Physical Layer Security Performance Study for Two-Hop Wireless Networks with Buffer-Aided Relay Selection

by

Xuening Liao

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, 2018

To my family

ABSTRACT

Physical Layer Security Performance Study for Two-Hop Wireless Networks with Buffer-Aided Relay Selection

by

Xuening Liao

As wireless communication technologies continue to evolve rapidly, an unprecedented amount of sensitive information, such as financial data, physical health details and personal profile data, are transmitted through various wireless networks. However, the broadcast nature of wireless medium makes it difficult to shield these sensitive information from unauthorized users (eavesdroppers), and thus securing wireless communication is becoming an increasingly urgent demand. Physical layer (PHY) security has been proposed as one promising technology to provide security guarantee for wireless communications, owing to its unique advantages over traditional cryptography-based mechanisms, like an everlasting security guarantee and no need for costly secret key distribution/management and complex encryption algorithms. This thesis therefore focuses on the PHY security performance study for two-hop wireless networks with buffer-aided relay selection (a typical PHY security technique), where relay buffers will be adopted to help the transmission of the message.

We first investigate the security-delay trade-off of the buffer-aided relay selection scheme in a two-hop wireless network with multiple randomize-and-forward (RF) re-

lays where different codebooks are used at the source and the relays respectively. To evaluate the security and delay performances of the system, we derive analytical expressions for the end-to-end (E2E) secure transmission probability (STP) and the expected E2E delay under both perfect and partial eavesdropper channel state information (CSI) cases. These analytical expressions help us to explore the inherent trade-off between the security and delay performances of the concerned system. In particular, the results in this thesis indicate that: 1) the maximum E2E STP increases as the constraint on the expected E2E delay becomes less strict, and such trend is more sensitive to the variation of the number of relays than that of the relay buffer size; 2) on the other hand, the minimum expected E2E delay tends to decrease when a less strict constraint on E2E STP is imposed, and this trend is more sensitive to the variation of the relay buffer size than that of the number of relays. This work is very important and can really reflect the interplay between the overall security and delay performances of two-hop wireless networks with RF relays.

We then investigate the PHY security performances of two-hop wireless networks with multiple decode-and-forward (DF) relays where the same codebook is adopted at the source and the relays, for which we extend the buffer-aided relay selection with RF relays and propose a new buffer-aided relay selection scheme to resist the combining decoding of the signals by the eavesdropper in two-hop wireless networks with DF relays. To validate the efficiency of the new scheme, a theoretical framework is developed to analyze the E2E delivery process of a packet. Based the theoretical framework, we derive the closed form of the security and delay performances in terms of the E2E STP and the expected E2E delay. Then, extensive numerical results are conducted to validate the efficiency of the new buffer-aided relay selection scheme, and to explore the security-delay trade-off issue of the achievable E2E STP (expected E2E delay) region under a given expected E2E delay (E2E STP) constraint. Finally, comparisons are made between the new buffer-aided relay selection scheme and the

conventional Max-Ratio scheme, and results show that our new scheme outperforms the Max-Ratio buffer-aided relay selection scheme in terms of the E2E STP. This work can provide theoretical models for the E2E security and delay performances of two-hop wireless networks with DF relays, and can be employed as guidelines for the design of future networks.

ACKNOWLEDGEMENTS

During my three-year doctoral career in Future University Hakodate, I would like to express my sincere thanks to all who provided me love and encouragement. The thesis would not have been possible without all their help. The experience here is certainly one of the most important and wonderful one which I will never forget in the rest of my life.

First and foremost, I would like to thank my advisor Professor Xiaohong Jiang, not only for his the financial support for me, but also for his encouragement and guidance on my research. It is honorable for me to be one of his students and I learned a lot from him which is very helpful for me to deal with difficulties in my life. During my studying here, he and his wife, Mrs Li, gave a lot of care for me, which made me very worm. The life in Hakodate would be very hard without the help of them.

Besides, I would like to thank Yuanyu Zhang for his help with my research. He gave me many good advices during the research to make the quality of my papers better. I also thank other members in our laboratory Xiaolan Liu, Lisheng Ma, Bo Liu, Wu Wang, Jia Liu, Ji He, Yongchao Dang, Huihui Wu and Xiaochen Li for their help with this thesis.

I would also like to acknowledge my thesis committee members, Professor Yuichi Fujino, Professor Hiroshi Inamura and Professor Masaaki Wada, for their constructive comments that help to improve the quality of my thesis.

I would also like to give my sincere thanks to Professor Zhenqiang Wu of Shaanxi

Normal University, China, who gave me the chance to do research in Hakodate with Professor Jiang and other members in Professor Zhenqiang Wu's laboratory. He is the person who encouraged me to see a different world and try new things, and showed me the way to be a better researcher.

Last but the least. I would like to thank my family. I would like to thank my parents, whose love and guidance are with me in whatever I peruse and also my brothers for their love for me. Specially, I would like to thank for my boyfriend Lu He who gave me unconditional support such that I have the courage to face any difficulties.

TABLE OF CONTENTS

LIST OF FIGURES

Figure

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

As wireless communication technologies continue to evolve rapidly, an unprecedented amount of sensitive information, such as financial data, physical health details and personal profile, will be transmitted through various wireless networks in the near future [1]. However, the broadcast nature of wireless medium makes it difficult to shield these sensitive information from unauthorized users (eavesdroppers), and thus security of wireless communication is becoming an increasingly urgent demand [2].

Traditionally, security issue is addressed by cryptographic methods which utilize secret keys and encryption/decryption algorithms to ensure the security of the transmitted information above the physical layer [3], [4]. A key premise of these methods is that eavesdroppers have limited computational capability such that the encryption algorithms are computationally infeasible for them to decrypt without the secret keys [4]. Unfortunately, this premise has been challenged as eavesdroppers are becoming increasingly computationally powerful [5]. Recently, the technology of physical layer

(PHY) security, which secures information at the physical layer by exploiting the inherent randomness of wireless channels and noise, has attracted considerable attentions [6]. Compared to cryptographic methods, PHY security technology can enjoy the following major advantages. First, PHY security technology eliminates the costly secret key distribution/management and encryption/decryption algorithms in cryptographic methods, making it more suitable for resource-limited wireless networks [7]. Second, different from cryptographic methods, PHY security technology assumes no limitations for eavesdroppers in terms of the computational capability, making it completely immune to the rapid advances in computing power of eavesdroppers [7]. Third, unlike the computational security achieved by cryptographic methods, PHY security approaches can achieve the information-theoretic security [8], which is regarded as an everlasting security guarantee and can be quantified precisely by multiple criteria like secrecy rate [9], [10], secrecy throughput [11], [12], and secrecy outage probability [13], [14]. Therefore, PHY security technology has been recognized as a highly promising approach to provide a strong form of security guarantee for the next-generation wireless communication networks [15].

The first work regarding the PHY security is conducted by Wyner [16], who introduced the wiretap channel in his paper. In the wiretap model, three nodes are included: a transmitter, a receiver and an eavesdropper. The transmitter wishes to transmit secure information to the legitimate receiver over a noisy main channel, and the eavesdropper attempts to intercept the information transmitted over the main channel though another noisy channel, which is called the wiretap channel or eavesdropper channel. It has been revealed by Wyner in his paper that, when the main channel is better than the eavesdropper channel, a non-zero secrecy rate can be achieved. This result is of great importance as it proves that information can be secured without a secret key, which will greatly save the cost of key distribution and management in secure communications. Wyner's work was then generalized by Csizar

and Korner in [17], their results showed that a non-zero secrecy rate is also achievable even when the main channel is not better than the eavesdropper channel, and they proved that this can be achieved by exploiting the technique of channel prefix to inject additional randomness into both the main and the eavesdropper channels to create a better main channel over the eavesdropper channel. Following these two works, extensive research efforts have been devoted to studies on the PHY security techniques by exploiting the randomness of wireless channels and noise. These techniques mainly includes artificial noise injection/cooperative jamming [18–20], beam-forming [21–23], coding [24–26] and relay selection with or without the consideration of relay buffers [27–40], etc.

Artificial noise injection/cooperative jamming ensures the security of wireless networks by adopting the non-transmitting nodes to act as jammers to transmit jamming signals to the eavesdropper, such that the signals received at the eavesdropper can be degraded. According to the types of jamming signals, cooperative jamming can be classified into two categories. One is cooperative jamming with Gaussian noise jamming signal which will cause interference to both the legitimate receivers and the eavesdropper [18]. Another is cooperative jamming with jamming signal of the same codebook and the jamming signal is predefined with a certain structure and thus can be eliminated at the intended receiver [20]. For the first category of cooperative jamming, the jamming process can be conducted without the requirement of the eavesdropper's channel state information (CSI), while the legitimate channels may be affected by the jamming signals. For the second category of cooperative jamming, a better security performance can be obviously achieved. However, due to the requirement of a certain structure of the jamming signals, the construction of the codebook is very complex and it usually requires the jammer to be located closer to the eavesdropper than to the intended receiver, which is not always possible in practice, especially for eavesdroppers who only wiretap the legitimate channel and

transmit no information all over the time.

Beam-forming is usually exploited in the multiple-in-multiple-out (MIMO) network, where all nodes are equipped with antennas and one data stream can be transmitted to the intended receiver over multiple antennas. It enhances the security of information transmitted in the network by controlling the direction and strength of signal such that the signal is radiated towards the direction of the intended receiver, while receivers in other directions can hardly receive the signal [22]. It has been proved in [21] that beam-forming can maximize the secrecy capacity of wireless networks by optimizing the beam-forming weights at the source and relay nodes. However, this technique requires high coordinations (such as synchronization and central optimization) among the source and relay nodes, which usually needs high overhead in implementation, as a large amount of information will be exchanged between the nodes. Moreover, to obtain better efficiency, the design of cooperative jamming also requires the CSI of the eavesdropper channels.

Coding aims to improve the security of wireless networks based on the idea of stochastic encoding [24]. For each legitimate information, the coding technique encodes the legitimate message together with multiple protection messages which carry no information. First, it will randomly choose a protection message and then associates the legitimate information and the protection message together into a single codeword. If the legitimate channel is better than the eavesdropper channel, the protection message is designed detrimental enough to interfere with the eavesdropper, but can remains ensure the resolvability of the confidential message at the intended receiver. This technique can notably achieve high security performance of the network, but the constructing of the codebook is hard and even challenging. Similar to the majority of the above two PHY secuirty techniques, coding also requires the CSI knowledge of the eavesdropper channel.

The relay selection technique aims to improve the security of wireless networks

by choosing a relay (called message relay) with a strong legitimate link but a weak eavesdropper link. According to whether the relay buffers are introduced or not, relay selection can be divided into two categories, i.e., relay selection without buffers (traditional relay selection) [27–29] and relay selection with buffers (buffer-aided relay selection) [30–40]. For traditional relay selection, its transmission manner is prefixed, i.e., the source-relay-destination transmission manner. If a relay is selected, the transmission of the information can be finished in two consecutive time slots. In the first time slot, the source transmits the information to the message relay and the message relay will directly transmit the information to the destination in the next time slot even if the current transmission link is not secure enough for transmission. However, for the buffer-aided relay selection, if a relay is selected for transmission, it can store the information in its buffer to wait for a better transmission link. Thus, each information now may go through three processes, i.e., the source-relay transmission process, queuing process in a relay buffer and the relay-destination transmission process, and in each time slot, there are three possible transmission states, i.e., source-relay transmission, relay-destination transmission and no transmission. Compared with the traditional relay selection, authors in [33] showed that buffer-aided relay 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 relay selection technique is easy to be accomplished and it has no extra bad effect on the signals at the legitimate nodes, while the design of relay selection may also requires the CSI of the eavesdropper channel.

1.2 Objective and Main Works

This thesis adopts the buffer-aided relay selection with Gaussian noise to ensure the security of wireless communications, considering its possibility of being implemented in practice with different network scenarios. Our objective is to fully explore

the PHY security performances of buffer-aided relay selection for two-hop wireless networks. Towards this end, we first study the PHY security performances of buffer-aided relay selection scheme for two-hop wireless networks with randomize-and-forward (R-F) relays where eavesdropper can only decode the packet in two hops independently. We then investigate the PHY security performances of buffer-aided relay selection scheme for two-hop wireless networks with decode-and-forward (DF) relays where the same codebook is adopted at the source and the relay nodes, and the eavesdropper can thus decode the packet by combing the signals received in two hops. Two commonly-used PHY security performance metrics are of particular interest, which are the end-to-end (E2E) secure transmission probability (STP) and E2E delay [39]. E2E STP characterizes the probability of successfully transmitting a packet from the source to the destination and E2E delay defines the time slots it takes a packet to reach its destination after it is generated at the source node. The main works and contributions of this thesis are summarized in the following subsections.

1.2.1 PHY Security Performance Study of Buffer-Aided Relay Selection Scheme for Two-Hop Wireless Networks with RF Relays

This work focuses on the security-delay trade-off study of the buffer-aided relay selection scheme for two-hop wireless networks with RF relays. While existing works [30–37] regarding the security performance study of two-hop wireless networks with buffer-aided relay selection mainly derived security performance of a single link (Please refer to Section 2.1 for related works), the E2E security performance of such networks remains largely unexplored. Moreover, the delay issue has not been addressed yet. In this work, as a first step towards the study of E2E security and delay performances for two-hop wireless networks with buffer-aided relay selection, we study the E2E STP and E2E delay of a two-hop wireless network with one source-destination pair, multiple RF relays and an eavesdropper intercepting both

the source-relay and relay-destination links. We consider the Max-Ratio buffer-aided relay selection scheme to select the message relay for receiving packets from the source or forwarding packets to the destination node. The main contributions of this work can be summarized as follows:

- Analytical expressions for E2E secure transmission probability (STP) and expected E2E delay: we consider a two-hop relay system, which consists of a source-destination pair, one eavesdropper and multiple relays each having a finite buffer, and study the E2E security and delay performances of the system under both perfect and partial eavesdropper CSI cases. To derive the E2E performances, we develop a theoretical framework consisting of two Markov chains, here the first one characterizes the buffer states for a packet in its source-relay delivery process while the second one characterizes the buffer states for the packet in its relay-destination delivery process. With the help of the framework, the analytical expressions for the E2E STP and the expected E2E delay are derived to evaluate the security and delay performances of the system.

- Study on the security-delay trade-off: based on the analytical expressions on the E2E STP and expected E2E delay, we provide extensive numerical results to illustrate our theoretical findings. These results indicate that there is a clear trade-off between the E2E security performance and delay performance in the concerned system. For example, if we impose a larger upper bound (i.e., a less strict constraint) on the expected E2E delay, the maximum E2E STP (in terms of either relay buffer size or number of relays) tends to increase, and such trend is more sensitive to the variation of the number of relays than that of the relay buffer size. On the other hand, if we impose a smaller lower bound (i.e., a more strict constraint) on the E2E STP, the minimum expected E2E delay (in terms of either relay buffer size or number of relays) tends to decrease, and this trend

is more sensitive to the variation of the relay buffer size than that of the number of relays.

With this work, we can further explore the overall interplay between the PHY security security and the delay performances for two-hop wireless networks with buffer-aided relay selection, which is of great importance for the design of future networks.

1.2.2 PHY Security Performance Study of Buffer-Aided Relay Selection Scheme for Two-Hop Wireless Networks with DF Relays

The available buffer-aided relay selection schemes consider mainly the networks with RF relays (Please refer to Section 2.1 for related works), which may significantly limit their applications to wireless networks with DF relays where the eavesdropper can decode the information by combining the signals received in two hops. This work considers a new two-hop wireless network with a source-destination pair, multiple DF relays each having a finite buffer and an eavesdropper who can combine the signals in two hops to conduct its decoding. A new buffer-aided relay selection scheme is proposed to resist the eavesdropper and we attempt to explore the effects of such eavesdropper's decoding strategy on the concerned network in terms of the E2E STP and expected E2E delay. The contributions of this work are summarized as follows.

- Propose new buffer-aided relay selection scheme to resist the eavesdropper's combining decoding. This is achieved to select the message relay by considering not only the link quality of the main and the eavesdropper channels and the relay buffer states, but also the eavesdropper's decoding strategy.

- Derive analytical expressions for E2E STP and expected E2E delay for both cases when either the instantaneous CSI, or only the distribution of eavesdropping channels are available: A theoretical framework which consists of two Markov chains are developed to derive the E2E performances. The first Markov chain

characterizes the buffer states for a packet in its source-relay delivery process, and the second Markov chain characterizes the buffer states for the packet in its relay-destination delivery process. With the help of the framework, the E2E STP and the expected E2E delay are derived to evaluate the security and delay performance of the proposed buffer-aided relay selection scheme.

- Conduct extensive numerical results to validate the efficiency of the proposed buffer-aided relay selection schemes in terms of the E2E STP and the expected E2E delay. Based on the theoretical results, the security-delay trade-off issue is then studied to explore the achievable E2E STP (expected E2E delay) region under a given expected E2E delay (E2E STP) constraint. Finally, comparisons are made between the new buffer-aided relay selection scheme and the conventional Max-Ratio scheme in terms of the E2E STP and expected E2E delay, results show that our new scheme outperforms the Max-Ratio buffer-aided relay selection scheme in terms of the E2E STP.

By conducting this work, we can provide theoretical models for the E2E security and delay performances of two-hop wireless networks with DF relays, which can be employed as guidelines for network designers.

1.3 Thesis Outline

The remainder of this thesis is outlined as follows. Chapter II introduces the related works of this thesis. In Chapter III, we introduce our work regarding PHY security performance study of buffer-aided relay selection scheme for two-hop wireless networks with RF relays, and Chapter IV presents the work on PHY security performance study of buffer-aided relay selection scheme for two-hop wireless networks with DF relays. Finally, we conclude this thesis in Chapter V.

1.4 Notations

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

Table 1.1: Main notations

Symbol	Definition
S	source node
D	destination node
E	eavesdropper
N	number of relays
R_n	the n-th relay
R_*	selected message relay
Q_n	queue of relay R_n
$\Psi(Q_n)$	number of packets in the relay R_n's queue
$\|h_{i,j}\|^2$	channel gain of link from node i to j
$C_s^{i,j}$	instantaneous secrecy of link i to j
ε	target secrecy rate
$\mathbb{E}[\cdot]$	expectation operator
$f(\cdot)$	probability-density-function (PDF)
$F(\cdot)$	cumulative-density-function (CDF)
$\mathbb{P}[\cdot]$	probability operator
P	common transmit power of source and relay nodes
σ	noise variance
$\mathbf{R}_t$	transmission rate of the main channel
$\mathbf{R}_s$	secrecy rate
γ_{se}	average channel gains of the source-eavesdropper link
γ_{re}	average channel gains of the relay-eavesdropper link
α	average channel gain ratio of the first hop

β	average channel gain ratio of the second hop
p_{st}	end-to-end (E2E) secure transmission probability (STP)
T	E2E delay
T_s	service time at the source node
T_r	service time at the relay node
T_q	queuing delay at the relay node
τ	E2E delay delay constraint
ρ	E2E STP constraint
S_i^+	sets of states s_i can move to for a successful source-relay transmission
S_i^-	sets of states s_i can move to for a successful relay-destination transmission
N_1	number of available relays for the source-relay transmission
N_2	number of available relays for the relay-destination transmission
s_i	relay buffer state
Θ_{s_i}	the set of states that have the same stationary probability as s_i
$\Xi(s_i, \Theta_{s_j})$	the set of states that state s_i has to pass through to reach a state in Θ_{s_j}
A	Markov chain for the source-relay delivery process
$\widetilde{A}$	Markov chain for the relay-destination delivery process
$a_{i,j}$	entry of the Markov chain for source-relay delivery process
$\widetilde{a}_{i,j}$	entry of the Markov chain for relay-destination delivery process
π_{s_i}	stationary probability of state s_i in the source-relay delivery process
$\widetilde{\pi}_{s_i}$	stationary probability of state s_i in the relay-destination delivery process

CHAPTER II

Related Works

This section introduces the existing works related to our study in this thesis, including the works on the E2E performance study of buffer-aided relay selection for two-hop wireless networks with RF relays and the works on the PHY security performance study of buffer-aided relay selection for two-hop wireless networks with DF relays.

2.1 PHY Security Performance Study of Buffer-Aided Relay Selection Scheme for Two-Hop Wireless Networks with RF Relays

By now, many works have been devoted to the study on the PHY security performances of wireless networks with buffer-aided relay selection [30–37]. These works mainly focused on two-hop relay systems with one source-destination pair and single/multiple relays. For the scenario with single relay, the buffer-aided relay selection problem reduces to the selection of a link among the links of source-relay, relay-destination and source-destination to meet a given security criteria [30–32]. For the relay system with a half-duplex (HD) relay where no direct source-destination link is available, the authors in [30] proposed two link selection policies with the considera-

tions of both transmission efficiency and secrecy constraints. They also considered the secrecy throughput maximization problem under secrecy outage probability (SOP) constraint and the SOP minimization problem under secrecy throughput constraint. This work was then extended to the scenario with a full-duplex (FD) relay in [31], where the authors proposed a hybrid HD/FD relaying scheme that allows the relay to switch between the FD mode and HD mode. The optimal setting of mode switching probability was also examined in [31] for the maximization of secrecy network throughput. For the relay system with direct source-destination link, the authors in [32] proposed a link selection scheme 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 [32] under certain SOP constraint.

Regarding the two-hop relay systems with multiple relays, the authors in [33] considered the case when there is only one eavesdropper and proposed relay selection schemes under both the perfect and partial eavesdropper CSI assumptions, where a link is selected based on the channel gain ratio between the main channel and the eavesdropping channel. The SOP of the selected link was derived to evaluate the security performance of the proposed schemes. This work was then extended in [34], where the relay selection is based on the instantaneous secrecy capacity of the individual links. For a MIMO relay system with one eavesdropper and unknown eavesdroppers CSI, the authors in [35] and [36] proposed a link selection scheme based on the maximum legitimate channel gain and derived the corresponding SOP performance of the selected link. The authors in [37] also considered a MIMO system in the presence of multiple eavesdroppers. Under the assumption of perfect eavesdroppers' CSI, they combined the relay selection scheme in [33] with the cooperative jamming technique and proposed a greedy algorithm to identify the best link and jammer to maximize the instantaneous single-link secrecy rate. It is notable from above that

existing works on the PHY security study of buffer-aided relay systems with multiple relays mainly focused on analyzing the single link rather than the E2E PHY security performances [33–37].

