Zhou *et al. J Wireless Com Network* (2022) 2022:44
https://doi.org/10.1186/s13638-022-02127-1

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Virtual full-duplex buffer-aided relay selection schemes for secure cooperative wireless networks

Jiayu Zhou[1], Deli Qiao[1,2*] and Haifeng Qian[3,4]

*Correspondence:
dlqiao@ce.ecnu.edu.cn

[1] School of Communication and Electronic Engineering, East China Normal University, Shanghai, China
Full list of author information is available at the end of the article

Abstract

This paper considers secure communication in buffer-aided cooperative wireless networks in the presence of one eavesdropper, which can intercept the data transmission from both the source and relay nodes. It is assumed that the relays employ the randomize-and-forward (RF) strategy such that the eavesdropper can only decode the signals received in the two hops independently. Two cooperative secure transmission schemes, i.e., hybrid imitating full-duplex max-max-ratio relay selection (HyIFD) scheme and threshold-based link selection (TBLS) scheme are proposed for adaptive- and fixed-rate transmissions aiming at improving the secrecy throughput and secrecy outage probability, respectively. For adaptive-rate transmissions (ART), the proposed scheme switches among three sub-strategies according to different conditions such as the number of relays and transmit power. Different relays are chosen for reception and transmission according to the ratio of the legitimate channels to the eavesdropper channels to imitate the full-duplex transmission mode. For fixed-rate transmissions (FRT), a hybrid HD/FD transmission mode is designed to increase the transmission probabilities of two hops under the transmission quality constraint. Two parameters are introduced and optimized to minimize the secrecy outage probability. A sub-optimal TBLS (SO-TBLS) scheme is also given. Theoretical analysis of the secrecy throughput and the secrecy outage probability are provided and the closed-form expressions are derived, and verified by numerical results. It is shown that the proposed schemes outperform benchmark schemes in terms of secrecy throughput and secrecy outage probability.

Keywords: Buffer-aided relay, Physical layer security, Cooperative communication, Virtual full-duplex, Link selection, Secrecy throughput analysis, Secrecy outage probability analysis

1 Introduction

1.1 Motivation

Wireless communication technologies play an important role in military and civil applications, and have become a necessitative part of our daily life [1]. However, the broadcast nature of wireless medium makes the communication over wireless networks susceptible to the interception attacks from unauthorized users (eavesdroppers), and

thus guaranteeing the security of wireless communication has become an increasingly urgent demand [2].

Traditionally, the security mechanism of wireless communication network is mainly learned from wired computer network, in which the problem of information confidentiality is mainly solved by encryption algorithms based on symmetric key and public key system. The security of encryption algorithms is guaranteed by the extremely high computational complexity required to crack the password [3]. However, with the improvement of computing capability and speed of the devices, more and more complicated algorithms are required to guarantee the same level of security as before.

On the other hand, physical layer security techniques provide a new way to enhance the security of wireless transmission from a new perspective. The core idea is to improve the information confidentiality from coding in information theory, which is highly promising to guarantee everlasting secure communication for wireless networks and has received a lot of attentions [4–9, 16–25]. In the seminal work by Wyner [5], the wiretap channel model was introduced and the possibility of creating perfectly secure communication links without relying on secret keys was demonstrated.

Moreover, cooperative communication is also a building block of current communication systems. The main idea of this technique is to enhance the system performance by providing additional paths between the source and the destination via the relays. It is worth noting that, cooperative relays can provide additional degrees of freedom and more flexible implementations for improving physical layer security. In [6], the relay-eavesdropper channel was studied and different node cooperation strategies were analyzed. It has been shown that cooperative communication provides an effective way to improve the secrecy capacity. On top of that, several relay strategies have been designed in literature [7–9].

Meanwhile, the use of buffers at the relays makes it possible to store packets and transmit them in more favorable wireless conditions, which greatly increases the network's resiliency, throughput and diversity, and has therefore been widely applied in cooperative networks to improve the system performance [10–15]. For instance, in [10], the authors applied the deep reinforcement learning for the relay selection in the delay-constrained buffer-aided relay networks. Two asynchronous learning algorithms for joint hybrid non-orthogonal-multiple-access (NOMA)/OMA relay selection and power allocation in buffer-aided delay-constrained networks were proposed in [11]. A buffer-aided relay selection scheme was presented in [12] to seamlessly include both NOMA and OMA transmission in the Internet of Things. The authors in [13] designed the buffer-aided adaptive transmission scheme for the buffer-aided wireless powered cooperative NOMA relaying network. A novel buffer-aided relay selection scheme which is able to balance the outage performance and packet delay was proposed in [14]. In [15], NOMA, buffer-aided full-duplex (FD) relaying and broadcasting were combined to improve the relay selection with low complexity.

Furthermore, the buffer-aided relay is widely used in the research area of physical layer security due to the advantage of improving the secrecy performance [16–25]. For instance, in [16], we have designed the link selection and power control policies for secure communication over a buffer-aided two hop communication link. In [17], the multi-agent deep reinforcement learning based joint design of relay selection and

intelligent reflecting surface reflection coefficients was investigated in IRS-assisted secure buffer-aided cooperative networks. In [18], the authors proposed several secure transmission schemes for an energy-harvesting based secure two-way relay network. The use of data and energy buffering in wireless powered relays was proposed while scheduling schemes were also designed to increase the secrecy throughput in [19]. In [20], the authors applied the reinforcement learning in the joint relay selection and power allocation in the secure cognitive radio (CR) relay network, where the data buffers and full-duplex jamming were applied at the relay nodes.

In general, there are three main techniques utilized to protect the confidential messages and improve the secrecy capacity in a cooperative network, including the beamforming [26, 27], the jamming [28, 29] and the relay selection [6, 24, 30]. In this work, we investigate the relay selection policies for achieving better security performance.

Note that a relay usually operates in either FD or half-duplex (HD) mode. In FD relaying, the relays transmit and receive at the same time and frequency, at the cost of hardware complexity [31, 32]. In HD relaying, relays are incapable of transmitting and receiving simultaneously, thus leading to reduced capacity of the whole network. Hence, we expect to achieve virtual FD communication with HD relays via link selection. Inspired by the space full-duplex max-max relay selection (SFD-MMRS) scheme in [33], which mimics FD relaying with HD relays via link selection. In this paper, we propose two novel max-ratio relay selection schemes for adaptive- and fixed-rate secure transmission in HD randomize-and-forward (RF) buffer-aided cooperative network with an eavesdropper which can intercept signals from both the source and relay nodes. It is worth noting that in such a scenario, the source-to-relay and relay-to-destination transmissions have different statistical characterizations even if the channel statistics are the same.

- The overall basic idea of the proposed hybrid imitate full-duplex (HyIFD) max-ratio relay selection scheme is that different relays are chosen for simultaneously reception and transmission according to the ratio of the legitimate channels to the eavesdropper channels to imitate the full-duplex transmission mode. In view of the asymmetry of two-hop channel in secure communication under the full CSI assumption, the proposed HyIFD scheme switches among three sub-strategies with different preference on the two-hops according to different conditions such as relay numbers and transmit power aiming at improving the secrecy throughput performance for adaptive rate transmissions (ART).
- The overall basic idea of the proposed threshold-based link selection (TBLS) scheme is that a hybrid HD/FD link selection policy is designed to increase the transmission probabilities of two hops under the transmission quality constraint. Two non-negative scalars were introduced to determine the threshold for choosing when the relay listens or transmits and optimized to assess the quality of both the $S-R$ link and the $R-D$ link in order to improve the secrecy outage probability performance for fixed rate transmissions (FRT).

A sub-optimal TBLS (SO-TBLS) scheme is then considered as a good alternative to TBLS with lower requirements for computational complexity by setting appropriate

values for these two parameters. Numerical results in accordance with theoretical analysis show the superiority of the proposed schemes over the existing max-ratio schemes in terms of secrecy throughput and secrecy outage probability.

1.2 Contributions

The main contributions of this paper can be summarized as follows:

1. We propose a novel HyIFD max-ratio relay selection scheme for ART in a secure buffer-aided RF cooperative system, in which different relays are selected for simultaneously reception and transmission to imitate the full-duplex transmission. Also, we derive the associated closed-form expressions for the secrecy throughput and obtain the asymptotic limit.
2. We propose a TBLS max-ratio relay selection scheme for FRT in a secure buffer-aided RF multi-relay network, where HD/FD modes are switched to maximize the transmission opportunity of two hops under transmission quality constraint. We derive the closed-form expressions for the secrecy outage probability of the TBLS scheme. We also propose a sub-optimal TBLS scheme with performance close to the optimal one.
3. Numerical results in accordance with theoretical analysis validate that the proposed schemes can further improve the secrecy throughput and secrecy outage probability performance compared with benchmark schemes. It is also shown that the relay with the best channel quality for the first-hop is preferred in the high-SNR regime while the relay with the best channel quality in the second-hop is always favored in the low-SNR regime.

1.3 Organization

The reminder of this paper is organized as follows. Section 2 presents the system model. Two existing max-ratio relay selection schemes for secure buffer-aided cooperative wireless networks are briefly introduced in Sect. 3. Section 4 gives the introduction of the HyIFD scheme, comprehensive analysis of the achievable secrecy throughput and the asymptotic closed-form expressions for the throughput performance limit. Section 5 proposes a TBLS scheme and analyzes the secrecy outage probability. Numerical results are provided in Sect. 6. Finally, conclusions are drawn in Sect. 7 with some lengthy proofs in the Appendices.

2 System model

We consider a HD two-hop wireless system formed by one source node S, a set of K RF relays $\{R_1, \ldots, R_K\}$, one destination node D, and one eavesdropper E which can intercept signals from both the source and relay nodes, as shown in Fig. 1. All nodes are assumed to be equipped with a single antenna. Under the RF decoding strategy, the relay uses a codebook different from that used by source, so the eavesdropper can only independently decode the message received in the two hops [9]. We assume that there is a buffer of infinite length at each relay such that each relay can store the information received from the source and transmit it in later time.

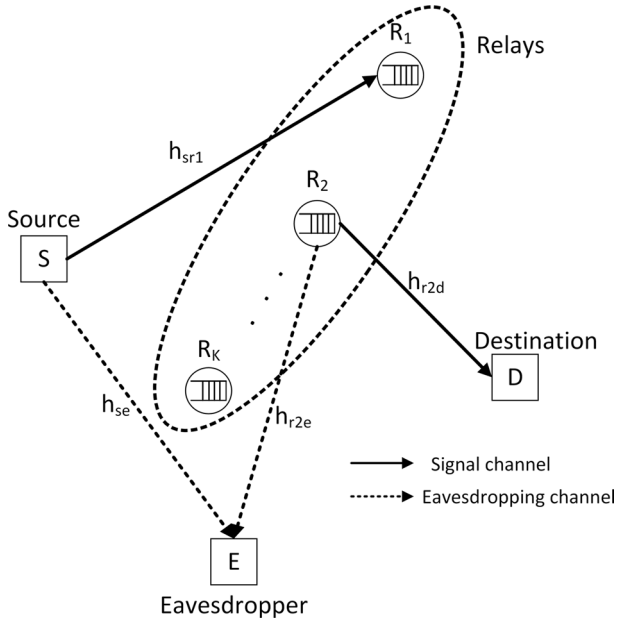

Fig. 1 Illustration of system model

We assume that the distance between the source and destination is large enough and the communications can be established only via relays. We use $h_{sr_k}(t)$, $h_{se}(t)$, $h_{r_kd}(t)$ and $h_{r_ke}(t)$ to denote the channel coefficients for $S-R_k$, $S-E$, R_k-D and R_k-E links at time t, respectively. The channel is assumed to be stationary and ergodic. We consider the Rayleigh block fading where the channel coefficients remain constant during one time slot and vary independently from one to another. In addition to fading, all wireless links are impaired by additive white Gaussian noise (AWGN) with variance N_0. Without loss of generality, we assume that the noise variances at the receiving nodes are equal to one, i.e., $N_0 = 1$. The transmit power of the source and relays are assumed to be P_S and P_R, respectively.

We assume that all $S-R_k$, $S-E$, R_k-D, and R_k-E links are independent and identically distributed (i.i.d.) fading, which is a typical assumption to facilitate analysis [21]. We assume that the mean of $S-R_k$, $S-E$, R_k-D and R_k-E channel gains are $\mathbb{E}[|h_{sr_k}|^2]=\gamma_{sr}$, $\mathbb{E}[|h_{se}|^2]=\gamma_{se}$, $\mathbb{E}[|h_{r_kd}|^2]=\gamma_{rd}$ and $\mathbb{E}[|h_{r_ke}|^2]=\gamma_{re}$, respectively, where $\mathbb{E}[\cdot]$ denotes the expectation. Same as [16] and [24], we assume the instantaneous channel state information (CSI) of legitimate channels (i.e., $|h_{sr_k}|^2$ and $|h_{r_kd}|^2$) are always known. Regarding the knowledge of eavesdropper CSI, we consider the perfect CSI case where the instantaneous eavesdropper CSI (i.e., $|h_{se}|^2$ and $|h_{r_ke}|^2$) are known. Note however that, when the eavesdropper is passive and its behavior can not be monitored, the assumption of the exact CSI of the eavesdropper's link might be unrealistic. We also consider the partial CSI case where only the average gains of the eavesdropping channels are available. Since the derivations are similar and much more simple, they are omitted in this paper due to the limit of space.

3 Existing relaying schemes

In this part, we review two existing relay selection protocols for secure buffer-aided cooperative wireless networks.

3.1 Max-min-ratio relay selection

With the RF relaying strategy applied at the relays, the instantaneous secrecy rate for the buffer-aided multi-relay systems is obtained as [6]

$$C_k(t) = \left[\frac{1}{2}\log_2 \max_{k\in\{1,\ldots,K\}} \left\{\min\left\{\frac{1+P_S|h_{sr_k}(t)|^2}{1+P_S|h_{se}(t)|^2}, \frac{1+P_R|h_{r_kd}(t)|^2}{1+P_R|h_{r_ke}(t)|^2}\right\}\right\}\right]^+, \tag{1}$$

where $[\cdot]^+ = \max\{\cdot, 0\}$. The secrecy throughput is given by $\mathbb{E}[C_k]$. The best relay node can be selected with the maximum $C_k(t)$. This scheme is termed as the max-min-ratio relay selection. For convenience in development, the time index t is ignored in the rest of the paper unless necessary.

3.2 Max-link-ratio relay selection

This protocol chooses the best link with the highest gain ratio among all available source-to-relay and relay-to-destination links [24]. If the exact knowledge of all channels, including the eavesdropping channels h_{se} and h_{r_ke}, are available, the max-link-ratio selects the best relay R_k as

$$k = \arg \max_{k\in\{1,\ldots,K\}} \left\{\frac{\max\limits_{k\in\{1,\ldots,K\}}\{|h_{sr_k}|^2\}}{|h_{se}|^2}, \max_{k\in\{1,\ldots,K\}}\left\{\frac{|h_{r_kd}|^2}{|h_{r_ke}|^2}\right\}\right\}. \tag{2}$$

4 The proposed methods for adaptive-rate transmissions

In this section, we propose a HyIFD relay selection scheme with three modes for ART and analyze its performance in terms of secrecy throughput. Based on the overall system power constraint, we define the maximal achievable secrecy throughput and obtain the asymptotic characterizations of the maximum achievable secrecy throughput in the high-SNR regime.

