On Security-Delay Trade-Off in Two-Hop Wireless Networks With Buffer-Aided Relay Selection

Xuening Liao, Yuanyu Zhang, Zhenqiang Wu, Yulong Shen, *Member, IEEE*, Xiaohong Jiang, *Senior Member, IEEE*, and Hiroshi Inamura, *Member, IEEE*

***Abstract*— This paper investigates 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 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 paper 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.**

***Index Terms*— Buffer-aided relay selection, physical layer security, delay, trade-off.**

I. Introduction

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 [1]. 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 [2].

Traditionally, security issues are addressed by cryptographic methods which utilize secret keys and encryption/decryption algorithms to provide secure data streams 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 challenging 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 attention [6]. As PHY security has the potential to achieve the information-theoretic security, it has been recognized as an important approach for providing a strong form of security guarantee for wireless networks [7]. In particular, the PHY security is promising to serve as a complementary approach for the conventional cryptography to achieve an enhanced security performance.

Since the seminal work of Wyner on PHY security [8], extensive research efforts have been devoted to the design of effective PHY security schemes, such as artificial noise injection/cooperative jamming [9]–[11], beam-forming [12], [13], coding [14], [15] and relay selection with or without the help of relay buffers [16]–[26]. This paper focuses on the relay selection with the help of buffers (i.e., buffer-aided relay selection). In the conventional relay selection without the help of buffers, the selected relay, which received packets from a source during previous time slot, must send out the packets to a destination in the current time slot, even if the link quality is poor for secure transmission [16]–[18]. In the buffer-aided relay selection, however, a packet can be temporarily stored in the relay buffer when its desired link in current time slot is not secure enough for transmission [19]–[26]. Thus, the buffer-aided relay selection can greatly improve the security performance of wireless communications.

By now, many works have been devoted to the study on the PHY security performances of wireless networks with buffer-aided relay selection [19]–[26]. 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

Manuscript received March 10, 2017; revised July 21, 2017 and November 5, 2017; accepted December 18, 2017. Date of publication December 29, 2017; date of current version March 8, 2018. This work was supported in part by the Japan JSPS under Grant 15H02692, in part by the China NSFC Grant 61571352, Grant 61373173, Grant 61672334, Grant 61602290, and Grant U1536202, and in part by China FRSCU Grant GK201501008. The associate editor coordinating the review of this paper and approving it for publication was T. Q. Duong. *(Corresponding author: Zhenqiang Wu.)*

X. Liao is with the School of Systems Information Science, Future University Hakodate, Hokkaido 041-8655, Japan, and also with School of Computer Science, Shaanxi Normal University, Xi'an 710119, China (e-mail: liaoxuening@sina.cn).

Y. Zhang is with the Graduate School of Information Science, Nara Institute of Science and Technology, Nara 630-0192, Japan (e-mail: yyzhang@is.naist.jp).

Z. Wu is with School of Computer Science, Shaanxi Normal University, Xi'an 710119, China (e-mail: zqiangwu@snnu.edu.cn).

Y. Shen is with the School of Computer Science, Xidian University, Xi'an 710071, China (e-mail: ylshen@mail.xidian.edu.cn).

X. Jiang and H. Inamura are with the School of Systems Information Science, Future University Hakodate, Hokkaido 041-8655, Japan (e-mail: jiang@fun.ac.jp; inamura@fun.ac.jp).

Digital Object Identifier 10.1109/TWC.2017.2786258

selection of a link among the links of source-relay, relay-destination and source-destination to meet a given security criteria [19]–[21]. For the relay system with a half-duplex (HD) relay where no direct source-destination link is available, the authors in [19] proposed two link selection policies with the considerations 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 [20], 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 [20] for the maximization of secrecy network throughput. For the relay system with direct source-destination link, the authors in [21] 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 [21] under certain SOP constraint.

Regarding the two-hop relay systems with multiple relays, the authors in [22] 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 [23], 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 [24] and [25] 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 [26] 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 [22] 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 end-to-end (E2E) PHY security performances [22]–[26].

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 [27]–[29]. 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 [30].

This paper extends our previous study in [31] and investigates the critical security-delay trade-off issue of two-hop relay systems, in particular, the inherent trade-off between the E2E security and delay performances in such systems. The main contributions of this paper are 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.

The remainder of this paper is organized as follows. Section II introduces the system model, transmission scheme, the buffer-aided relay selection schemes and performance metrics. Section III provides the general framework for characterizing the E2E packet delivery process. The E2E STP and delay performances are analyzed in Section IV, and the numerical results are provided in Section V. Finally, Section VI concludes this paper.

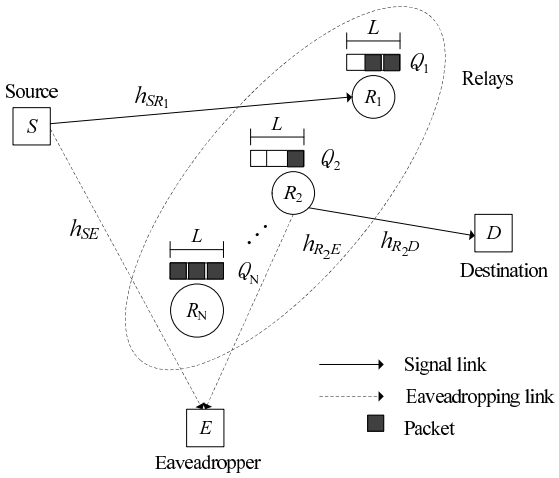


Fig. 1. Illustration of system model.

II. System Model and Definitions

A. System Model

As illustrated in Fig. 1, we consider a two-hop wireless system consisting of one source S, one destination D, N relays $R_1, R_2, \ldots, R_N$ adopting the Randomize-and-Forward (RF) decoding strategy, and one eavesdropper E wiretapping on both the source-relay and relay-destination links. Same as [32], [33], the RF strategy concerned in this paper 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 half-duplex (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. 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-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 $i \in \{S, R_1, R_2, \ldots, R_N\}$ and $j \in \{R_1, R_2, \ldots, R_N, E, D\}$. 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, $\mathbb{E}[\cdot]$ 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 paper, 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.