These works demonstrated that buffer-aided relay selection is flexible and promising for achieving a desirable PHY security performance. It is notable, however, that a significant delay may be introduced in buffer-aided relay systems due to its buffer queuing process and relay selection process. First, in the relay selection process, 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. While there are some works on the delay performance study of buffer-aided relay selection, the important security issue has not been considered therein [41–43]. Thus, some natural and crucial questions arise: how will the security and delay performances of buffer-aided relay systems interplay with each other, and what would be the achievable region of one performance metric if some constraints are imposed to the other? Answering these questions is very important for the applications of buffer-aided relay systems, especially when they are applied to support delay-sensitive applications in wireless communication scenarios [44].

2.2 PHY Security Performance Study of Buffer-Aided Relay Selection Scheme for Two-Hop Wireless Networks with DF Relays

Since the pioneer work of Huang [30], the PHY security performances of buffer-aided relay selection for two-hop wireless networks have been extensively studied

[30–40], and most of them mainly focus on the networks with RF relays where different codebooks are used at the source and the relay nodes respectively, and the eavesdropper can only conduct its decoding in each hop independently. Jing et al. [30] consider a two-hop network with one source, one destination, one DF relay with infinite buffer and an eavesdropper only wiretapping the relay-destination link. They proposed a link selection scheme based on the quality of the source-relay and relay-destination links, and studied the security performances of a single link in terms of the secrecy outage probability (SOP). Shafie et al. consider a wireless network with one source, one destination, one eavesdropper and one DF-full-duplex (FD) relay [31], [32]. They proposed a link selection scheme based on the instantaneous secrecy rate of all links and the target secrecy rate and also derived expression of the E2E secrecy throughput. Chen et al., however, consider a two-hop wireless network with one source-destination pair, an eavesdropper and multiple RF relays [33]. They proposed a Max-Ratio relay selection scheme based on the relay buffer states and channel gains of the main and eavesdropper channels and also explored the secrecy outage probability performance of a single link for their proposed scheme. For the same network scenario as in [33], Zhang et al. proposed a new Max-Ratio relay selection scheme by taking a consistent parameter into consideration and the SOP was also studied to validate the efficiency of their scheme [34]. Xuan et al. focus on a MIMO network with one source-destination pair, multiple RF relays each with a finite buffer and an eavesdropper intercepting both the source-relay and relay-destination links [35], [36]. A joint relay and transmit antenna selection scheme was proposed based on the relay buffer state and the instantaneous rate of the main channels and the SOP of a single link was derived in a closed form. Lu et al. consider a MIMO system with one source, multiple destinations, multiple intermediate relays and multiple eavesdroppers [37]. They provided an algorism to select the best relay based on the instantaneous secrecy rate. Results showed that their proposed scheme can achieve a higher secrecy rate

compared with the Max-Ratio relay selection scheme. Our previous work studies a two-hop wireless network with multiple RF relays, and the E2E security and delay performances were derived in a closed form for only perfect eavesdropper CSI case [38]. As an extension of the work in [38], we developed a general theoretical framework for the E2E performance analysis of Max-Ratio relay selection scheme in our previous work [39] and the E2E performances in terms of the E2E delay and secure transmission probability (STP) were also derived in a closed form for both perfect and partial eavesdropper CSI cases.

It is noticeable, however, that a more dangerous scenario exists where DF relays are included in the concerned network, i.e., the same codebook is adopted at the source and relay nodes [45], [46], and the eavesdropper can thus combine the signals received in two hops to conduct its decoding. In such scenario, the eavesdropper can achieve a higher decoding probability of the transmitted packet and the security performance of the concerned network will decrease. This makes the existing buffer-aided relay selection schemes unsuitable. However, the study of buffer-aided relay selection scheme and its E2E security and delay performances for this more dangerous network scenario remains unknown.

CHAPTER III

Physical Layer Security Performance Study of Buffer-Aided Relay Selection Scheme for Two-Hop Wireless Networks with RF Relays

This chapter focuses the security-delay trade-off of the buffer-aided relay selection scheme in a two-hop wireless system, which consists of a source-destination pair, one eavesdropper and multiple relays each having a finite buffer. To evaluate the security and delay performances of the system, we derive analytical expressions for the E2E STP and the expected E2E delay under both perfect and partial eavesdropper channel state information (CSI) cases. These analytical expressions help us to explore the inherent trade-off between the security and delay performances of the concerned system. In particular, the results in this chapter indicate that: 1) the maximum E2E STP increases as the constraint on the expected E2E delay becomes less strict, and such trend is more sensitive to the variation of the number of relays than that of the relay buffer size; 2) on the other hand, the minimum expected E2E delay tends to decrease when a less strict constraint on E2E STP is imposed, and this trend is more sensitive to the variation of the relay buffer size than that of the number of relays.

3.1 Outline

The remainder of this chapter is organized as follows. Section 3.2 introduces the system model, transmission scheme, the buffer-aided relay selection schemes and performance metrics. Section 3.3 provides the general framework for characterizing the E2E packet delivery process. The E2E STP and delay performances are analyzed in Section 3.4, and the numerical results are provided in Section 3.5. Finally, Section 3.6 summarizes this chapter.

3.2 System Model and Definitions

3.2.1 System Model

As illustrated in Figure 3.1, we consider a two-hop wireless system consisting of one source S, one destination D, N relays $R_1, R_2, ..., R_N$ adopting the RF decoding strategy, and one eavesdropper E wiretapping on both the source-relay and relay-destination links. Same as [47], [48], the RF strategy concerned in this work adopts different codebooks at the source and relay respectively, so the eavesdropper can only independently decode the signals received in the two hops. We assume all nodes have one antenna and operate in the HD mode such that they cannot transmit and receive data simultaneously. The source and relays are assumed to transmit with common power P. Each relay R_n $(1 \leq n \leq N)$ is equipped with a data buffer Q_n that can store at most L packets. Here the buffer size is defined by the number of packets and each packet is with the same bits M. We use $\Psi(Q_n)$ to denote the number of packets stored in the buffer Q_n and all packets in the buffer are served in a First-In-First-Out (FIFO) discipline. The source S is assumed to have an infinite backlog, i.e., always has packets to transmit.

We consider a time-slotted system where the time is divided into successive slots with equal duration. All wireless links are assumed to suffer from the quasi-

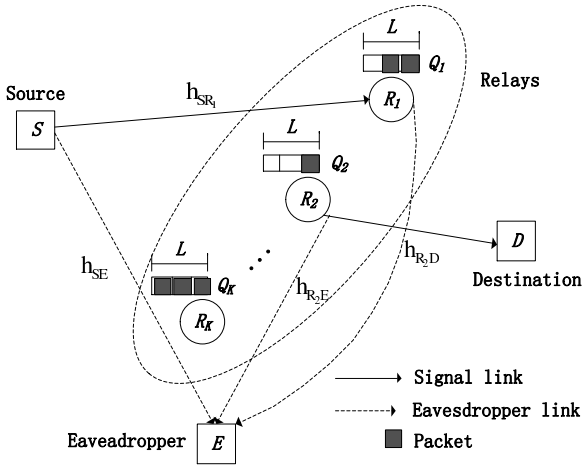


Figure 3.1: Illustration of the system model.

static Rayleigh block fading such that the channel gains remain constant during one time slot, but change independently and randomly from one time slot to the next. We use $|h_{ij}|^2$ to denote the channel gain of the link from node i to node j, where $i \in \{S, R_1, R_2, ..., R_N\}$ and $j \in \{R_1, R_2, ..., R_N, E, D\}$. We assume all source-relay, relay-destination and relay-eavesdropper channel gains are independent and identically distributed (i.i.d.) with mean $\mathbb{E}\left[|h_{SR_n}|^2\right] = \gamma_{sr}$, $\mathbb{E}\left[|h_{R_nD}|^2\right] = \gamma_{rd}$ and $\mathbb{E}\left[|h_{R_nE}|^2\right] = \gamma_{re}$, respectively. Here, $\mathbb{E}\left[\cdot\right]$ stands for the expectation operator. The mean of the source-eavesdropper channel gain is denoted as $\mathbb{E}\left[|h_{SE}|^2\right] = \gamma_{se}$. In this work, we assume the instantaneous channel state information (CSI) of legitimate channels (i.e., $|h_{SR_n}|^2$ and $|h_{R_nD}|^2$) are always known. Regarding the knowledge of eavesdropper CSI, we consider two cases, i.e., perfect CSI case where the instantaneous eavesdropper CSI (i.e., $|h_{SE}|^2$ and $|h_{R_nE}|^2$) are known and partial CSI case where only the average eavesdropper CSI (i.e., γ_{se} and γ_{re}) are available. In addition to fading, all links are also impaired by the additive white Gaussian noise (AWGN) with variance σ^2.

3.2.2 Transmission and Buffer-Aided Relay Selection Schemes

In this work, we assume that no direct link is available between the source S and the destination D, so a relay will be selected to help the $S \to D$ transmission. This work adopts the buffer-aided relay selection scheme that fully exploits the diversity of relays and buffers. More specifically, we adopt the Max-Ratio buffer-aided relay selection scheme in [33]. Although this scheme is called relay selection, its principle is to select the securest link from all individual source-relay and relay-destination links for transmission in each time slot. Thus, the relay selection is solely determined by the instantaneous secrecy rate of individual links.

Since we focus on the selection of the securest link from all available individual links, we adopt the secrecy capacity formulas of an individual link to conduct the relay selection in this work. Before introducing the relay selection scheme, we first introduce the selection criterion. Considering an individual link $A \to B$, where $A \in S$ and $B \in \{R_1, \cdots, R_n\}$ or $A \in \{R_1, \cdots, R_n\}$ and $B \in D$. The instantaneous secrecy capacity of link $A \to B$ is given by [49]

$$C_s^{AB} = \max\{C_m^{AB} - C_e^{AE}, 0\}, \tag{3.1}$$

where

$$C_m^{AB} = \log\left(1 + \frac{P|h_{AB}|^2}{\sigma^2}\right), \tag{3.2}$$

and

$$C_e^{AE} = \log\left(1 + \frac{P|h_{AE}|^2}{\sigma^2}\right), \tag{3.3}$$

denote the capacities of main channel $A \to B$ and eavesdropper channel $A \to E$, respectively. To transmit a message to B, the transmitter A chooses a rate pair ($\mathbf{R}_t^{AB}$, $\mathbf{R}_s^{AB}$) based on the Wyner's coding scheme [16], where $\mathbf{R}_t^{AB}$ denotes the total message rate and $\mathbf{R}_s^{AB}$ denotes the intended secrecy rate. The rate difference $\mathbf{R}_t^{AB} - \mathbf{R}_s^{AB}$

reflects the cost of protecting the message from being intercepted by the eavesdropper E, which means E cannot decode the message if $C_e^{AE} < \mathbf{R}_t^{AB} - \mathbf{R}_s^{AB}$. We use $\mathbf{R}_s^{AB}$ as the selection criterion in the relay selection scheme.

The value of $\mathbf{R}_s^{AB}$ is determined as follows. For a given time slot, if link $A \to B$ is selected for transmission, A uses the knowledge of the main channel CSI to adaptively adjust $\mathbf{R}_t^{AB}$ arbitrarily close to the instantaneous capacity of the main channel C_m^{AB} (i.e., $\mathbf{R}_t^{AB} = C_m^{AB}$), such that no decoding outage occurs at B. For the setting of $\mathbf{R}_s^{AB}$, as the instantaneous eavesdropper CSI is available in the perfect eavesdropper CSI case, we set $\mathbf{R}_s^{AB} = C_m^{AB} - C_e^{AE}$ at A to maximize the intended secrecy rate. However, only the average eavesdropper CSI is known in the partial eavesdropper CSI case, so A chooses the secrecy rate $\mathbf{R}_s^{AB} = C_m^{AB} - \log\left(1 + \frac{P\gamma_{AE}}{\sigma^2}\right)$ [50]. Notice that although the conventional approach is to choose a fixed $\mathbf{R}_s^{AB}$ in this case [30–32], the rationale behind our time-varying $\mathbf{R}_s^{AB}$ is that it can yield a higher secrecy throughput than the fixed one, as can be seen from the results in [50]. Although our $\mathbf{R}_s^{AB}$ is varying in each time slot, it can be determined based on the main channel CSI abstracted from the pilot signal of B [50–52]. In this work, we consider the high SNR regime, so C_m^{AB} and $\mathbf{R}_s^{AB}$ in the perfect eavesdropper CSI case are approximated by $C_s^{AB} = \mathbf{R}_s^{AB} \approx \log\left(\frac{|h_{AB}|^2}{|h_{AE}|^2}\right)$ [50], and the $\mathbf{R}_s^{AB}$ in the partial eavesdropper CSI is approximated as $\mathbf{R}_s^{AB} \approx \log\left(\frac{|h_{AB}|^2}{\gamma_{AE}}\right)$ where log is to the base of 2. To inform the transmitter A when to transmit, we place a threshold ε on the secrecy rate $\mathbf{R}_s^{AB}$, such that A can send messages to B if and only if $\mathbf{R}_s^{AB} > \varepsilon$.

Remark: Here we show the differences of several similar terms mentioned above: the secrecy capacity, the secrecy rate and the target secrecy rate. The secrecy rate represents the intended transmission rate of a link to securely transmit a message to the receiver, the secrecy capacity denotes the upper bound of the secrecy rate, and the target secrecy rate represents the security requirement of the concerned network, which is a given parameter of the network and is a threshold of the secrecy rate.

We are now ready to introduce the Max-Ratio buffer-aided relay selection scheme. In both eavesdropper CSI cases, the relay with the link that has the maximal intended secrecy rate will be selected. For the perfect eavesdropper CSI case, the best relay R_{PF} is selected as

$$R_{\mathrm{PF}} = \arg\max_{R_n} \max \left\{ \frac{|h_{SR_n}|^2 \cdot \mathbf{1}_{\Psi(Q_n)\neq L}}{|h_{SE}|^2}, \frac{|h_{R_nD}|^2 \cdot \mathbf{1}_{\Psi(Q_n)\neq 0}}{|h_{R_nE}|^2} \right\}, \tag{3.4}$$

where $\mathbf{1}_{\Psi(Q_n)\neq L}(\mathbf{1}_{\Psi(Q_n)\neq 0})$ equals 1 if $\Psi(Q_n) \neq L$ $(\Psi(Q_n) \neq 0)$, i.e., relay R_n is available for source-relay (relay-destination) transmission and equals 0 otherwise. For the partial eavesdropper CSI case, the best relay R_{PT} is selected as

$$R_{\mathrm{PT}} = \arg\max_{R_n} \max \left\{ \frac{|h_{SR_n}|^2 \cdot \mathbf{1}_{\Psi(Q_n)\neq L}}{\gamma_{se}}, \frac{|h_{R_nD}|^2 \cdot \mathbf{1}_{\Psi(Q_n)\neq 0}}{\gamma_{re}} \right\}. \tag{3.5}$$

In equations (3.4) and (3.5), the max operation is used to find the maximum of the channel gain ratios (i.e., the ratio of the main channel gain to the eavesdropper channel gain) of the available source-relay and relay-destination links for a particular relay R_n. Thus, the arg max operation, which is operated over all relays, returns the relay with the link that can yield the maximum channel gain ratio.

From (3.4) and (3.5), we can see that we select the message relay from all available relays in perfect case according to the instantaneous channel gain ratios of main and eavesdropper channels, and in the partial case according to the ratios of the instantaneous channel gains of main channels and the average channel gains of eavesdropper channels. With the RF strategy applied at the relays, if the relay R_n is selected for transmission, the instantaneous secrecy capacity of the buffer-aided relay system

when $L = 0$ is formulated as [48]

$$C_s = \frac{1}{2}\left[min \log_2 \left(\frac{1 + P|h_{SR_n}|^2}{1 + P|h_{SE}|^2}, \frac{1 + P|h_{R_nD}|^2}{1 + P|h_{R_nE}|^2}\right)\right]^+. \tag{3.6}$$

However, for the general buffer-aided relay system when $L > 0$, its secrecy capacity formulation in terms of different SNRs/SINRs is still an open issue. Notice that with the buffer-aided relay selection scheme concerned in this work, the relay selection in each time slot is only based on the instantaneous secrecy capacity of each link and states of all relay buffers. Thus, the secrecy capacity formulation of an individual link (3.1) is enough for us to derive the main results in this work (see Section IV-A and Section IV-B for details). It is also worth noting that the buffer-aided relaying scheme in this work is different from the traditional relaying. In the traditional relaying, a packet is transmitted to the relay, where it is decoded and forwarded to the destination in the following time slot. In the relaying scheme of this work, a packet is first transmitted from the source to a selected relay, where it will be decoded and stored, and will not be forwarded to the destination until the relay is selected again for the relay-destination transmission.

3.2.3 Performance Metrics

This chapter aims to investigate the trade-off between the PHY security and delay performances of the Max-Ratio buffer-aided relay selection scheme. To model the delay performance of the packet delivery process, we adopt the widely-used **end-to-end (E2E) delay**, which is defined as the time slots it takes a packet to reach its destination after it is generated at the source node. Consider the delivery process of a tagged packet from S to D via a relay R_*, the E2E delay can be calculated as the sum of the service time (i.e., the waiting time of the packet at both S and the head of R_*'s queue before it is transmitted) and the queuing delay (i.e., the time it

takes the packet to move from the end to the head of R_*'s queue). Defining T_q as the queuing delay and T_s (T_r) as the service time at the source node (the head of R_*'s queue queue), the E2E delay T can be formulated as

$$T = T_s + T_r + T_q. \tag{3.7}$$

It is notable that available studies on the PHY security performance study of buffer-aided relay selection schemes mainly focus on the secrecy outage probability of a *single link*, which is defined as the probability that the *secrecy outage* (i.e., the event that the instantaneous secrecy capacity C_s is below the target secret rate ε) occurs on this link [31], [33], [34]. However, such single link-oriented metric may fail to provide an intuitive insight into the PHY security performance of the whole packet delivery process. According to the definition of the notion of secure connection probability in [53], we define a similar a metric called **E2E secure transmission probability (STP)** to model the security performance. Focusing again on the delivery process of the tagged packet from S to D via R_*, the E2E STP is defined as the probability that neither the $S \to R_*$ nor $R_* \to D$ delivery suffers from secrecy outage. Based on the formulation of the secure connection probability in [53], we formulate the E2E STP as

$$p_{st} = \mathbb{P}(C_s^{SR_*} \geq \varepsilon, C_s^{R_*D} \geq \varepsilon), \tag{3.8}$$

where $C_s^{SR_*}$ ($C_s^{R_*D}$) denotes the instantaneous secrecy capacity of the $S \to R_*$ ($R_* \to D$) link, and $C_s^{SR_*} \geq \varepsilon$ ($C_s^{R_*D} \geq \varepsilon$) represents the event that the $S \to R_*$ ($R_* \to D$) link is selected and secure transmission is conducted when the tagged packet is at S (the head of R_*'s queue) and ε is the target secrecy rate.

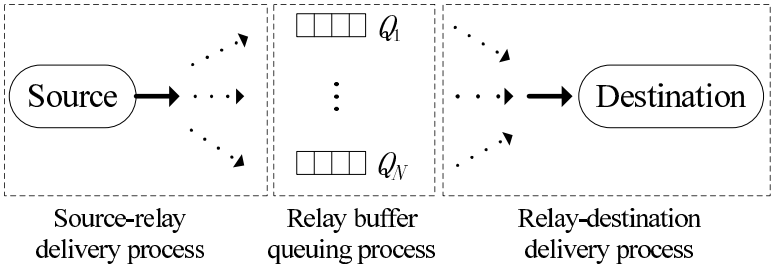


Figure 3.2: End-to-end delivery process of a packet.

3.3 General Framework for E2E Packet Delivery Process Modeling

In this section, we introduce our general framework for characterizing the E2E packet delivery process under both perfect and partial eavesdropper CSI cases, including the source-relay delivery process, buffer queuing process and relay-destination delivery process, as illustrated in Figure 3.2. To facilitate the introduction of the framework, we focus again on the delivery process of a tagged packet from S to D via a relay R_*.

For the modeling of source-relay (resp. relay-destination) delivery process, we first develop a Markov chain to model the transition of possible buffer states when the tagged packet is at S (resp. the head of R_*'s queue). Based on the absorbing Markov chain theory, we then determine the corresponding stationary probability distribution, such that the probability of each possible buffer state can be obtained. For the modeling of buffer queuing process, we regard the queues of all relays as a single queue and the resultant Markov chain is equivalent to a Bernoulli process. Notice that the buffer queuing process is relatively simple in our framework, and thus we focus on the modeling of the source-relay and relay-destination delivery processes of the tagged packet in this section.

$$\mu_{\mathrm{PF}}(s) = \sum_{n_1=0}^{N_1(s)} \binom{N_1(s)}{n_1} (-1)^{n_1} \frac{\alpha}{2^{\varepsilon} n_1 + \alpha} \left(\frac{2^{\varepsilon}}{\beta + 2^{\varepsilon}} \right)^{N_2(s)}, \tag{3.9}$$

$$\begin{aligned} \nu_{\mathrm{PF}}(s) = \sum_{n_1=0}^{N_1(s)} \binom{N_1(s)}{n_1} (-1)^{n_1} \\ \left[\frac{n_1 \cdot {}_2F_1\left(N_2(s), N_2(s)+1; N_2(s)+2; \frac{n_1\beta-\alpha}{\beta(\alpha+2^{\varepsilon}n_1)}\right)}{(N_2(s)+1)(\alpha+2^{\varepsilon}n_1)} \left(\frac{4^{\varepsilon}\alpha}{2^{\varepsilon}n_1\beta + \alpha\beta)} \right)^{N_2(s)} \right. \\ \left. - \frac{{}_2F_1\left(N_2(s), N_2(s)+1; N_2(s)+2; 1-\frac{\alpha}{n_1\beta}\right)}{N_2(s)+1} \left(\frac{\alpha}{n_1\beta} \right)^{N_2(s)} \right], \end{aligned} \tag{3.10}$$

$$\mu_{\mathrm{PT}}(s) = \left[1 - e^{-2^{\varepsilon}/\alpha}\right]^{N_1(s)} \left[1 - e^{-2^{\varepsilon}/\beta}\right]^{N_2(s)}, \tag{3.11}$$

$$\nu_{\mathrm{PT}}(s) = \sum_{n_2=0}^{N_2(s)} \sum_{n_1=0}^{N_1(s)-1} \binom{N_2(s)}{n_2} \binom{N_1(s)-1}{n_1} (-1)^{n_2+n_1} \frac{N_1(s)\beta e^{-\frac{(\alpha n_2+\beta+\beta n_1)2^{\varepsilon}}{\alpha\beta}}}{\alpha n_2 + \beta + \beta n_1} \tag{3.12}$$

3.3.1 Source-Relay Delivery Process Modeling

This subsection derives the stationary probability distribution for the source-relay delivery under both perfect and partial eavesdropper CSI cases. We first define the possible buffer states for the source-relay delivery. As the network contains N relays and each relay has a buffer of size L, there are $(L+1)^N$ possible states in total. Defining s_i the i-th $\left(i \in \{1, 2, \cdots, (L+1)^N\}\right)$ state, we can represent s_i by

$$s_i = [\Psi_{s_i}(Q_1), \cdots, \Psi_{s_i}(Q_n), \cdots, \Psi_{s_i}(Q_N)]^T, n \in \{1, 2, \cdots, N\}, \tag{3.13}$$

where $\Psi_{s_i}(Q_n) \in [0, L]$ gives the number of packets in buffer Q_n at state s_i. We can see that each buffer state s_i can determine a pair $(N_1(s_i), N_2(s_i))$, where $N_1(s_i) \in [0, N]$ and $N_2(s_i) \in [0, N]$ denote the number of available (i.e., $\Psi_{s_i}(Q_n) \neq L$) source-relay links and available (i.e., $\Psi_{s_i}(Q_n) \neq 0$) relay-destination links at state s_i, respectively.