4.1 Three sub-strategies of HyIFD policy

In ART, the source and relays can adjust their transmission rate according to the channel gains without causing outages. In view of the asymmetry of two-hop channel in secure communication under the full CSI assumption, we have three different modes with different preference on the two-hops.

4.1.1 Mode I

In mode I, the two hops are given the same priority and the relays with the best bottleneck link of the two hops are chosen in each time slot. Specifically, this mode is

similar to [33] whereas the eavesdropper channel is also included. First, we set the best and the second best relay for reception R_{r_1} and R_{r_2} respectively based on

$$r_1 = \arg \max_{k\in\{1,\ldots,K\}} \left\{ \frac{1+P_S|h_{sr_k}|^2}{1+P_S|h_{se}|^2} \right\}, \tag{3}$$

$$r_2 = \arg \max_{k\neq r_1 k\in\{1,\ldots,K\}} \left\{ \frac{1+P_S|h_{sr_k}|^2}{1+P_S|h_{se}|^2} \right\}, \tag{4}$$

and then set the best and the second best relay for transmission R_{t_1} and R_{t_2} respectively according to

$$t_1 = \arg \max_{k\in\{1,\ldots,K\}} \left\{ \frac{1+P_R|h_{r_k d}|^2}{1+P_R|h_{r_k e}|^2} \right\}, \tag{5}$$

$$t_2 = \arg \max_{k\neq t_1 k\in\{1,\ldots,K\}} \left\{ \frac{1+P_R|h_{r_k d}|^2}{1+P_R|h_{r_k e}|^2} \right\}. \tag{6}$$

Denote

$$z_{r_1} = \frac{\max\limits_{k\in\{1,\ldots,K\}} \left\{1+P_S|h_{sr_k}|^2\right\}}{1+P_S|h_{se}|^2}, \tag{7}$$

$$z_{r_2} = \frac{\max\limits_{k\neq r_1 k\in\{1,\ldots,K\}} \left\{1+P_S|h_{sr_k}|^2\right\}}{1+P_S|h_{se}|^2}, \tag{8}$$

$$z_{t_1} = \max_{k\in\{1,\ldots,K\}} \left\{ \frac{1+P_R|h_{r_k d}|^2}{1+P_R|h_{r_k e}|^2} \right\}, \tag{9}$$

$$z_{t_2} = \max_{k\neq t_1 k\in\{1,\ldots,K\}} \left\{ \frac{1+P_R|h_{r_k d}|^2}{1+P_R|h_{r_k e}|^2} \right\}. \tag{10}$$

Let

$$Q = \min\{z_{r_1}, z_{t_2}\} - \min\{z_{r_2}, z_{t_1}\}. \tag{11}$$

When the same relay share the best $S-R$ and the best $R-D$ channel, we would like to choose between the following two possibilities. One is to select the relay with the second best $S-R$ channel R_{r_2} and the relay with the best $R-D$ channel R_{t_1} for reception and transmission, respectively. The other is to select the relay with the best $S-R$ channel R_{r_1} and the relay with the second best $R-D$ channel R_{t_2} for reception and transmission, respectively. And the value Q defined here is used to indicate that which of the two options with the better bottleneck link.

Then, in the mode I, the relays selected for reception $R_{\tilde{r}}$ and transmission $R_{\tilde{t}}$ are chosen as

$$(R_{\tilde{r}}, R_{\tilde{t}}) = \begin{cases} (R_{r_1}, R_{t_1}), \text{ if } \quad r_1 \neq t_1 \\ (R_{r_1}, R_{t_2}), \text{ if } \quad r_1 = t_1 \text{ and } Q > 0 \\ (R_{r_2}, R_{t_1}), \text{ otherwise.} \end{cases} \tag{12}$$

4.1.2 Mode II

In the mode II, the best $S - R$ link will always be selected if the same relay is the best relay for both the S-R and R-D links, and the relays selected for reception $R_{\tilde{r}}$ and transmission $R_{\tilde{t}}$ are chosen as

$$(R_{\tilde{r}}, R_{\tilde{t}}) = \begin{cases} (R_{r_1}, R_{t_1}), \text{ if } \quad r_1 \neq t_1 \\ (R_{r_1}, R_{t_2}), \text{ otherwise.} \end{cases} \tag{13}$$

4.1.3 Mode III

In the mode III, the $R - D$ link is given higher priority, and the relays selected for reception $R_{\tilde{r}}$ and transmission $R_{\tilde{t}}$ are chosen as

$$(R_{\tilde{r}}, R_{\tilde{t}}) = \begin{cases} (R_{r_1}, R_{t_1}), \text{ if } \quad r_1 \neq t_1 \\ (R_{r_2}, R_{t_1}), \text{ otherwise.} \end{cases} \tag{14}$$

Besides, we should note that because of the buffers used at the relay, the proposed scheme introduces a delay in the network. It is expected that when more relays are employed in the network and no delay constraint is imposed, some packets may experience increased delays. The better secrecy throughput performance may at the cost of higher average delay. The analysis of involving average delay in the design would be interesting and are left for future research. For instance, statistical delay constraints can be considered [34–36].

4.2 Secrecy throughput analysis

In this part, we perform the secrecy throughput analysis for the above three modes, respectively.

4.2.1 Mode I

Considering that we employ the RF relaying strategy [8], the eavesdropper cannot combine the data transmitted by source and relay at each time slot. Same as [33], we assume that there is no inter-relay links and also no inter-relay interference when the receiving and transmitting relays are active in the same time-slot. In practice, this assumption is valid if the relays are located far away from each other or if fixed infrastructure-based relays with directional antennas are used [37]. Therefore, when either the source wishes to transmit confidential information to the relay or the relay sends private message to the destination, it can be viewed as a single hop transmission in the presence of the interference from the other hop.

Assuming that the eavesdropper employs decoding with successful interference cancellation and the decoding order at the eavesdropper is not known at the source

or the relays, the maximum eavesdropping data rate is assumed to be upperbounded by $\log_2(1+P_S|h_{se}|^2)$ for the link $S-E$, and $\log_2(1+P_R|h_{r_ke}|^2)$ for the link R_k-E. If the relay R_k is selected for the data transmission, the instantaneous secrecy rate of the first and second hop are lowerbounded by

$$C_{SR} \geq \left[\log_2\left(\frac{1+P_S|h_{sr_k}|^2}{1+P_S|h_{se}|^2}\right)\right]^+, \tag{15}$$

$$C_{RD} \geq \left[\log_2\left(\frac{1+P_R|h_{r_kd}|^2}{1+P_R|h_{r_ke}|^2}\right)\right]^+, \tag{16}$$

respectively. In the following, we adopt the lowerbound for the analysis, which represents the worst case and specifies the minimum throughput achievable.

The secrecy throughput for the buffer-aided multi-relay system is given by [38]

$$C_s = \min\{\mathbb{E}[C_{SR}], \mathbb{E}[C_{RD}]\}, \tag{17}$$

where $\mathbb{E}[C_{SR}]$ and $\mathbb{E}[C_{RD}]$ denote the average secrecy throughput of the $S-R$ and $R-D$ links, respectively.

The average secrecy rate of the first and second hop, $\overline{C}_k$, $k \in \{SR, RD\}$, can be expressed as [33, (9)]

$$\overline{C}_k = \mathbb{E}[C_k] = (1-p_s)\overline{C}_{k,1} + p_s(\overline{C}_{k,21} + \overline{C}_{k,22}), \tag{18}$$

where p_s denote the probability that $r_1 = t_1$, $\overline{C}_{k,1}$ is the average throughput of the best channel of the first and second hop, $k \in \{SR, RD\}$, $\overline{C}_{k,21}$ and $\overline{C}_{k,22}$ denote the average throughput of the best channel and the second best channel of the first and second hop when $Q > 0$ and $Q < 0$, respectively.

Note that our selection policy involves eight independent channel coefficients, and hence finding the closed-form expressions is very tricky, if not intractable. So we derive the approximate closed-form expressions for the average secrecy throughput of the mode I.

The approximate secrecy throughput for the mode I is given by

$$C_{\mathrm{I}} = \min\{\mathbb{E}[C_{SR}^{\mathrm{I}}], \mathbb{E}[C_{RD}^{\mathrm{I}}]\}. \tag{19}$$

Proposition 1 *The average secrecy rate of the first hop for mode I can be approximately expressed as*

$$\mathbb{E}[C_{SR}^{\mathrm{I}}] \approx (1-p_s)\mathbb{E}[C_{SR,1}] + p_s(p_{12}\mathbb{E}[C_{SR,1}] + p_{21}\mathbb{E}[C_{SR,2}]), \tag{20}$$

where p_s denotes the probability that $r_1 = t_1$, p_{12} denotes the probability that $Q > 0$, p_{21} denotes the probability that $Q < 0$, i.e., $p_{21} = 1 - p_{12}$, $\mathbb{E}[C_{SR,1}]$ and $\mathbb{E}[C_{SR,2}]$ denote the average secrecy capacity of the best and the second best $S-R$ channel, respectively. Similarly, the average secrecy rate of the second hop for mode I can be approximately given as

$$\mathbb{E}[C_{RD}^{\mathrm{I}}] \approx (1-p_s)\mathbb{E}[C_{RD,1}] + p_s(p_{12}\mathbb{E}[C_{RD,2}] + p_{21}\mathbb{E}[C_{RD,1}]), \tag{21}$$

where $\mathbb{E}[C_{RD,1}]$ *and* $\mathbb{E}[C_{RD,2}]$ *denote the average secrecy capacity of the best and the second best* $R-D$ *channel, respectively.*

Proof Based on (12), we can divide the time index t into three cases correspondingly. If $r_1 \neq t_1$, we select the relay R_{r_1} for reception and the relay R_{t_1} for transmission. We denote such indices as $t \in \Omega_1$. If $r_1 = t_1$, we need to determine whether Q is positive or negative. If $Q > 0$, we select the relay R_{r_1} for reception and the relay R_{t_2} for transmission. We denote such time indices as $t \in \Omega_2$. Inversely, if $Q < 0$, we select the relay R_{r_2} for reception and R_{t_1} for transmission, and denote such time indices as $t \in \Omega_3$. Let N_1 denote the number of times in N transmissions that $r_1 = t_1$, and hence N_{12} denote the number of time instances in N_1 transmissions that $Q > 0$, and N_{21} denote the number of time instances in N_1 transmissions that $Q < 0$, i.e., $p_s = \frac{N_1}{N}$, $p_{12} = \frac{N_{12}}{N_1}$, and $p_{21} = \frac{N_{21}}{N_1} = 1 - p_{12}$.

The average secrecy rate of the first hop is given by

$$\begin{aligned}
E[C_{SR}^{\mathrm{I}}] &= \lim_{N\to\infty} \frac{1}{N}\sum_{t=1}^{N} C_{SR}(t) \\
&= \lim_{N\to\infty} \frac{1}{N}\left(\sum_{t\in\Omega_1} C_{SR_{r_1}}(t) + \sum_{t\in\Omega_2} C_{SR_{r_1}}(t) + \sum_{t\in\Omega_3} C_{SR_{r_2}}(t)\right) \\
&= \lim_{N\to\infty} \frac{N-N_1}{N}\cdot\frac{1}{N-N_1}\sum_{t\in\Omega_1} C_{SR}(t) + \frac{N_1}{N}\cdot\frac{N_{12}}{N_1}\frac{1}{N_{12}}\sum_{t\in\Omega_2} C_{SR}(t) \\
&\quad + \frac{N_1}{N}\cdot\frac{N_{21}}{N_1}\frac{1}{N_{21}}\sum_{t\in\Omega_3} C_{SR}(t) \\
&= (1-p_s)\mathbb{E}[C_{SR,1}] + p_s\cdot p_{12}\mathbb{E}[C_{SR,1}] + p_s\cdot p_{21}\mathbb{E}[C_{SR,2}].
\end{aligned} \tag{22}$$

The average secrecy rate of the second hop can be proved by the same logic. □

Proposition 2 *Given* P_S *and* P_R*, the detailed expressions for the terms in* (20) *and* (21) *can be expressed as follows*:

$$p_s = \frac{1}{K}, \tag{23}$$

$$\mathbb{E}[C_{SR,1}] = \sum_{r=1}^{K}\binom{K}{r}(-1)^r \frac{e^{\frac{r}{P_S\gamma_{sr}}}}{\ln 2}\left[-E_1\left(\frac{r}{P_S\gamma_{sr}}\right) + e^{\frac{1}{P_S\gamma_{se}}}E_1\left(\frac{r}{P_S\gamma_{sr}} + \frac{1}{P_S\gamma_{se}}\right)\right], \tag{24}$$

$$\mathbb{E}[C_{SR,2}] = \sum_{r=1}^{K-1} \binom{K-1}{r} (-1)^r \frac{e^{\frac{r}{P_S\gamma_{sr}}}}{\ln 2} \left[-E_1\left(\frac{r}{P_S\gamma_{sr}}\right) + e^{\frac{1}{P_S\gamma_{se}}} E_1\left(\frac{r}{P_S\gamma_{sr}} + \frac{1}{P_S\gamma_{se}}\right)\right] + \binom{K-1}{K-2} \sum_{r=0}^{K-1} \binom{K-1}{r} (-1)^r \frac{e^{\frac{r+1}{P_S\gamma_{sr}}}}{\ln 2} \left[-E_1\left(\frac{r+1}{P_S\gamma_{sr}}\right) + e^{\frac{1}{P_S\gamma_{se}}} E_1\left(\frac{r+1}{P_S\gamma_{sr}} + \frac{1}{P_S\gamma_{se}}\right)\right], \tag{25}$$

$$\mathbb{E}[C_{RD,1}] = \sum_{r=1}^{K} \binom{K}{r} (-1)^r \frac{\gamma_{re} e^{\frac{r}{P_R}\left(\frac{1}{\gamma_{rd}} + \frac{1}{\gamma_{re}}\right)}}{\ln 2\gamma_{rd}} \left[- e^{-\frac{r}{P_R\gamma_{re}}} E_1\left(\frac{r}{P_R\gamma_{rd}}\right) + \sum_{i=1}^{r} \left(\frac{(-1)^{i+1}\left(\frac{r}{P_R\gamma_{re}}\right)^{i-1} E_1\left(\frac{r}{P_R}\left(\frac{1}{\gamma_{rd}} + \frac{1}{\gamma_{re}}\right)\right)}{(i-1)!} + \frac{e^{-\frac{r}{P_R}\left(\frac{1}{\gamma_{rd}} + \frac{1}{\gamma_{re}}\right)}}{\left(\frac{\gamma_{re}}{\gamma_{rd}} + 1\right)^{i-1}} \sum_{j=0}^{i-2} \frac{(-1)^j \left(\frac{r}{P_R\gamma_{re}}\right)^j \left(\frac{\gamma_{re}}{\gamma_{rd}} + 1\right)^j}{(i-1)(i-2)\ldots(i-1-j)} \right)\right], \tag{26}$$