B. Transmission and Buffer-Aided Relay Selection Schemes

In this paper, 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 $S \rightarrow D$ transmission. This paper 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 [22]. 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 paper. Before introducing the relay selection scheme, we first introduce the selection criterion. Considering an individual link $A \rightarrow B$, 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 $A \rightarrow B$ is given by [34]

$$C_s^{AB} = \max\{C_m^{AB} - C_e^{AE}, 0\}, \tag{1}$$

where

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

and

$$C_e^{AE} = \log\left(1 + \frac{P|h_{AE}|^2}{\sigma^2}\right), \tag{3}$$

denote the capacities of main channel $A \rightarrow B$ and eavesdropper channel $A \rightarrow E$, 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 [8], 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 $A \rightarrow B$ 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 $\mathbf{R}_s^{AB} = C_m^{AB} - \log\left(1 + \frac{P\gamma_{AE}}{\sigma^2}\right)$ [35]. Notice that although the conventional approach is to choose a

fixed $\mathbf{R}_s^{AB}$ in this case [19]–[21], 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 [35]. 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 [35]–[37]. In this paper, we consider the high SNR regime, so C_m^{AB} and $\mathbf{R}_s^{AB}$ in the perfect eavesdropper CSI case are approximated by $C_s^{AB} = \mathbf{R}_s^{AB} \approx \log\left(\frac{|h_{AB}|^2}{|h_{AE}|^2}\right)$ [35], 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 $\mathbf{R}_s^{AB} > \varepsilon$.

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

$$R_{\mathrm{PF}} = \arg\max_{R_n} \max \left\{ \frac{|h_{SR_n}|^2 \cdot \mathbf{1}_{\Psi(Q_n)\neq L}}{|h_{SE}|^2}, \frac{|h_{R_nD}|^2 \cdot \mathbf{1}_{\Psi(Q_n)\neq 0}}{|h_{R_nE}|^2} \right\}, \tag{4}$$

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

$$R_{\mathrm{PT}} = \arg\max_{R_n} \max \left\{ \frac{|h_{SR_n}|^2 \cdot \mathbf{1}_{\Psi(Q_n)\neq L}}{\gamma_{se}}, \frac{|h_{R_nD}|^2 \cdot \mathbf{1}_{\Psi(Q_n)\neq 0}}{\gamma_{re}} \right\}. \tag{5}$$

In equations (4) and (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 (4) and (5), we can see that the relay selection in each time slot is only based on the instantaneous secrecy capacity of each link and the states of all relay buffers. 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 [33]

$$C_s = \left[min \log_2 \left(\frac{1 + P|h_{SR_n}|^2}{1 + P|h_{SE}|^2}, \frac{1 + P|h_{R_nD}|^2}{1 + P|h_{R_nE}|^2} \right) \right]^+. \tag{6}$$

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 paper, 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 (1) is enough for us to derive the main results in this paper (see Section IV-A and Section IV-B for details). It is also worth noting that the buffer-aided relaying scheme in this paper 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 paper, 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.

C. Performance Metrics

This paper 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

$$T = T_s + T_r + T_q. \tag{7}$$

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 [20], [22], [23]. 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 [38], 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 $S \rightarrow R_*$ nor $R_* \rightarrow D$ delivery suffers from secrecy outage. Based on the formulation of the secure connection probability in [38], we formulate the E2E STP as

$$p_{st} = \mathbb{P}(C_s^{SR_*} \geq \varepsilon, C_s^{R_*D} \geq \varepsilon), \tag{8}$$

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

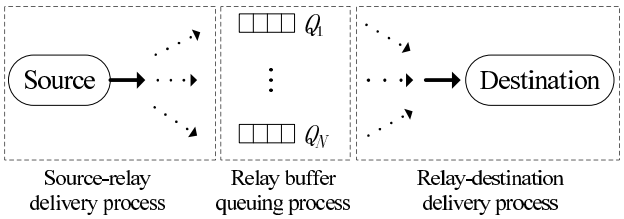


Fig. 2. End-to-end delivery process of a packet.

III. 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 Fig. 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.

A. 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

$$s_i = [\Psi_{s_i}(Q_1), \cdots, \Psi_{s_i}(Q_n), \cdots, \Psi_{s_i}(Q_N)]^T \quad n \in \{1, 2, \cdots, N\}, \tag{13}$$

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 II-B, 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 II-B, 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

$$a_{i,j} = \begin{cases} \mu_\Delta(s_i), & \text{if } s_j = s_i, \\ \frac{\nu_\Delta(s_i)}{N_1(s_i)}, & \text{if } s_j \in \mathcal{S}_i^+, \\ \frac{1-\mu_\Delta(s_i)-\nu_\Delta(s_i)}{N_2(s_i)}, & \text{if } s_j \in \mathcal{S}_i^-, \\ 0, & \text{elsewhere.} \end{cases} \tag{14}$$

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 (9) and (10), as shown at the bottom of this page, for the perfect CSI case and in (11) and (12), as shown at the bottom of this page, for the partial CSI case with the parameter $s = s_i$.

Proof: See Appendix for the proof. □

$$\mu_{\text{PF}}(s) = \sum_{n_1=0}^{N_1(s)} \binom{N_1(s)}{n_1} (-1)^{n_1} \frac{\alpha}{2^\varepsilon n_1 + \alpha} \left(\frac{2^\varepsilon}{\beta + 2^\varepsilon}\right)^{N_2(s)}, \tag{9}$$

$$\nu_{\text{PF}}(s) = \sum_{n_1=0}^{N_1(s)} \binom{N_1(s)}{n_1} (-1)^{n_1} \left[\frac{n_1 \cdot {}_2F_1\left(N_2(s), N_2(s)+1; N_2(s)+2; \frac{n_1\beta-\alpha}{\beta(\alpha+2^\varepsilon n_1)}\right)}{(N_2(s)+1)(\alpha + 2^\varepsilon n_1)} \left(\frac{4^\varepsilon \alpha}{2^\varepsilon n_1 \beta + \alpha\beta)}\right)^{N_2(s)} \right.$$
$$\left. - \frac{{}_2F_1\left(N_2(s), N_2(s)+1; N_2(s)+2; 1-\frac{\alpha}{n_1\beta}\right)}{N_2(s)+1} \left(\frac{\alpha}{n_1\beta}\right)^{N_2(s)} \right], \tag{10}$$

$$\mu_{\text{PT}}(s) = \left[1 - e^{-2^\varepsilon/\alpha}\right]^{N_1(s)} \left[1 - e^{-2^\varepsilon/\beta}\right]^{N_2(s)}, \tag{11}$$

$$\nu_{\text{PT}}(s) = \sum_{n_2=0}^{N_2(s)} \sum_{n_1=0}^{N_1(s)-1} \binom{N_2(s)}{n_2} \binom{N_1(s)-1}{n_1} (-1)^{n_2+n_1} \frac{N_1(s)\beta e^{-\frac{(\alpha n_2+\beta+\beta n_1)2^\varepsilon}{\alpha\beta}}}{\alpha n_2 + \beta + \beta n_1}. \tag{12}$$

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 [39]. 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 [39]. According to [40, Ch. 11, Definition 1 and Th. 2], 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 $\boldsymbol{\pi} = [\pi_{s_1}^{\Delta}, \cdots, \pi_{s_i}^{\Delta}, \cdots, \pi_{s_{(L+1)^N}}^{\Delta}]^T$ such that $A\boldsymbol{\pi} = \boldsymbol{\pi}$ and $\sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\Delta} = 1$, where $\pi_{s_i}^{\Delta}$ denotes the stationary probability of state s_i.