Next, we determine the state transition matrix. Suppose that the buffers are in state s_i at time slot t. According to the relay selection scheme in Section 3.2.2, one link will be selected from the available source-relay and relay-destination links for transmission at this time slot. Thus, the buffer state may move from s_i to several possible states at the next time slot, forming a Markov chain. We define $\mathbf{A}$ the $(L+1)^N \times (L+1)^N$ state transition matrix, where the (i,j)-th entry $a_{i,j} = \mathbb{P}(s_j|s_i)$ denotes the transition probability that the buffer state moves from s_i to s_j. According to the transmission scheme in Section 3.2.2, the state transition happens if and only if a successful transmission is conducted on the selected link (i.e., $\mathbf{R}_s \geq \varepsilon$). We use $\mathcal{S}_i^+$ ($\mathcal{S}_i^-$) to denote the set of states s_i can move to when a successful source-relay (relay-destination) transmission is conducted. Now, we are ready to give the following lemma regarding the state transition matrix $\mathbf{A}$.

Lemma 1 *Suppose that the buffers are in state s_i at time slot t, the (i,j)-th entry of the state transition matrix $\mathbf{A}$ under both the perfect and partial eavesdropper CSI cases is given by*

$$a_{i,j} = \begin{cases} \mu_\Delta(s_i), \text{ if } s_j = s_i, \\ \dfrac{\nu_\Delta(s_i)}{N_1(s_i)}, \text{ if } s_j \in \mathcal{S}_i^+, \\ \dfrac{1-\mu_\Delta(s_i)-\nu_\Delta(s_i)}{N_2(s_i)}, \text{ if } s_j \in \mathcal{S}_i^-, \\ 0, \text{ elsewhere.} \end{cases} \tag{3.14}$$

where $\Delta \in \{\text{PF} = \textit{perfect}, \text{PT} = \textit{partial}\}$ denotes the eavesdropper CSI case, and $\mu_\Delta(s_i)$ and $\nu_\Delta(s_i)$ are given in (3.9) and (3.10) for the perfect CSI case and in (3.11) and (3.12) for the partial CSI case with the parameter $s = s_i$.

Proof 1 *See Appendix A.1 for the proof.*

From Lemma 1, we can see that $a_{i,j} \neq 0$ and $\sum_{j=1}^{(L+1)^N} a_{i,j} = 1$, which means that the Markov chain can move to any state s_j $\left(j \in \{1, 2, \cdots, (L+1)^N\}\right)$ from a starting

state s_i with a non-zero probability, i.e., the Markov chain is irreducible [54]. We can also see from Lemma 1 that $a_{i,i} \neq 0$, which means that the Markov chain can return to state s_i in one time slot, i.e., the period of s_i equals 1. This proves that every state s_i is aperiodic and thus the Markov chain is aperiodic [54]. According to Definition 1 and Theorem 2 of Chapter 11 in [55], the irreducibility and aperiodicity properties ensure that our Markov chain that models the buffer states of the source-relay transmission process is stationary and there exists a unique stationary probability distribution $\boldsymbol{\pi} = [\pi^{\Delta}_{s_1}, \cdots, \pi^{\Delta}_{s_i}, \cdots, \pi^{\Delta}_{s_{(L+1)^N}}]^T$ such that $A\boldsymbol{\pi} = \boldsymbol{\pi}$ and $\sum_{i=1}^{(L+1)^N} \pi^{\Delta}_{s_i} = 1$, where $\pi^{\Delta}_{s_i}$ denotes the stationary probability of state s_i.

According to Lemma 2 in [54], the analytical expression of $\pi^{\Delta}_{s_i}$ can be given by

$$\pi^{\Delta}_{s_i} = \left(\sum_{j=1}^{(L+1)^N} \frac{\prod_{s_{i'} \in \Xi(s_i, \Theta_{s_j})} a_{i,i'}}{\prod_{s_{j'} \in \Xi(s_j, \Theta_{s_i})} a_{j,j'}} \right)^{-1}, \tag{3.15}$$

where Θ_{s_i} (Θ_{s_j}) denotes the set of states that have the same stationary probability as s_i (s_j) has, and $\Xi(s_i, \Theta_{s_j})$ ($\Xi(s_j, \Theta_{s_i})$) denotes the set of states that state s_i (s_j) has to pass through to reach a state in Θ_{s_j} (Θ_{s_i}).

3.3.2 Relay-Destination Delivery Process Modeling

This subsection derives the stationary probability distribution of all possible buffer states provided that the tagged packet is at the head of R_*'s queue. Since the buffer of R_* cannot be empty, there are $L \cdot (L+1)^{N-1}$ states in total. Similarly, we define the k-th $\left(k \in \{1, \cdots, L(L+1)^{N-1}\}\right)$ state as

$$\widetilde{s}_k = [\Psi_{\widetilde{s}_k}(Q_1), \cdots, \Psi_{\widetilde{s}_k}(Q_*), \cdots, \Psi_{\widetilde{s}_k}(Q_n), \cdots, \Psi_{\widetilde{s}_k}(Q_N)]^T, n \in \{1, \cdots, N\}, n \neq *, \tag{3.16}$$

where $\Psi_{\widetilde{s}_k}(Q_n)$ and $\Psi_{\widetilde{s}_k}(Q_*)$ represent the number of packets in the buffers of R_n and R_* at state $\widetilde{s}_k$ respectively. It's obvious that $0 \leq \Psi_{\widetilde{s}_k}(Q_n) \leq L$ and $1 \leq \Psi_{\widetilde{s}_k}(Q_*) \leq L$, and every state $\widetilde{s}_k$ corresponds to one pair $(N_1(\widetilde{s}_k), N_2(\widetilde{s}_k))$, where $N_1(\widetilde{s}_k)$ and $N_2(\widetilde{s}_k)$ denote the numbers of available source-relay and relay-destination links at state $\widetilde{s}_k$, respectively.

We denote $\widetilde{\mathbf{A}}$ as the $L(L+1)^{N-1} \times L(L+1)^{N-1}$ state transition matrix of all states $\widetilde{s}_k$, where the (k,l)-th entry $\widetilde{a}_{k,l} = \mathbb{P}(\widetilde{s}_l|\widetilde{s}_k)$ is the transition probability that the state moves from $\widetilde{s}_k$ to $\widetilde{s}_l$. Similarly, we use $\widetilde{\mathcal{S}}_k^+$ ($\widetilde{\mathcal{S}}_k^-$) to denote the set of states $\widetilde{s}_k$ can move to when a successful source-relay (relay-destination) transmission is conducted. Notice that the buffer state can move from $\widetilde{s}_k$ into $\widetilde{\mathcal{S}}_k^-$ only when a successful relay-destination transmission except for $R_* \to D$ occurs. Based on the above definitions, we give the following lemma regarding the state transition matrix $\widetilde{\mathbf{A}}$.

Lemma 2 *Suppose that the buffers are in state $\widetilde{s}_k$ when the tagged packet is at the head of relay R_*'s queue, the (k,l)-th entry of the state transition matrix $\widetilde{\mathbf{A}}$ under both the perfect and partial eavesdropper CSI cases is given by*

$$\widetilde{a}_{k,l} = \begin{cases} \mu_\Delta(\widetilde{s}_k), \text{ if } \widetilde{s}_l = \widetilde{s}_k, \\ \dfrac{\nu_\Delta(\widetilde{s}_k)}{N_1(\widetilde{s}_k)}, \text{ if } \widetilde{s}_l \in \widetilde{\mathcal{S}}_k^+, \\ \dfrac{1-\mu_\Delta(\widetilde{s}_k)-\nu_\Delta(\widetilde{s}_k)}{N_2(\widetilde{s}_k)-1}, \text{ if } \widetilde{s}_l \in \widetilde{\mathcal{S}}_k^-, \\ 0, \text{ elsewhere.} \end{cases} \tag{3.17}$$

where $\Delta \in \{\mathrm{PF} = \textit{perfect}, \mathrm{PT} = \textit{partial}\}$ denotes the eavesdropper CSI case, $\mu_\Delta(\widetilde{s}_k)$ and $\nu_\Delta(\widetilde{s}_k)$ are given in (3.9) and (3.10) for the perfect CSI case and in (3.11) and (3.12) for the partial CSI case.

Proof 2 *The proof is same as that for Lemma 1, so we have omitted it here.*

Similarly, according to [55], we can see from Lemma 2 that our Markov chain

$$\phi(s) = \sum_{n_1=0}^{N_1(s)} \sum_{n_2=0}^{N_2(s)} \binom{N_1(s)}{n_1} \binom{N_2(s)}{n_2} (-1)^{n_1+n_2} \frac{\alpha\beta}{2^{\varepsilon}(n_1\beta + n_2\alpha) + \alpha\beta}, \tag{3.19}$$

$$\omega(s) = \sum_{n_1=0}^{N_1(s)} \sum_{n_2=0}^{N_2(s)-1} \frac{\binom{N_1(s)}{n_1}\binom{N_2(s)-1}{n_2}(-1)^{n_1+n_2} N_2(s)\alpha^2\beta}{2^{\varepsilon}(n_1\beta + \alpha + n_2\alpha)^2 + \alpha\beta(n_1\beta + \alpha + n_2\alpha)}. \tag{3.20}$$

---

that models the buffer states of the relay-destination transmission process is also stationary. We use $\widetilde{\boldsymbol{\pi}} = [\widetilde{\pi}^{\Delta}_{\widetilde{s}_1}, \cdots, \widetilde{\pi}^{\Delta}_{\widetilde{s}_k}, \cdots, \widetilde{\pi}^{\Delta}_{\widetilde{s}_{L(L+1)^{N-1}}}]^T$ to denote the corresponding stationary probability distribution when the tagged packet is at the head of R_*'s queue, where $\widetilde{\pi}^{\Delta}_{\widetilde{s}_k}$ denotes the stationary probability of state $\widetilde{s}_k$. Based on the state transition matrix $\widetilde{\mathbf{A}}$ and Lemma 2 in [54], we can determine the analytical expression of the stationary probability of state $\widetilde{s}_k$ in $\widetilde{\boldsymbol{\pi}}$ as

$$\widetilde{\pi}^{\Delta}_{\widetilde{s}_k} = \left(\sum_{l=1}^{(L+1)^N} \frac{\prod_{\widetilde{s}_{k'} \in \Xi(\widetilde{s}_k, \Theta_{\widetilde{s}_l})} \widetilde{a}_{k,k'}}{\prod_{\widetilde{s}_{l'} \in \Xi(\widetilde{s}_l, \Theta_{\widetilde{s}_k})} \widetilde{a}_{l,l'}} \right)^{-1}, \tag{3.18}$$

where $\Theta_{\widetilde{s}_k}$ ($\Theta_{\widetilde{s}_l}$) denotes the set of states that have the same stationary probability as $\widetilde{s}_k$ ($\widetilde{s}_l$) has, and $\Xi(\widetilde{s}_k, \Theta_{\widetilde{s}_l})$ ($\Xi(\widetilde{s}_l, \Theta_{\widetilde{s}_k})$) denotes the set of states that state $\widetilde{s}_k$ ($\widetilde{s}_l$) has to pass through to reach a state in $\Theta_{\widetilde{s}_l}$ ($\Theta_{\widetilde{s}_k}$).

3.4 E2E STP and Delay Analysis

With the help of the stationary probability distributions in Section 3.3, this section provides theoretical analysis for the E2E STP and delay performances under both the perfect and partial eavesdropper CSI cases.

3.4.1 E2E STP Analysis

We derive the E2E STP in this subsection and summarize the main results in the following theorem.

Theorem III.1 *Consider the two-hop relay wireless system as illustrated in Figure 3.1. Under the transmission scheme and the Max-Ratio buffer-aided relay selection scheme in Section 3.2.2, the E2E STP for the perfect eavesdropper CSI case can be determined as*

$$p_{st}^{\mathrm{PF}} = \sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\mathrm{PF}} \nu_{\mathrm{PF}}(s_i) \sum_{k=1}^{L(L+1)^{N-1}} \pi_{\widetilde{s}_k}^{\mathrm{PF}} \frac{1-\mu_{\mathrm{PF}}(\widetilde{s}_k)-\nu_{\mathrm{PF}}(\widetilde{s}_k)}{N_2(\widetilde{s}_k)}, \tag{3.21}$$

where s_i ($\widetilde{s}_k$) denotes the buffer state when the tagged packet is at S (the head of a given relay queue), $\pi_{s_i}^{\mathrm{PF}}$ and $\pi_{\widetilde{s}_k}^{\mathrm{PF}}$ are given by (3.15) and (3.18) with $\Delta = \mathrm{PF}$, $\mu_{\mathrm{PF}}(\widetilde{s}_k)$ is given by (3.9) with $s = \widetilde{s}_k$, $\nu_{\mathrm{PF}}(s_i)$ and $\nu_{\mathrm{PF}}(\widetilde{s}_k)$ are given by (3.10) with $s = s_i$ and $s = \widetilde{s}_k$ respectively. The E2E STP for the partial eavesdropper CSI case is given by

$$p_{st}^{\mathrm{PT}} = \sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\mathrm{PT}} \cdot (1-\phi(s_i)-\omega(s_i)) \sum_{k=1}^{L(L+1)^{N-1}} \pi_{\widetilde{s}_k}^{\mathrm{PT}} \frac{\omega(\widetilde{s}_k)}{N_2(\widetilde{s}_k)}, \tag{3.22}$$

where $\pi_{s_i}^{\mathrm{PT}}$ and $\pi_{\widetilde{s}_k}^{\mathrm{PT}}$ are given by (3.15) and (3.18) with $\Delta = \mathrm{PT}$, $\phi(s_i)$ is given by (3.19) with $s = s_i$, $\omega(s_i)$ and $\omega(\widetilde{s}_k)$ are given by (3.20) with $s = s_i$ and $s = \widetilde{s}_k$ respectively.

Proof 3 *According to the formulation of E2E STP in (3.8), we have*

$$p_{st}^{\Delta} = \mathbb{P}\left(C_s^{SR_*} \geq \varepsilon, C_s^{R_*D} \geq \varepsilon\right). \tag{3.23}$$

Applying the law of total probability yields

$$p_{st}^{\Delta} = \sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\Delta} \cdot \mathbb{P}\left(C_s^{SR_*} \geq \varepsilon, C_s^{R_*D} \geq \varepsilon | s_i\right). \tag{3.24}$$

We define $R_* = R_n, n \in \mathcal{N}_1$ the event that relay R_n is selected for the source-relay delivery at buffer state s_i, where $\mathcal{N}_1 = \{n|\Psi_{s_i}(Q_n) \neq L\}$ denotes the index set of available relays. Obviously, $|\mathcal{N}_1| = N_1(s_i)$. Again, applying the law of total probability, we have

$$p_{st}^{\Delta} = \sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\Delta} \cdot \sum_{n \in \mathcal{N}_1} \mathbb{P}\left(C_s^{SR_*} \geq \varepsilon, C_s^{R_* D} \geq \varepsilon, R_* = R_n | s_i\right). \tag{3.25}$$

After changing the above probability into conditional probability, we have

$$\begin{aligned} p_{st}^{\Delta} = & \sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\Delta} \cdot \sum_{k \in \mathcal{N}_1} \mathbb{P}\left(C_s^{SR_*} \geq \varepsilon, R_* = R_n | s_i\right) \\ & \cdot \mathbb{P}\left(C_s^{R_* D} \geq \varepsilon | C_s^{SR_n} \geq \varepsilon, R_* = R_n, s_i\right) \qquad (3.26) \\ = & \sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\Delta} \cdot \sum_{n \in \mathcal{N}_1} \mathbb{P}\left(C_s^{SR_n} \geq \varepsilon | s_i\right) \mathbb{P}\left(C_s^{R_n D} \geq \varepsilon\right), \qquad (3.27) \end{aligned}$$

where (3.27) follows since the relay-destination delivery is independent of the buffer state and transmission in the first hop provided $R_* = R_n$. Notice that $\mathbb{P}\left(C_s^{SR_n} \geq \varepsilon | s_i\right)$ is the probability the link $S \to R_n$ is selected and the transmission is secure at state s_i when the tagged packet is at S, and $\mathbb{P}\left(C_s^{R_n D} \geq \varepsilon\right)$ represents the probability that the link $R_n \to D$ is selected and the transmission is secure when the tagged packet is at the head of R_n's queue.

For the perfect eavesdropper CSI case, it is easy to see $C_s^{SR_*} = \mathbf{R}_s^{SR_*}$ and $\mathbb{P}\left(C_s^{SR_n} \geq \varepsilon | s_i\right)$ is equivalent to the transition probability $a_{i,j}$ from s_i to s_j for $s_j \in S_i^+$. Thus, we have

$$\mathbb{P}\left(C_s^{SR_n} \geq \varepsilon | s_i\right) = \frac{\nu_{\mathrm{PF}}(s_i)}{N_1(s_i)}, \tag{3.28}$$

according to Lemma 1. Next, applying the law of total probability, we have

$$\mathbb{P}\left(C_s^{R_nD} \geq \varepsilon\right) = \sum_{k=1}^{L(L+1)^{N-1}} \pi_{\widetilde{s}_k}^{\mathrm{PF}} \cdot \mathbb{P}\left(C_s^{R_nD} \geq \varepsilon | \widetilde{s}_k\right). \tag{3.29}$$

Since $C_s^{R_nD} = \mathbf{R}_s^{R_nD}$*, we have*

$$\mathbb{P}\left(C_s^{R_nD} \geq \varepsilon | \widetilde{s}_k\right) = \mathbb{P}\left(\mathbf{R}_s^{R_nD} \geq \varepsilon | \widetilde{s}_k\right) \tag{3.30}$$

$$= \frac{1 - \mu_{\mathrm{PF}}(\widetilde{s}_k) - \nu_{\mathrm{PF}}(\widetilde{s}_k)}{N_2(\widetilde{s}_k)}, \tag{3.31}$$

where (3.31) follows from the proof of Lemma 2. Finally, the E2E STP for the perfect eavesdropper CSI case follows after substituting (3.31) into (3.29), and then substituting (3.29) and (3.28) into (3.27).

For the partial eavesdropper CSI case, based on the random variables $X^{'}$ *and* $Y^{'}$ *in Appendix A.1,* $\mathbb{P}\left(C_s^{SR_n} \geq \varepsilon | s_i\right)$ *is equivalent to*

$$\frac{1}{N_1(s_i)} \mathbb{P}\left(\frac{\max\{X^{'}, Y^{'}\}}{U} \geq 2^{\varepsilon}, X^{'} > Y^{'}\right) \tag{3.32}$$

$$= \frac{1}{N_1(s_i)} \left(1 - \mathbb{E}[F_{X'}(2^{\varepsilon}U) F_{Y'}(2^{\varepsilon}U)] - \mathbb{E}_U\left[\int_{2^{\varepsilon}U}^{\infty} \mathbb{P}(X^{'} < y) f_{Y'}(y) \mathrm{d}y\right]\right), \tag{3.33}$$

where $f_U(u) = e^{-u}$*,* $u_{a,b} = \frac{|h_{a,b}|^2}{\gamma_{ab}}$*,* $a, b \in \{SR_n, SE, R_nD, R_nE\}$ *and the first expectation in (3.33) is equivalent to*

$$\mathbb{P}\left(\frac{\max\{X^{'}, Y^{'}\}}{U} < 2^{\varepsilon}\right), \tag{3.34}$$

which can be given by the $\phi(s_i)$ *in (3.19) with* $s = s_i$*, and the second expectation in (3.33) is equivalent to*

$$\mathbb{P}\left(\frac{\max\{X^{'}, Y^{'}\}}{U} \geq 2^{\varepsilon}, X^{'} < Y^{'}\right), \tag{3.35}$$

which can be given by the $\omega(s_i)$ in (3.20) with $s = s_i$. Thus, we have

$$\mathbb{P}\left(C_s^{SR_n} \geq \varepsilon | s_i\right) = \frac{1 - \phi(s_i) - \omega(s_i)}{N_1(s_i)}, \tag{3.36}$$

and

$$\begin{aligned}\mathbb{P}\left(C_s^{R_n D} \geq \varepsilon | s_i\right) &= \frac{\mathbb{P}\left(\frac{\max\{X', Y'\}}{U} \geq 2^{\varepsilon}, X' < Y'\right)}{N_2(s_i)} \\ &= \frac{\omega(s_i)}{N_2(s_i)}.\end{aligned} \tag{3.37}$$

Following the same idea, we have

$$\mathbb{P}\left(C_s^{R_n D} \geq \varepsilon | \widetilde{s}_k\right) = \frac{\omega(\widetilde{s}_k)}{N_2(\widetilde{s}_k)}, \tag{3.38}$$

and thus

$$\mathbb{P}\left(C_s^{R_n D} \geq \varepsilon\right) = \sum_{k=1}^{L(L+1)^{N-1}} \pi_{\widetilde{s}_k}^{\mathrm{PT}} \frac{\omega(\widetilde{s}_k)}{N_2(\widetilde{s}_k)}. \tag{3.39}$$

Finally, substituting (3.36) and (3.39) into (3.27) yields the E2E STP for the partial eavesdropper CSI case.

