Wireless Physical Layer Security Enhancement with Buffer-Aided Relaying

Jing Huang and A. Lee Swindlehurst
Center for Pervasive Communications and Computing
University of California, Irvine, CA 92697
Email: {jing.huang; swindle}@uci.edu

***Abstract*—We consider utilizing a buffer-aided relay to enhance security for two-hop half-duplex relay networks with an external eavesdropper. We propose a link selection scheme that adapts reception and transmission time slots based on the channel quality, while considering both the two-hop transmission efficiency and the security. Closed-form expressions for the secrecy throughput and the secrecy outage probability (SOP) are derived, and the selection parameters are optimized to maximize the secrecy throughput or minimize the SOP. We also study two sub-optimal link selection schemes that only require a line search to solve the optimization problem. Numerical results show that buffer-aided relaying provides a significant improvement in security compared to conventional unbuffered relaying.**

I. Introduction

Security issues in relay networks have received considerable attention recently. Various cooperation strategies were proposed to improve the physical layer security. In these works, the relays can act as pure receive-and-forward nodes [1], or as jammers that cooperatively transmit artificial noise to confuse the eavesdropper [2], [3]. Relays can also play dual roles of simultaneously forwarding information and transmitting artificial noise [4]–[6]. More recently, there has been research conducted on scenarios with untrusted relays, where the relay is in effect also an eavesdropper, even though it complies with the source's request to forward messages to the destination [7]–[9].

The relays considered in most of the previous work on half-duplex relay-eavesdropper channels are assumed to receive the signal in one time slot and forward it in the following one. This fixed-schedule two-hop protocol, albeit relatively simple, has limitations on transmission efficiency and diversity performance. Recently, buffer-aided relays have been studied for conventional relay networks without secrecy concerns to further exploit the transmission flexibility. For example, [10]–[12] assume the relay can adapt reception and transmission time slots based on the quality of the source-relay and relay-destination channels. [10] shows that a buffer-aided relay can provide both throughput and diversity gain by adaptive link selection. In such cases, transmission efficiency can be improved by choosing to let the source transmit in the first hop, and then store the data in the relay's buffer if the second-hop channel is weak. The relay delays transmission until the quality of the second-hop channel improves sufficiently. This motivates the use of buffered relaying in the relay-eavesdropper channel, since this relaying protocol can not only improve the two-hop efficiency, but also enable an on-off transmission strategy [13], [14], which allows the transmitter to delay its signal if the legitimate link is relatively weak.

In this paper, we study a two-hop decode-and-forward (DF) relay channel with an external eavesdropper, where the relay is aided by a buffer and therefore can adaptively choose to either transmit or receive in each time slot. We propose a link selection scheme that considers both two-hop transmission efficiency and secrecy constraints to determine which node should transmit in each time slot. We then derive closed-form expressions for the secrecy throughput and the SOP, which we can use to optimize the link selection parameters for either maximizing the secrecy throughput or minimizing the SOP. The proposed schemes are shown to provide significant gains in security performance compared to conventional unbuffered relaying.

The remainder of this work is organized as follows. The mathematical model of the buffer-aided relaying protocol is introduced in Section II. The link selection policies are studied in Section III, where expressions for the corresponding secrecy throughput and SOP are derived. Selected numerical results are shown in Section IV, and we conclude in Section V.

II. Mathematical Model

We consider a half-duplex two-hop relaying network composed of a source (Alice), a destination (Bob), and a DF relay equipped with a buffer, as shown in Fig. 1. Each node is assumed to have a single antenna. The DF relay is able to store the decoded data packets received from Alice before forwarding them to Bob. Each transmission occurs in equal-length time slots. As in [3], [4], we assume there is no direct link for the Alice-Bob and Alice-Eve channels, and communication can only rely on the relay. The channel is assumed to be stationary and ergodic with frequency non-selective Rayleigh block fading, *i.e.* the channel gains remain constant during one time slot, but change independently from one time slot to the next. We also assume Alice and the relay transmit with a fixed power P_a and P_r, respectively.

