thus we can utilize the possible CDT bitmaps of the source and relays to track all states of the concerned system. We denote the state set of MC as $\mathbb{S} = \{S_1, S_2, \ldots, S_I\}$, where $S_i = \{U_s^i, \mathbb{U}_M^i\}$ $(i \in I)$ is the i-th state where $\mathbb{U}_M^i = \{U_1^i, U_2^i, \ldots, U_M^i\}$. The total number of MC states is equal to all possible combinations of the CDT bitmap. Although the impacts of all possible events are determined and conceptually simple, a refined formula determining the number of MC states is quite arduous. We know that a new state results from any one of the source transmission, relay transmission, and reliable outage events. Therefore, for a given set of states, we can find all associated states based on the CDT bitmap. For example, for $S_i = (U_s^i, \mathbb{U}_M^i)$, the new state transferred by the outage behavior, we only need to compute U_s^o and $\mathbb{U}_M^o$ by using (4.9), and determine whether $(U_s^o, \mathbb{U}_M^o)$ is a new state or not. For the new states resulting from source transmission, due to the possibility that the source may transmit the packet to anyone relay, we need to track all possible states and update the states set $\mathbb{S}$. Similarly, for the new states resulted from relay transmission, we should consider any non-empty relay may transmit the packet to the destination.

Thus, for the given number M of relays and the packet lifetime τ, we can find out all possible states of the concerned system. First, we set the initial state of the system as $\mathbb{S} = S_1$ where $S_1 = (1, \{0, 0, \ldots, 0\})$, which means only one packet with 0 delay is stored in the source queue. Second, we track and identify the new states caused by the possible decisions of the proposed communication protocol, and add the new states into $\mathbb{S}$. Then, we repeat tracking the possible states connected with the unchecked states until all states in $\mathbb{S}$ are checked. The algorithm is concluded as Algorithm 6.

Algorithm 6 States of MC Searching Algorithm

```
Require:
    The initial state of the system to $\mathbb{S}=\{S_I\}$ where $I=1$ and $S_1=(1,0,0,\ldots,0)$;
Ensure:
    Find out all possible MC states $\mathbb{S}$ with the proposed Algorithm 5;
while there is an unchecked state in $\mathbb{S}$ do
    Select any unchecked state $S_i$, compute $U_s^t$, $\mathbb{U}_R^r$, $U_s^r$, $\mathbb{U}_R^t$, $U_s^o$ and $\mathbb{U}_R^o$ according
    to (4.5)-(4.9), respectively
    for $(j = 1; j \leq I; j++)$ do
        a. compare the new state $(U_s^o, \mathbb{U}_M^o)$ with the state $S_j$ that is caused by the
        outage behavior;
        b. compare the new states $(U_s^t, \mathbb{U}_M^r)$ with the state $S_j$ that is caused by the
        source transmission;
        c. compare the new states $(U_s^r, \mathbb{U}_M^t)$ with the state $S_j$ that is caused by any
        relay $m$ transmission;
        if $U_s^t \neq U_s^j$ or $\mathbb{U}_M^o \neq \mathbb{U}_M^j$ then
            Set $I = I + 1$ and add the new state $S_{I+1} = (U_s^t, \mathbb{U}_M^o)$ into $\mathbb{S}$;
        else if $U_s^t \neq U_s^j$ or $\mathbb{U}_M^r \neq \mathbb{U}_M^j$ then
            Set $I = I + 1$ and add the new state $S_{I+1} = (U_s^t, \mathbb{U}_M^r)$ into $\mathbb{S}$;
        else
            Set $I = I + 1$ and add the new state $S_{I+1} = (U_s^r, \mathbb{U}_M^t)$ into $\mathbb{S}$;
        end if
    end for
end while
    Return all possible MC states $\mathbb{S}$;
```

4.3.2.2 Derivation of State Transition Matrix

The state transition matrix represents the MC of each node CDT bitmap and models the connectivity between them. It is a key element of the proposed analytical framework and its construction is also fundamental for the computation of performance metrics. Let $X_{t(t\geq 0)}$ denote the discrete-time Markov random process capturing the evolution of the network as a system. Also, let A denote all state transition matrix of the MC, in which the entry

$$A_{i,j} = \mathbb{P}(S_i \to S_j) \triangleq \mathbb{P}(X_{t+1} = S_j | X_t = S_i). \tag{4.10}$$

represents the probability to move from sate S_i at time t to state S_j at time $t+1$. In order to construct the state transition matrix A, identifying the connectivity between the different states of the system is of paramount importance. Notice that the connectivity is not only related to the number of the available links, but also related to the packet number and delay information. Thus, we first calculate the total numbers of the available links, and then categorize relays based on the packet number and delay information in the buffers.

The total number Ψ_{S_i} of the available links. For state S_i, the number of the available $s \to m$ links $\Psi_{S_i}^{sm}$ is equal to the number M of relay. Only a relay with non-empty buffer (i.e., $\psi(U_m^i) \neq 0$) can be selected to transmit the data. Consequently, for state S_i, the number of the available links $m \to d$ is equal to

$$\Psi_{S_i}^{md} = \sum_{m=1}^{M} \varphi_{S_i}^{md}(m), \tag{4.11}$$

where

$$\varphi_{S_i}^{md}(m) = \begin{cases} 1, & \text{if } \psi(U_m^i) > 0, \\ 0, & \text{otherwise.} \end{cases} \tag{4.12}$$

Thus, the total number of the available links for state S_i is

$$\Psi_{S_i} = \Psi_{S_i}^{sm} + \Psi_{S_i}^{md}. \tag{4.13}$$

Categorization of the available links. According to Algorithm 5, the protocol decision depends on the packet number and delay information. Thus, categorizing the available links is inevitable to track the state transition matrix. We define the sets $\mathbb{G}_l^{PNI}$ to categorize the available links based on the packet number l, i.e., the number of the filled elements in the bitmap of the corresponding relay, which stores the indices of link $s \to m$. As mentioned above, the buffer can store up to τ packets.

Thus, $l = \psi(U_m^i))$ and $l \in \{0, 1, \ldots, \tau\}$. The set $G_i^{PNI}(l)$ is defined to count the number for each element in $\mathbb{G}_l^{PNI}$ at state S_i, which is given by

$$G_i^{PNI}(l)_{l\in\{0,1,\ldots,\tau\}} = \sum_{m=1}^{M} g_m, \tag{4.14}$$

where

$$g_m = \begin{cases} 1, & \text{if } \psi(U_m^i) = l, \\ 0, & \text{otherwise.} \end{cases} \tag{4.15}$$

Otherwise, we use the sets $\mathbb{G}_d^{DSI}$ to categorize the available links based on the delay sate information of the involved relay bitmap, which stores the indices of the link $m \to d$. Likewise, we let the set $G_i^{DSI}(d)$ count the number for each element in $\mathbb{G}_d^{DSI}$ at state S_i, which can be formulated as

$$G_i^{DSI}(d)_{d\in\{1,2,\ldots,\tau-1\}} = \sum_{m=1}^{M} f_m \tag{4.16}$$

where

$$f_m = \begin{cases} 1, & \text{if } \phi(U_m^i) = d, \\ 0, & \text{otherwise.} \end{cases} \tag{4.17}$$

Based on the above formulations, we can derive the state transition probabilities (4.10) of the connected states caused by the protocol decisions, which are given by the following theorems and corollaries.

Theorem IV.1 Assume that all channels are i.n.d Rayleigh fading channels and suppose that the system is in sate S_i at current time slot, the probability that the reliable outage event leads to the connected state S_j is given by

$$A_{i,j}^{i.n.d} = \prod_{d=1}^{\tau-1} \Theta_{id}^{DSI} \prod_{l=0}^{\tau-1} \Theta_{il}^{PNI}, \tag{4.18}$$

where Θ_{id}^{DSI} denotes the probability that the channel equality of all $m \to d$ ($md \in \mathbb{G}_d^{DSI}$) does not satisfy the condition (4.3) and (4.4) at state i, and it is given by

$$\Theta_{id}^{DSI} = \begin{cases} 1, & \textit{if } G_i^{DSI}(d) = 0, \\ p_{md}^1 + p_{md}^2, & \textit{otherwise}, \end{cases} \tag{4.19}$$

where p_{md}^1 is given by

$$p_{md}^1 = \Gamma_M \left(\Omega_{m,d}\right) \prod_{k \in \mathcal{M}/m} \exp\left(-\frac{\theta_m}{\Omega_{k,d}\Xi_{mk}^d}\right), \tag{4.20}$$

and p_{md}^2 is given by

$$p_{md}^2 = \prod_{k \in \mathcal{M}/m} T\left(\Omega_{k,d}\Xi_{mk}^d, \Omega_{m,d}\right) - \prod_{k \in \mathcal{M}/m} \exp\left(-\frac{\theta_m}{\Omega_{k,d}\Xi_{mk}^d}\right)\left(1 - T\left(\Omega_{m,d}, \Omega_{k,d}\Xi_{mk}^d\right)\exp\left(-\frac{\theta_m}{\Omega_{m,d}}\right)\right), \tag{4.21}$$

the functions $\Gamma_u(x,y,z)$ and $T_u(x,y,z)$ are denoted as

$$\Gamma_u(x,y,\ldots) = \begin{cases} 1 - \exp\left(-\sum_{v=x,y,\ldots} \frac{\theta_s}{u}\right), & u = s, \\ 1 - \exp\left(-\sum_{v=x,y,\ldots} \frac{\theta_m}{u}\right), & u = m, \end{cases} \tag{4.22}$$

$$T_u(x,y,z) = \frac{x}{\sum_{v=x,y,z} v}. \tag{4.23}$$

Similarly, Θ_{in}^{PNI} denotes the probability that the channel equality of $s \to m$ ($sm \in \mathbb{G}_l^{PNI}$) does not satisfy the condition (4.3) and (4.4), and it is given by

$$\Theta_{il}^{PNI} = \begin{cases} 1, & \textit{if } G_i^{PNI}(l) = 0, \\ \prod_{sm \in \mathbb{G}_l^{PNI}} \left(p_{sm}^1 + p_{sm}^2\right), & \textit{otherwise}, \end{cases} \tag{4.24}$$

where p_{sm}^1 is given by

$$p_{sm}^1 = \Gamma_s\left(\Omega_{m,s}\right) \prod_{k\in\mathcal{M}/m} \exp\left(-\frac{\theta_s}{\Omega_{k,m}\Xi_{sk}^m}\right), \tag{4.25}$$

and p_{sm}^2 is given by

$$p_{sm}^2 = \prod_{k\in\mathcal{M}/m} T(\Omega_{km}\Xi_{sk}^m, \Omega_{sm}) - \prod_{k\in\mathcal{M}/m} \exp\left(\frac{-\theta_s}{\Omega_{km}\Xi_{sk}^m}\right)\left(1 - T\left(\Omega_{sm}, \Omega_{km}\Xi_{sk}^m\right)\exp\left(-\frac{\theta_s}{\Omega_{sm}}\right)\right). \tag{4.26}$$