3.4.2 E2E Delay Analysis

This subsection presents the analytical results for the E2E delay of the system under both the perfect and partial eavesdropper CSI cases. We first derive the mean service time of the tagged packet at the source and at the head of some relay R_*'s queue, and then derive the expected queuing delay of the tagged packet at relay R_*. Combining the mean service time and the expected queuing delay, we finally determine the expected E2E delay. We first establish the following lemma regarding the mean service time.

Lemma 3 *The mean service time when the tagged packet is at the source node S is*

$$T_s^{\Delta} = \frac{1}{\sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\Delta} \nu_{\Delta}(s_i)}, \tag{3.40}$$

where $\pi_{s_i}^{\Delta}$ is given by (3.15) and $\nu_{\Delta}(s_i)$ is given in Lemma 1, and the mean service time when the tagged packet is at the head of R_*'s queue is

$$T_r^{\Delta} = \frac{1}{\sum_{k=1}^{L(L+1)^{N-1}} \pi_{\widetilde{s}_k}^{\Delta} \frac{(1-\mu_{\Delta}(\widetilde{s}_k)-\nu_{\Delta}(\widetilde{s}_k))}{N_2(\widetilde{s}_k)}}, \tag{3.41}$$

where $\pi_{\widetilde{s}_k}^{\Delta}$ is given by (3.18), $\mu_{\Delta}(\widetilde{s}_k)$ and $\nu_{\Delta}(\widetilde{s}_k))$ are given in Lemma 2.

Proof 4 *According to the transmission scheme in Section 3.2.2 and the state transition matrix in Section 3.3, we can see the average service rate (i.e., average number of packets served per time slot) of a node is equivalent to the probability that a successful transmission is conducted per time slot by this node. Thus, the average service rate at S is*

$$\sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\Delta} \nu_{\Delta}(s_i), \tag{3.42}$$

and the average service rate at relay R_* is

$$\sum_{k=1}^{L(L+1)^{N-1}} \pi_{\widetilde{s}_k}^{\Delta} \frac{(1-\mu_{\Delta}(\widetilde{s}_k)-\nu_{\Delta}(\widetilde{s}_k))}{N_2(\widetilde{s}_k)}. \tag{3.43}$$

Finally, we obtain the mean service time by calculating the reciprocal of the average service rate.

Next, we give the following lemma to show the expected queuing delay of the tagged packet at relay R_*'s queue.

Lemma 4 *The expected queuing delay of the tagged packet at relay R_*'s queue is*

$$T_q^{\Delta} = \frac{\sum_{i=1}^{(L+1)^N} \sum_{n=1}^{N} \pi_{s_i}^{\Delta} \Psi_{s_i}(Q_n)}{N \sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\Delta} \nu_{\Delta}(s_i)}, \tag{3.44}$$

where $\pi_{s_i}^{\Delta}$ is given by (3.15), $\nu_{\Delta}(s_i)$ is given in Lemma 1.

Proof 5 *Based on the general framework in Section 3.3, we model the queues of all relays as a single Bernoulli queue. According to Little's Law [56], the expected queuing delay for this queue is*

$$T_q^{\Delta,total} = \frac{\mathbb{E}\left[\sum_{n=1}^{N} \Psi(Q_n)\right]}{r_{\text{arr}}}, \tag{3.45}$$

where the numerator and the denominator denote the expected queuing length and average arrival rate of relay, respectively. Considering all available buffer states, we can derive the expected queuing length as

$$\mathbb{E}\left[\sum_{k=1}^{N} \Psi(Q_n)\right] = \sum_{i=1}^{(L+1)^N} \sum_{n=1}^{N} \pi_{s_i}^{\Delta} \Psi_{s_i}(Q_n). \tag{3.46}$$

Notice the arrival rate is equivalent to the service rate of S. Based on Lemma 3, we have

$$\sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\Delta} \nu_{\Delta}(s_i). \tag{3.47}$$

Thus, the total average queuing delay of all relays is

$$T_q^{\Delta,total} = \frac{\sum_{i=1}^{(L+1)^N} \sum_{n=1}^{N} \pi_{s_i}^{\Delta} \Psi_{s_i}(Q_n)}{\sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\Delta} \nu_{\Delta}(s_i)}. \tag{3.48}$$

Due to the symmetry of all relays, the expected queuing delay of each relay is

$$T_q^{\Delta} = \frac{T_q^{\Delta,total}}{N}, \tag{3.49}$$

which completes the proof.

Based on Lemma 3 and 4, we are now ready to give the following theorem regarding the expected E2E delay of the system.

Theorem III.2 *Consider the two-hop relay wireless system as illustrated in Figure 3.1. Under the transmission scheme and the Max-Ratio buffer-aided relay selection scheme in Section 3.2.2, the E2E delay of the system for both eavesdropper CSI cases can be determined as*

$$T_{\Delta} = \frac{1 + \frac{1}{N} \sum\limits_{i=1}^{(L+1)^N} \sum\limits_{n=1}^{N} \pi_{s_i}^{\Delta} \Psi_{s_i}(Q_n)}{\sum\limits_{i=1}^{(L+1)^N} \pi_{s_i}^{\Delta} \nu_{\Delta}(s_i)} + \frac{1}{\sum\limits_{k=1}^{L(L+1)^{N-1}} \pi_{\widetilde{s}_k}^{\Delta} \frac{(1-\mu_{\Delta}(\widetilde{s}_k)-\nu_{\Delta}(\widetilde{s}_k))}{N_2(\widetilde{s}_k)}}, \tag{3.50}$$

where $\Delta \in \{\mathrm{PF}, \mathrm{PT}\}$, $\pi_{s_i}^{\Delta}$ is given by (3.15), $\nu_{\Delta}(s_i)$ is given in Lemma 1, $\pi_{\widetilde{s}_k}^{\Delta}$ is given by (3.18), $\mu_{\Delta}(\widetilde{s}_k)$ and $\nu_{\Delta}(\widetilde{s}_k))$ are given in Lemma 2.

Proof 6 *The E2E delay T_{Δ} directly follows after combining the mean service time in Lemma 3 and the expected queuing delay in Lemma 4.*

3.5 Simulation results

In this section, we first conduct extensive simulations to validate our theoretical analysis in terms of the E2E STP and the expected E2E delay. Based on the theoretical results, we then explore how the network parameters affect these two performances. Finally, we study the achievable E2E STP (delay) region under a certain

E2E delay (STP) constraint to illustrate the trade-off between the PHY security and delay performances.

3.5.1 Simulation Settings

To validate our theoretical results for the E2E STP and expected E2E delay, a dedicated C++ simulator was developed to simulate the E2E packet delivery process based on the Max-Ratio buffer aided relay selection schemes in (3.4) and (3.5), which is now available at [57]. With the help of the simulator, we conduct extensive simulations to calculate the simulated results of E2E STP and expected E2E delay. In all simulations, the total number of time slots is fixed as 10^5 and the corresponding relay selection scheme is performed once per slot for each eavesdropper CSI case. The simulated E2E STP is calculated as the ratio of the number of packets *securely* transmitted to the destination D to the total number of packets generated at the source S, i.e.,

$$p_{st} = \frac{\text{number of packets securely transmitted to } D}{\text{number of packets generated}}.$$

The expected E2E delay is calculated as the ratio of the total E2E delay (measured in time slots) of all packets transmitted to D to the number of these packets, i.e.,

$$T = \frac{\text{total E2E delay of packets transmitted to } D}{\text{number of packets transmitted to } D}.$$

Please notice that the metric T accounts for all packets in both eavesdropper CSI cases, but the meaning of "all packets" differs. In the partial CSI case, "all packets" refers to not only the securely transmitted packets but also the non-securely transmitted ones. In the perfect CSI case, "all packets" refers to the securely transmitted packets, because all packets can be securely transmitted.

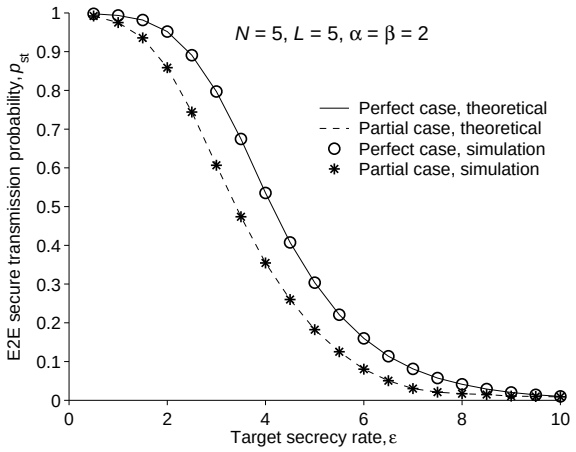
Similar to the settings in [54], we set the noise variance as $\sigma^2 = 1$, the trans-

mission power as $P = 20$, and the average channel gains of the source-relay and relay-destination links as $\gamma_{sr} = \gamma_{rd} = 5$dB. Thus, the corresponding average SNR high enough to guarantee successful decoding at the relays and the destination. We set the channel gain ratio α and β as $\alpha = \beta = 2$ and the average eavesdropping channel gains as $\gamma_{se} = \frac{\gamma_{sr}}{\alpha}$ and $\gamma_{re} = \frac{\gamma_{rd}}{\beta}$. Notice that simulations with other parameters can also be conducted with our simulator.

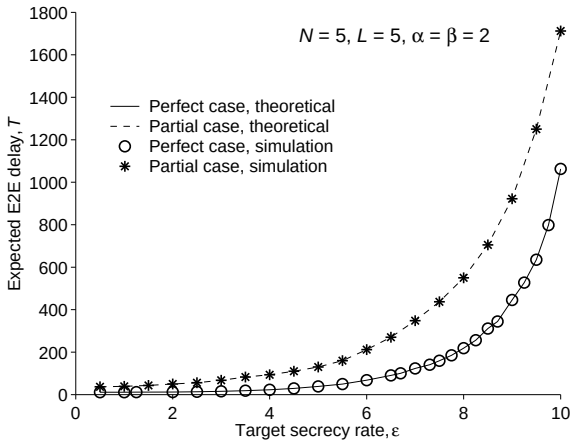
3.5.2 Model Validation

We first conduct simulations for various settings of the target secrecy rate ε under the network scenario of $N = 5$ and $L = 5$. The corresponding simulated and theoretical results of the E2E STP p_{st}^{Δ} ($\Delta = \{\text{PF}, \text{PT}\}$) are summarized in Figure 3.3a, and the results of expected E2E delay T_{Δ} are summarized in Figure 3.1, for both perfect and partial eavesdropper CSI cases. We then fix the buffer size as $L = 2$ and target secrecy rate as $\varepsilon = 1$, and conduct simulations by varying the number of relays N. We provide plots in Figure 3.4a for the simulated and theoretical results of p_{st}^{Δ} and in Figure 3.4b for the results of T_{Δ}, under both eavesdropper CSI cases. Finally, we consider a fixed number of relays $N = 2$ and a given target secrecy rate $\varepsilon = 1$. For this scenario, simulations under various settings of buffer size L are conducted, and the simulated/theoretical results of p_{st}^{Δ} and T_{Δ} are shown in Figure 3.5a and Figure 3.5b, respectively.

We can see from Figure 3.3a, Figure 3.4a and Figure 3.5a, the simulation results of p_{st}^{Δ} match nicely with the theoretical ones for both eavesdropper CSI cases under various network settings. This indicates that our theoretical analysis can be used to efficiently model the E2E STP of the system. For T_{Δ}, it can be seen from Figure 3.3b, Figure 3.4b and Figure 3.5b that all simulation results match proficiently with the corresponding theoretical curves, implying that our theoretical analysis is highly efficient for the E2E delay modeling of the system.



(a) E2E STP vs. target secrecy rate ε.



(b) Expected E2E delay vs. target secrecy rate ε.

Figure 3.3: E2E STP and expected E2E delay vs. target secrecy rate ε.

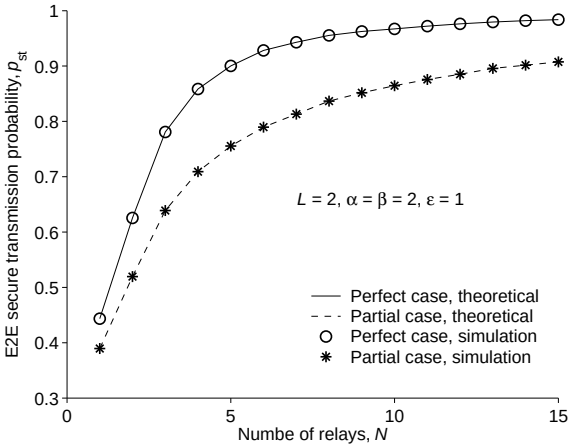
3.5.3 Performance Discussion

With the help of theoretical modeling for the E2E STP p_{st}^{Δ} and expected E2E delay T_{Δ}, we now explore how the network parameters (e.g., N, L and ε) affect the delay and security performances of the system under both eavesdropping CSI cases.

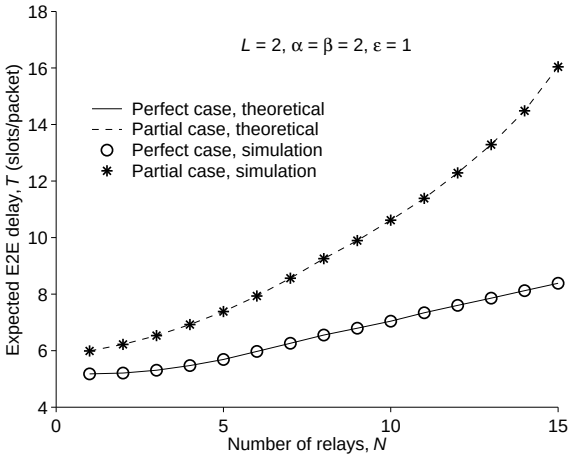
We first examine how the p_{st}^{Δ} and T_{Δ} vary with the target secrecy rate ε for a given N and L. It can be observed from Figure 3.3a that the p_{st}^{Δ} decreases as ε increases in both eavesdropper CSI cases. This is very intuitive since a larger ε represents a higher secrecy rate requirement, which is less likely to be satisfied for a secure transmission. Different from the behavior of p_{st}^{Δ}, we can see from Figure 3.3b that the T_{Δ} increases

as ε increases in both cases. According to the transmission schemes in Section 3.2.2, a larger ε results in a reduced successful transmission probability in each hop and thus a reduced service rate, as can be seen from Lemma 3. The reduction in service rate leads to not only an increased service time but also an increased queuing delay since a packet in the relay queue has to wait for a longer time before the service process of all the packets ahead of it is finished. Another observation from both figures indicates that the relay selection scheme in the perfect eavesdropper CSI case has consistently better STP and delay performances than that in the partial CSI case. Based on the relay selection criteria in (3.4) and (3.5), a link with a larger instantaneous secrecy rate (or secrecy capacity) can be selected in the perfect eavesdropper CSI, which thus yields a larger successful transmission probability (or secure transmission probability) in each hop for a given target secrecy rate ε. Thus, the relay selection scheme in the perfect eavesdropper CSI outperforms that in the partial case in terms of the E2E STP and E2E expected delay.

Next we investigate the impact of number of relays N on the p_{st}^{Δ} and T_{Δ} for given ε and L. Figure 3.4 illustrates how p_{st}^{Δ} and T_{Δ} vary with N for the setting of $L = 2$, $\alpha = \beta = 2$ and $\varepsilon = 1$. We can see from Figure 3.4a that the E2E STP increases as the number of relays N increases for both eavesdropper CSI cases. Notice that the affect of distributing more relays in the system on the E2E STP performance is two-edged. First, it leads to a link with a larger instantaneous secrecy capacity selected by the relay selection schemes, so the STP in the first hop increases. Second, however, the number of available relay-destination links competing for transmission increases, which may result in a decreased STP in the second hop. Actually, the increasing behavior the STP in the first hop dominates the whole behavior of the E2E STP, and thus the E2E STP increases as N increases. Similar to the E2E STP, it can be observed from Figure 3.4b that the expected E2E delay increases as the number of relays N increases simultaneously. This is also due to the two-edged



(a) E2E STP vs. number of relays N.

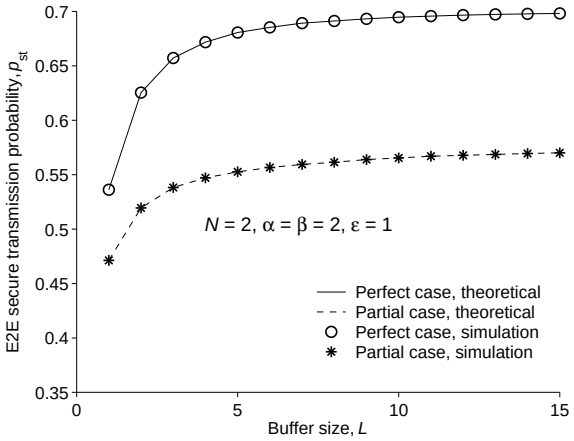


(b) Expected E2E delay vs. number of relays N.

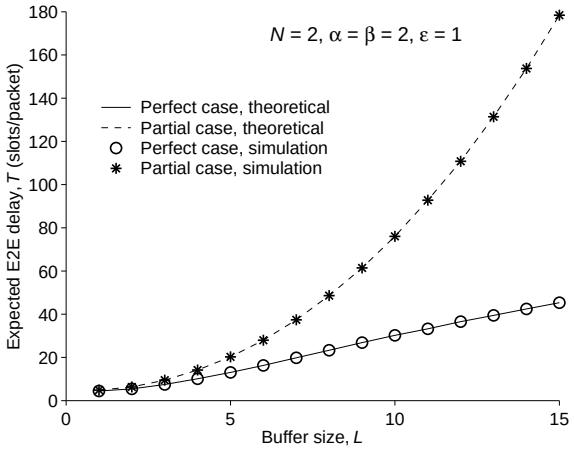
Figure 3.4: E2E STP and expected E2E delay vs. number of relays N.

impact of distributing more relays, which reduces the mean service time in the first hop, while increasing the average queuing delay and mean service time in the second hop. However, the latter impact is dominant, resulting in the increasing behavior of T_Δ vs. N.

Finally, we examine how the p_{st}^{Δ} and T_Δ vary with the buffer size L for a fixed setting of ε and N, as illustrated in Figure 3.5. As can be seen from Figure 3.5 that, both the E2E STP and expected E2E delay increase as the buffer size L increases under both eavesdropper CSI cases, which is due to the similar reason of distributing more relays. Another observation from Figure 3.5a indicates that as the buffer size



(a) E2E STP vs. buffer size L.



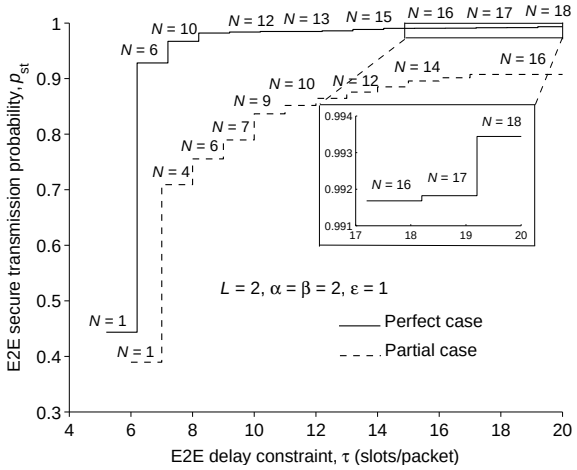
(b) Expected E2E delay vs. buffer size L.

Figure 3.5: E2E STP and expected E2E delay vs. buffer size L.

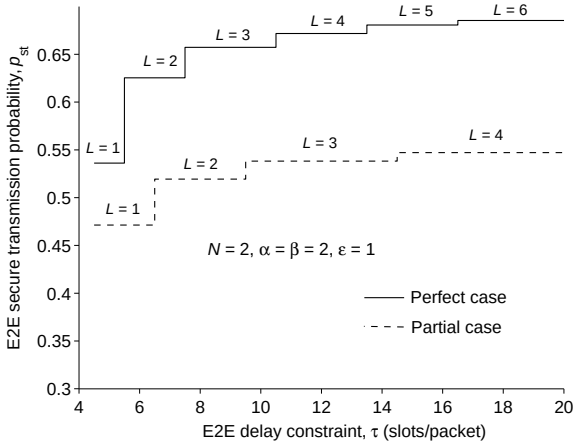
increases above a certain value, for example, $L = 5$ in Figure 3.5a, the E2E STP stays almost constant. This is because that almost all the source-relay and relay-destination links of all relays are available for relay selection, so the instantaneous secrecy capacity of the selected link can hardly be improved.

3.5.4 Security-Delay Trade-Off Analysis

Based on the theoretical results of p_{st}^{Δ} and T_{Δ}, we now investigate the trade-offs between the E2E STP and expected E2E delay of the concerned system with the Max-Ratio buffer aided relay selection schemes.



(a) Maximum achievable E2E STP for varying N.



(b) Maximum achievable E2E STP for varying L.

Figure 3.6: Maximum achievable E2E STP vs. E2E delay constraint τ.

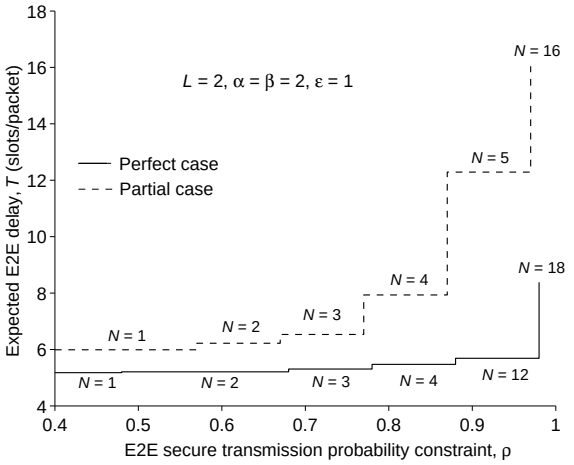
First, we study the achievable E2E STP region under a given constraint on the expected E2E delay in both eavesdropper CSI cases. For the scenario of $\alpha = \beta = 2$ and $\varepsilon = 1$, Figure 3.6a (resp. Figure 3.6b) illustrates the maximum E2E STP p_{st}^{Δ} achieved by the optimal number of relays N (resp. buffer size L) under various expected E2E delay constraints τ for a fixed setting of $L = 2$ (resp. $N = 2$). It can be seen from Figure 3.6a and Figure 3.6b that, as τ increases, the maximum achievable E2E STP increases in both cases, which implies that relaxing the delay constraint can achieve a larger STP region accordingly. This clearly shows the trade-off between the PHY security and delay performances of the system. Another observation from Figure

3.6a (resp. Figure 3.6b) shows that the maximum achievable E2E STP is a piecewise function of τ and an optimal N (resp. L) can apply to a small range of τ.