In the k-th time slot, the complex channel gains of each link are denoted as $h_{i,k}$ where $i \in \{a, b, e\}$ represents which of the three nodes Alice, Bob and Eve is involved. The noise

This work was supported by the U.S. Army Research Office MURI Grant W911NF-07-1-0318, and by the National Science Foundation by Grant CCF-1117983.

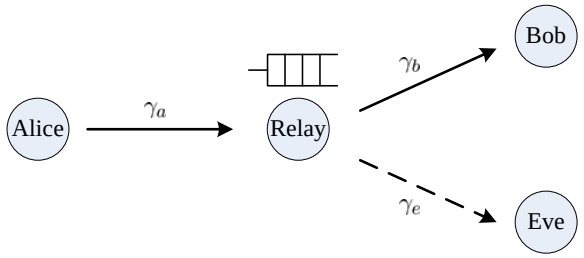

Fig. 1. Model of two-hop buffered relaying with an eavesdropper.

variances at the relay, Bob and Eve are denoted by $\sigma^2_{r,k}$, $\sigma^2_{b,k}$ and $\sigma^2_{e,k}$ respectively. The instantaneous SNRs for each link are then given by $\gamma_{a,k} = \frac{P_a}{\sigma^2_{r,k}}|h_{a,k}|^2$, $\gamma_{b,k} = \frac{P_r}{\sigma^2_{b,k}}|h_{b,k}|^2$ and $\gamma_{e,k} = \frac{P_r}{\sigma^2_{e,k}}|h_{e,k}|^2$ as labeled in Fig. 1, and thus $\gamma_{i,k}$ is exponentially distributed with hazard rate $\frac{1}{\bar{\gamma}_i}$. The probability density function (p.d.f.) of $\gamma_{i,k}$ is given by

$$f_{i,k}(x) = \frac{1}{\bar{\gamma}_i}\, e^{-\frac{x}{\bar{\gamma}_i}}, \quad x \geq 0, \quad i \in \{a, b, e\}. \tag{1}$$

We assume that Alice knows the relay's CSI, and the relay knows Bob's CSI, but neither of them knows the instantaneous CSI of Eve. In each time slot, due to the half-duplex constraint, either Alice or the relay will be selected for transmission. The *link selection* decision depends on the channel conditions, and the optimization of the decision parameters will be discussed in the following sections.

For a given time slot k, if a transmission occurs in the first hop, Alice will adaptively adjust her transmission rate $R_{a,k}$ arbitrarily close to the capacity, *i.e.* $R_{a,k} = C_{a,k} = \log_2(1 + \gamma_{a,k})$, such that no outage events occur in the first hop. If the second-hop link is selected, the relay will forward the secret messages decoded and stored in its buffer during the first hop. We assume the relay uses a codebook $\mathcal{C}(2^{nR_{b,k}}, 2^{nR'_s}, n)$ where R'_s is the intended secrecy rate, n is the codeword length, $2^{nR_{b,k}}$ is the size of the codebook, and $2^{nR'_s}$ is the number of confidential messages to send. The $2^{nR_{b,k}}$ codewords are randomly grouped into $2^{nR'_s}$ bins. To send confidential message $w \in \{1, \cdots, 2^{nR'_s}\}$, the relay will use a stochastic encoder to randomly select a codeword from bin w and send it over the channel. Since Bob's CSI is assumed to be available at the relay, the encoder will adaptively set $R_{b,k}$ to be arbitrarily close to the channel capacity from the rely to Bob, *i.e.* $R_{b,k} = C_{b,k} = \log_2(1 + \gamma_{b,k})$.