According to [39, Lemma 2], the analytical expression of $\pi_{s_i}^{\Delta}$ can be given by

$$\pi_{s_i}^{\Delta} = \left(\sum_{j=1}^{(L+1)^N} \frac{\prod_{s_{i'} \in \Xi(s_i, \Theta_{s_j})} a_{i,i'}}{\prod_{s_{j'} \in \Xi(s_j, \Theta_{s_i})} a_{j,j'}} \right)^{-1}, \tag{15}$$

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}).

B. 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

$$\widetilde{s}_k = [\Psi_{\widetilde{s}_k}(Q_1), \cdots, \Psi_{\widetilde{s}_k}(Q_*), \cdots, \Psi_{\widetilde{s}_k}(Q_n), \cdots, \Psi_{\widetilde{s}_k}(Q_N)]^T \quad n \in \{1, \cdots, N\}, n \neq *, \tag{16}$$

where $\Psi_{\widetilde{s}_k}(Q_n)$ and $\Psi_{\widetilde{s}_j}(Q_*)$ 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 $R_* \rightarrow D$ 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

$$\widetilde{a}_{k,l} = \begin{cases} \mu_{\Delta}(\widetilde{s}_k), & \text{if } \widetilde{s}_l = \widetilde{s}_k, \\ \frac{\nu_{\Delta}(\widetilde{s}_k)}{N_1(\widetilde{s}_k)}, & \text{if } \widetilde{s}_l \in \widetilde{\mathcal{S}}_k^+, \\ \frac{1-\mu_{\Delta}(\widetilde{s}_k)-\nu_{\Delta}(\widetilde{s}_k)}{N_2(\widetilde{s}_k)-1}, & \text{if } \widetilde{s}_l \in \widetilde{\mathcal{S}}_k^-, \\ 0, & \text{elsewhere.} \end{cases} \tag{17}$$

where $\Delta \in \{\text{PF} = \textit{perfect}, \text{PT} = \textit{partial}\}$ denotes the eavesdropper CSI case, $\mu_{\Delta}(\widetilde{s}_k)$ and $\nu_{\Delta}(\widetilde{s}_k)$ are given in (9) and (10) for the perfect CSI case and in (11) and (12) for the partial CSI case.

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

Similarly, according to [40], we can see from Lemma 2 that our Markov chain that models the buffer states of the relay-destination transmission process is also stationary. We use $\widetilde{\boldsymbol{\pi}} = [\widetilde{\pi}_{\widetilde{s}_1}^{\Delta}, \cdots, \widetilde{\pi}_{\widetilde{s}_k}^{\Delta}, \cdots, \widetilde{\pi}_{\widetilde{s}_{L(L+1)^{N-1}}}^{\Delta}]^T$ to denote the corresponding stationary probability distribution when the tagged packet is at the head of R_*'s queue, where $\widetilde{\pi}_{\widetilde{s}_k}^{\Delta}$ denotes the stationary probability of state $\widetilde{s}_k$. Based on the state transition matrix $\widetilde{\mathbf{A}}$ and in [39, Lemma 2], we can determine the analytical expression of the stationary probability of state $\widetilde{s}_k$ in $\widetilde{\boldsymbol{\pi}}$ as

$$\widetilde{\pi}_{\widetilde{s}_k}^{\Delta} = \left(\sum_{l=1}^{(L+1)^N} \frac{\prod_{\widetilde{s}_{k'} \in \Xi(\widetilde{s}_k, \Theta_{\widetilde{s}_l})} \widetilde{a}_{k,k'}}{\prod_{\widetilde{s}_{l'} \in \Xi(\widetilde{s}_l, \Theta_{\widetilde{s}_k})} \widetilde{a}_{l,l'}} \right)^{-1}, \tag{18}$$

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 $\Theta_{\widetilde{s}_l}$ ($\Theta_{\widetilde{s}_k}$).

IV. E2E STP and Delay Analysis

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

A. E2E STP Analysis

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

$$\phi(s) = \sum_{n_1=0}^{N_1(s)} \sum_{n_2=0}^{N_2(s)} \binom{N_1(s)}{n_1} \binom{N_2(s)}{n_2} (-1)^{n_1+n_2} \frac{\alpha\beta}{2^{\varepsilon}(n_1\beta + n_2\alpha) + \alpha\beta}, \tag{19}$$

$$\omega(s) = \sum_{n_1=0}^{N_1(s)} \sum_{n_2=0}^{N_2(s)-1} \frac{\binom{N_1(s)}{n_1} \binom{N_2(s)-1}{n_2} (-1)^{n_1+n_2} N_2(s) \alpha^2 \beta}{2^{\varepsilon}(n_1\beta + \alpha + n_2\alpha)^2 + \alpha\beta(n_1\beta + \alpha + n_2\alpha)}. \tag{20}$$

Theorem 1: Consider the two-hop relay wireless system as illustrated in Fig. 1. Under the transmission scheme and the Max-ratio buffer-aided relay selection scheme in Section II-B, the E2E STP for the perfect eavesdropper CSI case can be determined as

$$p_{st}^{\mathrm{PF}} = \sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\mathrm{PF}} \nu_{\mathrm{PF}}(s_i) \sum_{k=1}^{L(L+1)^{N-1}} \pi_{\widetilde{s}_k}^{\mathrm{PF}} \frac{1-\mu_{\mathrm{PF}}(\widetilde{s}_k)-\nu_{\mathrm{PF}}(\widetilde{s}_k)}{N_2(\widetilde{s}_k)}, \tag{21}$$

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 (15) and (18) with $\Delta = \mathrm{PF}$, $\mu_{\mathrm{PF}}(\widetilde{s}_k)$ is given by (9) with $s = \widetilde{s}_k$, $\nu_{\mathrm{PF}}(s_i)$ and $\nu_{\mathrm{PF}}(\widetilde{s}_k)$ are given by (10) with $s = s_i$ and $s = \widetilde{s}_k$ respectively. The E2E STP for the partial eavesdropper CSI case is given by

$$p_{st}^{\mathrm{PT}} = \sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\mathrm{PT}} \cdot (1-\phi(s_i)-\omega(s_i)) \sum_{k=1}^{L(L+1)^{N-1}} \pi_{\widetilde{s}_k}^{\mathrm{PT}} \frac{\omega(\widetilde{s}_k)}{N_2(\widetilde{s}_k)}, \tag{22}$$

where $\pi_{s_i}^{\mathrm{PT}}$ and $\pi_{\widetilde{s}_k}^{\mathrm{PT}}$ are given by (15) and (18) with $\Delta = \mathrm{PT}$, $\phi(s_i)$ is given by (19), as shown at the bottom of the previous page, with $s = s_i$, $\omega(s_i)$ and $\omega(\widetilde{s}_k)$ are given by (20), as shown at the bottom of the previous page, with $s = s_i$ and $s = \widetilde{s}_k$ respectively.