Corollary 3 When all channels are i.i.d Rayleigh fading channels, the probability that the reliable outage event leads to the connected state S_j is given by

$$A_{i,j}^{i.i.d} = \mathcal{P}_o^{md} \prod_{l=0}^{\tau-1} \Theta_{il}^{PNI}, \tag{4.27}$$

where $\mathcal{P}_o^{md}$ is given as

$$\begin{aligned}\mathcal{P}_o^{md} = &\sum_{n_1=0}^{\Psi_{S_i}^{md}} \sum_{n_2=0}^{n_1} \binom{\Psi_{S_i}^{md}}{n_1}\binom{n_1}{n_2} \\ &\times \mathcal{L}_1^{n_1-n_2} \mathcal{L}_2^{n_1} \left(\Gamma_m\left(\Omega_{m,d}\right)\right)^{\Psi_{S_i}^{md}-n_1} \exp\left(-\frac{(\Psi_{S_i}^{md}-1)(\Psi_{S_i}^{md}-2n_1)\theta_m}{\Omega_{k,d}\Xi_{mk}^d}\right),\end{aligned} \tag{4.28}$$

and $\mathcal{L}_1$ and $\mathcal{L}_2$ are denoted as

$$\mathcal{L}_1 = \left[1 - T\left(\Omega_{m,d}, \Omega_{k,d}\Xi_{mk}^d\right)\right]^{\Psi_{S_i}^{md}-1}, \tag{4.29}$$

$$\mathcal{L}_2 = \left[1 - T\left(\Omega_{m,d}, \Omega_{k,d}\Xi_{mk}^d\right)\exp\left(-\frac{\theta_m}{\Omega_{k,d}}\right)\right]^{\Psi_{S_i}^{md}-1}. \tag{4.30}$$

Theorem IV.2 Assume that all channels are i.n.d Rayleigh fading channels and suppose that the system is in sate S_i, the probability that the source transmission leads to the connected state S_j is given by

$$A_{i,j}^{i.n.d} = \begin{cases} \sum\limits_{\mathcal{G}_{l^*}^{sm^*}} \frac{1}{|\mathcal{G}_{l^*}^{sm^*}|} \mathcal{P}_1(\mathcal{G}_{l^*}^{sm^*}) \prod\limits_{d=1}^{\tau-1} \Theta_{id}^{DSI}, & \mathcal{D} = m^* \wedge l^* = 0 \quad , \\ \sum\limits_{\mathcal{G}_{l^*}^{sm^*}} \frac{1}{|\mathcal{G}_{l^*}^{sm^*}|} \mathcal{P}_2(\mathcal{G}_{l^*}^{sm^*}) \prod\limits_{d=1}^{\tau-1} \Theta_{id}^{DSI}, & \mathcal{D} = m^* \wedge 0 < l^* < \tau - 1, \\ \mathcal{P}_{km^*}^{1} \prod\limits_{l=1}^{\tau-1} \Gamma_s \left(\Omega_{s,m}\right) \prod\limits_{d=1}^{\tau-1} \Theta_{id}^{DSI}, & \mathcal{D} = (m^*, k) \wedge l^* = 0, \\ \mathcal{P}_{km^*}^{1} \prod\limits_{l=l^*+1}^{\tau-1} \Gamma_s \left(\Omega_{s,m}\right) \prod\limits_{l=0}^{l^*-1} \Theta_{il}^{PNI} \prod\limits_{d=1}^{\tau-1} \Theta_{id}^{DSI}, & \mathcal{D} = (m^*, k) \wedge 0 < l^* < \tau - 1, \end{cases} \tag{4.31}$$

where l^* is the packet number in the buffer of the selected relay m^*, $\mathcal{G}_{l^*}^{sm^*}$ is the subset of $\mathbb{G}_{l^*}^{PNI}$ which contains the link index sm^*, $\mathcal{P}_1(\mathcal{G}_{l^*}^{sm^*})$ and $\mathcal{P}_2(\mathcal{G}_{l^*}^{sm^*})$ are given by

$$\mathcal{P}_1(\mathcal{G}_{l^*}^{sm^*}) = \prod_{sm \in \mathcal{G}_{l^*}^{sm}} \big(1 - \Gamma_s \left(\Omega_{s,m}\right)\big), \prod_{\substack{s\hat{m} \notin \mathcal{G}_{l^*}^{sm} \\ s\hat{m} \in \mathbb{G}_{l^*}^{PNI}}} \Gamma_s \left(\Omega_{s,\hat{m}}\right), \tag{4.32}$$

$$\mathcal{P}_2(\mathcal{G}_{l^*}^{sm^*}) = \mathcal{P}_1(\mathcal{G}_{l^*}^{sm^*}) \prod_{l=0}^{l^*-1} \Gamma_s \left(\Omega_{s,m}\right), \tag{4.33}$$

$\mathcal{P}_{km^*}^{1}$ is the probability that the optimal partner pair (m^*, k) is selected where relay m^* own the fewest packets, which is given in (4.34) and $\mathcal{G}_{l^*}^{m}$ is the involved relay set in $\mathcal{G}_{l^*}^{sm}$.

$$\begin{aligned} \mathcal{P}_{km^*}^{1} = T\big(\Omega_{s,m^*}, \Omega_{km^*}\Xi_{sk}^{m^*}\big)\Bigg\{ \prod_{m \neq m^*, k} \Bigg\{\Bigg[1 - T\left(\Omega_{s,m^*}\Omega_{k,m^*}, \Omega_{k,m^*}\Omega_{s,m}\Xi_{sk}^{m^*}, \Omega_{s,m^*}\Omega_{m,m^*}\right)\Bigg] \\ - \exp\left(\frac{-\theta_s}{\Omega_{s,m^*}}\right) T(\Omega_{m,m^*}, \Omega_{k,m^*})\Bigg\} \times \prod_{\breve{m} \neq \bar{m}} \prod_{\substack{\bar{m} \in \mathbb{G}_{l^*}^{PNI} \\ \bar{m} \neq m^*}} \Bigg\{ - \exp\left(\frac{-\theta_s}{\Omega_{s,m^*}}\right) T(\Omega_{\breve{m},\bar{m}}\beta_{\bar{m}}, \Omega_{k,m^*}\beta_{m^*}) \\ + \Gamma_s(\Omega_{s,\bar{m}}) \Bigg[1 - T\big(\Omega_{s,m^*}\Omega_{k,m^*}\beta_{m^*}, \Omega_{k,m^*}\Omega_{\breve{m},\bar{m}}\Xi_{sk}^{m^*}\beta_{\bar{m}}, \Omega_{s,m^*}\Omega_{\breve{m},\bar{m}}\beta_{\bar{m}}\big)\Bigg]\Bigg\}\Bigg\}. \end{aligned} \tag{4.34}$$

Corollary 4 Assume that all channels are i.i.d Rayleigh fading channels and suppose that the system is in sate S_i, the probability that the source transmission leads to the connected state S_j is given by

$$A_{i,j}^{i.i.d} = \begin{cases} \sum_{\mathcal{G}_{l^*}^{sm^*}} \frac{1}{|\mathcal{G}_{l^*}^{sm^*}|} \mathcal{P}_1^{'}(\mathcal{G}_{l^*}^{sm^*}) \mathcal{P}_o^{md}, & \mathcal{D} = m^* \wedge l^* = 0 \quad , \\ \sum_{\mathcal{G}_{n^*}^{sm^*}} \frac{1}{|\mathcal{G}_{n^*}^{sm^*}|} \mathcal{P}_2(\mathcal{G}_{n^*}^{sm^*}) \mathcal{P}_o^{md}, & \mathcal{D} = m^* \wedge 0 < l^* < \tau - 1, \\ \mathcal{P}_{km^*}^1 \prod_{l=1}^{\tau-1} \Gamma_s \left(\Omega_{s,m^*}\right) \mathcal{P}_o^{md}, & \mathcal{D} = (m^*, k) \wedge l^* = 0, \\ \mathcal{P}_{km^*}^1 (\Gamma_s(\Omega_{s,m^*}))^{\Psi_{S_i}^{sm^*} - \sum_{l=0}^{l^*} G_i^{PNI}(l)} \prod_{l=0}^{l^*-1} \Theta_{il}^{PNI} (\Xi_{m^*k}^s) \mathcal{P}_o^{md}, & \mathcal{D} = (m^*, k) \wedge 0 < l^* < \tau - 1, \end{cases} \tag{4.35}$$

where $\mathcal{P}'_1(\mathcal{G}_{l^*}^{sm^*})$ *is given as*

$$\mathcal{P}'_1(\mathcal{G}_{l^*}^{sm^*}) = \sum_{n_1=0}^{|\mathcal{G}_{l^*}^{sm^*}|} \binom{n_1}{|\mathcal{G}_{l^*}^{sm^*}|} (-1)^{n_1} \Gamma_s \left(\Omega_{s,m^*}\right)^{|\mathcal{G}_{l^*}^{sm^*}| + n_1 - G_{l^*}^{PNI}} . \tag{4.36}$$

Theorem IV.3 Assume that all channels are i.n.d Rayleigh fading channels and suppose that the system is in sate S_i, the probability that relay m^* transmission leads to the connected state S_j is given by

$$A_{i,j}^{i.n.d} = \begin{cases} 1 - \Gamma_{m^*} \left(\Omega_{m^*,d}\right), & \mathcal{D} = m^* \wedge d^* = \tau - 1, \\ \left[1 - \Gamma_{m^*} \left(\Omega_{m^*,d}\right)\right] \prod_{d > d^*}^{\tau-1} \Gamma_m \left(\Omega_{m,d}\right), & \mathcal{D} = m^* \wedge 0 < d^* < \tau - 1, \\ \prod_{m \neq m^*,k} (\bar{\omega}_m - \underline{\omega}_m), & \mathcal{D} = (m^*, k) \wedge d^* = \tau - 1, \\ \prod_{\substack{d^1=1 \\ m \neq m^*,k}}^{d^*-1} (\bar{\omega}_{\bar{m}} - \underline{\omega}_{\bar{m}}) \prod_{\substack{d^2=d^*+1 \\ \bar{m} \neq m^*,k}}^{\tau-1} (\bar{\omega}_{\bar{m}} - \tilde{\omega}_{\hat{m}}), & \mathcal{D} = (m^*, k) \wedge 0 < d^* < \tau - 1, \end{cases} \tag{4.37}$$

where $d^1 = \phi(U^i_{\bar{m}})$, $d^2 = \phi(U^i_{\hat{m}})$, $\bar{\omega}_m$ *and* $\bar{\omega}_{\bar{m}}$ *can be collectively denoted as*

$$\begin{aligned}\bar{\omega}_{\Delta,\Delta\in(m,\bar{m})} = {} & T\big(\Omega_{\Delta_d}, \Omega_{k,d}\big)\Gamma_{m^*}\big(\Omega_{m^*,d}\big) \times \Big[T\big(\Omega_{\Delta d}, \Omega_{kd}\big) \\ & -T\big(\Omega_{\Delta d}\Omega_{k,d}\Xi_{kd}, \Omega^{m^*}_d\Omega_{k,d}, \Omega_{\Delta,d}\Omega_{m^*,d}\big)\Gamma_{m^*}\big(\Omega_{\Delta d}\Xi^d_{m^*k}, \Omega_{kd}\Xi^d_{m^*k}, \Omega_{m^*,d}\big)\Big],\end{aligned} \tag{4.38}$$

$\underline{\omega}_m$ *and* $\underline{\omega}_{\bar{m}}$ *are given as*

$$\underline{\omega}_{\Delta(\Delta\in m,\bar{m})} = \big(1-\Gamma_{\bar{m}}\big(\Omega_{\bar{m}d}\big)\big)\Bigg[\Gamma_{m^*}\big(\Omega_{m^*d}\big) - T\big(\Omega_{kd}\Xi^d_{m^*k}, \Omega_{m^*d}\big)\Gamma_{m^*}\big(\Omega_{kd}\Xi^d_{m^*k}, \Omega_{m^*d}\big)\Bigg], \tag{4.39}$$

and $\tilde{\omega}_{\hat{m}}$ *is given as*

$$\begin{aligned}\tilde{\omega}_{\hat{m}} = {} & T\big(\Omega_{\hat{m},d}, \Omega_{k,d}\Xi^d_{m^*k}\big)\Bigg[\Gamma_m\big(\Omega_{m*,d}\big) \\ & -T\big(\Omega_{\hat{m},d}\Omega_{k,d}\Xi^d_{m^*k}, \Omega_{m^*,d}\Omega_{kd}, \Omega_{\hat{m},d}\Omega_{m^*,d}\big)\Gamma_{m^*}\big(\Omega_{\hat{m},d}\Xi^d_{m^*k}, \Omega^k_d, \Omega_{m^*,d}\big)\Bigg].\end{aligned} \tag{4.40}$$