$$\begin{aligned}\mathbb{E}[C_{RD,2}] = {} & \sum_{r=1}^{K-1} \binom{K-1}{r} (-1)^r \frac{\gamma_{re} e^{\frac{r}{P_R}\left(\frac{1}{\gamma_{rd}} + \frac{1}{\gamma_{re}}\right)}}{\ln 2\gamma_{rd}} \left[- e^{-\frac{r}{P_R\gamma_{re}}} E_1\left(\frac{r}{P_R\gamma_{rd}}\right) \right. \\ & + \sum_{i=1}^{r} \left(\frac{(-1)^{i+1}\left(\frac{r}{P_R\gamma_{re}}\right)^{i-1} E_1\left(\frac{r}{P_R}\left(\frac{1}{\gamma_{rd}} + \frac{1}{\gamma_{re}}\right)\right)}{(i-1)!} + \frac{e^{-\frac{r}{P_R}\left(\frac{1}{\gamma_{rd}} + \frac{1}{\gamma_{re}}\right)}}{\left(\frac{\gamma_{re}}{\gamma_{rd}} + 1\right)^{i-1}} \right. \\ & \left. \left. \sum_{j=0}^{i-2} \frac{(-1)^j \left(\frac{r}{P_R\gamma_{re}}\right)^j \left(\frac{\gamma_{re}}{\gamma_{rd}} + 1\right)^j}{(i-1)(i-2)\ldots(i-1-j)} \right)\right] + \binom{K-1}{K-2} \sum_{r=0}^{K-1} \binom{K-1}{r} (-1)^r \frac{\gamma_{re} e^{\frac{r+1}{P_R}\left(\frac{1}{\gamma_{rd}} + \frac{1}{\gamma_{re}}\right)}}{\ln 2\gamma_{rd}} \\ & \left[- e^{-\frac{r+1}{P_R\gamma_{re}}} E_1\left(\frac{r+1}{P_R\gamma_{rd}}\right) + \sum_{i=1}^{r+1} \left(\frac{(-1)^{i+1}\left(\frac{r+1}{P_R\gamma_{re}}\right)^{i-1} E_1\left(\frac{r+1}{P_R}\left(\frac{1}{\gamma_{rd}} + \frac{1}{\gamma_{re}}\right)\right)}{(i-1)!} \right. \right. \\ & \left. \left. + \frac{e^{-\frac{r+1}{P_R}\left(\frac{1}{\gamma_{rd}} + \frac{1}{\gamma_{re}}\right)}}{\left(\frac{\gamma_{re}}{\gamma_{rd}} + 1\right)^{i-1}} \sum_{j=0}^{i-2} \frac{(-1)^j \left(\frac{r+1}{P_R\gamma_{re}}\right)^j \left(\frac{\gamma_{re}}{\gamma_{rd}} + 1\right)^j}{(i-1)(i-2)\ldots(i-1-j)} \right)\right],\end{aligned} \tag{27}$$

$$p_{12} = \int_1^{\infty} f_{Z_{r_2}}(z)(1 - F_{Z_{t_2}}(z))dz, \tag{28}$$

where

$$f_{Z_{r_2}}(z) = \sum_{r=0}^{K-1} \binom{K-1}{r} (-1)^r e^{-\frac{(z-1)r}{P_S \gamma_{sr}}} \left(\frac{-\frac{r}{P_S \gamma_{sr}}}{1+\frac{\gamma_{se} r}{\gamma_{sr}} z} - \frac{\frac{\gamma_{se} r}{\gamma_{sr}}}{\left(1+\frac{\gamma_{se} r}{\gamma_{sr}} z\right)^2} \right) + \binom{K-1}{K-2} \sum_{r=0}^{K-1} \binom{K-1}{r} (-1)^r e^{-\frac{(z-1)(r+1)}{P_S \gamma_{sr}}} \left(\frac{-\frac{r+1}{P_S \gamma_{sr}}}{1+\frac{\gamma_{se}(r+1)}{\gamma_{sr}} z} - \frac{\frac{\gamma_{se}(r+1)}{\gamma_{sr}}}{\left(1+\frac{\gamma_{se}(r+1)}{\gamma_{sr}} z\right)^2} \right), \tag{29}$$

$$F_{Z_{t_2}}(z) = \left(1 - \frac{e^{-\frac{z-1}{P_R \gamma_{rd}}}}{1+\frac{\gamma_{re} z}{\gamma_{rd}}}\right)^{K-1} \left(1 + \binom{K-1}{K-2} \frac{e^{-\frac{z-1}{P_R \gamma_{rd}}}}{1+\frac{\gamma_{re} z}{\gamma_{rd}}}\right). \tag{30}$$

Proof Please see Appendix A. □

Remark 1 Note that $\mathbb{E}[C_{SR}^{\mathrm{I}}]$ and $\mathbb{E}[C_{RD}^{\mathrm{I}}]$ can be obtained by substituting the above equations into (20) and (21). Finally, the approximate closed-form expression of the secrecy throughput for the mode I is obtained by substituting (20) and (21) into (19).

4.2.2 Mode II

The secrecy throughput for the mode II can be expressed as

$$C_{\mathrm{II}} = \min\{\mathbb{E}[C_{SR}^{\mathrm{II}}], \mathbb{E}[C_{RD}^{\mathrm{II}}]\}, \tag{31}$$

Based on (13), the average secrecy rate of the first hop for the mode II is given by

$$\mathbb{E}[C_{SR}^{\mathrm{II}}] = \mathbb{E}[C_{SR,1}], \tag{32}$$

And the average secrecy rate of the second hop for the mode II can be expressed as

$$\mathbb{E}[C_{RD}^{\mathrm{II}}] = (1-p_s)\mathbb{E}[C_{RD,1}] + p_s \mathbb{E}[C_{RD,2}], \tag{33}$$

Note that $\mathbb{E}[C_{SR}^{\mathrm{II}}]$ and $\mathbb{E}[C_{RD}^{\mathrm{II}}]$ can be obtained by substituting the Eqs. (23), (24), (26) and (27) into (32) and (33), respectively. Finally, the approximate closed-form expression of the secrecy throughput for the mode II is obtained by substituting (32) and (33) into (31).

4.2.3 Mode III

The secrecy throughput of mode III can be expressed as

$$C_{\mathrm{III}} = \min\{\mathbb{E}[C_{SR}^{\mathrm{III}}], \mathbb{E}[C_{RD}^{\mathrm{III}}]\}, \tag{34}$$

Based on (14), the average secrecy rate of the first hop for the mode III can be expressed as

$$\mathbb{E}[C_{SR}^{\mathrm{III}}] = (1-p_s)\mathbb{E}[C_{SR,1}] + p_s \mathbb{E}[C_{SR,2}], \tag{35}$$

And the average secrecy rate of the second hop for the mode III can be expressed as

$$\mathbb{E}[C_{RD}^{\mathrm{III}}] = \mathbb{E}[C_{RD,1}], \tag{36}$$

Note that $\mathbb{E}[C_{SR}^{\mathrm{III}}]$ and $\mathbb{E}[C_{RD}^{\mathrm{III}}]$ can be obtained by substituting the Eqs. (23), (24), (25) and (26) into (35) and (36) respectively. Finally, the approximate closed-form expression of the secrecy throughput for mode III is obtained by substituting (35) and (36) into (34).

It is worth noting that the values of C_{I}, C_{II}, and C_{III} only depend on the transmit power values, the total number of relays K, and the channel statistics. Therefore, given these parameters, we can compute the values of C_{I}, C_{II}, and C_{III} offline and conduct the following design on the optimal power allocation in advance.

Given the total power constraint denoted as SNR of the network, we can allocate the total power to the source and relays to achieve the best performance.

- **HyIFD**: We ought to allocate transmit energy to source and K relays. The sources work for all time slots, therefore, we should have $(P_S + KP_R) \leq \mathrm{SNR}$.
- **Max-Link-Ratio**: We are supposed to allocate transmit power to the source and K relays for each time slot to enable each link to be capable of being selected for reception or transmission, so we should have $(P_S + KP_R) \leq \mathrm{SNR}$ as well.
- **Max-Min-Ratio**: We should allocate transmit energy to the source and K relays, albeit the data transmission occupies two time slots, so we should have $\frac{1}{2}(P_S + KP_R) \leq \mathrm{SNR}$.

Consider the derived expressions of secrecy throughput. Once given the total power SNR, it is obvious that when P_S is small, the throughput is limited by first hop. On the other hand, when P_R is small, the second hop will be the bottleneck of the system. Therefore, there is always an optimal power allocation that maximizes the secrecy throughput.

Definition 1 The maximum secrecy throughput of the mode I is given by

$$C_{\mathrm{I}}^{\max} = \max_{(P_S+KP_R)\leq SNR} C_{\mathrm{I}}(P_S, P_R). \tag{37}$$

Similarly, we can define the maximum secrecy throughput for mode II and mode III, which can be denoted as $C_{\mathrm{II}}^{\max}$ and $C_{\mathrm{III}}^{\max}$, respectively. And the maximum secrecy throughput for the max-min-ratio scheme and max-link-ratio scheme can be defined in the same way.

4.3 HyIFD policy

The proposed HyIFD scheme can finally be expressed as

$$HyIFD = \arg \max_{i\in \mathrm{I,II,III}} C_i^{\max}. \tag{38}$$

That is, the HyIFD policy selects mode i which maximizes the secrecy throughput.

4.4 Asymptotic analysis

In this part, to see the performance gain more clearly, we perform the asymptotic analysis for the maximum achievable secrecy throughput of the proposed HyIFD scheme in

the high-SNR regime. Let $\widehat{C}_i^j$ denote the average secrecy rate of the i-th hop for mode j of the proposed HyIFD scheme in the high SNR regime, with $i \in \{SR, RD\}$ and $j \in \{\mathrm{I}, \mathrm{II}, \mathrm{III}\}$. We have the following result.

Theorem 1 *The maximum achievable secrecy throughput of the proposed mode I as the total power SNR increases, is upperbounded by* C_{I}^{limit}*, which is given by*

$$C_{\mathrm{I}}^{limit} = \min\{\widehat{C}_{SR}^{\mathrm{I}}, \widehat{C}_{RD}^{\mathrm{I}}\}, \tag{39}$$

$$\widehat{C}_{SR}^{\mathrm{I}} \approx (1-p_s)\widehat{C}_{SR,1} + p_s(\widehat{p}_{12}\widehat{C}_{SR,1} + \widehat{p}_{21}\widehat{C}_{SR,2}), \tag{40}$$

$$\widehat{C}_{RD}^{I} \approx (1-p_s)\widehat{C}_{RD,1} + p_s(\widehat{p}_{12}\widehat{C}_{RD,2} + \widehat{p}_{21}\widehat{C}_{RD,1}), \tag{41}$$

where

$$\widehat{C}_{SR,1} = \sum_{r=1}^{K} \binom{K}{r} (-1)^{r+1} \frac{\ln\left(1+\frac{\gamma_{sr}}{r\gamma_{se}}\right)}{\ln 2}, \tag{42}$$

$$\widehat{C}_{SR,1} = \sum_{r=1}^{K-1} \binom{K-1}{r} (-1)^{r} \frac{\ln\left(\frac{1}{1+\frac{\gamma_{sr}}{r\gamma_{se}}}\right)}{\ln 2} + \binom{K-1}{K-2} \sum_{r=0}^{K-1} \binom{K-1}{r} (-1)^{r+1} \frac{\ln\left(1+\frac{\gamma_{sr}}{(r+1)\gamma_{se}}\right)}{\ln 2}, \tag{43}$$

$$\widehat{C}_{RD,1} = \sum_{r=1}^{K} \binom{K}{r} (-1)^{r} \frac{\gamma_{re}}{\ln 2\gamma_{rd}} \left[-\ln\left(1+\frac{\gamma_{rd}}{\gamma_{re}}\right) + \sum_{i=2}^{r} \left(\frac{1}{(i-1)\left(\frac{\gamma_{re}}{\gamma_{rd}}+1\right)^{i-1}} \right) \right], \tag{44}$$

$$\begin{aligned} \widehat{C}_{RD,2} = {} & \sum_{r=1}^{K-1} \binom{K-1}{r} (-1)^{r} \frac{\gamma_{re}}{\ln 2\gamma_{rd}} \left[-\ln\left(1+\frac{\gamma_{rd}}{\gamma_{re}}\right) + \sum_{i=2}^{r} \left(\frac{1}{(i-1)\left(\frac{\gamma_{re}}{\gamma_{rd}}+1\right)^{i-1}} \right) \right] \\ & + \binom{K-1}{K-2} \sum_{r=0}^{K-1} \binom{K-1}{r} (-1)^{r} \frac{\gamma_{re}}{\ln 2\gamma_{rd}} \left[-\ln\left(1+\frac{\gamma_{rd}}{\gamma_{re}}\right) + \sum_{i=2}^{r+1} \left(\frac{1}{(i-1)\left(\frac{\gamma_{re}}{\gamma_{rd}}+1\right)^{i-1}} \right) \right], \end{aligned} \tag{45}$$

$$\widehat{p}_{12} = \int_1^{\infty} \widehat{f}_{Z_{r_2}}(z)(1-\widehat{F}_{Z_{t_2}}(z))dz, \tag{46}$$

with

$$\begin{aligned} \widehat{f}_{Z_{r_2}}(z) = {} & \sum_{r=0}^{K-1} \binom{K-1}{r} (-1)^{r} \left(-\frac{\frac{\gamma_{se} r}{\gamma_{sr}}}{\left(1+\frac{\gamma_{se} r}{\gamma_{sr}} z\right)^2} \right) \\ & + \binom{K-1}{K-2} \sum_{r=0}^{K-1} \binom{K-1}{r} (-1)^{r} \left(-\frac{\frac{\gamma_{se}(r+1)}{\gamma_{sr}}}{\left(1+\frac{\gamma_{se}(r+1)}{\gamma_{sr}} z\right)^2} \right), \end{aligned} \tag{47}$$

$$\widehat{F}_{Z_{t_2}}(z) = \left(1 - \frac{1}{1 + \frac{\gamma_{re} z}{\gamma_{rd}}}\right)^{K-1} \left(1 + \frac{\binom{K-1}{K-2}}{1 + \frac{\gamma_{re} z}{\gamma_{rd}}}\right). \tag{48}$$

Proof Please see Appendix B. □

Corollary 1 *The performance limit to the maximum achievable secrecy throughput for the mode II and mode III can be obtained by*

$$C_{\mathrm{II}}^{limit} = \min\{\widehat{C}_{SR}^{\mathrm{II}}, \widehat{C}_{RD}^{\mathrm{II}}\}, \tag{49}$$

$$C_{\mathrm{III}}^{limit} = \min\{\widehat{C}_{SR}^{\mathrm{III}}, \widehat{C}_{RD}^{\mathrm{III}}\}, \tag{50}$$

where

$$\widehat{C}_{SR}^{\mathrm{II}} = \widehat{C}_{SR,1}, \tag{51}$$

$$\widehat{C}_{RD}^{\mathrm{II}} = (1 - p_s)\widehat{C}_{RD,1} + p_s \widehat{C}_{RD,2}, \tag{52}$$

$$\widehat{C}_{SR}^{\mathrm{III}} = (1 - p_s)\widehat{C}_{SR,1} + p_s \widehat{C}_{SR,2}, \tag{53}$$

$$\widehat{C}_{RD}^{\mathrm{III}} = \widehat{C}_{RD,1}, \tag{54}$$

Note that $\widehat{C}_{SR}^{\mathrm{II}}$ *and* $\widehat{C}_{RD}^{\mathrm{II}}$ *can be obtained by substituting the Eqs.* (23), (42), (44) *and* (45) *into* (51) *and* (52), *respectively. Then the asymptotic closed-form expression for the maximum achievable secrecy throughput limit of mode II is obtained by substituting* (51) *and* (52) *into* (49). *And* C_{III}^{limit} *can be obtained in a similar way.*

Proof The proof is similar to that for mode I and hence is omitted here.