Since the instantaneous CSI for Eve is not available at the relay, we assume the encoder will set a fixed value for the intended positive secrecy rate R_s, and thus $R'_s = \min\{R_s, Q_k\}$ where Q_k represents the normalized number of bits (*i.e.* divided by the length of the time slot) in the buffer at the beginning of the k-th time slot. Note that in such case, a secrecy outage event [15] is possible to occur in the transmission and we will analyze the secrecy outage probability of such events in the following sections. We also assume that Alice always has data to transmit and the buffer at the relay is not limited in size.

III. Link Selection Design for Buffered-Aided Relaying

In this section, we propose link selection schemes aimed at maximizing the secrecy throughput under desired SOP constraints, or minimizing the SOP under certain throughput requirements.

A. Link Selection Policy

The relay decides whether she should transmit to Bob or listen to Alice during each time slot. The selection should consider the following two aspects: 1) *two-hop transmission efficiency* – for DF relaying without a direct connection, if the first-hop channel is significantly better than the second-hop, Alice should transmit and the relay should listen and store the decoded data in her buffer. Otherwise, the relay should be selected to forward data to Bob as long as the following condition is also satisfied, 2) *security performance* – the channel from the relay to Bob should be strong enough to guarantee a certain SOP. Based on the above considerations and the assumption that the instantaneous CSI of Eve is not available, we propose the following link selection criterion:

$$I_{k\in\{1,\ldots,N\}} = \begin{cases} 1 & \gamma_{b,k} \geq \max\{\alpha\gamma_{a,k}, \beta\} \\ 0 & \text{otherwise,} \end{cases} \tag{2}$$

where I_k is a binary-valued variable with $I_k = 1$ ($I_k = 0$) representing the relay transmits (listens) in the k-th time slot, and $\{\alpha, \beta\}$ are two non-negative scalars that determine the threshold for choosing when the relay transmits. The condition $\gamma_{b,k} \geq \alpha\gamma_{a,k}$ relates the relative quality of the links from the relay to Bob and Alice (and hence is important for maintaining the two-hop transmission efficiency), while $\gamma_{b,k} \geq \beta$ is used to assess the quality of the link to Bob in order to provide good secrecy performance. Note that both conditions must be satisfied for the relay to transmit in time slot k. The parameters α and β must be chosen to optimize the desired performance metric.

The transmission probability of the relay is a function of α and β, and can be calculated as

$$\begin{aligned} &p_b(\alpha, \beta) \\ &= Pr[\gamma_{b,k} \geq \max(\alpha\gamma_{a,k}, \beta)] \\ &= Pr(\gamma_{b,k} \geq \alpha\gamma_{a,k}, \alpha\gamma_{a,k} \geq \beta) + Pr(\gamma_{b,k} \geq \beta, \alpha\gamma_{a,k} < \beta) \\ &= Pr(\beta \leq \alpha\gamma_{a,k} \leq \gamma_{b,k}) + Pr(\gamma_{b,k} \geq \beta)Pr(\alpha\gamma_{a,k} < \beta) \\ &= e^{-\frac{\beta}{\bar{\gamma}_b}} - \frac{\alpha\bar{\gamma}_a}{\bar{\gamma}_b + \alpha\bar{\gamma}_a} e^{-(\frac{\beta}{\bar{\gamma}_b} + \frac{\beta}{\alpha\bar{\gamma}_a})}. \end{aligned} \tag{3}$$

B. Secrecy Throughput

According to the transmission model in Section II and (2), the average arrival and departure rates at the relay buffer can be written as

$$R_{\text{in}} = \lim_{N\to\infty} \frac{1}{N} \sum_{k=1}^{N} (1 - I_k) R_{a,k}, \tag{4}$$

and the departure secrecy rate considering the queue of the buffer is given by

$$R_{\text{out}} = \lim_{N\to\infty} \frac{1}{N} \sum_{k=1}^{N} I_k \min\{R_s, Q_k\}, \tag{5}$$

which is also the secrecy throughput of the channel. Note that $R_{\text{in}} \geq R_{\text{out}}$ is always valid due to the buffered relaying protocol, and when $R_{\text{in}} > R_{\text{out}}$, the queue of the buffer is said to be in the absorbing state.