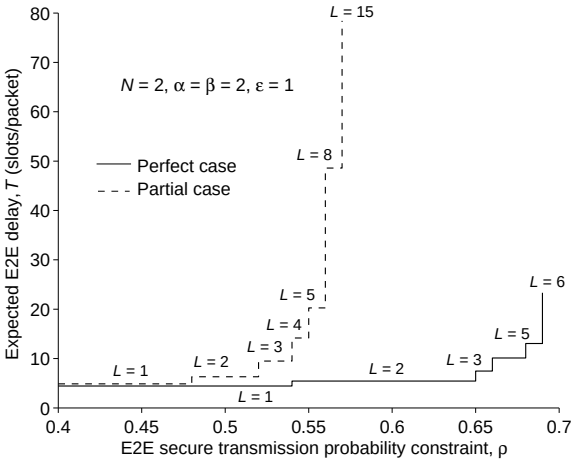
A further careful observation from Figure 3.6 indicates that, as τ scales up, the maximum achievable E2E STP with respect to L in Figure 3.6b becomes less sensitive to the variation of τ (i.e., as τ scales up an optimal L can apply to a wider range of τ), while this is not the case for the maximum achievable E2E STP with respect to N in Figure 3.6a. For example, under the perfect eavesdropper CSI case, as τ increases from 18 to 20, the maximum STP in Figure 3.6b remains unchanged while that in Figure 3.6a increases from 0.9917 to 0.9934. Under the partial eavesdropper CSI case, a similar observation can be found as τ increases from 16 to 18. Thus, compared to the maximum STP achieved by optimal L, the maximum STP achieved by optimal N depends more heavily on the variation of the delay constraint τ.

Next, we explore the achievable expected E2E delay region under a given E2E STP constraint under both eavesdropper CSI cases. For the same scenario of $\alpha = \beta = 2$ and $\varepsilon = 1$, we show in Figure 3.7a (resp. Figure 3.7b) the minimum expected E2E delay achieved by the optimal number of relays N (resp. buffer size L) under various E2E STP constraints ρ for a fixed setting of $L = 2$ (resp. $N = 2$). We can see from Figure 3.7a and Figure 3.7b that, as ρ increases, the minimum achievable expected E2E delay increases in both cases. This suggests that imposing a more stringent security constraint on the E2E packet delivery leads to a smaller delay region, which also illustrates a clear trade-off between the PHY security and delay performances.

It can also be observed from Figure 3.7a and Figure 3.7b that all the curves are truncated at a certain point of ρ (say threshold), i.e., the minimum expected E2E delay becomes indeterminable, as ρ increases above this threshold. For example, this threshold is about 1 (0.99) for the perfect (partial) CSI case in Figure 3.7a and about 0.7 (0.558) for the perfect (partial) CSI case in Figure 3.7b. This is because that, under the fixed setting of $\alpha = \beta = 2$ and $\varepsilon = 1$, the E2E STP of each case finally



(a) Minimum achievable expected E2E delay for varying N.



(b) Minimum achievable expected E2E delay for varying L.

Figure 3.7: Minimum achievable expected E2E delay vs. E2E STP constraint ρ.

converges to the corresponding threshold as N (resp. L) scales up for $L = 2$ (resp. $N = 2$), as can seen from Figure 3.4a (resp. Figure 3.5a). Thus, we cannot find an optimal N or L to satisfy the STP constraints larger than this threshold, so the minimum delay value cannot be determined.

A careful observation from Figure 3.7 indicates that the minimum achievable expected E2E delay in terms of N becomes less sensitive to the variation of ρ, while this is not the case for the minimum achievable expected E2E delay in terms of L. For example, under the perfect eavesdropper CSI case, as ρ increases from 0.5 to

0.6, the minimum E2E delay in Figure 3.7a remains unchanged while that in Figure 3.7b increases from 4.45 to 5.43. Under the partial eavesdropper CSI case, a similar observation can be found as ρ increases from 0.5 to 0.57. Thus, compared to the minimum expected E2E delay achieved by optimal N, the minimum expected E2E delay achieved by optimal L depends more heavily on the variation of STP constraint ρ.

3.6 Summary

This chapter provided analytical study on the end-to-end (E2E) secure transmission probability (STP) and expected E2E delay in a two-hop wireless system with the Max-Ratio buffer-aided relay selection, and explored the corresponding trade-offs between the physical layer (PHY) security and delay performances. The results under both perfect and partial eavesdropper CSI cases indicate that we can achieve a relatively higher E2E STP if a larger E2E delay can be tolerated. In contrast, we can guarantee a smaller E2E delay at the cost of a lower E2E secrecy rate. In particular, we can flexible control the security-delay trade-off in such system by adjusting the number of relays and the relay buffer size. These findings are useful for the design of buffer-aided relay systems in presence of eavesdroppers. Notice that this work considers the RF strategy such that the eavesdropper can only independently decode the signals received in the two hops , so one future research direction is to conduct the performance evaluation of a DF-based buffer-aided relay system where the eavesdropper can combine the signals received in the two hops to achieve a better decoding performance. Since the secrecy capacity formulation of general buffer-aided relay systems remains an open issue by now, it serves as another interesting future research topic.

CHAPTER IV

Physical Layer Security Performance Study of Buffer-Aided Relay Selection Scheme for Two-Hop Wireless Networks with DF Relays

This chapter focuses on the PHY security performance study of buffer-aided relay selection scheme for two-hop wireless networks with DF relays, for which we investigate the E2E STP and expected E2E delay performances of a two-hop relay wireless networks with an eavesdropper who conducts its decoding by combining the signals received in two hops. We consider two cases of the eavesdropper's CSI, i.e., case 1 when the instantaneous CSI of the eavesdropper channels are available, and case 2 when only the distributions of the eavesdropper channels are available. A new buffer-aided relay selection scheme is first proposed for both case 1 and case 2 respectively and the E2E STP and expected E2E delay are then derived in a closed form by adopting the Markov chain theory and Queuing theory. Finally, numerical results are conducted to validate the efficiency of our proposed scheme, the security-delay trade-off issue is addressed and the effects of eavesdropper's decoding strategy on the performances of the concerned network is also studied.

4.1 System Model and Assumptions

We consider a two-hop wireless system as illustrated in Figure 4.1, which consists of one source S, one destination D, N relays R_n ($n = 1, 2, \cdots, N$) adopting the Decode-and-Forward (DF) decoding strategy and an eavesdropper E wiretapping both the source-relay and the relay-destination links. As in [58–60], the DF strategy adopts the same codebook at both the source and relay nodes, thus the eavesdropper in this work can combine the signals received in the two hops to decode the packets. All nodes in the system are assumed to have one antenna and operate in the half-duplex mode such that they cannot transmit and receive signals simultaneously. Each relay R_n is aided by a finite buffer Q_n of size L to store the decoded packets (each packet is with the same bits M) received from S before they are forwarded to the destination D, and the eavesdropper is equipped with an infinite buffer to store the signals received in the first hop. It is obvious that ($0 \leq Q_n \leq L$). We use $\Psi(Q_n)$ to denote the number of packets stored in the buffer Q_n and all packets in the buffer are served in a First-In-First-Out (FIFO) discipline. Thus, if a $S \rightarrow R_n$ transmission succeeds, the corresponding $\Psi(Q_n)$ will be increased by 1. On the contrary, if a $R_n \rightarrow D$ transmission succeeds, the corresponding $\Psi(Q_n)$ will be decreased by 1. Specially, if $\Psi(Q_n) = L$ or $\Psi(Q_n) = 0$, the corresponding $S \rightarrow R_n$ link or $R_n \rightarrow D$ link is denoted as an unavailable link. The source S is assumed to be backlogged and it has the same transmit power P as the relay nodes.

We consider no direct link between S and D due to the path loss or deep shadowing [61], [62] and communication can be conducted only via a relay R_n. Time in the system is partitioned into equal slots, and all channels are assumed to suffer from quasi-static Rayleigh fading, i.e., the channel gains remain constant during one time slot, but change independently and randomly from one slot to the next. The channel gains of the links $S \rightarrow R_n$, $S \rightarrow E$, $R_n \rightarrow D$ and $R_n \rightarrow E$ are denoted as

$|h_{SR_n}|^2$, $|h_{SE}|^2$, $|h_{R_nD}|^2$ and $|h_{SE}|^2$ respectively, and $\mathbb{E}(|h_{SR_n}|^2) = \gamma_{sr}$, $\mathbb{E}(|h_{SE}|^2) = \gamma_{se}$, $\mathbb{E}(|h_{R_nD}|^2) = \gamma_{rd}$ and $\mathbb{E}(|h_{R_nE}|^2) = \gamma_{re}$. Here $\mathbb{E}(\cdot)$ stands for the expectation operator. We assume all source-relay, relay-destination and relay-eavesdropper links are independently and identically distributed (i.i.d.). Furthermore, all noises are assumed to be additive white Gaussian Noise (AWGN) with zero mean and unit variance $\sigma^2 = 1$ as in [63].

In this work, we assume that the instantaneous CSI of legitimate channels (i.e., $|h_{SR_n}|^2$ and $|h_{R_nD}|^2$) are always available. Regarding the CSI of eavesdropper channels, we consider two cases, i.e., the perfect eavesdropper case (Case 1) when the instantaneous eavesdropper CSIs (i.e., $|h_{SE}|^2$ and $|h_{SE}|^2$) are available, and the case 2 when only the distributions of the eavesdropper channels are available. If a relay R_n is selected for transmission, the instantaneous secrecy capacity of the $S \rightarrow R_n$ link or $R_n \rightarrow D$ link for perfect CSI case can be given as [64]

$$C_s^{SR_n} = C_{SR_n} - C_{SE} = log_2\left(\frac{1 + P|h_{SR_n}|^2}{1 + P|h_{SE}|^2}\right), \tag{4.1}$$

and

$$C_s^{R_nD} = C_{R_nD} - C_{R_nE} = log_2\left(\frac{1 + P|h_{R_nD}|^2}{1 + P|h_{R_nE}|^2}\right), \tag{4.2}$$

respectively, where C_{ij} is the instantaneous capacity of the link i to j.

We assume that the instantaneous CSI of the main channels are always available at the destination D, and the instantaneous CSI (distributions) of the eavesdropper channels are available at D for case 1 (case 2). Neither S nor R_n knows the instantaneous CSI of the eavesdropper channels, and we consider no feedback from the receiver. Before each time slot, S transmits a pilot signal to each R_n and each

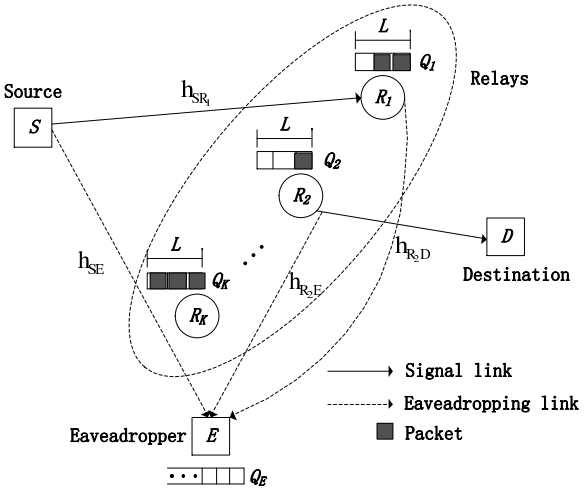


Figure 4.1: Network model.

R_n will transmit a pilot signal to D, thus R_n can get the information $|h_{SR_n}|^2$ and retransmit it to D, and D can thus get the information $|h_{SR_n}|^2$ and $|h_{R_nD}|^2$. Then a relay R_* will be selected as a receiver or a transmitter by the destination D, to receive the packet from S or forward the packet to D according to the relay selection scheme, which will be shown in the following section. Since the instantaneous CSI of the eavesdropper channels are unavailable at S and R_n and there's no feedback from R_n (D) to S (R_n), we consider in this work a fixed secrecy rate ε and a fixed transmission rate r_0. As in [36], the packet cannot be decoded when a transmission outage occurs, i.e., $C < r_0$ and will be eavesdropped by the eavesdropper when the secrecy outage occurs, i.e., $C_s < \varepsilon$. Notice that we assume a high SNR (which can be seen in many available works [33]) in this work, the transmission outage will never occurs during the transmission, i.e., the receiver can always decode the packet.

4.2 New Buffer-Aided Relay Selection Scheme

Most previous buffer-aided selection schemes are limited by the constraint that the eavesdropper can only independently decode the received information as different codebooks are adopted at the source and the relay nodes respectively. In this section,

we will propose new buffer-aided relay selection schemes for two-hop networks with DF relays and an eavesdropper who exploits the combining decoding strategy.

4.2.1 New Buffer-Aided Relay Selection Scheme

Different from most previous buffer-aided relay selection schemes where the message relay is selected based on the link quality and the buffer states of relays in the current time slot, we consider in this work also the decoding strategy of the eavesdropper. Based on the knowledge of the main and eavesdropper channels, we have two buffer-aided relay selection schemes.

Case 1: if the instantaneous CSI of the eavesdropper channels $|h_{SE}|^2$ and $|h_{R_nE}|^2$ are available at the destination, we select the message relay as

$$R_*^{case1} = arg \max_{R_n} \left\{ \frac{|h_{SR_n}|^2 \cdot \mathbf{1}_{\Psi(Q_n)\neq L}}{|h_{SE}|^2}, \frac{|h_{R_nD}|^2 \cdot \mathbf{1}_{\Psi(Q_n)\neq 0}}{|h_{SE}|^2 + |h_{R_nE}|^2} \right\}, \tag{4.3}$$

where $\mathbf{1}_{\Psi(Q_n)\neq L}$ ($\mathbf{1}_{\Psi(Q_n)\neq 0}$) equals 1 if $\Psi(Q_n) \neq L$ ($\Psi(Q_n) \neq 0$), i.e., the relay R_n is available for source-relay (relay-destination) transmission and equals 0 otherwise.

Case 2: if only the distributions of the eavesdropper channels are available at the destination, we select the message relay as

$$R_*^{case2} = arg \max_{R_n} \left\{ \frac{|h_{SR_n}|^2 \cdot \mathbf{1}_{\Psi(Q_n)\neq L}}{\gamma_{se}}, \frac{|h_{R_nD}|^2 \cdot \mathbf{1}_{\Psi(Q_n)\neq 0}}{\gamma_{se} + \gamma_{re}} \right\}, \tag{4.4}$$

where γ_{se} and γ_{re} are the average channel gains of the source-eavesdropper and the relay-eavesdropper channels, respectively.

From (4.3) and (4.4) we can see that, the new buffer-aided relay selection schemes select the message relay from all available relays, which can obtain a full diversity gain as the available buffer-aided relay selection schemes in [33]. However, for a packet transmitted from the source to the destination via a relay R_* which is selected according to the relay selection scheme in networks with RF relays, the packet will

be decoded at the eavesdropper with a higher probability as they consider no effects of the eavesdropper's decoding strategy in their schemes and select the message relay only based on the CSI of the main channels [30–32, 35–37] or CSI of both the main and eavesdropper links in the current time slot [33], which is dangerous for networks with high-security requirement. It is notable that, our new buffer-aided relay selection schemes can address this issue and ensure a strong form of security for the wireless communication. It is because, we select the message relay with the highest channels gain ratio of the main and the eavesdropper channels where the channels gain of the eavesdropper channel for the relay-destination transmission is obtained by combining the signals received in the previous time slot and the current time slot for a tagged packet, which can greatly improve the security of the concerned network.

4.2.2 Performance Metrics

To fully characterize the security and delay performances of the transmission, we adopt the same end-to-end (E2E) delay and E2E secure transmission probability (STP) definitions as in [39]. For a tagged packet from the source to the destination, we denote R_* as the message relay which is selected in two hops to transmit this packet, the **E2E delay** T is formulated as

$$T = T_s + T_r + T_q, \tag{4.5}$$

where T_s (T_r) is the waiting time of the packet at the source S (R_*) before it is transmitted, and T_q denotes the queuing delay which is defined as the time it takes the packet to move from the end to the head of R_*'s queue. The **E2E STP** p_{st} is defined as

$$p_{st} = \mathbb{P}(C_s^{SR_*} \geq \varepsilon, C_s^{R_*D} \geq \varepsilon), \tag{4.6}$$

where $C_s^{SR_*}$ ($C_s^{R_*D}$) denotes the instantaneous secrecy capacity of the $S \to R_*$ ($R_* \to D$) link and $C_s^{SR_*} \geq \varepsilon$ ($C_s^{R_*D} \geq \varepsilon$) represents the event that the $S \to R_*$ ($R_* \to D$) link is selected and secure transmission is conducted when the tagged packet is at S (the head of R_*'s queue).

4.3 E2E STP and Delay Analysis

To derive the E2E delay and E2E STP, we will first provide the state transition matrices in this subsection to depict the delivery process of a tagged packet at the source and the selected relay, which is shown in Lemma 5 and Lemma 6, respectively. Based on the state transition matrices in Lemma 5 and Lemma 6, the E2E STP and E2E delay are then derived in a closed form in Theorem IV.1 and Theorem IV.2, respectively.

Assuming that s_i ($\widetilde{s}_k$) is the buffer state when the tagged packet is at the source (head of the message relay R_*) and

$$s_i = \left[\Psi_{s_i}(Q_1), \Psi_{s_i}(Q_2), \cdots, \Psi_{s_i}(Q_n), \cdots, \Psi_{s_i}(Q_N)\right]^T, \tag{4.13}$$

$$\widetilde{s}_k = \left[\Psi_{\widetilde{s}_k}(Q_1), \cdots, \Psi_{\widetilde{s}_k}(Q_*), \cdots, \Psi_{\widetilde{s}_k}(Q_n), \cdots, \Psi_{\widetilde{s}_k}(Q_N)\right]^T, n \in \{1, \cdots, N\}, n \neq *, \tag{4.14}$$

where $\Psi(Q_n)$ is the number of packets in R_n's buffer and R_* denotes the message relay. It is obvious that each state corresponds to a pair of $(N_1(s), N_2(s))$, where $N_1(s)$, $s \in \{s_i, \widetilde{s}_k\}$ denotes the number of available relays for the source-relay, $N_2(s)$ denotes the number of available relays for the relay-destination transmission, and a relay R_n is available for the source-relay (relay-destination) transmission when $\Psi(Q_n) \neq L$ ($\Psi(Q_n) \neq 0$). Based on the relay selection schemes in (4.3), (4.4), a relay is selected for the source-relay transmission or relay-destination transmission at each time slot, and the number of packets in the relay buffer will increased (decreased) by one if

$$\mu_{\text{case1}}(s) = \sum_{n_1=0}^{N_1(s)} C_{N_1(s)}^{n_1}(-1)^{n_1}\frac{\alpha}{(n_1 2^{\varepsilon}+\alpha)}\left[1-\frac{\gamma_{re}^2}{(\gamma_{rd}+\gamma_{se}2^{\varepsilon})(\gamma_{rd}+\gamma_{re}2^{\varepsilon})}\right]^{N_2(s)}, \quad (4.7)$$

$$\nu_{\text{case1}}(s) = \int_{2^{\varepsilon}}^{\infty}\left[1-\frac{\gamma_{rd}^2}{(\gamma_{rd}+\gamma_{se}x)(\gamma_{rd}+\gamma_{re}x)}\right]^{N_2(s)} \times \sum_{n_1=0}^{N_1(s)}\frac{C_{N_1(s)}^{n_1}(-1)^{n_1+1}\alpha}{(n_1 x+\alpha)^2}dx, \quad (4.8)$$

$$\mu_{\text{case2}}(s) = \left[1-e^{-2^{\varepsilon}/\alpha}\right]^{N_1(s)}\left[1-e^{-2^{\varepsilon}(\gamma_{se}+\gamma_{re})/\gamma_{rd}}\right]^{N_2(s)}, \quad (4.9)$$

$$\nu_{\text{case2}}(s) = \sum_{n_2=0}^{N_2(s)}\sum_{n_1=0}^{N_1(s)-1}\binom{N_2(s)}{n_2}\binom{N_1(s)-1}{n_1}(-1)^{n_2+n_1}\frac{N_1(s)\gamma_{rd}e^{-\frac{n_2\alpha(\gamma_{se}+\gamma_{re})+\gamma_{rd}+n_1\gamma_{rd}}{\alpha\gamma_{rd}}}}{n_2\alpha(\gamma_{se}+\gamma_{re})+\gamma_{rd}+n_1\gamma_{rd}}, \quad (4.10)$$

$$\phi(s) = \sum_{n_1=0}^{N_1(s)}\sum_{n_2=0}^{N_2(s)}\binom{N_1(s)}{n_1}\binom{N_2(s)}{n_2}(-1)^{n_1+n_2}\frac{\alpha\gamma_{rd}}{2^{\varepsilon}[n_1\alpha(\gamma_{se}+\gamma_{re})+n_1\gamma_{rd}]+\alpha\gamma_{rd}}, \quad (4.11)$$

$$\omega(s) = \sum_{n_1=0}^{N_1(s)}\sum_{n_2=0}^{N_2(s)-1}\frac{\binom{N_1(s)}{n_1}\binom{N_2(s)-1}{n_2}(-1)^{n_1+n_2}N_2(s)\alpha^2\gamma_{rd}}{2^{\varepsilon}[n_1\gamma_{rd}+(n_2\alpha-\alpha)(\gamma_{se}+\gamma_{re})]^2+\alpha\gamma_{rd}(n_1\gamma_{rd}+\alpha+n_2\alpha(\gamma_{se}+\gamma_{re}))}. \quad (4.12)$$

---

there is a secure source-relay (relay-destination) transmission. Thus, the relay buffer state may move to several possible states in the next time slot, forming a Markov chain. However, if an outage event occurs, the relay buffer state remain unchanged in the next time slot.