Finally, the closed-form expressions for the limit to the maximum achievable secrecy throughput of the proposed HyIFD scheme, which is denoted as C_{HyIFD}^{limit}, can be obtained by

$$C_{HyIFD}^{limit} = \max\{C_{\mathrm{I}}^{limit}, C_{\mathrm{II}}^{limit}, C_{\mathrm{III}}^{limit}\}. \tag{55}$$

□

It can be seen from the above formula that when the transmit power is relatively large, the secrecy throughput no longer increases with the transmit power, but only depends on the number of available relays and channel statistics. This is easy to

understand because the increase in the transmit power is beneficial not only to the legitimate receiver but also to the eavesdropper, and the secrecy throughput is limited mainly by the difference in channel quality between the legitimate channels and eavesdropper channels. It is worth noting that the designed HyIFD policy takes into account both acquiring a larger channel gain ratio and balancing the gain of the two hops by switching between the three modes according to different conditions such as transmit power and channel statistics, thus can be seen as a more flexible and comprehensive scheme for such a system.

5 The proposed methods for fixed-rate transmissions

In this section, we first propose a novel link selection policy for FRT and analyze its performance in terms of secrecy outage probability (SOP). Subsequently, a sub-optimal TBLS scheme with lower computational complexity is provided as well.

5.1 Link selection policy

In FRT, the source and relays transmit with a constant rate R_s, and the relevant performance metric is the outage probability P_{out}. As another the most commonly used security measure for wiretap channels, SOP provides an idea about the fraction of fading realizations for which the channel can support a certain rate (or user's desired rate). Aiming at improving the SOP performance for FRT, we propose a TBLS scheme where two non-negative scalars λ and μ are introduced to determine the threshold for choosing when the relay listens or transmits. The conditions are used to assess the quality of both the $S-R$ link and the $R-D$ link in order to provide good SOP performance.

In the proposed TBLS scheme, the relays selected for reception $R_{\bar{r}}$ and transmission $R_{\bar{t}}$ are chosen as

$$(R_{\bar{r}}, R_{\bar{t}}) = \begin{cases} (R_{r_1}, R_{t_1}), \text{if } z_{r_1} \geq \lambda \text{ and } z_{t_1} \geq \mu \text{ and } r_1 \neq t_1 \\ (R_{r_1}, R_{t_2}), \text{if } z_{r_1} \geq \lambda \text{ and } z_{t_2} \geq \mu \text{ and } r_1 = t_1 \\ (R_{r_1}, 0), \text{if } z_{r_1} \geq \lambda \text{ and } z_{t_1} \geq \mu > z_{t_2} \text{ and } r_1 = t_1 \text{ or if } z_{r_1} \geq \lambda \text{ and } z_{t_1} < \mu \\ (0, R_{t_1}), \text{if } z_{r_1} < \lambda \text{ and } z_{t_1} \geq \mu \\ (0, 0), \text{otherwise,} \end{cases} \tag{56}$$

where z_{r_1}, z_{t_1}, and z_{t_2} have been defined in (7), (9), and (10), respectively. Obviously, this scheme is a hybrid HD/FD relaying scheme, which adapts reception and transmission time slots based on channel quality. Under the premise of ensuring transmission quality, the proposed TBLS scheme selects two relays for reception and transmission respectively if possible, which considers both the transmission efficiency and security.

5.2 Secrecy outage probability analysis

In this part, we perform the SOP analysis for the proposed TBLS scheme. The SOP is defined as the probability that the instantaneous secrecy capacity falls below a target secrecy rate R_s, i.e., the equivalent instantaneous z falls below a certain threshold z_{th} such that error-free transmission with rate R_s is not possible [41], i.e., $P_{out} = P(z \leq z_{th})$.

Proposition 3 *The SOP for the proposed TBLS scheme can be expressed as*

$$\begin{aligned} P_{out} = {} & (1-p_s)P\{\min\{z_{r_1}, z_{t_1}\} < z_{th_1}, z_{r_1} \geq \lambda, z_{t_1} \geq \mu\} \\ & + p_s P\{\min\{z_{r_1}, z_{t_2}\} < z_{th_1}, z_{r_1} \geq \lambda, z_{t_2} \geq \mu\} \\ & + p_s P\{z_{r_1} < z_{th_2}, z_{r_1} \geq \lambda, z_{t_1} \geq \mu > z_{t_2}\} + P\{z_{r_1} < z_{th_2}, z_{r_1} \geq \lambda, z_{t_1} < \mu\} \\ & + P\{z_{t_1} < z_{th_2}, z_{r_1} < \lambda, z_{t_1} \geq \mu\} + P\{z_{r_1} < \lambda, z_{t_1} < \mu\}, \end{aligned} \tag{57}$$

where $z_{th_1} = 2^{R_s}$ *and* $z_{th_2} = 2^{2R_s}$.

Proof Please see Appendix C. □

Note that when $\lambda = \mu = z_{th_2}$, the proposed scheme only fails to transmit data when both z_{r_1} and z_{t_1} are less than z_{th_2}. This scheme reduces to a scheme similar to max-link-ratio selection scheme, the secrecy outage performance is the same, i.e., $P_{out} = P\{z_{r_1} < z_{th_2}, z_{t_1} < z_{th_2}\} = P\{\max\{z_{r_1}, z_{t_1}\} < z_{th_2}\}$, but with one difference that, the max-link-ratio selection scheme only selects one link for one time slot while the proposed TBLS scheme selects two if possible, i.e., the transmission probabilities of the first and the second hop of TBLS are definitely higher than that of the max-link-ratio scheme, so is the throughput.

Proposition 4 *Given the policy, i.e.,* λ *and* μ*, the closed-form expressions for the SOP of the proposed TBLS scheme is given by*

$$
P_{out} = \begin{cases}
F_{Z_{r_1}}(\lambda)F_{Z_{t_1}}(\mu), & \lambda \geq z_{th_2} \ \& \ \mu \geq z_{th_2}; \\
F_{Z_{r_1}}(\lambda)F_{Z_{t_1}}(z_{th_2}), & \lambda \geq z_{th_2} \ \& \ z_{th_1} \leq \mu < z_{th_2}; \\
(1-F_{Z_{r_1}}(\lambda))[(1-p_s)(F_{Z_{t_1}}(z_{th_1})-F_{Z_{t_1}}(\mu)) & \\
\quad +p_s(F_{Z_{t_2}}(z_{th_1})-F_{Z_{t_2}}(\mu))]+F_{Z_{r_1}}(\lambda)F_{Z_{t_1}}(z_{th_2}), & \lambda \geq z_{th_2} \ \& \ \mu < z_{th_1}; \\
F_{Z_{t_1}}(\mu)F_{Z_{r_1}}(z_{th_2})+p_s(F_{Z_{r_1}}(z_{th_2}) & \\
\quad -F_{Z_{r_1}}(\lambda))(F_{Z_{t_2}}(\mu)-F_{Z_{t_1}}(\mu)), & z_{th_1} \leq \lambda < z_{th_2} \ \& \ \mu \geq z_{th_2}; \\
F_{Z_{t_1}}(\mu)(F_{Z_{r_1}}(z_{th_2})-F_{Z_{r_1}}(\lambda))+F_{Z_{r_1}}(\lambda)F_{Z_{t_1}}(z_{th_2}) & \\
\quad +p_s(F_{Z_{r_1}}(z_{th_2})-F_{Z_{r_1}}(\lambda))(F_{Z_{t_2}}(\mu)-F_{Z_{t_1}}(\mu)), & z_{th_1} \leq \lambda < z_{th_2} \ \& \ z_{th_1} \leq \mu < z_{th_2}; \\
(1-F_{Z_{r_1}}(\lambda))[(1-p_s)(F_{Z_{t_1}}(z_{th_1})-F_{Z_{t_1}}(\mu)) & \\
\quad +p_s(F_{Z_{t_2}}(z_{th_1})-F_{Z_{t_2}}(\mu))]+F_{Z_{t_1}}(\mu) & \\
\quad (F_{Z_{r_1}}(z_{th_2})-F_{Z_{r_1}}(\lambda))+F_{Z_{r_1}}(\lambda)F_{Z_{t_1}}(z_{th_2}) & \\
\quad +p_s(F_{Z_{r_1}}(z_{th_2})-F_{Z_{r_1}}(\lambda))(F_{Z_{t_2}}(\mu)-F_{Z_{t_1}}(\mu)), & z_{th_1} \leq \lambda < z_{th_2} \ \& \ \mu < z_{th_1}; \\
(F_{Z_{r_1}}(z_{th_1})-F_{Z_{r_1}}(\lambda))[(1-p_s) & \\
\quad (1-F_{Z_{t_1}}(\mu))+p_s(1-F_{Z_{t_2}}(\mu))] & \\
\quad +F_{Z_{t_1}}(\mu)F_{Z_{r_1}}(z_{th_2})+p_s(F_{Z_{r_1}}(z_{th_2}) & \\
\quad -F_{Z_{r_1}}(\lambda))(F_{Z_{t_2}}(\mu)-F_{Z_{t_1}}(\mu)), & \lambda < z_{th_1} \ \& \ \mu \geq z_{th_2}; \\
(F_{Z_{r_1}}(z_{th_1})-F_{Z_{r_1}}(\lambda))[(1-p_s) & \\
\quad (1-F_{Z_{t_1}}(\mu))+p_s(1-F_{Z_{t_2}}(\mu))]+F_{Z_{t_1}}(\mu) & \\
\quad (F_{Z_{r_1}}(z_{th_2})-F_{Z_{r_1}}(\lambda))+F_{Z_{r_1}}(\lambda)F_{Z_{t_1}}(z_{th_2}) & \\
\quad +p_s(F_{Z_{r_1}}(z_{th_2})-F_{Z_{r_1}}(\lambda))(F_{Z_{t_2}}(\mu)-F_{Z_{t_1}}(\mu)), & \lambda < z_{th_1} \ \& \ z_{th_1} \leq \mu < z_{th_2}; \\
(1-p_s)[(1-F_{Z_{r_1}}(\lambda))(1-F_{Z_{t_1}}(\mu))-(1-F_{Z_{r_1}}(z_{th_1})) & \\
\quad (1-F_{Z_{t_1}}(z_{th_1}))]+p_s[(1-F_{Z_{r_1}}(\lambda))(1-F_{Z_{t_2}}(\mu)) & \\
\quad -(1-F_{Z_{r_1}}(z_{th_1}))(1-F_{Z_{t_2}}(z_{th_1}))]+F_{Z_{t_1}}(\mu) & \\
\quad (F_{Z_{r_1}}(z_{th_2})-F_{Z_{r_1}}(\lambda))+F_{Z_{r_1}}(\lambda)F_{Z_{t_1}}(z_{th_2}) & \\
\quad +p_s(F_{Z_{r_1}}(z_{th_2})-F_{Z_{r_1}}(\lambda))(F_{Z_{t_2}}(\mu)-F_{Z_{t_1}}(\mu)), & \text{otherwise.}
\end{cases} \tag{58}
$$

where

$$
F_{Z_{r_1}}(z) = \sum_{r=0}^{K} \binom{K}{r} (-1)^r \cdot \frac{e^{-\frac{(z-1)r}{P_S \gamma_{sr}}}}{\frac{zr\gamma_{se}}{\gamma_{sr}}+1}, \tag{59}
$$

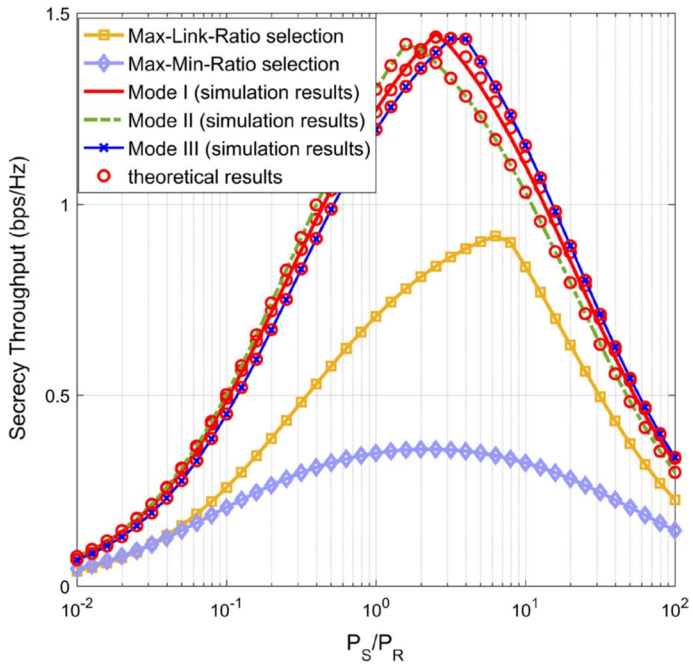

Fig. 2 The secrecy throughput versus P_S/P_R for different relaying protocols

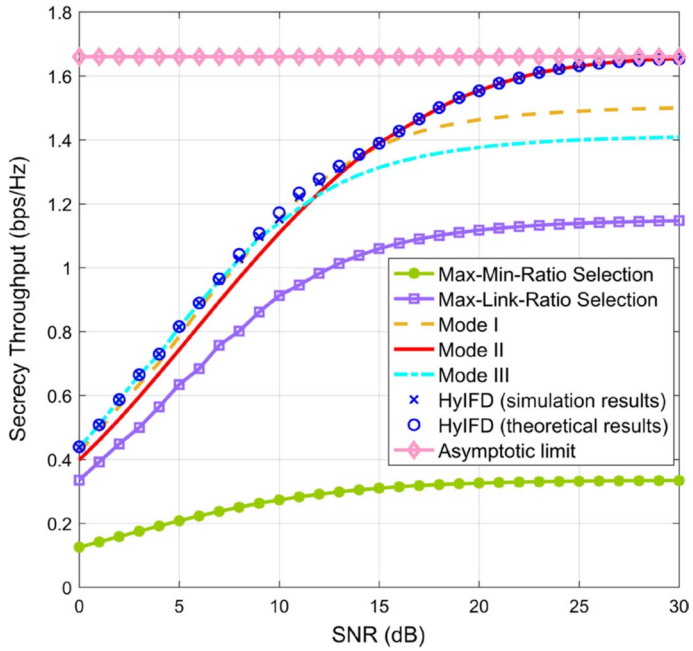

Fig. 3 The maximum secrecy throughput versus SNR for different relaying protocols

$$F_{Z_{t_1}}(z) = \left(1 - \frac{e^{-\frac{z-1}{P_R \gamma_{rd}}}}{1 + \frac{z\gamma_{re}}{\gamma_{rd}}}\right)^K, \tag{60}$$

$$F_{Z_{t_2}}(z) = \left(1 - \frac{e^{-\frac{z-1}{P_R \gamma_{rd}}}}{1 + \frac{\gamma_{re} z}{\gamma_{rd}}}\right)^{K-1} \left(1 + \binom{K-1}{K-2} \frac{e^{-\frac{z-1}{P_R \gamma_{rd}}}}{1 + \frac{\gamma_{re} z}{\gamma_{rd}}}\right). \tag{61}$$

Proof Please see Appendix D. □

There is always an optimal pair of λ and μ that minimize the SOP. That makes sense because as λ and μ increase, the requirement for the quality of the transmission link is higher, and correspondingly, the outage probability of the transmission is reduced, while the probability of choosing not to transmit due to the higher transmission requirement, which is also counted as outage, is increased. So there is a tradeoff between a reduced outage probability of the transmission and an increased outage probability of no transmission due to unmet requirements, which is also confirmed in the later simulation.