Lemma 1: Under a link selection policy that maximizes the throughput, the queue in the buffer is at the edge of non-absorption where

$$\lim_{N\to\infty} \frac{1}{N} \sum_{k=1}^{N} I_k \min\{R_s, Q_k\} = \lim_{N\to\infty} \frac{1}{N} \sum_{k=1}^{N} I_k R_s.$$

Therefore, assuming that $\gamma_{a,k}$ and $\gamma_{b,k}$ are ergodic and stationary random processes, then

$$\mathbb{E}\{(1-I_k)R_{a,k}\} = \mathbb{E}\{I_k R_s\} \tag{6}$$

and the corresponding throughput is

$$R_t = \mathbb{E}\{I_k R_s\}. \tag{7}$$

Proof: The proof is similar to that for Theorems 1 and 2 in [12] and is omitted here. ∎

Lemma 1 indicates that under the optimal link selection policy, the impact of the event where $R_s > Q_k, k \in \{1, \ldots, N\}$ is negligible, and the throughput maximization can be formulated based on (7) with the rate balance constraint (6). Since R_s is a fixed scalar, the throughput is

$$R_t = \mathbb{E}\{I_k R_s\} = p_b R_s \tag{8}$$

where p_b is given by (3).

Since $\gamma_{a,k}$, $\gamma_{b,k}$ and $\gamma_{e,k}$ are assumed to be time-invariant respectively, we will use $\gamma_a = \gamma_{a,k}$, $\gamma_b = \gamma_{b,k}$ and $\gamma_e = \gamma_{e,k}$, $k \in \{1, \ldots, N\}$ throughout the remainder of the paper for simplicity. Next, we calculate the average arrival rate at the relay. According to (2), Alice transmits when $\gamma_b < \max(\alpha\gamma_a, \beta)$ which is equivalent to $(\gamma_b < \beta) \cup (\beta < \gamma_b < \alpha\gamma_a)$. Therefore, we have the following proposition,

Proposition 1: The average arrival rate, based on the link selection scheme given in (2), can be written as

$$\begin{aligned}
&\mathbb{E}\{(1-I_k)R_a\} \\
&= \int_0^{\beta} \left(\int_0^{\infty} \log_2(1+\gamma_a) f_a(\gamma_a) d\gamma_a \right) f_b(\gamma_b) d\gamma_b \\
&\quad + \int_{\beta}^{\infty} \left(\int_{\frac{\gamma_b}{\alpha}}^{\infty} \log_2(1+\gamma_a) f_a(\gamma_a) d\gamma_a \right) f_b(\gamma_b) d\gamma_b \\
&= \log_2\left(1+\frac{\beta}{\alpha}\right) \frac{\alpha\bar{\gamma}_a}{\alpha\bar{\gamma}_a + \bar{\gamma}_b} e^{-(\frac{\beta}{\alpha\bar{\gamma}_a} + \frac{\beta}{\bar{\gamma}_b})} \\
&\quad + \frac{1}{\ln 2}(1 - e^{-\frac{\beta}{\bar{\gamma}_b}}) e^{\frac{1}{\bar{\gamma}_a}} E_1\left(\frac{1}{\bar{\gamma}_a}\right) \\
&\quad + \frac{1}{\ln 2} e^{(\frac{1}{\bar{\gamma}_a} - \frac{\beta}{\bar{\gamma}_b})} E_1\left(\frac{\alpha+\beta}{\alpha\bar{\gamma}_a}\right) \\
&\quad - \frac{1}{\ln 2} \frac{\bar{\gamma}_b}{\alpha\bar{\gamma}_a + \bar{\gamma}_b} e^{\frac{1}{\bar{\gamma}_a} + \frac{\alpha}{\bar{\gamma}_b}} E_1\left[\left(\frac{1}{\bar{\gamma}_a} + \frac{\alpha}{\bar{\gamma}_b}\right)\left(1+\frac{\beta}{\alpha}\right)\right]
\end{aligned} \tag{9}$$

where α and β are non-negative scalars representing the SNR threshold for the link selection policy, and $E_1(x) = \int_x^{\infty} \frac{e^{-t}}{t} d\,t$, $x > 0$ is the exponential integral function.