Corollary 5 Assume that all channels are i.i.d Rayleigh fading channels and suppose that the system is in sate S_i, the probability that relay m^* transmission leads to the connected state S_j is given by

$$A^{i.i.d}_{i,j} = \begin{cases} 1-\Gamma_{m^*}\left(\Omega_{m^*,d}\right), & \mathcal{D} = m^* \wedge d^* = \tau - 1, \\ \mathcal{P}^{m^*}_t, & \mathcal{D} = m^* \wedge 0 < d^* < \tau - 1, \\ \mathcal{P}^{m^*k}_t(\Psi^{md}_{S_i} - 2), & \mathcal{D} = (m^*, k) \wedge d^* = \tau - 1, \\ \mathcal{P}^{m^*k}_t(\chi_1)\mathcal{P}^{m^*k}_o(\chi_2), & \mathcal{D} = (m^*, k) \wedge\ 0 < d^* < \tau - 1, \end{cases} \tag{4.41}$$

where $\mathcal{P}^{m^*}_t$ *is given as*

$$\mathcal{P}^{m^*}_t = \sum_{n_1=0}^{\sum_{d=d^*+1}^{\tau-1} G_i^{DSI}(d)} \binom{n_1}{\sum_{d=d^*+1}^{\tau-1} G_i^{DSI}(d)} (-1)^n \exp\left(-\frac{n_1\theta_{m^*}}{\Omega_{m^*,d}}\right), \tag{4.42}$$

$\mathcal{P}_t^{m^*k}(x)$ *and* $P_o^{m^*k}(x)$ *are given in (4.43) and (4.44), respectively,*

$\mathcal{O}(x)$ *is denoted as*

$$\mathcal{O}(x) = \left[1 - \exp\left(-\frac{\theta_m}{T(x)\Omega_{m,d}}\right)\right] T(x), \tag{4.45}$$

χ_1 *is given as*

$$\chi_1 = \begin{cases} \sum_{d=1}^{d^*-1} G_i^{DSI}(d) - 1, & \textit{if } \phi(U_k^i) \in [1, d^* - 1], \\ \sum_{d=1}^{d^*-1} G_i^{DSI}(d), & \textit{otherwise}, \end{cases} \tag{4.46}$$

and χ_2 *is given as*

$$\chi_2 = \begin{cases} \sum_{d=d^*+1}^{\tau-1} G_i^{DSI}(d) - 1, & \textit{if } \phi(U_k^i) \in [d^* + 1, \tau - 1], \\ \sum_{d=d^*+1}^{\tau-1} G_i^{DSI}(d), & \textit{otherwise.} \end{cases} \tag{4.47}$$

Proof: The proof of Theorem IV.1 and Theorem IV.2 are given in Appendix B.2 and Appendix B.3. The proof of Corollary 1 is the same as that of Theorem IV.1, and the proofs of Corollary 2, Theorem IV.3 and Corollary 3 are similar to that of Theorem IV.2, so we omit them here. ■

$$\begin{aligned}\mathcal{P}_t^{m^*k}(x) = & \sum_{n_1=0}^{x} \sum_{n_2=0}^{x-2} \sum_{n_3=0}^{n_1} \binom{n_1}{x} \binom{n_2}{x - n_1} \binom{n_3}{n_1} \\ & \times \frac{(-1)^{\sum_{i=1}^3 n_i}}{2^{x-n_1}} \Big(1 - \Gamma_{m^*}\left(\Omega_{m^*d}\right)\Big)^{n_1} \Gamma_{m^*}\left(\Omega_{m^*d}\right)^{x-n_2-n_3} \Big(\mathcal{O}(\Xi_{m^*k}^d, 2)\Big)^{n_2} \Big(\mathcal{O}(\Xi_{m^*k}^d, 1)\Big)^{n_3}\end{aligned} \tag{4.43}$$

$$\begin{aligned}\mathcal{P}_o^{m^*k}(x) = & \sum_{n_1=0}^{x} \sum_{n_2=0}^{x-2} \sum_{n_3=0}^{n_1} \binom{n_1}{x} \binom{n_2}{x - n_1} \binom{n_3}{n_1} \\ & \times \frac{(-1)^{\sum_{i=1}^3 n_i}}{2^{x-n_1}} \Big(T\big(1, \Xi_{m^*k}^d\big)\Big)^{n_1} \Gamma_{m^*}(\Omega_{m^*d})^{x-n_2-n_3} \Big(\mathcal{O}(\Xi_{m^*k}^d, 2)\Big)^{n_2} \Big(\mathcal{O}(\Xi_{m^*k}^d, \Xi_{m^*k}^d, 1)\Big)^{n_3}\end{aligned} \tag{4.44}$$

4.3.3 Derivation of MC Stationary Distribution

From the above theorems and corollaries, we can see that $A_{i,j} \neq 0$. Furthermore, we know that the state transition is caused by source transmission, relay transmission or outage, thus we have $\sum_{j=1}^{I} A_{i,j}^{i.n.d} = 1$ and $\sum_{j=1}^{I} A_{i,j}^{i.i.d} = 1$, which means the state transition matrix A is a column stochastic. Otherwise, it is possible to get to any state from state $S_j (j \in I)$, i.e., the Markov chain is irreducible and positive recurrent. Thus, it can be readily verified that the Markov chain has a time invariant state distribution [67]. We denote the unique stationary probability distributions as $\boldsymbol{\pi}^{\Lambda} = [\pi_{S_1}^{\Lambda}, \ldots, \pi_{S_i}^{\Lambda}, \ldots, \pi_{S_I}^{\Lambda}]^T$, such that $\boldsymbol{\pi}^{\Lambda} = A\boldsymbol{\pi}^{\Lambda}$ and $\left\|\boldsymbol{\pi}^{\Lambda}\right\| = 1$, where $\Lambda \in \{\text{i.n.d, i.i.d}\}$.

According to Lemma 2 in [68], the analytical expression of $\pi_{S_i}^{i.n.d}$ can be given by

$$\pi_{S_i}^{\Lambda} = \left(\sum_{j=1}^{I} \frac{\prod_{S_i' \in \mathtt{C}(S_i, \Re_{S_j})} A_{i,i'}^{\Lambda}}{\prod_{S_j' \in \mathtt{C}(S_j, \Re_{S_i})} A_{j,j'}^{\Lambda}} \right)^{-1}, \tag{4.48}$$

where $\Re_{S_i}$ ($\Re_{S_j}$) is the set of states that have the same stationary probability with S_i (S_j), $\mathtt{C}(S_i, \Re_{S_j})$ ($\mathtt{C}(S_j, \Re_{S_i})$) is the set of states that S_i (S_j) has to pass through to reach a state in $\Re_{S_i}$ ($\Re_{S_j}$).

4.4 Performance Analysis

With the help of the stationary probability distribution of MC, in this section, we derive the closed-form expressions of some fundamental performance metrics, including the reliable outage probability (ROP), packet discard probability (PDP) and secrecy throughput (ST).

Derivation of ROP. When the transmission security of the packet cannot be ensured, the system will be temporary sleeping, which is called the reliable outage. As stated in Algorithm 5, a reliable outage occurs if and only if all links are in the outage, and the probability depends on the state of the system. Therefore, the total outage probability P_{ro} must be taken into account for all states, which can be formulated as

$$P_{ro}^{\Lambda} = \sum_{i=1}^{I} \pi_{S_i} p_{ou}^{\Lambda}(S_i), \tag{4.49}$$

where $p_{ou}^{\Lambda}(S_i)$ is given by (4.18) when $\Lambda =$ i.n.d, and $p_{ou}^{\Lambda}(S_i)$ when $\Lambda =$ i.i.d is given by (4.27).

Derivation of PDP. With consideration of the transmission timeliness of the packet, one of the main targets for the proposed protocol is to reduce the number of discarded packets. The PDP P_{dis} of the concerned system equals to the sum of the probability that the packets are discarded at the source node and all relays in all states, which is formulated as

$$P_{dis}^{\Lambda} = \sum_{i=1}^{I} \pi_{S_i} \left[X^{\Lambda}(S_i) + \sum_{m=1}^{M} Y_m^{\Lambda}(S_i) \right], \tag{4.50}$$

where $X^{\Lambda}(S_i)$ is the probability that the packet is discarded at the source node in state S_i, which is given by

$$X_{S_i}^{\Lambda} = \begin{cases} 1 - \sum_{m=1}^{M} p_{sm}^{\Lambda}(S_i), & \text{if } \phi(U_s^i) = \tau - 1, \\ 0, & \text{otherwise.} \end{cases} \tag{4.51}$$

where $p_{sm}^{\Lambda}(S_i)$ is given by (4.31) when $\Lambda =$ i.n.d, and ($\Lambda =$ i.i.d), $p_{sm}^{\Lambda}(S_i)$ is given by (4.35) when $\Lambda =$ i.i.d. $Y_m^{\Lambda}(S_i)$ is the probability that the packet is discarded from relay m in state S_i. Note that there is at most one packet in relay queues would reach the lifetime. Thus, $Y_m^{\Lambda}(S_i)$ is given by

$$Y_{S_i}^{\Lambda} = \begin{cases} 1 - p_{md}^{\Lambda}(S_i), & \text{if } \phi(U_m^i) = \tau - 1, \\ 0, & \text{otherwise.} \end{cases} \tag{4.52}$$

Table 4.1: Average Channel Gain of Links for I.n.d Case

Channel Gain settings	$\Omega_{s,1}$	$\Omega_{s,2}$	$\Omega_{s,3}$	$\Omega_{s,4}$	$\Omega_{1,d}$	$\Omega_{2,d}$	$\Omega_{3,d}$	$\Omega_{4,d}$	$\Omega_{s,e}$	
	12 dB	15 dB	15 dB	18 dB	10 dB	25 dB	20 dB	14 dB	5 dB	
Channel Gain settings	$\Omega_{1,e}$	$\Omega_{2,e}$	$\Omega_{3,e}$	$\Omega_{4,e}$	$\Omega_{1,2}$	$\Omega_{1,3}$	$\Omega_{1,4}$	$\Omega_{2,3}$	$\Omega_{2,4}$	$\Omega_{3,4}$
	5 dB	12 dB	15 dB	8 dB	2.5 dB	2 dB	3 dB	5 dB	4 dB	3.5 dB

where $p^{\Lambda}_{md}(S_i)$ is given by (4.37) when $\Lambda =$ i.n.d, and $p^{\Lambda}_{md}(S_i)$ is given by (4.41) when $\Lambda =$ i.i.d.

Derivation of achievable ST. The achievable ST $\mathcal{Q}$ is defined as the average rate of packet that can be transferred securely and timely to the destination, which is formulated as

$$\mathcal{Q}^{\Lambda} = \sum_{i=1}^{I}(\pi_{S_i} R_s(1 - P_{up}) \sum_{m=1}^{M} p^{\Lambda}_{md}(S_i)), \tag{4.53}$$

where $p^{\Lambda}_{md}(S_i)$ is the same with the one in (4.52).