It is worth noting that the values of SOP for the proposed TBLS scheme only depend on the transmit power values, the total number of relays K, the target secrecy rate R_s and the channel statistics, as is shown in (58). Therefore, given these parameters, we can compute the values of SOP for the proposed TBLS scheme offline and search for the optimal pair of λ and μ in advance.

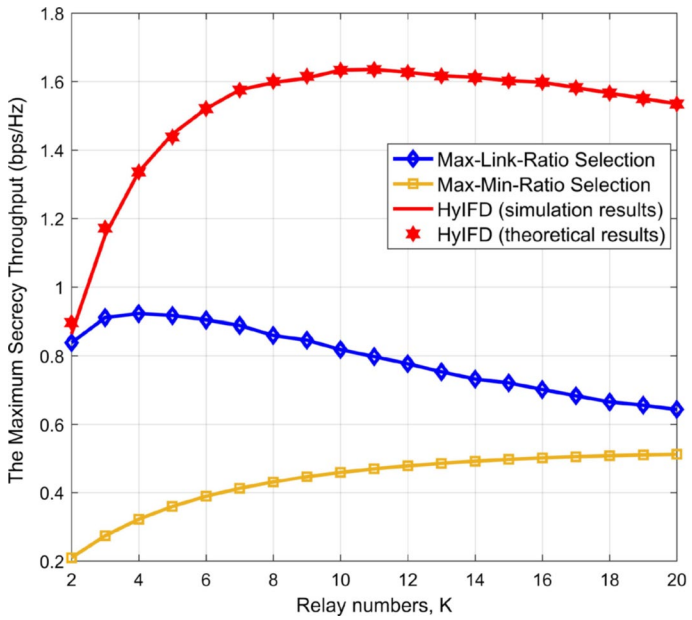

Fig. 4 The maximum secrecy throughput versus number of relays for different relaying protocols

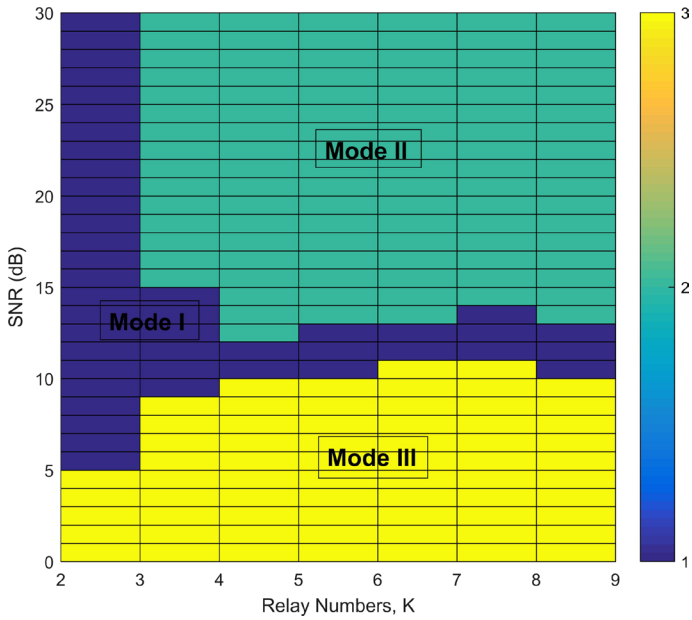

Fig. 5 The mode switch of the proposed HyIFD scheme as the SNR and relay numbers change

5.3 A sub-optimal TBLS scheme

Considering that the search for the optimal pair of λ and μ may bring extra computational complexity in implementation, we try to give the optimal values of λ and μ from the perspective of theoretical analysis. It is however very tricky to find the minimum for such a complex nine-segment piecewise function whose stationary points are very hard to express.

So we consider a sub-optimal TBLS (SO-TBLS) scheme, we set $\lambda = \mu = z_{th_1}$ in the TBLS scheme proposed in the previous section.

The SOP of the proposed sub-optimal TBLS scheme is given by

$$P_{out} = \sum_{r=0}^{K} \binom{K}{r} (-1)^r \left(\frac{e^{-\frac{(z_{th_2}-1)r}{P_S \gamma_{sr}}}}{\frac{z_{th_2} r \gamma_{se}}{\gamma_{sr}} + 1} - \frac{e^{-\frac{(z_{th_1}-1)r}{P_S \gamma_{sr}}}}{\frac{z_{th_1} r \gamma_{se}}{\gamma_{sr}} + 1} \right) \times \left(p_s \left(1 - \frac{e^{-\frac{z_{th_1}-1}{P_R \gamma_{rd}}}}{1 + \frac{\gamma_{re} z_{th_1}}{\gamma_{rd}}} \right)^{K-1} \left(1 + \binom{K-1}{K-2} \frac{e^{-\frac{z_{th_1}-1}{P_R \gamma_{rd}}}}{1 + \frac{\gamma_{re} z_{th_1}}{\gamma_{rd}}} \right) + (1 - p_s) \left(1 - \frac{e^{-\frac{z_{th_1}-1}{P_R \gamma_{rd}}}}{1 + \frac{z_{th_1} \gamma_{re}}{\gamma_{rd}}} \right)^{K} \right) + \left(1 - \frac{e^{-\frac{z_{th_2}-1}{P_R \gamma_{rd}}}}{1 + \frac{z_{th_2} \gamma_{re}}{\gamma_{rd}}} \right)^{K} \times \sum_{r=0}^{K} \binom{K}{r} (-1)^r \frac{e^{-\frac{(z_{th_1}-1)r}{P_S \gamma_{sr}}}}{\frac{z_{th_1} r \gamma_{se}}{\gamma_{sr}} + 1}, \tag{62}$$

which can be obtained directly by the substituting $\lambda = \mu = z_{th_1}$ into (58).

6 Results and discussion

In this section, we evaluate the proposed HyIFD scheme and TBLS scheme respectively.

6.1 The HyIFD performance

In this part, simulation results are given to verify the closed-form secrecy throughput for the proposed HyIFD scheme. We assume that $\gamma_{sr} = \gamma_{rd} = \gamma_{se} = \gamma_{re} = 2$, unless specified otherwise.

Figure 2 plots the secrecy throughput versus P_S/P_R of each scheme, where the relay number is set as $K = 5$. We assume SNR = 10 dB. We can find that the secrecy throughput always has a peak value as P_S/P_R varies, and the proposed HyIFD scheme will work

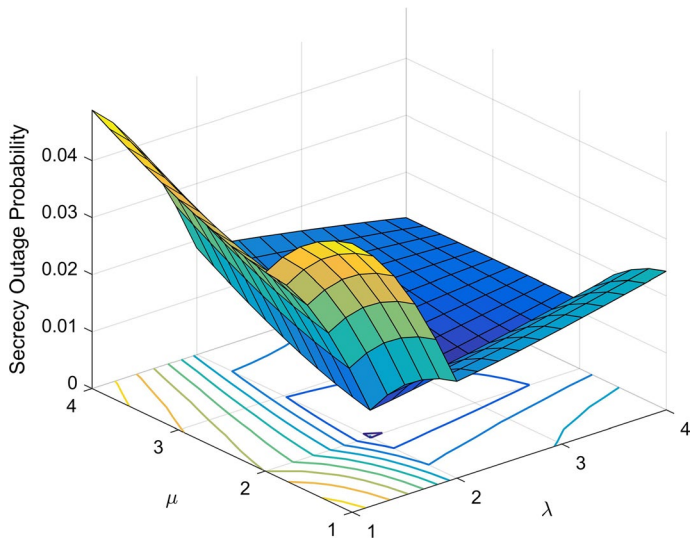

Fig. 6 The secrecy outage probability versus λ and μ for the proposed scheme

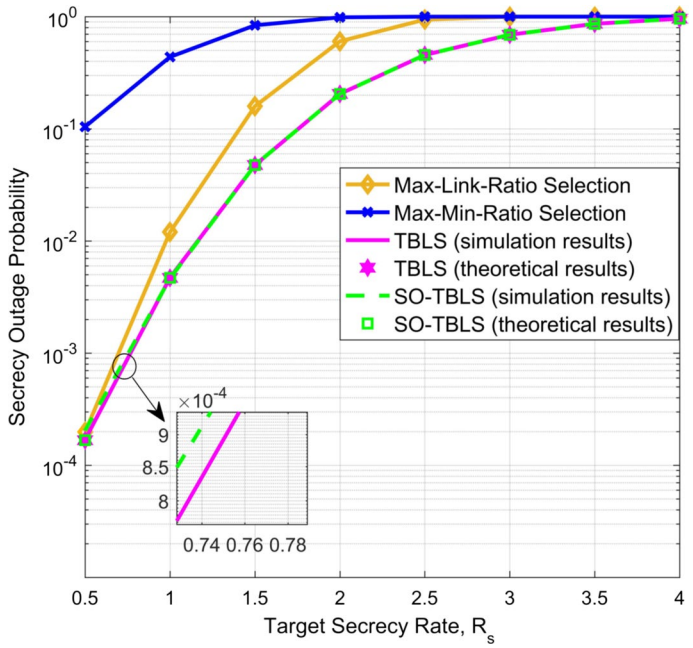

Fig. 7 The secrecy outage probability versus the target secrecy rate for different relaying protocols

in mode I for the given setting, which achieves the largest maximum secrecy throughput. It is interesting that, each scheme does not achieve the maximum secrecy throughput when $\frac{P_S}{P_R} = 1$, i.e., $P_S = P_R$, which would be the case for throughput maximization with symmetric channel conditions [33]. This is because, the equivalent channel distributions for the two hops is not symmetric even if the channel statistics for the links are the same, which can also be seen from (7)–(10). We also note that the analytical results obtained based on the derivation in Section III match the simulation results, which verifies the approximate closed-form secrecy throughput obtained in this paper.

In Fig. 3, we compare the maximum secrecy throughput of the proposed scheme with that of two existing max-ratio schemes as SNR varies, where the relay number is set as $K = 3$. It is clearly shown that the proposed HyIFD scheme switches between the three modes to achieve the best performance with power allocation. The approximate expression holds for a wide range of SNR values. Also, we can find that the secrecy throughput improvement diminishes in the high-SNR regime, i.e., there is a performance limit to throughput as the transmit power increases, in consistence with the closed-form expression derived in Section III-D.

Figure 4 plots the maximum secrecy throughput of each scheme versus the number of relays for SNR = 10 dB. We can find that the proposed HyIFD scheme achieves the best performance in all cases. It is interesting that for a given SNR, the proposed scheme achieves the best performance at a mediate number of relays, and the max-link-ratio scheme achieves the best performance when $K = 4$. This is generally due to the trade-off between the reduction in the power allocated to source and relays and the increased probability of choosing better channel as K increases considering the total power constraint.

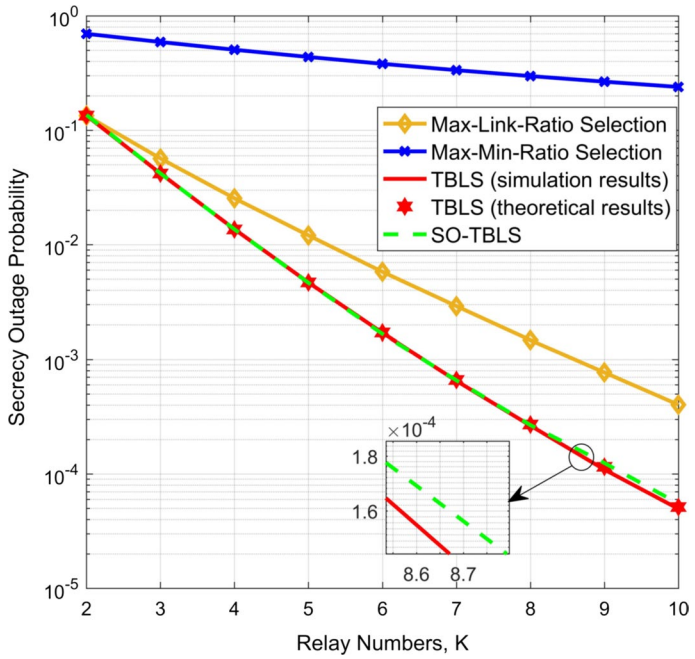

Fig. 8 The secrecy outage probability versus number of relays for different relaying protocols

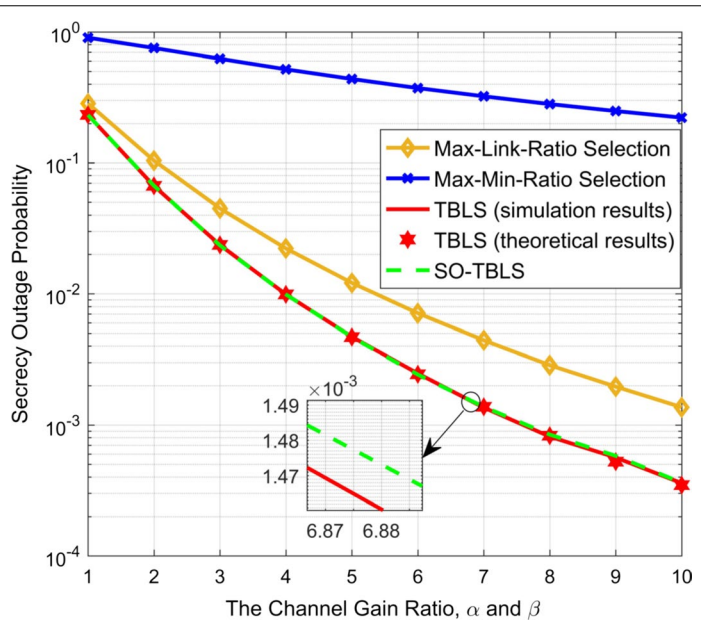

Fig. 9 The secrecy outage probability versus the channel gain ratio for different relaying protocols

Figure 5 shows how the proposed HyIFD scheme switches between the three modes as the SNR and the number of relays change. We can find that mode II is more preferred in the high-SNR regime and mode III is more preferred in the low-SNR regime, i.e., the relay with the best channel quality for the first-hop is preferred in the high-SNR regime while the relay with the best channel quality in the second-hop is always favored in the

low-SNR regime to achieve better throughput performance. This is because, for the high-SNR regime, the secrecy throughput depends mainly on the channel gain and the throughput is limited by the first hop considering (7)–(10), so the better throughput performance can be obtained by prioritizing the first hop. On the contrary, for the low-SNR regime, the secrecy throughput is mainly affected by the transmit power, more power ought to be allocated to the source than the transmitting relay to better utilize the total power, which means the second hop will be the bottleneck of the system, so the selection policy that be in favor of the second hop will get better throughput performance.

6.2 The TBLS performance

In this part, simulation results are given to verify the closed-form secrecy outage probability for the proposed TBLS scheme. The transmission powers are normalized to unity, i.e., $P_S = P_R = 1$. We set the average channel gains of the source-relay and relay-destination links as $\gamma_{sr} = \gamma_{rd} = 10$dB. We set the channel gain ratio α and β as $\alpha = \beta = 5$ and the average eavesdropping channel gains as $\gamma_{se} = \frac{\gamma_{sr}}{\alpha}$ and $\gamma_{re} = \frac{\gamma_{rd}}{\beta}$, unless specified otherwise.