Proof: Skipped due to space constraint. ∎

C. Secrecy Outage Probability

In addition to secrecy throughput, an important security measurement for our model is the SOP, which determines the likelyhood of achieving a certain secrecy rate in fading channels. For single-hop transmission, the traditional SOP is defined as $p_{\text{sop}} = Pr\{C_s < R_s\}$ where the secrecy capacity $C_s = \max\{0, C_b - C_e\}$ depends on the channel capacity at Bob C_b and at Eve C_e [15]. An alternative expression is given in [16] as $p_{\text{sop}} = Pr\{C_e > R_b - R_s\}$ which takes into account the rate of the transmitted codewords. More recently, the SOP conditioned on actual private message transmission is introduced in [14] as $p_{\text{sop}} = Pr\{C_e > R_b - R_s \mid \text{message transmission}\}$, which is more suitable to on-off secure transmission, and we will adopt this formulation in our buffered relaying case.

Since R_b is assumed to be adaptively adjusted to C_b, the SOP is written as

$$\begin{aligned}
&p_{\text{sop}}(R_s, \alpha, \beta) \\
&= Pr[C_e > C_b - \min(R_s, Q_k) | \gamma_b > \max(\alpha\gamma_a, \beta)] \\
&\overset{a}{\leq} Pr[C_e > C_b - R_s | \gamma_b > \max(\alpha\gamma_a, \beta)] \\
&= \frac{Pr[C_e > C_b - R_s, \gamma_b > \max(\alpha\gamma_a, \beta)]}{Pr[\gamma_b > \max(\alpha\gamma_a, \beta)]} \\
&= \frac{Pr[C_e > C_b - R_s, \beta \leq \alpha\gamma_a < \gamma_b]}{Pr[\gamma_b > \max(\alpha\gamma_a, \beta)]} \\
&\quad + \frac{Pr[C_e > C_b - R_s, \gamma_b > \beta, \alpha\gamma_a < \beta]}{Pr[\gamma_b > \max(\alpha\gamma_a, \beta)]} \\
&= \frac{Pr[\beta \leq \alpha\gamma_a < \gamma_b < 2^{R_s}(1+\gamma_e) - 1]}{Pr[\gamma_b > \max(\alpha\gamma_a, \beta)]} \\
&\quad + \frac{Pr[\beta < \gamma_b < 2^{R_s}(1+\gamma_e) - 1] Pr[\alpha\gamma_a < \beta]}{Pr[\gamma_b > \max(\alpha\gamma_a, \beta)]},
\end{aligned} \tag{10}$$

which is a function of the desired secrecy rate R_s and the link selection parameters α and β. Note that inequality (a) indicates that the result in (10) is an upper bound for the SOP. However, when using the optimal link selection policy (optimizing α and β such that (6) is satisfied), the queue of the buffer is at the edge of non-absorption and the probability of the event $R_s > Q_k$ is negligible. Therefore, the above upper bound is tight. Further manipulations reveal that,

$$\begin{aligned}
&p_{\text{sop}} \\
&= \frac{\int_{\frac{\beta+1}{2^{R_s}}-1}^{\infty} \int_{\beta}^{2^{R_s}(1+\gamma_e)-1} \int_{\beta/\alpha}^{\gamma_b/\alpha} f_a(\gamma_a) f_b(\gamma_b) f_e(\gamma_e) d\gamma_a d\gamma_b d\gamma_e}{p_b} \\
&\quad + \frac{\int_{\frac{\beta+1}{2^{R_s}}-1}^{\infty} \int_{\beta}^{2^{R_s}(1+\gamma_e)-1} f_b(\gamma_b) f_e(\gamma_e) d\gamma_b d\gamma_e}{p_b}
\end{aligned}$$