4.5 Simulation Results and Discussions

In this section, we first conduct simulations to verify the efficiency of the theoretical framework for performance modeling, and then provide numerical results to show the impacts of the protocol's parameters on the system performance.

4.5.1 Simulation Settings

To validate the theoretical performance evaluation, a dedicated MATLAB simulator was developed to simulate the packet delivery process under the proposed communication protocol, which is available at [64]. With the help of this simulator, we conduct extensive simulations to calculate the simulated results of ROP, PDP and achievable ST. The duration of each task of simulation runs throughout 1×10^6 time slots and the corresponding protocol is performed once per slot for both i.i.d and i.n.d cases. We set all the noise variances and the transmission power to be 1 Watts/Hz, the relay number $M = 4$, and SIC factors $\beta_1 = 0.4$, $\beta_2 = 1.0$, $\beta_3 = 0.6$, $\beta_4 = 0.8$. The detailed settings of average channel gains for i.n.d case are summarized in Table 4.1, and for i.i.d case we set $\Omega_{s,i} = 15$ dB, $\Omega_{i,d} = 17.25$ dB, $\Omega_{s,e} = 5$ dB and $\Omega_{i,e} = 8$ dB, where $i \in \{1, 2, 3, 4\}$. The average channel gains between relays are set as $\Omega_{i,j} = 3.56$ dB, where $i, j \in \{1, 2, 3, 4\}$ and $i \neq j$.

We count the number of time slots that the system reliable outage happens in a task of simulation as T, the numbers of packets transmitted by the source and received at the destination as N_0 and N_1, respectively, and the numbers of packets discarded at the source and the relays as N_2 and N_3, respectively. Then, the simulated ROP is calculated as

$$\text{Simulated ROP} = 100\% \times \frac{T}{1 \times 10^6}. \tag{4.54}$$

The simulated PDP and achievable ST are respectively calculated as

$$\text{Simulated PDP} = 100\% \times \frac{N_2 + N_3}{N_0}, \tag{4.55}$$

$$\text{Simulated ST} = R_s \times \frac{N_1}{1 \times 10^6}. \tag{4.56}$$

4.5.2 Validation

We first summarize in Fig. 4.2, Fig. 4.3 and Fig. 4.4 the simulation and theoretical results of the system performance under the variation of secrecy rate R_s, where we set $P_{up} = 0.1$ and $\tau = 10$. Then, Fig. 4.5, Fig. 4.6 and Fig. 4.7 present the simulation and theoretical results that how the system performance varies with the upper bound of SOP P_{up}, where we set $R_s = 0.5$ and $\tau = 10$. Finally, we plot Fig. 4.8, Fig. 4.9 and Fig. 4.10 to show the simulation and theoretical results of the system performance under the variation of packet lifetime τ, where we set $R_s = 0.5$ and $P_{up} = 0.1$. From these figures, we can see that all the simulation results match nicely with the

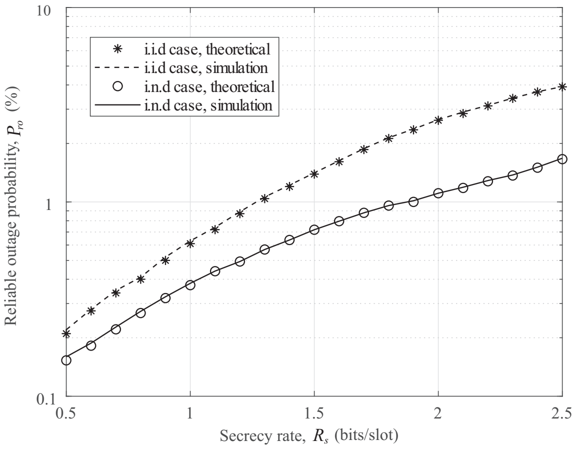


Figure 4.2: Reliable outage probability P_{ro} vs. secrecy rate R_s.

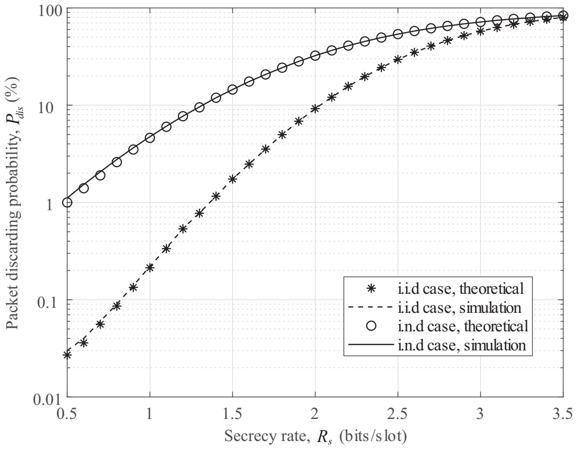


Figure 4.3: Packet discarding probability P_{dis} vs. secrecy rate R_s.

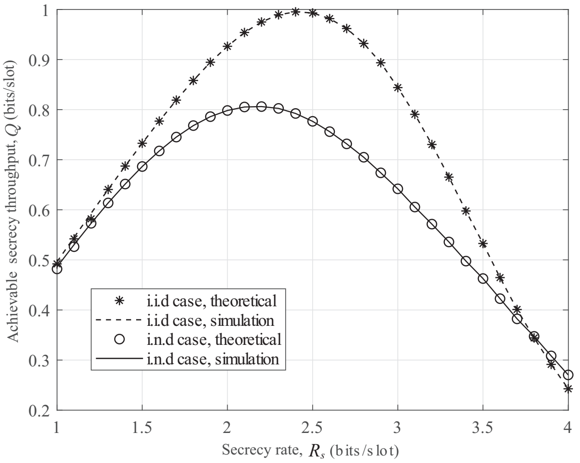


Figure 4.4: Achievable secrecy throughput $\mathcal{Q}$ vs. secrecy rate R_s.

corresponding theoretical curves for both the i.i.d and i.n.d cases, indicating that our theoretical framework is highly efficient to model the fundamental system-level performance for the concerned system with the proposed communication protocol. A more careful observation from Fig. 4.2∼Fig.4.10 is that there are very small gaps between the simulation and theoretical results. Such gaps are mainly due to the approximations in (B.2) and (B.4), which make the theoretical results shift slightly from the exact ones.

4.5.3 Performance Discussions

4.5.3.1 P_{ro} vs. $R_s/P_{up}/\tau$

Fig. 4.2, Fig. 4.5 and Fig. 4.8 show how P_{ro} varies with R_s, P_{up} and τ, respectively. We can see from Fig. 4.2 and Fig. 4.5 that P_{ro} increases monotonically as the secrecy rate R_s increases, but decreases monotonically as the upper bound of SOP P_{up} increases. Such behaviors are consistent with Proposition 1 that a larger R_s and P_{up} will result in fewer transmission opportunities at both the source and relays. Fig. 4.8 shows that as the lifetime τ increases P_{ro} first decreases quickly and then remains almost constant. This is due to the reason that according to Algorithm **??** the transmission behaviors of nodes are jointly determined by the security and lifetime constraints, but when τ increases to a specific value, they are dominated only by the security constraint. Additionally, we can observe that the system can always achieve a lower P_{ro} under the i.n.d case compared with that under the i.i.d case.

4.5.3.2 P_{dis} vs. $R_s/P_{up}/\tau$

We then discuss the impacts of R_s, P_{up} and τ on the PDP P_{dis}. From Fig. 4.3, Fig. 4.6 and Fig. 4.9, we can observe that the PDP P_{dis} increases monotonically as R_s increases, but decreases monotonically with the growth of P_{up} and τ. This is because that a larger R_s and/or a lower P_{up} can result in fewer transmission opportunities

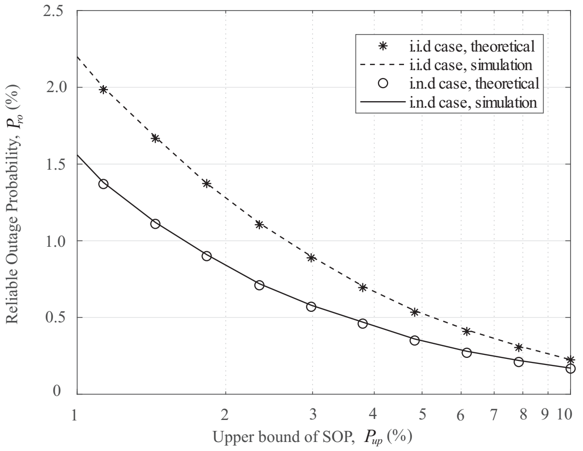


Figure 4.5: Reliable outage probability P_{ro} vs. secrecy rate P_{up}.

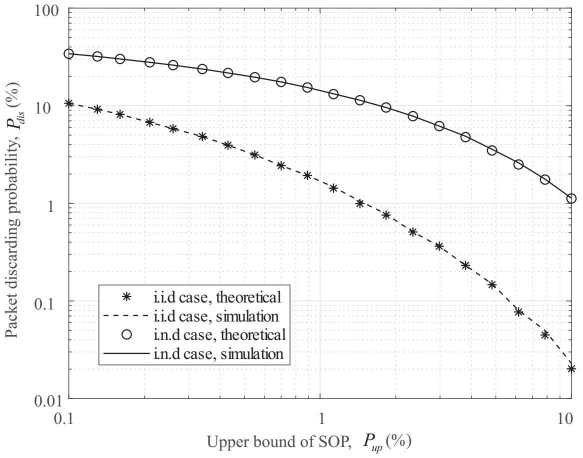


Figure 4.6: Packet discarding probability P_{dis} vs. upper bound of SOP P_{up}.

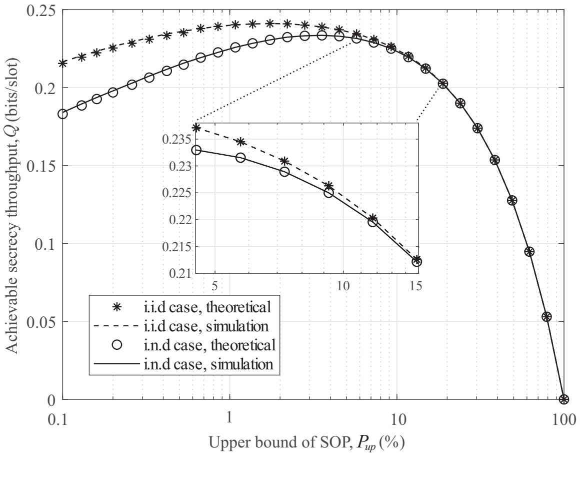


Figure 4.7: Achievable secrecy throughput $\mathcal{Q}$ vs. upper bound of SOP P_{up}.

and increase the service time in the buffer queue, which will lead to the growth of the risk of packet discarding. When adopting a larger τ, the system allows each packet to wait in the buffer queue for a longer time and thus fewer packets will be discarded. A further careful observation is that different from the behaviors of the ROP, the system can always achieve a better PDP performance under the i.i.d case than that under the i.n.d case.