In Fig. 6, we plot the secrecy outage probability of the proposed TBLS scheme versus λ and μ. We assume that the target secrecy rate $R_s = 1$ and the relay number is set as $K = 5$. We can find that it has different functional relationship with these two parameters in different regions, and the secrecy throughput always has a valley value as λ and μ varies, i.e., we can optimize these two parameters to achieve the best secrecy outage performance, which verifies our previous analysis. We also add the contour for this figure, and we can see that the two parameters do not have exactly the same effect on the secrecy outage probability. Note that the contour goes through the point $\lambda = \mu = 2$, which means $\lambda = \mu = z_{th_1}$ is not the optimal choice.

In Fig. 7, we plots the secrecy outage probability for each scheme as the target secrecy rate varies, where the relay number is set as $K = 5$. We can find that the proposed scheme performs better than two existing max-ratio relay selection schemes in terms of secrecy outage probability. The theoretical and simulation results are shown to essentially perfectly match, which verifies the closed-form secrecy outage probability obtained in this paper. We can also see that the performance of SO-TBLS is very close to that of TBLS, which indicates that SO-TBLS can be a good alternative to TBLS without searching for the optimal λ and μ. Note that we search for λ and μ within an interval with a step size of 0.2 in simulation, and we believe that if the search accuracy is improved, so is the secrecy outage performance of the proposed TBLS scheme.

Figure 8 plots the secrecy outage probability of each scheme versus the number of relays for $R_s = 1$. It is clearly shown that the increase in the relay number can significantly improve the secrecy outage performance and the proposed TBLS scheme achieves the best performance, which agree with the theoretical analysis. We can see that SO-TBLS performs almost as well as TBLS with the given parameters.

Figure 9 plots the secrecy outage probability of each scheme versus the channel gain ratio, which reflects the change in the intensity of the main channel. We assume $\alpha = \beta$. The relay number is set as $K = 5$ and the target secrecy rate is set as $R_s = 1$. It is obvious that the

secrecy outage probability decreases as the main channel becomes stronger and the proposed TBLS scheme achieves best performance.

7 Conclusion

In this paper, we studied the relay selection schemes for secure buffer-aided cooperative relay networks. We first proposed a HyIFD policy that switches between these three sub-strategies according to the different conditions to improve the secrecy throughput performance for ART transmissions. With the help of buffers at the relays, different relays for reception and transmission were selected with the largest or the second largest ratio among $S-R$ and $R-D$ links respectively, to simultaneously receive and transmit. Then, we proposed a hybrid HD/FD transmission scheme named TBLS protocol aiming at improving the secrecy outage performance for FRT transmissions. We introduced and optimized two selection parameters to ensure the transmission quality of both two hops. We also considered a SO-TBLS scheme as a good alternative to TBLS with lower requirements for computational complexity. We considered the RF strategy such that the eavesdropper can only independently decode the signals received in the two hops. Both the closed-form expressions for the secrecy throughput of the proposed HyIFD scheme and that for the secrecy outage probability of the proposed TBLS scheme were derived. The Numerical results in consistence with the analytical expressions demonstrated the performance superiority of the proposed schemes in secrecy throughput and secrecy outage probability compared with the benchmark schemes.

Appendix

Proof of Proposition 2

The probability that the best $S-R$ and the best $R-D$ channels share the same relay is $p_s = \frac{1}{K}$ [33], it follows directly from the fact that the channels for both $S-R$ and $R-D$ links are i.i.d. And it is obvious that we have $p_{21} = 1 - p_{12}$. So, to compute the secrecy throughput of the proposed HyIFD scheme, we need to find $\mathbb{E}[C_{SR,1}]$, $\mathbb{E}[C_{RD,1}]$, $\mathbb{E}[C_{SR,2}]$, $\mathbb{E}[C_{RD,2}]$ and p_{12}.

a) *Computation of* $\mathbb{E}[C_{SR,1}]$: In this case, we denote $z_{r_1} = \frac{1+P_S x}{1+P_S y}$, where $x = \max\{x_k\}$ with $x_k = |h_{sr_k}|^2, k \in \{1, 2, \ldots, K\}$, and $y = |h_{se}|^2$. Therefore, to derive $\mathbb{E}[C_{SR,1}]$, we need to compute the cumulative distribution function (CDF) of z_{r_1}. We first compute the CDF of x, the CDF of x can be obtained as

$$\begin{aligned} F_X(x) &= P\{\max\{x_k\} \le x\} = P\{x_1 \le x\}P\{x_2 \le x\}\ldots P\{x_K \le x\} \\ &= \left(1 - e^{-\frac{x}{\gamma_{sr}}}\right)^K. \end{aligned} \tag{63}$$

Since x is independent of y, we have $f_{XY}(x,y) = f_X(x)f_Y(y)$. Then the CDF of z_{r_1} can be calculated as

$$
\begin{aligned}
F_{Z_{r_1}}(z) &= P\left\{\frac{1+P_S X}{1+P_S Y} \le z\right\} = \int_0^{\infty} f_Y(y)\cdot F_X(x)\big|_0^{\frac{z}{P_S}+yz-\frac{1}{P_S}} dy \\
&= \sum_{r=0}^{K}\binom{K}{r}(-1)^r \cdot \frac{e^{-\frac{(z-1)r}{P_S\gamma_{sr}}}}{\frac{zr\gamma_{se}}{\gamma_{sr}}+1}.
\end{aligned} \tag{64}
$$

Then, we have

$$
\begin{aligned}
\mathbb{E}[C_{SR,1}] &= \int_1^{\infty} \log_2 z f_{Z_{r_1}}(z)dz \\
&= \int_1^{\infty} \log_2 z d\Big(F_{Z_{r_1}}(z)-1\Big) = \int_1^{\infty} \frac{\Big(1-F_{Z_{r_1}}(z)\Big)}{z\ln 2}dz \\
&= \log_2 z\Big(F_{Z_{r_1}}(z)-1\Big)\big|_1^{\infty} - \int_1^{\infty}\Big(F_{Z_{r_1}}(z)-1\Big)d(\log_2 z) \\
&= \int_1^{\infty} -\sum_{r=1}^{K}\binom{K}{r}(-1)^r \frac{e^{-\frac{(z-1)r}{P_S\gamma_{sr}}}}{\ln 2\Big(1+\frac{\gamma_{se}}{\gamma_{sr}}zr\Big)z}dz \\
&= -\sum_{r=1}^{K}\binom{K}{r}(-1)^r \frac{e^{\frac{r}{P_S\gamma_{sr}}}}{\ln 2}\int_1^{\infty}\left(\frac{e^{-\frac{zr}{P_S\gamma_{sr}}}}{z} - \frac{e^{-\frac{zr}{P_S\gamma_{sr}}}}{z+\frac{\gamma_{sr}}{\gamma_{se}r}}\right)dz \\
&= \sum_{r=1}^{K}\binom{K}{r}(-1)^r \frac{e^{\frac{r}{P_S\gamma_{sr}}}}{\ln 2}\times\Bigg[-E_1\left(\frac{r}{P_S\gamma_{sr}}\right) \\
&\quad + e^{\frac{1}{P_S\gamma_{se}}}E_1\left(\frac{r}{P_S\gamma_{sr}}+\frac{1}{P_S\gamma_{se}}\right)\Bigg],
\end{aligned} \tag{65}
$$

where $E_1(x) = \int_x^{\infty}(e^{-t}/t)dt, x > 0$ is the exponential integral function.

b) *Computation of* $\mathbb{E}[C_{RD,1}]$: In this case, we denote $z_{t_1} = \max\limits_{k\in\{1,2,\ldots,K\}}\{z_k\}$, where $z_k = \frac{1+P_R x_k}{1+P_R y_k}$ with $x_k = |h_{r_k d}|^2$ and $y_k = |h_{r_k e}|^2$. Since x_k is independent of y_k, we have $f_{X_k Y_k}(x_k, y_k) = f_{X_k}(x_k)f_{Y_k}(y_k)$. We first compute the CDF of z_k, the CDF of z_k can be obtained as

$$
\begin{aligned}
F_{Z_k}(z_k) &= P\left\{\frac{1+P_R X_k}{1+P_R Y_k} \le z_k\right\} \\
&= \int_0^{\infty}\int_0^{\frac{z_k}{P_R}+y_k z_k-\frac{1}{P_R}} f_{X_k Y_k}(x_k, y_k)dx_k dy_k \\
&= \int_0^{\infty}\left[-\frac{1}{\gamma_{re}}e^{-\frac{z_k-1}{\gamma_{rd}P_R}}e^{\left(-\frac{1}{\gamma_{re}}-\frac{z_k}{\gamma_{rd}}\right)y_k} + \frac{1}{\gamma_{re}}e^{-\frac{y_k}{\gamma_{re}}}\right]dy_k \\
&= \left[\frac{e^{-\frac{z_k-1}{\gamma_{rd}P_R}}}{1+\frac{z_k\gamma_{re}}{\gamma_{rd}}}\cdot e^{\left(-\frac{1}{\gamma_{re}}-\frac{z_k}{\gamma_{rd}}\right)y_k} - e^{-\frac{y_k}{\gamma_{re}}}\right]\Bigg|_0^{\infty} \\
&= 1 - \frac{e^{-\frac{z_k-1}{\gamma_{rd}P_R}}}{1+\frac{z_k\gamma_{re}}{\gamma_{rd}}}.
\end{aligned} \tag{66}
$$

Then the CDF of z_{t_1} can be calculated as

$$
\begin{aligned}
F_{Z_{t_1}}(z) &= P\{Z_{t_1} \le z\} = P\{\max\{Z_k\} \le z\} \\
&= P\{Z_1 \le z\}\{Z_2 \le z\} \ldots \{Z_K \le z\} \\
&= \left(1 - \frac{e^{-\frac{z-1}{P_R\gamma_{rd}}}}{1 + \frac{z\gamma_{re}}{\gamma_{rd}}}\right)^K .
\end{aligned} \tag{67}
$$

After computation of $F_{Z_{t_1}}(z)$ and after some simplifications, $\mathbb{E}[C_{RD,1}]$ can be obtained as

$$
\begin{aligned}
\mathbb{E}[C_{RD,1}] &= \int_1^\infty \log_2 z f_{Z_{t_1}}(z)dz = \int_1^\infty \log_2 z d\left(F_{Z_{t_1}}(z) - 1\right) \\
&= \log_2 z\left(F_{Z_{t_1}}(z) - 1\right)\Big|_1^\infty - \int_1^\infty \left(F_{Z_{t_1}}(z) - 1\right) d(\log_2 z) \\
&= -\sum_{r=1}^{K} \binom{K}{r} (-1)^r \frac{e^{\frac{r}{P_R\gamma_{rd}}}}{\ln 2} \int_1^\infty \frac{e^{-\frac{zr}{P_R\gamma_{rd}}}}{z\left(1 + \frac{\gamma_{re}}{\gamma_{rd}} z\right)^r} dz \\
&\overset{u=1+\frac{\gamma_{re}}{\gamma_{rd}}z}{=\!=\!=} -\sum_{r=1}^{K} \binom{K}{r} (-1)^r \frac{e^{\frac{r}{P_R\gamma_{rd}}}}{\ln 2} \int_{\frac{\gamma_{re}}{\gamma_{rd}}+1}^\infty \frac{e^{-\frac{r(u-1)}{P_R\gamma_{re}}}}{\frac{\gamma_{rd}}{\gamma_{re}}(u-1)u^r} du \\
&= -\sum_{r=1}^{K} \binom{K}{r} (-1)^r \frac{e^{\left(\frac{r}{P_R\gamma_{rd}} + \frac{r}{P_R\gamma_{re}}\right)}}{\ln 2 \frac{\gamma_{rd}}{\gamma_{re}}} \int_{\frac{\gamma_{re}}{\gamma_{rd}}+1}^\infty \left(\frac{e^{-\frac{r}{P_R\gamma_{re}}u}}{u-1} - \sum_{i=1}^{r} \frac{e^{-\frac{r}{P_R\gamma_{re}}u}}{u^i}\right) du \\
&= \sum_{r=1}^{K} \binom{K}{r} (-1)^r \frac{\gamma_{re} e^{\frac{r}{P_R}\left(\frac{1}{\gamma_{rd}} + \frac{1}{\gamma_{re}}\right)}}{\ln 2 \gamma_{rd}} \Bigg[-e^{-\frac{r}{P_R\gamma_{re}}} E_1\left(\frac{r}{P_R\gamma_{rd}}\right) \\
&\quad + \sum_{i=1}^{r} \Bigg(\frac{(-1)^{i+1}\left(\frac{r}{P_R\gamma_{re}}\right)^{i-1} E_1\left(\frac{r}{P_R}\left(\frac{1}{\gamma_{rd}} + \frac{1}{\gamma_{re}}\right)\right)}{(i-1)!} \\
&\quad + \frac{e^{-\frac{r}{P_R}\left(\frac{1}{\gamma_{rd}} + \frac{1}{\gamma_{re}}\right)}}{\left(\frac{\gamma_{re}}{\gamma_{rd}} + 1\right)^{i-1}} \sum_{j=0}^{i-2} \frac{(-1)^j \left(\frac{r}{P_R\gamma_{re}}\right)^j \left(\frac{\gamma_{re}}{\gamma_{rd}} + 1\right)^j}{(i-1)(i-2)\ldots(i-1-j)} \Bigg) \Bigg].
\end{aligned} \tag{68}
$$

c) *Computation of* $\mathbb{E}[C_{SR,2}]$ and $\mathbb{E}[C_{RD,2}]$: To compute $\mathbb{E}[C_{SR,2}]$ and $\mathbb{E}[C_{RD,2}]$, we need to compute the CDF of z_{r_2} and z_{t_2}, so we consider the following theory of order statistics [40]:

Let $Z_1, \ldots, Z_n$ be n independent variates, each with cdf $F(z)$. Let $Z_1, \ldots, Z_n$ denote the increasing order of $Z_1, \ldots, Z_n$, i.e., $Z_{(1)} \le Z_{(2)} \le Z_{(n)}$. Let $F_{(r)}(z), (r = 1, \ldots, n)$ denote the cdf of the r th order statistic $Z_{(r)}$. Then the cdf of $Z_{(r)}$ is given by

$$
F_{(r)}(z) = F^r(z) \sum_{j=0}^{n-r} \binom{r+j+1}{r-1} [1 - F(z)]^j . \tag{69}
$$

Based on (69), we obtain

$$
F_{Z_{r_2}}(z) = \sum_{r=0}^{K-1} \binom{K-1}{r} (-1)^r \frac{e^{-\frac{(z-1)r}{P_S\gamma_{sr}}}}{1 + \frac{\gamma_{se} zr}{\gamma_{sr}}} + \binom{K-1}{K-2} \sum_{r=0}^{K-1} \binom{K-1}{r} (-1)^r \frac{e^{-\frac{(z-1)(r+1)}{P_S\gamma_{sr}}}}{1 + \frac{\gamma_{se} z(r+1)}{\gamma_{sr}}}, \tag{70}
$$

$$F_{Z_{t_2}}(z) = \left(1 - \frac{e^{-\frac{z-1}{P_R\gamma_{rd}}}}{1+\frac{\gamma_{re}z}{\gamma_{rd}}}\right)^{K-1}\left(1+\binom{K-1}{K-2}\frac{e^{-\frac{z-1}{P_R\gamma_{rd}}}}{1+\frac{\gamma_{re}z}{\gamma_{rd}}}\right). \tag{71}$$

Since the computation of $\mathbb{E}[C_{SR,2}]$ and $\mathbb{E}[C_{RD,2}]$ are similar to that of $\mathbb{E}[C_{SR,1}]$ and $\mathbb{E}[C_{RD,1}]$ respectively, the detailed expressions of $\mathbb{E}[C_{SR,2}]$ and $\mathbb{E}[C_{RD,2}]$ are directly given above by (25) and (27), respectively.

d) *Computation of* p_{12}: Given that $z_{r_1} > z_{r_2}$, $z_{t_1} > z_{t_2}$, we have

$$\begin{aligned} p_{12} &= P\{Q>0\} = P\{\min\{z_{r_1}, z_{t_2}\} > \min\{z_{r_2}, z_{t_1}\}\} = P\{z_{t_2} > z_{r_2}\} \\ &= \iint\limits_{z_{t_2}>z_{r_2}} f_{z_{r_2},z_{t_2}}(z_{r_2}, z_{t_2}) dz_{r_2} dz_{t_2} = \int_0^\infty f_{z_{r_2}}(z)(1-F_{z_{t_2}}(z))dz. \end{aligned} \tag{72}$$

Since we have obtained the CDF of z_{r_2} and z_{t_2}, we can express the probability of $Q > 0$, i.e., p_{12}, as an integral form and calculate its value numerically.