$$= \left(\frac{2^{R_s}\bar{\gamma}_e}{(2^{R_s}\bar{\gamma}_e+\bar{\gamma}_b)(\frac{\alpha\bar{\gamma}_a}{\bar{\gamma}_b}+\frac{\alpha\bar{\gamma}_a}{2^{R_s}\bar{\gamma}_e}+1)} e^{-(\frac{\beta}{\alpha\bar{\gamma}_a}+\frac{\beta}{\bar{\gamma}_b}+\frac{1+\beta-2^{R_s}}{2^{R_s}\bar{\gamma}_e})} + \frac{2^{R_s}\bar{\gamma}_e}{(2^{R_s}\bar{\gamma}_e+\bar{\gamma}_b)} e^{-(\frac{1+\beta-2^{R_s}}{2^{R_s}\gamma_e}+\frac{\beta}{\bar{\gamma}_b})}(1-e^{-\frac{\beta}{\alpha\bar{\gamma}_a}}) \right) \frac{1}{p_b}. \tag{11}$$

Note that the encoding at the relay requires that $R_s \leq C_b = \log_2(1+\gamma_b)$, thus $\beta \geq 2^{R_s}-1$ always holds and the lower limit of the outer integration is non-negative.

D. Optimization of Link Selection Parameters (LS-OPT)

Now we are ready to formulate our optimization problem. We aim to optimize the secrecy rate R_s that the relay uses for encoding, and the transmission threshold α and β that the relay uses to perform link selection, such that 1) the secrecy throughput is maximized under a certain SOP constraint or 2) the SOP is minimized under a certain secrecy throughput requirement. We refer the former as Problem P1 and the latter as Problem P2 in the sequel.

Therefore, for Problem P1, we can formulate as

$$\begin{aligned} \mathbf{P1}: \quad & \max_{\mathrm{R_s},\alpha,\beta} \quad p_b(\alpha,\beta)R_s && \text{(12a)} \\ & \text{s.t.} \quad p_{\mathrm{sop}}(R_s,\alpha,\beta) \leq \eta && \text{(12b)} \\ & \quad \mathbb{E}\{(1-I_k)C_a\} = \mathbb{E}\{I_k R_s\} && \text{(12c)} \\ & \quad R_s>0, \alpha \geq 0, \beta \geq 2^{R_s}-1, && \text{(12d)} \end{aligned}$$

where η ($\eta \leq 1$) is the desired maximum SOP, the expression for (12b) is given in (11), (12c) is the condition for maximum throughput, and the average rates are given in (8) and (9), respectively.

For Problem P2, we have

$$\begin{aligned} \mathbf{P2}: \quad & \min_{\mathrm{R_s},\alpha,\beta} \quad p_{\mathrm{sop}}(R_s,\alpha,\beta) && \text{(13a)} \\ & \text{s.t.} \quad p_b(\alpha,\beta)R_s \geq \mu && \text{(13b)} \\ & \quad \mathbb{E}\{(1-I_k)C_a\} = \mathbb{E}\{I_k R_s\} && \text{(13c)} \\ & \quad R_s>0, \alpha \geq 0, \beta \geq 2^{R_s}-1, && \text{(13d)} \end{aligned}$$

where μ ($\mu > 0$) is the minimum desired throughput. Closed-form solutions to P1 and P2 are in general intractable, and thus a two dimensional search over R_s and β is used in order to demonstrate the performance of the optimal link selection policy. For given R_s and β, the value of α can be obtained numerically by solving (12c) or (13c). Next, we will study two sub-optimal schemes that only require a line search.