4.5.3.3 $\mathcal{Q}$ vs. $R_s/P_{up}/\tau$

Fig. 4.4, Fig. 4.7 and Fig. 4.10 present how R_s, P_{up} and τ affect the system performance in terms of the ST $\mathcal{Q}$, respectively. It can be observed from Fig. 4.4 that as R_s increases to 2.1 and 2.4, the system ST under the i.n.d and i.i.d cases first increases to its peak (i.e., 0.8061 and 0.9952) and then decreases monotonically, respectively. This is because the ST is an integrated measure for the transmission performance, and R_s has two side effects on ST. On the one hand, a larger R_s results in more secrecy data per transmission; on the other hand, a larger R_s leads to a higher SOP such that the transmission opportunities will be reduced. Fig. 4.7 shows that as P_{up} increases $\mathcal{Q}$ first increases gradually and then decreases to 0. It is due to the reason that a larger P_{up} will lead to more transmission opportunities for the relays, and when P_{up} increases to a large value, more packets arrive at the destination, but most of them are wiretapped by the eavesdropper. As can be seen from Fig. 4.10 that as τ increases the ST increases rapidly, and when $\tau = 16$ and $\tau = 10$, $\mathcal{Q}$ reaches its maximal values (i.e., 0.246 and 0.2445) under the i.n.d and i.i.d cases, respectively. This is because that when τ is relatively small, the delay constraint mainly determines the transmission behaviors of nodes, but when τ is relatively large, the security constraint (which is determined by R_s and P_{up}) will become dominant. Moreover, we can observe that the system can always achieve a higher ST under the i.i.d case than that under the i.n.d case.

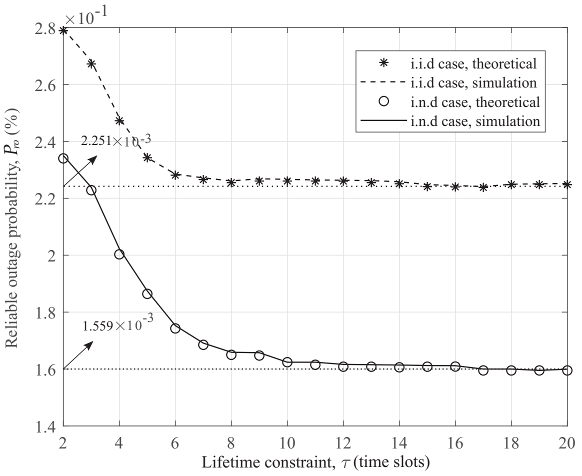


Figure 4.8: Reliable outage probability P_{ro} vs. lifetime constraint τ.

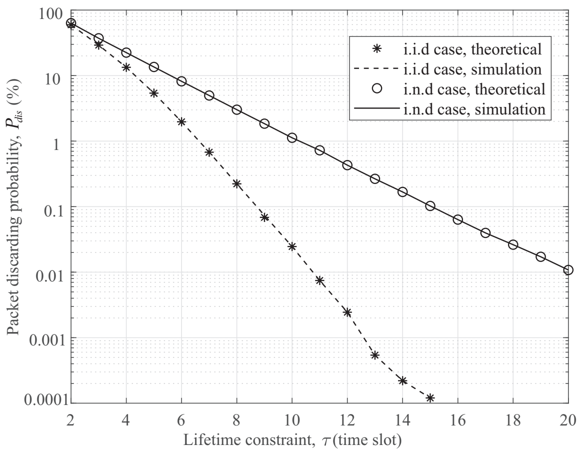


Figure 4.9: Packet discarding probability P_{dis} vs. lifetime constraint τ.

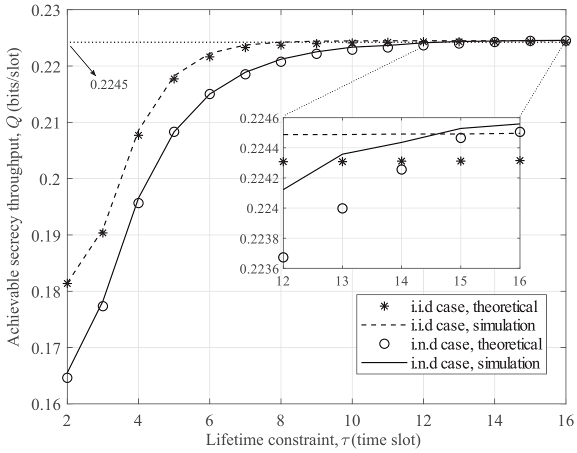


Figure 4.10: Achievable secrecy throughput $\mathcal{Q}$ vs. lifetime constraint τ.

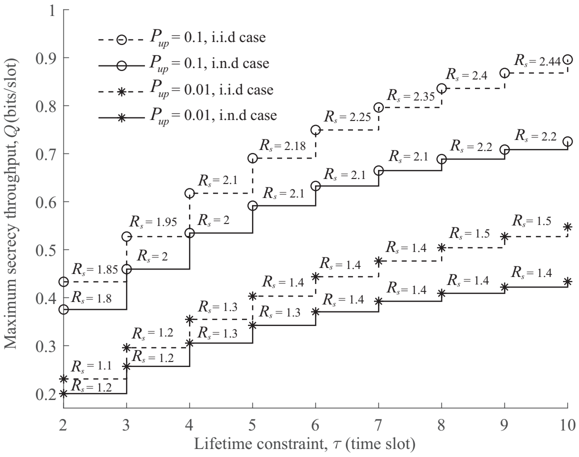


Figure 4.11: Maximum achievable secrecy throughput $\mathcal{Q}$ vs. lifetime constraint τ under optimal secrecy rate R_s.

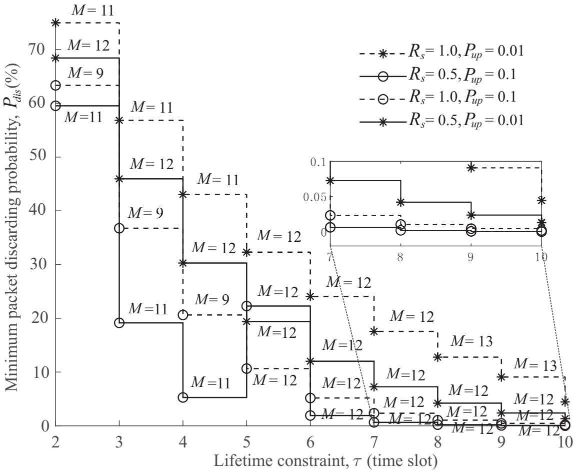


Figure 4.12: Minimum packet discarding probability P_{dis} vs. lifetime constraint τ under optimal relay number M.

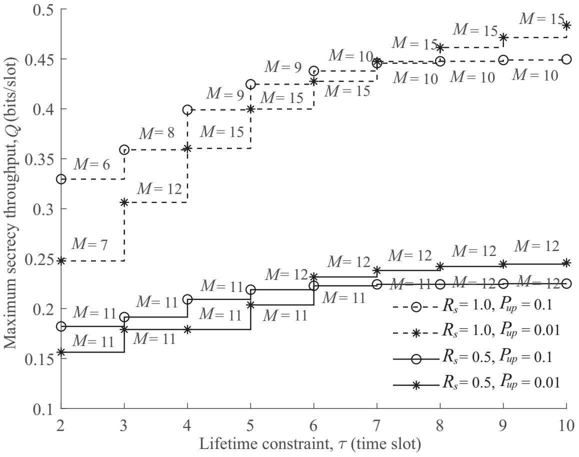


Figure 4.13: Maximum achievable secrecy throughput $\mathcal{Q}$ vs. lifetime constraint τ under optimal relay number M.

4.5.4 Optimal Parameter Settings

We summarize in Fig. 4.11 the maximum ST that can be achieved by setting the optimal secrecy rate R_s under the variation of lifetime constraint. It can be seen that for a slack lifetime τ or SOP constraint P_{up}, we need to configure a larger R_s for the transmitters to achieve the optimal ST. Another observation is that the maximal achievable ST is a piecewise function of τ, and an optimal value of R_s can apply to a small range of τ (e.g., for i.n.d case, when $P_{up} = 0.01$, the optimal secrecy rate $R_s = 1.2$ can apply to $\tau = 2$ and $\tau = 3$). We can further observe from Fig. 4.11 that as τ scales up, the maximal achievable ST becomes less sensitive to the variation of τ. For example, under the i.n.d case with $P_{up} = 0.1$, when τ varies from 2 to 3, the maximal ST increases from 0.3754 to 0.4595, while when τ varies from 9 to 10, the maximal ST increases just from 0.7254 to 0.7405.

Taking into consideration that deploying too many relays will waste the system resources, we further investigate the optimal setting for the number of relays under some performance constraints. Fig. 4.12 presents the optimal setting of the number of relays for minimizing the system PDP P_{dis}. We can observe from Fig. 4.12 that when the system adopts a smaller R_s, we should deploy more relays to improve the PDP performance. Furthermore, for a fixed R_s and P_{up}, the optimal number of relays increases as the lifetime τ becomes large. Another interesting behavior is that the optimal number of relays remains constant when the system adopts a small R_s and a slack P_{up}. For example, when $R_s = 0.5$ and $P_{up} = 0.1$, the optimal number of relays is always 12 no matter how the lifetime varies.

Finally, we examine in Fig. 4.13 the optimal setting of the number of relays for maximizing the achievable ST $\mathcal{Q}$ with different packet lifetime. From Fig. 4.13, we can see that for a given R_s, it needs to deploy more relays to improve the system ST when a strict security performance is required. We can also note that when $P_{up} = 0.1$, the optimal number of relays with $R_s = 0.5$ is bigger than that with $R_s = 1.0$, but when $P_{up} = 0.01$, the situation becomes reverse. A further careful observation of Fig. 4.13 is that for a given R_s, the system first achieves a larger $\mathcal{Q}$ with $P_{up} = 0.1$ than that with $P_{up} = 0.01$, but when the lifetime constraint is relaxed to 6 time slots, the system first achieves a larger $\mathcal{Q}$ with $P_{up} = 0.01$ than that with $P_{up} = 0.1$. This is due to the reason that the system ST is an integrated measure for both the security and relay transmission probability p_{md}, when τ is less than 6, the system ST is mainly determined by p_{md}, but as τ increases, we can provide more relays to increase p_{md} and the system ST is dominated by P_{up}.

4.6 Summary

This work focused on a buffer-aided relaying system with a limited packet lifetime. To support secure and timely data delivery in the concerned system, we proposed a novel communication protocol that grants transmission nodes different priorities for packet delivery based on the combinative information of wireless channel state, real-time buffer state, and packet delay. For the theoretical performance modeling, we built a delicate CDT bitmap structure to track the packet number and delay information in the buffer queues. After that, we applied the Markov chain theory to capture the state transitions of the CDT bitmap, which enables to model the communication QoS of the proposed communication protocol, i.e., ROP, PDP and achievable ST. The results in this work shed new insights into the design and performance analysis of the two-hop secure communication system.

CHAPTER V

Conclusions

This final chapter summarizes our contributions and points out several topics for future research.

5.1 Summary of Thesis

In this thesis, we studied the design of communication protocol to enhance the PHY security for two-hop buffer-aided relaying systems, where the instantaneous CSIs of eavesdropping channels are unavailable. We first designed the secure communication protocols for two-hop buffer-aided relaying systems with/without the CSI of the main channel at the transmitter. Then, we proposed the security/delay-aware communication protocol for two-hop buffer-aided relaying systems with the statistic CSIs of eavesdropping channels.

Chapter III investigated the secure communication in a two-hop cooperative wireless system, where a buffer-aided relay helps forward data from the source to destination, and a passive eavesdropper attempts to intercept data transmission from both the source and relay. Considering two communication scenarios, i.e., the instantaneous channel state information is available or unavailable at the source node, we designed two secure communication protocols without the CSIs of eavesdropping channels, respectively, to ensure both the PHY security and communication QoS.

In order to evaluate the system performance, we developed a general framework to derive the expressions of E2E SOP, throughput and ST. Based on the theoretical performance analysis, we further explored the performance optimization issues, revealing the insightful tradeoffs between transmission security and QoS. An iterative algorithm was developed to make sure that the proposed communication protocols can flexibly configure the link selection parameters to satisfy various system performance requirements. This work is very important and can serve as guidelines for the design of communication protocol in future wireless cooperative networks.