Proof: According to the formulation of E2E STP in (8), we have

$$p_{st}^{\Delta} = \mathbb{P}\left(C_s^{SR_*} \geq \varepsilon, C_s^{R_*D} \geq \varepsilon\right). \tag{23}$$

Applying the law of total probability yields

$$p_{st}^{\Delta} = \sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\Delta} \cdot \mathbb{P}\left(C_s^{SR_*} \geq \varepsilon, C_s^{R_*D} \geq \varepsilon | s_i\right). \tag{24}$$

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

$$p_{st}^{\Delta} = \sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\Delta} \cdot \sum_{n \in \mathcal{N}_{\mathrm{l}}} \mathbb{P}\left(C_s^{SR_*} \geq \varepsilon, C_s^{R_*D} \geq \varepsilon, R_* = R_n | s_i\right). \tag{25}$$

After changing the above probability into conditional probability, we have

$$\begin{aligned} p_{st}^{\Delta} &= \sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\Delta} \cdot \sum_{k \in \mathcal{N}_{\mathrm{l}}} \mathbb{P}\left(C_s^{SR_*} \geq \varepsilon, R_* = R_n | s_i\right) \\ &\quad \mathbb{P}\left(C_s^{R_*D} \geq \varepsilon | C_s^{SR_n} \geq \varepsilon, R_* = R_n, s_i\right) \qquad (26) \\ &= \sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\Delta} \cdot \sum_{n \in \mathcal{N}_{\mathrm{l}}} \mathbb{P}\left(C_s^{SR_n} \geq \varepsilon | s_i\right) \mathbb{P}\left(C_s^{R_nD} \geq \varepsilon\right), \qquad (27) \end{aligned}$$

where (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 $S \rightarrow R_n$ is selected and the transmission is secure at state s_i when the tagged packet is at S, and $\mathbb{P}\left(C_s^{R_nD} \geq \varepsilon\right)$ represents the probability that the link $R_n \rightarrow D$ 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

$$\mathbb{P}\left(C_s^{SR_n} \geq \varepsilon | s_i\right) = \frac{\nu_{\mathrm{PF}}(s_i)}{N_1(s_i)}, \tag{28}$$

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

$$\mathbb{P}\left(C_s^{R_nD} \geq \varepsilon\right) = \sum_{k=1}^{L(L+1)^{N-1}} \pi_{\widetilde{s}_k}^{\mathrm{PF}} \cdot \mathbb{P}\left(C_s^{R_nD} \geq \varepsilon | \widetilde{s}_k\right). \tag{29}$$

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

$$\begin{aligned} \mathbb{P}\left(C_s^{R_nD} \geq \varepsilon | \widetilde{s}_k\right) &= \mathbb{P}\left(\mathbf{R}_s^{R_nD} \geq \varepsilon | \widetilde{s}_k\right) \qquad (30) \\ &= \frac{1-\mu_{\mathrm{PF}}(\widetilde{s}_k)-\nu_{\mathrm{PF}}(\widetilde{s}_k)}{N_2(\widetilde{s}_k)}, \qquad (31) \end{aligned}$$

where (31) follows from the proof of Lemma 2. Finally, the E2E STP for the perfect eavesdropper CSI case follows after substituting (31) into (29), and then substituting (29) and (28) into (27).

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

$$\begin{aligned} &\frac{1}{N_1(s_i)} \mathbb{P}\left(\frac{\max\{X', Y'\}}{U} \geq 2^{\varepsilon}, X' > Y'\right) \qquad (32) \\ &= \frac{1}{N_1(s_i)} \Bigg(1 - \mathbb{E}[F_{X'}(2^{\varepsilon}U) F_{Y'}(2^{\varepsilon}U)] \\ &\quad - \mathbb{E}_U\left[\int_{2^{\varepsilon}U}^{\infty} \mathbb{P}(X' < y) f_{Y'}(y) \mathrm{d}y\right]\Bigg), \qquad (33) \end{aligned}$$

where the first expectation in (33) is equivalent to

$$\mathbb{P}\left(\frac{\max\{X', Y'\}}{U} < 2^{\varepsilon}\right), \tag{34}$$

which can be given by the $\phi(s_i)$ in (19) with $s = s_i$, and the second expectation in (33) is equivalent to

$$\mathbb{P}\left(\frac{\max\{X', Y'\}}{U} \geq 2^{\varepsilon}, X' < Y'\right), \tag{35}$$

which can be given by the $\omega(s_i)$ in (20) with $s = s_i$. Thus, we have

$$\mathbb{P}\left(C_s^{SR_n} \geq \varepsilon | s_i\right) = \frac{1-\phi(s_i)-\omega(s_i)}{N_1(s_i)}, \tag{36}$$

and

$$\mathbb{P}\left(C_s^{R_n D} \geq \varepsilon | s_i\right) = \frac{\mathbb{P}\left(\frac{\max\{X', Y'\}}{U} \geq 2^{\varepsilon}, X' < Y'\right)}{N_2(s_i)} = \frac{\omega(s_i)}{N_2(s_i)}. \quad (37)$$

Following the same idea, we have

$$\mathbb{P}\left(C_s^{R_n D} \geq \varepsilon | \widetilde{s}_k\right) = \frac{\omega(\widetilde{s}_k)}{N_2(\widetilde{s}_k)}, \quad (38)$$

and thus

$$\mathbb{P}\left(C_s^{R_n D} \geq \varepsilon\right) = \sum_{k=1}^{L(L+1)^{N-1}} \pi_{\widetilde{s}_k}^{\mathrm{PT}} \frac{\omega(\widetilde{s}_k)}{N_2(\widetilde{s}_k)}. \quad (39)$$

Finally, substituting (36) and (39) into (27) yields the E2E STP for the partial eavesdropper CSI case. □

B. 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

$$T_s^{\Delta} = \frac{1}{\sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\Delta} \nu_{\Delta}(s_i)}, \quad (40)$$

where $\pi_{s_i}^{\Delta}$ is given by (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

$$T_r^{\Delta} = \frac{1}{\sum_{k=1}^{L(L+1)^{N-1}} \pi_{\widetilde{s}_k}^{\Delta} \frac{(1-\mu_{\Delta}(\widetilde{s}_k)-\nu_{\Delta}(\widetilde{s}_k))}{N_2(\widetilde{s}_k)}}, \quad (41)$$

where $\pi_{\widetilde{s}_k}^{\Delta}$ is given by (18), $\mu_{\Delta}(\widetilde{s}_k)$ and $\nu_{\Delta}(\widetilde{s}_k))$ are given in Lemma 2.