E. Sub-optimal Link Selection Policies

1) Link Selection with Two-Hop Condition (LS-TC): When the relay only considers the two-hop condition, *i.e.* when it only uses α as the threshold parameter in selecting the link, the selection policy can be written as:

$$I_k^{TC} = \begin{cases} 1 & \gamma_b \geq \max\{\alpha\gamma_a, 2^{R_s}-1\} \\ 0 & \text{otherwise.} \end{cases} \tag{14}$$

This approach reduces to a scheme similar to that used in [12] for conventional buffer-aided relaying, but with two differences: 1) The throughput maximized in [12] is the public data rate to Bob, while the throughput in our work is the average secrecy rate constrained by the SOP, and 2) we have a minimum threshold $2^{Rs}-1$ for γ_b to ensure a feasible secrecy codebook. The transmission probability p_b, the average arrival rate $\mathbb{E}\{(1-I_k)C_a\}$, and the SOP p_{sop} are then given by (3), (9) and (11) with β fixed at $2^{Rs}-1$. To solve for P1 and P2, one only needs to perform a line search over R_s, and given R_s the value of α can be obtained by solving $\mathbb{E}\{(1-I_k)C_a\} = p_b R_s$.

2) Link Selection with Secrecy Condition (LS-SC): Alternatively, a link selection scheme that only considers β can be expressed as

$$I_k^{SC} = \begin{cases} 1 & \gamma_b \geq \beta \\ 0 & \text{otherwise.} \end{cases} \tag{15}$$

This policy not only considers secrecy, but also indirectly considers the two-hop transmission efficiency since the relay only transmits when her channel to Bob is relatively strong. Note that this approach is similar to the *on-off* transmission scheme in [14], although the case considered therein focuses on a single-hop channel. Similar to LS-TC, the transmission probability, the average arrival rate, and the SOP are given by (3), (9) and (11) with α equating zero, and corresponding P1 and P2 can be solved via a line search over R_s.

IV. Numerical Results

In this section, we present numerical examples of the security performance for the proposed link selection schemes, LS-OPT, LS-TC and LS-SC. In order to show the security improvement introduced by buffer-aided relaying, we also compare its performance with the conventional unbuffered approach.

Fig. 2 shows the secrecy throughput versus the desired SOP constraint (Problem P1) for various link selection polices, assuming average SNRs of $\bar{\gamma}_a = 5$dB, $\bar{\gamma}_b = 15$dB, $\bar{\gamma}_e = 0$dB, and assuming adaptive rate at the relay. As expected, in general for all schemes, a higher η results in a larger secrecy throughput. When η is close to 1, the performance of all schemes saturates to the conventional throughput without secrecy constraints. We can also see that the throughput gain of buffered over unbuffered relaying is significant. The performance of LS-OPT is always the best among all schemes, and it is observed that the performance of LS-OPT converges to that of LS-SC when η is low, and converges to that of LS-TC as η grows. This indicates that the selection parameter β dominates with a stricter secrecy constraint, and α dominates in turn when the secrecy constraint is more relaxed.

Fig. 3 illustrates the SOP as a function of the desired secrecy throughput threshold μ (Problem P2) assuming $\bar{\gamma}_a = 5$dB, $\bar{\gamma}_b = 15$dB, $\bar{\gamma}_e = 0$dB. It shows a significant performance gain for buffered relaying compared with the unbuffered case. For example, when $\mu \geq 0.9$ bps/Hz, unbuffered relaying hardly allows any secure transmission while LS-OPT can still guarantee an SOP as low as 10^{-3}. When μ is small, the SOP of LS-TC is obviously worse than that of other selection schemes, and the SOP of LS-OPT converges to that of LS-SC. On the