Chapter IV investigated the secure communication in a wireless relaying system, where the packet lifetime is limited, multiple buffer-aided relays help the source forward packets to the destination, and a passive eavesdropper attempts to wiretap the transmissions over both hops. We designed a novel security/delay-aware communication protocol to guarantee the end-to-end transmission security and timeliness. Based on the wireless channel state, real-time buffer state, and packet delay requirement, we grant the transmission nodes different priorities for packet delivery. In addition, to create more transmission opportunities, one of the idle relays is opportunistically selected as the jammer. For performance evaluation of the proposed protocol, we first built a delicate CDT bitmap structure to track the packet number and delay information in the buffer queues. After that, we then developed a Markov chain-based theoretical framework to fully characterize the packet delivery process in two hops. With the help of this framework, we further derived under two typical fading channel cases the closed-form expressions for three fundamental system performance metrics, namely reliable outage probability, packet discarding probability and achievable secrecy throughput. This work can serve as guidelines for the design of secure communication protocol in future delay-sensitive wireless networks. The established framework can shed new insights into the performance analysis in terms of the information discarding due to overdue for the two-hop cooperative communication system.

5.2 Future Works

The potential research directions to extend this thesis are summarized as follows.

- **Secure communication protocol for buffer-aided relaying systems with data arrival.** In this thesis, we mainly focus on the two-hop buffer-aided relaying system where the data of the source is backlog. However, in the actual network environment, the data of the source usually is received from other transmitters. So, one meaningful and interesting work is to design a secure communication protocol for buffer-aided relaying systems with data arrival. It's worth noting that, when selecting the transmission link or relay, the buffer state of both source and relays must be considered to avoid the packet overflows and empty transfers. Furthermore, the new communication protocol needs to balance the transmission opportunity between the first hop and second hop based on the arrival rate of the data. Besides, if the data timeliness is required, the delivery delay must be redefined as the difference between the time that the tagged data enters in the source queue and the time that the tagged data enters the destination queue.

- **Secure communication protocol with dynamic transmission power and secrecy rate for buffer-aided relaying systems.** In this thesis, we mainly consider the fixed transmission powers and secrecy rate to facilitate protocol design and theoretical analysis. However, when the main channels have low channel quality or the eavesdropping channels have high channel quality, the fixed transmission power and secrecy rate would result in the fact that the system has low-level information redundancy. Therefore, the system may waste a lot of transmission opportunities. If the transmission power and security rate can be adjusted dynamically, the system throughput and security throughput will be increased. However, how to design the communication protocol with dynamic transmission power and secrecy rate is still an open problem, due to the following reasons: 1) From the results in this thesis, we know that the throughput and secrecy throughput reach the maximum only when the system is in an equilibrium state, i.e., the probability of the relay receiving is equal to the probability of its transmitting, which is determined by the communication protocol. However, the transmission power and secrecy rate determine the communication protocol, and in turn, the communication protocol determines the dynamic adjustment of them. The coupling between them makes the design of communication protocol hard; 2) Intuitively, high-level security, throughput and secrecy throughput will result in higher power consumption. Thus, for the sake of fairness, one new performance metric, i.e., secrecy energy efficiency needs to be introduced, which increases the difficulty of the protocol design. Therefore, a new and dedicated communication protocol is deserved on dynamic transmission power and secrecy rate for secure communication, and the study of this topic is of great importance for the secrecy of the buffer-aided relaying systems.

- **Secure communication protocol with non-orthogonal multiple access (NOMA) for buffer-aided relaying systems.** Available communication protocols for secure two-hop buffer-aided relaying systems always select only one relay for the data transmission, while making most of the relay nodes remain idle during each transmission. The innovative concept of non-orthogonal multiple access (NOMA) has been proposed to support more users than the number of available orthogonal time-, frequency-, or code-domain resources. Thus, embedding the NOMA technique into the design of communication protocol can be capable of significantly reducing the transmission latency and increasing the secrecy throughput. On the one hand, the NOMA technique allows multiple relays to synchronously receive the data, which results in a lower waiting time of the data. On the other hand, it increases the amount of data that reaches the relay per unit time slot, and according to the law of conservation of fluid, the relay-destination link is allowed more transmission opportunities to facilitate the system to reach equilibrium. However, it is worth noting that: 1) the interference among the relays will affect the selection of receiving relays and their optimal number; 2) the power allocation and decoding order also need to be thoughtfully considered.

APPENDICES

APPENDIX A

Proofs in Chapter III

A.1 Proof of Lemma 2

Regarding the case of AR transmission mechanism, according to Algorithm 1, the probability P_A that Alice is selected to transmit message at a time slot can be calculated as

$$\begin{aligned} P_A &= \Pr\{I_k = 0\} = \Pr\left\{\gamma_{a,r}[k] \geq \max\left\{\alpha, \frac{\alpha\gamma_{r,b}[k]}{\beta}\right\}\right\} \\ &= \Pr\left\{\gamma_{a,r}[k] \geq \alpha, \gamma_{r,b}[k] < \beta\right\} + \Pr\left\{\gamma_{a,r} \geq \frac{\alpha\gamma_{r,b}}{\beta}, \gamma_{r,b} \geq \beta\right\} \\ &= \left(\int_0^\beta \int_\alpha^\infty + \int_\beta^\infty \int_{\alpha y/\beta}^\infty\right) f_{\bar{\gamma}_{a,r}}(x) f_{\bar{\gamma}_{r,b}}(y) dx dy \\ &= \mu(\alpha, \beta). \end{aligned} \tag{A.1}$$

Regarding the case of FR transmission mechanism, the expression of P_A changes with the relationship between α and $2^{R_a} - 1$. According to Algorithm 2, when we set $\alpha \geq 2^{R_a} - 1$, we have $P_A = \Pr\left\{\gamma_{a,r}[k] \geq \max\left\{\alpha, \frac{\alpha}{\beta}\gamma_{r,b}[k]\right\}\right\} = \mu(\alpha, \beta)$; when we set

$\alpha < 2^{R_a} - 1$, then we have

$$\begin{aligned} P_A &= \Pr\left\{\gamma_{a,r}[k] \geq \max\left\{2^{R_a} - 1, \frac{\alpha\gamma_{r,b}[k]}{\beta}\right\}\right\} \\ &= \Pr\left\{\gamma_{a,r}[k] \geq \frac{\alpha\gamma_{r,b}[k]}{\beta}, \gamma_{r,b}[k] \geq \frac{\beta(2^{R_a} - 1)}{\alpha}\right\} \\ &\quad + \Pr\left\{\gamma_{a,r}[k] \geq 2^{R_a} - 1, \gamma_{r,b}[k] < \frac{\beta(2^{R_a} - 1)}{\alpha}\right\} \\ &= \left(\int_{\beta(2^{R_a}-1)/\alpha}^{\infty}\int_{\alpha y/\beta}^{\infty} + \int_{0}^{\beta(2^{R_a}-1)/\alpha}\int_{2^{R_a}-1}^{\infty}\right) f_{\bar{\gamma}_{a,r}}(x) f_{\bar{\gamma}_{r,b}}(y)\,dx\,dy \\ &= \nu(\alpha, \beta), \end{aligned} \tag{A.2}$$

where $f_{\bar{\gamma}_{a,r}}(x)$ and $f_{\bar{\gamma}_{r,b}}(y)$ denote the probability density functions of $\bar{\gamma}_{a,r}$ and $\bar{\gamma}_{r,b}$, respectively.

A.2 Proof of Corollary 2

From expressions (3.11) and (3.12) we have

$$\frac{\partial\mu}{\partial\alpha} = -\frac{\exp\left(-\frac{\alpha}{\bar{\gamma}_{a,r}}\right)}{\bar{\gamma}_{a,r}}\left[1 - \frac{\alpha\bar{\gamma}_{r,b}\exp\left(-\frac{\beta}{\bar{\gamma}_{r,b}}\right)}{\alpha\bar{\gamma}_{r,b} + \beta\bar{\gamma}_{a,r}}\right] - \frac{\beta\bar{\gamma}_{a,r}\bar{\gamma}_{r,b}\exp\left(-\frac{\alpha}{\bar{\gamma}_{a,r}}\right)}{(\alpha\bar{\gamma}_{r,b} + \beta\bar{\gamma}_{a,r})^2} < 0, \tag{A.3}$$

$$\frac{\partial\nu}{\partial\alpha} = -\left[\frac{\beta\bar{\gamma}_{a,r}\bar{\gamma}_{r,b}}{(\alpha\bar{\gamma}_{r,b}+\beta\bar{\gamma}_{a,r})^2} + \frac{(2^{R_a-1})\beta}{\alpha\bar{\gamma}_{r,b}(\alpha\bar{\gamma}_{r,b}+\beta\bar{\gamma}_{a,r})}\right]\exp\left(-\frac{2^{R_a-1}}{\bar{\gamma}_{a,r}} - \frac{\beta(2^{R_a-1})}{\alpha\bar{\gamma}_{a,r}}\right) < 0. \tag{A.4}$$

From expressions (3.14) and (3.15) we have $\frac{\partial\bar{\mu}}{\partial\alpha} > 0$ and $\frac{\partial\bar{\nu}}{\partial\alpha} > 0$. Thus, for any given β and R_s, as α increases, P_A monotonically decreases while P_R monotonically increases.

Assuming there is, if any, α^* which makes $P_A^* = P_R^*$ for the given β and R_s, then for $\alpha > \alpha^*$ we have $P_A(\alpha) < P_A^*$ and thus $\Phi(\alpha) = P_A(\alpha) \cdot R_s < \Phi^* = P_A^* \cdot R_s$; for $\alpha < \alpha^*$ we have $P_A(\alpha) < P_A^*$ and thus $\Phi(\alpha) = P_A(\alpha) \cdot R_s < \Phi^* = P_A^* \cdot R_s$. It indicates that for any given β and R_s, when Φ reaches its maximum, we have $P_A = P_R$.

Similarly, by solving partial derivatives we can verify that for any given α and R_s, as β increases, P_A monotonically increases while P_R monotonically decreases. Through similar arguments we know that for any given α and R_s, when $\mathit{\Phi}$ reaches its maximum, there is $P_A = P_R$.

Therefore, we can conclude that $P_A = P_R$ is a necessary condition for the throughput $\mathit{\Phi}$ reaching its maximum. Notice that $P_A = P_R$ indicates the arrival rate equals to the service rate for the Relay queue, in Queuing Theory, such a case is called at the edge of non-absorbing state.

A.3 Proof of Lemma 3

According to [62, 63], $\mathbf{d}$ is the descent direction of $\Psi(\mathbf{x}^{(n)})$ if and only if $\mathbf{d}^T \nabla \Psi(\mathbf{x}^{(n)}) < 0$ at the point $\mathbf{x}^{(n)}$. Furthermore, if $\mathbf{d}^T \nabla g_i(\mathbf{x}^{(n)}) < 0$ holds at $\mathbf{x}^{(n)}$, $\mathbf{d}$ is called the strictly feasible direction. Therefore, in order to find a feasible descent direction at $\mathbf{x}^{(n)}$, we only need to find out $\mathbf{d}^{(n)}$ and the minimum value of σ which satisfy the constraints (3.43b)-(3.43d). $\mid \mathbf{d}_j \mid \leq 1$ is added to guarantee a finite optimal solution. Thus, finding a feasible descent direction can be formulated as the linear programming problem (3.43).