Denoting $\mathbf{A}$ ($\widetilde{\mathbf{A}}$) as the state transition matrix of the Markov chain and $a_{j,i}$ ($\widetilde{a}_{k,l}$) as the entry of $\mathbf{A}$ ($\widetilde{\mathbf{A}}$) for the source-relay (relay-destination) delivery of the tagged packet. Thus, $a_{i,j}$ ($\widetilde{a}_{k,l}$) gives the transition probability that state s_i ($\widetilde{s}_k$) moves to s_j ($\widetilde{s}_l$) in the next time slot. From (4.3) and (4.4), we can see that the selection of a

source-relay link and a relay-destination link at each time slot is not equal. To derive $\mathbf{A}$ ($\widetilde{\mathbf{A}}$), we divide all states that s_i ($\widetilde{s}_k$) can moves to into two sets as in [33], i.e., $\mathcal{S}^+$ ($\widetilde{\mathcal{S}}^+$) and $\mathcal{S}^-$ ($\widetilde{\mathcal{S}}^-$), where $\mathcal{S}^+$ ($\widetilde{\mathcal{S}}^+$) contains all states s_i ($\widetilde{s}_k$) can move to as a secure source-relay transmission is conducted and $\mathcal{S}^-$ ($\widetilde{\mathcal{S}}^-$) contains all states s_i ($\widetilde{s}_k$) can move to as a secure relay-destination transmission is conducted.

Lemma 5 *Suppose that the relay buffers are in state s_i when the tagged packet is at the source node, the (i,j)-th entry of the state transition matrix $\mathbf{A}$ for the source-relay delivery process under case 1 and case 2 is given by*

$$a_{i,j} = \begin{cases} \mu_\Delta(s_i), \text{ if } s_j = s_i, \\ \dfrac{\nu_\Delta(s_i)}{N_1(s_i)}, \text{ if } s_j \in \mathcal{S}_i^+, \\ \dfrac{1-\mu_\Delta(s_i)-\nu_\Delta(s_i)}{N_2(s_i)}, \text{ if } s_j \in \mathcal{S}_i^-, \\ 0, \text{ elsewhere.} \end{cases} \tag{4.15}$$

where $\Delta \in \{\text{case1}, \text{case2}\}$ denotes the eavesdropper CSI case, and $\mu_\Delta(s_i)$ and $\nu_\Delta(s_i)$ are given in (4.7) and (4.8) for case 1, and in (4.9) and (4.10) for case 2 with the parameter $s = s_i$.

Proof 7 *See Appendix B.1 for the proof.*

When the tagged packet is at the source source node, there are possible $(L+1)^N$ buffer states as there are N relays and each relay can store at most L packets in its buffer. Thus, the transition matrix for the source-relay transmission is a $(L+1)^N \times (L+1)^N$ matrix. As in [18], the transition matrix $\mathbf{A}$ is irreducible and aperiodic. Denoting $\boldsymbol{\pi} = [\pi^\Delta_{s_1}, \cdots, \pi^\Delta_{s_i}, \cdots, \pi^\Delta_{s_{(L+1)^N}}]^T$ as the stationary state probability vector of the Markov chain, we have $\mathbf{A}\boldsymbol{\pi} = \boldsymbol{\pi}$ and $\sum_{i=1}^{(L+1)^N} \pi^\Delta_{s_i} = 1$, where $\pi^\Delta_{s_i}$ denotes the stationary probability of state s_i, and from [18], we can get

$$\boldsymbol{\pi} = (\mathbf{A} - \mathbf{I} + \mathbf{B})^{-1}\mathbf{b}, \tag{4.16}$$

where $\mathbf{b} = (1, \cdots, 1)^T$, $\mathbf{I}$ is the identity matrix and $\mathbf{B}$ is an all-one matrix.

Lemma 6 *Suppose that the relay buffers are in state s_k when the tagged packet is at end of the message relay R_*, the (k,l)-th entry of the state transition matrix $\widetilde{\mathbf{A}}$ for the relay-destination delivery process under case 1 and case 2 is given by*

$$\widetilde{a}_{k,l} = \begin{cases} \mu_\Delta(\widetilde{s}_k), \text{ if } \widetilde{s}_l = \widetilde{s}_k, \\ \dfrac{\nu_\Delta(\widetilde{s}_k)}{N_1(\widetilde{s}_k)}, \text{ if } \widetilde{s}_l \in \widetilde{\mathcal{S}}_k^+, \\ \dfrac{1 - \mu_\Delta(\widetilde{s}_k) - \nu_\Delta(\widetilde{s}_k)}{N_2(\widetilde{s}_k) - 1}, \text{ if } \widetilde{s}_l \in \widetilde{\mathcal{S}}_k^-, \\ 0, \text{ elsewhere.} \end{cases} \tag{4.17}$$

where $\Delta \in \{\text{case1}, \text{case2}\}$ denotes the eavesdropper CSI case, $\mu_\Delta(\widetilde{s}_k)$ and $\nu_\Delta(\widetilde{s}_k)$ are given in (4.7) and (4.8) for case 1 and in (4.9) and (4.10) for case 2.

Proof 8 *The proof is same as that for Lemma 5, so we have omitted it here.*

When the tagged packet is at the head of the selected relay R_*, the buffer of R_* cannot be empty and there are only $L \cdot (L+1)^{N-1}$ possible buffer states in total. Thus, the transition matrix $\widetilde{\mathbf{A}}$ is a $L(L+1)^{N-1} \times L(L+1)^{N-1}$ matrix and the stationary probability vector of the Markov chain for the relay-destination delivery process $\widetilde{\boldsymbol{\pi}} = (\pi^\Delta_{\widetilde{s}_1}, \cdots, \pi^\Delta_{\widetilde{s}_k}, \cdots, \pi^\Delta_{\widetilde{s}_{L(L+1)^{N-1}}})^T$ can be determined as

$$\widetilde{\boldsymbol{\pi}} = (\widetilde{\mathbf{A}} - \widetilde{\mathbf{I}} + \widetilde{\mathbf{B}})^{-1}\widetilde{\mathbf{b}}, \tag{4.18}$$

where $\widetilde{\mathbf{b}} = (1, \cdots, 1)^T$, $\widetilde{\mathbf{I}}$ is the identity matrix and $\widetilde{\mathbf{B}}$ is an all-one matrix.

Combing the results in Lemma 5, Lemma 6 and the definitions of E2E STP in (4.6) and the E2E delay in (4.5), the E2E STP and the E2E delay of the system

concerned in this work can be derived as follows.

Theorem IV.1 *Consider the two-hop wireless system in Figure 4.1 and under our the buffer-aided relay selection scheme in Section 4.2, the E2E STP for case 1 can be determined as*

$$p_{st}^{\text{case1}} = \sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\text{case1}} \nu_{\text{case1}}(s_i) \sum_{k=1}^{L(L+1)^{N-1}} \pi_{\widetilde{s}_k}^{\text{case1}} \frac{1-\mu_{\text{case1}}(\widetilde{s}_k)-\nu_{\text{case1}}(\widetilde{s}_k)}{N_2(\widetilde{s}_k)}, \tag{4.19}$$

where s_i ($\widetilde{s}_k$) denotes the buffer state when the tagged packet is at S (the head of a given relay queue), $\pi_{s_i}^{\text{case1}}$ and $\pi_{\widetilde{s}_k}^{\text{case1}}$ are given by (4.16) and (4.18) with $\Delta = \text{case1}$, $\mu_{\text{case1}}(\widetilde{s}_k)$ is given by (4.7) with $s = \widetilde{s}_k$, $\nu_{\text{case1}}(s_i)$ and $\nu_{\text{case1}}(\widetilde{s}_k)$ are given by (4.8) with $s = s_i$ and $s = \widetilde{s}_k$ respectively. The E2E STP for case 2 is given by

$$p_{st}^{\text{case2}} = \sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\text{case2}} \cdot (1-\phi(s_i)-\omega(s_i)) \sum_{k=1}^{L(L+1)^{N-1}} \pi_{\widetilde{s}_k}^{\text{case2}} \frac{\omega(\widetilde{s}_k)}{N_2(\widetilde{s}_k)}, \tag{4.20}$$

where $\pi_{s_i}^{\text{case2}}$ and $\pi_{\widetilde{s}_k}^{\text{case2}}$ are given by (4.16) and (4.18) with $\Delta = \text{case2}$, $\phi(s_i)$ is given by (4.11) with $s = s_i$, $\omega(s_i)$ and $\omega(\widetilde{s}_k)$ are given by (4.12) with $s = s_i$ and $s = \widetilde{s}_k$ respectively.

Proof 9 *The proof is the same as that for the Theorem III.1 in Chapter III with $\pi_{s_i}^{\Delta}$ and $\pi_{\widetilde{s}_k}^{\Delta}$ being replaced by (4.16) and (4.18), $\phi(s_i)$ being replaced by (4.11), and $\omega(s_i)$ and $\omega(\widetilde{s}_k)$ being replaced by (4.12), respectively.*

Now we are ready to give the following theorem regarding the expected E2E delay of the system.

Theorem IV.2 *Consider the two-hop relay wireless system as illustrated in Figure 4.1. Under the buffer-aided relay selection scheme in Section 4.2, the E2E delay of*

the system for both case 1 and case 2 can be determined as

$$T_{\Delta} = \frac{1+\frac{1}{N}\sum\limits_{i=1}^{(L+1)^N}\sum\limits_{n=1}^{N}\pi_{s_i}^{\Delta}\Psi_{s_i}(Q_n)}{\sum\limits_{i=1}^{(L+1)^N}\pi_{s_i}^{\Delta}\nu_{\Delta}(s_i)} + \frac{1}{\sum\limits_{k=1}^{L(L+1)^{N-1}}\pi_{\widetilde{s}_k}^{\Delta}\frac{(1-\mu_{\Delta}(\widetilde{s}_k)-\nu_{\Delta}(\widetilde{s}_k))}{N_2(\widetilde{s}_k)}}, \quad (4.21)$$

where $\Delta \in \{\text{case1}, \text{case2}\}$, $\pi_{s_i}^{\Delta}$ *is given by (4.16),* $\nu_{\Delta}(s_i)$ *is given in Lemma 5,* $\pi_{\widetilde{s}_k}^{\Delta}$ *is given by (4.18),* $\mu_{\Delta}(\widetilde{s}_k)$ *and* $\nu_{\Delta}(\widetilde{s}_k)$*) are given in Lemma 6.*

Proof 10 *The proof is the same as that that for the Theorem III.2 in Chapter III with* $\pi_{s_i}^{\Delta}$ *and* $\pi_{\widetilde{s}_k}^{\Delta}$ *being replaced by (4.16) and (4.18),* $\mu_{\Delta}(s_i)$ *being replaced by* $\mu_{\Delta}(s_i)$ *in Lemma 5, and* $\mu_{\Delta}(\widetilde{s}_k)$ *and* $\nu_{\Delta}(\widetilde{s}_k)$ *being replaced by* $\mu_{\Delta}(\widetilde{s}_k)$ *and* $\nu_{\Delta}(\widetilde{s}_k)$ *in Lemma 6, respectively.*

4.4 Numerical Results and Discussions

In this section, we first provide simulation results to verify the theoretical models for the E2E STP and expected E2E delay, then proceed to study the security-delay trade-off in our concerned network, and finally comparisons will be made between our proposed schemes and the Max-Ratio relay selection scheme to explore the effects of eavesdropper's decoding strategy on the E2E STP and delay performances.

4.4.1 Simulation Settings

A dedicated C++ simulator was developed to simulate the E2E delivery process of the packet based on our proposed buffer-aided relay selection schemes in (4.3) and (4.4) respectively, where the transmission power of each node is set as $P = 15$ and the noise variance $\sigma^2 = 1$. In all simulations, the total time slots is fixed as 10^5, and the buffer-aided relay selection scheme is performed once per time slot for both case 1 and case 2. The average channel gains of the main and eavesdropper links γ_{sr}

and γ_{rd} are set as $\gamma_{sr} = \gamma_{rd} = 5$ dB. Thus, the corresponding SNR is high enough to guarantee the successful decoding of each packet at the relays and destination. The average channel gains of the eavesdropper channels γ_{se} and γ_{re} are set as $\frac{\gamma_{sr}}{\alpha}$ and $\frac{\gamma_{rd}}{\beta}$ respectively, where α and β are the channel gain ratios of the main and eavesdropper links. The simulated E2E STP is calculated as

$$p_{st} = \frac{N_s}{N_t}, \tag{4.22}$$

where N_s is the number of packets securely transmitted to the destination D and N_t denotes the number of totally transmitted packet from the source S. The simulated expected E2E delay is calculated as

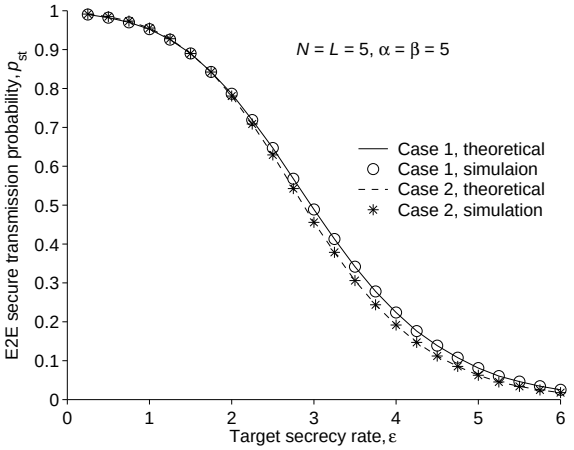
$$T = \frac{T_t}{N_s}, \tag{4.23}$$

where T_t is the total E2E delay (measured in time slots) of all packets reached at D.

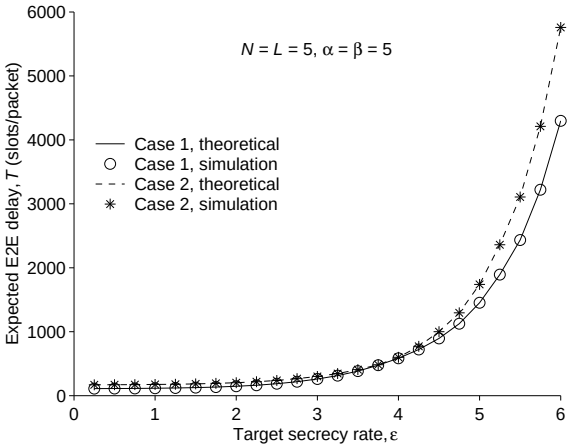
4.4.2 Model Validation

Extensive numerical results have been conducted to verify the theoretical results of the E2E STP and expected E2E delay. For the network scenario of $N = L = 5$, we first conduct simulation results of E2E STP and expected E2E delay under various settings of the target secrecy rate ε. The corresponding simulated and theoretical results of E2E STP p_{st}^{Δ} ($\Delta \in \{case1, case2\}$) are shown in Figure 4.2a, and the results of expected E2E delay T_{Δ} are depicted in Figure 4.2b, for both case 1 and case 2 respectively. We can see from Figure 4.2 that the simulation results match nicely with the theoretical ones for both cases, which indicates that our theoretical framework is highly efficient in depicting the E2E delivery process of the packet in the concerned network.

Then, with the network settings of $L = 5$, $\alpha = \beta = 5$ and $\varepsilon = 2$, we provide plots



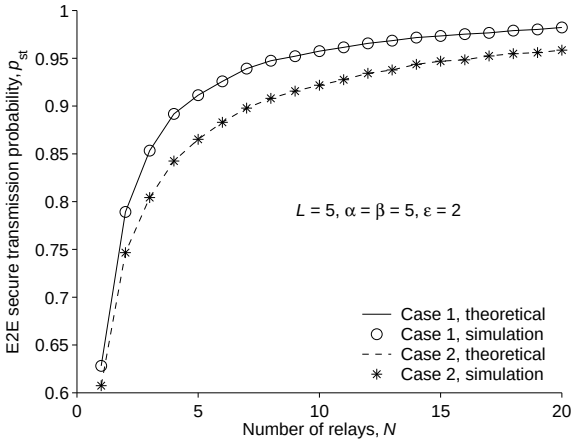
(a) E2E STP vs. target secrecy rate ε.



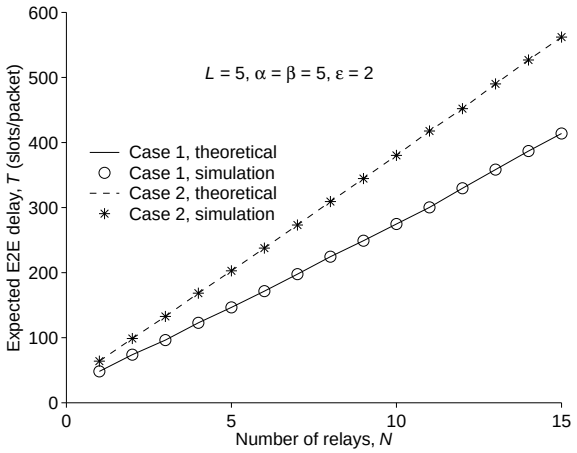
(b) Expected E2E delay vs. target secrecy rate ε.

Figure 4.2: Simulation results vs. theoretical results for E2E STP and expected E2E delay with different target secrecy rate ε.

of the theoretical and simulated results of the p_{st}^{Δ} and T_{Δ} under various value of the number of relays N in Figure 4.3, and for network settings of $N = 5$, $\alpha = \beta = 2$ and $\varepsilon = 2$ under various value of the relay buffer size L in Figure 4.4. It can be observed from Figure 4.3 and Figure 4.4 that all the simulations results can match the theoretical results very nicely, indicating that our theoretical framework is highly efficient for the p_{st}^{Δ} and T_{Δ} modeling.



(a) E2E STP vs. number of relays N.

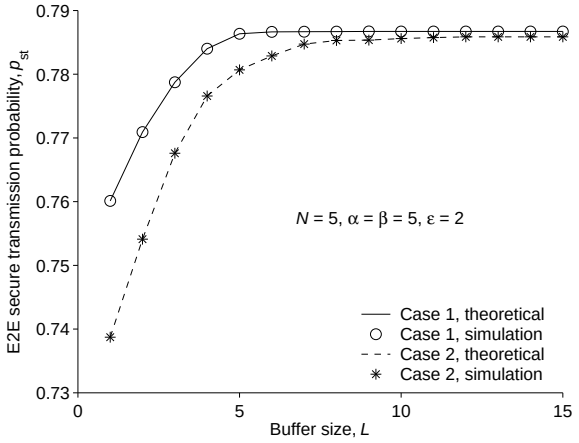


(b) Expected E2E delay vs. number of relays N.

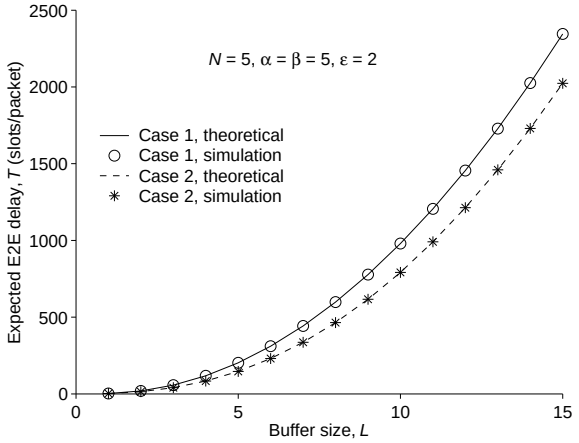
Figure 4.3: Simulation results vs. theoretical results for E2E STP and expected E2E delay with different number of relays N.

4.4.3 Performance Discussion

Based on our theoretical results, we now study the effects of the network parameters (e.g., ε, N and L) on the security and delay performances (p_{st}^{Δ} and T_{Δ}) of the concerned system. Regarding the effects of target secrecy rate ε, we can see from Figure 4.2 that the p_{st}^{Δ} decreases as the target secrecy rate ε increases and the T_{Δ} increases as ε increases in both case 1 and case 2. This is because that, the buffer-aided relay selection scheme (See Section 4.2) allows a packet to be transmitted only if the instantaneous secrecy capacity of the selected link is higher than ε. So, as ε increases,



(a) E2E STP vs. buffer size L.



(b) Expected E2E delay vs. buffer size L.

Figure 4.4: Simulation results vs. theoretical results for E2E STP and expected E2E delay with different buffer size L.

the probability of securely transmitting a packet will decrease for each transmission, which will result in a lower p_{st}^{Δ}. Moreover, as the packet has to be stored in the relay buffer to wait for the next transmission if the current link is not secure, which will cause a larger queuing delay of the packet and thus a higher T_{Δ}.

For the effects of the number of relays N on the p_{st}^{Δ} and T_{Δ}, we can see from Fig 4.3a that the p_{st}^{Δ} increases as N increases for both case 1 and case 2, and from 4.3b that T_{Δ} also increases as the number of relays N increases. This is because that more relays will introduce more available links for the transmission and thus a higher p_{st}^{Δ}. On the other hand, however, more relays will result in a higher queuing delay and

mean service time in the second hop. Thus, T_Δ increases as the number of relays N increases.

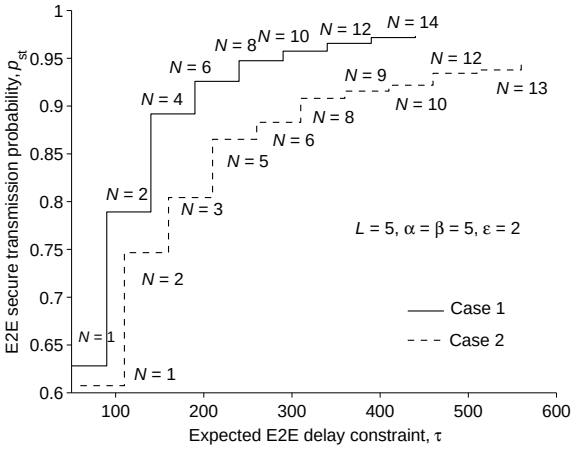
Finally, for the effects of the number of relays N on the p_{st}^Δ and T_Δ, we can observe from Figure 4.4 that p_{st}^Δ and T_Δ increase as L increases for both case 1 and case 2, which is due to the similar reason of introducing more relays in the system. We can also see from Figure 4.4a that p_{st}^Δ tends to be a constant as the relay buffer size L increases above a certain value. This occurs due to the relay that almost all links are available for either the source-relay or relay-destination transmissions as the relay buffer size increases above a certain value, thus the link quality of the selected link at each time slot can hardly to be improved, which will cause a constant E2E STP.