Proof: According to the transmission scheme in Section II-B and the state transition matrix in Section III, 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

$$\sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\Delta} \nu_{\Delta}(s_i), \quad (42)$$

and the average service rate at relay R_* is

$$\sum_{k=1}^{L(L+1)^{N-1}} \pi_{\widetilde{s}_k}^{\Delta} \frac{(1-\mu_{\Delta}(\widetilde{s}_k)-\nu_{\Delta}(\widetilde{s}_k))}{N_2(\widetilde{s}_k)}. \quad (43)$$

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

$$T_q^{\Delta} = \frac{\sum_{i=1}^{(L+1)^N} \sum_{n=1}^{N} \pi_{s_i}^{\Delta} \Psi_{s_i}(Q_n)}{N \sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\Delta} \nu_{\Delta}(s_i)}, \quad (44)$$

where $\pi_{s_i}^{\Delta}$ is given by (15), $\nu_{\Delta}(s_i)$ is given in Lemma 1.

Proof: Based on the general framework in Section III, we model the queues of all relays as a single Bernoulli queue. According to Little's Law [41], the expected queuing delay for this queue is

$$T_q^{\Delta,total} = \frac{\mathbb{E}\left[\sum_{n=1}^{N} \Psi(Q_n)\right]}{r_{\mathrm{arr}}}, \quad (45)$$

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

$$\mathbb{E}\left[\sum_{k=1}^{N} \Psi(Q_n)\right] = \sum_{i=1}^{(L+1)^N} \sum_{n=1}^{N} \pi_{s_i}^{\Delta} \Psi_{s_i}(Q_n). \quad (46)$$

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

$$\sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\Delta} \nu_{\Delta}(s_i). \quad (47)$$

Thus, the total average queuing delay of all relays is

$$T_q^{\Delta,total} = \frac{\sum_{i=1}^{(L+1)^N} \sum_{n=1}^{N} \pi_{s_i}^{\Delta} \Psi_{s_i}(Q_n)}{\sum_{i=1}^{(L+1)^N} \pi_{s_i}^{\Delta} \nu_{\Delta}(s_i)}. \quad (48)$$

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

$$T_q^{\Delta} = \frac{T_q^{\Delta,total}}{N}, \quad (49)$$

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 2: Consider the two-hop relay wireless system as illustrated in Fig. 1. Under the transmission scheme and the Max-ratio buffer-aided relay selection scheme in Section II-B, the E2E delay of the system for both eavesdropper CSI cases

can be determined as

$$T_\Delta = \frac{1+\frac{1}{N}\sum_{i=1}^{(L+1)^N}\sum_{n=1}^{N}\pi_{s_i}^{\Delta}\Psi_{s_i}(Q_n)}{\sum_{i=1}^{(L+1)^N}\pi_{s_i}^{\Delta}\nu_\Delta(s_i)} + \frac{1}{\sum_{k=1}^{L(L+1)^{N-1}}\pi_{\widetilde{s}_k}^{\Delta}\frac{(1-\mu_\Delta(\widetilde{s}_k)-\nu_\Delta(\widetilde{s}_k))}{N_2(\widetilde{s}_k)}}, \quad (50)$$

where $\Delta \in \{\mathrm{PF}, \mathrm{PT}\}$, $\pi_{s_i}^{\Delta}$ *is given by (15),* $\nu_\Delta(s_i)$ *is given in Lemma 1,* $\pi_{\widetilde{s}_k}^{\Delta}$ *is given by (18),* $\mu_\Delta(\widetilde{s}_k)$ *and* $\nu_\Delta(\widetilde{s}_k)$*) are given in Lemma 2.*

Proof: The E2E delay T_Δ directly follows after combining the mean service time in Lemma 3 and the expected queuing delay in Lemma 4. □

V. 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.

A. Simulation Settings

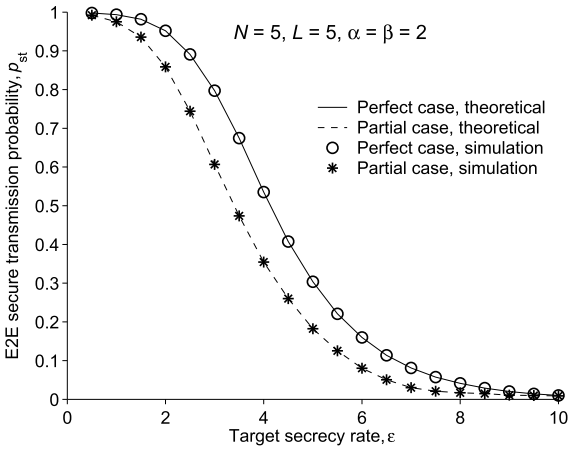
To validate our theoretical results for the E2E STP and expected E2E delay, a dedicated C++ simulator was developed to simulate the E2E packet delivery process based on the Max-ratio buffer aided relay selection schemes in (4) and (5), which is now available at [42]. With the help of the simulator, we 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.,

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

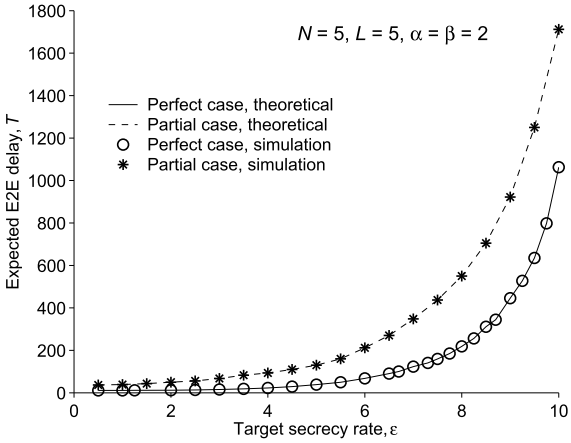
The expected E2E delay is calculated as the ratio of the total E2E delay (measured in time slots) of all packets transmitted to D to the number of these packets, i.e.,

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

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.



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



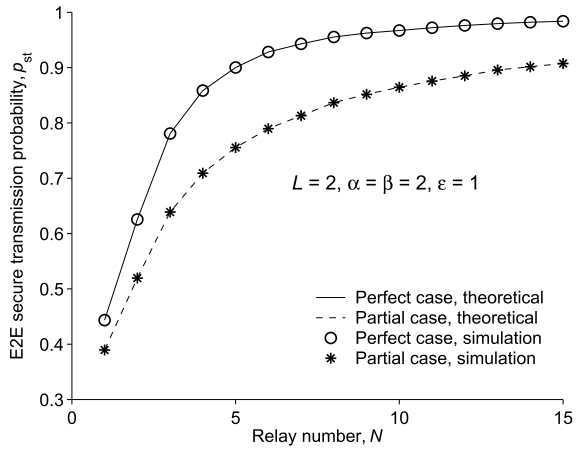
(b) Expected E2E delay vs. target secrecy rate ε.

Fig. 3. E2E STP and expected E2E delay vs. target secrecy rate ε.