APPENDIX B

Proofs in Chapter IV

B.1 Proof of Proposition 1

When no jammer is adopted in the given time slot n, Source s forwards the confidential data to node m at the rate of channel capacity while being eavesdropped by e. Then, the instantaneous secrecy rate [10] of system is given by

$$\begin{aligned} R_{sec}[n] &= C_{s,m}[n] - C_{m,e}[n] \\ &= \log_2\left(1 + \frac{P_s g_{s,m}[n]}{\delta_m^2}\right) - \log_2\left(1 + \frac{P_s g_{i,e}[n]}{\delta_e^2}\right), \end{aligned} \tag{B.1}$$

where $C_{s,m}[n]$ and $C_{m,e}[n]$ are the instantaneous channel capacity of transmission and eavesdropping link, respectively. The SOP can be derived as

$$\begin{aligned} P_{so} &= \mathbb{P}(R_{sec}[n] \leq R_s) \\ &\approx \mathbb{P}\left(\log_2\left(\frac{g_{s,m}[n]}{g_{m,e}[n]}\right) \leq R_s\right) = \exp\left(-\frac{g_{s,m}[n] 2^{R_s}}{\Omega_{m,e}}\right). \end{aligned} \tag{B.2}$$

Letting $P_{so} \leq P_{up}$, we can obtain $g_{s,m}[n] \geq 2^{-R_s}\Omega_{s,e} \ln P_{up}$. When relay k is selected as a jammer, the secrecy rate at time slot n is given by

$$\begin{aligned} R_{sec}[n] &= C_{s,m}[n] - C_{m,e}[n] \\ &= \log_2\left(1 + \frac{P_s g_{s,m}[n]}{\delta_m^2 + \beta_m P_k g_{k,m}[n]}\right) - \log_2\left(1 + \frac{P_s g_{s,e}[n]}{\delta_e^2 + P_k g_{k,e}[n]}\right) \end{aligned} \tag{B.3}$$

Similarly, the SOP of system can be derived as

$$P_{so} = \mathbb{P}(R_{sec}[n] \leq R_s) \tag{B.4}$$

$$\begin{aligned} &\approx \mathbb{P}\left(\log_2\left(\frac{g_{s,m}[n]g_{k,e}[n]}{\beta_m g_{k,m}[n]g_{s,e}[n]}\right) \leq R_s\right) \\ &= \int_0^\infty \int_0^{\left(2^{R_s}\beta_m g_{k,m}[n]x\right)/(g_{s,m}[n])} f_{g_{k,e}}(y) f_{g_{s,e}}(x) dydx. \end{aligned} \tag{B.5}$$

Letting $P_{so} \leq P_{up}$, we can obtain $g_{s,m}[n] \geq g_{k,m}[n]\Xi_{sk}^m$. For the second hop, we can obtain $g_{m,d}[n] \geq g_{k,d}[n]\Xi_{mk}^d$ by the similar proof.

B.2 Proof of Theorem IV.1

Based on the proposed communication protocol, the concerned system is outage only when all channel quality does not satisfy the condition (4.3) and (4.4). First, we derive the probability that all $m \to d$ links are outage in state S_i. Note that only non-empty relays can be selected to transmit data, such that $\Theta_{id}^{DSI} = 1$ when $G_i^{DSI}(d) = 0$. When $G_i^{DSI}(d) \neq 0$, the probability that $m \to d$ link is outage in state S_i is given by

$$\Theta_{id}^{DSI} = \mathbb{P}(g_{m,d} < \theta_m \wedge g_{m,d} < \min_{k \in \mathcal{M}/m} \{g_{k,d}\Xi_{mk}^d\}) \tag{B.6}$$

Then, by doing some numerical calculations and simplification on (B.6), we can obtain the result (4.19). Since every oldest packet in each relay buffer has different delay information d, d can be on behalf of each $m \to d$ link. Therefore, the probability that all $m \to d$ links are outage in state S_i is denoted as $\prod_{d=1}^{\tau-1} \Theta_{id}^{DSI}$.

Apparently $G_{il}^{PNI} = 1$ when $G_i^{PNI}(l) = 0$. Similarly, when $G_i^{PNI}(l) \neq 0$, we have

$$\Theta_{il}^{PNI} = \mathbb{P}(g_{s,m} < \theta_s \wedge g_{s,m} < \min_{k \in \mathcal{M}/m} \{g_{k,m} \Xi_{sk}^m\}) \tag{B.7}$$

Different from the above case, because different relays may own the same packet number, the packet number l in the buffer of relay m cannot uniquely represent the $s \to m$ link. Thus, for each l, we need to find out all $s \to m$ links which satisfy $\psi(U_m^i) = l$, i.e., $\forall sm \in \mathbb{G}_l^{PNI}$. After some numerical calculations and simplification on (B.7), we can obtain the result (4.24). Thus, the probability that all $s \to m$ links are outage in state S_i is denoted as $\prod_{l=0}^{\tau-1} \Theta_{il}^{PNI}$.

Eventually, the probability that the concerned system is outage in state S_i is denoted as $\prod_{d=1}^{\tau-1} \Theta_{id}^{DSI} \prod_{l=0}^{\tau-1} \Theta_{il}^{PNI}$.

B.3 Proof of Theorem IV.2

According to Algorithm 5, the relay is given higher priority than source on packet transmission due to lifetime constraint. Therefore, source can be selected to transmit packet only when all $m \to d$ links are outage, and there would be four cases.

Case 1: The selected relay is m^* and the packet number in its buffer is 0, i.e., $\mathcal{D} = m^* \wedge l^* = 0$. The elements of $\mathbb{G}_{l^*}^{PNI}$ are divided into two categories, one belongs to the subset $\mathcal{G}_{l^*}^{sm^*}$ (i.e., $sm \in \mathcal{G}_{l^*}^{sm^*}$) whose channel quality satisfies the condition (4.3), the other one belongs to the subset $\mathcal{G}_{l^*}^{sm^*}$ but not to the set $\mathbb{G}_{l^*}^{PNI}$ (i.e., $s\hat{m} \notin \mathcal{G}_{l^*}^{sm^*}$ and $s\hat{m} \in \mathbb{G}_{l^*}^{PNI}$), and theirs channel quality dose not satisfy the condition (4.3). Note that for different sets of $\mathcal{G}_{l^*}^{sm^*}$, the probabilities that $s \to m^*$ link is selected for transmission leading to the state transition from S_i to S_j have different values. Therefore, we need to find out all possible subsets of $\mathbb{G}_{l^*}^{PNI}$ that each contains the link $s \to m^*$. Overall, when $\mathcal{D} = m^* \wedge l^* = 0$, the probability that the source transmission leads to the connected state S_j can be formulated as

$$A_{i,j}^{i.n.d} = \sum_{\mathcal{G}_{l^*}^{sm^*}} \frac{1}{|\mathcal{G}_{l^*}^{sm^*}|} \mathbb{P}\Big(g_{sm} \geq \theta_s, \forall sm \in \mathcal{G}_{l^*}^{sm}\Big) \mathbb{P}\Big(g_{s\hat{m}} < \theta_s, \forall s\hat{m} \in \mathbb{G}_{l^*}^{PNI} \backslash \mathcal{G}_{l^*}^{sm}\Big) \prod_{d=1}^{\tau-1} \Theta_{id}^{DSI} \tag{B.8}$$

where the term $1/|\mathcal{G}_{l^*}^{sm^*}|$ is due to the fact that we select one of them uniformly when $\mathcal{G}_{l^*}^{sm^*}$ consists of multiple elements and $\prod_{d=1}^{\tau-1} \Theta_{id}^{DSI}$ is the probability that all $m \to d$ links are outage.

Case 2: The selected relay is m^* and the packet number in its buffer is $0 < l^* < \tau - 1$, i.e., $\mathcal{D} = m^* \wedge 0 < l^* < \tau - 1$. Based on Algorithm 1, the fewer packets the relay owns, the higher priority it is selected as the receiver. Thus, only when the quality of these $s \to m$ links does not satisfy the condition (4.3) where the involved relays own fewer packets than m^*, i.e., $\psi(U_m^i) \in [0, l^* - 1]$. Thus, when $\mathcal{D} = m^* \wedge 0 < l^* < \tau - 1$, the probability that the source transmission leads to the connected state S_j can be formulated as

$$\begin{aligned} A_{i,j}^{i.n.d} = \sum_{\mathcal{G}_{l^*}^{sm^*}} \frac{1}{|\mathcal{G}_{l^*}^{sm^*}|} \prod_{sm \in \mathcal{G}_{l^*}^{sm^*}} \mathbb{P}(g_{s,m} \geq \theta_s) \prod_{s\hat{m} \in \mathbb{G}_{l^*}^{PNI} \backslash \mathcal{G}_{l^*}^{sm^*}} \mathbb{P}(g_{s,\hat{m}} \geq \theta_s) \\ \times \mathbb{P}\Big(g_{s,m} < \theta_s, \forall sm \in \mathbb{G}_l^{PNI} \wedge 0 \leq l \leq l^* - 1\Big) \prod_{d=1}^{\tau-1} \Theta_{id}^{DSI}. \end{aligned} \tag{B.9}$$

Case 3: The selected partner pair is (m^*, k) and the packet number in its buffer is $l^* = 0$, i.e., $\mathcal{D} = (m^*, k) \wedge l^* = 0$. Notice that we would select one idle relay as the cooperative jammer only when the quality of all $s \to m$ links does not satisfy the condition (4.3). So, when the relays m^* and k are selected as the partner pair, there have three-level meanings: 1) the channel gains of these $s \to m$ links where the involved relays have the non-empty buffers, i.e., $\psi(U_m^i) \geq 1$, must satisfy the condition $\theta_s > g_{s,m}$; 2) the channel gains of $s \to m^*$ and $m^* \to k$ links must satisfy the condition $\theta_s > g^{s,m^*} \geq g_{k,m^*}\Xi_{sk}^{m^*}$ and $g_{k,m^*}\beta_{m^*} \leq \min_{m \neq m^*,k}\{g_{m,m^*}\beta_{m^*}\}$; 3) for other relays which own the empty buffer, i.e., $\bar{m} \in \mathbb{G}_{l^*}^{PNI} \wedge \bar{m} \neq m^*$, we have $\theta_s > g_{s,\bar{m}}$ and $g_{k,m^*}\beta_{m^*} < \min_{\hat{m} \neq \bar{m}}\{g_{\hat{m},\bar{m}}\beta_{\bar{m}}\}$. Thus, when $\mathcal{D} = (m^*, k) \wedge l^* = 0$, the probability that the source transmission leads to the connected state S_j can be formulated as

$$A_{i,j}^{i.n.d} = \prod_{l=1}^{\tau-1} \mathbb{P}(g_s^m < \theta_s) \prod_{d=1}^{\tau-1} \Theta_{id}^{DSI}\ \mathbb{P}\Big(g_s^m < \theta_s, \bar{m} \in \mathbb{G}_{l^*}^{PNI} \wedge m \neq m^*\Big)$$
$$\mathbb{P}\left(\Big(\theta_s > g_{sm^*} \geq g_{km^*}\Xi_{sk}^{m^*}\Big) \wedge g_k^{m^*}\beta_{m^*} \leq \min\left\{\min_{\substack{\bar{m} \in \mathbb{G}_{l^*}^{PNI}/m^* \\ \hat{m} \neq \bar{m}}}\{g_{\hat{m}\bar{m}}\beta_{\bar{m}}\}, \min_{m \neq m^*,k}\{g_{mm^*}\beta_{m^*}\}\right\}\right). \tag{B.10}$$

Case 4: The selected partner pair is (m^*, k) and the packet number in its buffer is $0 < l^* < \tau - 1$, i.e., $\mathcal{D} = (m^*, k) \wedge 0 < l^* < \tau - 1$. The difference between this case and Case 3 is that all $s \to m$ links are outage where the number of the packets in the buffer of the involved relay m is less than l^*. Similar to the Case 3, the probability that the source transmission leads to the connected state S_j can be formulated as

$$A_{i,j}^{i.n.d} = \prod_{l=1}^{\tau-1} \mathbb{P}(g_{sm} < \theta_s) \prod_{d=1}^{\tau-1} \Theta_{id}^{DSI}\ \mathbb{P}\Big(g_{s,m} < \theta_s, \bar{m} \in \mathbb{G}_{l^*}^{PNI} \wedge m \neq m^*\Big) \prod_{l=0}^{l*-1} \Theta_{il}^{PNI}$$
$$\mathbb{P}\left(\Big(\theta_s > g_{sm^*} \geq g_{k,m^*}\Xi_{sk}^{m^*}\Big) \wedge g_k^{m^*}\beta_{m^*} \leq \min\left\{\min_{\substack{\bar{m} \in \mathbb{G}_{l^*}^{PNI}/m^* \\ \hat{m} \neq \bar{m}}}\{g_{\hat{m},\bar{m}}\beta_{\bar{m}}\}, \min_{m \neq m^*,k}\{g_{m,m^*}\beta_{m^*}\}\right\}\right). \tag{B.11}$$

Overall, the state transition caused by the source transmission from state S_i to state S_j under the proposed communication protocol only have the above four cases. Therefore, by some numerical calculations and simplification on the formulas (B.8)-(B.11), we can derive $A_{i.j}$ as the result (4.31).