4.4.4 Security-Delay Trade-Off Analysis

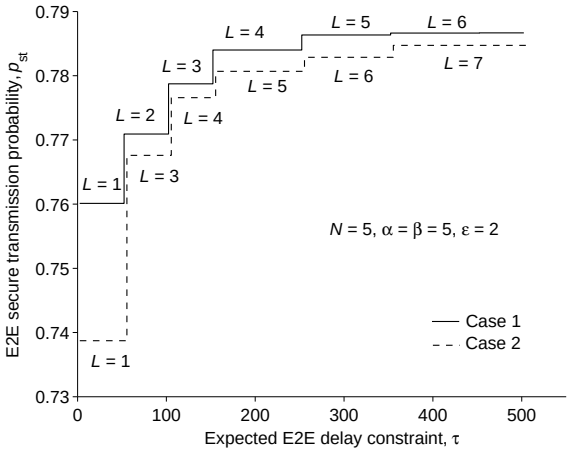
Based on the theoretical results of p_{st}^Δ and T_Δ, we now investigate the trade-off between the E2E STP and the expected E2E delay with the new buffer-aided relay selection scheme in Section 4.2.

Set $\alpha = \beta = 5, \varepsilon = 2$, we illustrate in Figure 4.5a for $L = 5$ and in Figure 4.5b for $N = 5$ the maximum achievable E2E STP vs. the expected E2E delay constraint τ, respectively. From curves in Figure 4.5a and Figure 4.5b we can see that, the achievable E2E STP increases when τ increases in both case 1 and case 2. This indicates that, as the E2E delay constraint of the network is relaxed, i.e., a higher delay can be tolerated, a higher maximum E2E STP performance can be achieved. This clearly shows the trade-off between the E2E security and delay performances of the system. Moreover, according to results Figure 4.5a (Figure 4.5b), we can select an optimal N (L) for the corresponding maximum E2E STP for each given delay constraint τ of the network.

Then, we can carefully observe from Figure 4.5 that, as the delay constraint τ scales up, the maximum E2E STP in Figure 4.5b has different trend as that in Figure



(a) Maximum achievable E2E STP for varying L.

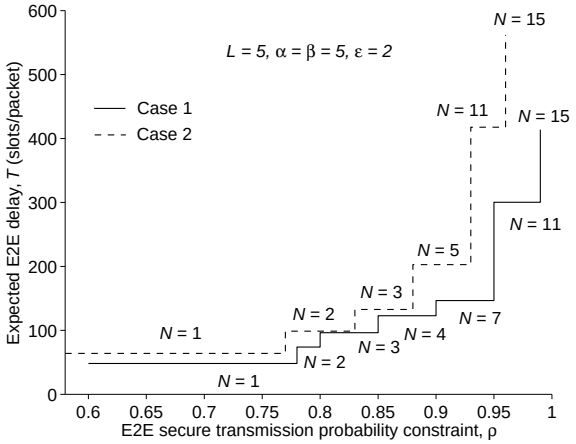


(b) Maximum achievable E2E STP for varying N.

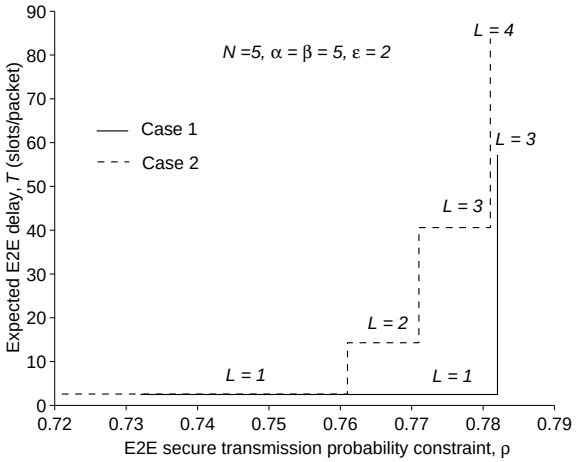
Figure 4.5: Maximum achievable E2E STP vs. expected E2E delay constraint τ.

4.5a. For example, in case 1, as τ varies from 0 to 100, the maximum E2E STP in Figure 4.5a changes from 0.63 to 0.79, while the maximum E2E STP in Fig 4.5b increases from 0.76 to 0.77. In case 2, as τ increases from 100 to 200, the maximum E2E STP in Figure 4.5a varies from 0.766 to 0.779, while the maximum E2E STP in Fig 4.5b increases from 0.75 to 0.8. Thus, we can conclude that, the maximum achievable E2E STP respect to N are more sensitive to the delay constraint τ.

Figure 4.6a and Figure 4.6b show the corresponding achievable expected E2E delay under a given E2E STP constraint ρ for fixed $L = 5$ and fixed $N = 5$ in both case 1 and case 2, respectively. It can be seen from Figure 4.6a and Figure 4.6b that



(a) Minimum achievable expected E2E delay for varying N.



(b) Minimum achievable expected E2E delay for varying L.

Figure 4.6: Minimum achievable expected E2E delay vs. E2E STP constraint ρ.

the minimum achievable expected E2E delay increases as the E2E STP constraint ρ increases. Notice that a higher ρ means a higher security requirement of the system. Thus, the results in Figure 4.6a and Figure 4.6b indicate that, to improve the security performance of the system, extra delay will be introduced in the system, which also shows the trade-off between the E2E security and delay performances of the concerned system.

We can also see from Figure 4.6a and Figure 4.6b that, as the E2E STP constraint ρ increases above a certain value, the minimum expected E2E delay becomes indeter-

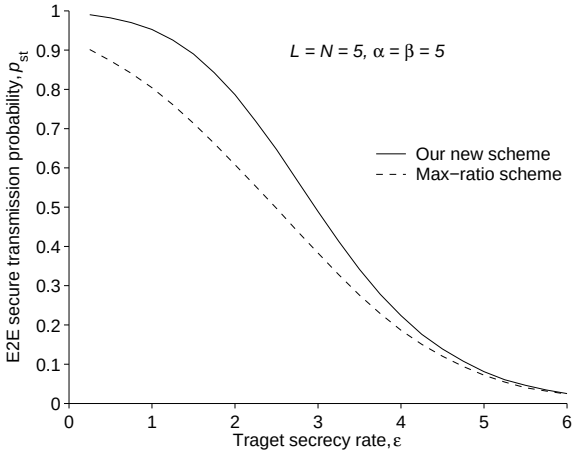
minable. This is because that, for given α, β and the target secrecy rate ε, the E2E STP will finally converges to the corresponding threshold as N (resp. L) increase (See results in Figure 4.6a and Figure 4.6b). Thus, as ρ increases above a certain value, we cannot determine the corresponding L and N and the minimum expected E2E delay thus cannot be determined.

A further observation from Figure 4.6a and Figure 4.6b shows that, as ρ increases, the trend of minimum expected E2E delay respect to N and L are different. For example, as ρ increases from 0.72 to 0.8 in case 1, the minimum E2E delay increases from 50 to 65 in Figure 4.6b while the minimum E2E delay increases from 3 to 56 in Figure 4.6a. In case 2, as ρ increases from 0.72 to 0.8, the minimum E2E delay in Figure 4.6b increases from 70 to 100, but the minimum E2E delay in Figure 4.6a increases from 3 to 90. Thus, compared with the minimum achievable expected E2E delay respect to N, the minimum achievable expected E2E delay respect to L depends more heavily on ρ.

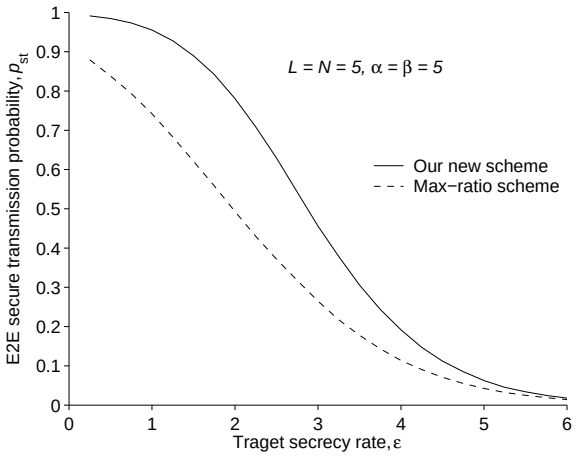
4.4.5 Effects of Eavesdropper's Decoding Strategy on E2E STP and E2E Delay

Based on our theoretical results, we explore in this section the effects of eavesdropper's decoding strategy on the E2E STP and the expected E2E delay performances of different buffer-aided relay selection schemes.

In Figure 4.7, we plot the E2E STP of the Max-Ratio buffer-aided relay selection scheme and our proposed scheme for network settings of $N = L = 5, \alpha = \beta = 5$ in both case 1 (resp. Figure 4.7a) and case 2 (resp. Figure 4.7b) by varying the target secrecy rate ε. We can see from the Figure 4.7 that E2E STP of our new proposed buffer-aided relay selection scheme is always higher than that of the conventional Max-Ratio buffer-aided relay section scheme, showing that our proposed new relay selection scheme outperforms the Max-Ratio buffer-aided relay selection scheme in



(a) E2E STP vs. target secrecy rate ε with different relay selection schemes for case 1.

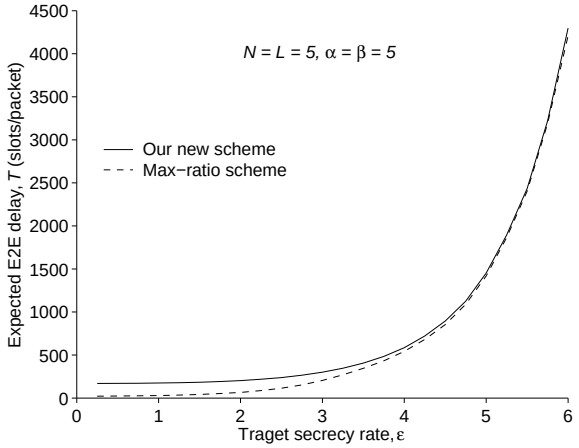


(b) E2E STP vs. target secrecy rate ε with different relay selection schemes for case 2.

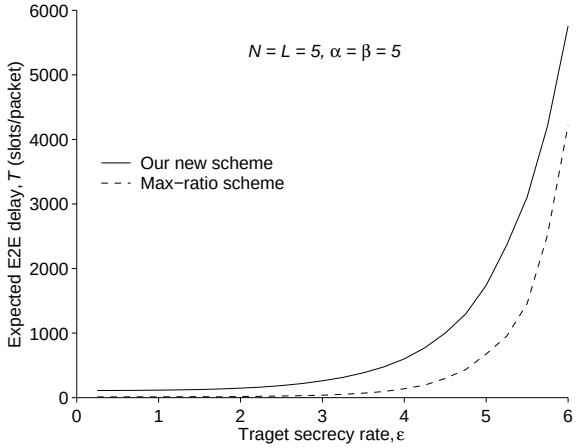
Figure 4.7: E2E STP vs. target secrecy rate ε with different relay selection schemes.

terms of the E2E STP for both case 1 and case 2. This indicates that, by considering the decoding strategy of the eavesdropper in the design of the buffer-aided relay selection scheme, the security performance of the network can be largely improved.

In. Figure 4.8, we show the expected E2E delay of the Max-Ratio buffer-aided relay selection scheme and our proposed scheme for network settings of $N = L = 5, \alpha = \beta = 5$ in both case 1 (resp. Figure 4.8a) and case 2 (resp. Figure 4.8b) by varying the target secrecy rate ε. We can observe from Figure 4.8 that, the expected E2E delay of our scheme is higher than that of the Max-Ratio buffer-aided relay



(a) Expected E2E delay vs. target secrecy rate ε with different relay selection schemes for case 1.



(b) Expected E2E delay vs. target secrecy rate ε with different relay selection schemes for case 2.

Figure 4.8: Expected E2E delay vs. target secrecy rate ε with different relay selection schemes.

selection scheme. This is because, in our buffer-aided relay selection scheme, the packet has to wait longer in the relay buffer for a strong link, which will result in a larger queuing delay of the packet and thus a higher expected E2E delay.

4.5 Summary

This chapter investigates the buffer-aided relay selection scheme design for two-hop wireless networks with DF relays. Unlike the available buffer-aided relay selection

schemes, the proposed buffer-aided relay selection scheme can defence the combining decoding by the eavesdropper. The E2E STP and expected E2E delay are derived in a closed for to validate the efficiency of the proposed scheme. The security-delay trade-off issue is addressed to explore the maximum achievable E2E STP (minimum achievable expected E2E delay) under a given expected E2E delay constraint (E2E STP constraint). Moreover, the effects of the eavesdropper's decoding strategy on the security and delay performances are examined. Results show that our proposed buffer-aided relay selection scheme outperforms the Max-Ratio buffer-aided relay selection scheme in terms of the E2E STP. Since the packet in this work has to wait for a longer time in the relay buffer, which will result in a larger E2E delay. Thus, we will consider in our future work a delay-reduced buffer-aided relay selection scheme design for secure two-hop wireless networks.

CHAPTER V

Conclusions

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

5.0.1 Summary of the Thesis

In this thesis, we studied the PHY security performances of two-hop wireless networks, where the PHY security technique of buffer-aided relay selection is adopted to ensure security of the communication. We first explored the E2E PHY security performance of buffer-aided relay selection scheme for two-hop wireless networks with RF relays, and then investigated the E2E PHY security performance of buffer-aided relay selection scheme for two-hop wireless networks with DF relays.

For the PHY security performance of buffer-aided relay selection scheme for two-hop wireless networks with RF relays, we studied in Chapter III the E2E STP and expected E2E delay of a two-hop wireless network with one source-destination pair, multiple relays each having a finite buffer and an eavesdropper who can only independently decode its received packets. A general framework is first developed to characterize the E2E delivery process of a tagged packet for the Max-Ratio buffer-aided relay selection scheme. Based on the theoretical framework, we then determined the E2E STP and the expected E2E delay of the scheme. The main results in Chapter

III showed that there is a clear trade-off between the E2E security performance and delay performance in the concerned system. For example, if we impose a larger upper bound (i.e., a less strict constraint) on the expected E2E delay, the maximum E2E STP (in terms of either relay buffer size or number of relays) tends to increase, and such trend is more sensitive to the variation of the number of relays than that of the relay buffer size. On the other hand, if we impose a smaller lower bound (i.e., a more strict constraint) on the E2E STP, the minimum expected E2E delay (in terms of either relay buffer size or number of relays) tends to decrease, and this trend is more sensitive to the variation of the relay buffer size than that of the number of relays. This work is very important and can be future explored as guidelines for the design of future networks.

For the PHY security performance of buffer-aided relay selection scheme with two-hop wireless networks with DF relays, we investigated in Chapter IV the E2E STP and expected E2E delay of a two-hop wireless network with one source-destination pair, multiple relays and an eavesdropper who can combine the signals received in two hops to conduct its decoding. We consider two eavesdropper CSI cases, i.e., the case 1 where the instantaneous CSI of the eavesdropper channels are available, and the case 2 where only distributions of the eavesdropper channels are available. Two buffer-aided relay selection schemes were proposed to resist the combining decoding of the packets by the eavesdropper such that the security performance of the concerned network can be improved. Expressions of the E2E STP and expected E2E delay were derived in a closed form to validate the efficiency of the proposed buffer-aided relay selection schemes. The security-delay trade-off was explored and the comparisons were made between our proposed buffer-aided relay selection scheme and the conventional Max-Ratio buffer-aided relay selection scheme to explore the effects of eavesdropper's decoding strategy on the network performances. The results in Section IV indicated that our new scheme outperforms the Max-Ratio buffer-aided relay selection scheme

in terms of the E2E STP. With this work, we can provide theoretical models for the two-hop wireless networks with DF relays, which can be applied for the performance study of general multi-hop networks.

5.0.2 Future Works

The work presented in this thesis can be extended in many interesting directions.

- **Packet delay-reduced buffer-aided relay selection scheme design for two-hop wireless networks.** In this thesis, we mainly focus on buffer-aided relay selection schemes to enhance the security of wireless networks which is also the main goals of available work. However, the packet in the relay buffer may have to wait for a very long time for a good link. Since then the introduction of buffers at the relays will naturally make a large packet delay for the concerned network, especially for delay-sensitive networks. So a meaningful and interesting work is to study the packet delay-reduced buffer-aided relay selection scheme for secure wireless networks to explore or impose constraint on the maximum delay that can be tolerated. For example, if the delay is near the maximum allowable value, the relay may be forced to transmit the packet regardless of the link quality. Another idea is that we can design the relay selection scheme based on the states of the relay buffers, and give priority to relays whose buffer is nearly full or empty.

- **Secrecy capacity analysis for buffer-aided relay wireless networks.** Due to the buffer-aided relay selection schemes adopted in this thesis, the secrecy capacity formulation of an individual link is enough for us to derive the main results in this thesis, i.e., the E2E secure transmission probability and the expected E2E delay. This is because that, based on the buffer-aided relay selection schemes adopted in this thesis, in each time slot we select a best relay for trans-

mission from all relays only based on the instantaneous secrecy capacity of each link and states of all relay buffers. Thus, the above secrecy capacity formulation of an individual link is enough for us to derive the main results in this thesis. But the secrecy capacity formulation of the overall buffer-aided relay networks is still an open problem. This is because that in such system, 1) each packet now may go through three processes, i.e., the source-relay transmission process, queuing process in a relay buffer and the relay-destination transmission process; 2) in each time slot, there are three possible transmission states, i.e., source-relay transmission, relay-destination transmission and no transmission. These two basic properties make the time T' it takes to transmit a packet from the source to the destination highly uncertain (T' can vary from 2 to infinite), and the possible number of transmission states during these T time slots is in the order of $\mathrm{O}(3^{T'})$. These two main issues make the secrecy capacity formulation and analysis of the buffer-aided relay system highly challenging (if not impossible). Therefore, a new and dedicated study is deserved on the secrecy capacity formulation of the general buffer-aided relay systems, and the study of this topic is of great importance for the secrecy capacity of buffer-aided relay wireless networks.

- **f-cast buffer-aided relaying scheme in wireless networks.** Available buffer-aided relay selection schemes for secure two-hop wireless networks always select only one relay for the data transmission, making most of the relay nodes non-transmitting during each transmission. This is a waste of the network resource. Moreover, the data may have to wait for a long time to be securely transmitted to the destination if the link from/to the message relay is not secure, which will cause a larger delay of the data. While selecting multiple message relays before each transmission can not only improve the security performance of the network, but also can reduce the network delay. This is due

to two reasons: 1) Any secure transmission of the selected multiple message relays means a secure and successful transmission of the network, i.e., a higher secure transmission probability of the network; 2) The more message relays, the higher probability to securely transmit the data, and thus a lower waiting time of the data, which will lead to a lower delay performance of the network. Therefore, the study of buffer-aided relay selection with multiple message relays is an interesting and meaningful future direction for performances of secure two-hop wireless networks. Actually, we can select the top n "best" relay as the message relays based on the link quality and the states of relay buffers to help the transmission of a tagged packet.

APPENDICES

APPENDIX A

Proofs in Chapter III

A.1 Proof of Lemma 1

We first provide proof for the perfect eavesdropper CSI case. Let $X = \frac{\max\limits_{R_n:\Psi_{s_i}(Q_n)\neq L}\{|h_{SR_n}|^2\}}{|h_{SE}|^2}$ and $Y = \max\limits_{R_n:\Psi_{s_i}(Q_n)\neq 0}\{\frac{|h_{R_nD}|^2}{|h_{R_nE}|^2}\}$. From [33], we know that the cumulative distribution functions (CDFs) of X and Y are

$$F_X(x) = \sum_{n_1=0}^{N_1(s_i)} \binom{N_1(s_i)}{n_1} (-1)^{n_1} \frac{\alpha}{n_1 x + \alpha}, \tag{A.1}$$

and

$$F_Y(y) = \left(\frac{y}{\beta + y}\right)^{N_2(s_i)}, \tag{A.2}$$

respectively, where $\alpha = \frac{\gamma_{sr}}{\gamma_{se}}$, $\beta = \frac{\gamma_{rd}}{\gamma_{re}}$. According to the relay selection scheme in (3.4) and (3.5), transmission at each time slot occurs on the link with instantaneous channel gain $\max\{X, Y\}$. According to the transmission scheme in Section 3.2.2, the probability of no state transition (i.e., $s_j = s_i$) equals the probability of $R_s < \varepsilon$. Thus,

$a_{i,i}$ can be given by

$$a_{i,i} = \mathbb{P}\left(\log(\max\{X,Y\}) < \varepsilon\right) \tag{A.3}$$

$$= \mathbb{P}(\max\{X,Y\} < 2^{\varepsilon}) \tag{A.4}$$

$$= F_X(2^{\varepsilon}) \cdot F_Y(2^{\varepsilon}) \tag{A.5}$$

$$= \mu_{\mathrm{PF}}(s_i), \tag{A.6}$$

where $\mu_{\mathrm{PF}}(s_i)$ is given in (3.9) with $s = s_i$ and the last step follows after substituting (A.1) and (A.2) into (A.3). Next, the probability that s_i moves to $\mathcal{S}_i^-$ can be given by

$$\mathbb{P}(\mathcal{S}_i^-|s_i) = \mathbb{P}\left(\max\{X,Y\} \geq 2^{\varepsilon}, X < Y\right) \tag{A.7}$$

$$= \int_0^{2^{\varepsilon}} \mathbb{P}(Y \geq 2^{\varepsilon}) f_X(x)\mathrm{d}x + \int_{2^{\varepsilon}}^{\infty} \mathbb{P}(Y > x) f_X(x)\mathrm{d}x \tag{A.8}$$

$$= 1 - \mu_{\mathrm{PF}} - \int_{2^{\varepsilon}}^{\infty} F_Y(x) f_X(x)\mathrm{d}x \tag{A.9}$$

$$= 1 - \mu_{\mathrm{PF}}(s_i) - \nu_{\mathrm{PF}}(s_i), \tag{A.10}$$

where $\nu_{\mathrm{PF}}(s)$ is given in (3.10) with $s = s_i$. Due to the i.i.d. property of channels, the selection of one particular link within all available relay-destination links is equally likely. Thus, for any state $s_n \in \mathcal{S}_i^-$, $a_{i,j} = \frac{1-\mu_{\mathrm{PF}}(s_i)-\nu_{\mathrm{PF}}(s_i)}{N_2(s_i)}$. Notice that the buffer state can only move from s_i to s_i itself, the states in $\mathcal{S}_i^-$ or $\mathcal{S}_i^+$. Hence, for any state $s_j \in \mathcal{S}_i^+$, $a_{i,j} = \frac{\nu_{\mathrm{PF}}(s_i)}{N_1(s_i)}$.