Proof of Theorem 1

First, to compute the secrecy throughput for mode I of the proposed HyIFD scheme in high SNR regime, we need to find $\mathbb{E}[C_{SR,1}]$, $\mathbb{E}[C_{RD,1}]$, $\mathbb{E}[C_{SR,2}]$, $\mathbb{E}[C_{RD,2}]$ and p_{12} in high SNR regime, which is denoted as $\widehat{C}_{SR,1}$, $\widehat{C}_{RD,1}$, $\widehat{C}_{SR,2}$, $\widehat{C}_{RD,2}$ and $\widehat{p}_{12}$, respectively.

a) *Computation of* $\widehat{C}_{SR,1}$: As the total power SNR $\to \infty$, we know that $P_S \to \infty$, and $\widehat{C}_{SR,1}$ can be obtained as

$$\begin{aligned} \widehat{C}_{SR,1} &= \lim_{P_S\to\infty}\mathbb{E}[C_{SR,1}] = \lim_{P_S\to\infty}\sum_{r=1}^{K}\binom{K}{r}(-1)^r \frac{e^{\frac{r}{P_S\gamma_{sr}}}}{\ln 2} \\ &\quad\times\left[-E_1\left(\frac{r}{P_S\gamma_{sr}}\right) + e^{\frac{1}{P_S\gamma_{se}}}E_1\left(\frac{r}{P_S\gamma_{sr}}+\frac{1}{P_S\gamma_{se}}\right)\right] \\ &\overset{a}{=} \lim_{P_S\to\infty}\sum_{r=1}^{K}\binom{K}{r}(-1)^r\frac{1}{\ln 2}\times\left[-\ln\left(\frac{P_S\gamma_{sr}}{r}\right)+\ln\left(\frac{1}{\frac{r}{P_S\gamma_{sr}}+\frac{1}{P_S\gamma_{se}}}\right)\right] \\ &= \sum_{r=1}^{K}\binom{K}{r}(-1)^{r+1}\log_2\left(1+\frac{\gamma_{sr}}{r\gamma_{se}}\right), \end{aligned} \tag{73}$$

where equality (a) is obtained comes from the fact that as $P_S \to \infty$, $e^{\frac{r}{P_S\gamma_{sr}}} \to 1$, $e^{\frac{1}{P_S\gamma_{se}}} \to 1$, and an approximation has been used for the exponential integral function $E_1(x)$ [39]:

$$E_1(x) = \ln(\frac{1}{x}) - \gamma - \sum_{k=1}^{\infty}\frac{(-x)^k}{kk!}, x > 0, \tag{74}$$

where $\gamma \approx 0.5772156649$ is the Euler constant.

b) *Computation of* $\widehat{C}_{RD,1}$: As the total power SNR $\to \infty$, we also have $P_R \to \infty$, and $\widehat{C}_{RD,1}$ can be obtained as

$$\begin{aligned}\widehat{C}_{RD,1} &= \lim_{P_R\to\infty}\mathbb{E}[C_{RD,1}]\\ &\overset{b}{=} \lim_{P_R\to\infty}\sum_{r=1}^{K}\binom{K}{r}(-1)^r\frac{\gamma_{re}}{\ln 2\gamma_{rd}}\times\left[-E_1\left(\frac{r}{P_R\gamma_{rd}}\right)+\sum_{i=1}^{r}\left(\frac{\left(-\frac{r}{\gamma_{re}}\right)^{i-1}}{(i-1)!}\cdot\underbrace{\frac{E_1\left(\frac{r}{P_R}\left(\frac{1}{\gamma_{rd}}+\frac{1}{\gamma_{re}}\right)\right)}{P_R^{i-1}}}_{A}\right)+\sum_{i=2}^{r}\left(\frac{1}{\left(\frac{\gamma_{re}}{\gamma_{rd}}+1\right)^{i-1}}\cdot\frac{1}{i-1}\right)\right],\end{aligned}\tag{75}$$

where equality (b) is obtained comes from the fact that as $P_R\to\infty$, $e^{\frac{r}{P_R}\left(\frac{1}{\gamma_{rd}}+\frac{1}{\gamma_{re}}\right)}\to 1$, $e^{-\frac{r}{P_R\gamma_{re}}}\to 1$, $(\frac{r}{P_R\gamma_{re}})^j\to 0$ as $j\neq 0$ and $(\frac{r}{P_R\gamma_{re}})^j\to 1$ as $j=0$. We first consider the term $\lim_{P_R\to\infty} A$. Here, we use the approximation (74) for the calculation process. Then the value of A as $P_R\to\infty$ can be calculated as

$$\begin{aligned}\lim_{P_R\to\infty}A &= \lim_{P_R\to\infty}\frac{E_1\left(\frac{r}{P_R}\left(\frac{1}{\gamma_{rd}}+\frac{1}{\gamma_{re}}\right)\right)}{{P_R}^{i-1}}\\ &= \lim_{P_R\to\infty}\frac{\ln\left(\frac{P_R}{r\left(\frac{1}{\gamma_{rd}}+\frac{1}{\gamma_{re}}\right)}\right)-\gamma-\sum_{k=1}^{\infty}\frac{\left(\frac{r}{P_R}\left(\frac{1}{\gamma_{rd}}+\frac{1}{\gamma_{re}}\right)\right)^k}{kk!}}{{P_R}^{i-1}}\\ &= \begin{cases}\lim_{P_R\to\infty}\ln\left(\frac{P_R}{r\left(\frac{1}{\gamma_{rd}}+\frac{1}{\gamma_{re}}\right)}\right), & i=1;\\ 0, & i>1.\end{cases}\end{aligned}\tag{76}$$

Then $\widehat{C}_{RD,1}$ can be obtained by

$$\begin{aligned}\widehat{C}_{RD,1} &= \lim_{P_R\to\infty}\sum_{r=1}^{K}\binom{K}{r}(-1)^r\frac{\gamma_{re}}{\ln 2\gamma_{rd}}\left[-\ln\left(\frac{P_R\gamma_{rd}}{r}\right)+\gamma+\ln\left(\frac{P_R}{r\left(\frac{1}{\gamma_{rd}}+\frac{1}{\gamma_{re}}\right)}\right)\right.\\ &\quad\left.-\gamma+\sum_{i=2}^{r}\left(\frac{1}{(i-1)\left(\frac{\gamma_{re}}{\gamma_{rd}}+1\right)^{i-1}}\right)\right]\\ &= \sum_{r=1}^{K}\binom{K}{r}(-1)^r\frac{\gamma_{re}}{\ln 2\gamma_{rd}}\left[-\ln\left(1+\frac{\gamma_{rd}}{\gamma_{re}}\right)+\sum_{i=2}^{r}\left(\frac{1}{(i-1)\left(\frac{\gamma_{re}}{\gamma_{rd}}+1\right)^{i-1}}\right)\right].\end{aligned}\tag{77}$$

c) *Computation of* $\widehat{C}_{SR,2}$ and $\widehat{C}_{RD,2}$: The computation of $\widehat{C}_{SR,2}$ and $\widehat{C}_{RD,2}$ is similar to that of $\widehat{C}_{SR,1}$ and $\widehat{C}_{RD,1}$, respectively. The details of the computation are hence omitted here, and the detailed expressions of $\mathbb{E}[C_{SR,2}]$ and $\mathbb{E}[C_{RD,2}]$ are given above by (43) and (45), respectively.

d) *Computation of* $\widehat{p}_{12}$: The $\widehat{p}_{12}$ can be obtained as

$$\widehat{p}_{12} = \lim_{\substack{P_S\to\infty,\\ P_R\to\infty}} p_{12} = \int_1^{\infty}\lim_{\substack{P_S\to\infty,\\ P_R\to\infty}} f_{Z_{r_2}}(z)(1-F_{Z_{t_2}}(z))dz.\tag{78}$$

For brevity, we denote $\lim_{P_S\to\infty} f_{Z_{r_2}}(z)$ and $\lim_{P_R\to\infty} F_{Z_{t_2}}(z)$ as $\widehat{f}_{Z_{r_2}}(z)$ and $\widehat{F}_{Z_{t_2}}(z)$, respectively. And due to space constraints, the detailed expressions are given above by (47) and (48), respectively.

Proof of Proposition 3

Based on the link selection policy given in (56), the proposed TBLS scheme contains six cases that work in either FD or HD mode. Note that for FD mode, each of the two hops has one link transmitting in one time slot, the outage means that at least one of the two hops cannot successfully transmit, and the threshold z_{th_1}, corresponding to the target secrecy rate R_s, is $z_{th_1} = 2^{R_s}$. While for HD mode, only one link is transmitting in one time slot, the outage occurs when that transmission hop fails to achieve the target transmission rate, and the threshold z_{th_2}, corresponding to R_s, is $z_{th_2} = 2^{2R_s}$. The term "$2R_s$" is due to the fact that it takes two time slots to transmit one packet from S to D [24, 25]. Denote P^i_{out} as the the probability of being at case i and having an outage event, the SOP for six cases can be correspondingly analyzed as follows.

- When $z_{r_1} \geq \lambda$ and $z_{t_1} \geq \mu$, there are three possibilities:

  1 If $r_1 \neq t_1$, we select the relay R_{r_1} for reception and the relay R_{t_1} for transmission in this time slot. Record this case as case 1. Case 1 works in FD mode and the equivalent instantaneous $z = \min\{z_{r_1}, z_{t_1}\}$. The SOP for case 1 is obtained as

  $$P^1_{out} = (1-p_s)P\{\min\{z_{r_1}, z_{t_1}\} < z_{th_1}, z_{r_1} \geq \lambda, z_{t_1} \geq \mu\}. \tag{79}$$

  2 If $r_1 = t_1$ and $z_{t_2} \geq \mu$, we select the relay R_{r_1} for reception and the relay R_{t_2} for transmission in this time slot. Record this case as case 2. Case 2 works in FD mode and the equivalent instantaneous $z = \min(z_{r_1}, z_{t_2})$. The SOP for case 2 is given by

  $$P^2_{out} = p_s P\{\min\{z_{r_1}, z_{t_2}\} < z_{th_1}, z_{r_1} \geq \lambda, z_{t_2} \geq \mu\}. \tag{80}$$

  3 If $r_1 = t_1$ and $z_{t_2} < \mu$, we only select the relay R_{r_1} for reception in this time slot. Record this case as case 3. Case 3 works in HD mode and the equivalent instantaneous $z = z_{r_1}$. The SOP for case 3 can be expressed as

  $$P^3_{out} = p_s P\{z_{r_1} < z_{th_2}, z_{r_1} \geq \lambda, z_{t_1} \geq \mu > z_{t_2}\}. \tag{81}$$

- When $z_{r_1} > \lambda$ and $z_{t_1} < \mu$, we only select the relay R_{r_1} for reception in this time slot. Record this case as case 4. Case 4 works in HD mode and the equivalent instantaneous $z = z_{r_1}$. The SOP for case 4 is

  $$P^4_{out} = P\{z_{r_1} < z_{th_2}, z_{r_1} \geq \lambda, z_{t_1} < \mu\}. \tag{82}$$

- When $z_{r_1} < \lambda$ and $z_{t_1} > \mu$, we only select the relay R_{t_1} for transmission in this time slot. Record this case as case 5. Case 5 works in HD mode and the equivalent instantaneous $z = z_{t_1}$. The SOP for case 5 is given as

$$P_{out}^{5} = P\{z_{t_1} < z_{th_2}, z_{r_1} < \lambda, z_{t_1} \geq \mu\}. \tag{83}$$

- When $z_{r_1} < \lambda$ and $z_{t_1} < \mu$, the relay neither receives nor transmits message in this time slot. Record this case as case 6. Case 6 can be directly considered as an outage. The SOP for case 6 is

$$P_{out}^{6} = P\{z_{r_1} < \lambda, z_{t_1} < \mu\}. \tag{84}$$

Considering all possible cases above, the SOP of the TBLS scheme can finally be expressed by summing up the SOP for all cases. It is given by

$$\begin{aligned} P_{out} &= \sum_{i=1}^{6} P_{out}^{i} \\ &= (1-p_s)P\{\min\{z_{r_1}, z_{t_1}\} < z_{th_1}, z_{r_1} \geq \lambda, z_{t_1} \geq \mu\} \\ &\quad + p_s P\{\min\{z_{r_1}, z_{t_2}\} < z_{th_1}, z_{r_1} \geq \lambda, z_{t_2} \geq \mu\} \\ &\quad + p_s P\{z_{r_1} < z_{th_2}, z_{r_1} \geq \lambda, z_{t_1} \geq \mu > z_{t_2}\} + P\{z_{r_1} < z_{th_2}, z_{r_1} \geq \lambda, z_{t_1} < \mu\} \\ &\quad + P\{z_{t_1} < z_{th_2}, z_{r_1} < \lambda, z_{t_1} \geq \mu\} + P\{z_{r_1} < \lambda, z_{t_1} < \mu\}. \end{aligned} \tag{85}$$

Proof of Proposition 4

Following the discussions in Section IV-B, the SOP of the proposed TBLS scheme is given as

$$\begin{aligned} P_{out} = (1-p_s) &\underbrace{P\{\min\{z_{r_1}, z_{t_1}\} < z_{th_1}, z_{r_1} \geq \lambda, z_{t_1} \geq \mu\}}_{A} \\ &+ p_s \underbrace{P\{\min\{z_{r_1}, z_{t_2}\} < z_{th_1}, z_{r_1} \geq \lambda, z_{t_2} \geq \mu\}}_{B} \\ &+ p_s \underbrace{P\{z_{r_1} < z_{th_2}, z_{r_1} \geq \lambda, z_{t_1} \geq \mu > z_{t_2}\}}_{C} + \underbrace{P\{z_{r_1} < z_{th_2}, z_{r_1} \geq \lambda, z_{t_1} < \mu\}}_{D} \\ &+ \underbrace{P\{z_{t_1} < z_{th_2}, z_{r_1} < \lambda, z_{t_1} \geq \mu\}}_{E}] + \underbrace{P\{z_{r_1} < \lambda, z_{t_1} < \mu\}}_{F}. \end{aligned} \tag{86}$$

So, to compute the SOP of the proposed TBLS scheme, we could compute the term A, B, C, D, E and F separately.