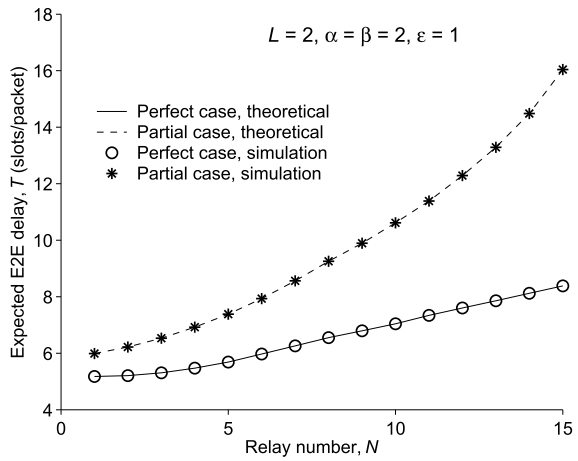
Similar to the settings in [39], we set the noise variance as $\sigma^2 = 1$, the transmission power as $P = 20$, and the average channel gains of the source-relay and relay-destination links as $\gamma_{sr} = \gamma_{rd} = 5$dB. Thus, the corresponding average SNR high enough to guarantee successful 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.

B. 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} ($\Delta = \{\mathrm{PF}, \mathrm{PT}\}$) are summarized in Fig. 3a, and the results of expected E2E delay T_Δ are summarized in Fig. 3b, 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 Fig. 4a for the simulated and theoretical results of p_{st}^{Δ} and in Fig. 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 $\varepsilon = 1$.

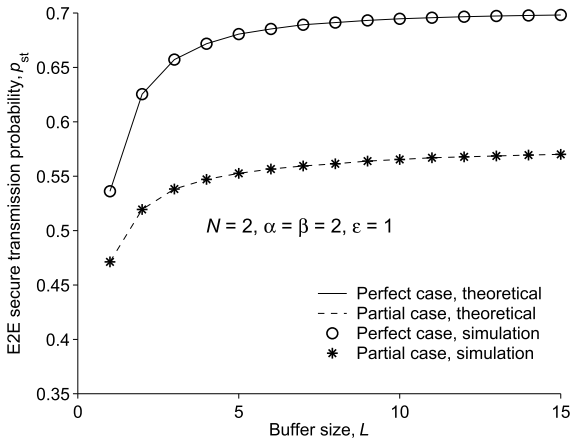


(a) E2E STP vs. relay number N.

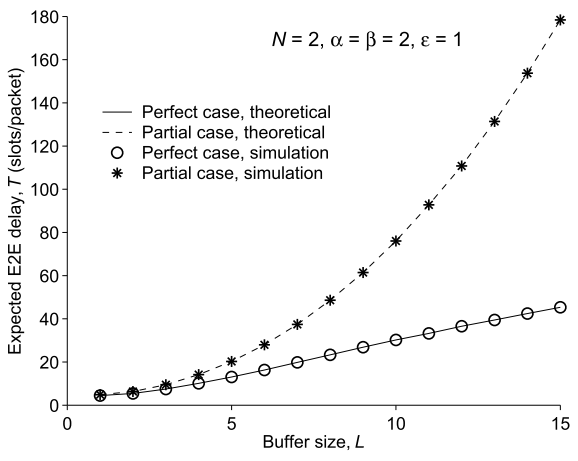


(b) Expected E2E delay vs. relay number N.

Fig. 4. E2E STP and expected E2E delay vs. number of relays N.



(a) E2E STP vs. buffer size L.



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

Fig. 5. E2E STP and expected E2E delay vs. buffer size L.

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 Fig. 5a and Fig. 5b, respectively.

We can see from Fig. 3a, Fig. 4a and Fig. 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 Fig. 3b, Fig. 4b and Fig. 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.

C. Performance Discussion

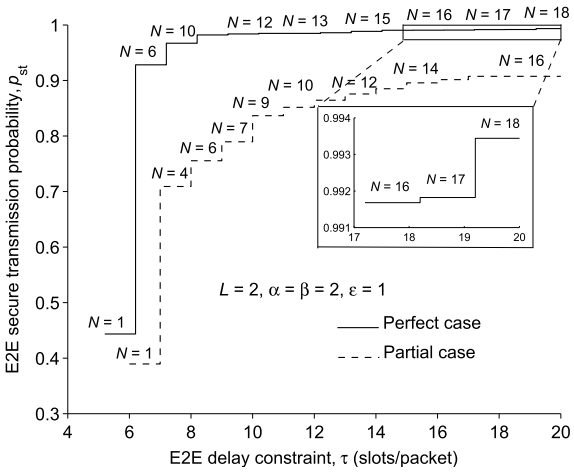
With the help of theoretical modeling for the E2E STP p_{st}^{Δ} and expected E2E delay T_{Δ}, we now explore how the network parameters (e.g., N, L and ε) affect the delay and security performances of the system under both eavesdropping CSI cases.

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 Fig. 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 Fig. 3b that the T_{Δ} increases as ε increases in both cases. According to the transmission schemes in Section III-B, 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 (4) and (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.

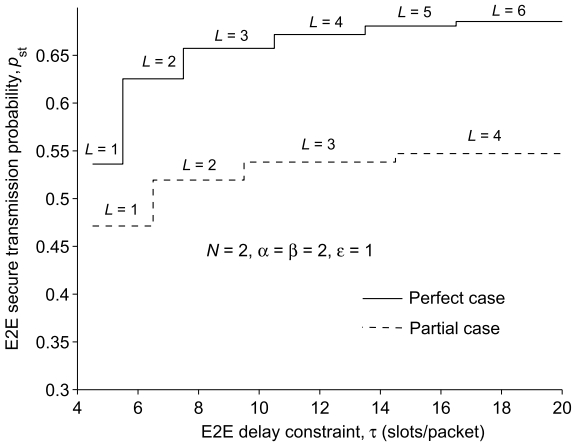
Next we investigate the impact of number of relays N on the p_{st}^{Δ} and T_{Δ} for given ε and L. Fig. 4 illustrates how p_{st}^{Δ}

and T_Δ vary with N for the setting of $L = 2$, $\alpha = \beta = 2$ and $\varepsilon = 1$. We can see from Fig. 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 Fig. 4b that the expected E2E delay increases as the number of relays N increases simultaneously. This is also due to the two-edged 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 Fig. 5. As can be seen from Fig. 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 Fig. 5a indicates that as the buffer size increases above a certain value, for example, $L = 5$ in Fig. 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.



(a) Maximum achievable E2E STP for varying N.



(b) Maximum achievable E2E STP for varying L.

Fig. 6. Maximum achievable E2E STP vs. E2E delay constraint τ.