Next, we provide proof for the partial eavesdropper CSI case. We first define new random variables $X' = \frac{\max\limits_{R_n:\Psi_{s_i}(Q_n)\neq L}\{|h_{SR_n}|^2\}}{\gamma_{se}}$ and $Y' = \frac{\max\limits_{R_n:\Psi_{s_i}(Q_n)\neq 0}\{|h_{R_nD}|^2\}}{\gamma_{re}}$ with CDF given by $F_{X'}(x) = (1-e^{-\frac{x}{\alpha}})^{N_1(s_i)}$ and $F_{Y'}(y) = (1-e^{-\frac{y}{\beta}})^{N_2(s_i)}$, respectively. Following the proof for the perfect eavesdropper CSI case, we can calculate the state transition probabilities $a_{i,j}$ for $s_j = s_i$, $s_j \in \mathcal{S}_i^-$ and $s_j \in \mathcal{S}_i^+$ as $\mu_{\mathrm{PT}}(s_i)$, $\frac{1-\mu_{\mathrm{PT}}(s_i)-\nu_{\mathrm{PT}}(s_i)}{N_2(s_i)-1}$ and

$\frac{\nu_{\mathrm{PT}}(s_i)}{N_1(s_i)}$ respectively, where

$$\mu_{\mathrm{PT}}(s_i) = F_{X'}(2^{\varepsilon}) \cdot F_{Y'}(2^{\varepsilon}), \tag{A.11}$$

is given by (3.11) after substituting $F_{X'}(2^{\varepsilon})$ and $F_{Y'}(2^{\varepsilon})$ in and

$$\nu_{\mathrm{PT}}(s_i) = \int_{2^{\varepsilon}}^{\infty} F_{Y'}(x) f_{X'}(x) \mathrm{d}x \tag{A.12}$$

is given by (3.12) after calculating the above integral.

APPENDIX B

Proofs in Chapter IV

B.1 Proof of Lemma 5

We first provide proof for the case 1. Assuming that $X = \arg \max_{R_n:\Psi_{s_i}(Q_n)\neq L} \frac{|h_{SR_n}|^2}{|h_{SE}|^2}$, $Y = \arg \max_{R_n:\Psi_{s_i}(Q_n)\neq 0} \frac{|h_{R_nD}|^2}{|h_{SE}|^2+|h_{R_nE}|^2}$. From [33], we know that the cumulative distribution function (CDF) of X is

$$F_X(x) = \sum_{n_1=0}^{N_1(s_i)} \binom{N_1(s_i)}{n_1} (-1)^{n_1} \frac{\alpha}{n_1 x + \alpha}, \tag{B.1}$$

where $\alpha = \frac{\gamma_{sr}}{\gamma_{se}}$. Then, let $Y_1 = |h_{R_nD}|^2$,$Y_2 = |h_{SE}|^2 + |h_{R_nE}|^2$, the CDF of $\frac{Y_1}{Y_2}$ can be determined as

$$
\begin{aligned}
F_{\frac{Y_1}{Y_2}}(y) &= \mathbb{P}(Y_1 \leq Y_2 y) \\
&= \int_0^\infty F_{y_1}(y_2 y) f_{Y_2}(y_2) dy_2 \\
&= \int_0^\infty \left(1 - e^{-\frac{y_2 y}{\gamma_{rd}}}\right) \times \frac{1}{\gamma_{se} - \gamma_{re}} \left(e^{-\frac{y_1}{\gamma_{se}}} + e^{-\frac{y_1}{\gamma_{re}}}\right) dy_2 \\
&= \frac{1}{\gamma_{se} - \gamma_{re}} \int_0^\infty \left(1 - e^{-\frac{y_1 y}{\gamma_{rd}}}\right) \times \left(e^{-\frac{y_1}{\gamma_{se}}} + e^{-\frac{y_1}{\gamma_{re}}}\right) dy_2 \\
&= 1 - \frac{\gamma_{rd}^2}{(\gamma_{rd} + \gamma_{se} y)(\gamma_{rd} + \gamma_{re} y)}, \qquad \text{(B.2)}
\end{aligned}
$$

where

$$
F_{Y_1}(y_1) = 1 - e^{-\frac{y_1}{\gamma_{rd}}}, \qquad \text{(B.3)}
$$

and

$$
F_{Y_2}(y_2) = \frac{1}{\gamma_{se} - \gamma_{re}} \left(e^{-\frac{y_2}{\gamma_{se}}} + e^{-\frac{y_2}{\gamma_{re}}}\right). \qquad \text{(B.4)}
$$

Thus, based on the probability theory, the CDF of Y is

$$
F_Y(y) = \left[1 - \frac{\gamma_{rd}^2}{(\gamma_{rd} + \gamma_{se} x)(\gamma_{rd} + \gamma_{re} x)}\right]^{N_2}. \qquad \text{(B.5)}
$$

According to the buffer-aided relay selection scheme in (4.3) and (4.4), a message relay is selected at each time slot with instantaneous channel gain ratio $\max\{X, Y\}$, and the state s_i remains unchanged as $C_s < \varepsilon$. Thus, the entry $a_{i,i}$ of the transition

matrix $\mathbf{A}$ can be given by

$$\begin{aligned} a_{i,i} &= \mathbb{P}\left(\log(\max\{X,Y\}) < \varepsilon\right) && \text{(B.6)} \\ &= \mathbb{P}(\max\{X,Y\} < 2^{\varepsilon}) && \text{(B.7)} \\ &= F_X(2^{\varepsilon}) \cdot F_Y(2^{\varepsilon}) && \text{(B.8)} \\ &= \mu_{\text{case1}}(s_i), && \text{(B.9)} \end{aligned}$$

where $\mu_{case1}(s_i)$ is given in (4.7) with $s = s_i$ and the last step follows after substituting (B.1) and (B.5) into (B.6). The probability that state s_i moves to state s_j ($s_j \in \mathcal{S}^-$) can be given as

$$\begin{aligned} p_{i,j} &= \mathbb{P}(X \leq Y, Y \geq 2^{\varepsilon}) \\ &= \int_0^{\infty} \mathbb{P}(x \leq Y, Y \geq 2^{\varepsilon}) f_X(x) dx \\ &= \int_0^{2^{\varepsilon}} \mathbb{P}(Y \geq 2^{\varepsilon}) f_X(x) dx + \int_{2^{\varepsilon}}^{\infty} \mathbb{P}(Y \geq x) f_X(x) dx \\ &= \mathbb{P}(Y \geq 2^{\varepsilon}) \mathbb{P}(X \leq 2^{\varepsilon}) + \int_{2^{\varepsilon}}^{\infty} f_X(x) dx - \int_{2^{\varepsilon}}^{\infty} F_Y(x) f_X(x) dx \\ &= 1 - F_X(2^{\varepsilon}) F_Y(2^{\varepsilon}) - \int_{2^{\varepsilon}}^{\infty} F_Y(x) f_X(x) dx \\ &= 1 - \nu_{case1}(s_i) - \mu_{case1}(s_i), && \text{(B.10)} \end{aligned}$$

where $\nu_{case1}(s)$ is given in (4.8) with $s = s_i$. Since the selection of a particular relay from all available relays is equally likely due to the i.i.d. property of main channels, for any state $s_j \in \mathcal{S}_i^-$, $a_{i,j} = \frac{1-\mu_{case1}(s_i)-\nu_{case1}(s_i)}{N_2(s_i)}$. Notice that a state s_i can only move to three types of states, the s_i itself, the states in $\mathcal{S}_i^-$ and states in $\mathcal{S}_i^+$. Hence, for any state $s_j \in \mathcal{S}_i^+$, $a_{i,j} = \frac{\nu_{case1}(s_i)}{N_1(s_i)}$.

Next, we provide proof for case 2. Let $X' = \arg \max_{R_n : \Psi_{s_i}(Q_n) \neq L} \frac{|h_{SR_n}|^2}{\gamma_{se}}$,

$Y' = \arg \max_{R_n : \Psi_{s_i}(Q_n) \neq 0} \frac{|h_{R_n D}|^2}{\gamma_{se}+\gamma_{re}}$ with the CDFs of X' and Y' given by

$$F_{X'}(x) = (1 - e^{-\frac{x}{\alpha}})^{N_1(s_i)}, \tag{B.11}$$

and

$$F_{Y'}(x) = (1 - e^{-\frac{(\gamma_{se}+\gamma_{re})x}{\gamma_{rd}}})^{N_2(s_i)}, \tag{B.12}$$

respectively. Following the proof for case 1, we can obtain $a_{i,j}$ for $s_i = s_j$, $s_j \in \mathcal{S}_i^+$ and $s_j \in \mathcal{S}_i^-$ as $\nu_{case2}(s_i)$, $\frac{\mu_{case2}(s_i)}{N_1(s_i)}$ and $\frac{1-\mu_{case2}(s_i)-\nu_{case2}(s_i)}{N_2(s_i)-1}$ and respectively, where

$$\mu_{\text{case2}}(s) = F_{X'}(2^{\varepsilon}) \cdot F_{Y'}(2^{\varepsilon}), \tag{B.13}$$

is given in (4.9) by substituting $F_{X'}(2^{\varepsilon})$ and $F_{Y'}(2^{\varepsilon})$ into (B.13) and

$$\nu_{\text{case2}}(s) = \int_{2^{\varepsilon}}^{\infty} F_{Y'}(x) f_{X'}(x) \mathrm{d}x, \tag{B.14}$$

is given in (4.10).

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," IEEE International Conference on Computer Science and Electronics Engineering (ICCSEE), vol. 1, pp. 647-651, 2012.

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

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

[4] T. Chan Dai Truyen, J. Lee, and T. QS Quek, "Physical-layer secret key generation with colluding untrusted relays," IEEE Trans. Wireless Commun., vol. 15, no. 2, pp. 1517-1530, 2016.

[5] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in Foundations of Computer Science, 1994 Proceedings, 35th Annual Symposium on, pp. 124-134, 1994.

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

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

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

[9] Z. Zheng, Z. Haas, and M. Kieburg, "Secrecy Rate of distributed cooperative MIMO in the presence of multi-antenna eavesdropper," arXiv preprint arXiv:1709.05383, 2017.

[10] K. Cumanan, Z. Ding, B. Sharif, et al., "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," IEEE Trans. Vehicular Technology, vol. 63, no. 4, pp. 1678-1690, 2014.

[11] C. Wang and H. M. Wang, "On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels," IEEE Trans. Inf. Forensics and Security, vol. 9, no. 11, pp. 1814-1827, 2014.

[12] Y. Liang, H. V. Poor, and L. Ying, "Secrecy throughput of MANETs with malicious nodes," IEEE International Symposium Inf. Theory (ISIT 2009), pp. 1189-1193, 2009.

[13] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," IEEE Trans. Inf. Forensics and Security, vol. 7, no. 2, pp. 704-716, 2012.

[14] B. V. Nguyen and K. Kim, "Secrecy outage probability of optimal relay selection for secure AnF cooperative networks," IEEE Commun. Letters, vol. 19, no. 12, pp. 2086-2089, 2015.

[15] N. Yang, L. Wang, G. Geraci, et al., "Safeguarding 5G wireless communication networks using physical layer security," IEEE Commun. Magazine, vol. 53, no. 4, pp. 20-27, 2015.

[16] A. D. Wyner, "The wire-tap channel," The bell system technical journal, vol. 54, no. 8, pp. 1355-1387, 1975.

[17] I. Csiszarr and J. Korner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339-348, 1978.

[18] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," IEEE Trans. Wireless Commun., vol. 10, no. 8, pp. 5003-5011, Oct. 2009.

[19] J. Huang and A. Lee Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," IEEE Trans. Signal Process., vol. 59, no. 10, pp. 4871-4884, 2011.

[20] R. A. Chou and A. Yener, "Polar coding for the multiple access wiretap channel via rate-splitting and cooperative jamming," IEEE International Symposium Inf. Theory (ISIT), 2016.

[21] F. Zhu, F. Gao, and M. Yao, "Zero-forcing beamforming for physical layer security of energy harvesting wireless communications," EURASIP Journal on Wireless Commun. and Networking, pp. 1-9, Mar. 2015.

[22] T. M. Hoang, T. Q. Duong, H. A. Suraweera, et al., "Cooperative beamforming and user selection for improving the security of relay-aided systems," IEEE Trans. Wireless Commun., vol 63, no. 12, pp. 5039-5051, Dec. 2015.

[23] N. D. Sidiropoulos, T. N. Davidson, and Z. Q. Luo, "Transmit beamforming for physical-layer multicasting," IEEE Trans. Signal Process., vol. 54, no. 6, pp. 2239-2251, 2006.

[24] H. Wen, P. H. Ho, and B. Wu, "Achieving secure communications over wiretap

channels via security codes from resilient functions," IEEE Wireless Commun. Letters , vol. 3, no. 3, pp. 273-276, 2014.

[25] D. Klinc, J. Ha, S. W. Mclaughlin, et al., "LDPC codes for the Gaussian wiretap channel," Inf. Theory Workshop, pp. 95-99, 2009.

[26] W. K. Harrison, J. Almeida, M. R. Bloch, et al., "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," IEEE Signal Process. Magazine, vol. 30, no. 5, pp. 41-50, 2013.

[27] H. Fang, L. Xu, and K. K. R. Choo, "Stackelberg game based relay selection for physical layer security and energy efficiency enhancement in cognitive radio networks," Applied Mathematics and Computation, vol. 296, pp. 153-167, 2017.

[28] N. Nomikos, A. Nieto, P. Makris, D. N. Skoutas, et al., "Relay selection for secure 5G green communications," Telecommunication Systems, vol. 59, no. 1, pp. 169-187, 2015.

[29] H. Hu, R. Lu, C. Huang, and Z. Zhang, "PTRS: a privacy-preserving trust-based relay selection scheme in VANETs," Peer-to-Peer Networking and Applications, pp. 1-15, 2016.

[30] J. Huang and A. Lee Swindlehurst, "Buffer-aided relaying for two-hop secure communication," IEEE Trans. Wireless Commun., vol. 14, no. 1, Jan. 2015.

[31] 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, 2016.

[32] A. El Shafie, D. Niyato, and N. Al-Dhahir, "Enhancing the PHY-layer security of MIMO buffer-aided relay networks," IEEE Wireless Commun. Letters, vol. 5, no. 4, pp. 400-403, 2016.

[33] 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, Apr. 2014.

[34] Y. Zhang, T. Liang, and A. Sun, "A new Max-ratio relay selection scheme in secure buffer-aided cooperative wireless networks," the 8th International Symposium on Computational Intelligence and Design (ISCID), vol. 1, 2015.

[35] 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 Tran. Vehicular Technology, 2017, [Online]. Available: Early Access. doi: 10.1109/TVT.2017.2695500.

[36] X. Tang, Y. Cai, Y. Huang, T. Q. Duong, W. Yang, and W. Yang, "Secrecy outage analysis of buffer-aided multi-antenna relay systems without eavesdropper's CSI," 2017 IEEE International Conference on Communications (ICC), pp. 1-6, 2017.

[37] X. Luo and Rodrigo C. de Lamare, "Study of relay selection for physical-layer security in buffer-aided relay networks based on the secrecy rate criterion," arXiv preprint arXiv:1605.04487, 2016.

[38] X. Liao, Z. Wu, Y. Zhang, and X. Jiang, "The delay-security trade-off in two-hop buffer-aided relay wireless network," International Conference on Networking and Network Applications, pp. 173-177, 2016.

[39] X. Liao, Y. Zhang, Z. Wu, et al., "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, 2018.

[40] J. He, J. Liu, Y. Shen, et al., "Link selection for secure cooperative networks with buffer-aided relaying," arXiv preprint arXiv:1802.06538, 2018.

[41] S. Luo and K. C. Teh, "Buffer state based relay selection for buffer-aided cooperative relaying systems," IEEE Trans. Wireless Commun., vol. 14, no. 10, pp. 5430-5439, 2015.

[42] T. Islam, A. Ikhlef, R. Schober, et al., "Diversity and delay analysis of buffer-aided BICM-OFDM relaying," IEEE Trans. Wireless Commun., vol. 12, no. 11, pp. 5506-5519, 2013.

[43] V. Jamali, N. Zlatanov, and R. Schober, "Bidirectional buffer-aided relay networks with fixed rate transmission-Part I: Delay-unconstrained case," IEEE Trans. Wireless Commun., vol. 14, no. 3, pp. 1323-1338, 2015.

[44] F. Wang, J. Huang, and Y. Zhao, "Delay sensitive communications over cognitive radio networks," IEEE Trans. Wireless Commun., vol. 11, no. 4, pp. 1402-1411, 2012.

[45] S. S. Ikki and M. H. Ahmed, "Performance analysis of adaptive decode-and-forward cooperative diversity networks with best-relay selection," IEEE Trans. Commun., vol. 58, no. 1, 2010.

[46] R. Senanayake, S. Atapattu, J. Evans, et al., "Decentralized relay selection in multi-user multihop decode-and-forward relay networks," IEEE Trans. Wireless Commun., 2018.

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

[48] O. O. Koyluoglu, C. E. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," IEEE Trans. Inf. Theory, vol. 58, no. 5, pp. 3000-3015, 2012.

[49] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," IEEE Trans. Info. Theory, vol. 54, no. 10, pp. 4687-4698, 2008.

[50] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," IEEE Trans. Vehicular Technology, vol. 62, no. 5, pp. 2170-2181, 2013.

[51] N. Yang, S. Yan, J. Yuan, et al., "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," IEEE Trans. Commun., vol. 63, no. 5, pp. 1771-1783, 2015.

[52] C. Wang and H. M. Wang, "On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels," IEEE Trans. Inf. Forensics and Security, vol. 9, no. 11, pp. 1814-1827, 2014.

[53] C. Cai, Y. Cai, X. Zhou, et al., "When does relay transmission give a more secure connection in wireless ad hoc networks," IEEE Trans. Inf. Forensics and Security, vol. 9, no. 4, pp. 624-632, 2014.

[54] 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, 2012.

[55] J. R. Norris, *Markov Chains*, Cambridge, U.K.: Cambridge Univ. Press, 1998.

[56] T. Robertazzi, "Computer Networks and Systems: Queueing Theory and Performance Evaluation," Springer, 2012.

[57] C++ simulator for E2E delay and STP performance in two-hop wireless networks, 2017, [Online]. Available: http://xnliao.blogspot.com/.

[58] N. C. Beaulieu and J. Hu, "A closed-form expression for the outage probability of decode-and-forward relaying in dissimilar Rayleigh fading channels," IEEE Commun. Letters, vol. 10, no. 12.

[59] Z. Yi and I. M. Kim, "Diversity order analysis of the decode-and-forward cooperative networks with relay selection," IEEE Trans. Wireless Commun., vol. 7, no. 5, 2008.

[60] J. He, V. Tervo, S. Qian, et al., "Performance analysis of lossy decode-and-forward for non-orthogonal MARCs," IEEE Trans. Wireless Commun., vol. 17, no. 3, pp. 1545-1558, 2018.

[61] H. Chen, C. Zhai, Y. Li, et al., "Cooperative strategies for wireless-powered communications: An overview," IEEE Wireless Commun., 2018.

[62] K. S. Gomadam and S. A. Jafar, "Optimal relay functionality for SNR maximization in memoryless relay networks," IEEE Journal on Selected Areas in Commun., vol. 25, no. 2, 2007.

[63] A. Ikhlef, D. S. Michalopoulos, and R. Schober, "Max-max relay selection for relays with buffers," IEEE Trans. Wireless Commun., vol. 11, no. 3, pp. 1124-1135, 2012.

[64] R. Bassily, E. Ekrem, X. He, et al., "Cooperative security at the physical layer: A summary of recent advances," IEEE Signal Process. Magazine, vol. 30, no. 5, pp. 16-28, 2013.

PUBLICATIONS

Publications

Jounal Articles

[1] Xuening Liao, Yuanyu Zhang, Zhenqiang Wu, Yulong Shen, Xiaohong Jiang and Hiroshi Inamura, On Security-Delay Trade-Off in Two-Hop Wireless Networks with Buffer-Aaided Relay Selection, *IEEE Transactions on Wireless Communications* 17(3): 1893-1906, 2018.

[2] Xuening Liao, Yuanyu Zhang, Zhenqiang Wu, Xiaohong Jiang and Horoshi Inamura, Buffer-Aided Relay Selection Scheme for Secure Two-Hop Wireless Networks with Decode-and-Forward Relays, *Ad Hoc Networks*, 2018. (Submitted)

[3] Ahamed Salem, Xuening Liao, Yulong Shen and Xiaohong Jiang, Provoking the Adversary by Detecting Eavesdropping and Jamming Attacks: A Game Theoretical Framework, *Special Issue on Wireless Communications and Mobile Computing*, 2018. (Accepted)

[4] Huihui Wu, Yuanyu Zhang, Xuening Liao, Yulong Shen and Xiaohong Jiang, Covert Wireless Communication in Two-Way Relay Channel, *Ad Hoc Networks*, 2018. (Submitted)

Conference Papers

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

[6] Huihui Wu, Xuening Liao, Yulong Shen and Xiaohong Jiang, Limits of Covert Communication on Two-Hop AWGN Channels, 2017 International Conference on Networking and Network Applications (NaNA 2017), Nepal, 2017, pp. 42-47.

[7] Ahamed Salem, Xuening Liao and Yulong Shen, Provoking the Adversary by Dual Detection Techniques: A Game Theoretical Framework, 2017 International

Conference on Networking and Network Applications (NaNA 2017), Nepal, 2017, pp. 326-329.

[8] Sasaki Kenda, Xuening Liao and Xiaohong Jiang, Cooperative jamming in a Two-Hop Relay Wireless Network with Buffer-Aided Relays, The Fifth International Symposium on Computing and Networking (CANDAR 2017), Aomori, 2017.