We first consider the term A. It can be calculated as

$$\begin{aligned} A &= P\{\min\{z_{r_1}, z_{t_1}\} < z_{th_1}, z_{r_1} \geq \lambda, z_{t_1} \geq \mu\} \\ &= P\{z_{r_1} > \lambda, z_{t_1} > \mu\} - P\{\min\{z_{r_1}, z_{t_1}\} \geq z_{th_1}, z_{r_1} > \lambda, z_{t_1} > \mu\} \\ &= P\{z_{r_1} > \lambda, z_{t_1} > \mu\} - P\{z_{r_1} \geq z_{th_1}, z_{t_1} \geq z_{th_1}, z_{r_1} > \lambda, z_{t_1} > \mu\} \\ &= P\{z_{r_1} > \lambda, z_{t_1} > \mu\} - P\{z_{r_1} \geq z_{th_1}, z_{r_1} > \lambda\} P\{z_{t_1} \geq z_{th_1}, z_{t_1} > \mu\} \\ &= \begin{cases} (1-F_{Z_{r_1}}(\lambda))(1-F_{Z_{t_1}}(\mu)) \\ \qquad -(1-F_{Z_{r_1}}(z_{th_1}))(1-F_{Z_{t_1}}(z_{th_1})), & \text{if } \lambda < z_{th_1} \text{ and } \mu < z_{th_1}; \\ (1-F_{Z_{r_1}}(\lambda))(F_{Z_{t_1}}(z_{th_1}) - F_{Z_{t_1}}(\mu)), & \text{if } \lambda \geq z_{th_1} \text{ and } \mu < z_{th_1}; \\ (1-F_{Z_{t_1}}(\mu))(F_{Z_{r_1}}(z_{th_1}) - F_{Z_{r_1}}(\lambda)), & \text{if } \lambda < z_{th_1} \text{ and } \mu \geq z_{th_1}; \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \tag{87}$$

The value of B can be obtained in a similar manner, and is given by

$$B = \begin{cases} (1 - F_{Z_{r_1}}(\lambda))(1 - F_{Z_{t_2}}(\mu)) \\ \qquad -(1 - F_{Z_{r_1}}(z_{th_1}))(1 - F_{Z_{t_2}}(z_{th_1})), & \text{if } \lambda < z_{th_1} \text{ and } \mu < z_{th_1}; \\ (1 - F_{Z_{r_1}}(\lambda))(F_{Z_{t_2}}(z_{th_1}) - F_{Z_{t_2}}(\mu)), & \text{if } \lambda \geq z_{th_1} \text{ and } \mu < z_{th_1}; \\ (1 - F_{Z_{t_2}}(\mu))(F_{Z_{r_1}}(z_{th_1}) - F_{Z_{r_1}}(\lambda)), & \text{if } \lambda < z_{th_1} \text{ and } \mu \geq z_{th_1}; \\ 0, & \text{otherwise.} \end{cases} \tag{88}$$

The value of C can be obtained as

$$\begin{aligned} C &= P\{z_{r_1} < z_{th_2}, z_{r_1} \geq \lambda, z_{t_1} \geq \mu > z_{t_2}\} \\ &= P\{z_{r_1} < z_{th_2}, z_{r_1} \geq \lambda\} P\{z_{t_1} \geq \mu > z_{t_2}\} \\ &= \begin{cases} (F_{Z_{r_1}}(z_{th_2}) - F_{Z_{r_1}}(\lambda))(F_{Z_{t_2}}(\mu) - F_{Z_{t_1}}(\mu)), & \lambda < z_{th_2}; \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \tag{89}$$

The value of D can be calculated as

$$\begin{aligned} D &= P\{z_{r_1} < z_{th_2}, z_{r_1} > \lambda, z_{t_1} < \mu\} = P\{\lambda < z_{r_1} < z_{th_2}\} P\{z_{t_1} < \mu\} \\ &= \begin{cases} F_{Z_{t_1}}(\mu)(F_{Z_{r_1}}(z_{th_2}) - F_{Z_{r_1}}(\lambda)), & \lambda < z_{th_2}; \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \tag{90}$$

The computation of E and F are similar and can be obtained as

$$E = \begin{cases} F_{Z_{r_1}}(\lambda)(F_{Z_{t_1}}(z_{th_2}) - F_{Z_{t_1}}(\mu)), & \mu < z_{th_2}; \\ 0, & \text{otherwise.} \end{cases} \tag{91}$$

$$F = F_{Z_{r_1}}(\lambda) F_{Z_{t_1}}(\mu). \tag{92}$$

Finally, substituting (87)–(92) into (86) yields (58), which completes the proof.

Abbreviations

FD: Full-duplex; HD: Half-duplex; SFD-MMRS: Space full-duplex max-max relay selection; RF: Randomize-and-forward; HyIFD: Hybrid imitate full-duplex; TBLS: Threshold-based link selection; SO-TBLS: Sub-optimal threshold-based link selection; ART: Adaptive rate transmissions; FRT: Fixed rate transmissions; SNR: Signal-to-noise-ratio; AWGN: Additive white Gaussian noise; i.i.d.: Independent and identically distributed; CSI: Channel state information; SOP: Secrecy outage probability; CDF: Cumulative distribution function.

Acknowledgements

Not applicable.

Author contributions

JZ was responsible for the theoretical analysis, numerical simulation, and manuscript writing of this research. DQ and HQ contributed to the model construction and revised the manuscript. All authors read and approved the final manuscript.

Funding

This work is supported in part by the National Natural Science Foundation of China (61671205), in part by the Shanghai Rising-Star Program (21QA1402700), and also in part by the open research fund of National Mobile Communications Research Laboratory, Southeast University (No. 2020D02). Haifeng Qian was supported by National Natural Science Foundation of China (61571191, 61632012) and the "Shuguang Program" supported by Shanghai Education Development Foundation and Shanghai Municipal Education Commission (No. 16SG21).

Availability of data and materials

The datasets used or analyzed during the current study are available from the corresponding author on reasonable request.

Declarations

Competing interests

The authors declare that they have no competing interests.

Author details
[1]School of Communication and Electronic Engineering, East China Normal University, Shanghai, China. [2]National Mobile Communications Research Laboratory, Southeast University, Nanjing, China. [3]School of Software Engineering, East China Normal University, Shanghai, China. [4]Shanghai Institute of Intelligent Science and Technology, Tongji University, Shanghai, China.

Received: 3 December 2021 Accepted: 2 May 2022
Published online: 12 May 2022

References

1. M. Agiwal, A. Roy, N. Saxena, Next generation 5g wireless networks: a comprehensive survey. IEEE Commun. Surv. Tutor. **18**(3), 1617–1655 (2016)
2. T. Karygiannis, L. Owens, Wireless network security. NIST Special Publication **800**, 48 (2002)
3. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5th edn. (Prentice-Hall, Englewood Cliffs, 2010)
4. M. Bloch, J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering* (Cambridge University Press, Cambridge, 2011)
5. A.D. Wyner, The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)
6. L. Lai, H.E. Gamal, The relay eavesdropper channel: cooperation for secrecy. IEEE Trans. Inf. Theory. **54**(9), 4005–4019 (2008)
7. L. Dong, Z. Han, A.P. Petropulu, H.V. Poor, Improving wireless physical layer security via cooperating relays. IEEE Trans. Signal Process. **58**(3), 1875–1888 (2010)
8. O.O. Koyluoglu, C.E. Koksal, H. El Gamal, On secrecy capacity scaling in wireless networks. IEEE Trans. Inf. Theory. **58**(5), 3000–3015 (2012)
9. J. Mo, M. Tao, Y. Liu, Relay placement for physical layer security: a secure connection perspective. IEEE Commun. Lett. **16**(6), 878–881 (2012)
10. C. Huang, G. Chen, Y. Gong, Delay-Constrained buffer-aided relay selection in the internet of things with decision-assisted reinforcement learning. IEEE Internet Things J. **8**(12), 10198–10208 (2021)
11. C. Huang, G. Chen, Y. Gong, P. Xu, Z. Han, J.A. Chambers, Buffer-Aided relay selection for cooperative hybrid NOMA/OMA networks with asynchronous deep reinforcement learning. IEEE J. Sel. Areas Commun. **39**(8), 2514–2525 (2021)
12. M. Alkhawatrah, Y. Gong, G. Chen, S. Lambotharan, J.A. Chambers, Buffer-Aided relay selection for cooperative NOMA in the internet of things. IEEE Internet Things J. **6**(3), 5722–5731 (2019)
13. X. Lan, Y. Zhang, Q. Chen, L. Cai, Energy efficient buffer-aided transmission scheme in wireless powered cooperative NOMA relay network. IEEE Trans. Commun. **68**(3), 1432–1447 (2020)
14. Y. Gong, G. Chen, T. Xie, Using buffers in trust-aware relay selection networks with spatially random relays. IEEE Trans. Wirel. Commun. **17**(9), 5818–5826 (2018)
15. N. Nomikos, T. Charalambous, D. Vouyioukas, R. Wichman, G.K. Karagiannidis, Integrating broadcasting and NOMA in full-duplex buffer-aided opportunistic relay networks. IEEE Trans. Veh. Technol. **69**(8), 9157–9162 (2020)
16. J. Wan, D. Qiao, H. Wang, H. Qian, Buffer-aided two-hop secure communications with power control and link selection. IEEE Trans. Wirel. Commun. **17**(11), 7635–7647 (2018)
17. C. Huang, G. Chen, K. Wong, Multi-agent reinforcement learning-based buffer-aided relay selection in IRS-assisted secure cooperative networks. IEEE Trans. Inf. Forensics Secur. **16**, 4101–4112 (2021)
18. Y. Nie, X. Lan, Y. Liu, Q. Chen, G. Chen, L. Fan, D. Tang, Achievable rate region of energy-harvesting based secure two-way buffer-aided relay networks. IEEE Trans. Inf. Forensics Secur. **16**, 1610–1625 (2021)
19. J. Ren, X. Lei, P.D. Diamantoulakis, Q. Chen, G.K. Karagiannidis, Buffer-aided secure relay networks with SWIPT. IEEE Trans. Veh. Technol. **69**(6), 6485–6499 (2020)
20. C. Huang, G. Chen, Y. Gong, Z. Han, Joint buffer-aided hybrid-duplex relay selection and power allocation for secure cognitive networks with double deep Q-network. IEEE Trans. Cogn. Commun. Netw. **7**(3), 834–844 (2021)
21. X. Liao, Y. Zhang, Z. Wu, Y. Shen, X. Jiang, H. Inamura, On security-delay trade-off in two-hop wireless networks with buffer-aided relay selection. IEEE Trans. Wirel. Commun. **17**(3), 1893–1906 (2018)
22. K.T. Phan, Y. Hong, E. Viterbo, Adaptive resource allocation for secure two-hop relaying communication. IEEE Trans. Wirel. Commun. **17**(12), 8457–8472 (2018)
23. D. Wang, P. Ren, J. Cheng, Cooperative secure communication in two-hop buffer-aided networks. IEEE Trans. Commun. **66**(3), 972–985 (2018)
24. G. Chen, Z. Tian, Y. Gong, Z. Chen, J.A. Chambers, Max-ratio relay selection in secure buffer-aided cooperative wireless networks. IEEE Trans. Inf. Forensics Secur. **68**(4), 719–729 (2014)
25. X. Tang, Y. Cai, Y. Huang, T.Q. Duong, W. Yang, W. Yang, Secrecy outage analysis of buffer-aided cooperative MIMO relaying systems. IEEE Trans. Veh. Technol. **67**(3), 2035–2048 (2018)
26. C. Wang, H. Wang, D.W.K. Ng, X. Xia, C. Liu, Joint beamforming and power allocation for secrecy in peer-to-peer relay networks. IEEE Trans. Wirel. Commun. **14**(6), 3280–3293 (2015)
27. H. Deng, H. Wang, W. Guo, W. Wang, Secrecy transmission with a helper: to relay or to jam. IEEE Trans. Inf. Forensics Secur. **10**(2), 293–307 (2014)
28. Z. Chu, K. Cumanan, Z. Ding, M. Johnston, S.Y. Le Goff, Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer. IEEE Trans. Veh. Technol. **64**(5), 833–1847 (2015)
29. X. Lu, RCd. Lamare, Opportunistic relaying and jamming based on secrecy-rate maximization for multiuser buffer-aided relay systems. IEEE Trans. Veh. Technol. **69**(12), 15269–15283 (2020)

30. R. Nakai, S. Sugiura, Physical layer security in buffer-state-based max-ratio relay selection exploiting broadcasting with cooperative beamforming and jamming. IEEE Trans. Inf. Forensics Secur. **14**(2), 431–444 (2019)
31. M. Jain et al., Practical, real-time, full duplexing wireless, in *Proceedings of the ACM Mobile Computing and Networking (MobiCom)* (Las Vegas, USA, 2011)
32. D. Bharadia, E. McMilin, S. Katti, Full duplex radio, in *Proceedings of the ACM SIGCOMM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications* (Hong Kong, China, 2013)
33. A. Ikhlef, J. Kim, R. Schober, Mimicking full-duplex relaying using half-duplex relays with buffers. IEEE Trans. Veh. Technol. **61**(7), 3025–3037 (2012)
34. D. Qiao, M.C. Guroy, S. Velipasalar, Secure wireless communications and optimal power control under statistical queueing constraints. IEEE Trans. Inf. Forensics Secur. **6**(3), 628–639 (2011)
35. L. Qian, X. Chi, L. Zhao, M. Obeed, A. Chaaban, User-centric secure cell formation for visible light networks with statistical delay guarantees. IEEE Trans. Wirel. Commun. **20**(3), 1831–1846 (2021)
36. C. Li, C. She, N. Yang, T.Q.S. Quek, Secure transmission rate of short packets with queueing delay requirement. IEEE Trans. Wirel. Commun. **21**(1), 203–218 (2022)
37. S. Wang, M. Xia, K. Huang, Y. Wu, Wirelessly powered two-way communication with nonlinear energy harvesting model: rate regions under fixed and mobile relay. IEEE Trans. Wirel. Commun. **16**(12), 8190–8204 (2017)
38. B. Xia, Y. Fan, J. Thompson, H. Vincent, Poor, Buffering in a three-node relay network. IEEE Trans. Wirel. Commun. **7**(11), 4492–4496 (2008)
39. D. Barry, J.Y. Parlange, L. Li, Approximation for the exponential integral (Theis well function). J. Hydrol. **227**(14), 287–291 (2000)
40. H.A. David, H.N. Nagaraja, *Order Statistics*, 3rd edn. (Wiley, New York, 2003)
41. M. Bloch, J. Barros, M.R.D. Rodrigues, S.W. McLaughlin, Wireless information-theoretic security. IEEE Trans. Inf. Theory. **54**(6), 2525–2534 (2008)

Publisher's note