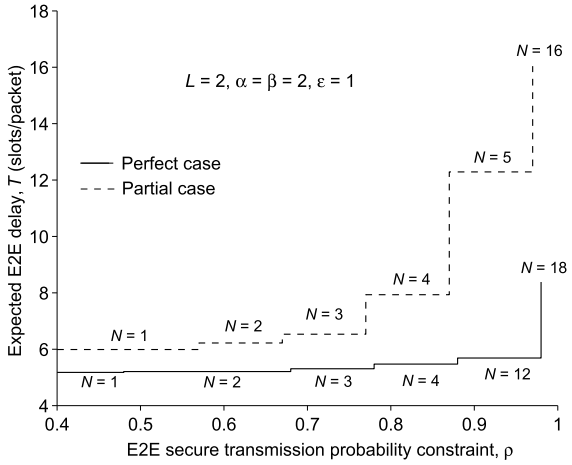
D. Security-Delay Trade-Off Analysis

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.

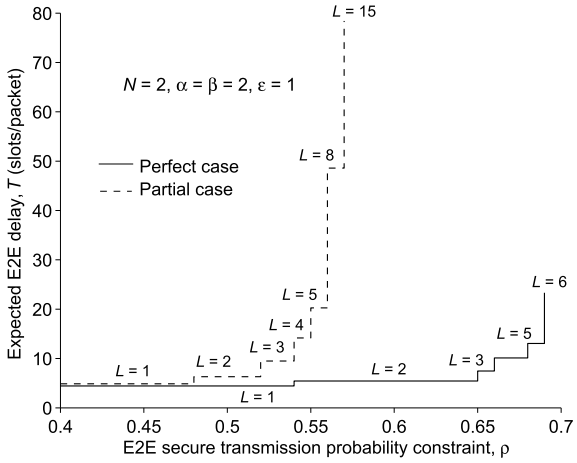
First, we study the achievable E2E STP region under a given constraint on the expected E2E delay in both eavesdropper CSI cases. For the scenario of $\alpha = \beta = 2$ and $\varepsilon = 1$, Fig. 6a (resp. Fig. 6b) illustrates the maximum E2E STP p_{st}^{Δ} achieved by the optimal number of relays 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 Fig. 6a and Fig. 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 Fig. 6a (resp. Fig. 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 Fig. 6 indicates that, as τ scales up, the maximum achievable E2E STP with respect to L in Fig. 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 Fig. 6a. For example, under the perfect eavesdropper CSI case, as τ increases from 18 to 20, the maximum STP in Fig. 6b remains unchanged while that in Fig. 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 Fig. 7a (resp. Fig. 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 Fig. 7a and Fig. 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.



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



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

Fig. 7. Minimum achievable expected E2E delay vs. E2E STP constraint ρ.

It can also be observed from Fig. 7a and Fig. 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 Fig. 7a and about 0.7 (0.558) for the perfect (partial) CSI case in Fig. 7b. This is because that, under the fixed setting of $\alpha = \beta = 2$ and $\varepsilon = 1$, the E2E STP of each case finally converges to the corresponding threshold as N (resp. L) scales up for $L = 2$ (resp. $N = 2$), as can seen from Fig. 4a (resp. Fig. 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 Fig. 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 Fig. 7a remains unchanged while that in Fig. 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.

VI. Conclusion

This paper 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 paper 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.

Appendix
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 [22], we know that the cumulative distribution functions (CDFs) of X and Y are

$$F_X(x) = \sum_{n_1=0}^{N_1(s_i)} \binom{N_1(s_i)}{n_1} (-1)^{n_1} \frac{\alpha}{kx+\alpha}, \tag{51}$$

and

$$F_Y(y) = \left(\frac{y}{\beta+y}\right)^{N_2(s_i)}, \tag{52}$$

respectively, where $\alpha = \frac{\gamma_{sr}}{\gamma_{se}}$, $\beta = \frac{\gamma_{rd}}{\gamma_{re}}$. According to the relay selection scheme in (4) and (5), transmission at each time slot occurs on the link with instantaneous channel gain $\max\{X, Y\}$. According to the transmission scheme in Section II-B, 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

$$a_{i,i} = \mathbb{P}\left(\log(\max\{X, Y\}) < \varepsilon\right) \tag{53}$$

$$= \mathbb{P}(\max\{X, Y\} < 2^{\varepsilon}) \tag{54}$$

$$= F_X(2^{\varepsilon}) \cdot F_Y(2^{\varepsilon}) \tag{55}$$

$$= \mu_{\mathrm{PF}}(s_i), \tag{56}$$

where $\mu_{\mathrm{PF}}(s_i)$ is given in (9) with $s = s_i$ and the last step follows after substituting (51) and (52) into (53). Next, the probability that s_i moves to $\mathcal{S}_i^-$ can be given by

$$\mathbb{P}(\mathcal{S}_i^-|s_i) = \mathbb{P}\left(\max\{X, Y\} \geq 2^{\varepsilon}, X < Y\right) \quad (57)$$

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

$$= 1 - \mu_{\mathrm{PF}} - \int_{2^{\varepsilon}}^{\infty} F_Y(x) f_X(x)\mathrm{d}x \quad (58)$$

$$= 1 - \mu_{\mathrm{PF}}(s_i) - \nu_{\mathrm{PF}}(s_i), \quad (59)$$

where $\nu_{\mathrm{PF}}(s)$ is given in (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 $\mu_{\mathrm{PT}}(s_i)$, $\frac{1-\mu_{\mathrm{PT}}(s_i)-\nu_{\mathrm{PT}}(s_i)}{N_2(s_i)}$ and $\frac{\nu_{\mathrm{PT}}(s_i)}{N_1(s_i)}$ respectively, where

$$\mu_{\mathrm{PT}}(s_i) = F_{X'}(2^{\varepsilon}) \cdot F_{Y'}(2^{\varepsilon}), \quad (60)$$

is given by (11) after substituting $F_{X'}(2^{\varepsilon})$ and $F_{Y'}(2^{\varepsilon})$ in and

$$\nu_{\mathrm{PT}}(s_i) = \int_{2^{\varepsilon}}^{\infty} F_{Y'}(x) f_{X'}(x)\mathrm{d}x \quad (61)$$

is given by (12) after calculating the above integral.

REFERENCES

[1] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in *Proc. IEEE Int. Conf. Comput. Sci. Electron. Eng. (ICCSEE)*, vol. 1. Mar. 2012, pp. 647–651.

[2] T. Karygiannis and L. Owens, "Wireless network security," *NIST Special Publication*, vol. 800, p. 48, Nov. 2002.

[3] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5th ed. Englewood Cliffs, NJ, USA: Prentice-Hall, Jan. 2010.

[4] C. D. T. Thai, J. Lee, and T. Q. S. Quek, "Physical-layer secret key generation with colluding untrusted relays," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1517–1530, Feb. 2016.

[5] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, 1994, pp. 124–134.

[6] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

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

[8] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[9] 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.