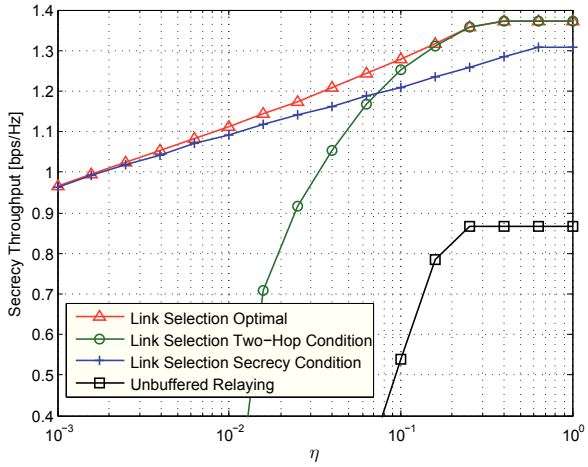

Fig. 2. Secrecy throughput versus desired SOP constraint η, adaptive-rate transmission at the relay, Problem P1 with $\bar{\gamma}_a = 5$dB, $\bar{\gamma}_b = 15$dB, $\bar{\gamma}_e = 0$dB.

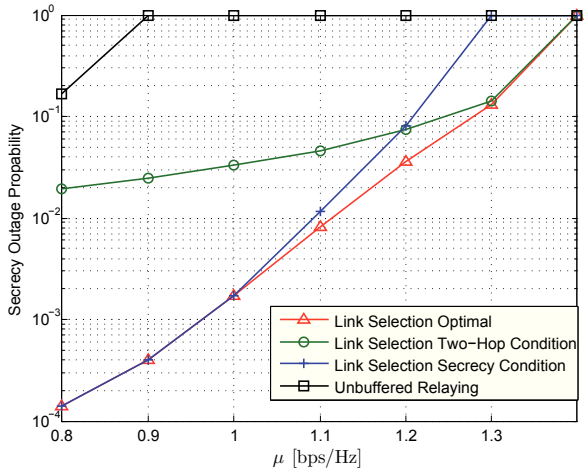

Fig. 3. Secrecy outage probability versus desired secrecy throughput constraint μ, adaptive-rate transmission at the relay, Problem P2 with $\bar{\gamma}_a = 5$dB, $\bar{\gamma}_b = 15$dB, $\bar{\gamma}_e = 0$dB.

other hand, when we require a larger μ, the performance of LS-SC degrades and LS-OPT converges to LS-TC, which seeks a better throughput.

V. Conclusions

This paper has considered a two-hop DF relay network with an eavesdropper, where the relay is aided by a buffer and thus can dynamically control whether each time slot is used for reception or transmission. We proposed a link selection policy that takes into account both the two-hop rate balance and the security constraint, and we optimized the link selection parameters based on the closed-form expressions derived for the secrecy throughput and SOP. We have also discussed two sub-optimal link selection schemes based on the optimal approach that consider either only the two-hop conditions or the secrecy constraint. Numerical examples demonstrated that buffer-aided relaying provides significant performance improvement in terms of both secrecy throughput and secrecy outage probability.

References

[1] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[2] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[3] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secrecy," in *Proc. IEEE Int Communications Conf (ICC)*, May 2010, pp. 1–5.

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

[5] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting," *IEEE Trans. Wireless Commun.*, vol. 10, no. 6, pp. 1725–1729, Jun. 2011.

[6] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[7] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Jul. 2010.

[8] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310–325, Jan. 2012.

[9] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Trans. Signal Process.*, 2013, early Access.

[10] N. Zlatanov, R. Schober, and P. Popovski, "Throughput and diversity gain of buffer-aided relaying," in *Proc. Global Telecommunications Conference (GLOBECOM)*, Dec. 2011, pp. 1–6.

[11] 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.

[12] N. Zlatanov, R. Schober, and P. Popovski, "Buffer-aided relaying with adaptive link selection," *IEEE J. Sel. Areas Commun.*, 2013, early Access.

[13] 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.

[14] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Communications Letters*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

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

[16] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1591, Apr. 2009.