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] M. Agiwal, A. Roy, and N. Saxena, “Next generation 5G wireless networks: A comprehensive survey,” *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1617–1655, Feb. 2016.

[2] 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, May 2016.

[3] W. Stallings and M. P. Tahiliani, *Cryptography and network security: principles and practice*, 4th ed. Prentice Hall, Jan. 2014.

[4] B. Schneier, “Cryptographic design vulnerabilities,” *IEEE Computer*, vol. 31, no. 9, pp. 29–33, Sept. 1998.

[5] J.-P. Aumasson, “The impact of quantum computing on cryptography,” *Computer Fraud & Security*, vol. 2017, no. 6, pp. 8–11, Jun. 2017.

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

[7] J. Barros and M. R. Rodrigues, “Secrecy capacity of wireless channels,” in *Proc. IEEE International Symposium on Information Theory (ISIT)*, Jul. 2006, pp. 356–360.

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

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

[10] P. K. Gopala, L. Lai, and H. E. Gamal, “On the Secrecy Capacity of Fading Channels,” *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Sept. 2008.

[11] L. J. Rodríguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, “Physical layer security in wireless cooperative relay networks: state of the art and beyond,” *IEEE Commun. Mag.*, no. 12, pp. 32–39, Dec. 2015.

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

[13] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[14] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

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

[16] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[17] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE ISIT*, Adelaide, Australia, Sept. 2005, pp. 2152–2155.

[18] L. Lai and H. El Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Aug. 2008.

[19] T. Lv, H. Gao, and S. Yang, "Secrecy transmit beamforming for heterogeneous networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 6, pp. 1154–1170, Jun. 2015.

[20] 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 Trans. Signal Process.*, vol. 65, no. 3, pp. 677–689, Feb. 2017.

[21] Z. Sheng, H. D. Tuan, T. Q. Duong, and H. V. Poor, "Beamforming optimization for physical layer security in miso wireless networks," *IEEE Trans. Signal Process.*, vol. 66, no. 14, pp. 3710–3723, Jul. 2018.

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

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

[24] ——, "Secure degrees of freedom of one-hop wireless networks," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3359–3378, Jun. 2014.

[25] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of ldpc codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

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

[27] O. O. Koyluoglu, A. S. Rawat, and S. Vishwanath, "Secure cooperative regenerating codes for distributed storage systems," *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5228–5244, Sept. 2014.

[28] Y. Zou, X. Li, and Y.-C. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE J. Sel.Areas in Commun.*, vol. 32, no. 11, pp. 2222–2236, Nov. 2014.

[29] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 215–228, Jan 2015.

[30] 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, May 2015.

[31] L. Yang, J. Chen, H. Jiang, S. A. Vorobyov, and H. Zhang, "Optimal relay selection for secure cooperative communications with an adaptive eavesdropper," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 26–42, Jan. 2017.

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

[33] A. El Shafie, A. Sultan, and N. Al-Dhahir, "Physical-layer security of a buffer-aided full-duplex relaying system," *IEEE Commun. Letters*, vol. 20, no. 9, pp. 1856–1859, Sept. 2016.

[34] J. Wan, D. Qiao, H. Wang, and H. Qian, "Buffer-aided two-hop secure communications with power control and link selection," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7635–7647, Nov. 2018.

[35] D. Wang, P. Ren, and J. Cheng, "Cooperative secure communication in two-hop buffer-aided networks," *IEEE Trans. Commun.*, vol. 66, no. 3, pp. 972–985, Nov. 2018.

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

[37] N. Nomikos, T. Charalambous, I. Krikidis, D. N. Skoutas, D. Vouyioukas, M. Johansson, and C. Skianis, "A survey on buffer-aided relay selection," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1073–1097, Dec. 2015.

[38] A. El Shafie, D. Niyato, and N. Al-Dhahir, “Enhancing the phy-layer security of mimo buffer-aided relay networks,” vol. 5, no. 4. IEEE, 2016, pp. 400–403.

[39] X. Tang, Y. Cai, Y. Huang, T. Q. Duong, W. Yang, and W. Yang, “Secrecy outage analysis of buffer-aided cooperative mimo relaying systems,” *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2035–2048, Mar. 2017.

[40] 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, Apr. 2019.

[41] Y. Zhao, H. Chen, L. Xie, and K. Wang, “Secrecy throughput optimization in the buffer-aided mimo full-duplex relaying system,” in *30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC).* IEEE, 2019, pp. 1–6.

[42] V. Jamali, N. Zlatanov, and R. Schober, “Bidirectional buffer-aided relay networks with fixed rate transmission—part ii: Delay-constrained case,” *IEEE Trans. Wireless Commun.*, vol. 14, no. 3, pp. 1339–1355, Mar. 2015.

[43] 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 Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1893–1906, Dec. 2018.

[44] Q. Du and Y. Xu, “Secure transmission for buffer-aided relay networks with delay constraints,” in *Computing, Communications and IoT Applications (ComComAp).* IEEE, Oct. 2019, pp. 259–264.

[45] C. Wei, Z. Yin, W. Yang, and Y. Cai, “Enhancing physical layer security of DF buffer-aided relay networks with small buffer sizes,” *IEEE Access*, vol. 7, pp. 128 684–128 693, Sept. 2019.

[46] 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, Mar. 2020.

[47] J. He, J. Liu, Y. Xu, and X. Jiang, “Buffer-aided relaying for two-hop secure communication with limited packet lifetime,” in *Proc. IEEE 20th HPSR*, Xi’An, China, May 2019, pp. 1–7.

[48] J. He, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, “Link selection for security-QoS tradeoffs in buffer-aided relaying networks,” *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1347–1362, Sept. 2019.

[49] E. Arikan, “Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels,” *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.

[50] N. Zlatanov and R. Schober, "Buffer-aided relaying with adaptive link selection—fixed and mixed rate transmission," *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 2816–2840, May 2013.

[51] N. Zlatanov, R. Schober, and P. Popovski, "Buffer-aided relaying with adaptive link selection," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 8, pp. 1530–1542, Aug. 2013.

[52] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Commun. Lett.*, vol. 16, no. 6, pp. 878–881, Apr. 2012.

[53] R. Tanbourgi, H. S. Dhillon, J. G. Andrews, and F. K. Jondral, "Effect of spatial interference correlation on the performance of maximum ratio combining," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3307–3316, Jun. 2014.

[54] O. Güngör, J. Tan, C. E. Koksal, H. E. Gamal, and N. B. Shroff, "Secrecy outage capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5379–5397, Aug. 2013.

[55] M. Neiman, "The principle of reciprocity in antenna theory," *Proceedings of the IRE*, vol. 31, no. 12, pp. 666–671, Aug. 1943.

[56] H. Daduna, *Queueing Networks with Discrete Time Scale: Explicit Expressions for the Steady State Behavior of Discrete Time Stochastic Networks.* Springer Verlag, 2001.

[57] C. Zhang, Y. Song, Y. Fang, and Y. Zhang, "On the price of security in large-scale wireless ad hoc networks," *IEEE/ACM Trans. Netw.*, vol. 19, no. 2, pp. 319–332, Apr. 2011.

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

[59] Y. Xu, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, "Physical layer security-aware routing and performance tradeoffs in ad hoc networks," *Computer Networks*, vol. 123, pp. 77–87, May. 2017.

[60] Y. Xu, J. Liu, Y. Shen, X. Jiang, and T. Taleb, "Security/qos-aware route selection in multi-hop wireless ad hoc networks," in *IEEE International Conference on Communications, (ICC)*, May. 2016, pp. 1–6.

[61] D. P. Bertsekas, *Nonlinear programming.* Athena scientific Belmont, 1999.

[62] D. M. Topkis and A. F. Veinott, Jr, "On the convergence of some feasible direction algorithms for nonlinear programming," *SIAM Journal on Control*, vol. 5, no. 2, pp. 268–279, Aug. 1967.

[63] S. Boyd and L. Vandenberghe, *Convex optimization.* Cambridge university press, 2004.

[64] J. He. (Dec. 2019) Matlab Simulator for Link Selection for Secure Cooperative Networks with Buffer-Aided Relaying. [Online]. Available: https://github.com/Future-heji/research/tree/Future-heji-patch-2

[65] Z. Tian, G. Chen, Y. Gong, Z. Chen, and J. A. Chambers, "Buffer-aided max-link relay selection in amplify-and-forward cooperative networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 2, pp. 553–565, May. 2014.

[66] O. Gungor, J. Tan, C. E. Koksal, H. El-Gamal, and N. B. Shroff, "Secrecy outage capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5379–5397, Aug. 2013.

[67] J. R. Norris, *Markov Chains*, 2nd ed. U.K. Cambridge Univ. Press, 1998.

[68] I. Krikidis, T. Charalambous, and J. S. Thompson, "Buffer-aided relay selection for cooperative diversity systems without delay constraints," *IEEE Trans. Wireless Commun.*, vol. 11, no. 5, pp. 1957–1967, Apr. 2012.

PUBLICATIONS

PUBLICATIONS

Journal Articles

[1] Ji He, Jia Liu, Yulong Shen, Xiaohong Jiang, and Norio Shiratori, Link Selection for Security-QoS Tradeoffs in Buffer-Aided Relaying Networks, *IEEE Transactions on Information Forensics and Security*, Vol. 15, pp. 1347-1362, Sept. 2019.

[2] Ji He, Jia Liu, Yulong Shen, Xinghui Zhu, Xiaohong Jiang, and Norio Shiratori, Secure and Delay-aware Communication in Buffer-aided Relaying Networks with Limited Packet Lifetime, *IEEE Transaction on Communication*, 2020. (Under Review)

Conference Papers

[3] Ji He, Yuanyu Zhang, Yulong Shen, and Xiaohong Jiang, Link selection for secure two-hop transmissions in buffer-aided relay wireless networks, 2016 International Conference on Networking and Network Applications (NaNA 2016), Hakodate, Japan, 2016, pp. 64-68.

[4] Ji He, Jia Liu, Yang Xu, and Xiaohong 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), Xi'an, China, 2019, pp. 1-7.