[10] 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, Oct. 2011.

[11] R. A. Chou and A. Yener, "Polar coding for the multiple access wiretap channel via rate-splitting and cooperative jamming," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2016, pp. 983–987.

[12] F. Zhu, F. Gao, and M. Yao, "Zero-forcing beamforming for physical layer security of energy harvesting wireless communications," *EURASIP J. Wireless Commun. Netw.*, vol. 2015, no. 1, p. 58, Dec. 2015

[13] T. M. Hoang, T. Q. Duong, H. A. Suraweera, C. Tellambura, and H. V. Poor, "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.

[14] H. Wen, P.-H. Ho, and B. Wu, "Achieving secure communications over wiretap channels via security codes from resilient functions," *IEEE Wireless Commun. Lett.*, vol. 3, no. 3, pp. 273–276, Jun. 2014.

[15] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," in *Proc. Inf. Theory Workshop*, 2009, pp. 95–99.

[16] 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," *Appl. Math. Comput.*, vol. 296, pp. 153–167, Mar. 2017.

[17] N. Nomikos *et al.*, "Relay selection for secure 5G green communications," *Telecommun. Syst.*, vol. 59, no. 1, pp. 169–187, 2015.

[18] H. Hu, R. Lu, C. Huang, and Z. Zhang, "PTRS: A privacy-preserving trust-based relay selection scheme in VANETs," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 5, pp. 1204–1218, 2017.

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

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

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

[22] 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.

[23] Y. Zhang, T. Liang, and A. Sun, "A new Max-ratio relay selection scheme in secure buffer-aided cooperative wireless networks," in *Proc. 8th Int. Symp. Comput. Intell. Design (ISCID)*, vol. 1. 2015, pp. 314–317.

[24] X. Tang, Y. Cai, Y. Huang, T. Q. Duong, W. Yang, and W. Yang, "Secrecy outage analysis of buffer-aided cooperative MIMO relaying systems," *IEEE Trans. Veh. Technol.*, to be published, doi: 10.1109/TVT.2017.2695500.

[25] 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," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[26] X. Luo and R. C. de Lamare. (2016). "Study of relay selection for physical-layer security in buffer-aided relay networks based on the secrecy rate criterion." [Online]. Available: https://arxiv.org/abs/1605.04487

[27] 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, Oct. 2015.

[28] T. Islam, A. Ikhlef, R. Schober, and V. K. Bhargava, "Diversity and delay analysis of buffer-aided BICM-OFDM relaying," *IEEE Trans. Wireless Commun.*, vol. 12, no. 11, pp. 5506–5519, Nov. 2013.

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

[30] 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, Apr. 2012.

[31] X. Liao, Z. Wu, Y. Zhang, and X. Jiang, "The delay-security trade-off in two-hop buffer-aided relay wireless network," in *Proc. Int. Conf. Netw. Netw. Appl.*, 2016, pp. 173–177.

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

[33] 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, May 2012.

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

[35] 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. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013.
[36] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1771–1783, May 2015.
[37] C. Wang and H.-M. Wang, "On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1814–1827, Nov. 2014.
[38] C. Cai, Y. Cai, X. Zhou, W. Yang, and W. Yang, "When does relay transmission give a more secure connection in wireless ad hoc networks?" *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 624–632, Apr. 2014.
[39] 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, May 2012.
[40] J. R. Norris, *Markov Chains*. Cambridge, U.K.: Cambridge Univ. Press, 1998.
[41] T. Robertazzi, *Computer Networks and Systems: Queueing Theory and Performance Evaluation*. New York, NY, USA: Springer, 2012.
[42] (2017). *C++ Simulator for E2E Delay and STP Performance in Two-Hop Wireless Networks*. [Online]. Available: http://xnliao.blogspot.com/

Xuening Liao received the B.S. degree in software engineering in computer science from Shaanxi Normal University, Xi'an, China, in 2012. She is currently pursuing the Ph.D. degree in Future University Hakodate, Hakodate, Japan. From 2012 to 2015, she did research on network security as a Doctor Student in computer software and theory with Shaanxi Normal University. Her research interests include network coding, physical layer security of wireless communication, and performance modeling of buffer-aided relay wireless networks.

Yuanyu Zhang received the B.S. degree in software engineering and the M.S. degree in computer science from Xidian University, Xi'an, China, in 2011 and 2014, respectively, and the Ph.D. degree from the School of Systems Information Science, Future University Hakodate, Hokkaido, Japan, in 2017. He is currently an Assistant Professor with the Graduate School of Information Science, Nara Institute of Science and Technology, Japan. His research interests include physical layer security of wireless communications, and performance modeling, and evaluation of wireless networks.

Zhenqiang Wu received the B.S. degree from Shaanxi Normal University, China, in 1991, and the M.S. and Ph.D. degrees from Xidian University, China, in 2002 and 2007, respectively. He is currently a Full Professor with Shaanxi Normal University, China. His research interests include computer communications networks, mainly wireless networks, network security, anonymous communication, and privacy protection. He is a member of ACM and senior of CCF.

Yulong Shen (M'08) received the B.S., M.S., and Ph.D. degrees in computer science from Xidian University, Xi'an, China, in 2002, 2005, and 2008, respectively. He is currently a Full Professor with the School of Computer Science and Technology, Xidian University and a Researcher with the State Key Laboratory of Integrated Services Networks, China. He has also served on the technical program committees of several international conferences, including ICEBE, INCoS, CIS, and SOWN. He is an ACM member. His research interest is wireless network security.

Xiaohong Jiang (M'03–SM'08) received the B.S., M.S., and Ph.D. degrees from Xidian University, China, in 1989, 1992, and 1999, respectively. He was an Associate Professor with Tohoku University from 2005 to 2010. He is currently a Full Professor with Future University Hakodate, Japan. His research interests include computer communications networks, mainly wireless networks and optical networks, network security, and routers/switches design. He has published over 300 technical papers at premium international journals and conferences, which include over 70 papers published in the top IEEE journals and the top IEEE conferences, like the IEEE–ACM TRANSACTIONS ON NETWORKING, the IEEE JOURNAL OF SELECTED AREAS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, and the IEEE INFOCOM. He received the Best Paper Award of the IEEE HPCC 2014, IEEE WCNC 2012, IEEE WCNC 2008, IEEE ICC 2005-Optical Networking Symposium, and the IEEE/IEICE HPSR 2002. He is a Member of IEICE.

Hiroshi Inamura (M'09) received the B.S., M.S., and Ph.D. degrees from Keio University, Japan. He was an Executive Research Engineer at NTT Docomo, Inc. from 2006 to 2009. He is currently a Full Professor with the School of Systems Information Science, Future University Hakodate, Hakodate, Japan. His research interests include mobile computing, system software for smart devices, mobile/sensor network, and their security. He is a member of IPSJ, IEICE, and ACM.